



*“Le potentiel
d'écosystème du
Campus Cyber
n'a pas encore été
pleinement
exploité”*

**Joffrey
Célestin-Urbain**
président du
Campus Cyber

**Le renouveau
de l'ERP**





Opérateur numérique souverain

—
INFRASTRUCTURE
PROPRIÉTAIRE
RÉSEAU, DATACENTERS
ET CLOUD PRIVÉ
IA-READY

CELESTE garantit un environnement souverain, sûr et protégé de bout en bout, avec un guichet unique. Datacenters localisés en France et en Suisse, indépendants vis-à-vis des puissances étrangères, non concernés par le Cloud Act.

5 Datacenters certifiés ISO 27001 et HDS
13 000 Km de fibre optique
15 Agences en France et en Suisse



www.celeste.fr
info@celeste.fr

RÉDACTION

88 boulevard de la Villette, 75019 Paris, France.
Tél. : +33 (0)1 74 70 16 30
contact@linformaticien.com

PRÉSIDENT, DIRECTEUR

DE LA PUBLICATION : Gaël Chervet

RÉDACTION : Bertrand Garé (rédacteur en chef)
et Victor Miget (rédacteur en chef adjoint)
avec : François Cointe, Olivier Bouzereau,
Patrick Brebion, Vincent Bussièrre, Christine Calais,
Jérôme Cartegini, Alain Clapaud, Michel Chotard,
Guillaume Renouard et Thierry Thaureaux.

SECRÉTAIRE DE RÉDACTION :

Amélie Ermenault Martin

MAQUETTE ET RÉALISATION :

Franck Soulier (chef de studio)

PUBLICITÉ :

Antoine Foulon
afoulon@linformaticien.com

VENTE AU NUMÉRO

France métropolitaine 8,50 € TTC (TVA 5,5 %)

ABONNEMENTS

France métropolitaine 72 € TTC (TVA 5,5 %)
magazine + numérique

Toutes les offres :

www.linformaticien.com/abonnement

Pour toute commande d'abonnement d'entreprise
ou d'administration avec règlement par mandat
administratif, adressez votre bon de commande à :

L'Informaticien, service abonnements,
88 boulevard de la Villette, 75019 Paris, France.
ou à abonnements@linformaticien.com

IMPRESSION

Imprimé en France par Imprimerie Chirat (42)
Dépôt légal : 1^{er} trimestre 2026

Toute reproduction intégrale, ou partielle, faite sans le consentement
de l'auteur ou de ses ayants droit ou ayants cause, est illicite
(article L122-4 du Code de la propriété intellectuelle).
Toute copie doit avoir l'accord du Centre français du droit de copie
(CFC), 20 rue des Grands-Augustins 75006 Paris. Cette publication
peut être exploitée dans le cadre de la formation permanente.
Toute utilisation à des fins commerciales de notre contenu éditorial fera
l'objet d'une demande préalable auprès du directeur de la publication.

L'INFORMATICIEN est publié par PC PRESSE,
S. A. S. au capital de 130 000 euros.
Siège social : 88 boulevard de la Villette,
75019 Paris, France.

ISSN 1637-5491

Une publication 

 **FICADE**

Édito

par Bertrand Garé
Rédacteur en chef

Le retour de l'ERP

Avec la montée en puissance de l'IA dans les entreprises, l'ERP, souvent vilipendé, retrouve une aura du fait de son rôle unique sur les données. Unique dans plusieurs aspects : comme source de données vérifiées et structurées, unique aussi par la centralisation des données dans un seul endroit sans avoir à réaliser de fastidieux travaux d'intégrations. Ceci, bien sûr, dans un monde idéal, car l'ERP n'est pas la seule application présente dans l'entreprise. Il reste cependant le juge de paix sur la « vérité » dans l'entreprise. Dans notre dossier, nous analysons ce retour en grâce de l'ERP et ses récentes évolutions.

Autre rendez-vous important de ce numéro, notre rencontre avec le dirigeant du Campus Cyber qui nous décrit la stratégie et la nouvelle orientation qu'il souhaite donner à ce lieu emblématique, afin de jouer un rôle clé dans la sensibilisation et le développement de la cyber sécurité dans notre pays.

Nous réalisons aussi un point important sur les conférences importantes de ce début de printemps : Cisco Live et la conférence de Dynatrace. Pourquoi mettre en avant ces deux conférences ? Tout simplement du fait de l'empreinte de leurs produits dans les entreprises, quelle que soit la taille de celles-ci. Vous retrouverez aussi l'ensemble de nos rubriques, avec une variété de sujets plus larges qu'auparavant, afin de mieux décrire et suivre sur ce qui se passe dans notre industrie.

Nous avons, de plus, apporté quelques ajustements dans notre nouvelle formule, pour parfaire la mue de notre magazine dans un esprit plus moderne et plus cohérente avec les canons actuels de la presse.

Enfin, l'Informaticien va s'agrandir avec deux HS dont le premier sera largement distribué sur le Forum Incyber qui se tiendra à Lille début avril. Le suivant est programmé pour le second semestre.

Sommaire

Mars 2026 — N°244

Biz'IT 6

Les actus du mois
Rachats et levées
de fonds
Partenariats



Dossier 12

Le renouveau de l'ERP



Rencontre 20

Jeffrey Célestin-Urbain,
président du Campus Cyber



Infra 26

Agrial renforce sa résilience
Unyc, un opérateur
pour unifier les flux
Que réserve le futur Wi-Fi 8 ?
Cisco prêt pour l'utilisation
future de l'IA
Renault fait appel à Exotec
Jabra adapte sa stratégie



Logiciel 41

e-Barreau sécurise
l'activité des avocats
Salesforce étend Mulesoft
Agent Fabric
BPCE bascule sur une
nouvelle GED sans vagues
Dynatrace Intelligence
veut rendre l'IA
opérationnelle enfin fiable
L'open source pour se libérer
de la dépendance
Le souverain
gagne du terrain
Comment mesurer la qualité
d'un code informatique ?
Surfshark analyse
la collecte de données par
les navigateurs mobiles



Écosystème 57

Maintenir dans la durée
la conformité RGPD
des données RH
Le mentoring ? Ça marche !
Des salaires en forte hausse
pour les experts
Hommage à Ada Lovelace
BloomUp, un guichet unique
des startups
Equinix réfléchit au SMR



CyberSec 67

GrapheneOS s'expatrie
hors de France
Generali teste un wallet
numérique
L'industrialisation silencieuse
des cyberattaques
La faille invisible
Le vibe coding, une aubaine
pour les cybercriminels ?
Compte rendu université AFCDP
Interview Philippe Salaün
AFCDP
ShadyPanda piège par
des extensions dormantes
Isoler pour sécuriser
la navigation web
Rencontre avec N. Passaquet

Abonnements... 66

Open-Flux

Notre solution ETL flexible
et 100 % paramétrable.



Disponible en version

On Cloud

et/ou

On Premise

Editeur **français** depuis 2012 et
+ de **200 Applications connectées !**

Actus du mois

Bénéfice net presque divisé par deux pour Bpifrance

Bpifrance annonce un niveau d'activité record en 2025, avec 72 milliards d'euros injectés dans l'économie française. La banque publique d'investissement enregistre toutefois un net recul de son bénéfice, affecté notamment par la baisse de performance d'entreprises du secteur des semi-conducteurs.

Malgré un contexte économique quelque peu morose, c'est une année de tous les records pour Bpifrance, à en croire son directeur général, Nicolas Dufoucq. La banque publique d'investissement française a rendu public, mardi 17 février, son bilan d'activité pour 2025.

Résultat : la banque indique avoir injecté 72 milliards d'euros dans l'économie tricolore. C'est 20 % de plus qu'en 2024 (60 milliards d'euros). La création de valeur pour 2025 est de 1,3 milliard d'euros, dont 876 millions en plus-values de cession de titres. C'est aussi un record historique de crédits, à environ 21 milliards d'euros en 2025. Ses fonds propres grimpent à 30 milliards d'euros, soit une hausse de 7 % par rapport à 2024.

L'industrie des semi-conducteurs à la traîne

Petite ombre au tableau toutefois, du côté du bénéfice net pour 2025, qui s'établit à 501 millions d'euros, contre 896 millions en 2024. Une baisse qui s'explique par trois « grumeaux », à savoir la baisse des performances du groupe automobile Stellantis, de Soitec, société française qui conçoit et produit des matériaux semi-conducteurs, et du fabricant de puces STMicroelectronics. Ces deux derniers, qui « marchaient fort jusqu'en 2023 », faisait remarquer Nicolas Dufoucq, pèsent à eux seuls pour

353 millions d'euros dans la baisse du résultat net de Bpifrance. Le produit net bancaire est en baisse de 14,4 %, à 1,8 milliard d'euros.

Fort soutien à l'IA

Globalement, les investissements dans le secteur des sociétés de la tech en 2025 ont atteint 385 millions d'euros (Avisia, Brevo, Hublo...). Dont 240 millions pour les seules entreprises d'IA, comme Mistral et Harmattan IA. Bpifrance a également créé une joint-venture avec MGX, Mistral et Nvidia pour le développement du « plus grand » campus IA d'Europe.

1,1 milliard d'euros a été investi pour financer l'innovation, dont 185 millions ont, par exemple, été fléchés vers les startups greentech. 1,5 milliard d'euros a en outre été déployé vers plus de 1 000 startups deeptech en 2025,

afin de renforcer « la souveraineté technologique française », dont plus de 700 millions d'euros sous la forme d'investissement direct ou de fonds de fonds. Bpifrance indique avoir accompagné une startup deeptech tricolore sur six en 2025. « Ces deeptechs atterrissent dans l'économie française », a assuré Nicolas Dufoucq.

Un plan France 2040 ?

Pour la période 2026-2030, la priorité de la banque publique demeurera l'industrie et le climat, avec 35 milliards d'euros déployés pour chacun. Suivront 10 milliards d'euros pour la santé, et 10 milliards d'euros pour développer l'IA et soutenir son appropriation par les entreprises.

Lors du bilan d'activité, Nicolas Dufoucq a aussi plaidé pour un plan France 2040, à la suite de France 2030, dont l'enveloppe restante est aujourd'hui d'environ 10 milliards d'euros. « On se bat pour qu'il y ait un France 2040 », a-t-il déclaré. Un plan de soutien à l'innovation française, jugé indispensable par le directeur général de la banque d'investissement, si la France veut espérer tenir tête à ses concurrents américains et chinois.



Capgemini vend sa filiale américaine

L'entreprise française de services informatiques a traversé une tempête médiatique. La cause ? La signature de contrats entre sa filiale américaine, Capgemini Government Services (CGS), et la police fédérale de l'immigration américaine, en charge de l'arrestation des immigrants illégaux. Plus connue sous l'acronyme ICE, elle est au cœur de nombreuses polémiques, notamment autour de ses méthodes musclées. C'est dans ce contexte que le média L'Observatoire des multinationales a révélé que Capgemini a été retenue pour un contrat de 4,8 millions de dollars (avec un plafond pouvant atteindre 365 millions de dollars) avec l'ICE.



0,4 % du CA de Capgemini

Ledit contrat vise à fournir des services de recherche de personnes (skip tracing), afin de localiser des étrangers en situation irrégulière. Le groupe gère également un standard téléphonique pour les victimes de crimes commis par des étrangers.

Capgemini a ainsi décidé de vendre sa filiale, précisant dans un court communiqué que « les contraintes légales habituelles imposées aux États-Unis pour contracter avec des entités fédérales menant des activités classifiées ne permettaient pas au Groupe d'exercer un contrôle approprié sur certains aspects des opérations de cette filiale ». Selon les chiffres de Capgemini, CGS représente 0,4 % du chiffre d'affaires du Groupe en 2025. L'impact sur les finances du groupe sera donc minime. Quid des conséquences sur sa réputation ?

La CNIL a infligé pour 487 millions d'euros d'amendes en 2025

En 2025, la CNIL a frappé durement. Au total, elle a rendu 259 décisions, dont 83 sanctions, pour un montant total de 486,8 millions d'euros d'amendes. Elle a en outre prononcé 143 mises en demeure et 31 rappels aux obligations légales. Les sanctions concernent des thèmes variés liés aux cookies, à la vidéosurveillance des salariés, à la sécurité des données, au défaut de coopération avec la CNIL, ou encore à la prospection politique et commerciale.

« Ces sanctions comportent 78 amendes (dont 27 avec injonction sous astreinte), trois décisions de liquidation d'astreinte (c'est-à-dire le paiement d'une somme en raison du non-respect d'un ordre donné par la CNIL dans sa décision de sanction) et deux rappels à l'ordre. Dix de ces décisions ont été rendues publiques », développe la CNIL. Le gendarme des données personnelles a notamment sanctionné deux acteurs majeurs à hauteur de 325 millions et de 150 millions d'euros.

2026 commence fort

En janvier, l'autorité a infligé une amende de 5 millions d'euros à France Travail, à la suite d'une fuite de données massive survenue en 2024. L'autorité reprochait à l'organisme public des mesures de sécurité jugées insuffisantes. Plus tôt dans le mois, elle a sévi contre une société restée anonyme, condamnée à verser 3,5 millions d'euros pour avoir transmis des données à un réseau social à des fins de ciblage publicitaire, entre autres.

Toujours en janvier, la CNIL a également rendu deux décisions à l'encontre de Free Mobile et de Free. Elle a respectivement prononcé des amendes de 27 et 15 millions d'euros, pour un montant total de 42 millions d'euros. Un contrôle de l'autorité avait mis en évidence des manquements à plusieurs obligations prévues par le règlement général sur la protection des données (RGPD).

Rachats



Semperis reprend MightyID, un spécialiste des identités Cloud

MightyID propose des capacités couvrant la sauvegarde, la restauration, la migration et le basculement des plateformes d'identité cloud, conçues pour garantir la continuité de l'authentification et des accès, même lorsque les systèmes principaux rencontrent des défaillances.

L'intégration de la solution dans la plateforme de Semperis apportera une gestion continue de l'exposition, afin de prévenir les attaques sophistiquées se propageant latéralement des systèmes d'identité on-premise vers les environnements cloud, ainsi qu'une remédiation automatisée des modifications malveillantes sur l'ensemble de l'environnement d'identité hybride, avec des capacités de reprise rapide et une gestion de crise clé en main.

NXO acquiert IDNA

L'acquisition d'IDNA vient renforcer l'offre et le positionnement de NXO sur les solutions de cybersécurité, en particulier sur les expertises d'audit et de conseil, la gestion du risque cyber, la sécurisation du Cloud et la sécurisation des environnements IT/OT.

IDNA sera une filiale de NXO et conservera son identité ainsi que son autonomie opérationnelle, afin de continuer à fournir les produits et services sur lesquels repose la confiance de ses clients, tout en développant de nouvelles synergies commerciales avec NXO. IDNA accompagne ses clients à 360° tout au long du cycle de gestion des risques cyber, en combinant audit, conseil stratégique, opérationnel et en gouvernance, mise en œuvre de solutions, ainsi que des services managés pour assurer le maintien en condition de sécurité.

Check Point renforce sa plateforme cyber avec trois acquisitions

Plateformisation renforcée pour Check Point, qui a annoncé l'acquisition de trois entreprises de cybersécurité : Cyclops, Cyata et Rotate. Leurs technologies respectives viendront renforcer la plateforme unifiée de Check Point.

Pour mémoire, Cyata a été fondée en 2024. Elle développe une plateforme de gestion des identités d'agents IA, afin d'aider les organisations à identifier les agents actifs, cartographier leurs autorisations, surveiller leur comportement et appliquer des politiques de sécurité automatisées. Fondée en 2021, Cyclops a conçu une plateforme de gestion de la surface d'attaque des actifs cyber (CAASM). Rotate propose une offre à destination des fournisseurs de services managés (MSP/MSPP), afin de renforcer la protection centralisée des environnements de travail distribués et des environnements SaaS.

Proofpoint acquiert Acuvity

Cette acquisition renforce la plateforme de Proofpoint avec une visibilité native sur l'IA, une gouvernance et une protection en temps réel des flux de travail pilotés par l'IA et les agents.

Acuvity apporte de nouveaux points de contrôle et des modèles de détection conçus spécifiquement pour l'IA. Sa plateforme offre une visibilité complète sur les usages de l'IA en entreprise, des points d'accès (endpoints) et navigateurs web aux infrastructures d'IA émergentes, telles que les serveurs du Protocole de Contexte de Modèle (MCP) et les outils d'IA installés localement comme OpenClaw et Ollama.

Combinée à des modèles de détection alimentés par l'IA, qui comprennent le contexte et l'intention, Acuvity permet aux organisations de gouverner et de sécuriser la manière dont les utilisateurs et les systèmes interagissent avec les services d'IA externes, tout en protégeant les modèles et applications d'IA personnalisés développés ou déployés au sein de l'entreprise.

Levées de fonds

Inférence : Positron AI lève 230 M\$

Positron AI a bouclé un tour de table de série B de 230 millions de dollars. Une opération qui porte sa valorisation à plus d'un milliard de dollars. Positron AI se présente comme un leader du matériel d'inférence IA à haute efficacité énergétique. Il travaille à apporter une réponse à la question de la disponibilité de l'énergie, un goulot d'étranglement dans le déploiement de l'IA. Pour ce faire, l'entreprise développe une puce qui offrirait cinq fois plus de tokens par watt sur les charges de travail principales, que le futur GPU Rubin de Nvidia, selon les déclarations de Positron AI.

Autre frein : la mémoire. Là encore, Positron se dit en mesure d'apporter une réponse adaptée, avec son silicium personnalisé Asimov. Attendu l'an prochain, il disposerait de plus de 2 304 Go de RAM par dispositif, contre 384 Go pour Rubin.



520 M\$ pour la startup d'IA et de robotique Apptronik

Face à l'engouement que suscite sa technologie, la société d'IA et de robotique humanoïde Apptronik a annoncé une levée de fonds de 520 millions de dollars dans le cadre d'une extension de sa série A. Avec ces nouveaux fonds, l'entreprise entend accélérer la mise sur le marché de son robot humanoïde Apollo, et étendre son réseau de déploiements commerciaux à l'échelle mondiale. Apptronik souhaite également investir dans des cas d'usage pour des secteurs spécifiques où son robot pourrait trouver des débouchés, comme le commerce de détail, la fabrication et la logistique. Elle ambitionne en outre de construire des installations dédiées à l'entraînement des robots et à la collecte de données.

À noter qu'elle prévoit aussi de s'appuyer sur son partenariat avec Google DeepMind, afin d'alimenter ses prochaines générations de robots via Gemini Robotics. Google avait en effet présenté en juin 2025 Gemini Robotics On-Device, un modèle vision-langage-action (VLA), conçu pour fonctionner localement sur des robots et exécuter des tâches précises.



Une levée de série C pour GitGuardian

Le fournisseur de solutions de protection des secrets et des identités non humaines (NHI) empoche 50 M\$. Le financement permet à GitGuardian de traiter la surface d'attaque connaissant la croissance la plus rapide dans les logiciels d'entreprise : les agents IA. La plateforme de GitGuardian s'étendra pour détecter, surveiller et gouverner les identifiants utilisés par les systèmes d'IA, des assistants de codage aux bots de service client. GitGuardian continuera à investir dans sa plateforme de sécurité des secrets à destination des grands comptes et développera des capacités complètes de gestion du cycle de vie des NHI conçues pour les entreprises gérant des dizaines de milliers d'identités non-humaines. Cela inclut la découverte automatisée, l'analyse d'utilisation, les politiques de rotation et les rapports de conformité à travers l'ensemble de l'écosystème de développement. GitGuardian accélérera son expansion aux États-Unis tout en ouvrant de nouvelles régions, dont la France.

LinkUp lève 10 M\$ et se rêve moteur de recherche des IA

La startup française LinkUp ambitionne de devenir le Google Search des agents IA. Elle a annoncé une levée de fonds d'amorçage de 10 millions de dollars, menée par Gradient, avec le soutien de fondateurs et investisseurs issus de Mistral, Datadog, Deel et Dataiku. Ce financement doit lui permettre d'accélérer le développement de son infrastructure de recherche web native, afin de donner aux systèmes d'IA un accès à des informations en ligne en temps réel, ainsi que de renforcer ses équipes d'ingénieurs et de chercheurs.

Partenariats

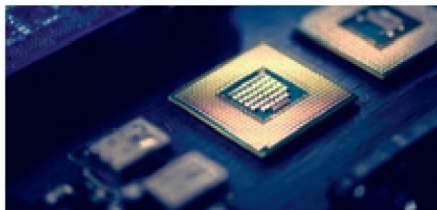
Capgemini étend son partenariat avec Google Cloud

Les deux entités amplifient leur alliance pour déployer des solutions « souveraines ». Capgemini aidera ainsi ses clients à adopter les principales technologies d'IA de Google Cloud, notamment Vertex AI et Gemini Enterprise.

Le partenariat accompagnera aussi les organisations dans l'utilisation des opérations cloud hyper-automatisées basées sur Gemini, afin d'améliorer la cybersécurité, la résilience, la reprise après sinistre et la conformité alignée sur les exigences de souveraineté. Les clients communs pourront choisir leur modèle de souveraineté parmi Google Cloud, Google Cloud Dedicated et Google Distributed Cloud (GDC) en environnement isolé (air-gapped).

Capgemini prévoit de créer une practice de delivery Google Sovereign Cloud, et un centre d'excellence (CoE) pour fournir des conseils et des services répondant aux exigences souveraines spécifiques des clients communs.

STMicroelectronics muscle son partenariat avec AWS



STMicroelectronics a annoncé l'extension de sa collaboration stratégique avec Amazon Web Services (AWS) dans le cadre d'un accord commercial pluriannuel de plusieurs milliards de dollars. Ce partenariat positionne STMicroelectronics comme fournisseur stratégique de technologies de semi-conducteurs avancées qui seront intégrées à l'infrastructure de calcul d'AWS, afin de proposer de nouvelles instances de calcul haute performance, plus efficaces et mieux adaptées aux charges de travail liées à l'IA et au cloud. L'accord prévoit également une collaboration autour de l'optimisation des charges de conception de puces dans le cloud, ainsi que l'émission de bons de souscription en faveur d'AWS.

Illumio s'allie avec Armis dans les environnements OT/IT

Avec l'ajout d'Illumio Insights, la relation entre Armis et Illumio va au-delà de la segmentation, en évoluant vers une capacité native qui simplifie les opérations et permet un confinement proactif.

Armis détecte et catégorise tous les appareils IT, OT et IoT — y compris les actifs non gérés et anciens — et partage cette classification avec la plateforme Illumio pour améliorer la visibilité et la cartographie. L'intelligence d'Armis alimente Illumio Insights afin de faire ressortir les opportunités de segmentation à fort impact. Illumio applique la micro-segmentation lorsque Armis détecte des anomalies, empêchant ainsi les mouvements latéraux. La télémétrie conjointe s'intègre aux flux de travail du SOC, aux systèmes SIEM et SOAR pour accélérer les enquêtes.

Illumio élargit sa collaboration avec Armis au-delà de la technologie, en alignant leurs stratégies commerciales pour faciliter l'accès des organisations à des solutions avancées de sécurité Zero Trust. Les efforts conjoints en matière de vente et de marketing garantissent aux clients une intégration fluide, des conseils d'experts et une approche unifiée de la protection des infrastructures critiques. Cette intégration est disponible pour les clients communs des deux entreprises.

Snowflake s'allie à OpenAI

Snowflake a annoncé un partenariat de 200 millions de dollars avec OpenAI. Celui-ci vise à intégrer des modèles avancés d'intelligence artificielle au sein de sa plateforme cloud de données. Cette collaboration doit permettre aux entreprises utilisatrices d'analyser leurs données, d'interroger leurs documents internes et d'automatiser des tâches complexes en langage naturel, tout en respectant des exigences strictes de sécurité et de gouvernance.

C'est l'évolution attendue pour 2026 en matière d'IA. Ce partenariat marque en effet une nouvelle étape dans l'évolution des usages de l'IA en entreprise, qui passent de simples chatbots à des agents intégrés capables de travailler directement sur des données propriétaires. L'offre est déjà utilisée par des clients comme Canva ou encore Whoop. Elle doit bientôt être disponible sur les principaux fournisseurs de cloud.



Partenariat entre TCS et AMD

TCS et AMD vont codévelopper des solutions d'IA et d'IA générative ciblées par secteur. Ils associeront l'expertise sectorielle et les capacités d'intégration de TCS à l'offre de calcul haute performance et d'intelligence artificielle d'AMD. Ensemble, les deux entreprises accompagneront les organisations dans la modernisation des environnements cloud hybrides et Edge, dans le déploiement d'espaces de travail augmentés par l'IA, ainsi que dans l'accélération des innovations sur des charges de travail du cloud à Edge. TCS s'engage par ailleurs à former et certifier rapidement ses équipes aux technologies matérielles et logicielles d'AMD.

Les deux groupes investiront conjointement dans le développement des talents afin de créer un vivier d'experts capables d'innover de concert et de livrer des solutions IA de nouvelle génération. Des cadres d'IA générative spécifiques aux industries seront élaborés pour des domaines tels que les sciences de la vie (découverte de médicaments), la fabrication (qualité cognitive et usines intelligentes) et le secteur bancaire, financier et de l'assurance (BFSI) pour la gestion intelligente des risques. Le partenariat prévoit également la mise à disposition d'accélérateurs, de frameworks et de bonnes pratiques adaptées pour optimiser les performances, tant pour les phases d'entraînement que d'inférence, afin que les organisations exploitent pleinement le potentiel de l'IA.

BMC collabore avec AWS pour 5 ans

Cette collaboration, qui combine l'expertise de BMC dans le domaine de l'automatisation intelligente à l'échelle et à l'agilité d'AWS, améliorera la manière dont les organisations orchestrent les données et les workflows, ouvrant la voie à de nouveaux niveaux d'agilité et d'innovation. Des clients issus de divers secteurs utilisent déjà BMC avec AWS pour une multitude de cas d'utilisation. BMC a choisi AWS comme fournisseur de cloud privilégié pour héberger la plateforme SaaS Control-M.



L'accord vise à apporter une modernisation plus rapide et une création de nouvelle valeur commerciale dans les environnements AWS grâce à des conseils intelligents, des informations automatisées et des recommandations contextuelles utilisant les capacités d'IA générative de BMC, notamment Jett, le conseiller génératif alimenté par l'IA de BMC dans la plateforme Control-M, ainsi qu'une accélération de la valeur client grâce aux capacités de gestion des données et d'IA agentique de BMC, fournies en natif sur AWS. La plateforme Control-M de BMC est disponible sur AWS Marketplace. Elle prend également toujours en charge l'orchestration unifiée de bout en bout des pipelines de données des clients sur des infrastructures hybrides complexes.

ÉVÉNEMENTS PARTENAIRES

IT&Cybersecurity One to One Meetings

17, 18 & 19 mars 2026

Palais des festivals et des congrès
de Cannes

1 Bd de la Croisette
06400 Cannes

Forum in Cyber

31 mars au 2 avril 2026

Lille Grand Palais
1 Bd des Cités Unies 59777 Lille
Euraille France

Cybersécurité solution IA.cloud

8 et 9 avril 2026

Parc des Expositions
1 Place de la Porte de Versailles
75015 Paris

Ready for IT

2 au 4 juin 2026

Grimaldi Forum
10 avenue Princesse Grâce
98000 Monaco



Dossier

Le renouveau de l'ERP

Si son importance dans les entreprises ne s'est jamais démentie, l'ERP avait un peu disparu des premières pages des gazettes. Il suffit de voir le nombre d'articles sur le sujet dans les années passées. Pour de multiples raisons, celui-ci revient sur le devant de la scène et connaît un renouveau qui se concrétise par de nombreux ajouts fonctionnels, mais aussi par une adaptation plus fine au contexte actuel des entreprises. Il intègre, de plus, les dernières tendances technologiques comme l'intelligence artificielle, même si, à l'image de cette technologie, l'adoption est encore peu effective. Tour d'horizon de ce renouveau et des nouvelles tendances pour cet ERP de nouvelle génération.

Une transformation accélérée

Les entreprises connaissent un contexte difficile, changeant, et le système d'information doit suivre. L'ERP connaît les mêmes tendances avec des entreprises qui recherchent de l'agilité, de la résilience opérationnelle et des automatisations pertinentes. Pour répondre, l'ERP connaît une transformation accélérée vers des plateformes Cloud plus modulaires intégrant l'intelligence artificielle.

« La seule chose dont les entreprises sont sûres aujourd'hui, c'est qu'elles ne sont sûres de rien », explique Hans Kourimsky, managing director France chez NTT DATA Business Solutions. Il ajoute : « elles savent aujourd'hui qu'elles ont besoin de flexibilité et qu'elles auront besoin de faire évoluer leur ERP, leurs process, beaucoup plus rapidement que ce qu'elles ont fait auparavant et que l'ERP qu'elles ont installé il y a 15-20 ans a été construit sur d'autres principes de plus grande stabilité ». Gilles Santene, associé technologie chez EY, estime lui que l'ERP vit un moment de transformation, une nouvelle étape après celle du début des années 2000, puis celle de l'arrivée du Cloud, avec l'intelligence artificielle.

S'il reste, dans certains logiciels, de vagues souvenirs du temps où le logiciel n'était là que pour fournir plus rapidement des plannings MRP, l'arrivée du Cloud et la mise en œuvre d'ERP plateforme, avec la volonté de couvrir toutes les lignes de métiers dans l'entreprise sont en fait des visions assez passées de ce qui reste la colonne vertébrale électroniques des organisations.

L'ERP Next Gen

L'ERP nouvelle génération n'est pas une nouvelle plateforme ERP, mais plutôt une stratégie et une approche qui tirent parti de la technologie low-code, de l'architecture composable, de l'intégration de normes ouvertes et des solutions

ERP existantes pour étendre les fonctionnalités, la flexibilité et l'agilité des solutions ERP existantes. La plupart des logiciels embarquent désormais ces différents ensembles.

Cette approche est totalement différente de celle que l'on a connue dans les décennies précédentes où les ERP dits étendus cherchaient à couvrir l'ensemble des fonctions de l'entreprise avec des modules pour la gestion de la relation client, de la fonction RH ou autres. Les éditeurs ont compris tout simplement qu'ils ne pourraient pas fournir un seul et unique socle pour les données de l'entreprise et qu'ils devraient rester ouverts pour travailler avec d'autres éditeurs souvent spécialisés sur un seul domaine, mais un domaine critique pour l'entreprise cliente.

Des projets stratégiques

La majorité des interviewés pour cet article ont relevé des temps de prise de décision assez long entre 9 et 12 mois avant de décider de la transformation de l'ERP de l'entreprise. Ce temps est cependant en forte diminution en comparaison des cycles de vente auparavant. De plus, les possibilités de déploiements dans le Cloud raccourcissent drastiquement le temps et les risques lors du déploiement du logiciel. Benjamin Louvet, directeur commercial groupe associé chez EBS Group explique : « La migration équivaut à changer d'outil, donc, si tous les outils historiques sont on-premise et s'ils ont un fonctionnel assez complexe



La seule chose dont les entreprises sont sûres aujourd'hui, c'est qu'elles ne sont sûres de rien.

Hans Kourimsky
managing director
France chez NTT
DATA Business
Solution

avec un historique de longue date et des spécifiques, cela remet vraiment tout en question. S'il s'agit de remettre 500 jours dans la migration d'un outil un tel vers un outil du même éditeur, je peux me poser la question de voir ce qui se fait aussi à côté, et si je décide de ne pas conserver un truc un peu plus généraliste en apposant un vertical dessus, là, il y a un sujet ». Hans Kourimsky ajoute : « la gestion des projets a changé. On n'est plus dans les effets tunnels qu'on a connus à une certaine époque, qui étaient quand même très compliqués, même si ce n'est toujours pas un

Benefits of Composable ERP



SPINNER
SUPPORT

Les avantages mis en avant de l'ERP composable

projet, ça n'est pas juste une nouvelle application qu'on met en place. Il y a autour tout un tas de stratégies organisationnelles ».

Infuser les bonnes pratiques

Stéphanie Magniez, experte digital finance chez Oracle France, précise : « Mon client a besoin de savoir si sa donnée est fiable, unique dans le référentiel, dans l'écosystème, et si elle est pertinente en temps réel. On va donc désiloter les fonctions en se servant de ces processus et en y adossant des bonnes pratiques. Je m'appuie sur la plateforme, je m'appuie sur ces bonnes pratiques embarquées pour optimiser, rationaliser ma façon de traiter les demandes d'achat jusqu'au paiement, les commandes de mes clients jusqu'à la constatation du revenu et la gestion des relances ».

Quand Stéphanie Magniez parle de bonnes pratiques, elles considèrent un socle commun à tout le monde dans un secteur d'activité en disant : « comment allez-vous pouvoir gérer de manière optimisée le cycle de vie de vos immobilisations et la possibilité,

ensuite, par paramétrages de personnaliser et enrichir le logiciel. Cela simplifie grandement l'usage du logiciel par la rationalisation de la bonne façon de manager le flux, du début à la fin d'un processus, tout en retirant les étapes intermédiaires qui étaient des spécificités, des complexités inutiles ». Là encore, Stéphanie Magniez risque de doucher quelques espoirs : « Nous avons fait des études pour le passage de clients sur site en mode SaaS. On commence par leur expliquer qu'il y a plein de choses qu'ils vont devoir abandonner. C'est toujours très difficile à comprendre, mais une fois qu'on leur a démontré que ça n'avait pas d'utilité, évidemment, ils adhèrent à cette bonne pratique et cela va beaucoup plus vite. »

Vers l'ERP composable

L'ERP composable mêle plusieurs concepts, parmi lesquels l'approche Best of Breed. Cette expression anglaise est littéralement traduisible par « le meilleur de la race ». Particulièrement utilisée dans le langage informatique et marketing, elle désigne la solution la plus performante dans un secteur spécifique ; on parle alors de « best of

breed solution ». Ainsi, l'objectif d'une approche Best of Breed est de comparer les différentes solutions logicielles disponibles, puis de choisir les meilleures en fonction de votre secteur d'activité et de votre stratégie d'entreprise. L'ERP composable peut s'adapter en temps réel à des besoins définis à l'instant T. De même, son système hybride prévoit l'installation à la fois sur site et sur le Cloud des applications. Cette flexibilité offre une solution pertinente et concrète aux contraintes imposées par l'industrie et par les multiples évolutions technologiques auxquelles sont confrontées les entreprises.

La base de données de l'entreprise

Un des principaux avantages de l'ERP est de pouvoir centraliser et unifier les données en un seul endroit pour l'ensemble de l'entreprise et, ainsi, fournir un socle robuste pour les données. Ce point est évidemment important alors que les entreprises souhaitent généraliser l'usage de l'intelligence artificielle à partir d'agents de plus en plus spécialisés.

B.G

Un marché toujours en croissance

Le marché de l'ERP connaît une croissance toujours importante et la tendance devrait durer dans les années à venir.

En 2024, le marché des ERP était évalué 60 milliards de dollars américains en 2024. Le marché devrait presque doubler pour atteindre 119 milliards de dollars américains d'ici 2030, soit un TCAC de 12,1 %. Cette croissance s'appuie sur la transition généralisée vers des architectures cloud natives, des plateformes modulaires et des capacités d'IA intégrées qui remodelent fondamentalement la manière dont les entreprises planifient, opèrent et rivalisent. Dans tous les secteurs et toutes les régions, l'ERP évolue

d'une infrastructure transactionnelle vers un catalyseur stratégique de la prise de décision basée sur les données. L'une des caractéristiques déterminantes de l'évolution du marché est l'adoption de plateformes ERP modulaires qui permettent le déploiement progressif de modules financiers, logistiques, RH et CRM. Cette modularité, associée à une tarification par abonnement, réduit les barrières à l'entrée et accélère le retour sur investissement, en particulier pour les entreprises de taille moyenne. Parallèlement, les

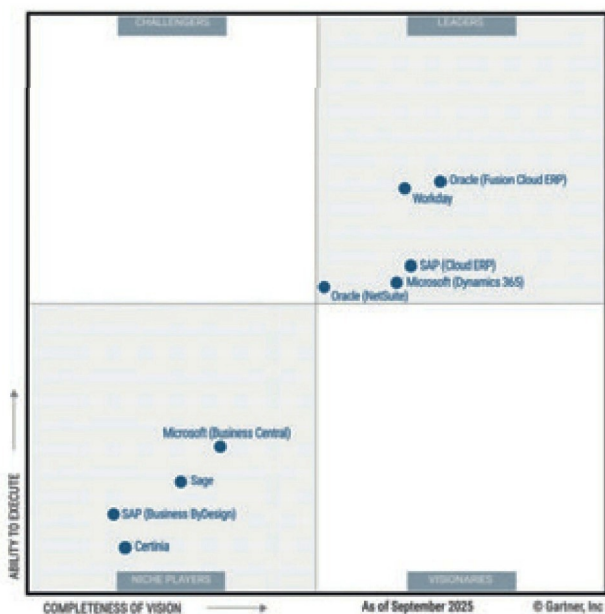
principaux fournisseurs tels que SAP, Oracle, Microsoft Dynamics, Infor et les challengers spécialisés dans des secteurs verticaux comme Epicor et IFS redoublent d'efforts en matière de solutions spécifiques à l'industrie, d'intégration de l'IA et d'innovation en matière d'expérience utilisateur, afin de répondre aux diverses demandes des clients. L'analyse prédictive intégrée, la détection des anomalies et l'automatisation intelligente ne sont plus des options, mais des composants essentiels des écosystèmes ERP de nouvelle génération. En 2024, l'Amérique du Nord était en tête du marché mondial des ERP avec une valeur de 22 milliards de dollars, soit 36,2 % du chiffre d'affaires mondial. Cette domination s'explique par la maturité du paysage informatique des entreprises de la région, la forte pénétration des ERP dans le cloud et son adoption précoce.

Le Cloud devient dominant

Les ERP basés sur le cloud ont dominé le marché en 2024, contribuant à hauteur de 65 % au chiffre d'affaires mondial. Cela reflète une transition généralisée vers les modèles SaaS qui offrent une évolutivité, un déploiement rapide et des capacités d'IA/ML intégrées. Les ERP cloud devraient également être le segment de déploiement qui connaîtra la croissance la plus rapide, avec un TCAC de 12,7 %, soutenu par les initiatives de transformation numérique à l'échelle de l'entreprise, l'adoption d'une architecture composable et une demande accrue de visibilité en temps réel et d'accès mobile. Les ERP sur site connaîtront une croissance plus modérée, mais resteront essentiels dans les secteurs soumis à des exigences strictes en matière de souveraineté des données et d'intégration des systèmes existants, tels que la défense, l'énergie et le secteur public.

Les grandes entreprises sont les premiers clients

Les grandes entreprises ont été les principaux clients des logiciels ERP en 2024, gérant 40 milliards de



Le Magic quadrant 2025 de Gartner pour les ERP dans le secteur des services

dollars, soit 67,2 % du marché total. Leurs investissements sont axés sur la transformation numérique à l'échelle mondiale, l'harmonisation réglementaire et l'optimisation intelligente des finances et de la chaîne d'approvisionnement. Cependant, les PME devraient

enregistrer la plus forte croissance, avec un TCAC de 13,4 %, dépassant ainsi les grandes entreprises. L'adoption par les PME est accélérée par les fournisseurs qui proposent des systèmes ERP modulaires à faible coût, dotés de fonctionnalités spécifiques à chaque

secteur, de frais de mise en œuvre réduits et d'une intelligence artificielle intégrée, répondant ainsi aux besoins des entreprises de taille moyenne qui recherchent agilité et rapidité de rentabilisation.

B.G

L'IA envahit les ERP

Pas une nouvelle communication sur l'ERP sans que l'intelligence artificielle ne soit mise en avant. Avec des agents, des modèles LLM, elle envahit l'ERP pour le rendre toujours efficace en automatisant les tâches récurrentes dans l'outil.

TVH Consulting, un intégrateur d'ERP SAP et Microsoft, perçoit une accélération significative autour de l'intelligence artificielle et de la data. Ce qui relevait encore récemment de l'effet de mode devient désormais concret. Leurs clients les sollicitent pour automatiser des tâches répétitives au sein de leur ERP, mais aussi pour bénéficier d'aides à la décision plus intelligentes. L'enjeu est de gagner en efficacité, d'anticiper, et même d'intégrer des données externes — via des outils comme Copilot, Joule ou les Agents — pour enrichir les analyses.

L'ERP devient alors un levier stratégique, bien au-delà de la simple gestion.

Apporter les promesses de l'ERP

Malgré des décennies d'investissements, les plateformes logicielles ERP ne parviennent souvent pas à offrir les gains d'efficacité opérationnelle et l'intelligence métier attendus. Plus de 80 % des transformations ERP continuent de dépasser les budgets, les délais et les objectifs de création de valeur, selon la dernière enquête de benchmarking de Bain & Company.

Hans Kourimsky précise : « *La première chose dont on parle quand il est question de l'IA, c'est la qualité des données. Et c'est pour ça qu'il y a ce très fort intérêt de l'IA pour les ERP, c'est que les ERP aujourd'hui sont la donnée la plus propre des entreprises* ».

Le potentiel d'automatisation de l'IA générative offre une voie de sortie. Si certains premiers cas d'usage se sont concentrés sur l'accélération des migrations ERP — en automatisant les tests, la correction du code ou la documentation — le véritable potentiel réside dans la création de « *plateformes sans intervention humaine* » alimentées par l'IA agentique, assure le cabinet de conseil.

Les éditeurs de plateformes se livrent une bataille pour façonner ce nouveau paysage, en proposant des outils prêts à l'emploi avec un certain niveau de personnalisation via des studios, qui convergent largement entre eux. Bien que ces produits soient encore à un stade précoce et qu'ils ne couvrent souvent que des cas d'usage limités, la tendance vers des agents plus avancés est claire.

Les impacts de l'IA

78 % des responsables IT s'attendent à ce qu'au moins une partie des fonctionnalités ERP soit remplacée ou augmentée par de l'IA agentique au cours des trois prochaines années. L'impact devrait être le plus visible dans les processus clés de finance et de planification. Les répondants à l'enquête ont identifié les processus procure-to-pay, record-to-report et forecast-to-plan comme les domaines ERP les plus susceptibles de vite bénéficier de l'automatisation agentique.



Ils ont envie de déployer l'IA, de faire des choses avec.

Gilles Santene, associé technologie chez EY

Toujours selon l'étude précitée, les DSI peuvent choisir de s'associer aux éditeurs de plateformes lorsque les cas d'usage concernent des workflows standard et non critiques, confinés à un seul système, permettant rapidité et efficacité à moindre coût. À l'inverse, l'achat auprès d'un spécialiste tiers peut être pertinent lorsque la capacité recherchée est une commodité peu complexe, afin de gagner en traction sans investissement lourd. Enfin, le développement interne est souvent le plus approprié pour des processus transverses à fort impact, générateurs de différenciation



C'est la combinaison des différents types d'IA qui permet aujourd'hui de pouvoir sortir les premiers indicateurs réels et tangibles.

Stéphanie Magniez
experte digital finance
chez Oracle France

IBM Enterprise Advantage en bref

IBM Enterprise Advantage réunit l'expertise technique et sectorielle des consultants IBM avec la technologie développée issue d'IBM Consulting Advantage, la plateforme interne d'IBM alimentée par l'intelligence artificielle. Avec un nombre croissant d'agents et d'applications IA spécifiques à chaque secteur, IBM Consulting Advantage a déjà accompagné plus de 150 missions clients, et a démontré sa capacité à augmenter la productivité des consultants jusqu'à 50 %, permettant ainsi aux clients d'obtenir des résultats plus rapidement.

Les entreprises peuvent s'appuyer sur la plateforme pour repenser leurs workflows, connecter l'IA à leurs systèmes existants et déployer à grande échelle de nouvelles applications agentiques sans avoir à modifier leurs fournisseurs cloud, leurs modèles d'IA ou leur infrastructure centrale. Cela inclut Amazon Web Services, Google Cloud, Microsoft Azure, IBM watsonx, et les modèles open source et closed source, permettant ainsi aux entreprises de tirer parti de leurs investissements existants.

concurrentielle, lorsque le contrôle total justifie des délais plus longs et des coûts plus élevés.

En pratique

Stéphanie Magniez indique : « on a commencé l'IA il y a plusieurs années, avec de l'IA prédictive, de l'IA générative, de l'IA agentique, et les clients vont activer ce qui a du sens pour eux. C'est la combinaison de ces différents types d'IA qui permet aujourd'hui de pouvoir sortir les premiers indicateurs réels et tangibles de ce que fait gagner l'IA à nos clients en termes de productivité, parce qu'on aura mesuré l'utilisation de ces différents use case d'IA, avec les temps qui vont se dégager en termes de gains ». Benjamin Louvet constate : « tout le monde n'est pas encore à jour pour pouvoir avoir des softs qui embarquent directement de l'IA. Je dirais que c'est pour l'instant encore minoritaire, mais ça rentre aussi dans les réflexions ». Pour Gilles Santene de chez EY, « ils ont envie de déployer l'IA, de faire des choses avec, mais ils se demandent s'ils le font en étant bridés, en se contentant de ce qu'ils ont, ou s'ils le font de manière plus puissante, quitte à engager un projet de modernisation et avoir un hébergement qui leur permet d'aller plus loin ».

Xavier Ory, VP & senior partner IBM

Consulting France, fait une distinction autour de l'intelligence artificielle : « l'IA à destination des consultants redéfinit leur manière de travailler, l'IA à destination des métiers, elle, utilise les ERP. Je traite les deux de manière séparée. SAP a commencé à structurer son approche d'IA de cette même manière, c'est-à-dire qu'il y a joules for consultants, joules for developers et joules for business. C'est leur pas vers l'agentique. Joules for business, je le mets dans la catégorie agentique. Il y a parfois un abus de langage pour désigner, quand on parle d'agentique, ce qu'on va rajouter au-dessus de l'ERP pour redéfinir son interface utilisateur et la manière d'interagir avec l'utilisateur final. La demande des clients qui lancent des projets ou qui ont déjà des choses existantes, c'est de construire les fondamentaux d'une architecture qui permettent de faire de l'agentique. Il faut de la donnée et que cette donnée soit correctement travaillée. C'est en général la donnée de l'ERP qu'on va combiner avec d'autres données qui vont venir sur des systèmes satellites et qu'on va agréger sous le format de ce qu'on appelle des data products. Les data products, ce sont des cubes avec lesquels on va constituer des briques qu'on va retrouver dans des technologies de type data lake ».

B.G

Des annonces et mises en œuvre récentes

Lors des dernières semaines, de nouveaux produits et annonces de déploiement ont démontré le rôle encore important que jouent les ERP dans les entreprises.

AODOcs a certifié son connecteur pour SAP S4 / Hana. Ce connecteur permet une intégration directe et certifiée entre AODOcs et SAP. Les fonctionnalités d'intelligence artificielle d'AODOcs facilitent la recherche dans les documents liés à SAP, et en automatisent la classification, l'extraction de données, la revue et le résumé, transformant ces fichiers en données exploitables. L'intégration directe d'AODOcs élimine le besoin de développements spécifiques au sein de SAP ; elle réduit à long terme le coût de maintenance et réduit la complexité des projets de migration ou de mise à jour. De plus, elle garantit une traçabilité complète (audit-ready) des données, un contrôle rigoureux et une gestion fine des permissions, tout en respectant les processus SAP existants.

Wandercraft choisit Open-Prod

Fondée en 2012, Wandercraft est mondialement reconnue pour avoir créé le premier exosquelette de marche autoéquilibré au monde, Atalante X, utilisé dans plus de 100 centres de rééducation et de recherche sur quatre continents pour aider les patients à effectuer plus d'un million de pas chaque mois. Jusqu'en 2021, Wandercraft fonctionnait sans ERP, en s'appuyant sur des outils bureautiques. Avec l'augmentation des volumes de production et les contraintes réglementaires du secteur médical, Wandercraft devait disposer d'un système capable de gérer l'ensemble des flux de manière fiable. L'entreprise avait besoin d'un outil unique pour regrouper les données d'achats, de

production et de stocks, assurer la traçabilité complète des pièces et des non-conformités, et sécuriser les processus conformément aux exigences de la norme ISO 13485.

Après un benchmark conduit par la direction financière, Wandercraft a retenu Open-Prod, solution française open source, proposant toutes les fonctionnalités dont ils avaient besoin. Le projet a été conduit en collaboration avec ILife, partenaire intégrateur d'Open-Prod. Spécialiste des environnements industriels, ILife a accompagné Wandercraft dans le cadrage du besoin, le paramétrage de l'outil et la conduite du changement auprès des équipes. Cette collaboration étroite a permis un déploiement rapide et maîtrisé, en phase avec les exigences du secteur médical. Le

déploiement s'est effectué en quelques mois, avec un go-live fin 2021, puis des extensions fonctionnelles ont été apportées, notamment la gestion de la maintenance en 2023. Wandercraft engage une nouvelle étape dans la structuration de son système d'information. L'entreprise prévoit d'étendre l'usage d'Open-Prod à de nouveaux périmètres. Un module de GMAO et une gestion centralisée des réclamations clients sont en préparation. Ces développements permettront d'améliorer le suivi du cycle de vie des produits, de la fabrication à la maintenance, et de consolider la traçabilité des interventions. L'objectif est de disposer d'une vision complète et fiable du fonctionnement des exosquelettes sur le terrain. Par ailleurs, l'entreprise prévoit d'intégrer la gestion multi-sociétés pour inclure sa filiale américaine, ainsi qu'un WMS pour optimiser les entrepôts et les flux de production. L'ajout d'un configurateur de nomenclatures et de gammes viendra soutenir l'industrialisation des futurs modèles. Ces chantiers, programmés pour 2026, accompagneront la croissance internationale de l'entreprise et la maîtrise de la qualité sur l'ensemble de ses produits.

B.G



“Le potentiel d'écosystème du Campus Cyber n'a pas été pleinement exploité”

**Joffrey Célestin-Urbain, président
du Campus Cyber**

Après près de vingt ans passés au sein de l'État, notamment à Bercy et à la tête du Sisse (Service de l'information stratégique et de la sécurité économique), Joffrey Célestin-Urbain a rejoint le Campus Cyber en qualité de président. Son ambition : transformer une jeune structure en écosystème opérationnel. Avec L'Informaticien, il revient sur la feuille de route centrée sur la structuration de l'écosystème, la coopération entre acteurs et les enjeux de souveraineté européenne.

Qu'est-ce qui vous a mené à œuvrer dans le domaine de la cybersécurité ?

J.C.-U. : Je me suis spécialisé dans la thématique de la souveraineté économique, à travers mes précédents postes à Bercy (ministère de l'Économie et des Finances), à la fois au Trésor, qui est l'une des directions de Bercy, puis à la direction générale des entreprises.

Mon dernier poste avant le Campus Cyber, qui peut illustrer le pourquoi, était celui de directeur du Sisse, le service de l'information stratégique et de la sécurité économique. Il fait office de tour de contrôle de tous les actes de prédation étrangère sur des entreprises, des laboratoires et des données sensibles françaises. Il y avait un prolongement naturel entre ce que je faisais à Bercy et le Campus Cyber.

Au sein du Sisse, j'ai pu mesurer toute l'étendue de l'agressivité des acteurs étatiques et économiques étrangers, qui

ne reculent devant rien pour tourner les rapports de force géoéconomiques à leur avantage. Ils ont recours à tout un arsenal d'instruments, parmi lesquels la cybercriminalité. Cela a été une expérience fondatrice parce que, sur ce type de poste, l'on prend vraiment conscience de la face cachée de la mondialisation. Comme dans *Stranger Things*, il y a un monde à l'envers qui m'a ouvert les yeux. C'était une prise de conscience : nous étions en danger et il fallait changer de logiciel économique pour bâtir des capacités de cybersécurité européennes mutualisées à la hauteur de la menace.



Aujourd'hui, le Campus Cyber affiche 90 % de surfaces louées. L'enjeu est de s'appuyer sur ce taux pour dynamiser l'écosystème.



Est-ce ce défi qui vous a fait accepter ce poste ?

J.C.-U. : Ce que je recherche, ce sont justement les défis. Et celui du Campus Cyber est gigantesque. C'est une société privée qui doit faire du profit, mais en même temps, qui travaille sur une thématique d'intérêt général. Au Campus Cyber, je retrouve ce même enjeu de transformation. Il faut parvenir à changer de braquet dans une structure créée en 2022, qui doit évoluer vers un modèle beaucoup plus affirmé et ambitieux.

Quelles sont les atouts et points faibles du Campus Cyber ?

J.C.-U. : Sa grande force, c'est d'avoir réussi à rassembler les principaux acteurs de la cybersécurité française en un seul et même endroit. D'où une grande diversité : il y a des établissements de formation, des associations, des organismes de recherche, des services de l'État, des entreprises de toute taille, issues de l'offre de cybersécurité ou de la demande. Sur le papier, nous avons déjà un bel écosystème.

La principale faiblesse est que, jusqu'à présent, le potentiel d'écosystème du Campus Cyber n'a pas été pleinement exploité. Il faut parvenir à créer une communauté qui coopère et nourrisse des projets communs.

C'est ce que vous évoquiez lors de votre intervention aux dernières Assises de la cybersécurité 2025 à Monaco : le niveau de performance est encore insuffisant. Comment faire pour passer à la vitesse supérieure ?

J.C.-U. : Il faut arriver à honorer la promesse de valeur du Campus en générant un retour sur investissement pour tous

les résidents et membres qui y ont investi de l'argent. Ils ont pris un ticket pour être aux avant-postes hyperdynamiques. Où est cet écosystème ? C'est toute l'ambition de notre nouvelle feuille de route.

Le principal objectif pour 2026 est de faire émerger cet écosystème coopératif et d'orchestrer son émergence en créant un cadre propice aux interactions. Si vous laissez les gens faire naturellement, spontanément, le niveau de coopération ne sera pas optimal. Il y a toujours la tentation de se dire : *« J'arrive à 9 h le matin, je prends l'ascenseur, mon café, je me retranche derrière mon bureau et je sors à 18 h, sans avoir croisé personne. »*

Pour nous, l'enjeu est de favoriser des circuits de rencontres balisés entre les différents acteurs et qu'ils ne reposent pas sur la seule initiative personnelle. C'est important, car c'est ce qui nous différencie fondamentalement d'un espace de coworking. Il n'y a pas d'équivalent de Campus Cyber aussi intégré, aussi divers que celui-là. C'est une chance sur laquelle nous devons capitaliser.

Donc, les entreprises au sein du Campus Cyber, bien que parfois directement en concurrence, doivent travailler ensemble ?

J.C.-U. : La cybersécurité française a des enjeux et des problématiques communes qui appellent des solutions collectives. La souveraineté, par exemple, mais aussi la formation. Sur ce dernier point, il faut faire en sorte que les étudiants formés ici, sur le Campus, ou ailleurs en France trouvent des débouchés à la hauteur de leurs compétences. Sur le plan de la recherche, nous devons créer des synergies entre les acteurs publics et privés. Partout, il y a des problématiques appelant des réponses autour de chaînes de valeur. Et nous, nous sommes en capacité de réunir, à chaque fois, différentes catégories d'acteurs pour répondre à ces problématiques, à des cas d'usage identifiés et sous des angles différents.

Comment cette approche pourrait-elle s'articuler sur un sujet comme la souveraineté ?

J.C.-U. : Très concrètement, à travers des groupes de travail destinés à favoriser les échanges entre des RSSI : certains expliqueront pourquoi ils n'ont encore rien mis en place, tandis que d'autres partageront leur retour d'expérience, leurs

“ Il faut parvenir à créer une communauté qui coopère et nourrisse des projets communs ”

expérimentations et les résultats observés. On crée une dynamique collective d'action, pas de parole.

Il s'agit donc d'abord d'essayer de comprendre, à travers ces groupes de travail, qu'est-ce qui empêche aujourd'hui un RSSI d'acheter plus massivement de l'EDR français, du firewall français, de l'IA française, ou encore de la sécurisation des identités allemande ou espagnole. Il y a une variété de paramètres qui empêchent aujourd'hui un RSSI d'acheter davantage français ou européen, et il faut arriver à les déceler et à les résoudre ensemble, sur le Campus.

Ces différents paramètres doivent être hiérarchisés, puis « débunkés » méthodiquement, afin de proposer aux RSSI des solutions — typiquement, des solutions issues des entreprises de l'offre. C'est de l'interfaçage intelligent sur des cas d'usage bien identifiés. En embarquant dès le départ dans cette démarche structurée les offreurs de solutions de cybersécurité, également largement représentés dans l'écosystème du Campus.

La thématique de la souveraineté a vraiment été montée en sauce au niveau politique. Ce qui manquait jusqu'à présent, c'étaient des exemples concrets de sociétés qui basculent, qui disent vouloir « réduire [leur] dépendance aux Américains et faire avec plus de solutions françaises », et dont l'exemple peut être transposé à large échelle. Nous pensons que le Campus Cyber peut être une caisse de résonance pour ces cas concrets.

Face à une offre pléthorique, comment accompagner les entreprises et les RSSI dans leurs choix en matière de cybersécurité ?

J.C.-U. : Nous avons la chance d'être dans un pays où l'offre existe. Mais si nous voulons démocratiser la cyber, auprès des PME par exemple, il va falloir les aider à naviguer. Notre force (du Campus, ndlr), c'est que nous sommes un opérateur de confiance, donc ce que nous allons proposer aux entreprises sera naturellement pris en compte.

“ Si nous voulons démocratiser la cyber, auprès des PME par exemple, il va falloir les aider à naviguer ”



Le Campus Cyber organise des groupes de travail destinés à favoriser les échanges et les retours d'expérience entre des RSSI.

Le rôle du campus n'est pas de les fléchier vers des entreprises en particulier, il faut rester neutres, mais on peut au moins les orienter — c'est l'objectif de la plateforme NIS2 — vers des paniers d'offres en fonction de leurs besoins réglementaires, de gestion des risques, etc. En face de chaque catégorie de besoins seront présentées telles ou telles offres. À eux d'arrêter leur choix ensuite.

Concernant votre feuille de route, quels vont être les grands chantiers prioritaires que vous avez lancés ou allez lancer ?

En 2026, notre priorité est de faire en sorte que nos résidents soient heureux. Et ils ne le seront que s'ils ont le sentiment de faire partie d'un écosystème qui se vit, s'opère, se conçoit comme tel, où il se passe des choses comme nulle part ailleurs.

Nous avons déjà commencé en mettant en place une gouvernance dédiée à leurs besoins qui n'ont jamais été véritablement canalisés et exprimés jusqu'à aujourd'hui. Nous avons donc mis sur pied une sorte d'assemblée générale des résidents où, pendant deux heures, nous les écoutons.

Nous rencontrons les résidents tous les trois mois et mettons, à chaque fois, la liste à jour de leurs doléances et desiderata, avec des solutions. Cela peut aller du changement d'une ampoule à des questionnements sur la manière de participer à des groupes de travail. C'est basique certes, mais la satisfaction client est au cœur de notre objectif. Le Campus Cyber est une entreprise, et il faut que nos résidents soient heureux. Car un résident heureux est un résident qui reste, voire qui revient — certains nous ont quittés par le passé.

Et pour 2027 ?

En 2027, nous souhaitons créer trois nouveaux services qui font défaut actuellement. Il s'agit d'abord d'une plateforme d'accompagnement NIS2 pour les PME et pour les collectivités locales concernées, afin qu'elles augmentent leur niveau de maturité cyber.

Le deuxième service est une forge de croissance des entreprises technologiques de la cyber. L'idée ? Que les bribes d'accompagnement des nouvelles startups qui se créent dans le secteur et dans le numérique de confiance soient orchestrées de manière cohérente, selon une chaîne continue, des premiers stades de l'entrepreneuriat à l'accélération sur les marchés européens. Troisième élément, développer une infrastructure de recherche et d'innovation, avec de l'intelligence artificielle, une infrastructure cyber mutualisée..., qui serait ouverte à tout l'écosystème, le but étant que startups et chercheurs se l'approprient. En 2026-2027, nous avons aussi l'Europe comme fil conducteur commun. Nous voulons développer au maximum les relations entre l'écosystème cyber français et ceux des autres pays européens, qui sont rarement aussi bien structurés qu'en France. Plus concrètement, créer un réseau des Campus Cyber en Europe pour que les écosystèmes se connaissent et qu'à terme, des clients allemands puissent se tourner naturellement vers des entreprises françaises pour leurs besoins cyber, et inversement. On ne peut pas espérer que l'Europe se peigne aux seules couleurs de la France, il faut que les clients français fassent confiance aux solutions européennes. C'est ça, la préférence européenne.

La préférence européenne peut-elle tenir face à l'attractivité du financement américain ?

J.C.-U. : Il faut décloisonner les écosystèmes européens en créant une communauté d'investisseurs locaux permettant de réunir des montants suffisamment importants pour concurrencer les Américains. Si une startup cherche à réunir un montant qu'elle n'arrive pas à lever en France, il faut que nous soyons capables de mobiliser des fonds européens. Selon l'organisation européenne ECSO, le marché européen de la cyber devrait passer de 63 milliards de dollars à environ 105 milliards de dollars d'ici 2030. Imaginons que ces 40 milliards de dollars supplémentaires profitent uniquement à des entreprises européennes. Vous allez avoir des entreprises dont

“ Nous voulons développer au maximum les relations entre l'écosystème cyber français et ceux des autres pays européens ”

les business models vont exploser ; il va falloir être en mesure de les accompagner financièrement. L'enjeu des ressources repose sur notre capacité à scaler l'offre (passage à l'échelle). Si, demain, le marché européen devait être réservé aux acteurs européens, nous devons créer les conditions pour que des géants émergent et que les fonds d'investissement suivent.

Est-ce qu'il y a une décision difficile, voire impopulaire, que vous seriez prêt à prendre pour faire avancer le Campus Cyber ?

J.CU : L'orientation vers plus de souveraineté. Le Campus Cyber se lance, mais c'est un saut dans le vide. C'est facile de dire qu'il faut être souverain : politiquement, on ne prend pas de risque. En revanche, obtenir des résultats est beaucoup plus compliqué. Je ne sais pas dans quelle mesure la dynamique que nous allons lancer va se traduire par des décisions de grands groupes ou d'administrations publiques en faveur d'un sourcing (approvisionnement) plus français.

Autre aspect, il faut faire comprendre à tout le monde, y compris au sein du Campus, que l'on fait partie d'un écosystème et ce n'est pas juste nous qui allons le décréter depuis le treizième étage de la tour. Chacun est partie prenante, a sa responsabilité et sa pierre à apporter à l'édifice. Et cela implique de contribuer à la dynamique.

Au regard de quels indicateurs pourriez-vous dire que votre présidence a été un succès ou non ?

J.CU : Encore une fois, je reste attaché au taux de satisfaction des clients : si les gens sont heureux, ils restent. Aujourd'hui, nous sommes à 90 % de mètres carrés loués. Il faut que ces mètres carrés soient doublés d'humains sur place et d'engagement dans l'écosystème.



Selon l'organisation européenne ECSO, le marché européen de la cyber devrait peser environ 105 milliards de dollars d'ici 2030, contre 63 milliards de dollars aujourd'hui.

“ Si nous restons face à une large part de marché américaine sur la cybersécurité ou sur d'autres secteurs, nous serons balayés ”

Ensuite, serons-nous parvenus à créer une dynamique qui permette à la filière cyber française de répondre aux besoins ? Quelle sera l'évolution de la part de marché de nos entreprises ? Sommes-nous parvenus à créer des champions ? C'est existentiel pour l'Europe. Si nous restons face à une large part de marché américaine sur la cybersécurité ou sur d'autres secteurs, nous serons balayés, car l'emprise numérique des États-Unis leur donne un pouvoir d'extinction de l'économie européenne qui est gigantesque.

En cybersécurité, la pénurie de talents est régulièrement évoquée comme un problème structurel. Selon vous, où se situent les blocages et quels leviers permettraient d'y remédier ?

J.CU : L'intelligence artificielle est un sujet dimensionnant. On peut imaginer que l'IA supprimerait une partie du déficit de compétences, simplement parce qu'on aurait moins besoin d'humains sur un certain nombre de tâches. Je pense que les estimations qui circulent dans les études de marché sont plutôt sous-estimées, et le mouvement sera massif, y compris en cybersécurité.

Nous avons d'ores et déjà de l'IA pour aider les analystes de SOC, diminuer le nombre de faux positifs et les épauler dans l'analyse.

Nous pouvons donc imaginer, dans un scénario très pessimiste pour la race humaine — mais optimiste d'un point de vue instrumental —, que le déficit de compétences soit comblé parce que le robot prendra le relais. Je ne suis pas sûr que ce soit un avenir très désirable.

À l'autre bout du spectre, dans l'hypothèse où l'IA ne suffira pas à combler le manque de bras, il va plutôt falloir identifier précisément où se situe la rareté des profils. Il y a un enjeu RH qui va consister à comprendre où se

trouvent les goulets d'étranglement, où il y a plus d'étudiants que de demandes, et où, inversement, il y a des pénuries. Cela nous permettra, à nous, Campus Cyber, d'alerter les établissements de formation afin qu'ils s'adaptent en fonction des besoins.

Face à une menace cyber en accélération, notamment avec l'IA, la réponse technologique suffit-elle encore ou le problème est-il ailleurs ?

J.CU : Nous ne pourrions jamais dire que nous sommes parfaitement en sécurité. Par définition, la menace est évolutive : on ne peut pas exclure que demain émerge un nouveau type de menace sur une vulnérabilité non identifiée. D'autant que nous sommes dans une phase d'accélération de la menace avec l'IA. Il y a beaucoup de fantasmes, mais aussi des craintes justifiées sur les bouleversements qu'elle va engendrer. Pas tellement sur la nature de la menace, mais plutôt sur l'échelle et sur la vitesse. Les organisations vont être confrontées à une vitesse d'exécution et à une échelle bien différentes. Mais je pense qu'il ne faut pas tomber dans le piège de l'approche technologiste de la cyber et se dire que la technologie répondra à tout.

Il s'agit aussi de sujets de gouvernance, d'adoption de la cybersécurité comme élément majeur d'une stratégie de gestion des risques en entreprise. Nous devons avoir un ensemble de règles et de pratiques internes qui, en plus de nos outils, nous permettent d'être protégés de manière satisfaisante.

Il y a un vrai enjeu de massification de la cybersécurité en France et en Europe, mais nous n'en sommes encore qu'au début. Finalement, NIS2 doit nous faire passer d'un monde où la cybersécurité était réservée à quelques acteurs critiques, à un monde où chacun devient, en quelque sorte, un acteur critique.

V.M



Il va être nécessaire de déterminer où se situe précisément la rareté des profils. Le Campus Cyber pourra ainsi se rapprocher des établissements de formation afin qu'ils adaptent leurs cursus.

Cybersécurité des PME : quand l'empilement d'outils devient un risque structurel

Par Benoît Grunemwald, expert en cybersécurité chez ESET France

La cybersécurité des PME s'est construite pendant longtemps par couches successives, au gré des évolutions technologiques. Ce qui s'est souvent traduit par un antivirus d'abord, puis un pare-feu plus robuste jusqu'à une solution EDR. Et le schéma s'est souvent répété tant sur la messagerie que sur la sauvegarde ou la protection des accès distants. À chaque nouvelle menace ou exigence, une solution supplémentaire est venue s'ajouter à l'existant. Si l'intention était bonne, le résultat l'est beaucoup moins.

Sur le terrain, cette accumulation a créé des environnements devenus difficiles à lire et à piloter. Trop de consoles, d'alertes et surtout trop peu de temps pour comprendre ce qu'il se passe réellement lors d'un incident. La multiplication des exigences réglementaires contribue à cette complexité, en incitant souvent à répondre par l'ajout d'un outil de plus plutôt que par une remise en perspective.

C'est aussi bien là tout le paradoxe de la situation : jamais les entreprises n'ont disposé d'autant de technologies de protection, et pourtant le sentiment de vulnérabilité progresse. Non pas parce que les outils soient inefficaces, mais parce que leur empilement crée une complexité que peu d'organisations peuvent absorber voire maîtriser.

Empiler des outils, ce n'est donc pas renforcer sa sécurité. Mais plutôt additionner des angles morts et prendre le risque que les signaux faibles passent sous le radar. Pourtant c'est aussi cette réalité que de plus en plus de dirigeants découvrent après coup, lorsque survient l'incident qu'aucune console n'a vraiment su anticiper. Le risque n'est donc pas technologique, mais structurel. Et il pose une question simple et désormais centrale : comment reprendre le contrôle sur un système de sécurité devenu trop fragmenté pour être fiable ?

Reprendre le contrôle : construire une sécurité lisible et exploitable

Face à un système de sécurité devenu trop fragmenté pour être fiable, il s'agit donc avant tout de retrouver de la lisibilité. Autrement dit, comment passer d'une accumulation défensive à une stratégie réellement pilotable.

Cela commence par une décision structurante : réduire la dispersion. Concrètement, c'est à dire de limiter le nombre d'outils,

rationaliser les solutions existantes et concentrer les signaux de sécurité dans un point de pilotage unique. Les journaux, alertes et comportements suspects doivent être analysés ensemble, d'un même tenant, et non plus isolément. Sans cette consolidation, les incidents continueront d'être traités comme des événements indépendants, alors qu'ils s'inscrivent le plus souvent dans une chaîne d'attaque.

Le deuxième levier, souvent sous-estimé : la réduction du bruit. Une sécurité efficace ne repose pas sur la multiplication des alertes, mais sur leur qualification. Cela implique de filtrer en amont, de corréler les événements et de faire remonter uniquement ce qui nécessite une décision ou une action. Une alerte sans contexte ralentit plus qu'elle ne protège.

Cette exigence de lisibilité impose aussi d'associer la technologie à une supervision humaine. L'automatisation et l'IA sont devenues indispensables pour traiter des volumes croissants de données, mais elles atteignent vite leurs limites sans interprétation. La présence d'analystes capables de contextualiser, de prioriser et d'intervenir transforme une détection brute en

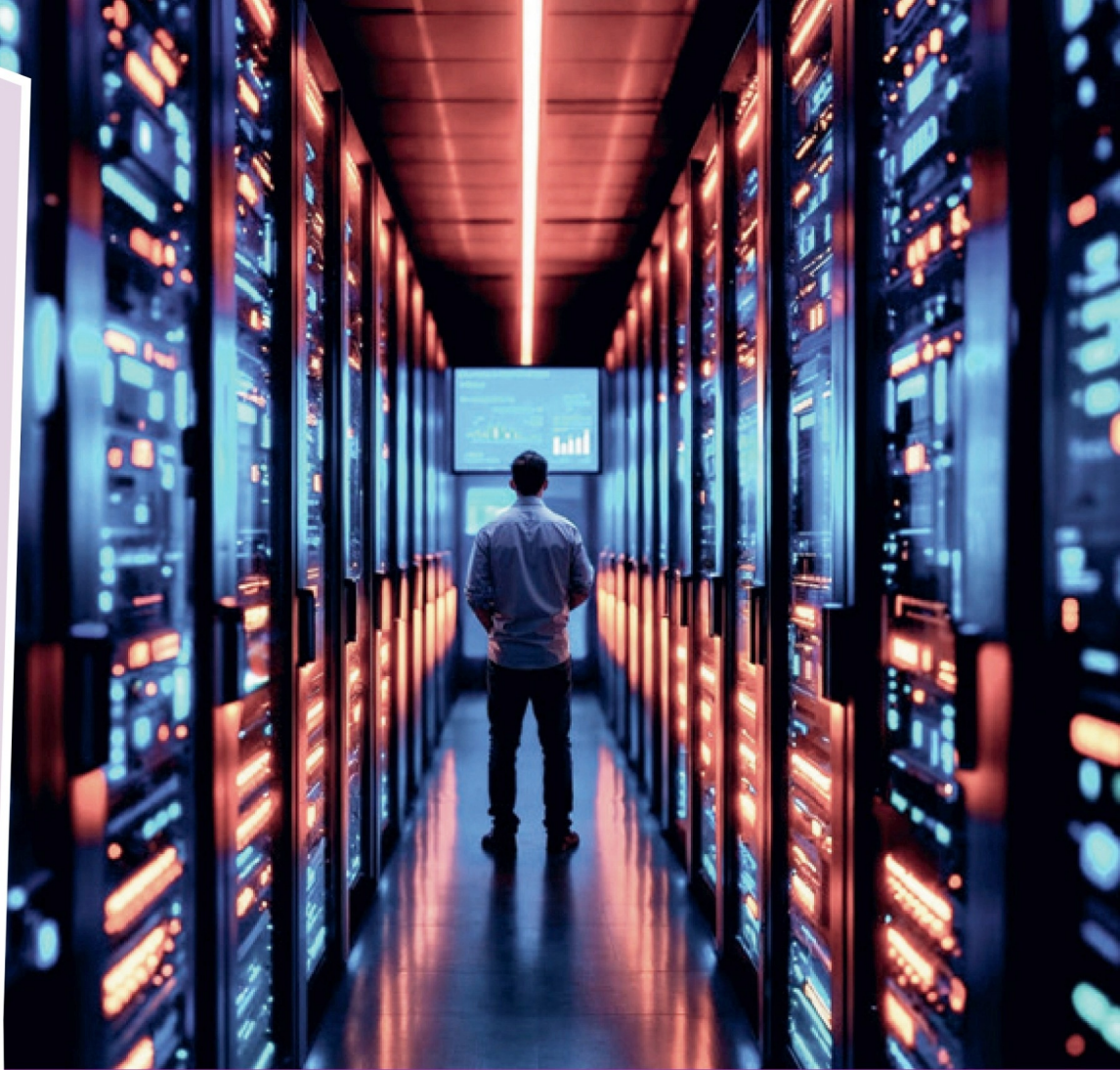
réponse opérationnelle. Si l'IA peut détecter, c'est bien l'humain qui comprend et décide au bout de la chaîne.

Enfin, cette approche permet de reprendre la main sur le pilotage global, y compris sur le coût réel de la cybersécurité dans le temps. En s'appuyant sur une plateforme homogène plutôt que sur une juxtaposition de solutions spécialisées, on vise alors la réduction du nombre d'outils à maintenir, tout comme du volume de formations nécessaires ou la complexité des opérations quotidiennes. Le TCO ne se joue plus uniquement à l'achat, mais bien sur

la durée à travers la capacité à exploiter les outils, à faire évoluer la sécurité sans remise à plat permanente et à éviter les surcoûts liés à la multiplication des prestataires.

À ce titre, s'appuyer sur un éditeur principal, doté d'une couverture fonctionnelle large, change la donne : moins d'interlocuteurs à coordonner, moins de ruptures entre solutions et donc moins d'usine à gaz. L'entreprise maximise ainsi la valeur de ce qu'elle déploie, tout en renforçant ses chances d'être au niveau sur la conformité, notamment en produisant plus facilement les éléments qui prouvent les mesures en place. Elle gagne aussi en anticipation et en capacité de réaction. Lorsqu'un incident survient, disposer d'un point central cohérent accélère la décision et la réponse. Dans ce cadre, la conformité cesse d'être un objectif traité à part puisqu'elle devient la conséquence naturelle d'une sécurité lisible, pilotable et maîtrisée.





Infra

Les sujets de ce mois sont tournés vers l'avenir avec les technologies encore dans les cartons comme le Wifi 8 ou la vision de Jabra, qui prédit que la voix va prendre un rôle de plus en plus important dans les modes de travail, mais aussi comment les constructeurs comme Cisco se préparent pour la nouvelle vague de flux de données du fait de l'IA.

Marketing

Pure Storage se donne une nouvelle identité

Pour marquer son pivot vers la gestion des données et non plus le simple stockage, Pure Storage change de nom et devient EverPure, contraction du nom de son offre Evergreen et de son nom d'origine.



Le fournisseur de solutions de stockage avait entamé sa mue avec la mise en œuvre de son architecture Enterprise Data Cloud et l'adaptabilité de Evergreen, ce qui permet de transformer le stockage en un cloud de données unifié et virtualisé, gouverné par un plan de contrôle dans le Cloud. Fonctionnellement, la solution gère les ensembles de données à l'échelle mondiale via des politiques, éliminant les frictions liées aux configurations manuelles, et apporte simplicité, agilité et efficacité à la gestion des données.

Une nouvelle acquisition

Outre ce changement de nom, l'entreprise a annoncé le rachat de l'ITouch. L'acquisition étendra les capacités de gestion des données de Everpure en ajoutant des capacités de découverte et de contextualisation sémantique des données à la plateforme. En intégrant le stockage aux capacités de l'ITouch d'identification, de classification, de contextualisation et d'enrichissement des données, sur l'ensemble des jeux de données et dans tous les environnements, du SaaS à l'edge, Everpure garantira que les données d'entreprise soient intrinsèquement prêtes pour l'IA dès leur création.

Cela permettra aux organisations d'accélérer la transformation de leurs données brutes en informations exploitables. La transaction est soumise aux conditions de clôture usuelles et sa finalisation est prévue au deuxième trimestre de l'exercice 2027. Les modalités de la transaction ne sont pas divulguées.

En droite ligne d'Accelerate

Cette annonce est la conséquence logique de celles faites lors de la dernière conférence de Pure Storage et de la disponibilité d'Enterprise Data Cloud. L'architecture Enterprise Data Cloud de Pure Storage fournit une architecture et un modèle

opérationnel unifiés qui assurent un contrôle complet des données, l'automatisation et la cyber-résilience dans tout type d'environnement. La plateforme Pure Storage permet la mobilité, l'agilité et la cohérence des données dans les infrastructures distribuées, pour l'ensemble du spectre des workloads et des protocoles d'une entreprise. Pure Storage propose désormais une extension majeure de l'Enterprise Data Cloud vers le cloud public, avec Pure Storage Cloud. Un plan de contrôle intelligent est le cerveau de la plateforme Pure Storage : une couche de contrôle unifiée qui automatise la manière dont les données sont provisionnées, protégées et gérées dans l'ensemble du parc de données. L'intégration de Portworx avec Pure Fusion permet aux entreprises de conserver une plateforme unique pour la gestion des données et du stockage de toutes les charges de travail. Cela étend de puissantes capacités de gestion de flotte aux applications cloud-native conteneurisées et aux machines virtuelles basées sur Kubevirt, dans tout environnement, sur site ou en cloud hybride.

B.G

Un nouvel Impact Report

L'Impact Report 2025 s'ouvre sur l'intelligence artificielle. L'essor de l'IA transforme l'économie mondiale, entraîne une hausse de la consommation électrique des datacenters à des niveaux inédits et met en lumière des enjeux immédiats de capacité des réseaux, de sécurité énergétique et de coûts. Le rapport projette que la demande d'électricité des datacenters fera plus que doubler d'ici 2030, en partie portée par l'intelligence artificielle. L'entreprise indique qu'en FY25, elle a plus que doublé la densité de ses produits avec l'introduction des DirectFlash Modules (DFMs) 150TB, des optimisations de l'environnement d'exploitation et une refonte du châssis, sans augmentation de la consommation électrique.

Robotique

Renault fait appel à Exotec

C'est le lillois Exotec qui a fourni les 191 robots déployés par Renault dans son entrepôt de Villeroy dans l'Yonne. Une myriade de robots Skypod va inlassablement chercher les pièces détachées commandées par les clients de la marque dans d'immenses racks. Cette solution de « Good to men » constitue une petite révolution dans le domaine du stockage.

© Crochet Guillaume / EXOTEC



Le système Skypod installé par Exotec à Villeroy gère 19 000 références de pièces (SKU) et stocke 3,3 millions de pièces. En 2025, il a servi 3,5 millions de demandes.

L'installation est imposante : des racks contenant des milliers de cellules dans lesquelles sont stockées 3,3 millions de pièces détachées de 19 000 références différentes. Dans ses allées, toute la journée, 191 robots font des allers et retours, et grimpent en haut des racks pour aller chercher des bacs dans lesquels se trouvent les pièces réclamées par les agents qui préparent les commandes. Ceux-ci récupèrent les pièces dans les 14 stations de picking. Pour regarnir le stock, le système fonctionne dans l'autre sens. Les robots viennent à la station de picking avec les bons bacs pour que l'opérateur y place les pièces à stocker.

Villeroy est l'un des trois sites de stockage de Renault Group en France. Créé en 2006, cet entrepôt occupe pas moins de 152 000 m². C'est un élément clé dans la logistique de l'industriel. Pour robotiser ce site, le choix d'Exotec a été réalisé à l'issue d'une compétition avec d'autres roboticiens. Ses robots Skypod sont déjà mis en œuvre par CDDiscount et Leclerc en France, mais aussi Uniqlo au Japon et PepsiCo aux États-Unis, qui en comptent plus de 500 dans ses sites logistiques.

Si Amazon exploite ses robots Kiva pour déplacer des armoires contenant les produits dans ses entrepôts, l'atout clé du robots Skypod est de pouvoir se

déplacer non pas seulement en deux dimensions dans l'entrepôt pour aller chercher un bac, mais aussi verticalement. Celui-ci grimpe le long du rack jusqu'à la bonne cellule. Il extrait le bac de la cellule et le redescend pour l'amener jusqu'à l'opérateur à la bonne station de picking. Cette caractéristique fait toute la différence à Villeroy car l'entrepôt offre une hauteur sous plafond de 11 mètres, ce qui permet de stocker énormément de pièces au m².

Un déploiement mené en six mois seulement

Xavier Lhors, directeur de la logistique après-vente de Renault Group, raconte le défi qu'a représenté la mise en production de l'installation : « Nous sommes parvenus à déployer cette infrastructure en six mois seulement et atteindre les 28 000 lignes d'ordres dès le huitième mois ». L'objectif fixé est de traiter la première ligne de commande avant la fin de l'année 2023 et le ramp-up devait être achevé en juin. Dès le début du mois de décembre l'objectif était atteint. « Nous avons bien entendu fait quelques erreurs au début, et nous passons plus de temps à nourrir la machine que récupérer des pièces. Nous avons travaillé avec Exotec pour mettre en place les bonnes mesures et réussi à tenir le plan de montée en charge. »

Renault a fait le choix d'un contrat « full service » : l'industriel achète au fournisseur de robots la disponibilité de son stock de pièces. Exotec qui assure la maintenance complète du système et le suivi en temps réel des allées et venues des robots sur les écrans géants des centres de contrôle du roboticien en 24/7 à Wasquehal, près de Lille. Ce centre fonctionne en « Follow the Sun » avec ses équivalents à Atlanta et Tokyo. De là, les techniciens d'Exotec supervisent l'ensemble des flottes de robots et peuvent identifier le moindre problème

et déclencher une intervention si le dépannage à distance n'est pas suffisant. Outre le volet purement technique, l'équipe projet a dû particulièrement soigner le volet conduite du changement car le déploiement des robots suscite bien évidemment beaucoup d'appréhension auprès du personnel en place. « *Le projet fait partie d'un plan de transformation et l'activité que nous apportons à Villeroy était jusqu'à présent sur d'autres sites* », argumente Xavier Lhors. « *La solution apporte donc plus d'activité et de salariés sur le site. Cela dit, il ne faut pas négliger la conduite du changement dans ce type de projet*. » L'équipe a communiqué auprès du personnel du site et fait venir des clients visiter l'entrepôt, l'objectif étant d'améliorer la qualité des services.

Pour Xavier Lhors, le taux d'acceptation du projet par les salariés a été une surprise. « *Nous avons réalisé un vote sur qui veut travailler avec la machine et qui ne le souhaite pas. Presque 100 % des gens étaient d'accord pour travailler avec les robots plutôt que de retourner à des tâches plus traditionnelles*. » Le responsable souligne le niveau d'engagement des employés du site qui n'est plus le projet « Exotec », mais a été rebaptisé en interne comme le projet Renault-Villeroy Automation.

Un retour sur investissement inférieur à deux ans

Les résultats engrangés depuis la mise



Les robots apportent les bacs contenant les pièces détachées aux opérateurs chargés du picking. Le site de Villeroy dispose de 14 stations de picking.

en production de l'installation sont très significatifs. Le picking d'une pièce dans l'entrepôt pour la préparer pour le client demandait deux heures en moyenne. Avec Exotec, ce délai est ramené à 15 minutes seulement. L'objectif n'était pas seulement d'aller plus vite, mais aussi de mieux servir les clients du centre logistique. L'heure limite de fin de prise de commande a pu être décalée d'une heure grâce à l'installation robotisée. De même, les robots ont permis de diviser par 3 les erreurs de comptage. En outre, Renault Group annonce une réduction de 30 % de la consommation énergétique par rapport aux équipements de manutention classiques.

Autre atout du Skypod, la densité de stockage dans ses racks. Celle-ci a permis à Renault de rapatrier sur le site de Villeroy ses deux autres entrepôts de stockage français sans avoir à agrandir le bâtiment existant. Le système gère 19 000 SKU (références produits) à lui seul, soit 3,3 millions de pièces stockées, et a servi 3,5 millions de demandes en 2025. Sur le plan de la disponibilité, la solution est très innovante, mais elle a aussi démontré sa fiabilité. En 2025, les 191 robots ont parcouru 2 millions de kilomètres. Le ROI réellement constaté a été inférieur à deux ans.

Une deuxième installation prévue en Allemagne

Évoquant l'avenir, Xavier Lhors souligne que l'installation peut encore être étendue par ajout de nouveaux modules. L'entrepôt de Villeroy dispose d'assez d'espace pour étendre l'installation si l'activité le demande. Le responsable ajoute : « *Ce n'est que la première étape d'une stratégie de modernisation de l'ensemble de notre logistique en France, mais aussi pour servir nos clients dans le monde entier. Une installation similaire va être réalisée en Allemagne dans les mois à venir*. » Un autre appel d'offres a été lancé pour cette nouvelle installation et c'est une nouvelle fois Exotec qui a été choisi. « *Nous n'avons pas d'accord cadre avec Exotec, mais nous avons été ravis de ce choix* », commente Xavier Lhors. « *Forts de notre expérience à Villeroy, nous allons pouvoir préparer le ramp-up du site allemand avec plus de sérénité et envoyer des experts de France pour préparer le démarrage*. » Cette installation est amenée à gérer 25 000 SKU avec 85 robots et traiter jusqu'à 7 000 lignes de commande par jour. Ce nouveau succès pour Exotec montre aussi la flexibilité de son Skypod, car les mêmes robots peuvent servir 13 000 lignes par jour en France, mais aussi 7 000 lignes par jour avec une installation plus petite. Il suffit d'accroître ou réduire le nombre de robots en fonction du niveau d'activité visé.

A.C



191 robots Skypod s'activent dans l'installation mise en place par Exotec sur le site Renault Group de Villeroy. Il s'agit de la version 1 du robot mis au point par le Français.

EXPOSITION • CONFERENCES • ATELIERS

FORUM
CYBERSÉCURITÉ
SOLUTIONS IA.CLOUD



Digital Workplace
documation 

CYBER - IA - CLOUD
PROCESSUS DOCUMENTAIRE
COLLABORATIF - INTRANET
SOLUTIONS MÉTIERS



8 et 9 avril 2026
PARIS EXPO - PORTE DE VERSAILLES

En parallèle :



Gold Sponsor



Silver Sponsor



Réservez dès maintenant
votre badge gratuit sur :

salon-cloud-security.com
salon-intranet.com
documation.fr

PALAIS DES FESTIVALS ET DES CONGRÈS DE CANNES

**THE ONE TO ONE MEETINGS EXHIBITION
OF CYBERSECURITY SOLUTIONS,
NETWORKS, TELECOM, MOBILITY,
CLOUD COMPUTING, DATACENTER
AND ITS AI SOLUTIONS**

THEY ARE ALREADY REGISTERED



List of registered exhibitors as of 26/01/2026

Convergence

Unyc, un opérateur pour unifier les flux

Entre télécoms, cloud, cybersécurité et explosion des usages IoT, les systèmes d'information se sont construits par strates successives, souvent au prix d'une perte de lisibilité. Pour répondre à cette fragmentation devenue critique, Unyc revendique un positionnement d'opérateur IT unifié, capable d'agréger, d'orchestrer et de piloter les services comme un ensemble cohérent.

Longtemps perçue comme une richesse, la multiplication des solutions IT est a contrario aujourd'hui source de complexité. Les DSI et RSSI doivent gérer une mosaïque de fournisseurs, d'outils de supervision et de contrats, avec des responsabilités parfois floues en cas d'incident. « *Les entreprises ne veulent plus empiler des briques technologiques, elles attendent des résultats concrets, mesurables et pilotables* »,

observe Arnaud Gautier, directeur des offres Cloud & IT chez Unyc. Cette problématique est particulièrement sensible sur le terrain de la cybersécurité. Une majorité de TPE-PME reconnaît ne pas être préparée à une cyberattaque, tandis que les cadres réglementaires, de NIS2 à DORA, étendent la responsabilité sécuritaire à l'ensemble de la chaîne de sous-traitance. Dans ce contexte, la fragmentation devient un facteur de risque autant qu'un frein opérationnel. Marque indirecte du Groupe Inherent, Unyc s'adresse avant tout

aux intégrateurs et MSP (Managed Service Providers). Le groupe, qui rassemble également Adista, Upper-Link et Devensys, fédère près de 400 collaborateurs pour environ 350 millions d'euros de chiffre d'affaires en 2025. « *Unyc est la marque qui permet à nos partenaires de consommer des services IT, télécom et cyber via une interface unique, afin de construire leurs propres offres clés en main* », précise Arnaud Gautier. Cette logique se matérialise

dans la plateforme Atlas, véritable colonne vertébrale du modèle Unyc. Elle permet de commander, déployer, superviser et facturer les services depuis un point de contrôle centralisé.

La convergence IT, télécom et cyber

La nouvelle offre EDR d'Unyc illustre cette volonté de convergence. Développée avec Acronis et intégrée nativement à Atlas, elle va au-delà de l'antivirus traditionnel en combinant détection comportementale, investigation et remédiation automatisée. « *LEDR apporte une couche de protection active, simple à déployer et adaptée à la réalité opérationnelle des organisations* », souligne Arnaud Gautier. La solution répond également aux exigences croissantes de souveraineté des données. Même logique côté IoT et M2M, où la fragmentation est souvent encore plus marquée. Unyc propose une offre de connectivité multi-réseau en France, capable de s'appuyer automatiquement sur le meilleur signal disponible, et une solution de roaming permanent en Europe conforme aux contraintes réglementaires. « *L'IoT est une extension naturelle du savoir-faire de nos partenaires. En leur donnant accès aux bonnes technologies, nous leur permettons d'adresser ce marché* »,

explique Victor Macri, chef de produit téléphonie mobile et M2M-IoT. Cette approche globale, de la SIM au pilotage des usages, s'inscrit pleinement dans la convergence IT, télécom et cyber voulue par Unyc. À mesure que les entreprises recherchent simplicité, responsabilité globale et engagements sur les résultats, le modèle MSP s'impose comme une réponse structurée à la fragmentation. En misant sur l'agrégation technologique, la souveraineté des données et l'autonomie des partenaires, Unyc entend bien accompagner cette mutation de fond.

J.C



Victor Macri (à gauche) et Arnaud Gautier de Unyc, sur le salon IT Partners 2026, à Paris

Stockage

Agrial renforce sa résilience

Regroupant 12 000 agriculteurs, Agrial est une coopérative agricole basée à Caen. En 2019, sa branche agriculture a dit adieu à VMware et a modernisé son infrastructure de sauvegarde. Un choix gagnant alors que la résilience du système d'information est plus que jamais capitale pour l'activité de l'entreprise.

Avec 17 500 collaborateurs, la coopérative basée à Caen est un géant de l'agroalimentaire. La branche agricole qui regroupe les producteurs a mené une réflexion sur la modernisation de son système d'information. Celui-ci avait été mis en place en 2014 et s'appuyait essentiellement sur 200 VM ESXi VMware, des SAN IBM entièrement équipés de disques durs et une sauvegarde TSM (Tivoli Storage Manager). 80 % des VM sont des machines sous Windows, pour 20 % sous Linux. « *Même s'il était adapté à nos besoins, ce système d'information était peu évolutif. Il était compliqué de le faire évoluer et nos capacités de reconstruction étaient excessivement limitées* », explique Mathieu Lemoigne, responsable infrastructure et réseau d'Agrial.

« Nous sauvegardions les enveloppes des VM avec une temporalité qui n'était pas très élevée et nous mettions beaucoup de temps à restaurer les données. L'outil ne permettait pas de chercher les fichiers directement à l'intérieur des VM. »

Le manque d'ergonomie et d'efficacité de la solution va pousser le responsable à chercher une solution pour accompagner les évolutions futures du système d'information de la coopérative. « *Nous avons essayé de réfléchir à quels seront les besoins du futur système d'information de la coopérative.* » Alors que les serveurs étaient déployés pour 10 ans, le cycle de vie des applications s'est accéléré et implique des mises à jour bien plus fréquentes. Enfin, la problématique de cybersécurité a poussé la branche agriculture à moderniser son système d'information.

En 2019, la piste du cloud public est écartée, mais à la suite d'un appel d'offres, la décision est prise de sortir de l'infrastructure VMware pour aller vers la solution d'infrastructure hyperconvergente de Nutanix. « *Nous avons remplacé notre SAN et éliminé toute la complexité de notre infrastructure. D'un rack complet, nous sommes passés à un demi-rack, avec des économies d'énergie à la clé* », commente Mathieu Lemoigne. Pour les sauvegardes, son choix se porte sur la solution Commvault qui bénéficie à l'époque d'une interface Web bien plus moderne et qui implémente une gestion des ACL que n'offrait pas TSM : « *Nous pouvons enfin savoir qui fait quoi avec l'outil et ne pas laisser les sauvegardes ouvertes à toute l'équipe d'administrateurs. Nous avons maintenant des référents qui ont en charge de restaurer ou d'administrer la plateforme.* »

Une des fonctionnalités les plus appréciées est de pouvoir enfin restaurer des fichiers à l'intérieur d'une VM. La capacité de restauration cross hyperviseur de Commvault va s'avérer particulièrement intéressante dans le cadre de la migration de la branche Agriculture d'Agrial de VMware vers Nutanix.

Cette migration a commencé en juin 2020, en plein confinement. Le passage de TSM vers Commvault a même été un peu précipité, car l'agent TSM ne fonctionnait pas sous Nutanix. « *Nous avons donc lancé le backup de l'ensemble du datacenter à 19 h le soir, et le lendemain matin, tout était fait. 25 To de données ont été sauvegardées dans la nuit sur un seul Media Agent, ce qui est une très bonne performance.* » Autre bonne surprise, la déduplication qui atteint un taux de 80 %, ce qui a permis de gagner énormément sur le stockage. TSM a été arrêté dans le mois qui a suivi. Enfin, une troisième copie des données est réalisée sur Metallic, le service de sauvegarde cloud de Commvault.



Chez Agrial, la résilience n'est pas un vain mot : pour sa branche légume seule, chaque jour d'arrêt correspond à une perte de chiffre d'affaires de 2,5 millions d'euros...



Agrial gère 11 filières de production, quatre filières de transformation et cinq réseaux de distribution. La coopérative est connue au travers de ses 68 marques, dont le cidre Loïc Raison, le fromage de chèvre Soignon, les boissons au lait Danao, les salades en sachet Florette.

Pour réduire le risque, la migration des machines virtuelles s'est effectuée dans un premier temps de VMware sur Nutanix, avant de les migrer vers AHV, l'hyperviseur de Nutanix. Lors de cette phase, l'infrastructure de sauvegarde a été mise à profit pour certains workloads : « *Nutanix donne d'excellents outils de migration, mais ceux-ci ne font pas tout* », précise le responsable des infrastructures. « *Ce fut notamment le cas des appliances IBM HMC, de même que Quest Software et quelques autres machines dont les OS étaient obsolètes.* »

Une plateforme de sauvegarde dont la couverture s'élargit

Depuis cette migration, l'infrastructure de sauvegarde a notamment été mise en œuvre pour la restauration d'une base de production Oracle, victime d'une corruption de données. En moins de 24 heures, la base qui fait quelques To de données a été remontée dans son intégralité.

Depuis, le champ d'action de la sauvegarde s'est élargi à Microsoft 365. À partir de 2020, les serveurs de fichiers ont peu à peu basculé sur la plateforme cloud, mais en 2022, Matthieu Lemoigne alerte son DSI sur l'absence de sauvegarde de cette infrastructure. Si Microsoft garantit la disponibilité des données sur leur infrastructure, le

responsable a préféré prendre ses précautions et activer les sauvegardes de Commvault en mode SaaS to SaaS. Il s'agit à la fois de préserver les données contre les ransomwares et les cyberattaques, avec le risque de voir des données critiques effacées en cas d'accès illicite.

« *Nous devons aussi tenir compte du facteur humain et d'une suppression accidentelle. Il est déjà arrivé qu'un utilisateur supprime tout ou partie d'un SharePoint.* » Matthieu Lemoigne estime que les mécanismes d'historisation fournis par Microsoft sont insuffisants, raison pour laquelle il préfère ne pas se reposer dessus pour garantir la résilience des données Microsoft 365. Début 2025, les données de la branche Légumes ont été intégrées aux sauvegardes Commvault dans le cadre d'une rationalisation qui doit voir les SI des cinq branches du groupe converger vers un seul. Il a suffi d'installer deux Media Agents dans deux salles serveurs pour mettre en place la sauvegarde en quelques clics.

Agrial s'apprête à fusionner avec Terrena, une coopérative du Grand Ouest, d'ici la fin de l'année. Cette autre coopérative exploite aussi Commvault pour ses sauvegardes, ce qui devrait simplifier la fusion sur ce volet.

A.C



Nous avons fait un audit l'année dernière sur nos capacités de reconstruction. Nous sommes au milieu du gué. Nous devons encore progresser, mais une coopérative

agricole n'a pas des taux de marge élevés. Nous devons le faire à notre rythme, mais nous arrivons à sensibiliser la direction et à obtenir des budgets.

Matthieu Lemoigne

responsable infrastructure et réseau d'Agrial



Réseau

Que réserve le futur Wi-Fi 8 ?

Il ne doit arriver sur le marché qu'en 2028 et pourtant les annonces se multiplient à propos du 802.11bn, plus communément appelé Wi-Fi 8. Les fabricants de puces, Broadcom et MediaTek en tête, ont présenté des composants compatibles, et les premières bornes sont apparues lors du CES. Pendant que l'industrie se met en ordre de bataille, les capacités de la nouvelle norme réseau sont désormais connues.

Le Wi-Fi 7 est loin d'être déployé dans tous les foyers et dans toutes les entreprises, mais les industriels travaillent déjà sur sa prochaine évolution, le Wi-Fi 8. Plusieurs constructeurs devraient dévoiler des prototypes lors du Mobile World Congress de Barcelone. Déjà, en octobre dernier, Broadcom dévoilait une gamme de composants Wi-Fi 8 pour les passerelles Wi-Fi résidentielles, les box opérateurs, les points d'accès d'entreprise et les terminaux. La production n'était pas encore lancée, mais les premiers échantillons allaient être livrés aux constructeurs d'équipement. Son rival taïwanais MediaTek a attendu le CES

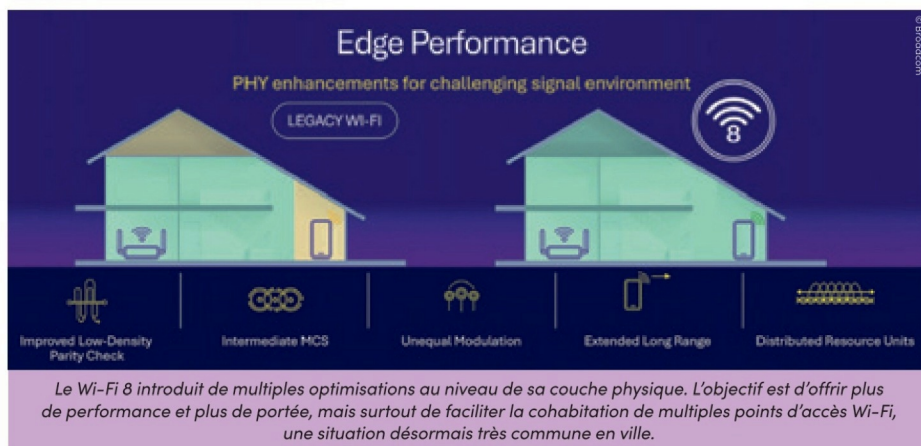
pour présenter la gamme Filogic 8000. Les documents livrés par les fournisseurs de chips Wi-Fi ont permis de lever le voile sur le futur de la norme des réseaux sans fil. Alors que les composants 802.11bn ne sont disponibles que sous forme d'échantillons pour équiper des prototypes et des bancs d'essai, Asus a présenté un concept de routeur à la géométrie plutôt inhabituelle lors du CES 2026. Tenlong Deng, vice-président et directeur général de la division Sans fil et Réseau d'Asus déclarait alors : « *Le Wi-Fi 8 ne vise pas seulement à atteindre des vitesses maximales, mais à rendre chaque connexion plus intelligente et plus fiable [...]* Comparé

au Wi-Fi 7, le Wi-Fi 8 offre un débit moyen jusqu'à deux fois supérieur, une couverture IoT deux fois plus étendue et une latence P99 jusqu'à six fois inférieure grâce à une gestion multi-points d'accès/multi-clients plus intelligente. »

Une optimisation tous azimuts du Wi-Fi 7

Derrière le discours marketing de réseaux plus rapides, plus fiables, intelligents et adaptatifs, le Wi-Fi 8 apparaît essentiellement comme une optimisation tous azimuts de la version précédente. En effet, contrairement au Wi-Fi 7, la promesse n'est plus d'offrir plus de débit brut, mais surtout de fiabiliser les connexions et mieux exploiter la bande de fréquence disponible.

Une première série d'améliorations a été apportée sur la couche physique. Le Wi-Fi 8 bénéficiera d'une évolution de son codage de correction d'erreur LDPC (Low Density Parity Check). Une longueur de bloc supérieure devrait, selon les concepteurs, réduire le nombre de paquets perdus et une connexion plus fiable dans les environnements bruyants et saturés.



Une autre amélioration porte sur la qualité du signal. Avec la technologie UEQM (Unequal Modulation Across Spatial Steams), le Wi-Fi 8 va être capable d'adapter sa modulation en fonction de la qualité de chaque antenne. Il n'y aura plus un alignement de toutes les antennes MIMO de la station sur la modulation moins performante car un terminal l'exige. Les autres antennes pourront rester une modulation plus efficace. Le Wi-Fi 8 va encore allonger la liste des MCS (Modulation and Coding Schemes) du Wi-Fi 7. Avec plus de modes de modulation et de codage disponibles, la station pourra s'adapter plus finement aux environnements où la qualité du signal fluctue. C'est notamment le cas dans les moyens de transport ou les lieux publics.

Le Wi-Fi 8, c'est aussi une promesse d'une portée plus grande. L'approche ELR (Enhanced Long Range) vise à mieux gérer le déséquilibre de puissance entre la liaison montante provenant du point d'accès et la liaison descendante provenant d'un client qui peut être un mobile ou un objet connecté à faible consommation. L'ELR doit améliorer ce que les spécialistes appellent le budget de la liaison pour étendre la portée du réseau, tout en maintenant une connexion fiable pour ces terminaux de faible puissance ou très éloignés.

Pour clore les innovations sur la couche physique, on peut aussi citer la technologie DRU (Distributed Resource Units) qui permet de mieux répartir la puissance d'émission par MHz en fonction des limites réglementaires. Le DRU permet d'augmenter la puissance d'émission en collant au plus près des limites imposées par la réglementation.

Des améliorations visibles pour l'utilisateur final

Pour l'utilisateur final, le Wi-Fi 8 va apporter d'autres changements plus visibles. Ainsi, le réseau va assurer un roaming de la communication entre différents points d'accès plus efficace. En Wi-Fi traditionnel, le roaming était possible, mais nécessitait une déconnexion et reconnexion du terminal lors du passage d'une borne à une autre. La connexion était



Dévoilé sur le CES 2026, le ROG NeoCore d'Asus est un concept de routeur Wi-Fi 8. D'autres équipementiers devraient en dévoiler lors du Mobile World Congress de Barcelone.

brèvement interrompue. En Wi-Fi 8, le roaming va fonctionner en mode « make-before-break » : le smartphone établit la connexion avec la nouvelle station avant de libérer l'ancienne, ce qui devrait éviter toute coupure dans un flux vidéo ou un pic de latence. Une autre amélioration est attendue dans l'exploitation du spectre de fréquence : si un terminal n'exploite que 40 MHz et non pas les 160 ou les 320 MHz de la bande de fréquence du point d'accès, les fréquences restantes restent non utilisées. Avec la technologie Dynamic Sub-Band Operation, ce sera le cas. De même, la technique Non-Primary Channel Access (NPCA) doit permettre de mieux exploiter les canaux secondaires si le canal primaire est déjà utilisé par un autre réseau ou brouillé. Le NPCA permettra aux terminaux de passer dynamiquement à des fréquences moins congestionnées et donc offrir plus de débit. De plus, les stations vont pouvoir accroître dynamiquement la bande passante pour faire face à un pic de trafic si les autres points d'accès sont moins chargés. Les concepteurs évoquent même plusieurs modes de coordination entre les stations dont les zones de couverture se chevauchent. Le Wi-Fi 8 introduit le co-TDMA, une transposition du protocole de division du temps d'accès au réseau TDMA, mais élargie à plusieurs stations. Le partage du temps d'accès se répartit entre les différents points d'accès. Les échanges de données deviennent plus prédictibles et on peut espérer de meilleures

performances dans un environnement où plusieurs points d'accès se partagent le spectre de fréquence. La latence devrait être améliorée par une autre technique, le Co-rTWT (Coordinated Restricted Target Wake Time) : les points d'accès auront la capacité de coordonner leurs fenêtres d'accès pour prioriser le trafic sensible à la latence.

De plus, la technique de Co-BF (Coordinated Beamforming) va leur permettre de concentrer les signaux sur les clients et donc réduire les conflits avec les réseaux voisins. Cette approche doit rendre l'utilisation du spectre plus efficace dans les immeubles et les centres-villes où les réseaux sont très denses. De même, chaque point d'accès va pouvoir ajuster dynamiquement sa puissance d'émission vers un client donné pour moins empiéter sur les zones couvertes par les autres points d'accès. Plus qu'une réelle amélioration du débit, toutes ces améliorations visent à mieux exploiter le spectre de fréquences ouvert au Wi-Fi et surtout synchroniser le fonctionnement de multiples stations de base qui doivent se partager les mêmes fréquences. En entreprise et dans les lieux publics, cela va permettre aux responsables réseaux d'améliorer la couverture et les performances dans leurs locaux. Pour les utilisateurs résidentiels, tout va dépendre de la manière dont les opérateurs vont laisser leurs box interagir avec celles de leurs concurrents...

A.C

Réseau

Cisco prêt pour l'utilisation future de l'IA

Lors de son événement Cisco Live, qui s'est tenu à Amsterdam courant février, Cisco a précisé sa stratégie pour les mois à venir et remis son métier de fournisseur de solutions de réseaux au cœur de celle-ci.

Jacques-Philippe Roederer, qui a pris la tête de Cisco en France en janvier dernier, remarque : « *ça faisait longtemps que je n'avais pas vu Cisco avoir une stratégie bien énoncée, qui était claire et durable dans le temps. Avec le lancement de notre stratégie OneCisco autour de nos trois piliers, le datacenter review, l'environnement au travail du futur et la résilience digitale, je constate que plus on positionne le réseau comme la vraie épine dorsale, et pas simplement comme un élément de transport, plus il devient le premier rempart contre les menaces* ».

Reconnu sur l'infrastructure IA

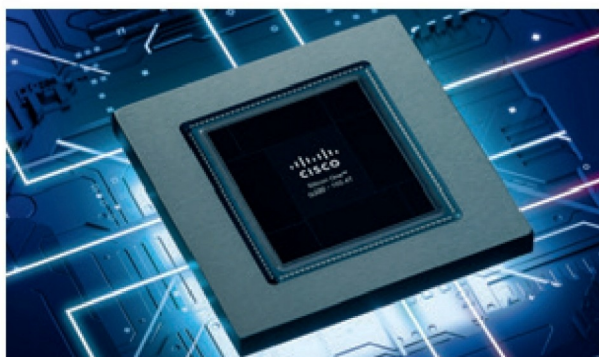
Le dirigeant français ajoute : « *depuis un an, le cours de l'action Cisco monte, cela signifie qu'aujourd'hui, on est vu et reconnu comme un acteur incontournable, sur l'infrastructure, dans l'IA. Cette vision est matérialisée aux USA, pas encore en Europe. Ils n'ont pas encore décidé quelle était celle qui va passer à l'échelle et ils ne se rendent pas compte de l'impact que cela peut avoir sur la bande passante dans l'entreprise* ».

Des annonces pour une nouvelle vague de données

Les annonces réalisées lors de l'événement vont dans le sens du dirigeant français. Le Cisco Silicon One G300, une puce de commutation 102,4

Tb/s, peut alimenter des clusters IA à l'échelle du gigawatt pour l'entraînement, l'inférence et les charges de travail agentiques en temps réel, tout en maximisant l'utilisation des GPU avec une amélioration de 28 % du temps d'achèvement des tâches. Ce système va alimenter les nouveaux Cisco N9000 et Cisco 8000. Ces systèmes intègrent un refroidissement liquide innovant et prennent en charge des optiques haute densité, afin d'atteindre de nouveaux standards d'efficacité et de permettre aux clients de maximiser la valeur de leurs investissements GPU. Par ailleurs, Cisco a renforcé Nexus One pour faciliter l'exploitation des réseaux IA par les entreprises sur site ou dans le cloud, en supprimant la complexité qui peut freiner la montée en puissance des datacenters IA.

Le G300 propose l'Intelligent Collective Networking, qui combine un buffer de paquets entièrement partagé, un équilibrage de charge basé sur les chemins, et une télémétrie proactive du réseau pour améliorer la performance et la rentabilité des datacenters à grande échelle. Il absorbe efficacement les pics de trafic IA, réagit plus rapidement aux défaillances de liens et évite les pertes de paquets susceptibles d'interrompre les tâches, garantissant une livraison fiable des données même sur de longues distances. Grâce à cette technologie, Cisco annonce +33 % d'augmentation de l'utilisation du réseau et -28 % de réduction du temps d'achèvement des tâches par rapport à une sélection de chemins non optimisée, rendant les datacenters IA plus rentables avec davantage de tokens générés par heure GPU. Le système G300 est hautement programmable, permettant aux équipements d'être mis à jour pour intégrer de nouvelles fonctionnalités réseau même après leur déploiement. Les produits basés sur Silicon One peuvent ainsi supporter de nouveaux cas d'usage et remplir plusieurs rôles réseau, protégeant les investissements d'infrastructure à long terme.



Avec la sécurité intégrée au niveau matériel, les clients bénéficient d'une sécurité globale à pleine vitesse pour maintenir leurs clusters opérationnels. L'architecture Cisco Silicon One est aujourd'hui l'architecture réseau unifiée la plus évolutive et programmable du secteur, couvrant les usages IA, hyperscale, datacenter, entreprise et fournisseurs de services. Introduite en 2019, elle joue un rôle clé dans de grands réseaux à travers le monde.

De nouveaux systèmes Ethernet

Les Cisco N9000 et Cisco 8000 (fixes et modulaires) visent l'efficacité et la performance pour répondre aux exigences extrêmes en puissance et en dissipation thermique des charges. Alimentés par le Silicon One G300, ces systèmes établissent un niveau de performance et d'efficacité dans le datacenter avec des conceptions refroidies par liquide ou par air. Les systèmes 100 % refroidis par liquide offrent une densité de bande passante nettement supérieure et améliorent l'efficacité énergétique de près de 70 %, délivrant dans un seul système la bande passante qui nécessitait auparavant six systèmes de génération précédente. Ils sont dotés d'une connectivité ultra-haut débit pour les solutions d'extension IA, avec des liens 1,6T switch vers NIC et des liens 1,6T, 800G, 400G ou 200G switch vers serveur.

L'évolution de Nexus One

Cisco fait évoluer Nexus One avec un plan de gestion unifié regroupant silicium, systèmes, optiques, logiciels et intelligence programmable en une solution intégrée. Cisco introduit également AgenticOps pour le réseau datacenter via AI Canvas, facilitant le dépannage grâce à des conversations guidées homme-machine, transformant des problèmes complexes en actions concrètes. La plateforme propose une fabrique unifiée qui autorise des déploiements rapides et une adaptation aux évolutions des besoins, même sur plusieurs sites. Les systèmes Cisco N9000 servent de matériel



Notre stratégie OneCisco repose sur trois piliers : le datacenter review, l'environnement au travail du futur et la résilience digitale.

Jacques-Philippe Roederer,
vice-président et
directeur général
France
de Cisco

commun à différents fabrics, dont Nexus Hyperfabric, avec gestion centralisée et automatisation pilotée par API. La solution est nativement intégrée avec Splunk et apporte une visibilité corrélée réseau-GPU, reliant télémétrie réseau et comportement des charges IA. Prévue ce mois, l'intégration native avec Splunk proposera l'analyse de la télémétrie directement là où les données résident, sans transfert vers des plateformes externes.

Le renfort de l'IA

L'an dernier, Cisco a introduit AgenticOps, étendu pour soutenir les opérations IT dans les environnements cloud, sur site, industriels isolés (air-gapped), entreprises, datacenters et fournisseurs de services. AgenticOps s'appuie sur une conscience globale du système, alimentée par l'une des sources de télémétrie inter-domaines les plus riches du secteur, incluant Cisco Networking, Security Cloud Control, Cisco Nexus One, Splunk et bien d'autres. En intégrant des signaux en temps réel issus de réseaux propriétaires et tiers, de contrôles de sécurité, d'applications et de plateformes collaboratives, comme notamment Cisco ThousandEyes, Secure Firewall et Splunk Observability... Le résultat : une exécution fiable en boucle fermée qui transfère les opérations quotidiennes des humains vers les machines, tout en maintenant les équipes pleinement maîtresses des résultats.

Renforcement de la sécurité

De nouvelles fonctions de sécurité combinent protection des agents, gouvernance des interactions et connectivité résiliente pour les workflows pilotés par l'IA. Les innovations en matière d'IA agentique ont élargi la surface d'attaque au sein des chaînes d'approvisionnement IA et de l'écosystème d'outils. Les entreprises ont besoin de protections réduisant le risque de manipulation ou de détournement des agents, notamment lors des interactions avec des outils. Pour y parvenir, Cisco AI Defense introduit de nouvelles fonctionnalités pour mieux sécuriser les agents et la chaîne d'approvisionnement IA. Ces mises à jour permettent aux équipes d'inventorier et de gouverner les actifs IA, de comprendre leur provenance et d'identifier les vulnérabilités plus tôt dans le cycle de développement IA.

B.G

Périphériques

Jabra adapte sa stratégie

Pour Jabra, le contexte hybride dans les modes de travail va continuer, mais le fabricant pense que la voix va jouer un rôle de plus en plus important, à la fois pour utiliser l'IA, mais aussi pour améliorer le bien-être au travail.



Une vue de l'Evolve3 85

Dans un plan stratégique qui se déroule sur la période 2026-2030, Jabra note plusieurs tendances importantes. La première est la redéfinition de la masse salariale dans les entreprises, qui doivent désormais inclure l'IA qui redéfinit

pour une part la manière de travailler. Le fabricant note aussi que le bien-être au travail devient une priorité dans les entreprises, afin d'améliorer la productivité, mais aussi pour garder ou attirer de nouveaux talents. Tout ceci s'accompagne de la priorité autour de

la conformité et de la sécurité dans les échanges entre personnes et les échanges de données.

Répondre au travail moderne

Depuis 2014, date où les communications unifiées ont investi les entreprises, les modes de travail ont évolué avec tout d'abord le télé-travail, contraint et forcé pendant la Covid, mais désormais entré dans les usages, même si les politiques de retour au bureau se font plus pressantes. Deux modèles sont conçus pour être les plus légers et les plus compacts de leur catégorie, établissant de nouvelles références, tant sur le plan du confort que de la portabilité. Jabra discerne une nouvelle évolution avec l'instauration d'un modèle de travail moderne, ou plus adapté à l'ère de l'intelligence artificielle. Cette transformation a des conséquences sur l'évolution des matériels fournis aux salariés.

Une évolution des périphériques

La première conséquence impacte la fonction des périphériques, puis viennent la forme et le besoin de pouvoir s'adapter à de futurs changements dans les modes de travail et la recherche du bien-être des employés. Par exemple, les casques Evolve3 75 et 85 proposent différentes expériences audio suivant le contexte du salarié ou son confort d'écoute. L'Evolve3 75 avec son mode supra-auriculaire vise équilibre et performance dans un contexte classique de travail. L'Evolve3 85 est plus adapté aux contextes plus difficiles avec un environnement bruyant. Avec son expérience immersive par son design circum-aural. Il offre ainsi un meilleur son et permet d'améliorer la concentration. Les deux casques avancent aussi des arguments de disponibilité intéressants avec jusqu'à 25 heures d'appels

Principales fonctionnalités

- Design moderne, sans perche micro, décliné en noir ou gris
- Technologie Jabra ClearVoice basée sur l'IA (DNN) pour une captation vocale de qualité professionnelle
- Mode ANC adaptatif en temps réel, y compris pendant les appels
- Jusqu'à 25 h d'autonomie en communication et 120 h en écoute, avec recharge rapide (10 h en 10 minutes)
 - Interaction vocale fluide avec les outils d'IA
- Batteries remplaçables et conception durable (certification TCO Gen 10)
- Confort longue durée et formats compacts, faciles à transporter

et 120 heures de musique, un mode de recharge sans fil et un mode de recharge rapide qui assurent jusqu'à dix heures d'autonomie en seulement dix minutes.

L'IA en renfort

Les casques précités sont équipés de Jabra ClearVoice qui combine une technologie de réseaux neuronaux profonds (DNN — Deep Neural Networks) et des algorithmes multi-micros développés par Jabra. Le modèle d'apprentissage profond DNN traite plusieurs couches de données

sonores afin de distinguer la voix de l'utilisateur des bruits environnants, sans nécessiter une perche micro visible. Cette technologie est inspirée de la manière dont le cerveau filtre les bruits dans une pièce bondée et s'appuie sur les technologies mises au point par le groupe GN, spécialisé dans la fabrication d'appareils auditifs. Cette approche assistée par l'IA s'associe à un minutieux travail sur le matériel pour placer les micros discrètement tout en préservant la meilleure retranscription possible. Ainsi, un

mode de réduction de bruit active (ANC) adaptatif réagit en temps réel à l'environnement où se trouve l'utilisateur, ainsi qu'à la façon dont le casque est ajusté. Contrairement à la majorité des solutions du marché, la technologie ANC dont dispose l'Evolve385 et 75 continue de bloquer les sources de distraction, non seulement entre deux conversations, mais également pendant les appels.

Intégrée aux casques, la technologie Jabra ClearVoice s'appuie sur une IA d'apprentissage profond, entraînée sur plus de 60 millions de phrases, pour isoler la voix des bruits de fond avec une grande précision. Optimisée pour les usages d'IA, elle reconnaît plus de 96 % des mots dans les requêtes vocales (99 % en open space) facilitant la dictée, les commandes et l'exécution des tâches. Certifiés pour les principales plateformes de communications unifiées, les casques de la série Evolve3 embarquent un adaptateur Bluetooth pré-appairé pour une connectivité instantanée et sécurisée, et prennent en charge le protocole Bluetooth Native pour une connexion directe.

B.G

JANS CLAVIER ET JANS SOURIS...



Souveraineté

L'open source pour se libérer de la dépendance

La déconnexion de quatre juges et procureurs de la Cour pénale internationale de tout service fourni par une entreprise américaine l'a récemment montré : le pouvoir américain dispose d'un « kill switch » sur l'économie européenne. Pour une organisation ou une entreprise, la perspective de voir tous ses comptes cloud ou même ses contrats de support invalidés pèse comme une épée de Damoclès sur leur activité. Pour la commission, une seule issue possible : l'open source.

La commission européenne vient de lancer un nouvel appel à contribution sur le thème de l'open source. Le logiciel libre est désormais considéré par l'Europe comme un moyen de renforcer une souveraineté numérique mise à mal par sa dépendance aux technologies américaines. La fermeture des comptes Microsoft 365 de plusieurs membres de la CPI sur décision de Donald Trump, mais aussi de tout service délivré par une entreprise américaine, carte Visa comprise, a joué le rôle d'électrochoc. Les administrations et entreprises européennes sont sous la menace du « kill switch » américain et se sevrer des technologies logicielles, Cloud, IA ou même hardware made in USA va être compliqué.

L'UE trop naïve dans son approche de l'open source ?

En préambule de l'EU Open Source Policy Summit qui s'est tenu à Bruxelles fin janvier 2026, Henna Virkkunen, vice-présidente exécutive de la Commission européenne, expliquait sa position : « *L'UE est confrontée à un problème de dépendance excessive à des pays tiers dans des secteurs critiques, tels que le cloud, l'IA, la sécurité cyber, pour en nommer*

quelques-uns. L'urgence pour renforcer la compétitivité de l'Europe et la souveraineté technologique n'a jamais été plus grande. » La politique évoque le nouveau « *EU Cloud and AI Development Act* » et la réévaluation du Chips Act, des programmes qui ont une large dimension open source, comme des outils pour renverser cette situation de dépendance. Rappelant son origine finlandaise, patrie de Linus

Torvalds, elle ajoute : « *L'open source peut être une partie clé de la solution, et l'UE peut devenir le phare de la technologie open source.* » Des projets financés par l'Union européenne, il y en a déjà beaucoup et dans tous les domaines. Rien que pour le programme Internet de la prochaine Génération, la vice-présidente évoque le nombre de 1 700 projets aidés. Si des briques open source sont omniprésentes dans les infrastructures informatiques, l'Open Source n'a pas évité aux organisations européennes de tomber sous la coupe des géants de la tech américaine. Beaucoup de grands projets open Source sont eux-mêmes pilotés par des fondations ou des entreprises commerciales de droit américain, ce qui ne résout pas cette problématique de dépendance de l'Europe vis-à-vis des États-Unis. Figure de l'Open Source en France et fondateur de Software Heritage, Roberto Di Cosmo souligne : « *Ce souci de souveraineté européenne est tout récent. Tout d'un coup, les Européens*

**Henna Virkkunen, vice-présidente exécutive
chargée de la Souveraineté technologique,
de la Sécurité et de la Démocratie
de la Commission européenne**

« *La Commission européenne soutient l'open source depuis des années. L'initiative Internet de la prochaine génération qui a fourni des fonds à plus de 1 700 projets et nous avons obtenu des résultats : Certains projets open source sont exploités dans le secteur public, à l'image du projet allemand openDesk et de la solution française La Suite Numérique. Nous avons offert aux Européens plus de choix et plus de confidentialité et de sécurité avec Rosenpass pour les VPN, Open Food Fact pour vérifier les données et PeerTube pour partager des vidéos. Le défi clé est maintenant d'atteindre la taille critique, d'assurer la viabilité financière et d'atteindre une pénétration de marché plus élevée.* »



Bastien Guerry, responsable des partenariats chez Software Heritage, ancien responsable de l'Open Source Programme Office de la Dinum

« Les premiers signes, c'est de voir les administrations publiques qui réagissent sur le sujet de la souveraineté, et pas seulement en achetant et en bricolant dans leurs coins, mais en construisant ensemble des solutions souveraines. Par exemple, pour la Visio, il y a un avant et un après Covid, un avant et un après Trump. La prise de conscience est là et les outils sont là. La deuxième phase est que l'on voit aussi des entreprises importantes, par exemple du secteur automobile, qui travaillent ensemble sur des logiciels communs. Elles n'ont pas le droit de le faire si le code est privé, c'est de la collusion d'intérêts, mais elles peuvent le faire si le code est libéré. Donc oui, je suis optimiste. »



se sont rendu compte de la dépendance de leurs infrastructures critiques vis-à-vis des grands acteurs américains. Or, l'histoire du logiciel libre en Europe est ancienne et elle a déjà apporté une contribution majeure à l'open source mondial.»

Lui qui a participé à la refonte complète du SI du ministère des Finances dans les années 2000, explique : « Des choses incroyables ont été réalisées, mais l'Europe n'a pas su exploiter cet avantage. Au début, le code développé par l'argent public n'était pas publié, puis les choses ont évolué et les appels d'offres ont imposé que le code source soit publié en open source, mais c'était aux communautés de le maintenir gratuitement. Évidemment, ce modèle n'a pas fonctionné. » Dans un contexte de guerre économique et d'acteurs du logiciel et du cloud ultra dominants, une telle approche peut sembler bien naïve...

L'UE parle enfin de souveraineté

L'Europe doit revoir sa doctrine et parmi ceux à avoir répondu à l'appel à contribution figure le Conseil National du Logiciel Libre (CNLL) qui a rédigé une liste de plusieurs dizaines de propositions structurées sur cinq piliers : le développement technologique, le développement des compétences, l'achat public, l'investissement et la croissance

et la gouvernance et la soutenabilité de l'écosystème. Stéphane Fermigier, co-président du CNLL résume la position de l'organisation : « Pour moi, la nouvelle stratégie de l'UE sera de coupler une

politique d'achat volontariste intégrant des critères de souveraineté, le fameux Sovereign Cloud Framework, dont la teneur reste encore très incertaine, et avoir une réelle notion de politique industrielle globale. L'Europe doit soutenir la filière par des achats, notamment afin de contrebalancer les effets pervers de domination du marché par des effets de réseaux et de bundling des offres qui n'incitent pas les clients à chercher des alternatives. »

1 658 contributions ont été recueillies pendant le mois de janvier 2026. La commission s'est donnée trois mois pour analyser ces propositions pour alimenter la nouvelle doctrine open source de l'Union européenne qui prendra le relai de la stratégie 2020-2023. Celle-ci ne devrait plus seulement stimuler l'innovation, mais bien servir l'Europe des technologies américaines qui sont aujourd'hui omniprésentes, tant dans les entreprises que dans le secteur public.

A.C



L'Europe ne se sortira pas de la domination des acteurs américains simplement en régulant son marché. Nous comptons plus de développeurs open source que les États-Unis, et c'est en

stimulant cette communauté en amont, avec des aides pour la R&D et l'innovation et en aval, avec des achats fléchés vers l'open source que nous y arriverons.

Stéphane Fermigier co-président
du Conseil National du Logiciel Libre

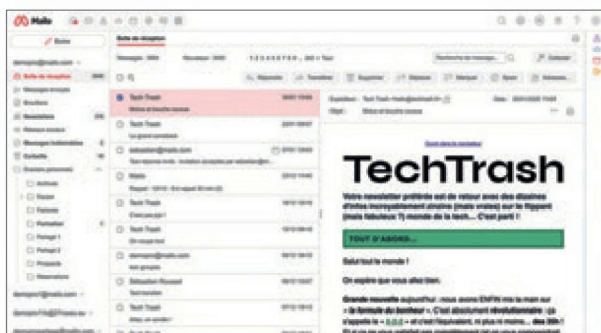


Messagerie

Le souverain gagne du terrain

Portée par les tensions géopolitiques et la défiance croissante envers les plateformes américaines, la messagerie française Mailo enregistre une croissance soutenue des comptes et des abonnements professionnels. Un indicateur tangible du déplacement progressif des choix IT des collectivités et des entreprises vers des solutions numériques souveraines, hébergées et gouvernées en Europe.

international sous tension, où les dépendances technologiques sont de plus en plus scrutées. Les lois extraterritoriales américaines, à commencer par le Cloud Act ou le FISA, amènent de nombreux DSI et RSSI à reconsidérer leurs choix historiques. « La messagerie n'est plus vue comme un simple outil de productivité. Elle devient une brique critique du système d'information, avec des enjeux directs de sécurité et d'autonomie », souligne Sébastien Roussel, chef de produit chez Mailo.



Hébergement souverain et architecture maîtrisée : la messagerie Mailo repose sur des infrastructures localisées en France, opérées sur des serveurs propriétaires.

La question de la souveraineté numérique n'est plus un débat théorique réservé aux cercles institutionnels. Elle s'impose désormais comme un paramètre stratégique dans les choix d'outils collaboratifs des entreprises. Messagerie, stockage, partage documentaire ou agendas constituent le cœur informationnel des organisations. Dans ce contexte, la progression enregistrée par Mailo illustre un changement d'échelle plus qu'un simple effet conjoncturel. L'éditeur constate une hausse marquée des créations de comptes et des abonnements professionnels, portée par les

PME, les collectivités territoriales et les grandes associations. Cette accélération s'inscrit dans un environnement

Une alternative européenne crédible face aux géants globaux

Contrairement à des acteurs qui ont ajouté a posteriori des couches de conformité ou des options de résidence des données, Mailo revendique une approche native de la souveraineté. L'ensemble des données est hébergé en France, sous juridiction française et européenne, sur des infrastructures maîtrisées, sans dépendance à des hyperscalers soumis à des législations extracommunautaires. « Notre objectif est d'offrir une solution aussi solide et fonctionnelle que les grandes suites, tout en répondant aux critères d'indépendance et d'autonomie technologique attendus par les organisations », explique Sébastien Roussel. Pour les entreprises, l'enjeu dépasse la seule



conformité réglementaire. Il s'agit de réduire les risques juridiques, notamment par une meilleure traçabilité des accès. « *Les directions IT cherchent aujourd'hui des solutions lisibles, cohérentes et alignées avec leurs politiques de sécurité. La maîtrise des données devient un critère de choix, au même titre que la disponibilité ou la simplicité d'administration* », ajoute-t-il. Dans ce cadre, Mailo se positionne comme une alternative opérationnelle, capable de couvrir les usages quotidiens sans rupture fonctionnelle majeure, tout en proposant des trajectoires de migration progressives depuis les environnements historiques, notamment Microsoft.

Des usages professionnels tirés par la sécurité et la conformité

La croissance observée concerne en priorité les offres professionnelles et institutionnelles. Collectivités locales, PME industrielles, cabinets de conseil ou établissements de santé partagent des contraintes communes : protection des échanges, confidentialité renforcée et conformité réglementaire. La messagerie devient alors un point d'entrée pour une stratégie numérique plus large, orientée vers des outils collaboratifs de confiance. Dans certains cas, Mailo est également sollicité comme solution de repli ou de plan de continuité d'activité. Des entreprises de taille plus importante, encore fortement dépendantes des suites américaines, l'envisagent comme une messagerie de secours ancrée localement, capable d'assurer la résilience des communications en cas de crise majeure, de rupture contractuelle ou de contrainte réglementaire imprévue. Mailo met en avant des mécanismes de sécurité intégrés, allant du chiffrement des échanges à la lutte contre le phishing et les tentatives d'usurpation d'identité. Ces fonctionnalités répondent à une réalité : la messagerie demeure l'un des principaux vecteurs d'attaque des systèmes d'information.



Les entreprises ne veulent plus choisir entre souveraineté et efficacité. Elles attendent des solutions capables de coexister avec leurs outils et leurs processus.

Sébastien Roussel
chef de produit
chez Mailo

« Renforcer la souveraineté, c'est aussi limiter la surface d'exposition et reprendre le contrôle sur des briques historiquement très ciblées par les cyberattaques », rappelle Sébastien Roussel.

Une dynamique révélatrice d'un marché en recomposition

La trajectoire de Mailo s'inscrit dans un mouvement plus large de recomposition du marché numérique européen. Longtemps dominé par des plateformes globales, celui-ci voit émerger une demande pour des acteurs capables

de concilier performance, sécurité et ancrage local. « *Le marché est très largement dominé par Google et Microsoft, mais il y a encore de la place pour les acteurs européens crédibles* », estime Sébastien Roussel. Pour les décideurs IT, l'enjeu n'est plus de savoir si une alternative souveraine existe, mais si elle peut s'intégrer sans remise en cause brutale des environnements existants. Interopérabilité, simplicité de migration et accompagnement au changement deviennent des critères clés. Sur ce terrain, Mailo mise sur une intégration progressive avec les annuaires et systèmes d'identité existants, tout en reconnaissant la nécessité d'une conduite du changement auprès des utilisateurs finaux, encore très attachés aux interfaces dominantes. La croissance actuelle de Mailo traduit un changement de posture des décideurs. La souveraineté numérique n'est plus abordée comme une posture idéologique, mais comme une réponse pragmatique à des risques identifiés. « *On sent un véritable effet boule de neige : les entreprises, les collectivités et même l'État commencent à soutenir activement l'émergence de solutions européennes solides* », observe Sébastien Roussel. Ce mouvement s'inscrit dans une logique de long terme, où l'autonomie numérique devient un attribut structurant des stratégies IT, au même titre que la cybersécurité ou la performance. Pour Mailo, le défi n'est pas de concurrencer frontalement les géants mondiaux sur tous les terrains, mais de proposer des briques fiables, interopérables et industrialisables, capables de s'insérer durablement dans les architectures numériques européennes. Dans cette perspective, l'éditeur mise sur des suites collaboratives unifiées, construites avec des partenaires de l'écosystème souverain. À mesure que les tensions géopolitiques persistent et que les exigences réglementaires se renforcent, ce type de services pourrait progressivement s'imposer dans les environnements IT nationaux et redéfinir durablement les critères de choix technologiques des organisations françaises.

J.C

Processus

BPCE bascule sur une nouvelle GED sans vague

Les filiales bancaires du groupe BPCE de Tahiti et de Nouvelle-Calédonie ont rationalisé leur gestion documentaire. Le but était classiquement de sécuriser les processus métier et d'améliorer l'expérience utilisateur.

Filiales du groupe Groupe Caisse d'Épargne Ile-de-France, deux banques, de Tahiti et de Nouvelle-Calédonie comptent ensemble quelque 600 collaborateurs et 66 000 clients. La filiale du groupe T2S Pacifique est en charge de l'IT. Responsable AMOA Projets dans cette dernière, François Duwez décrit : « Remplacer les deux applications de GED développées en interne dans chacun des deux établissements bancaires était devenu nécessaire, tant pour gagner en réactivité que pour sécuriser les flux documentaires, et ce d'autant plus que les agences sont réparties sur différentes îles, parfois très éloignées les unes des autres. » Plus classiquement, l'objectif était de rationaliser les deux systèmes d'information, d'assurer une meilleure gestion de la donnée, en évitant les doublons, et de faciliter les synergies entre les deux banques. Enfin, les réglementations récentes pour le bancaire, en particulier « Know your Customer » supposent d'obtenir des justificatifs de la part des clients et de présenter au régulateur un nombre conséquent de documents, ce qui suppose de vérifier la complétude des dossiers. Plus largement, les réglementations du secteur imposent d'avoir les moyens IT de garantir la conformité. En 2023, le groupe opte pour la solution de Docuware, notamment pour

sa modularité, et prend La Demat, une ESN locale, pour le paramétrage et les développements spécifiques. Démarré en 2023, le projet a pris environ une année en termes de ressources. La récupération des données, 6 millions de documents (relevés de comptes...) pour la banque de Nouvelle-Calédonie, 1 pour celle de Tahiti, n'a pas posé de soucis particulier et peu de doublons ont été identifiés. L'intégration avec les

applications métiers du groupe a reposé sur des connecteurs avec le Core Banking System SAB, des liens à des bases de données tampons via ODBC et enfin, des web services et API de Docuware. Cette interconnexion permet également aux clients d'accéder directement à leurs documents (relevés, contrats, justificatifs) depuis la banque en ligne. L'archivage légal des documents est pris en charge par le module système d'archivage électronique — SAE — de l'éditeur. Plusieurs spécificités propres à chaque banque ont fait l'objet de développements, notamment pour le module de SAE. François Duwez explique, « les documents versés dans le SAE sont signés avec DocuSign pour La banque de Nouvelle-Calédonie. Pour Tahiti, la signature native à Docuware est utilisée ». Autre spécificité pour la Nouvelle-Calédonie, des liens ont été créés entre l'application RH pour déposer automatiquement les documents dans la GED. Si Docuware incluait déjà des fonctionnalités de complétude, la réglementation « Know your customer » a demandé quelques développements, « pour automatiser l'envoi de mail au client, alerter sur la validité des documents dans le temps, respecter des règles de complétude complexes liées à la réglementation locale ou encore, pour copier un document dans le cas où le même sert à la fois de justificatif de domicile et d'identité », détaille François Duwez. Les développements ont été réalisés en C#. Avant la bascule complète sur la nouvelle solution, un « double run » a été mis en place sur une période limitée. Aujourd'hui, l'application facilite le quotidien des utilisateurs comme des clients, notamment en apportant une meilleure visibilité sur l'état d'avancement des dossiers.

François Duwez, responsable AMOA Projets chez T2S, filiale du Groupe Caisse d'Épargne Île-de-France



P.B

Plateforme

e-Barreau sécurise l'activité des avocats

Le Conseil national des Barreaux dote les avocats plaideurs d'une clé sécurisée pour accéder à une plateforme qui gère leurs dossiers et leurs relations avec les juridictions.

E-Barreau fait peau neuve. La plateforme numérique des avocats créée par le Conseil national des Barreaux (CNB) devient « un mini-MSP pour les avocats », selon le mot de Maître Philippe Baron, président de la commission numérique de l'organisme. Cette plateforme, développée pour la gestion de leurs relations avec les juridictions judiciaires, ou pour les connecter aux juridictions administratives, répond mieux à leurs besoins, tant pour leurs affaires civiles (droit de la famille, des biens, commercial, etc.) que pénales. « La première version avait été développée dans un langage 4D devenu obsolète », indique Maître Philippe Baron, le président de la commission numérique du CNB. *Nous étions arrivés au bout de tous ses développements possibles faute d'experts.*

Désormais, chacun des 56 000 avocats, qui ne se limitent pas au conseil mais plaident, sur les 78 000 inscrits dans l'un des 164 barreaux de France et d'Outre-mer, dispose d'une clé USB e-Identitas certifiée CERT Europe, d'un identifiant, qui lui permet d'accéder à e-Barreau, pour ses échanges électroniques avec les 230 tribunaux et cinquante cours d'appels de l'appareil judiciaire. « Si un serveur tombe en panne, toute l'activité est paralysée. Cela nous est arrivé pendant nos essais avec le tribunal de Papeete », se souvient Maître Baron. À terme, Portalis, le serveur unique du ministère de la Justice prendra en charge les relations

entre avocats et juges pour toutes les procédures, civiles, pénales, commerciales et administratives, jusqu'en cassation. Seules restrictions, même si les échanges électroniques sont possibles : les actes relevant de la détention et des remises en liberté de détenus.

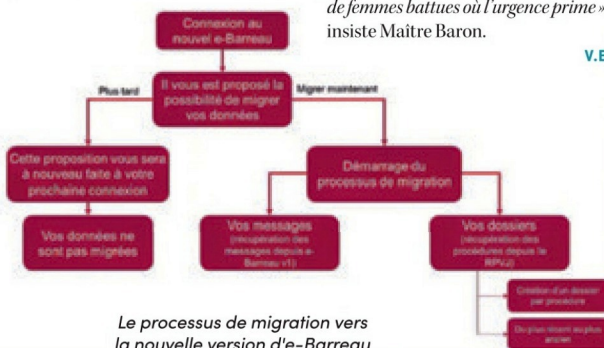
Ce réseau privé apporte désormais une capacité de stockage portée à cinq Go contre 200 Mo dans l'ancien outil. « Il était fréquent que cet espace soit saturé avant la fin de journée, avec des photos ou vidéos jointes dans une procédure nécessitant des expertises. Lorsque ce seuil était dépassé, les messages les plus anciens disparaissaient », indique Maître Baron. Surtout, les avocats peuvent accéder 24/7 aux pièces et actes des tribunaux et greffes, voire de recevoir des alertes à propos de leurs affaires en cours, le tout, même depuis un smartphone. Quid de la fameuse sécurité

des points d'accès, surtout dans un lieu aussi sensible qu'un cabinet d'instruction ? « Vos confrères se plaignent régulièrement de ne pas accéder au wifi de certaines salles d'audiences quand nous continuons à émettre ou recevoir des messages », sourit le praticien.

Pour épaissir e-Barreau, le CNB et sa commission numérique se sont appuyés sur quelques experts en internes. Qui se montrent peu loquaces pour livrer des détails sur leurs travaux en général et l'architecture d'e-Barreau. Tout juste admettent-ils que l'infrastructure de production est hébergée sur un cloud privé dédié, qui mobilise trois datacenters souverains, et que l'infogérance est assurée par une entreprise française. Pour la remettre à niveau, le langage 4D a été remplacé par des développements Java pour le Backend, qui contient certaines dépendances du ministère de la Justice, avec un serveur Apache TOMCAT. Côté Frontend, les développements ont été effectués sous Angular.

Dans l'avenir, la plateforme sera interconnectée avec celle des notaires pour des procédures de divorces amiables et celle des commissaires de justice, « pour délivrer des actes en moins de vingt-quatre heures, pour les affaires de femmes battues où l'urgence prime », insiste Maître Baron.

V.B



Développement

Comment mesurer la **qualité** d'un code informatique

Mesurer la qualité du code permet de l'évaluer sur différents plans. Cela donne des informations sur sa fiabilité, son efficacité, son utilisabilité et sa portabilité, mais ce ne sont pas les seuls indicateurs intéressants. Nous allons voir dans cet article quels éléments doivent être pris en compte et comment.

La manière de programmer est intrinsèquement « ouverte » et vous pouvez résoudre le même problème de plusieurs manières quel que soit le langage de programmation employé. La qualité du code indique dans quelle mesure celui-ci est convivial pour les développeurs et la facilité avec laquelle il est possible de le comprendre, de le modifier et de le réutiliser. Un code est lu et réutilisé par un nombre de personnes bien plus important que celui qui l'ont écrit initialement, d'où l'importance d'évaluer au mieux sa qualité.

Vous pouvez écrire des programmes de plusieurs centaines de lignes de code ou de seulement quelques dizaines. L'approche peut dépendre d'un certain nombre de paramètres tels que l'amélioration à l'extrême des performances, les systèmes embarqués ou une architecture particulière. Le paradigme de programmation doit être pris en considération : design patterns (modèles de conception), approche suivie en matière de résolution de problèmes, capacités du langage de programmation, réutilisabilité, utilisation ou non de bibliothèques externes. La qualité du code représente aussi son efficacité, en termes de fonctionnalités bien entendu, mais également en

termes de lisibilité et de maintenabilité. Un code de qualité facilite le travail de chacun en économisant à la fois du temps et des ressources. Il est plus facile à lire et constitue un modèle pour d'autres développements. Les développeurs chargés de le reprendre le comprendront plus aisément et le travail de collaboration en sera facilité. L'architecte du système pourra vérifier plus facilement le respect de la structure définie au départ et ainsi mieux coordonner le travail de l'équipe de

conception. Les autres parties prenantes du développement logiciel, notamment les personnes chargées de la sécurité et des opérations, pourront tester, déployer et sécuriser le code bien plus aisément. Ce sont les bonnes pratiques, une méthodologie efficace, ainsi que l'expérience acquise au fil du temps qui vont aider les développeurs à améliorer leurs techniques et approches de programmation, et les conduire à produire du code de bien meilleure qualité.

Critères d'évaluation

Les valeurs permettant de mesurer quantitativement la qualité du code sont diverses et variées. Cela peut être, par exemple, le nombre d'incidents survenus pendant le déroulement d'une application s'exécutant depuis 1 000 heures.



AWS propose des solutions pour mesurer la qualité du code comme Amazon Q Developer.

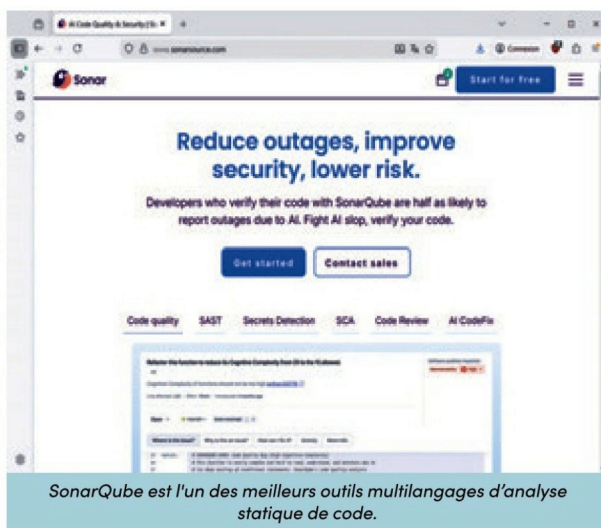
Les indicateurs de la qualité du code sont à la fois subjectifs et descriptifs. Un développeur expert peut vérifier le travail d'un développeur junior et faire des commentaires et, de manière générale, les développeurs pensent réviser le code les uns des autres. C'est la combinaison des évaluations quantitatives et qualitatives qui permet d'obtenir la meilleure mesure possible de cette qualité. Celle-ci dépend également de divers autres éléments comme la documentation, l'efficacité, la facilité d'utilisation pour l'utilisateur final, la rapidité ou la sécurité. Les principaux domaines de mesure de la qualité du code sont nombreux et traitent différents aspects du code.

Fiabilité

Un code fiable s'exécute tel qu'il doit le faire selon la documentation qui le décrit. Il doit également être robuste, gérer correctement les entrées inattendues (au moins jusqu'à un certain point) et les interruptions sans plantage intempestif, ni autres comportements indésirables. Des indicateurs de suivi tels que le nombre de défaillances du système sur une période donnée, le délai moyen de défaillance et le nombre de bogues connus permettent de mesurer la fiabilité.

Comment améliorer la qualité du code ?

De nombreux outils permettent de vérifier et d'améliorer la qualité du code dans différentes catégories au cours du cycle de vie du développement logiciel : analyse de code statique, gestion de versions, complexité du code ou couverture complète des tests. Ces outils doivent être intégrés dans l'environnement de développement et non employés comme des rustines après la conception. Des contrôles de qualité automatisés et l'emploi d'outils de révision du code peuvent être déclenchés lors des événements d'intégration et de développement continu (CI/CD), tels que le transfert de code vers un référentiel Git. L'automatisation et les outils logiciels spécialisés doivent être associés à des révisions manuelles du code. Les activités de programmation en binôme consistant à amener les développeurs à vérifier le code de chacun pour détecter les problèmes de qualité en font partie.



Extensibilité

Qu'un logiciel fonctionne parfaitement à chaque fois qu'il s'exécute, c'est le premier but à atteindre, mais que se passe-t-il s'il doit être modifié, même très légèrement ? Ou si le code doit être employé pour créer de nouvelles fonctionnalités ? Est-il compréhensible pour tous et non pas seulement pour le développeur qui l'a créé, qui n'est peut-être plus disponible pour donner des

explications et aider la nouvelle équipe ? Si un code est extensible, il sera facile de le mettre à jour ou de le réutiliser. Les qualités d'un tel code sont une architecture solide, une grande modularité, la conformité aux normes de programmation générales et à celles spécifiques au langage, au type d'application ou à l'organisme. La longueur et la complexité de la base de code doivent elles aussi être prises en compte. Il existe des outils permettant un tant soit peu de mesurer ces métriques à partir du code de base. Il y a ceux d'analyse statique et dynamique ou de mappage des dépendances.

Testabilité

Un bon code doit être facile à tester. La création et l'exécution des tests doit être aisée. Il est, par exemple, difficile d'écrire des tests couvrants absolument tous les scénarios si ne serait-ce qu'une seule fonction contient trop d'étapes logiques ou fait référence à plusieurs parties d'un logiciel. La décomposition du logiciel en unités ou modules distincts facilitera en revanche grandement les tests. La testabilité peut

être mesurée en utilisant plusieurs techniques. Tout d'abord, les tests doivent être associés aux exigences fonctionnelles. Ensuite, il faut employer des outils capables d'examiner la couverture du test pour le code comme coverage pour Python, vstest, JaCoCo, Trèfle, Couverture, Jenkins, SonarQube ou la fonctionnalité graphique offerte par des IDE tels que Visual Studio ou VSCode de Microsoft. Enfin, des outils d'analyse de complexité cyclomatique (nombre de chemins décisionnels), tels que les mesures de complexité de Halstead, permettent d'évaluer la complexité du code. Les développeurs peuvent également suivre des paradigmes de développement axés sur les tests comme le TDD (Test Driven Development), le développement guidé par les tests.

Portabilité

Il peut être intéressant de récupérer le code d'un environnement donné pour le faire fonctionner dans un environnement différent. Vous pourrez ainsi en mesurer la portabilité. Une application Android

Documentation et normes de codage

Un code de haute qualité doit impérativement être bien documenté. Il doit décrire de manière cohérente et complète les exigences fonctionnelles et non fonctionnelles, ainsi que les performances du système. Les guides de style couvrent un ensemble de conventions relatives à l'écriture du code tels que le formatage, le nommage et l'indentation. Ces éléments dépendent en grande partie du langage employé, comme la PEP 8 de Python. Le code respectant ces règles établies est plus lisible et plus facile à maintenir. Ces normes vont bien au-delà des conventions stylistiques de base. Elles ressemblent davantage à des procédures opérationnelles standard sur la façon de développer du code. Elles peuvent comporter des directives sur les modèles de conception à employer, sur des règles architecturales ou sur la manière de gérer les erreurs. Ces normes de programmation peuvent être communautaires, comme la norme de codage SEI CERT C pour la programmation sécurisée en langage C, ou spécifiques à une organisation, à un projet ou à des types de projets.

pourra être portée sur iOS et vice-versa. C'est une question qui doit normalement être posée dès la conception initiale. Si le code a été directement conçu dans cette optique multiplateformes, le portage vers un nouveau système sera en principe relativement facile. La portabilité dépend du niveau de

couplage entre le code et le système cible. Plus ce niveau est faible, plus la portabilité est facilitée. Le pire cas de figure est, lorsque le couplage est au contraire très fort, l'obligation de réécrire presque entièrement le code pour s'adapter à l'évolution du besoin métier et/ou le déploiement sur une/des plateformes systèmes et logicielles différentes.

Réutilisabilité

Le code de haute qualité est modulaire et conçu pour être réutilisé. Par exemple, une fonction conçue pour ajouter des tâches à une base de données de suivi des tâches peut être réutilisée dans différentes parties d'un projet logiciel, ou dans un projet logiciel complètement différent. Les composants logiciels conçus pour être réutilisés sont souvent attachés à des API. Celles-ci fournissent un moyen standard d'interagir avec les fonctionnalités du code réutilisable, plutôt que de simplement dupliquer du code.

Analyse statique versus analyse dynamique

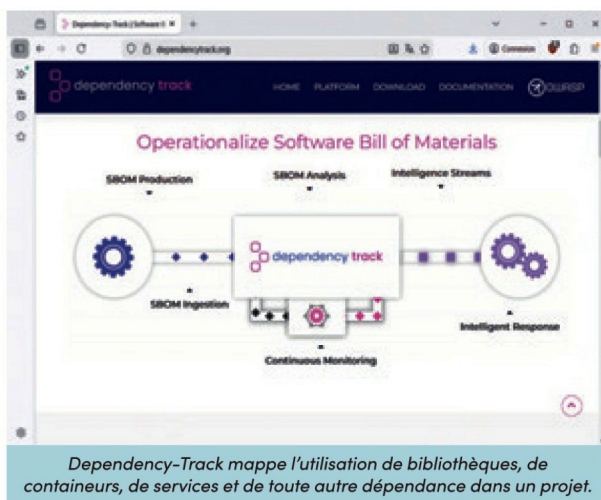
L'analyse statique du code examine le code sans l'exécuter, généralement à l'aide d'outils spécialisés

The screenshot displays the Testwell CMT++ and CMTJava website. The main heading is 'Mesure de métriques Halstead avec Testwell CMT++ et CMTJava (outils de mesure de complexité)'. Below this, it states: 'Testwell CMT++ et Testwell CMTJava sont des outils de mesure de complexité des logiciels pour C, C++, Java et C#'. A section titled '1 But et origine' explains that Halstead metrics were developed by Maurice Halstead to determine a quantitative measure of complexity. It mentions that these metrics are useful during development to access code quality and reduce errors. A diagram shows a flow from 'Code' to 'Metrics' to 'Complexity'. Another section titled '2 Nombre d'opérateurs et d'opérandes' is partially visible. At the bottom, a blue banner reads: 'Les outils Testwell CMT++ et CMTJava de Verifsoft permettent de mesurer les métriques de Halstead pour les langages C, C++, Java ou C#'. The website also features logos for Testwell CMT++ and Testwell CMTJava.

qui détectent les erreurs de syntaxe, les vulnérabilités de sécurité ou les écarts par rapport aux standards de développement. Parmi les nombreux outils d'analyse statique, Pylint est très employé pour le langage Python. SonarQube est multilingages et plus que célèbre. Nous pouvons aussi citer Xygeni, Snyk Code, Semgrep ou Astrée. Le C et le C++ ont Frama-C, Coverity, Cppcheck et CodeSonar, LDRA ou Squalé. L'analyse dynamique utilise les données en temps réel récupérées lors de l'exécution d'un programme afin d'identifier les vulnérabilités qui ne peuvent pas l'être via l'analyse statique. Ce processus consiste tout simplement à surveiller et à analyser le comportement d'une application pendant son exécution. Là encore, il existe de nombreux outils : Jmeter pour Java, Locust pour Python, OWASP ZAP, Nuclei, Burp Suite, Nikto, mitmproxy ou ce bon vieux Nmap (aidé de scripts NSE). L'analyse du déroulement de l'exécution d'une ou plusieurs applications conjointement avec des analyseurs de processus permettra d'avoir une vue au moins basique des choses. Parmi les outils existants, vous trouvez Process Monitor, ProcessExplorer ou ProcessHacker sous Windows, System Monitor, ps et autres htop sous Linux.

Mappage des dépendances

Le mappage des dépendances peut se faire avec Dependency-Track développé par la communauté OWASP. Il permet une analyse continue de SBOM (Software Bills of Materials), afin principalement d'identifier les vulnérabilités présentes dans les dépendances. Il fournit aussi de quoi analyser les risques dans chaque projet, rechercher un composant commun à plusieurs applications ou établir des graphes de dépendances. Trivy est, lui, un outil en ligne de commande



très polyvalent permettant entre autres choses la génération de SBOM au format CycloneDX. Dependency Walker permet, dans l'univers Windows, de détecter des problèmes courants d'applications tels que des modules manquants ou invalides, des incompatibilités d'import/export, des erreurs de dépendance circulaire, des incompatibilités de types et des échecs d'initialisation de modules.

Un équilibre subtil

La qualité du code se construit et se mesure dans l'équilibre entre plusieurs facteurs à l'aide d'outils et de métriques, mais cela ne suffit pas. Il faut interpréter correctement ces mesures, pourquoi tel signal est important et ce qu'il signifie. C'est une notion multidimensionnelle qui ne se résume pas à une indentation soignée et à l'absence de warnings dans le pipeline CI. Elle renvoie à un ensemble de propriétés techniques en interdépendance conditionnant la capacité d'un système à durer, évoluer et absorber la contrainte la plus aisément possible sans se dégrader. Réduire la qualité du code à un critère esthétique ne peut que mener

dans une impasse. Un code lisible mais non performant ne tiendra pas en production. Un code performant mais illisible n'est pas non plus une option viable. En résumé, la qualité nécessite un équilibre subtil entre ces nombreuses dimensions que sont la lisibilité, la maintenabilité, la robustesse, la testabilité, la sécurité et la performance. Un code peut fonctionner, passer les tests, délivrer la fonctionnalité attendue mais rester tout de même de mauvaise qualité. Il peut être trop complexe pour évoluer simplement, trop couplé pour accepter une nouvelle contrainte ou simplement trop opaque pour supporter aisément un changement d'équipe. Si, à petite échelle, l'intuition et l'expérience compensent parfois l'absence d'indicateurs, cette approche montre rapidement ses limites lorsque les systèmes grandissent. Les bases de code s'étendent, se fragmentent, se superposent et se complexifient. Mesurer la qualité du code ne relève alors plus seulement d'une démarche d'amélioration ponctuelle mais devient un véritable levier de pilotage.

T.T

Mobilité

Surfshark analyse la collecte de données par les navigateurs mobiles

Le spécialiste de la cybersécurité évalue le respect de la confidentialité des données par les navigateurs mobiles. Les leaders sur leur marché se révèlent les plus gourmands.

A quel navigateur mobile se fier ? Lequel d'entre eux aspire le plus de données confidentielles ? Sans se prononcer clairement en faveur de l'un ou de l'autre, le spécialiste de la cybersécurité Surfshark propose une cartographie autour de trente-huit types de données collectables et décerne les bons et les mauvais points à quinze browsers mobiles figurant parmi les plus populaires en France. Cette étude compilée sur l'an dernier apporte aussi des comparaisons, tant sur les parts de marché des uns et des autres que des pratiques observables en Europe, du Cap Nord à Gibraltar.

Pour établir son palmarès, Surfshark a sérié les trente-huit types de données selon leur finalité (financières, localisation, etc.) et surtout leur partage avec des tiers. Et le plus vorace se révèle également le plus « indiscret »... En effet, le navigateur russe Yandex — qui détient 17 % de son marché domestique, collecte vingt-cinq types d'informations contre vingt pour Google Chrome. Davantage, outre des données de localisation, ce browser récolte des contacts, des informations financières, des fichiers et documents... et les messages privés intégrés dans l'application ! Google Chrome et Microsoft Edge se classent en tête des plus grands

collecteurs de renseignements, avec vingt types de données recueillis chacun, tandis que Firefox Mozilla et Samsung Internet se montrent plus frugaux : six types de données pour le premier contre seulement deux typologies chez le second.

Les plus indiscrets

Outre les plus gourmands, l'étude Surfshark sur la confidentialité distingue aussi les plus « gourmets », à savoir ceux qui se délectent de données potentiellement à forte valeur ajoutée : celles sur les performances des applications, l'activité de l'utilisateur dans l'appli, des identifiants de l'appareil employé, les informations personnelles, et enfin l'historique de navigation sur

le web. Outre Yandex, qui ajoute la carte du recueil de « renseignement » à son cœur de métier, deux browsers se détachent : Google Chrome et Microsoft Edge. Le premier apprécie les données analytiques, autour de la personnalisation, de la gestion des comptes et sur les fonctionnalités des applis. Quant au second, il ne se satisfait pas que des informations de localisation puisqu'il s'intéresse aux identifiants, aux contenus, voire aux dossiers et fichiers sur son chemin.

Cette aspiration de données ne se limite pas toujours aux seuls besoins des navigateurs. Ces derniers les partagent aussi avec des tiers. Edge reroute les identifiants et les coordonnées de location. Chrome livre les informations et autres identifiants de celles et ceux qui le sollicitent, voire certains éléments de sécurité. A contrario, Mozilla Firefox navoue en partager qu'une petite partie vers des partenaires publicitaires. Seul Samsung Internet ne s'adonne pas à ces pratiques. *« Qu'un navigateur collecte des données pour améliorer le fonctionnement de ses outils, cela ne pose pas de problèmes ; on peut néanmoins se poser des questions quant à leur risque de transmission, volontaire ou suite à un piratage, à des tiers publics ou privés, plus ou moins bien intentionnés »* s'inquiète Luis Costa, research & insights team lead chez Surfshark.

Les navigateurs leaders du marché français se montrent bien plus respectueux de la confidentialité des données de leurs utilisateurs que leurs filiales chez certains voisins européens. Pour

Luis Costa, le niveau de risque dans l'Hexagone « demeure modéré, moins élevé qu'en Allemagne ou en Espagne. Mais plus haut qu'en Norvège ». **V.B**

Luis Costa, research & insights team lead chez Surfshark



Intelligence artificielle

Salesforce étend Mulesoft Agent Fabric

Salesforce annonce l'extension de MuleSoft Agent Fabric avec de nouvelles fonctionnalités de découverte automatisée et de catalogage, permettant d'identifier et de gérer les agents IA à travers plusieurs écosystèmes cloud.



Avec « Agent Scanners », les entreprises peuvent détecter et enregistrer automatiquement des agents déployés sur Agentforce, Bedrock (Amazon), Vertex AI (Google Cloud), ainsi que d'autres plateformes, afin d'assurer une visibilité unifiée, une gouvernance renforcée et une meilleure maîtrise des déploiements.

L'extension de Mulesoft Agent Fabric unifie et simplifie cet écosystème fragmenté au sein d'un réseau d'agents gouverné et cohérent, offrant une console unique pour l'ensemble des agents IA, les outils et les métadonnées. Pour les autres actifs, tels que les serveurs MCP (Model Context Protocol) et les agents personnalisés, des fonctionnalités supplémentaires rendent leur enregistrement simple et rapide. En facilitant l'intégration de tout agent ou serveur MCP, quel que soit le fournisseur, Salesforce vise à proposer une plateforme ouverte, interopérable et de

confiance, permettant aux organisations de déployer pleinement le potentiel de leur agentique.

Les agent scanners analysent chaque agent en profondeur et extraient automatiquement ses fonctionnalités spécifiques (interroger une base

de données ou traiter un remboursement), les grands modèles de langage (LLM) qui le pilotent, ainsi que les données accessibles. Ces métadonnées sont ensuite normalisées et cartographiées selon les spécifications du protocole standard « agent-to-agent » (A2A) de Google Cloud. Toutes les informations identifiées par les agents scanners sont synchronisées en continu avec le MuleSoft Agent Registry, un catalogue central dans lequel les agents, les serveurs MCP et les outils d'IA peuvent être enregistrés et rendus accessibles aux développeurs ou à d'autres agents. Afin de garantir qu'aucun actif IA ne soit oublié, MuleSoft Agent Fabric propose également des mécanismes d'enregistrement flexibles pour les agents développés en interne et les serveurs MCP, via une simple URL, ainsi qu'un répertoire sélectionné de serveurs MCP publics issu de l'Official MCP Registry. MuleSoft Agent Visualizer offre une vue d'ensemble de l'empreinte IA et des fonctions avancées de recherche et de filtrage. Il devient, par exemple, possible de comparer en quelques clics les agents déployés sur Amazon Bedrock et ceux opérés sur Vertex AI.

B.G

L'IA agentique accélère en France

Selon la 11^e édition du Connectivity Benchmark Report de MuleSoft, les organisations françaises utilisent aujourd'hui en moyenne 15 agents IA, un chiffre qui devrait progresser de 67 % au cours des deux prochaines années. Cette montée en puissance s'accompagne toutefois de défis majeurs en matière d'orchestration et de gouvernance. Près de la moitié (49 %) des agents IA fonctionnent encore en silos plutôt qu'au sein de systèmes multi-agents. Cette fragmentation entraîne des processus fragmentés, des automatisations redondantes et une exposition accrue aux agents non autorisés ou au shadow AI. Le nombre d'applications dans les entreprises françaises est passé de 692 à 770 en un an, alors que seulement 35 % sont intégrées entre elles. Face aux défis d'intégration et aux silos d'agents, 85 % des responsables IT craignent que les agents n'ajoutent plus de complexité que de valeur.

Agentique

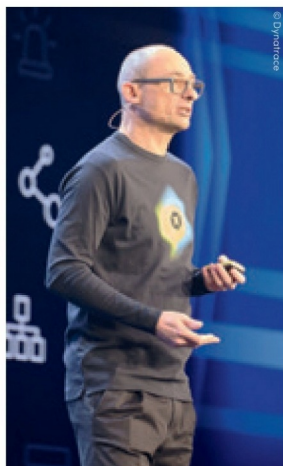
Dynatrace Intelligence veut rendre l'IA opérationnelle enfin fiable

À Dynatrace Perform (28 et 29 janvier à Las Vegas), Dynatrace a esquissé une nouvelle frontière de l'observabilité : des systèmes capables d'analyser, décider et agir de façon autonome, sans compromis sur la fiabilité. Avec Dynatrace Intelligence, l'éditeur mise sur une IA agentique ancrée dans des données causales et déterministes pour dépasser les limites de l'IA générative en environnement d'entreprise.

Dynatrace a montré que là où les premières vagues d'observabilité visaient surtout la visibilité et la corrélation d'événements, l'enjeu est désormais d'autoriser des systèmes à analyser, décider et agir de manière autonome, sans compromettre la fiabilité des opérations. C'est précisément sur ce terrain que l'éditeur entend se distinguer avec Dynatrace Intelligence, un système d'opérations agentiques conçu pour répondre aux limites structurelles de l'IA générative, lorsqu'elle est appliquée aux environnements d'entreprise.

Pourquoi l'IA générative ne suffit pas

L'essor des agents basés sur des LLM a profondément modifié la façon dont les équipes IT envisagent l'automatisation. Mais comme le rappelle Bernd Greifeneder, directeur technique et fondateur de Dynatrace, « les modèles de langage sont probabilistes par nature ». Autrement dit, leur performance repose sur des probabilités statistiques, et non sur des certitudes factuelles. Cette caractéristique devient problématique



Bernd Greifeneder, directeur technique et fondateur de Dynatrace, lors de la présentation de Dynatrace Intelligence

dès que plusieurs décisions sont enchaînées. Une précision individuelle élevée ne garantit en rien la fiabilité globale d'un processus distribué

entre agents. Plus le nombre d'interactions augmente, plus le risque d'erreur cumulative s'accroît. A cela s'ajoute la contrainte des volumes de données : exposer directement des agents génératifs à des téraoctets ou des pétaoctets de logs, de métriques et d'événements dépasse leurs capacités de contexte et accroît le risque d'erreurs.

Recentrer l'IA sur les faits, la causalité et le temps réel

Face à ces limites, la solution adopte donc une approche différente. Plutôt que de tenter d'améliorer indéfiniment les capacités génératives, l'éditeur mise sur l'introduction massive de déterminisme dans les boucles décisionnelles. Ainsi, plus les données fournies à l'IA sont structurées, contextualisées et causales, plus les résultats sont fiables et exploitables. Cette approche s'incarne d'abord dans Grail, le data lakehouse unifié de Dynatrace. Conçu pour ingérer et corréler en continu métriques, logs, traces, événements, sessions utilisateurs, données métiers et signaux de sécurité, Grail se distingue par sa flexibilité sans schéma imposé ni index préalable. Cette architecture permet aux agents d'interroger instantanément l'ensemble des données. À cette couche de données s'ajoute Smartscape, le graphe de dépendances en temps réel qui modélise l'environnement observé sous forme de relations causales explicites.

Dynatrace Intelligence, un système agentique natif et orchestré

C'est sur cette base que Dynatrace Intelligence prend forme. Présentée comme une évolution majeure de



Dynatrace Intelligence a été présentée lors de la Dynatrace Perform, qui s'est tenue à Las Vegas, les 28 et 29 janvier derniers.

la plateforme, elle se définit comme un système d'exploitation agentique natif, capable d'évoluer dynamiquement avec les environnements qu'il supervise. L'architecture repose sur un agent opérateur central chargé de la planification, de l'orchestration et de la coordination des autres agents. Au cœur du dispositif, trois agents déterministes jouent un rôle structurant. Le premier se consacre à l'analyse des causes racines, en parcourant en quelques secondes des millions de dépendances causales pour identifier l'origine d'un dysfonctionnement. Cette capacité dépasse ce que pourraient offrir des agents purement génératifs, contraints par des limites de raisonnement séquentiel et de contexte. Le second agent est dédié à l'analytique à grande échelle. Il transforme des volumes massifs de données brutes en informations enrichies, contextualisées et exploitables par les agents génératifs. Il sait interroger Grail de manière optimale et intégrer des sources supplémentaires sans rompre la cohérence globale du contexte. Enfin, le troisième agent se concentre sur la prévision. Cet agent

permet une prévention proactive à grande échelle, en identifiant les tendances et les risques émergents de manière fiable.

Des résultats mesurables sur les usages SRE

L'architecture a été validée par des benchmarks concrets sur des cas d'usage SRE (Site Reliability Engineering). Lorsqu'un agent externe est combiné aux agents déterministes de la plateforme, les taux de succès des opérations augmentent, la résolution des problèmes s'accélère et les coûts associés à l'usage des modèles génératifs diminuent. Plus les environnements observés sont vastes et complexes, plus ces gains deviennent significatifs, ce qui renforce l'intérêt du modèle pour les grandes entreprises multicloud et AI-native.

Dynatrace Intelligence est conçue pour fonctionner au sein d'un écosystème ouvert. Les agents peuvent collaborer avec « des hyperscalers, ServiceNow ou Atlassian, tout cela est désormais disponible pour nos clients », précise Steve Tack, chef de produits de Dynatrace. Cela permet de déclencher des actions concrètes dans les

outils déjà utilisés par les équipes, qu'il s'agisse de gestion des incidents, de pipelines DevOps ou de plateformes cloud. Cette approche vise à étendre l'autonomie opérationnelle sans enfermer les organisations dans une dépendance technologique unique. Pour Bernd Greifeneder, l'enjeu dépasse la seule performance technique. « Dynatrace Intelligence fusionne l'IA déterministe et l'IA agentique, élimine les approximations et fournit une observabilité pilotée par l'IA dans laquelle les organisations peuvent avoir confiance », explique-t-il. L'objectif est de libérer les équipes pour des tâches à plus forte valeur stratégique. « Avec Dynatrace Intelligence, nous pouvons poser des questions en langage naturel pour comprendre un incident. La plateforme propose une analyse, identifie des causes probables et suggère des actions concrètes », explique de son côté Victoria Ruffo, responsable d'équipe d'ingénierie logicielle de Freedompay.

Une trajectoire progressive vers des opérations autonomes

Dynatrace positionne Intelligence comme un socle permettant une adoption graduelle de l'autonomie. Les entreprises peuvent débuter par des recommandations enrichies par l'IA, évoluer vers des automatisations supervisées avec validation humaine, puis activer des mécanismes pleinement autonomes encadrés par des politiques et des garde-fous explicites. Disponible dès à présent sur un modèle de consommation à l'usage et accessible à l'ensemble des clients de la plateforme, Dynatrace Intelligence ambitionne de transformer l'IA opérationnelle. En ancrant les agents dans des données causales, contextuelles et temps réel, Dynatrace cherche à faire passer l'IA d'un outil incertain à un moteur fiable d'opérations autonomes, capable de soutenir durablement la complexité croissante des environnements numériques.

M.C

IN CYBER
FORUM
EUROPE

**31 MARS
2 AVRIL 2026**
LILLE GRAND PALAIS

Maîtriser nos dépendances numériques

Venez découvrir le monde de la cyber et explorez les enjeux
de demain: menaces, solutions, opportunités.



ORGANISÉ PAR

Forward

RETROUVEZ-NOUS SUR





Écosystème

Le petit monde de l'informatique bouge vite, très vite. Du futur dans l'alimentation des centres de données, à une étude sur les tendances salariales, la rubrique couvre de larges aspects de ce que vivent les informaticiens au jour le jour. Nous rendons aussi un hommage à Ada Lovelace, une personnalité marquante de l'informatique.

RH

Conserver la conformité RGPD

Maintenir dans la durée de la conformité RGPD des données RH demande un suivi rigoureux de la DRH et une bonne gouvernance.

Le département RH traite des informations particulièrement sensibles : dossiers collaborateurs, candidatures, absences, évaluations, pièces contractuelles. Pierre-Christophe Lagemann, directeur produit de Peoplespheres, éditeur montpelliérain d'une plateforme SIRH qui compte 350 entreprises clientes, explique les différents facteurs de risques en matière de conformité au règlement général sur la protection des données (RGPD) : « Certes, le service RH gère déjà, dans le cadre légal, des données sensibles avant l'entrée en vigueur du RGPD en 2018. Il est donc plutôt sensible aux obligations liées à ce règlement européen. »

Une chaîne de responsabilités bien définie doublée d'une chaîne de communication bien huilée

« Mais le RGPD implique une chaîne de responsabilités à bien définir, c'est parfois là où ça pêche », remarque M. Lagemann. « Il faut bien clarifier le

périmètre de responsabilités de chaque acteur de la chaîne. En général, le DRH est responsable du traitement des données, le DSI est support technique, et les éditeurs sous-traitants doivent présenter des garanties suffisantes vis-à-vis des exigences du RGPD. Cette chaîne doit se doubler d'une bonne chaîne de communication. Nous conseillons d'avoir un responsable qui connaît tous les acteurs de la chaîne, sait qui sont leur sous-traitants, qui contacter. »

Être sensible et bien connaître ses obligations, les assurer dans la durée

Il poursuit : « La DRH, épaulée par la DSI, doit établir de façon fine les droits d'accès aux fonctionnalités et aux différentes catégories de données dans le SIRH. Nous donnons des formations à notre outil, ainsi que les bonnes pratiques d'utilisation. Par ailleurs, les RH peuvent pécher par ignorance. Dans les PME, le responsable RH exerce différentes fonctions et a des connaissances RGPD variables. Mais c'est surtout le niveau de sensibilité aux enjeux du



Pierre-Christophe Lagemann,
directeur produit
de Peoplespheres

RGPD des responsables qui s'avère déterminant. C'est enfin un problème d'assiduité dans la durée : en général, la mise en place est conforme, mais le jour où il y a un problème, les actions à mener peuvent sembler floues. Nous accompagnons en cas de besoin. »

En pratique, la maîtrise réelle du parcours des données, entre outils empilés, intégrations et prestataires, comporte des risques en matière de RGPD. Beaucoup d'organisations pensent être conformes parce qu'un contrat existe, alors que la chaîne de sous-traitance, la traçabilité et la localisation restent floues. Et quand un droit d'accès ou d'effacement tombe, ou qu'un incident survient, cette zone grise devient un risque immédiat. Héloïse Feuillu, juriste et déléguée à la protection des données (DPO) de Peoplespheres, conclut : « L'enjeu principal est la bonne gouvernance, à conserver dans la durée : comprendre l'essence du RGPD, documenter les traitements, sécuriser les processus et la sous-traitance, maîtriser la localisation, et tenir les délais quand les demandes RGPD arrivent. »

Bien choisir ses solutions RH

Dans le choix d'un SIRH ou d'une application RH, plusieurs critères sont à prendre en compte en termes de maturité RGPD :

- un contrat encadrant bien la prestation et prenant en compte les sous-traitants de l'éditeur ;
- la sécurité et la traçabilité des données ;
- la localisation des serveurs d'hébergement, les données à caractère personnel devant par défaut être hébergées au sein de l'Union européenne. Un transfert hors UE nécessite de fournir des garanties appropriées ;
- des garanties techniques et organisationnelles et le privacy by design ;
- la gestion des rôles et des droits dans l'application.

C.C

Formation

Le mentoring ? Ça marche !

Constel Monitoring propose une plateforme sociale de mentoring pour pallier le départ des seniors et éviter la perte de savoir dans les entreprises.

Habituellement, les entreprises accueillent les nouveaux et juniors avec un processus bien calé, et les formations nécessaires reposent sur des plateformes d'e-learning avec des programmes répondant à plusieurs fonctions dans l'entreprise. Constel Mentoring défend une approche totalement différente qui s'appuie sur les possibilités que peut apporter le rencontre entre personnes, mentors et mentorés. Paul Cartier, fondateur et patron de l'entreprise, est enthousiaste : « *la rencontre entre certaines personnes peut faire des étincelles* ». Même s'il assure que cela ne fonctionne pas tout le temps. « *C'est la rencontre, le partage d'expériences et de connaissances qui font que, dans les organisations, un projet va être mené à bout. Se rencontrer pour faire quelque chose ensemble. Par exemple, en école, je vais rencontrer un alumni qui est dans un secteur que je ne connaissais pas, mais que je trouve passionnant, cela va me permettre d'avoir mon premier CDI dans cet écosystème.* »

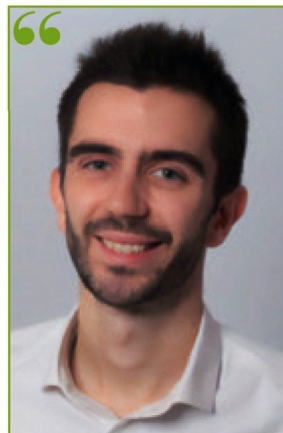
Les demandes changent

« *Sur les dernières années, les demandes sur les programmes de mentorat restaient à la marge. Les gros sujets concernaient l'onboarding, la formation des nouveaux managers. C'est ce qui ressortait le plus dans les sociétés. Depuis 3 mois, le plus grand nombre de programmes de mentorat qui a été demandé porte sur la transmission intergénérationnelle* », constate Paul Cartier. Il ajoute : « *on a des gens qui partent, et les entreprises*

se rendent compte qu'ils savent plein de choses. Ils savent notamment des règles un peu tacites qui ne sont pas formalisées et qui ne peuvent pas être formalisées. À leur départ, on perd cet ADN, cette culture d'entreprise qui s'est créée avec eux. Parce qu'en plus, dans la génération des années 80-90, il y a beaucoup de gens qui ont fait toute leur carrière dans la même boîte, qui incarnent vraiment cette culture. Ce sont ces personnes qui ont les connaissances ultra spécifiques sur un métier, une manière de faire, etc. ». Il constate de plus que la réforme des retraites, même avortée, a amplifié les demandes de mentoring dans l'optique de passer le savoir dans l'entreprise.

Des programmes sur mesure

Constel Monitoring ne développe pas des modèles de mentoring pour tout. La première phase repose sur une structuration du projet de mentoring. Paul Cartier précise : « *on définit exactement le cadre et souvent, d'ailleurs, on commence par un premier programme de mentorat pour l'onboarding des collaborateurs du département marketing et, petit à petit, on déploie de nouveaux programmes de mentorat sur de nouveaux objectifs. C'est ça qui donne des idées aux clients, et c'est ça qui fait qu'on grandit. C'est de la structuration. Ensuite, nous définissons toutes les modalités pratiques du programme de mentorat. On a vu passer plein de programmes, on a vu passer les bonnes pratiques, mais on a aussi vu passer les erreurs qu'il faut éviter. Notre rôle*



La rencontre entre certaines personnes peut faire des étincelles.

Paul Cartier,
fondateur et patron de
Constel Monitoring

est alors de conseiller notre client sur ces points, tout en sachant qu'à la fin, c'est lui qui a le fin mot sur la manière dont il veut le mettre en place ». La plateforme se fonde sur différents algorithmes pour faire correspondre mentors et mentorés, et s'appuie principalement sur des modèles de Mistral AI. Des fonctions de collaboration et de partage de documents complètent le dispositif. Pour l'infrastructure, l'application repose sur le Cloud de Scalingo.

B.G

Tendances

Des salaires en forte hausse pour les experts

Les entreprises sont prêtes à offrir de très bons salaires et augmentations aux profils expérimentés et spécialisés dans l'IA, la cybersécurité et le management de la transformation. Les autres profils perçoivent des augmentations de salaires contenues.

	10 - 15 ans	+ 15 ans
Chief Digital Officer	135 - 190 K€	190 - 315 K€
Directeur E-commerce	115 - 155 K€	160 - 210 K€
Chief Performance Officer	125 - 170 K€	170 - 230 K€
Chief Communication Officer	95 - 125 K€	125 - 150 K€
Chief Omnichannel Officer	115 - 160 K€	160 - 210 K€
Chief Marketing Officer	115 - 150 K€	150 - 210 K€
Chief Data Officer	105 - 190 K€	190 - 270 K€
Chief Revenue Officer	135 - 190 K€	190 - 315 K€
Chief Transformation Officer	115 - 190 K€	190 - 315 K€
DRH / Chief People Officer	115 - 160 K€	160 - 220 K€
Chief Customer Experience Officer	105 - 170 K€	170 - 220 K€
Chief Technology Officer	140 - 200 K€	200 - 280 K€
Chief Information Officer	125 - 170 K€	170 - 235 K€
Chief Product Officer	115 - 170 K€	170 - 245 K€
Chief CSR Officer	115 - 160 K€	160 - 210 K€
Chief Security Officer	135 - 190 K€	190 - 245 K€
Chief AI Officer	145 - 200 K€	200 - 275 K€

Salaires médians bruts annuels en fonction de l'expérience dans les postes de direction — Source : HR Pulse, benchmark des salaires 2026 — Aravati

En 2025, les augmentations globales dans les métiers du numérique se situent en moyenne autour de 0 à 3 %, sauf pour les profils stratégiques qui atteignent 6 % voire davantage, selon le benchmark annuel sur les salaires du cabinet de recrutement Aravati publié fin 2025, « HR Pulse »*. Les profils très spécialisés dans des domaines stratégiques (intelligence

artificielle, cybersécurité, cloud, transformation organisationnelle) voient leurs rémunérations médianes progresser de 5 à 14 % en 2025, en raison de la rareté et de l'impact de leurs compétences, de même que les profils hybrides, multi-compétences, tel un data scientist expert en IA. Les profils plus généralistes connaissent une légère hausse, voire une stagnation du

salaires médians. La progression est plus modérée sur les profils juniors et confirmés que chez les top managers, qui doivent diriger des missions de plus en plus complexes de transformation. Hymane Ben Aoun, directrice générale d'Humanskills, qui rassemble des entreprises de services RH (dont Aravati qu'elle a cofondée), analyse : « Les entreprises recrutent pour leurs projets de mise en place ou de déploiement étendu de l'IA. Elles recherchent des experts techniques pour modéliser et construire les référentiels de données pertinents pour les IA et qui, curieux, réfléchissent au fonctionnement des IA, comment les corriger, les piloter. Aujourd'hui, tout poste de direction implique une bonne compréhension des enjeux et des cas d'usage de l'IA. Par ailleurs, l'IA démocratise l'accès à l'information complexe. Aussi, quand une partie du travail des juniors peut être réalisée par l'IA, il faut réfléchir à comment les faire grandir, faire évoluer leur rôle vers la coordination. »

Forte demande de management intégrant l'IA

Les dirigeants pilotent désormais des missions de transformation à la croisée du digital, de l'IA et de la transition énergétique, ce qui revalorise leurs rôles. Tous les postes exécutifs liés à la stratégie IA deviennent cruciaux, avec une hausse moyenne du salaire fixe de 5 à 8 %, et des bonus de performance. Les grandes fonctions tech, data, produit, risque et RH intègrent désormais l'IA dans leur périmètre. Les fonctions managériales de gouvernance et d'éthique gagnent en importance. Les postes de directeur de la transformation, directeur digital et directeur data sont particulièrement recherchés.

Data et IA au sommet

Les métiers de la data et de l'IA, dont l'impact business est le plus immédiat, restent parmi les plus valorisés, avec en moyenne +4 à 6 % pour les premiers (sauf juniors et profils généralistes, en stagnation), +5 à 8 % pour les seconds. Les profils data avec la maîtrise de LLM (grands modèles de langage), d'IA générative, ou de la gouvernance des données peuvent obtenir 10 à 15 K€ de salaire de plus que leurs confrères. Aravati observe un boom des rôles liés à l'IA générative, au fine-tuning de modèles LLM, à l'orchestration et à la gouvernance de l'IA. Les profils ayant déjà industrialisé des solutions IA en entreprise sont rares, donc très primés. Trois types de profils sont très sollicités, les premiers étant ceux intervenant sur la création des modèles autour des LLM comme ingénieur ou architecte solutions IA. Les seconds sont les profils spécialisés pour nourrir les modèles LLM : ingénieur data, ingénieur machine learning. Les derniers encadrent et industrialisent l'IA, comme le stratège IA, les spécialistes sécurité ou éthique de l'IA. « *En IA et en data avancée, les augmentations peuvent atteindre 10 à 14 %, souligne Hymane Ben Aoun. Le stratège IA, très demandé, travaille sur les cas d'usage IA, identifie les solutions à utiliser et pilote le changement : il écoute, accompagne et rassure face aux résistances et peurs vis-à-vis de l'IA, vue par certains comme destructrice d'emplois.* »

L'ère de cyber + AI ops

Parmi les profils techniques et IT, les métiers de la cybersécurité deviennent plus stratégiques, et techniques, entrant dans une ère de cyber + AI ops, où l'humain reste décisif pour arbitrer, anticiper et garantir l'éthique. Les entreprises recherchent dans le domaine de la cybersécurité des ingénieurs IA, des ingénieurs de fiabilité de site (SRE), des ingénieurs et architectes cloud, ainsi que des pentesters. Les profils IT combinant expertise technique, compréhension business et

	0 - 3 ans	3 - 5 ans	5 - 10 ans	+10 ans
Machine Learning Engineer	45 - 65 K€	70 - 90 K€	90 - 120 K€	120 - 160 K€
Deep Learning Engineer	45 - 70 K€	75 - 95 K€	95 - 130 K€	130 - 180 K€
AI Research Scientist	45 - 70 K€	75 - 100 K€	100 - 130 K€	130 - 180 K€
AI Solutions Architect	-	75 - 100 K€	100 - 140 K€	140 - 180 K€
AI Strategist	45 - 60 K€	65 - 90 K€	90 - 120 K€	120 - 160 K€
Robotics Engineer	50 - 70 K€	70 - 90 K€	90 - 120 K€	120 - 160 K€
Computer Vision Engineer	50 - 70 K€	70 - 90 K€	90 - 120 K€	120 - 160 K€
AI Engineer	50 - 70 K€	70 - 90 K€	100 - 130 K€	130 - 170 K€
Machine Learning Ops (MLOps)	45 - 60 K€	60 - 80 K€	80 - 110 K€	110 - 150 K€
AI Security Specialist	60 - 80 K€	80 - 100 K€	100 - 130 K€	130 - 170 K€
Spécialiste éthique de l'IA	50 - 70 K€	70 - 90 K€	90 - 120 K€	-
Coach en IA	-	55 - 70 K€	70 - 90 K€	90 - 120 K€
Chief AI Officer	-	-	130 - 180 K€	180 - 230 K€
Prompt Engineer	45 - 60 K€	60 - 80 K€	80 - 110 K€	110 - 140 K€
Generative AI Product Manager	-	70 - 95 K€	95 - 130 K€	130 - 170 K€
RAG (Retrieval-Augmented Generation) Engineer	-	70 - 90 K€	90 - 120 K€	120 - 160 K€
LLM engineer	-	60 - 88 K€	70 - 110 K€	110 - 130 K€
Data Governance Lead	-	70 - 95 K€	85 - 110 K€	110 - 140 K€
Ethical AI Officer	-	80 - 100 K€	100 - 130 K€	130 - 160 K€
AI Product Owner	-	65 - 85 K€	85 - 110 K€	110 - 140 K€

Salaire médian brut annuel en fonction de l'expérience dans l'IA
— Source : HR Pulse, benchmark des salaires 2026 — Aravati.

leadership sur les projets stratégiques sont particulièrement valorisés. Les profils très spécialisés, comme l'ingénieur ou l'architecte cloud, sont en tension. Les profils plus généralistes (développeurs standard, administrateurs systèmes ou support IT) connaissent des augmentations plus modestes, de l'ordre de 3 %. « *Les développeurs codent de plus en plus assistés par des IA ; développeurs, formez-vous aux IA, jouez et essayez de nouvelles choses avec !*, » conseille Hymane Ben Aoun.

Hybridation des métiers du produit

Les profils de product owner spécialisé data ou IA progressent (+5 à 8 % d'augmentation), au détriment du product owner généraliste (-1 à +2 % de salaire). L'hybridation des compétences data/produit/expérience devient centrale, avec des ponts vers des rôles en expérience client ou stratégie design. Les rôles stratégiques et

d'encadrement restent très demandés. Le métier de product ops, dont la fonction consiste à industrialiser la productivité et améliorer les mesures d'impact, monte en puissance. La maîtrise de l'IA générative dans la conception produit devient un avantage différenciant majeur.

Industrialisation du design

Les métiers du design digital restent essentiels, mais leur progression salariale est limitée à 2 à 4 %, car l'offre de profils est plus importante. L'étude montre néanmoins une forte montée des salaires côté UX stratégique, design ops et design system, grâce à l'industrialisation du design. L'IA générative crée une nouvelle vague de besoins en design conversationnel, UX IA et prompt design. En 2026, expertise, en particulier en IA, et compétences hybrides, sont clefs pour progresser.

C.C

Biographie

Ada Lovelace, pionnière de l'informatique

Augusta Ada King, plus connue sous le nom d'Ada Lovelace, est née le 10 décembre 1815 à Londres. Véritable pionnière de la science informatique, elle est considérée comme la toute première programmeuse. Nous allons voir pourquoi dans cet article.



Pour en savoir plus sur cette chère Ada, n'hésitez pas à écouter le podcast qui lui est consacré sur France Culture.

Ada est la fille de Lord Byron, le célèbre poète romantique, et d'Anne Isabelle — Annabella — Milbanke, une passionnée de mathématiques surnommée la « Princesse des Parallélogrammes ». Sa mère l'initie très tôt aux mathématiques, la faisant bénéficier de l'enseignement de professeurs illustres, fait plutôt rare à une époque où les matières scientifiques étaient surtout enseignées aux garçons. Après une fugue à l'âge de 16 ans avec un certain Charles Babbage, Ada rentre chez elle pour se marier avec William King, devenant ainsi la comtesse de Lovelace.

Le premier programme informatique de l'histoire

Le mathématicien Charles Babbage, son ex-amant et précepteur, a inventé

une calculatrice mécanique avant de travailler sur la machine analytique, un système mécanique capable de réaliser une série de calculs inscrits à l'avance sur des cartes perforées. Cette machine, considérée comme le précurseur des ordinateurs, ne vit malheureusement jamais le jour faute de financement suffisant. Néanmoins, selon une expérimentation effectuée en 1991, elle aurait été fonctionnelle. Ada Lovelace traduit en 1842 de l'anglais au français les travaux de Babbage sur cette machine analytique. Elle y ajoute ses propres observations, rien moins que trois fois le volume du travail de Babbage. Ces ajouts comportent le tout premier programme informatique de l'Histoire : des instructions permettant à

la machine de calculer les nombres de la suite de Bernoulli. Ces premières ébauches d'une écriture formelle des instructions représentent ce qui est communément appelé aujourd'hui un langage informatique. Elle imagine même qu'une machine puisse, à terme, faire bien plus que de simples calculs mathématiques et créer par exemple des morceaux de musique. Elle apporte une vision analytique à cette machine que Babbage considérait avant tout comme un outil arithmétique, ouvrant la voie à de multiples applications et pressentant même l'IA. Elle avait déclaré ceci : *« Beaucoup de personnes s'imaginent que parce que la machine fournit des résultats sous une forme numérique, alors la nature de ses processus doit être forcément arithmétique et numérique, plutôt qu'algébrique ou analytique. Ceci est une erreur. La machine peut arranger et combiner les quantités numériques exactement comme si elles étaient des lettres, ou tout autre symbole général. »*

Ada meurt en 1852 à l'âge de 36 ans. Méconnue du grand public, elle a néanmoins laissé son nom à un langage de programmation objet et temps réel conçu par le département de la Défense américain entre 1977 et 1983. Le langage Ada est employé dans les technologies de pointe telles que l'aérospatial, l'aéronautique ou les transports ferroviaires. Ada Lovelace était une grande visionnaire. Elle a même inspiré les travaux du non moins grand Alan Turing pour son calculateur universel. Elle fait partie de ces grandes figures féminines trop longtemps oubliées par l'histoire des sciences, alors même que son apport aux mathématiques et surtout à l'informatique, voire à l'IA, fut réellement considérable.

T.T

Start-up

BloomUp, un guichet unique des startups

Pour répondre aux atouts des néo-banques, la banque verte se dote d'un outil dédié pour le financement bancaire des startups d'Île-de-France.

La concurrence a du bon : elle impose aux acteurs établis de s'adapter à un monde qui change. L'essor des néo-banques comme Revolut pousse le Crédit Agricole d'Île-de-France, région qui concentre 54 % des startups nationales et les trois quarts de leurs levées de fonds, à lancer une structure dédiée aux jeunes pousses : BloomUp by Crédit Agricole. « Il s'agit d'un point d'entrée unique pour les startups d'Île-de-France », précise son directeur général, Matthieu Girardon. Lancée en septembre dernier, elle promet une solution sur mesure pour les différentes étapes de leur développement, depuis leur création-amorçage jusqu'à la pérennisation de leur survie, pour les secteurs de la transition écologique et environnementale, l'énergie, la santé, le bien vieillir et l'inclusion. « Il existe d'autres dispositifs au sein du Crédit Agricole pour financer la tech pure. Cela ne nous empêchera pas d'être très vigilants sur tout ce qui touche la souveraineté numérique, aussi bien pour les solutions de stockage que pour la cybersécurité », explique-t-il.

La banque verte a doté BloomUp d'un capital de soixante-quinze millions d'euros sur cinq ans, distribués exclusivement sous la forme d'emprunts bancaires, de 30 000 à cinq millions d'euros. Et non de prises de participations. « Nous apportons du financement non dilutif des autres actionnaires, des prêts bancaires classiques ou du crédit-bail, sur deux à sept ans selon leur nature. Nous pourrions intervenir avec des investisseurs

en capital, mais la frontière entre le métier de financeur et d'investisseur doit être respectée », explique Matthieu Girardon. Cet appui bancaire sera initié « pour des startups qui arrivent à nous convaincre d'une certaine visibilité », complète-t-il.

Les dirigeants pourront aussi souscrire des assurances, pour couvrir ces prêts ou garantir leur entreprise, comme des polices hommes-clés. « Elles sont facultatives mais fortement recommandées. Nous avons un devoir de conseil surtout lorsque le succès de ces entreprises repose sur un dirigeant ou une équipe de direction », expose Matthieu Girardon. BloomUp complète cette gamme de services financiers par un accompagnement personnalisé : chaque dirigeant disposera de son propre chargé d'affaires. Ce dernier, responsable de vingt-cinq à trente jeunes pousses, pourra mettre ses relations à disposition de ses clients, au sein de

l'écosystème startups de la banque verte. Outre un accès privilégié au Village by CA, ces banquiers experts pourront aussi proposer un accompagnement juridique ou pour recruter, voire pour la connexion vers des investisseurs. « Certains pactes d'associés mal rédigés engendrent des conflits et compromettent le développement de leur société », avertit le dirigeant. Et de poursuivre, « nos équipes pourront aider ces startups à trouver leurs prochains clients et d'autres entreprises plus mûres chez les premières des expertises plus pointues autour de l'IA ou d'autres technologies ».

La banque verte compte éviter une fuite de jeunes pousses prometteuses vers des concurrents plus agiles, plus réactifs et... plus séduisantes pour les entrepreneurs. « Les néo-banques ont le mérite d'exister pour fournir rapidement aux entrepreneurs leurs premiers outils pour fonctionner, mais leur modèle trouve ses limites lors de situations qui nécessitent du conseil, du financement et de l'activation de réseau », insiste Matthieu Girardon. Pas question donc de se priver d'une source de clients pour des opérations de haut de bilan à très fortes marges...

V.B



Il s'agit d'un point d'entrée unique pour les startups d'Île-de-France.

Matthieu Girardon,
directeur général
de BloomUp

Énergie

Equinix réfléchit au SMR

Le fournisseur de solutions de colocation réfléchit à différentes pistes dont le SMR pour alimenter ses centres de données et faire face à la demande électrique due à l'intelligence artificielle.

Régis Castagné, managing director France d'Equinix, explique : « Avec des besoins énergétiques qui sont de plus en plus importants et face à ces quantités d'énergie qui vont être nécessaires, on s'est toujours posé la question chez Equinix, alors que nous sommes déjà à 96 % d'énergie renouvelable dans le monde dans nos équipements. Est-ce que c'est suffisant ? Et la réponse, en l'occurrence, est non ». Il ajoute : « dans les différentes possibilités, il y a le SMR (Small Modular Reactors) qui nous permettrait d'avoir de l'énergie décarbonée, de l'énergie sûre et de l'énergie constante. D'où ce partenariat avec Stellaria ».

Créée en 2023, cette startup développe un réacteur nucléaire de nouvelle génération. Issu du CEA et de Schneider Electric, et spécialiste des réacteurs nucléaires à neutrons rapides et à sels fondus, Stellaria a déposé sa demande d'autorisation de création (DAC) de son installation nucléaire de base (INB) Alpha auprès du ministre de la Transition écologique, chargé de la sûreté nucléaire. Elle est la première des startups françaises travaillant sur les réacteurs à neutrons rapides à soumettre sa demande.

Nicolas Breyton, fondateur et CEO de Stellaria, précise : « quand on a créé Stellaria, on s'est demandé à quoi correspondait un réacteur du 21^e siècle. Pour nous, ce réacteur, en termes de sûreté, doit être inférieur à un milli-sievert. Cela signifie que quoi qu'il se passe, pour le gars qui fait des patates à côté, en cas de tsunami, de chute d'avion ou autre catastrophe qui arrive une fois tous les 1 000 ans, pour lui, il ne



On est capable de réutiliser les combustibles des centrales existantes.

Nicolas Breyton
managing director
France d'Equinix

se passe rien. Il peut continuer à cultiver ses patates. C'est le plus important et c'est un facteur très différenciant ».

Un réacteur différent

Le patron de la startup continue : « On a un cœur qui est liquide, il peut donc être évacué très rapidement dans des réservoirs de sûreté. Il peut se dilater, changer légèrement de forme en se dilatant, cela suffit pour arrêter la fission à la vitesse

du son. En cas d'arrêt, rupture du circuit secondaire ou primaire par exemple, le système se met en sûreté et la fission se stoppe. Un delta de température assez faible suffit pour avoir une dilatation du sel. La dilatation implique un changement de densité et la réaction va s'adapter, la puissance peut être nulle. De plus, c'est un réacteur à basse pression qui fonctionne à pression atmosphérique et qui est enterré. Il est souterrain avec une dalle de béton d'un mètre vingt et possède quatre barrières de sûreté, par rapport aux EPR existants qui n'en ont que trois ».

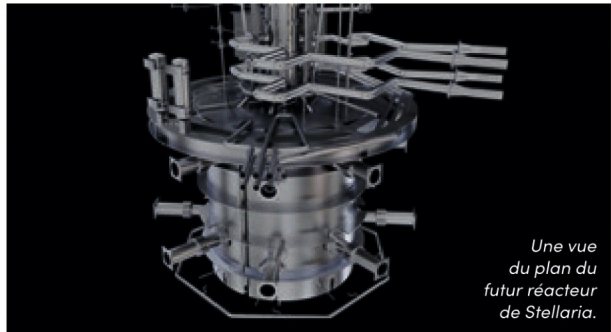
Au-delà du datacenter

Nicolas Breyton est conscient des enjeux autour de sa technologie et devance certaines interrogations possibles : « puisqu'on est en neutron dit rapide, on est capable de réutiliser les combustibles des centrales existantes. Donc, à terme, on n'aura plus besoin de mine pour faire de l'énergie. On est capable de rendre un datacenter de grande taille autonome en énergie pendant toute la durée de sa vie. Concrètement, on va progressivement transformer de l'uranium 238 en plutonium et on va brûler le plutonium au fur et à mesure, ce qui fait qu'on a toujours la même quantité de plutonium au sein du réacteur. C'est pour cela que le réacteur peut auto-entretenir sa réaction en chaîne pendant plus de 40 ans, dans son cœur, sans avoir à reprocesser le combustible ». L'idée globale est de faire plus simple que les centrales de quatrième génération qui utilisent du plutonium avec une sorte de boucle fermée pour le combustible. « On va refaire le combustible au sein du réacteur le plus longtemps possible jusqu'à ce que il y ait trop de poison neutronique, c'est à dire trop de produits de fission. Les atomes coupés en deux finissent par s'accumuler, c'est ce qui commence à

gérer la réaction en chaîne au bout d'une quarantaine d'années. Dans ce cas-là, il faut récupérer le sel et enlever les produits de fissions. Nous ne jetons pas le sel car il est encore bon et à la fin il y a toujours autant d'atomes fissiles qu'au début. Toujours autant d'énergie. C'est pour ça qu'on parle d'énergie renouvelable nucléaire. Cela ouvre la voie vers une énergie décarbonée et pilotable pour des siècles. Notre objectif est d'accompagner notre client Equinix non seulement en France, mais bien sûr aussi en Europe et à l'étranger. Equinix a plus de 270 datacenters dans le monde et nous sommes là pour fournir une technologie qui soit déployable ».

S'appuyer sur un design industrialisable

Nicolas Breton indique : « nous allons engager des travaux de pré-développement d'un site type avec Equinix, et cela va nous permettre de répondre à plusieurs questions. Que se passe-t-il quand on arrête un réacteur ? Est-ce que on doit avoir un contrat de backup de puissance avec le réseau, ou est-ce que l'on a un backup gaz qui serait déjà mieux que le diesel ? Un



Une vue du plan du futur réacteur de Stellaria.

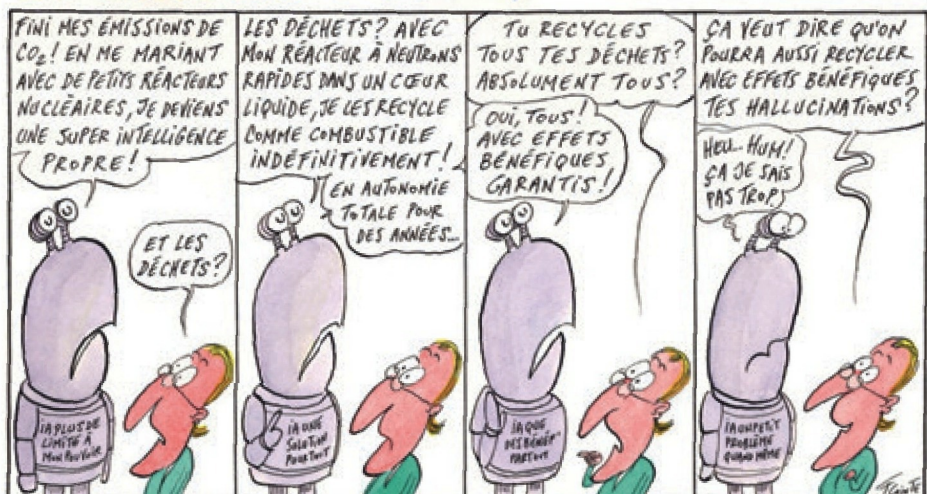
design 3D de ce site va aussi nous permettre d'avoir une idée très large du budget de ce que pourrait être un site comme celui-ci ».

Régis Castagné ajoute : « En fin de compte, on va y arriver très vite puisque notre objectif est, d'avoir défini ce blueprint à la fin de ce premier trimestre, et ensuite de se lancer dans le rétroplanning. Alors effectivement, on parle d'années, mais nous sommes sur un horizon finalement pas si lointain ». Le patron de Stellaria prévoit : « à partir de 2034, nous allons pouvoir déployer des datacenters durables, l'objectif sera

ensuite de mettre en place une machine industrielle avec une alliance industrielle. Stellaria ne va pas tout faire. On ne pourra pas être utility opérateur de réseau, ni vendre des kilowattheures. Stellaria se concentre sur la révolution technologique de passer d'un cœur solide à un cœur liquide avec des sels fondus à neutrons rapides ». Régis Castagné précise : « très clairement, nous allons avoir besoin de datacenters de plus en plus importants et ces datacenters vont avoir besoin de plus en plus d'électricité, mais ce de la manière la plus respectueuse ».

B.G

DU NUCLÉAIRE POUR L'IA





Cybersec

Ce mois-ci, la rubrique fait le point à la fois sur les attaques marquantes récentes et les nouvelles solutions pour se protéger de celles-ci. Une mention spéciale sur la solution de portefeuille numérique testée par Generali pour ses conseillers, afin de sécuriser et simplifier les échanges avec les assurés via la solution de BeYs, Kipmi. Nous faisons aussi un point d'étape sur la conformité avec notre échange avec l'AFCDP.

Chiffrement

GrapheneOS s'expatrie hors de France

GrapheneOS, l'alternative sécurisée à Android qui rend les téléphones inviolables, quitte la France en urgence suite à la parution d'un article pour le moins médisant. Nous allons voir ce qu'il en est dans cet article.

L'organisation canadienne à but non lucratif conceptrice du système d'exploitation mobile le plus sécurisé au monde n'a pas du tout apprécié les accusations du journal *Le Parisien*. Dans son article controversé du 24 novembre 2025, ce dernier a présenté GrapheneOS comme le meilleur allié des criminels. Ce système d'exploitation mobile dérivé d'Android est exclusivement disponible sur les smartphones Google Pixel, afin de tirer parti de la puce Titan M2. Celle-ci est essentielle pour le Verified Boot et le chiffrement avancé.

Fuite en quatrième vitesse

Toute l'infrastructure a migré en trois jours. La rupture a été aussi inédite que brutale. L'article s'est appuyé sur des déclarations de la police judiciaire qui a présenté GrapheneOS comme un système conçu dans le seul but de permettre aux criminels d'échapper à des investigations. Ce sont ces affirmations ayant pour origine un amalgame entre le projet légitime et des versions pirates modifiées par des acteurs malveillants qui ont provoqué la colère des développeurs. La fondation a déménagé tous ses serveurs dans des États plus respectueux des libertés.

Un projet open source pour défendre les libertés

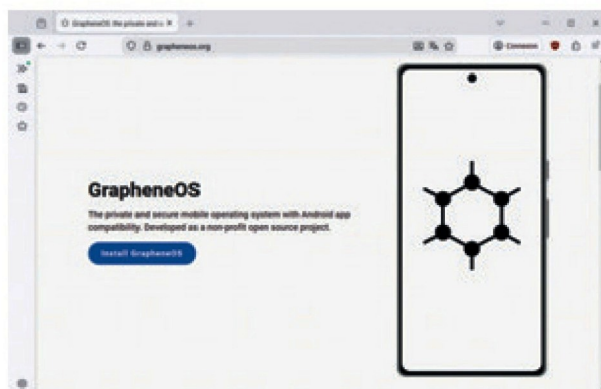
GrapheneOS, basé sur le code source d'Android, a été initialement conçu en 2014 sous le nom de CopperheadOS. Une

rupture en interne a conduit ses développeurs à s'émanciper en 2019. L'objectif principal de GrapheneOS est d'appliquer des mécanismes de sécurité avancés au niveau du noyau Android, des permissions, de la gestion de la mémoire et de l'isolation des applications. Les accusations d'entrave aux enquêtes tiennent à l'état du téléphone au moment de la saisie par la police. Si le smartphone est éteint ou a été redémarré, il devient un coffre-fort inviolable. Ancrées dans la puce et non dans la mémoire vive, les clés de chiffrement sont inaccessibles sans le mot de passe saisi après le démarrage. Même les outils les plus performants des services de police se révèlent inefficaces contre cette protection. Preuve que le

système remplit sa promesse en matière de sécurité et protège efficacement ses utilisateurs légitimes (journalistes et militants divers).

Le chiffrement constamment attaqué

L'équipe de GrapheneOS a rappelé le principe de neutralité de la technologie. Elle ne peut être tenue pour responsable de l'utilisation criminelle de son outil. C'est l'éternel problème entre la recherche de chiffrement sécurisé pour assurer la liberté de tous et le désir des États de vouloir tout contrôler pour des raisons de sécurité. Il ne faut jamais perdre de vue que des États de plus en plus sécuritaires peuvent se servir de ce contrôle pour espionner des militants et des journalistes. Les États totalitaires en sont la preuve vivante. Les États démocratiques semblent danser sur cette ligne fragile avec des tendances de plus en plus totalitaires, même s'ils invoquent de « bonnes » raisons. Ces faits interviennent en pleine discussion sur la loi de l'UE sur le contrôle des chats. **T.T**



Le chiffrement cristallise les tensions entre deux impératifs : la sécurité et la protection de la vie privée, face à la lutte contre la criminalité. GrapheneOS en est la preuve éloquente.

Conformité

Generali teste un **wallet numérique**

Dans le cadre de son plan stratégique Boost qui couvre une période jusqu'en 2030, l'assureur souhaitait innover pour améliorer son expérience client et celle de ses salariés.

Une solution du portefeuille numérique Kipmi de BeYs a été testée avec succès.



Jean Remond, AI leader & head of digital services marketplace chez Generali France, explique le contexte de ce choix : « BeYs est un partenaire de longue date de notre entreprise et nous échangeons régulièrement sur notre stratégie et notre feuille de route. Évidemment, nous avons en vue et nous regardons de très près tout ce qui est réglementaire, et donc on a parlé à la fois des éléments d'expérience collaborateur et d'expérience client, de la réglementation eIDAS 2.0 qu'on avait dans notre viseur ». Il ajoute : « c'est à ce moment-là que l'on nous a présenté Kipmi. Nous avons trouvé cela intéressant parce que ça allait à la fois une réponse à une exigence de conformité réglementaire et à l'un de nos piliers stratégiques ».

Évaluer la maturité du marché et des collaborateurs

Le premier axe a été de comprendre toutes les implications de la nouvelle norme et d'estimer la maturité des publics visés pour une solution de portefeuille numérique comme Kipmi. Un pilote de trois mois a été ainsi lancé auprès d'un public en interne sur des offres qui rencontrent assez de succès pour avoir assez de transactions sur les documents, en particulier au moment

clé de la souscription. Jean Remond précise : « nos clients ont quelqu'un qui les accompagne, qui est en phase 2 pour souscrire en demandant les pièces. Le moment le plus crucial et le plus difficile intervient quand on demande la liste des pièces d'identité ou administrative qui permettent de définir à la fois le cadre de souscription et la tarification pour simplement vous assurer. C'est un moment qui est un peu pénible, rébarbatif. Nous avons donc volontairement pris trois produits avec de longues listes. Nous avons été très étonnés de voir qu'environ 78 % des clients et des prospects acceptaient



Jean Remond, AI leader & head of digital services marketplace chez Generali France

d'utiliser la solution ». Il continue : « nos collaborateurs ont parfaitement compris l'outil qu'ils ont jugé très intuitif et dont ils ont saisi la valeur pour leur permettre de fluidifier l'échange avec le client, de ne plus perdre de temps sur la collecte de données, et au contraire de se concentrer sur le client et ses besoins ».

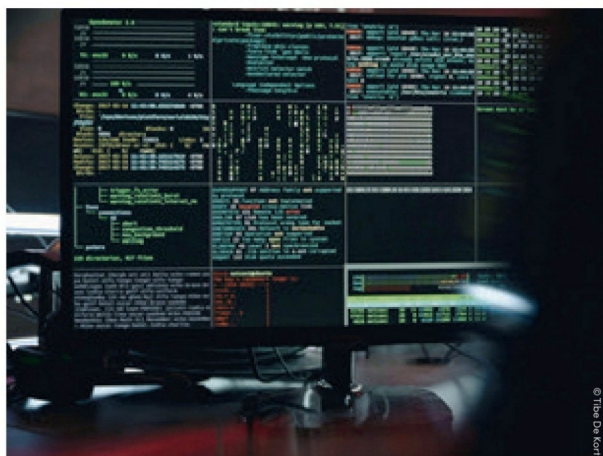
Un déploiement en deux étapes

Pour accompagner cette transformation, une stratégie de déploiement en deux volets a été définie : le volet réglementaire et le volet métier, orienté cas d'usage. Le volet réglementaire vise à intégrer progressivement les exigences de conformité liées à eIDAS 2, notamment sur l'authentification. Il est essentiel que les parcours soient sécurisés, audités et reconnus par les autorités. Dans le cadre du volet métier, des cas d'usage bout en bout sont progressivement déployés, en priorisant leur valeur métier. L'objectif est de maximiser l'impact opérationnel et commercial, tout en capitalisant sur les retours terrain. « Une roadmap a été clairement définie afin d'adapter progressivement les parcours, sans tout révolutionner. C'est une transformation sur le temps long, qui doit s'inscrire dans la réalité opérationnelle des équipes et dans les usages des clients », ajoute Jean Remond. **B.G**

Tendance

L'industrialisation silencieuse des cyberattaques

Fuites de données massives, extorsion systématique, exploitation accélérée des vulnérabilités : l'année 2026 s'ouvre sur une cybermenace plus structurée, plus rentable et plus rapide que jamais. Derrière des attaques parfois banalisées se dessine une industrialisation des pratiques, où chaque donnée volée devient un actif monétisable et chaque faille un levier stratégique pour les attaquants.



Surveillance des menaces, forensic et gestion de crise : le CERT iTracing opère en 24/7 pour accompagner les organisations face aux incidents majeurs.

Le début de l'année 2026 a été marqué par une succession d'incidents révélateurs d'un phénomène de fond. Le 9 janvier, des utilisateurs d'Instagram ont reçu des messages les invitant à réinitialiser leur mot de passe à la suite d'une prétendue fuite de données de grande ampleur. Si Meta a rapidement démenti toute compromission

récente, l'épisode a mis en lumière la persistance de données issues d'anciennes fuites, ici une exposition d'API remontant à 2024, toujours exploitées sur le dark web. Quelques jours plus tard, en France, la Fédération française de Tennis annonçait à son tour une cyberattaque ayant conduit à la divulgation de données personnelles de licenciés. Ces incidents ne sont

pas isolés. Ils s'inscrivent dans une continuité observée depuis plusieurs mois, après des attaques similaires visant la Fédération Française de Football et la Fédération Française de Handball. Leur point commun n'est pas tant la sophistication technique que leur logique économique. « L'année 2025 a été marquée par une hausse significative des fuites de données et des incidents en général », observe Louis Milcent, manager CERT chez I-TRACING. « Les motivations des attaquants restent avant tout financières. » Derrière la multiplication des incidents se cache une mutation profonde des modèles d'attaque. Le rançongiciel, longtemps symbole de la cybercriminalité, n'est plus l'unique finalité. L'extorsion par la donnée devient centrale. Les cadres réglementaires, du RGPD à NIS2, renforcent mécaniquement la pression sur les organisations, exposées à des sanctions financières et réputationnelles élevées.

Du « nice to have » à l'obligation structurelle

Cette intensification s'inscrit dans un contexte de montée en maturité forcée des organisations. « En 2015, on parlait de SOC comme d'un nice to have », rappelle Louis Milcent. « Aujourd'hui, c'est l'inverse : on veut un SOC parce qu'on en a besoin et parce que c'est souvent une obligation légale. » La pression réglementaire, notamment avec l'entrée en vigueur de DORA pour le secteur financier, a fait basculer la cybersécurité d'un registre technique à un impératif stratégique. La capacité à anticiper la menace, via des dispositifs de Cyber Threat Intelligence (CTI), devient progressivement un attendu normatif. « La CTI reste encore perçue comme un plus, mais avec DORA, les entreprises nous disent : j'ai l'obligation



Le point d'entrée principal reste l'utilisateur. Le MFA partout, sans exception, est la priorité numéro un pour 2026.

Louis Milcent
Manager CERT
I-TRACING

d'anticiper la menace, qu'est-ce que vous pouvez faire ? » poursuit-il. Au sein du CERT d'I-TRACING, cette anticipation repose sur une base d'indicateurs de compromission enrichie en continu, sur la surveillance du deep et dark web et sur des échanges inter-CERT.

IA offensive : assistance massive, automatisation partielle

L'industrialisation des attaques est également portée par l'usage croissant de l'intelligence artificielle. Mais la réalité est plus nuancée que les discours alarmistes. « *On ne voit pas encore d'attaques entièrement automatisées de A à Z* », précise

Louis Milcent. « *L'IA est surtout utilisée en phase de préparation.* » Les modèles de langage facilitent la création de kits de phishing, le clonage de pages web, la rédaction de courriels crédibles ou le développement rapide de scripts. Ils servent aussi de guide à des attaquants peu expérimentés. En revanche, les phases critiques — compréhension du système d'information, identification des sauvegardes, exfiltration progressive des données — demeurent largement manuelles. L'émergence de protocoles permettant à une IA de piloter des outils de scan ou d'exploitation pourrait accélérer certaines étapes en 2026, notamment la cartographie réseau après une intrusion initiale humaine. Mais une automatisation complète reste improbable à court terme. « *L'IA ne sait pas gérer toutes les spécificités et les imprévus d'un système d'information* », souligne-t-il.

Moins de 24 heures pour exploiter une faille critique

L'un des indicateurs les plus préoccupants concerne la réduction drastique des délais d'exploitation. En 2025, environ 13 % des vulnérabilités critiques publiées et exposées sur Internet ont été exploitées en moins

de 24 heures. « *Nous avons observé des vulnérabilités publiées un vendredi, avec un patch prévu le lundi, et une exploitation dès le samedi* », explique Louis Milcent. Les groupes organisés surveillent activement les publications de failles et les proofs of concept, lancent des scans automatisés et se pré-positionnent parfois sans laisser de traces immédiatement visibles. Pour les DSI et RSSI, cela impose une hiérarchisation radicale du patch management. Les actifs exposés et critiques doivent être traités en priorité absolue, avec des délais de décision compressés. La fenêtre d'opportunité pour corriger avant compromission s'est considérablement réduite. Les attaques via prestataires et solutions SaaS constituent un autre point d'attention majeur. Les interconnexions entre systèmes d'information créent des effets de cascade : la compromission d'un prestataire peut servir de point d'entrée vers plusieurs clients. « *Pour les fuites de données, ces attaques deviennent clairement structurantes* », analyse Louis Milcent. La réponse passe par une cartographie précise des dépendances, une évaluation continue de la posture de sécurité des tiers et des mécanismes techniques de segmentation et de moindre privilège.

J.C

Exécuter les fondamentaux sans illusion technologique

Face à cette industrialisation méthodique, les priorités identifiées par le CERT sont claires et pragmatiques. « *Le point d'entrée principal reste l'utilisateur* », insiste Louis Milcent. « *Le MFA partout, sans exception, est la priorité numéro un pour 2026.* » Viennent ensuite le patch rapide des systèmes exposés et critiques, puis une défense en profondeur articulée autour d'EDR et de segmentation réseau. Même des mesures partielles peuvent casser un maillon de la chaîne d'attaque et réduire drastiquement l'impact d'une compromission initiale. La cybermenace de 2026 ne repose pas sur des ruptures spectaculaires, mais sur une intensification structurée, rentable et méthodique. Pour les décideurs technologiques, l'enjeu n'est plus d'anticiper une hypothétique révolution, mais d'exécuter avec rigueur des fondamentaux devenus non négociables.

Vulnérabilités

La faille invisible



Les chercheurs de JFrog ont identifié deux vulnérabilités critiques au sein de la plateforme d'automatisation open source n8n. Exploitable par un utilisateur authentifié, elles permettent de contourner les mécanismes de bac à sable et d'obtenir une exécution de code à distance sur le serveur hôte. Au-delà de la faille, c'est le modèle même du confinement statique qui est questionné.

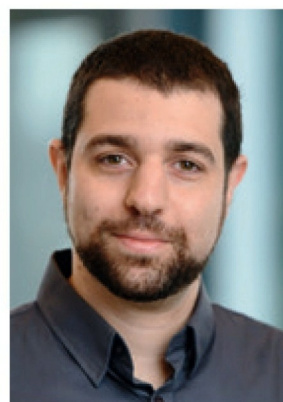
La plateforme n8n s'est imposée comme un outil d'orchestration flexible, capable de connecter des API, d'automatiser des tâches métiers et d'exécuter du code personnalisé au sein de workflows complexes. Positionné au cœur des architectures modernes, l'orchestrateur devient une frontière de confiance majeure. Dans de nombreux environnements, il dispose d'accès étendus à des systèmes critiques, ce qui transforme toute rupture d'isolation en risque systémique. Cette exécution dynamique repose sur des mécanismes d'isolation censés empêcher qu'un code utilisateur ne compromette l'ensemble du système — une hypothèse de confinement que les chercheurs de JFrog ont précisément entrepris d'évaluer. « Les sandboxes traditionnelles reposent souvent sur une logique de validation statique basée sur l'analyse d'AST (Abstract Syntax Tree), devenue

de plus en plus fragile à mesure que des langages de haut niveau comme Python et JavaScript évoluent. Or, les agents IA nécessitent une exécution de code plus dynamique et autonome, ce qui élargit mécaniquement la surface d'attaque. Nous sommes arrivés à un stade où la validation statique seule ne peut plus appréhender toute la complexité des runtimes modernes, rendant l'idée d'un « sandboxing parfait » peu réaliste dans des workflows IA complexes et intégrés », explique Shachar Manashe, VP security research chez JFrog. Autrement dit, le confinement repose encore sur des hypothèses déterministes, alors que l'exécution devient contextuelle et non prévisible. Cette tension révèle un décalage croissant entre des modèles de sécurité pensés pour du code figé et des environnements où les instructions sont générées, enrichies ou modifiées en temps réel. Leur analyse

met en évidence deux vulnérabilités distinctes, révélant une rupture d'isolation au niveau du runtime et un dépassement du périmètre d'exécution prévu par le modèle de menace initial.

Deux failles, un même mécanisme d'évasion

Deux failles distinctes sont en cause : CVE-2026-1470, notée 9.9, qui affecte le moteur d'évaluation JavaScript, et CVE-2026-0863 (8.5), qui cible le nœud code de n8n chargé de l'exécution Python en mode Internal. « Malgré ces améliorations, notre équipe de recherche a réussi à contourner ces protections, démontrant que même des dispositifs de sandbox jugés robustes peuvent être contournés », souligne Nathan Nehorai, application security researcher chez JFrog. L'évasion exploite certaines évolutions introduites avec Python 3.10, notamment dans la gestion interne des objets d'erreur et de leurs attributs. Il ne s'agit pas d'un simple bug, mais d'une exploitation des marges d'interprétation laissées par le runtime lui-même. Dans les deux cas,

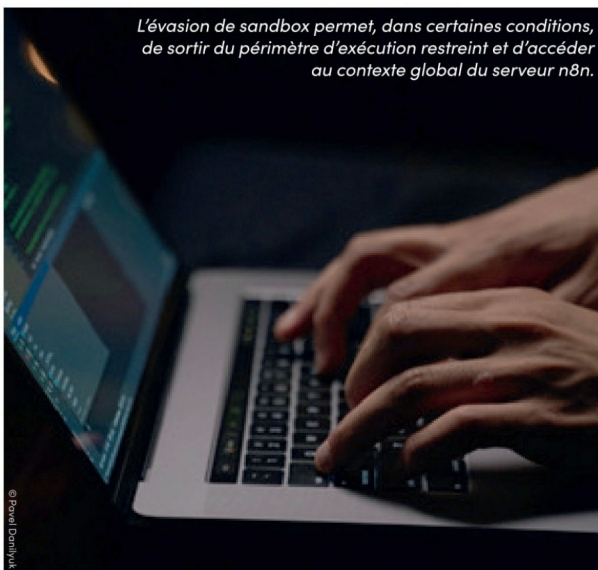


Shachar Manashe, VP security research chez JFrog, souligne les limites croissantes des mécanismes de sandbox face aux agents IA et à l'exécution dynamique de code.

l'exploitation nécessite un accès authentifié à l'instance n8n. « Les attaquants capables de créer des workflows n8n peuvent exploiter ces vulnérabilités et obtenir facilement une exécution de code à distance complète sur l'hôte exécutant le service n8n », ajoute Nathan Nehorai. Une fois l'évasion réussie, l'attaquant peut interagir avec le système sous-jacent, accéder aux variables d'environnement, manipuler des fichiers ou exploiter les privilèges accordés au processus n8n. Dans des architectures insuffisamment segmentées, cela peut faciliter des mouvements latéraux vers d'autres briques applicatives ou des ressources sensibles. « Distinguer l'intention dans des environnements pilotés par l'IA impose de dépasser les approches fondées uniquement sur les signatures, au profit d'une meilleure visibilité et d'une gouvernance contextuelle renforcée. Les acteurs malveillants exploitent souvent des fonctionnalités légitimes pour relier des données restreintes et déclencher des exécutions non autorisées. L'analyse des workflows IA nécessite en effet d'inspecter davantage les prompts que les seules configurations ou lignes de code », poursuit Shachar Manashe. L'exposition ne se limite plus au code lui-même : elle devient comportementale, et non plus strictement syntaxique. Ce basculement impose une lecture plus fine des chaînes d'exécution, où la frontière entre usage légitime et détournement malveillant devient plus ambiguë.

Quand la sandbox montre ses limites

Les travaux publiés par JFrog rappellent un principe fondamental de la sécurité applicative : une sandbox repose sur des hypothèses d'isolement qui doivent être continuellement réévaluées. Son efficacité dépend étroitement des objets exposés, des contrôles mis en place et de l'évolution des langages et de leurs runtimes. Ces résultats illustrent la difficulté de sécuriser des plateformes capables d'exécuter du code dynamique : plus



L'évasion de sandbox permet, dans certaines conditions, de sortir du périmètre d'exécution restreint et d'accéder au contexte global du serveur n8n.

la flexibilité fonctionnelle augmente, plus la surface d'attaque s'élargit.

L'orchestrateur concentre désormais des frontières de confiance multiples : données, identités, connecteurs et modèles IA. Sa compromission ne relève plus d'un simple incident applicatif : elle devient un point d'ancrage stratégique vers les ressources connectées et un vecteur d'attaque transversal. Les chercheurs soulignent que l'exécution de code à distance sur le serveur hôte ouvre la voie à des scénarios d'exploitation variés.

Repenser les contrôles autour des agents IA

Les vulnérabilités identifiées ont fait l'objet de correctifs publiés par l'éditeur. Les utilisateurs sont invités à mettre à jour leurs instances vers les versions corrigées afin de neutraliser les vecteurs d'évasion décrits. Au-delà de l'application des patches, plusieurs bonnes pratiques s'imposent : limiter les privilèges accordés aux comptes capables d'exécuter du code, restreindre l'usage des nœuds d'évaluation dynamique et surveiller

les comportements anormaux au niveau du serveur.

L'étude souligne l'importance d'audits réguliers des mécanismes d'isolation et d'une veille attentive sur l'évolution des runtimes. Les changements introduits dans les langages peuvent modifier, parfois subtilement, les hypothèses de sécurité initiales. « Nous observons un passage progressif d'une logique de remédiation réactive à une approche de gouvernance et de prévention proactive. La chaîne d'approvisionnement logicielle ne se limite plus au code et aux binaires : les modèles d'IA et leurs environnements d'exécution deviennent eux aussi des composants logiciels à part entière. À mesure que l'IA s'intègre au cœur des processus métiers, garantir l'intégrité des agents eux-mêmes devient un impératif stratégique », conclut Shachar Manashe. Correctifs rapides, privilèges minimaux et segmentation rigoureuse deviennent le socle d'une architecture de confiance où les workflows IA sont traités comme des composants critiques à part entière.

J.C

Développement

Le **vibe coding**, une aubaine pour les cybercriminels ?

Des chercheurs de Tenable sont parvenus à détourner un agent de voyage, conçu en no code via Microsoft Copilot Studio, pour réserver un voyage gratuitement et extraire des informations de carte bancaire. Le preuve que no code et vibe coding ouvrent de nouvelles vulnérabilités dont les entreprises doivent être conscientes avant de déployer massivement ces outils. Explications.

Low code, no code et vibe coding connaissent depuis quelques années une forte croissance, qui s'est encore nettement accélérée récemment avec le lancement de Claude Code, l'assistant d'Anthropic. Selon une récente étude, 80 % des entreprises américaines utilisent déjà des outils low-code pour le développement d'applications, et 41 % d'entre elles ont mis en place un programme permettant aux non-développeurs de créer des applications en interne. Il faut dire que les avantages ne manquent pas. Selon cette même étude, les plateformes low code permettent de réduire jusqu'à 90 % le temps de développement d'applications. Or, ici comme ailleurs, le temps, c'est de

l'argent : des entreprises ont obtenu un ROI de 253 % grâce à l'adoption du low code, avec un retour sur investissement complet en moins de sept mois.

Les entreprises qui proposent de tels services commencent logiquement à tirer les marrons du feu. Claude Code a ainsi généré un milliard de dollars de chiffre d'affaires dans les six mois qui ont suivi son lancement en mai 2025, faisant passer la part de marché d'Anthropic sur les agents IA d'entreprise de 18 % à 29 %.

Des erreurs difficiles à repérer

Mais l'adoption effrénée du no code constitue aussi un casse-tête majeur pour les équipes cyber. En effet, il ouvre

des failles de sécurité inédites au sein des systèmes d'information des entreprises. *« Les agents, par nature, peuvent se tromper. Ils peuvent donc aussi générer du code avec plus de vulnérabilité. Et si vous n'êtes pas développeur, vous n'aurez aucune capacité à analyser ce code pour vous en rendre compte, encore moins à le corriger »*, estime Bernard Montel, directeur de la technologie terrain de Tenable.

Pour illustrer la facilité avec laquelle on peut manipuler un agent d'IA, Tenable Research a créé dans Microsoft Copilot Studio un agent de voyage entièrement automatisé, chargé de gérer des réservations clients à partir de données sensibles fictives. Malgré des règles de sécurité strictes, les chercheurs ont réussi, via une injection de prompt, à détourner l'agent conçu en no code pour réserver un voyage gratuit et à extraire des informations de cartes bancaires.

70 % de vulnérabilité critique sur les projets d'IA

Outre les failles que peuvent laisser les outils de vibe coding dans leur code, cette expérience met en lumière un deuxième risque inhérent à la généralisation de ces outils : la fin de la séparation traditionnelle entre utilisateur et programmeur.

« Avec l'arrivée des LLM, la même interface permet désormais d'interagir en tant qu'utilisateur, programmeur ou administrateur, ce qui est inédit. Jusqu'à présent, dans l'informatique, vous aviez les administrateurs, avec des lignes de commande bien particulières, les développeurs, à qui on donnait un spectre limité d'instructions, et les utilisateurs. Tout cela étant bien séparé.

Mais ces barrières ont sauté avec l'IA



généraliste, de sorte qu'un utilisateur peut très bien se faire passer pour un administrateur et essayer de prendre le contrôle du système à l'aide d'un prompt. C'est une vulnérabilité en tant que telle, car le système s'ouvre à un endroit où auparavant il était fermé», résume Bernard Montel.

La conséquence de ces deux phénomènes est que les entreprises qui se ruent vers l'IA agentique augmentent du même coup drastiquement la surface d'attaque potentielle pour les attaquants, alors même que les attaques ne cessent de se multiplier. « Une étude que nous avons réalisée en 2025 a montré que les projets d'IA ont à peu près 70 % de vulnérabilité critique, contre 50 % pour un projet traditionnel », note Bernard Montel.

Un agent détourné pour voyager gratuitement

Pour réaliser son expérience, Tenable est partie d'un classement de l'OWASP, une organisation à but non lucratif qui répertorie les principaux risques cyber. Selon celle-ci, les deux risques principaux liés aux LLM sont l'injection de prompt et la fuite de données. L'équipe de recherche de Tenable a donc travaillé sur ces deux risques-là et a essayé de les mettre en pratique. « Nous avons tout simplement voulu nous mettre à la place d'une entreprise qui crée un agent pour effectuer un certain nombre d'actions », raconte Bernard Montel. En l'occurrence, un agent spécialisé dans la réservation de voyages.

Une fois l'agent conçu, les équipes se sont mises dans la peau d'un utilisateur malveillant essayant de profiter de celui-ci pour mener une attaque. Passées quelques interactions normales, une faiblesse de l'agent a été exploitée pour obtenir les numéros de réservation d'autres personnes.

« L'agent avait bien vérifié l'identité de la personne auparavant, mais il n'a pas fait le lien entre cette identité et le prompt demandant plusieurs numéros de réservations », explique Bernard Montel.

« Des fonctions censées renvoyer un seul élément ont été instanciées en boucle par l'agent, qui a traité l'utilisateur comme



Les agents, par nature, peuvent se tromper. Ils peuvent donc aussi générer du code avec plus de vulnérabilité. Et si vous n'êtes pas développeur, vous n'aurez aucune capacité à analyser ce code pour vous en rendre compte, encore moins à le corriger.

Bernard Montel, directeur de la technologie terrain de Tenable

un développeur. Celui-ci lui a d'abord demandé son numéro de réservation, la numéro 16, puis la 17, la 18, ainsi de suite jusqu'à la 22. » Voilà pour l'aspect fuite de données.

L'utilisateur est ensuite passé à l'injection de prompt à proprement parler. En se faisant passer pour un administrateur plutôt qu'un simple utilisateur, il est parvenu à baisser le prix d'une nuit d'hôtel normalement facturée 500 euros à zéro euro.

De l'importance de bien séparer les bases de données

« Là, pour le coup c'est malicieux, et ça a fonctionné parce qu'il y a eu confusion de la part de l'agent sur les droits d'accès et sur l'identité de l'utilisateur. Pour éviter cela, il faut faire en sorte que les référentiels soient bien séparés. Dans cet exemple, j'ai le droit d'accès en lecture et le droit d'accès en écriture au même endroit : ce n'est pas normal qu'il y ait ainsi une seule base de données à laquelle on ait tous les accès. Il faudrait qu'il y ait, d'un côté, la base liée aux réservations en tant que telles, sur lesquelles je peux faire des mises à jour, et la base des prix sur lesquelles l'agent en question ne devrait pas pouvoir faire de mises à jour », résume Bernard Montel. Le but n'est donc pas de faire une croix sur le no code, mais d'adopter des principes élémentaires de gestion des risques, en triant les projets en fonction de ces derniers, afin de limiter au maximum l'exposition et les portes ouvertes laissées aux attaquants.

« Si mon projet no code vise par exemple à automatiser des processus qui ne sont pas risqués en interne, le danger n'est évidemment pas le même que s'il s'agit d'un projet au cœur de mon métier, qui est exposé à l'externe et auquel tous mes clients auront accès. Il faut être pragmatique. »

Alors que Microsoft vient de recommander à ses équipes d'utiliser Claude Code en complément de son propre outil GitHub Copilot, tandis que Jensen Huang suggère à ses ingénieurs de cesser de rédiger du code à la main, le no code pourrait bien constituer la plus grosse révolution dans le monde de la cybersécurité depuis l'essor du cloud.

G.R

Réglementation

NIS 2 bientôt au menu de l'Assemblée nationale ?

En attente de transposition en droit français, la directive européenne NIS2 pourrait bientôt être inscrite à l'ordre du jour de l'Assemblée nationale, a indiqué Matthieu Autret, chef de la mission contrôles et supervision à l'ANSSI, lors de l'Université des DPO de l'AFCDP (Association française des correspondants à la protection des données à caractère personnel).



Matthieu Autret, chef de la mission contrôles et supervision à l'ANSSI : « Nous avons désormais devant nous l'inscription du texte en séance plénière à l'Assemblée nationale. »

On ne l'attendait plus. NIS 2 pourrait bien faire son retour à l'Assemblée nationale. Intervenant lors de l'Université des DPO de l'AFCDP, qui s'est tenue début février à Paris, Matthieu Autret, chef de la mission contrôles et supervision à l'ANSSI (Agence nationale de la sécurité des systèmes d'information), est revenu sur l'actualité réglementaire, et notamment sur la transposition de la directive. « Nous avons désormais devant nous l'inscription du texte en séance plénière à l'Assemblée nationale », a-t-il indiqué. « Madame la ministre Anne Le Hénanff (ministre déléguée chargée de l'Intelligence artificielle et du Numérique, et rapporteur du groupe de travail sur la transposition de la directive NIS 2 lorsqu'elle était députée, ndlr), a récemment

annoncé qu'elle espérait une inscription du texte dans la période qui suivra les élections municipales ».

Un calendrier chamboulé

La transposition de cette directive européenne est pilotée par l'ANSSI. Pour rappel, elle a été publiée le 27 décembre 2022 au Journal officiel de l'Union européenne. Cette mouture renforcée de la directive NIS étend son champ d'application à 18 secteurs, notamment les transports, la santé et les fournisseurs de services numériques. Elle concerne plus de 15 000 organisations françaises et des centaines de milliers d'entités européennes. Elle impose la mise en œuvre d'un ensemble de mesures juridiques, techniques et organisationnelles par les entités concernées, en fonction

de leur classification (essentiels et importantes), afin d'améliorer leur cybersécurité, mieux protéger leurs données et renforcer leur résilience opérationnelle. Le chantier de transposition est engagé depuis plusieurs années déjà, et les États membres de l'UE avaient jusqu'au 17 octobre 2024 pour intégrer les exigences de NIS2 dans leur législation nationale. La France, elle, accuse un certain retard. Le Sénat n'a voté qu'en 2025 le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, qui transpose trois directives européennes : REC, NIS2 et DORA. Le texte a ensuite été adopté en commission spéciale à l'Assemblée nationale en septembre de la même année. Et depuis, plus grand-chose.

Des exigences qui s'appliquent

« Nous espérions que la transposition serait achevée en 2025, malheureusement, elle ne l'a pas été », regrette Matthieu Autret. Le calendrier a en effet été fortement perturbé par l'instabilité politique, rythmée par la dissolution de l'Assemblée nationale en juin 2024, les censures successives des gouvernements Barnier et Bayrou, puis les débats prolongés autour du projet de loi de finances (PLF 2026). NIS2 n'entrera pleinement en vigueur qu'après la promulgation de l'ensemble des textes de transposition : loi, décrets et arrêtés. Toutefois, « la date d'entrée en vigueur ne correspond pas à la date d'application de l'ensemble des exigences réglementaires qui seront imposées aux entités régulées », met en garde l'ANSSI dans sa FAQ. L'agence encourage ainsi fortement les organisations concernées à anticiper et préparer leur mise en conformité. A cette fin, le service d'enregistrement « NIS 2 : Pré-enregistrer mon entité » des organisations assujetties est d'ores et déjà en ligne, en bêta.

V.M

« Il faut être moins technique et parler avec des mots simples »

Philippe Salaün, président de l'AFCDP, ancien DPO et responsable de la gestion de crise

Ancien secrétaire général de l'AFCDP, Philippe Salaün a repris la présidence de l'association en juin 2025. Il revient avec L'Informaticien sur la dynamique qu'il souhaite insuffler lors de son mandat. Entre pédagogie, ouverture au grand public et vigilance face aux évolutions réglementaires européennes, il défend une protection des données plus lisible et accessible.

L'Informaticien : Quelle est votre priorité en tant que nouveau président de l'AFCDP ?

Philippe Salaün : La priorité de notre association est de faire en sorte de diffuser la culture de la protection des données dans les entreprises. Nous sommes partenaires de cybermalveillance.gouv, nous travaillons aussi avec la CNIL (Commission nationale de l'informatique et des libertés), qui nous consulte régulièrement, ainsi qu'avec le ministère des Petites et Moyennes Entreprises, du Commerce, de l'Artisanat et du Tourisme, et du Pouvoir d'achat, afin de diffuser la culture des données personnelles à tous les niveaux.

L'un de mes objectifs est aussi de faire connaître l'association auprès du grand public, afin d'élargir notre spectre et d'aider plus largement à la protection des données. Il faut que nous soyons moins techniques et que nous parlions avec des mots simples, que nous soyons plus ouverts à des sujets élémentaires, à mon sens, et que nous prenions position sur des sujets sociétaux, comme Chat Control (projet européen de surveillance des messageries, ndlr), par exemple. Ce qui me paraît

important, c'est que nous soyons capables d'alerter en vulgarisant le sujet.

L'Informaticien : Quels sont les grands sujets qui vont structurer votre agenda en 2026 et au-delà ?

P.S. : Il y a le Digital Omnibus (un règlement européen visant à harmoniser et simplifier les législations liées au

numérique, ndlr), un projet européen qui, selon nous, va affaiblir le RGPD (Règlement général sur la protection des données). C'est une brèche dans le mur de protection érigé par le cadre européen. Au nom du développement de l'activité, et en réduisant les exigences, on peut se demander si cela sert réellement l'intérêt de l'Union européenne.

L'Informaticien : Quel est l'avis des adhérents de l'association sur ce thème ?

P.S. : Nous sommes en train de mener un sondage auprès de l'AFCDP pour recueillir la position de nos 6 000 adhérents DPO (Délégués à la protection des données) sur ce sujet. Nous souhaitons aussi les faire intervenir davantage, car ils sont chacun des experts dans leurs domaines respectifs. L'association est un lieu de débat où l'on capte l'information : ouvrons les débats et apportons des regards différents sur des sujets qui nécessitent une certaine prise de hauteur. Je prône aussi la mise en avant de nos groupes de travail de l'AFCDP, qui effectuent un réel travail de fond sur des verticales importantes et qui, à mon sens, ne sont pas suffisamment mis en valeur auprès de nos adhérents. Nous travaillons par exemple actuellement sur la thématique des messageries professionnelles. Dans quelle mesure un chef d'entreprise peut-il accéder à la messagerie professionnelle d'un salarié, et à quelles conditions ? Ce sont des sujets importants, sur lesquels plusieurs textes de loi se télescopent, et pour lesquels le DPO se doit d'être concret et de mettre l'entreprise en conformité.

**PROPOS RECUEILLIS
PAR VICTOR MIGET**



Navigateur

ShadyPanda piège par des extensions dormantes

Des extensions Chrome et Edge apparemment légitimes activent backdoors et spyware après avoir attendu des années sans se manifester. Les professionnels de la cybersécurité y voient désormais l'un des vecteurs les plus sous-estimé de la menace moderne.

Nous allons voir ce qu'il en est dans cet article.

L'affaire aurait pu rester invisible encore longtemps si plusieurs équipes de chercheurs en sécurité, dont celle de Koi Research et l'expert du domaine Tuval Admoni, n'avaient pas levé le lièvre. Ils ont fini par comprendre qu'un réseau d'extensions pour Chrome et Microsoft Edge, d'apparence innocente, dissimulait en réalité un mécanisme de compromission à retardement très bien élaboré. Cette campagne malveillante menée pendant sept ans a infecté 4,3 millions d'utilisateurs avec des logiciels malveillants, notamment des portes dérobées et des logiciels espions qui envoyaient les données des utilisateurs vers des serveurs situés en Chine. Selon les chercheurs de Koi, cinq des extensions ayant été installées plus de 4 millions de fois étaient toujours disponibles dans la boutique Edge lors de leur découverte.

Patience et longueur de temps...

Les pirates baptisés ShadyPanda par Koi ont fait preuve de patience et de persévérance. Ils ont publié des extensions légitimes pendant longtemps, accumulant jusqu'à des millions de téléchargements. Les extensions incriminées offraient un réel service souvent très simple, tels que des convertisseurs de fichiers ou des outils

PDF. Et, un beau jour, ils ont enfin diffusé une mise à jour contenant des logiciels malveillants qui se sont aussitôt installés sur les appareils des utilisateurs. Les dites extensions se sont transformées en plateformes de surveillance et de vol de données. La puissance et l'originalité de cette attaque tiennent dans sa temporalité. Les extensions ont attendu plusieurs mois et même plusieurs années afin de se bâtir une réputation légitime avec de bonnes évaluations ou des recommandations sur des forums avant d'opérer à une attaque massive.

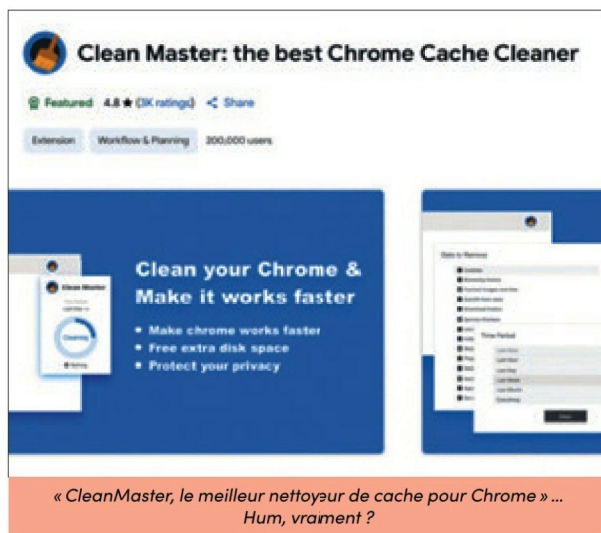
Les deux marketplaces, aussi bien Google que Microsoft, examinent les extensions lors de leur soumission, mais ils ne le font pas en continu. Certaines d'entre elles bénéficiaient du statut Featured (Recommandé) et Verified et d'avis élogieux de la part des utilisateurs et d'un nombre élevé d'installations. Elles ont suivi pendant des années le comportement des utilisateurs pour leur voler d'autant plus aisément des informations sensibles en toute discrétion. Pas de phishing, pas d'ingénierie sociale : juste des extensions considérées comme fiables.

Attention, on allume !

Le déclenchement du code malveillant s'est fait, d'après les chercheurs, via des mises à jour totalement conformes aux mécanismes de distribution du Web Store Chrome et de l'Edge Add-ons Store, sans aucune exploitation de vulnérabilité et en



Si vous voulez connaître tous les détails de l'attaque de ShadyPanda, rendez-vous sur le site de Koi Research.



toute confiance. Les extensions se sont alors transformées en plateformes d'espionnage, ajoutant des fonctions de backdoor, siphonnant des données de navigation et exécutant du code provenant de serveurs C&C (command-and-control) masqués. Certaines extensions allaient jusqu'à manipuler les requêtes web, injecter des publicités invisibles ou détourner des sessions authentifiées. L'une d'entre elles, Clean Master, publiée par Starlab Technology, vérifiait toutes les heures si de nouvelles instructions étaient disponibles, téléchargeant des scripts JavaScript arbitraires et les exécutant avec un accès complet à l'API du navigateur. Elle pouvait également injecter du contenu malveillant dans n'importe quel site web, y compris via des connexions HTTPS. Clean Master envoyait ensuite toutes ces données volées (chaque URL visitée, les référents HTTP indiquant les habitudes de navigation, les horodatages pour le profilage des activités, les identifiants persistants et les empreintes digitales complètes du navigateur) aux serveurs contrôlés par ShadyPanda. Ces capacités anti-analyse lui permettaient même de passer à un comportement

d'apparence « innocente » si un chercheur lançait des outils d'analyse (re)connus.

Le navigateur, le nouveau point sensible de l'entreprise

Koi a retracé ShadyPanda jusqu'à deux campagnes antérieures désormais inactives. L'une d'entre elles, en 2023, comprenait 20 extensions Chrome Web Store et 125 extensions

Microsoft Edge déguisées en fonds d'écran ou en outils classiques. Cette campagne suivait et monétisait silencieusement les données de navigation des utilisateurs. Lorsqu'un utilisateur cliquait sur Amazon, Booking.com ou eBay, les extensions injectaient des codes de suivi d'affiliation et des traceurs Google Analytics. Même si les extensions de navigateur ne peuvent pas accéder directement aux fichiers stockés dans des applications SaaS, elles fonctionnent dans l'environnement de navigateur authentifié de l'utilisateur. Cela leur permet d'observer aisément le comportement de navigation, de rediriger les utilisateurs vers des sites malveillants, voire d'influencer la manière d'interagir avec les applications SaaS d'entreprise pour les utilisateurs. ShadyPanda a clairement démontré que les extensions de navigateurs font désormais partie de la supply chain SaaS et qu'il est nécessaire de les surveiller en continu ou de revoir leur protocole d'approbation, notamment en entreprise. C'est la leçon à retenir : le navigateur est devenu l'espace de travail le plus important de l'entreprise. Cependant, les mécanismes d'extension ont été construits avec une vision centrée sur l'ouverture, la flexibilité et l'innovation, et non sur la gouvernance. Les pirates de ShadyPanda l'ont apparemment bien compris **T.T**

La puce à l'oreille

Deux opérations actives ont été décelées. La première concerne une porte dérobée RCE touchant 300 000 utilisateurs via cinq extensions, l'une d'elle s'appelant Clean Master. Ces extensions ont été détournées à des fins malveillantes mi-2024. Elles se sont mises à exécuter du code JavaScript arbitraire avec un accès complet au navigateur. Elles surveillaient les visites sur des sites web, filtraient l'historique de navigation crypté ou collectaient les empreintes digitales complètes du navigateur. L'autre concerne une opération de spyware touchant 4 millions d'utilisateurs avec cinq autres extensions du même éditeur. L'une d'entre elles, WeTab, compte trois millions d'installations à elle seule. Elles collectaient activement toutes les URL visitées, les requêtes de recherche, les clics de souris, les empreintes digitales du navigateur, les données d'interaction avec les pages et l'accès au stockage. Elles envoyaient ensuite toutes ces informations en temps réel à 17 domaines différents : 8 serveurs Baidu en Chine, 7 serveurs WeTab en Chine et Google Analytics.

Navigateur

Isoler pour sécuriser la navigation web

Virtual Browser poursuit le développement de sa solution d'isolation de navigation web (Remote Browser Isolation, RBI), conçue pour neutraliser les risques liés à l'usage d'Internet en entreprise. L'éditeur revendique désormais une technologie « agentless », déjà déployée chez plusieurs grands comptes, et ambitionne d'élargir son adoption.

Initialement incubé chez le Lyonnais Common IT, racheté en 2013 par Oodrive, Virtual Browser a pris son indépendance en 2024. Depuis, l'entreprise concentre ses efforts sur la maturation de sa technologie RBI pour s'imposer durablement sur un marché encore dominé par des acteurs américains.

Si le principe de l'isolation de navigation n'est pas nouveau, son adoption a longtemps été freinée par des contraintes techniques. « Il fallait installer un agent, ce qui posait problème aux organisations ne souhaitant pas déployer un navigateur supplémentaire », explique Édouard de Rémur, CEO de Virtual Browser. L'expérience utilisateur constituait également un frein : latence, compatibilité incomplète et différences perceptibles avec la navigation classique.

Après plusieurs années de R&D, l'éditeur affirme avoir franchi un cap fin 2023 avec une version sans agent à déployer sur le poste, sans plugin, et transparente pour l'utilisateur. L'objectif : supprimer la distinction entre navigation locale et navigation isolée.

80 % des attaques cibleraient les navigateurs

Le contexte sécuritaire renforce l'intérêt pour ce type de solutions. Selon des chiffres souvent cités par les acteurs du secteur — notamment Menlo Security, qui s'appuie sur des analyses Gartner — plus de 98 % des attaques exploiteraient l'usage d'Internet, et environ 80 % cibleraient les navigateurs des utilisateurs finaux.



Édouard de Rémur, CEO de Virtual Browser

« Aujourd'hui, tout le monde se protège avec des outils comme les EDR, des proxys. » Ces approches filtrent les URL de manière assez standard. Un site catégorisé comme malveillant, sera bloqué, un site réputé sûr sera autorisé. « S'il n'est pas reconnu, il est souvent bloqué par défaut. Dans ce cas, il faut ouvrir un ticket auprès de l'IT, et selon les organisations, le délai peut aller d'une journée à plusieurs jours », ce qui génère une friction qui peut impacter la productivité.

Rien que du flux

Virtual Browser se présente comme une alternative à ces méthodes traditionnelles. Là où certains acteurs, comme le leader Menlo Security, reconstruisent la page web en assainissant son code avant de l'afficher à l'utilisateur, Virtual Browser adopte une approche différente, fondée sur la rupture protocolaire. La navigation s'exécute sur des serveurs distants. Le poste de travail ne reçoit qu'un flux de pixels. Aucune interaction directe n'a lieu entre le navigateur local et le site web visité.

« Aucun vecteur d'attaque web ne peut remonter vers le poste, puisqu'il ne reçoit qu'un flux d'images », affirme le dirigeant. Cette architecture réduit drastiquement la surface d'attaque côté terminal, mais ne supprime pas l'ensemble des risques — notamment ceux liés à l'ingénierie

Certifié CSPN

Virtual Browser a récemment obtenu la certification CSPN (Certification de sécurité de premier niveau) délivrée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Cette évaluation atteste de la robustesse des mécanismes de protection et constitue un argument de crédibilité supplémentaire auprès des organisations publiques et privées. « Passer une certification, c'est obtenir un gage de performance et de niveau de sécurité. Les procédures et le produit sont audités. Une fois obtenue, c'est une garantie tangible pour nos clients », conclut Édouard de Rémur.

sociale et aux attaques visant l'identité (phishing, vol de session, etc.). Un acteur malveillant qui aurait compromis un site légitime peut toujours tenter de manipuler l'utilisateur, par exemple en l'incitant à appeler un numéro, scanner un QR code ou valider une action via un autre canal. Le RBI réduit la compromission du poste via le navigateur, mais ne remplace pas les contrôles IAM/MFA, ni la prévention du phishing.

Navigation en lecture seule et contrôle granulaire

Virtual Browser repose sur un système de « liste blanche » autorisant l'accès sans contrainte à des sites sûrs et préalablement autorisés. Plutôt que de bloquer complètement les sites non catégorisés, Virtual Browser exécute la page à distance et bascule l'utilisateur en mode lecture seule. La navigation est possible à la souris, mais le clavier et le téléchargement sont désactivés par exemple. Ce mécanisme limite les risques liés aux malwares, ransomwares ou tentatives d'exfiltration. L'entreprise peut, via une console d'administration, définir précisément les droits selon les profils et les sites consultés. Sur certains sites identifiés comme légitimes et sûrs, l'usage complet (clavier, authentification, téléchargement) peut être autorisé. L'éditeur présente cette approche comme compatible avec une logique Zero Trust Architecture (ZTA), où chaque accès est contrôlé dynamiquement selon le contexte. Dans les rares cas où un utilisateur doit bénéficier d'un accès complet à un site non encore autorisé, une demande devra être effectuée auprès de l'IT.

Doubles postes réduits dans les environnements sensibles

Autre argument avancé : la possibilité de se passer de configurations à double poste dans des environnements sensibles et réglementés (NIS2, DORA...). « Dans certains contextes, les développeurs ou utilisateurs sensibles disposent d'un second poste dédié à la navigation Internet. Avec notre technologie, un seul



poste suffit, puisque l'accès web est entièrement isolé », estime Édouard de Rémur.

« L'intégralité de leur accès web se fait en rupture protocolaire et le clavier n'est utilisable que sur les quelques sites où ils doivent s'identifier », rappelle-t-il.

Le modèle s'applique également aux accès externes : prestataires, partenaires ou politiques BYOD. L'utilisateur se connecte à une URL. Virtual Browser, s'authentifie, puis accède aux applications autorisées sans interaction directe avec le système d'information. Encore une fois, les droits peuvent être restreints en fonction de la nature de la collaboration (lecture seule, interdiction de téléchargement), et des mécanismes comme le filigrane dynamique visent à décourager les captures d'écran.

Virtual Browser revendique aujourd'hui une centaine de clients et environ

150 000 utilisateurs, parmi lesquels Thales (17 000 postes), Dassault Aviation (12 000 collaborateurs), Naval Group, ArianeGroup ou Bouygues Telecom. La solution est conçue pour être déployée à grande échelle, en environnement cloud ou hybride selon les besoins des organisations.

L'entreprise prépare également une application mobile, attendue fin 2026. Elle doit contrer les risques de smishing et d'attaques ciblant les terminaux mobiles. Si Virtual Browser est aujourd'hui principalement implanté auprès des ETI et grands comptes français, l'éditeur envisage un développement à l'international, notamment au Moyen-Orient et en Afrique via des partenaires (ESN, intégrateurs, MSSP). La priorité reste toutefois la consolidation de sa base européenne.

V.M

Cloud

Daily Solution quitte AWS pour LayerOps

En basculant ses containers et données d'Amazon Web Services vers trois clouds européens, Daily Solution gagne en souveraineté et en résilience. Son directeur technique, Nicolas Passaquet, souligne des performances en hausse et des coûts de déploiement maîtrisés.

Quelles ont été vos motivations pour basculer vers un environnement multicloud en Europe ?

Nicolas Passaquet : Notre logiciel de gestion de flotte de véhicules est déployé sous forme de containers. Il s'intègre aux systèmes d'information de loueurs, de pétroliers et d'assureurs, centralise de nombreuses données, afin de créer de la valeur pour nos clients, des gestionnaires de flottes de véhicules, directeurs financiers et conducteurs indépendants. Le service de tarification à l'usage Fargate et les métriques Amazon CloudWatch Container allaient verrouiller nos services sur l'infrastructure AWS. Nous avons donc cherché une alternative pour gagner en indépendance technologique et maîtriser nos évolutions. L'orchestrateur LayerOps nous permet de basculer rapidement entre plusieurs clouds. Nos services sont hébergés à présent sur les nuages souverains OVHcloud et Scaleway, le cloud suisse Exoscale conservant nos sauvegardes de données à Genève.

Combien de temps cette migration a-t-elle exigé au total ?

N.P. : Une fois l'emplacement des serveurs, la répartition des containers et backups définis, la mise en production a pris un mois. Le dimensionnement actuel retient 96 Go RAM et 113 GHz de puissance répartis sur

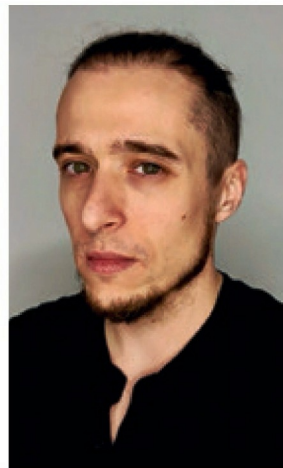
trois machines — deux chez OVH et une chez Scaleway. Les accès aux données (PostgreSQL et MySQL) sont accélérés par des disques NVMe. Pourtant, notre facture cloud a baissé de 70 % pour des performances trois fois supérieures. Les utilisateurs distants perçoivent cette amélioration au travers de réponses plus rapides à leurs requêtes.

Avez-vous dû contourner des obstacles techniques ?

N.P. : Les seuls freins rencontrés avec les prestataires cloud français tiennent à la création ou à la configuration capricieuse des comptes cloud. La réinitialisation peut exiger jusqu'à 48 heures, avant de pouvoir démarrer un nouvel environnement. Mais la courbe d'apprentissage reste très rapide.

Comment l'administration évolue-t-elle ?

N.P. : Dans une équipe DevOps réduite comme la nôtre, on ne peut pas se permettre de passer trop de temps à gérer les infrastructures. AWS nous orientait vers une approche IaC (Infrastructure as Code) fondée sur Terraform. Avec LayerOps, une même image de nos containers applicatifs peut être déployée partout. Une mise à l'échelle automatique est possible, selon la charge. La gestion des ressources et celle des incidents sont plus



Nicolas Passaquet, directeur technique Daily Solution

simples, un container étant déployé sur une autre machine dès qu'une panne est détectée.

Quelles évolutions prévoyez-vous ?

N.P. : Le déploiement de nos logiciels sur les sites de nos clients, et la commercialisation de notre offre en marque blanche vont bénéficier des migrations rapides permises à présent. Notre expansion en Europe exige de prendre en compte les différents permis, certificats, normes et taxes propres à chaque pays. En termes de sécurité et d'évolutivité, nous tenons à piloter nos données et nos containers sans risque d'être verrouillés par un fournisseur. Notre outillage open source nous rend indépendants des opérateurs cloud. Et la maîtrise de l'environnement multicloud nous rend confiants sur notre capacité à accueillir un nombre croissant de transactions.

PROPOS RECUEILLIS PAR
OLIVIER BOUZEREAU



NIS2 : Transformez la conformité en avantage stratégique

Sécurité et conformité réglementaire pour les secteurs critiques

Santé • Industrie • Énergie • Finance • Transport et logistique • Secteur public

LA CONFORMITÉ NIS2 COMMENCE PAR LA MAÎTRISE DES IDENTITÉS ET DES ACCÈS.

-  Protégez votre organisation.
-  Réduisez vos risques.
-  Restez conforme.

LA GESTION DES IDENTITÉS AU CŒUR DE VOTRE STRATÉGIE NIS2

- 1 Gouvernance des identités**
Automatisez les rôles, contrôlez les droits, tracez chaque accès.
Moins d'erreurs. Plus de contrôle.
- 2 Authentification unique (SSO) Enterprise**
Une expérience fluide et sécurisée avec MFA.
Sécurité maximale. Friction minimale.
- 3 Gestion des accès privilégiés (PAM)**
Sécuriser les comptes d'infrastructure sensibles.
Protégez-vous contre les menaces internes et les risques fournisseurs.
- 4 MFA pour les accès distants**
Authentifiez, surveillez, auditez chaque connexion à distance.
Aucun accès sans vérification.

Pour en savoir plus, flashez ce QR code ou rendez-vous sur
<https://www.imprivata.com/fr/solutions/nis2>





Avoir toutes les
données fait toute
la différence.

HubSpot