N° 206 — Mai 2022

www.linformaticien.com

L'INFORMATICIEN

DevOps
Neuvector

Les postes de travail s'adaptent à de nouveaux besoins



Blockchain

Une lame de fond discrète

Retex
- Samusocial
- Papernest

Tactic
La dictature du bonheur

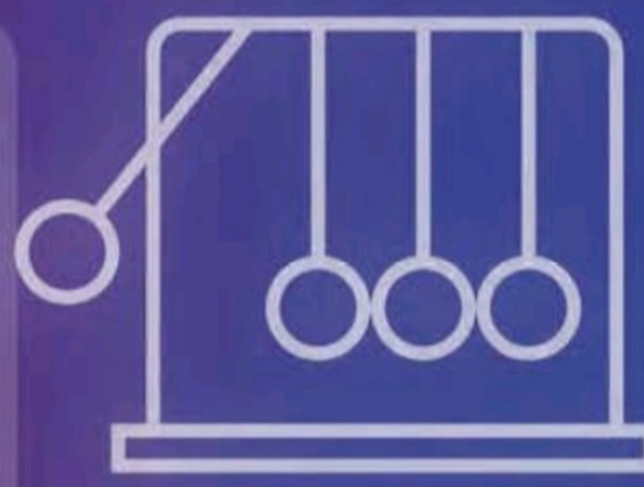
Innovation
Santé connectée

Emploi / Formation / RH
Inetum lance un recrutement géant !

L 14614 - 206 - F: 8,50 € - RD

SEKOIA.IO

Protéger efficacement son organisation n'a jamais été aussi exigeant.



De la prolifération des menaces à la sophistication des attaquants en passant par la complexification des systèmes à protéger, gérer les opérations de cybersécurité peut rapidement virer au cauchemar.

C'est pourquoi depuis 2016 nous avons développé SEKOIA.IO:



Votre back-end de cybersécurité

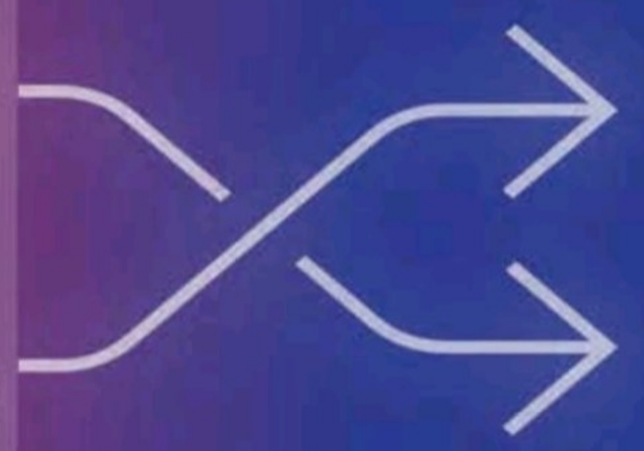
SEKOIA.IO est la plateforme intégrée de cybersécurité qui permet aux équipes SOC, aux analystes CTI et aux DSI et RSSI de piloter leurs opérations à travers les silos, en toute transparence, avec un budget déterministe.
Depuis la détection et la chasse aux menaces avancées jusqu'à la réponse et la supervision de circonstance, SEKOIA.IO fournit la boite à outils ultime pour fédérer vos ressources et amplifier vos efforts.

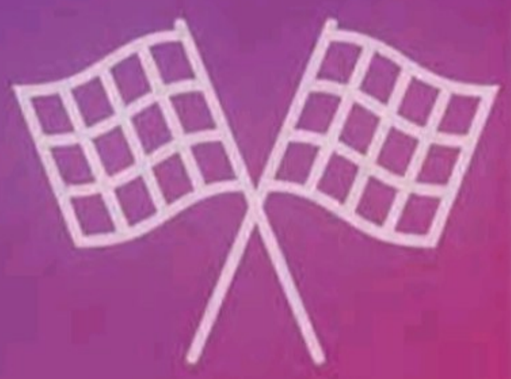
Retrouvez le premier XDR Européen sur sekoia.io/fr/sekoia-io-xdr

Au croisement des intelligences

Le secret des performances de SEKOIA.IO est au croisement des intelligences: l'expertise, l'intelligence artificielle, l'intelligence collective, et la threat intelligence.
Nos 20+ analystes CTI croisent et modélisent en permanence la menace issue de 500+ sources publiques et privées, et la diffusent vers vos équipes, vos équipements, vos prestataires de sécurité.

Retrouvez la CTI préférée des lecteurs de L'Informaticien sur sekoia.io/fr/sekoia-io-cti





Neutralisez les menaces avant impact

L'agilité et la flexibilité de SEKOIA.IO vous permettent d'intercepter les attaques à leurs stades initiaux, parfois bien avant que des charges utiles malveillantes aient pu arriver chez vous.
Notre architecture cloud-native permet un déploiement quasi-instantané: fini le temps des 18 mois de déploiement et des frais professionnels sans fond.

>100
Intégrations natives

>1 Million
endpoints supervisés

>1 Milliard
events/jour



Réservez vite votre démonstration sur

sekoia.io

ou écrivez nous sur:

contact@sekoia.io



SEKOIA, Société par Actions Simplifiées au capital social de 68 464,20 € immatriculée au RCS de Paris sous le numéro B 502 067 705, dont le siège social est sis18-20 Place de la Madeleine à Paris (75008).
SIREN : 502 067 705 — N°TVA intracommunautaire : FR 28 502067705 — © SEKOIA 2022

www.linformaticien.com
L'INFORMATICIEN

RÉDACTION

5, rue Saulnier, 75009 Paris, France.
Tél. : +33 (0)1 74 70 16 30 — *contact@linformaticien.com*

RÉDACTION : Bertrand Garé (rédacteur en chef) et Guillaume Périssat (chef de rubrique)
avec : Eliot Caliorne, Jérôme Cartegini, Michel Chotard, François Cointe, Alain Clapaud, Christophe Guillemin, Victor Miget et Thierry Thaureaux

SECRÉTAIRE DE RÉDACTION : Boutheïna Saddi

MAQUETTE ET RÉALISATION : Franck Soulier (chef de studio)

PUBLICITÉ
Tél. : +33 (0)1 74 70 16 30 — *pub@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,
5, rue Saulnier, 75009 Paris, France
ou à abonnements@linformaticien.com

IMPRESSION

Imprimé en France par Imprimerie Chirat (42)
Dépôt légal : 2ème trimestre 2022

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 : 5, rue Saulnier, 75009 Paris, France.

ISSN 1637-5491

Une publication PCpresse,

GROUPE FICADE

PRÉSIDENT, DIRECTEUR DE LA PUBLICATION :
Gaël Chervet

Tout le monde en parle

Pas un jour sans que ces deux thèmes reviennent dans les colonnes des médias, sur les réseaux sociaux ou dans les conversations. Et ce ne sont pas l'élection présidentielle, ni les prochaines législatives ou encore le conflit en Ukraine. Je veux parler de la blockchain et du travail hybride.

Le plus souvent, les discussions ne tournent qu'autour des cours du Bitcoin ou des attaques sur les Blockchains. Pourtant, cette technologie s'insinue dans tous les secteurs d'activité et prend une place de plus en plus prépondérante sur certains domaines. Plus récemment, un deuxième pays après le Salvador a choisi le Bitcoin comme monnaie. Il est largement temps de se pencher sur les apports et bénéfices qu'apportent cette technologie, et notre dossier est là pour vous montrer sa place réelle. Les bonnes feuilles que nous publions sont sur le corollaire de cette technologie, les NFT, et comment ceux-ci suivent le même chemin en chamboulant différents secteurs de l'économie. Leur émergence préfigure donc le monde de demain. Autant l'appréhender pour en tirer les pleins avantages.

De la même manière, si on discute beaucoup sur le télétravail, ou sur ses conséquences sur les organisations, il n'y a pas vraiment d'analyse sur les impacts qu'a ce changement d'organisation sur les environnements de travail et les matériels qu'utilisent les salariés tous les jours. Notre second dossier fait le point sur les multiples changements induits sur les différentes composantes d'un espace de travail moderne : PC, mobiles, casques audio, caméras, écrans, téléphones…

La réalité virtuelle ou augmentée apporte de nouvelles possibilités. H.G Wells l'avait rêvé dans son roman *« La machine à remonter le temps »*. Il est maintenant possible de revivre dans son fauteuil ce qui faisait la vie des gens ordinaires dans des époques révolues. Vous pouvez faire une chasse aux mammouths, revivre les fêtes vénitiennes de la renaissance, vous mettre dans la peau de personnages célèbres.

Bien sûr, vous retrouverez aussi tout ce qui fait l'actualité de l'informatique et des retours d'expérience dans les entreprises pour s'ancrer dans la réalité du terrain.

Un dernier mot sur notre prochain classement, le Top Tech ESN qui est dans sa dernière ligne droite. Vos votes sont toujours les bienvenus pour mettre en avant les partenaires avec qui vous aimeriez travailler sur vos projets. □

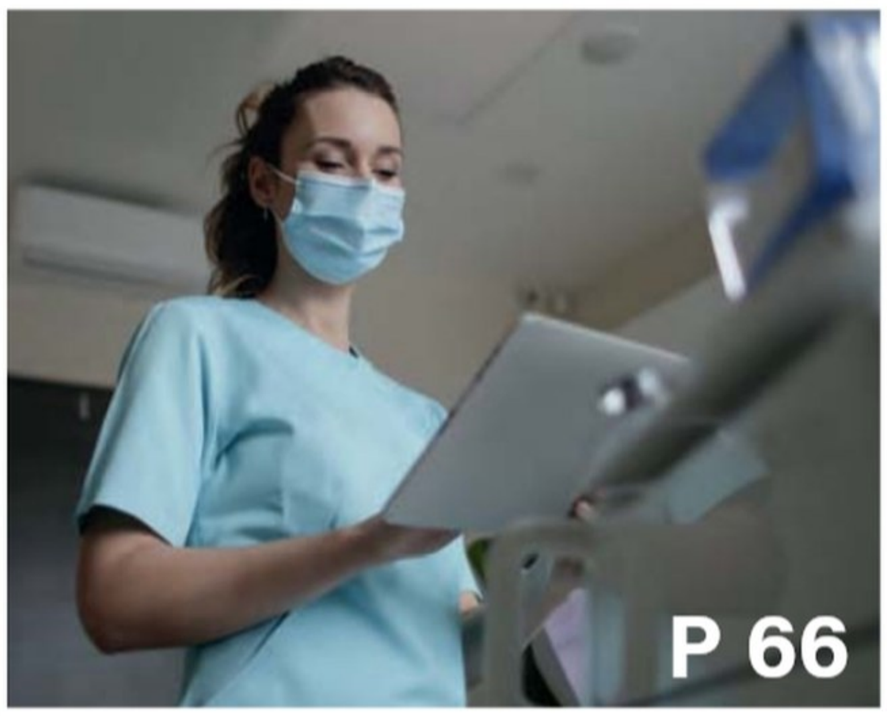
Bertrand Garé
Rédacteur en Chef

La sophistication de la simplicité est un choix assumé

Simple CRM

by S!MPL

https://crm-pour-pme.fr/go









DOSSIERS ..... P 15
Blockchain : une lame de fond discrète
Les postes de travail s'adaptent à de nouveaux besoins

BIZIT ..... P 8
Les actualités du mois

BIZIT PARTENARIATS ..... P 12
Les partenariats à retenir

TACTIC ..... P 23
La dictature du bonheur

HARDWARE ..... P 26
HPE GreenLake
IBM Z16
Intel GPU

RÉSEAU ..... P 32
SD-WAN Juniper
Jaguar Cloud XPR
FortiOS 7.2
Étude F5

LOGICIELS ..... P 37
ITPT Israël
DAM Keepeek
Google BigLake

SÉCURITÉ ..... P 44
Kaspersky dans le viseur
Pindrop traque les fraudes vocales

CLOUD ..... P 48
AWS Summit Paris 2022
Ideta

RETEX ..... P 52
Samusocial
Papernest

DEVOPS ..... P 56
NeuVector

BONNES FEUILLES ..... P 61
Bitcoin et les cryptomonnaies pour les nuls

INNOVATIONS ..... P 66
Santé connectée

ÉTUDE ..... P 68
Étude Veritas sécurité Kubernetes

RH/EMPOI/FORMATION ..... P 71
Inetum recrute

HAVE FUN ..... P 74
Réalité virtuelle

ABONNEMENTS ..... P 73

Penser que la cyberdéfense est compliquée et coûteuse peut porter atteinte à votre entreprise

BT BLUE

BLUE CYBER, sécurisation et protection des systèmes d'information

www.cybersecurite.blue // Ligne dédiée 02 30 30 00 00

• Gosselin design & digital - RCS Rennes 489 918 366 - 11/2021

TOUT SUR LA BLOCK-CHAIN!



FOCUS

Salesforce veut investir 3,5 milliards de dollars en France

Le géant du CRM a annoncé fin mars un important plan d'investissement en France. Depuis 2018, Salesforce a déboursé 2,2 milliards dans l'Hexagone, et prévoit d'injecter à cette enveloppe 3,5 milliards supplémentaires sur cinq ans.

En amont de l'étape parisienne de son Salesforce World Tour, le géant Américain a dévoilé ses nouveaux projets d'investissements en France. En avril 2018, Salesforce avait présenté un plan de 2,2 milliards d'euros sur cinq ans : il rallonge de 3,5 milliards d'euros et de cinq années supplémentaires, afin de soutenir sa phase de croissance actuelle. La branche hexagonale du spécialiste du CRM entend notamment étendre considérablement sa surface de bureaux, principalement à Paris, afin d'accueillir ses effectifs en constante augmentation. Il y compte pour l'heure 1500 salariés et des locaux dans la capitale, à Lyon, Nantes et Grenoble. En outre, l'Américain veut répondre aux préoccupations croissantes en matière de souveraineté et de localisation des données : il investira dans son offre d'infrastructures, afin que ses clients puissent traiter et stocker leurs données dans l'Union européenne (UE).

Émilie Sidiqian, Vice-présidente exécutive et Directrice générale de Salesforce France.



« Cet investissement à long terme, contribuera également au développement économique du territoire français au cours des cinq prochaines années. »

Hyperforce en VF

C'est en ce sens que Salesforce a annoncé la disponibilité en France d'Hyperforce, cette déclinaison de l'architecture de la plateforme de Salesforce, prévue pour que Salesforce Customer 360° puisse fonctionner sur les principaux clouds publics *« de façon fiable et sécurisée »* comptera d'ici à la fin de l'année une « EU Operating Zone ». Ce qui, selon le géant, *« permettra aux clients de Salesforce de traiter et stocker leurs données dans l'Union européenne »*. Articulée autour d'une offre de services dédiés aux clients dans l'Union européenne, et une assistance 24/7 basée elle aussi sur le territoire européen, Hyperforce EU Operating Zone s'appuie sur les offres d'hébergement au sein de l'UE déjà proposées par Salesforce et Slack, de sorte que les utilisateurs de Salesforce Customer 360° n'aient pas à transférer leurs données, leurs index et leurs clés de chiffrement de l'autre côté de l'Atlantique. *« Hyperforce EU Operating Zone s'inscrit dans le cadre de notre engagement historique en faveur du respect de la protection des données, et offre les meilleures protections contractuelles qui soient pour contester les demandes d'accès à des données émanant d'autorités gouvernementales »* assure le géant.

But non lucratif

« Salesforce continue de prospérer aux côtés d'un écosystème florissant de clients et partenaires. Nous sommes donc ravis de développer notre présence, d'accroître notre investissement sur de nouveaux talents, et d'orienter notre entreprise et nos parties prenantes sur la voie de la réussite », explique Émilie Sidiqian, Vice-présidente exécutive et Directrice générale de Salesforce France. *« Notre croissance rapide est le résultat du choix de nos clients d'accélérer leur transformation numérique, et de faire appel à Salesforce en tant que partenaire de confiance. Nous sommes fiers de répondre ainsi à l'engagement que démontrent, auprès de nous, nos clients et partenaires. Cet investissement à long terme, contribuera également au développement économique du territoire français au cours des cinq prochaines années »*.

Fidèle à la stratégie 1/1/1, l'éditeur prévoit enfin des investissements à des fins caritatives. Dernièrement, sa plateforme gratuite d'apprentissage en ligne Trailhead comptait 1 500 partenaires pour 50 000 apprenants. En outre, l'entreprise a fait don de 270 000 euros à l'association Sport dans la Ville, qui œuvre en faveur de l'insertion professionnelle par le sport de jeunes adultes n'étant ni à l'emploi, ni aux études, ni en formation et issus de milieux défavorisés à Paris et Lyon.

La **reprise de Sigfox** otage des élections présidentielles

Au moment où nous écrivons ces lignes, on ne sait qui d'Emmanuel Macron ou de Marine Le Pen l'aura emporté au second tour. Et on ignore également qui reprendra Sigfox. Pourtant, la décision du tribunal de commerce de Toulouse était attendue le 14 avril. Quatre mois plus tôt, après plusieurs années de vache maigre, le fleuron français, le spécialiste de la 0G, était placé en redressement. Neuf repreneurs se sont manifestés et trois se sont retrouvés dans le dernier carré. Parmi eux, un certain UnaBiz, opérateur du réseau Sigfox en Asie monté par un ancien de l'entreprise de Labège, Henri Bong, et une poignée d'entrepreneurs français, en majorité des expatriés. Cette offre était plébiscitée aussi bien par la direction de Sigfox que par ses salariés. *« L'offre déposée par UnaBiz est la plus intéressante sur le volet social [...]. Le CSE estime crédible et intéressante la diversification des sources de revenus expliquée dans la stratégie. UnaBiz est légitime et inspire confiance dans l'exécution de cette stratégie [...], ainsi que sur sa vision technique. Pour ces raisons, le CSE se prononce donc favorablement sur l'offre de reprise proposée par UnaBiz »* explique Antoine Maïer, élu au CSE de Sigfox.

Mais la proposition d'UnaBiz, considéré comme un investisseur étranger, est soumise à une procédure spéciale pilotée par Bercy. Dont le feu vert se fait cruellement attendre. Le dossier du repreneur, quoique complet, est toujours en cours d'instruction. Selon le CSE, le ministère de l'Économie n'entend pas, pour des raisons politiques, donner son accord avant le 24 avril, date du second tour


Jeremy Prince, CEO de Sigfox.

des élections présidentielles. Second problème : c'était le 14 avril que le tribunal de commerce de Toulouse doit statuer sur le sort de Sigfox. *« Les salariés ne souhaitent pas que des enjeux politiques viennent perturber leur avenir, et ne comprennent pas que des considérations d'entre-deux-tours puissent les priver de leur emploi et mettre à risque la technologie pour laquelle ils ont tant investi »* écrit le CSE. Pire encore, le 13 avril, Henri Bong écrivait que le dossier d'UnaBiz aurait été rejeté par Bercy. *« Je peux difficilement comprendre et encore moins accepter que la politique puisse priver une société déjà en péril et ses employés de bénéficier du meilleur projet pour la sauver »*, déplore-t-il.

Télécoms en Italie : la marche à la concentration se poursuit, lentement

Après qu'Iliad se soit cassé les dents dans la péninsule sur Vodafone Italia, un autre acteur de poids est à la peine. Le fonds américain KKR n'entend pas revoir son offre de 10,8 milliards d'euros pour s'offrir TIM, anciennement Telecom Italia, tandis que le principal actionnaire de l'opérateur, Vivendi, campe sur ses positions, considérant l'offre trop basse. Mais voici que TIM révèle avoir été approché par un autre fond, CVC Capital Partners. Lequel se contenterait pour l'heure d'une participation minoritaire au capital de l'opérateur italien… non sans préparer l'hypothèse d'une scission du groupe entre ses activités sur le segment du fixe et ses activités de services. Si l'accord venait à aboutir, la nouvelle entité *« inclurait les activités de la division Enterprise de TIM (connectivité et services ICT) en plus de celles de Noovle (stockage des données), Olivetti (informatique), Telsy (cybersécurité) et Trust Technologies »* indique TIM dans son communiqué. Avec, au capital, un CVC tout disposé à prendre le contrôle de la société de services nouvellement créée.



RACHATS

Feu **DenyAll** change encore de main

L'éditeur français de solutions de sécurité des applications, racheté en 2017 par Rohde & Schwarz, est revendu au Néerlandais Total Specific Solutions. Rohde & Schwarz Cybersecurity France n'est rien de moins que la quatorzième acquisition de TSS en France, après celles d'Adapt Informatique en février dernier et d'Alcuin et de Tribofilm en 2020. Mais il s'agit de la première dans le domaine de la cybersécurité pour le Néerlandais. Notons que TSS est un fournisseur de solutions logicielles diverses et variées basé aux Pays-Bas et filiale européenne du Canadien Topicus, lui-même filiale de Constellation Software, géant de Toronto aux multiples ramifications. Stéphane de Saint Albin, le patron de Rohde & Schwarz Cybersecurity France, explique que *« en tant que propriétaire perpétuel, TSS achète des entreprises sans jamais les revendre, dans le but de les aider à croître : cela apporte une fondation solide pour les prochaines étapes de notre entreprise. Être une entreprise française et propriété européenne signifie que nos clients peuvent continuer à profiter de nos solutions souveraines et conformes au RGPD »*.

HP sort 3,3 milliards pour **Poly**

Le constructeur a annoncé son intention de s'offrir le fabricant d'équipements audio et vidéo, et spécialiste des communications d'entreprise. Le montant de l'opération s'élève à 1,7 milliards de dollars, en numéraire, un bonus de 53% par rapport au cours de l'action, et grimpe à 3,3 milliards en incluant la reprise de la dette de Poly. L'acquisition devrait contribuer significativement au chiffre d'affaires de HP dès sa conclusion après les étapes réglementaires habituelles, soit vers la fin de cette année.



KKR prend **Barracuda Networks** à Thoma Bravo

Le fonds d'investissements rachète Barracuda Networks à Thoma Bravo, qui en avait fait l'acquisition en 2017. KKR prévoit d'accélérer cette croissance sur des secteurs clés comme les services autour de la détection et réponses aux attaques et les technologies présentes dans le modèle SASE (Secure Access Service Edge). Avec cette acquisition qui devrait se conclure d'ici la fin de l'année, KKR regroupe DarkTrace, Cylance, et Ping Identity aux côtés de Barracuda Networks.



Perforce rachète **Puppet**

Le spécialiste du DevOps a signé un accord définitif pour reprendre la plate-forme d'automatisation Puppet. Aucun détail n'a été donné sur la transaction. Pionnier de l'infrastructure as code, Puppet va apporter un complément important à la plate-forme de Perforce par ses capacités d'automatisation et ses fonctions de sécurisation des pipelines de développement. Au total, ce sont 40 000 organisations qui utilisent Puppet dans le monde.

Kaseya s'offre **Datto**

Victime d'une attaque à l'été dernier qui avait laissé nombre de ses clients sur le carreau, l'intégrateur se rachète une image avec l'acquisition de Datto, pour 6,2 milliards de dollars. Datto fournit entre autres des solutions de PCA, de sécurité réseaux et de protection des endpoints à destination des MSP. La transaction, effectuée entière en numéraire, est financée par une poignée d'investisseurs de Kaseya. L'opération doit être bouclée, sous réserve de validation par les autorités compétentes, au second semestre 2022.

Sailpoint tombe dans le giron de **Thoma Bravo** pour 6,9 milliards de dollars

Un an tout juste après s'être offert Proofpoint, Thoma Bravo s'offre un autre acteur de la cybersécurité en la personne de SailPoint, éditeur de solutions de gestion et de protection des identités en entreprise. La transaction, entièrement en espèces, coûtera 6,9 milliards de dollars au fonds. Une fois l'opération bouclée, SailPoint sortira du NYSE.

Beamy grandit avec une première levée de fonds

Beamy est un spécialiste de « l'informatique décentralisée », ce que d'aucuns qualifient de « shadow IT ». Fournissant une plateforme de gestion du parc applicatif SaaS de l'entreprise, cette jeune pousse lilloise a su séduire des grands comptes, de LVMH à Orange en passant par BNP Paribas. Et elle attire également les investisseurs. Dans un communiqué, Beamy nous apprend avoir bouclé sa première levée de fonds, une Série A d'un peu plus de 8 millions d'euros. Ont abondé à ce tour de table les fonds Aglaé Ventures, ISAI ainsi que des Business Angels. Forte de cet argent frais, la jeune entreprise compte désormais accélérer à l'international, sachant qu'elle est déjà présente de l'autre côté de la Manche. *« Nous sommes convaincus que la problématique SaaS est un enjeu majeur pour les grandes entreprises, qu'elles soient françaises ou internationales »* explique Andréa Jacquemin, CEO et cofondateur de Beamy. *« Avec cette levée, réalisée auprès de grands fonds dont Aglaé Ventures et Isai, tous deux reconnus pour offrir des expertises pointues dans le secteur de la tech à l'image des startups déjà soutenues, nous partons à la conquête de l'international »*. L'entreprise, qui assure avoir réalisé une *« très belle fin d'année 2021 »*, prévoit d'employer ces fonds dans deux objectifs. D'une part, recruter une quarantaine de salariés dans les douze prochains mois. Et de l'autre, renforcer son produit, autour de la détection et des workflows de décentralisation.



Andréa Jacquemin, CEO et cofondateur de Beamy.

2 milliards de dollars de plus pour **Epic Games**



Avec cette nouvelle levée de fonds abondée, à nouveau, par Sony, la valorisation d'Epic Games atteint 31,5 milliards de dollars. Avec cette nouvelle enveloppe, l'entreprise ambitionne de s'aventurer sur le long terme dans le Metavers. Cet investissement doit permettre à Epic Games de *« créer des espaces où les joueurs peuvent s'amuser avec des amis, les marques peuvent créer des expériences créatives et immersives et les créateurs peuvent construire une communauté et prospérer »*, a précisé Tim Sweeney, PDG et fondateur d'Epic Games.

Binance lève 200 millions de dollars

La plateforme d'échanges de cryptomonnaies lève 200 millions de dollars auprès de RRE Ventures, Foundation Capital, Original Capital, VanEck et Circle Ventures. Sa valorisation est portée à 4,5 milliards de dollars, bien loin derrière son pire ennemi Coinbase, mais Binance compte à nouveau lever des fonds dans les prochains mois.

Remote valorisée 3 milliards de dollars

La start-up développeuse d'une plateforme SIRH annonce sa troisième levée de fonds, à 300 millions de dollars, menée par Softbank. Sa Serie B à 150 millions de dollars a eu lieu en fin d'année dernière. Remote se trouve ainsi valorisée 3 milliards de dollars en trois ans d'existence. *« Grâce à cette levée de fonds, nous serons en mesure de développer davantage de produits, notamment nos plateformes de paie internationale et de gestion des indépendants, ainsi que d'élargir notre offre de services et d'avantages »* se réjouit Job van der Voort, cofondateur et CEO de Remote.

Deloitte et VMware créent un pôle commun sur le cloud distribué

Les deux partenaires annoncent conjointement la création de Deloitte VMware Distributed Cloud.

Le pôle aura pour mission d'aider les clients à transformer leurs activités et leurs secteurs, en mettant en place et en utilisant plus efficacement des architectures Cloud distribuées. Créé au sein de Deloitte, ce pôle DVDC stratégique proposera des services de développement logiciel et multi-Cloud avancés pour accélérer le lancement de produits grâce à des environnements Cloud distribués. Les services VMware Cross-Cloud (notamment VMware Tanzu) permettront de bâtir une plateforme pour des applications Cloud-natives modernes. Deloitte pourra ainsi accélérer et sécuriser la mise en production d'applications destinées à une variété d'industries (commerce de détail, secteur public, santé, services financiers ou encore automobile).

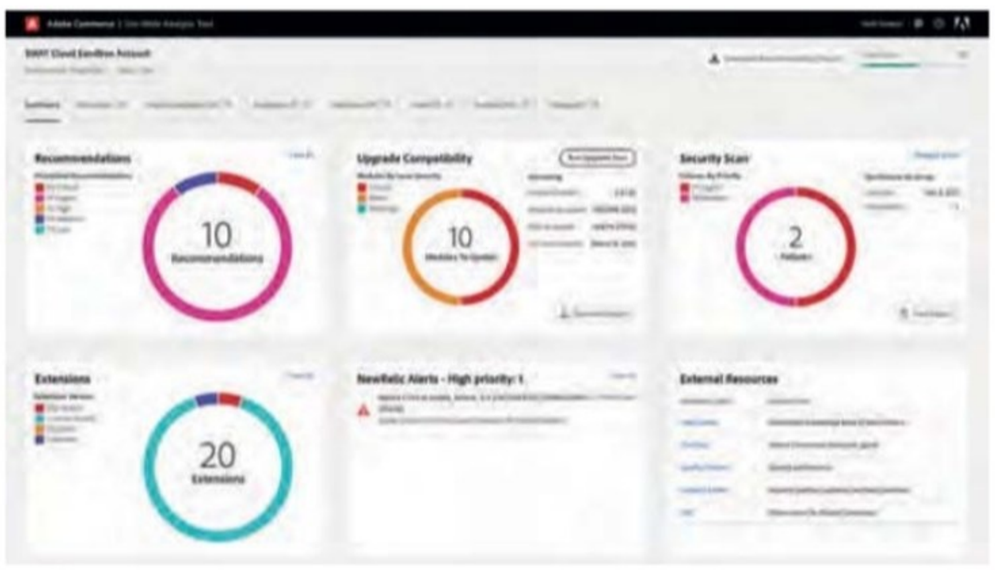
Centreon validé par AWS

L'éditeur français de solutions de supervision a un accord de collaboration stratégique avec Amazon Web Services (AWS) pour héberger Centreon Cloud, sa nouvelle plateforme de supervision en mode SaaS (Software as a Service). Après une phase bêta réussie en collaboration avec des clients sélectionnés, Centreon Cloud est entré dans une phase de Controlled Availability pour six mois et est désormais commercialisé dans certaines régions depuis le 1er Mars 2022. Cette offre SaaS sera disponible sur tous les marchés dans le courant de l'année. Les équipes d'AWS collaborent avec Centreon depuis le début du projet pour concevoir une solution Cloud Native et sélectionner les services AWS appropriés offrant une combinaison optimale de coût, de sécurité, et de performance.
La plateforme Centreon peut découvrir automatiquement et superviser les infrastructures Cloud avec des alertes sans configuration, une connectivité et des intégrations « No-Code » pour plus de 700 types de composants IT. Elle peut également superviser en même temps les équipements hérités, sur site et en bordure de réseau (Edge), offrant ainsi une visibilité Cloud-to-Edge. En complétant les revues techniques (FTR) et d'architecture (WAR) pour Centreon Cloud, Centreon valide son parcours software au sein du programme AWS Partner Network.

Partenariat renouvelé pour 5 ans entre Platform.sh et Adobe

Durant une nouvelle période de cinq ans, Adobe Commerce continuera d'exploiter le service PaaS (Platform as a Service) de Platform.sh.

Dans le cadre de cet accord, Platform.sh devient un partenaire privilégié du programme Adobe Exchange. L'extension du partenariat s'inscrit dans l'évolution d'Adobe Commerce permettant aux clients de créer, d'exécuter et de faire évoluer facilement une expérience commerciale complète, le tout dans le cloud. La gestion de l'infrastructure Platform.sh pour Adobe Commerce Managed Services et Cloud Pro



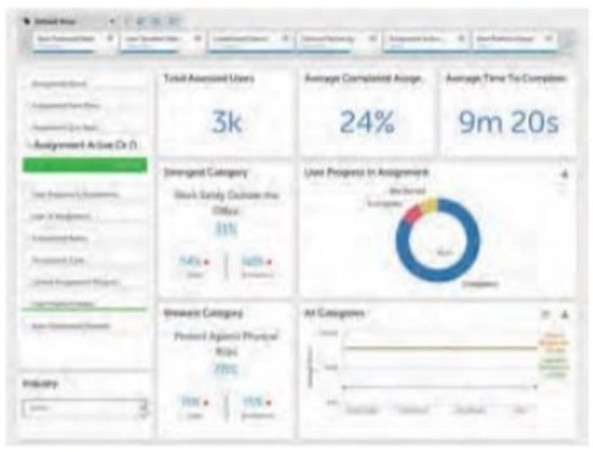
rationalise l'expérience des développeurs et la vitesse de déploiement, tout en optimisant les performances du cloud et l'efficacité de l'infrastructure. Enfin, en se concentrant sur l'efficacité, Platform.sh aide Adobe à réduire son empreinte carbone sur sa plateforme de commerce en ligne.

Fivetran étend sa relation avec Google Cloud

L'éditeur de solutions d'intégration de données prend en charge le Google Cloud Cortex Framework et devient partenaire du nouveau programme Google Cloud Ready-Big Query.
Fivetran a prouvé la capacité de sa solution à gérer les besoins complexes et à haut volume de données essentiels pour tirer parti de la structure Cortex de Google Cloud. De plus, en tant que partenaire de lancement du programme Google Cloud Ready - BigQuery, Fivetran est reconnue et certifiée pour sa capacité à répliquer les données provenant d'applications clés, de flux d'événements, de stockages de fichiers et plus encore dans BigQuery.

Proofpoint et Orange Cyberdefense partenaires autour de la formation des employés

Proofpoint s'associe à Orange Cyberdéfense pour sensibiliser et former les employés à la cybersécurité.



Orange a obtenu la certification « partenaire spécialisé » pour proposer à ses clients des programmes reconnus de formation et de sensibilisation à la cybersécurité. La combinaison des services des experts Orange Cyberdefense avec la solution de sensibilisation à la sécurité de Proofpoint, vise à fournir la bonne sensibilisation au bon utilisateur, au bon moment. Elle s'appuie sur une simulation de phishing personnalisée basée sur des menaces réelles, en évaluant le risque pour l'utilisateur selon un modèle centré sur les employés. Elle leur donne les moyens de signaler les messages suspects depuis leur boîte mail, réduisant ainsi le temps nécessaire pour neutraliser une menace active de plusieurs heures à quelques minutes. Dans ce programme, les entreprises bénéficient d'une assistance complète du conseil à l'intégration, incluant la création de plans de sensibilisation et le suivi des changements de comportement, pour aider les clients à optimiser leur déploiement en fonction de leurs capacités et des ressources disponibles. Le service est accessible en français et en 40 langues.

Panasas rejoint le réseau de partenaires de Thales

Le fournisseur de solutions de stockage pour les environnements HPC rejoint le réseau de partenaires de Thales.

Panasas a récemment rejoint le réseau de partenaires Thales Accelerate et collabore avec Thales sur la sécurité du stockage HPC et les charges de travail AI/ML dans des secteurs variés tels que le monde universitaire, le gouvernement, les sciences de la vie, la recherche, la fabrication et les services financiers. Cela inclut l'intégration de Thales TCT CipherTrust Manager avec Panasas PanFS, le système de fichiers parallèle Panasas, pour atténuer la menace d'un accès non autorisé aux données cryptées.

Rackspace s'accorde avec Cohesity

Le fournisseur de services de Cloud et d'hébergement annonce un accord de partenariat stratégique avec Cohesity, un spécialiste de la sauvegarde et de la gestion des données. S'appuyant sur la solution DataProtect de Cohesity, Rackspace Data Protection simplifie la sauvegarde et la restauration globales en remplaçant plusieurs produits ponctuels par une solution unique de sauvegarde et de restauration sur tous les Clouds VMware. Elle permet également aux entreprises de protéger et de gérer les sources de données traditionnelles et modernes à partir d'une interface utilisateur unique et mondiale. La solution vise surtout à la protection contre les rançongiciels avec la fonction de snapshots immutables empêchant de chiffrer les données de sauvegarde. La solution embarque aussi des fonctions d'apprentissage machine pour aider à découvrir des menaces cachées et alerter les clients dès qu'une cyberattaque potentielle est repérée. Les snapshots entièrement hydratés peuvent permettre aux utilisateurs disposant d'accès administrateurs de restaurer rapidement les données dans leur granularité ainsi que l'ensemble des applications et ce à tout moment. De plus, Rackspace Data Protection optimise la capacité de stockage et la mobilité des données grâce à la déduplication et à la compression globale à longueur variable, qui réduit considérablement la place prise par les données des clients ainsi que la surface d'attaque potentielle.

AGENDA

Dell World
2-5 mai 2022
Las Vegas, USA
The Venetian Resort

Zendesk Relate
11 mai 2022
Virtuel

Kube con + CloudNativeCon
16 au 20 mai
Valence, Espagne
Feria Valencia

FIC
7-8-9 Juin 2022
Lille Grand Palais

Teratec Forum
14 Juin 2022
Ecole Polytechnique, Palaiseau

IT Partners
15-16 juin 2022
Disneyland Paris

Cloud Computing World Expo
29 Juin 2022
Parc des Expositions, Paris Porte de Versailles

MtoM & Objets connectés
29 Juin 2022
Parc des Expositions, Paris Porte de Versailles

RTS embedded systems
29 Juin 2022
Parc des Expositions, Paris Porte de Versailles

iExec
Blockchain

Solution tout-en-un pour la gouvernance, la confidentialité, la confiance

Et s'il était possible de tirer parti de vos données sensibles ou confidentielles, sans jamais les révéler ?

Alliant Blockchain et Calcul Confidentiel, iExec fournit une solution permettant de traiter et de partager des données confidentielles entre plusieurs parties prenantes.

Blockchain

Calcul Confidentiel

Gouvernance

Définir qui peut accéder aux données, à quelles données spécifiques et sous quelles conditions.

Confidentialité

Les données sont chiffrées et restent totalement confidentielles et sécurisées.

Confiance

Le détail des tâches exécutées est enregistré de manière transparente et infalsifiable.

Visitez notre site internet

iex.ec/fr/consulting-blockchain-france

UNE LAME DE FOND DISCRÈTE

Comment la technologie blockchain s'impose dans toutes les industries

Elle ne peut pas être résumée à des effets de mode, comme les ICO (Initial Coin Offering) ou les NFT (Non Fungible Token), qui tirent parti de ses fonctionnalités. Non : la technologie blockchain se diffuse rapidement dans tous les secteurs, notamment grâce à ses arguments techniques que sont la sécurité, la décentralisation ou la traçabilité par exemple. Retour aux sources !

Il existe un phénomène étrange. Combien de fois entendez-vous parler de cryptomonnaies, Bitcoin en tête, des NFT, ces jetons non fongibles dont les volumes d'échanges explosent, des financements parfois ahurissants récoltés en actifs numériques, *etc.* ? Ces derniers temps, le concept de Web3 semble aussi tenir la corde, tout comme les métavers grâce à Facebook qui s'est renommé Meta. C'est étrange, effectivement, car le lien entre tous ces éléments est unique : c'est la technologie blockchain, et rien d'autre. Et ses applications concrètes et utiles ne sont, quant à elles, que rarement mises en avant.

Les projets blockchain : une véritable lame de fond

Avant tout, les chiffres montrent concrètement que nous ne sommes plus face à un phénomène de mode comme ces dernières années. Les projets qui étaient encore en phase de PoC (Proof of Concept), il y a quelque temps, se muent de plus en plus en produits concrets, utilisables et commercialisables. Et ce, grâce notamment aux budgets qui ne cessent de croître. En l'occurrence, plus de la moitié des projets portés par des « pure players » dans le monde sont désormais en phase de commercialisation, contre 22% des projets similaires dans les entreprises traditionnelles. Sur la France uniquement, 58% des projets blockchain sont désormais disponibles sur le marché.

Selon une étude de PwC, fondée sur les témoignages de plus de 140 sociétés dans le monde, ce sont aussi les dépenses allouées qui grimpent en flèche. En effet, plus de la moitié des entreprises traditionnelles interrogées ont débloqué des montants dépassant le million d'euros pour l'année 2021. *« Les entreprises ayant développé un projet blockchain ont d'ailleurs la volonté de poursuivre leurs investissements dans cette technologie. 99 % des acteurs dans le monde veulent maintenir (33 %) ou augmenter (66 %) le budget consacré à la blockchain »*, lit-on encore dans l'étude.

Rappelons évidemment qu'en France, les levées de fonds records de ces derniers mois ont eu un impact non négligeable sur cet engouement quasi généralisé. Outre la vague des NFT évidemment qui agit comme un véritable effet de levier, des entreprises ont marqué au fer rouge l'année 2021. En l'occurrence, le français Ledger, spécialiste de la sécurisation des portefeuilles électroniques, a levé 380 millions de dollars en juin dernier. Mais ce n'est pas le plus impressionnant : la start-up Sorare, dont le jeu de Fantasy Football repose sur la blockchain, a bouclé une série B de

QUELS SONT LES CRITÈRES PRINCIPAUX POUR LE CHOIX D'UNE BLOCKCHAIN ?

Outre les qualités naturelles des différents protocoles, chaque projet dispose également de ses propres nécessités. Comme dans tout projet informatique, les décideurs doivent donc se focaliser sur leurs besoins. Et en termes de choix, les Français en retiennent clairement trois, dans l'ordre : sécurité du protocole (à 75%), scalabilité (62%) et coût des transactions (à 53%). D'autres critères entrent en jeu comme notamment la vitesse, le nombre de transactions par seconde. En France particulièrement, celui de la consommation énergétique revêt une importance particulière, avec 49% des répondants de l'étude PwC qui disent y être très sensibles…

L'IMPACT DE LA BLOCKCHAIN SUR L'ÉCONOMIE FRANÇAISE

Comme le cloud computing en son temps, la blockchain au sens large est aussi synonyme de révolution technologique, et donc de retombées économiques. Les derniers chiffres donnent effectivement le tournis et permettent de mettre en lumière l'adoption de cette technologie. Tout d'abord sur le PIB : en France uniquement, on estime qu'elle permettra de l'augmenter de 58,5 milliards de dollars d'ici 2030, soit environ 2% du PIB actuel. Ce chiffre grimpe à 1760 milliards de dollars au niveau international. Toujours à un point de vue mondial et à horizon 2030, on évalue la création d'emplois à près de 40 millions, dont 500000 le seront en France. Enfin, les cinq secteurs les plus impactés positivement dans l'économie française pour les années à venir seront :



- **La traçabilité (33 milliards de dollars) ;**
- **La titrisation et les paiements (13 milliards de dollars) ;**
- **L'identité et la certification numérique (8 milliards de dollars) ;**
- **Les accords et les litiges (4 milliards de dollars) ;**
- **La fidélisation et l'engagement client (1 milliard de dollars).**

680 millions de dollars, signant la plus grosse levée de l'histoire de la French Tech. Au niveau international, ce ne sont pas moins de 30,5 milliards de dollars qui ont été investis en 2021, soit une augmentation de 450% par rapport à 2020.

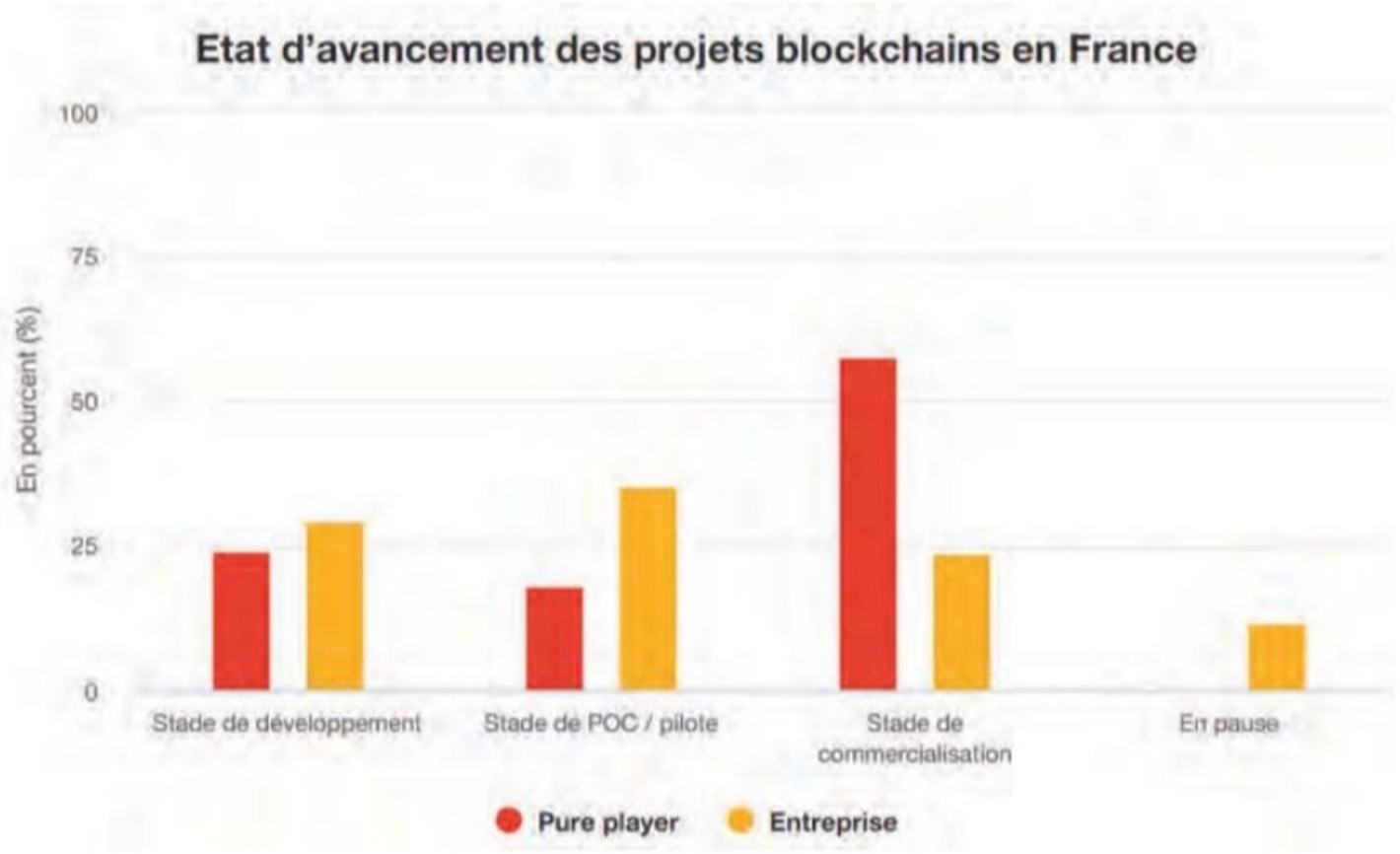
Les qualités des blockchains par l'exemple

Tous les chiffres cités ci-avant en feraient presque oublier pourquoi la technologie blockchain fait une entrée tonitruante dans les entreprises et par extension, dans le quotidien. Sans trop de lyrisme, on serait tenté de dire que c'est tout d'abord un nouveau monde qui se développe sous nos yeux. Et c'est bel et bien le cas : transparence, sécurité, décentralisation... Tous ces qualificatifs ne sont pas que des mots, ce sont des faits. Mieux : ils sont applicables à quasiment tous les secteurs industriels ou non. Globalement, à quasi toutes les entreprises, les métiers et les chaînes de valeur.

En l'occurrence, prenons l'exemple d'un secteur qui n'a pas encore été touché par la révolution numérique. Il s'agit du système mondial des services environnementaux, et par extension de l'émission et de la vérification des crédits carbone. Encore actuellement, ce système est majoritairement manuel, basé sur l'élaboration de registres internationaux archaïques. Le principe consiste à définir des protocoles scientifiques, lesquels sont audités sur le terrain par des sociétés de conseil auprès de propriétaires forestiers. Une redevance est ensuite perçue pour chaque crédit carbone généré. On estime qu'il faut 3 ans et environ de 700 000 dollars pour certifier une zone arborée, quelle que soit sa taille. D'autant plus que chaque



Le service de stockage cloud Filecoin est aussi adapté pour les entreprises avec de gros volumes de données via le service largedata.filecoin.io



L'année 2021 marque clairement une avancée des projets blockchain qui ne sont plus simplement des essais, mais deviennent bel et bien des projets industriels.

transaction est recensée au sein d'une base de données classique. Sur ce dernier point, la blockchain pourrait facilement faire son office : enregistrer les transactions de crédits carbone sur un registre décentralisé, transparent, auditable et résistant aux attaques externes. Elle permettrait donc tout d'abord de réduire drastiquement les coûts et la facturation (élevée !) de ces services par des instances internationales. De plus, elle règle également un problème épineux : celui de la « double dépense ». Un crédit carbone ne pourrait donc plus être utilisé ou vendu plus d'une fois, et encore moins sans que son origine et sa viabilité soit remis en question.

Blockchains : retour aux sources

Si l'on a vu apparaître de nombreux protocoles publics différents ces dernières années, la base et le concept général ne changent pas : une blockchain reste un outil de stockage et d'échange de valeur décentralisé. C'est donc une base de données qui regroupe tous les échanges et l'historique depuis sa création. Étant distribuée, et sans autorité centrale, chacun peut ainsi en vérifier la validité et l'intégrité.

Le fonctionnement global est même relativement simple : les transactions sont regroupées dans un bloc, lui-même validé par les nœuds du réseau ; cette même validation qui fait l'objet de débats entre la preuve de travail utilisée par Bitcoin, et la preuve d'enjeu, moins énergivore et désormais utilisée par la majorité des protocoles. Quoi qu'il en soit, une fois le bloc validé, il est horodaté puis ajouté à la chaîne générale.

Cela ne veut pas dire que les blockchains peuvent tout résoudre. D'ailleurs, l'apparition de multiples protocoles est aussi le signe que chaque secteur, chaque application, a des besoins bien différents. Il peut s'agir de la sécurité, du coût des transactions ou de la mise à l'échelle (scalabilité) du réseau par exemple. Ceci est généralement schématisé par le concept de « trilemme des blockchains ». Ce terme, popularisé par le créateur d'Ethereum, Vitalik Buterin, indique que la valeur d'un protocole et de sa cryptomonnaie associé peut être évalué en fonction de trois critères : sécurité, décentralisation et scalabilité. Il est ainsi complexe pour une blockchain d'allier ces trois atouts. Bitcoin par exemple est très décentralisée et sécurisée, mais cela joue sur sa capacité à supporter un grand nombre de transactions simultanées ; d'où la naissance du « Lightning Network », qui permet de réaliser des opérations « off chain », en dehors du réseau.

Quoi qu'il en soit, ces blockchains ont toutes des atouts communs : transparence, traçabilité et auditabilité, sécurité, confidentialité et absence de SPF (Single Point of Failure) ou encore décentralisation. Ces avantages ont ainsi donné lieu à la création d'applications que l'on pourrait qualifier de « Web3 » (voir encadré).

QU'EST-CE QUE LE WEB3 ?

S'il est clair que c'est la continuité logique du Web2, il est encore délicat de dessiner précisément ses contours, car il se construit actuellement et progressivement. Il n'existe pas encore dans la mesure où son périmètre n'est pas encore bien défini, et que son existence est encore limitée. Voici toutefois ce que l'on sait :

- **Le Web3 est décentralisé par nature ;**
- **Il est détenu par ses utilisateurs et ses concepteurs ;**
- **Il fonctionne grâce à l'économie des jetons numériques (token economy) ;**

Il s'agit aussi et avant tout d'un assemblage de technologies comme la blockchain évidemment, pierre centrale de la constitution d'un réseau global, décentralisé et moderne. Mais aussi les Dapps (applications décentralisées), les portefeuilles numériques qui sont au centre de l'échange de valeur, les NFT (Non Fungible Tokens) qui représentent la certification numérique de biens numériques, les DAO (Decentralized Autonomous Organisations) qui sont un système de fonctionnement aux règles communes et définies par des smart contracts (contrats intelligents) ou encore les métavers, des univers virtuels reposant eux aussi sur les fondations techniques du Web3.

L'interface de Storj est très simple à prendre en main. Ici, nous avons stocké le logo de *L'Informaticien*, instantanément découpé en 80 morceaux lesquels sont stockés sur plus d'une trentaine de nœuds de par le monde.



Des applications industrielles en pagaille

Comme expliqué précédemment, la blockchain est intrinsèquement une technologie de stockage et de traçabilité des données. C'est pourquoi ces applicatifs ont rapidement fleuri, et sont même adaptés aux règles et au contexte réglementaire. En la matière, KeeeX fait office de fleuron tricolore, son procédé breveté allant plus loin que la simple preuve. En effet, *« Il permet à nos clients d'y ajouter des signatures et des horodatages qui peuvent être qualifiés au sens du règlement eIDAS, et bénéficier ainsi d'une présomption de fiabilité par défaut en justice »*, explique l'entreprise marseillaise.

C'est donc sur les atouts des blockchains que se sont construits de nombreuses applications, et notamment sur l'aspect de la décentralisation. En France, iExec fut l'un des pionniers du cloud computing 2.0 : il connecte fournisseurs et utilisateurs de ressources informatiques, et leur permet de louer de l'espace ou de le monétiser. En utilisant le protocole P2P distribué IPFS (InterPlanetary File System), Filecoin permet quant à lui à n'importe qui de participer à un réseau de stockage mondial tout en profitant de la sécurité du réseau et des possibilités d'authentification des documents. Et même de l'intégrité d'un fichier, assurant son inaltérabilité, et de son nombre de copies ! Enfin, Filecoin utilise un mécanisme de chiffrement des données de bout en bout : les fournisseurs de stockage n'ayant évidemment pas accès aux clés de déchiffrement.

Cette approche du cloud décentralisé a été répliquée par d'autres projets, avec des approches différentes. Car Filecoin limite la conservation des fichiers (ou plutôt fixe leur durée de stockage avant qu'ils puissent être effacés) dans le temps, sauf à utiliser un service tiers comme Pinata ou Eternum. Ainsi, les projets Siacoin par exemple, ou le plus connu Storj, ont vu le jour. La différence majeure réside dans le traitement des fichiers, qui sont divisés dans le cas de ce dernier, et dans la permanence par défaut du stockage. □

Eliot Caliorne

PROTOCOLES DE STOCKAGE : IPFS ET ARWEAVE

InterPlanetary File System (ou IPFS, système de fichier interplanétaire) est depuis longtemps le protocole P2P distribué plébiscité dans l'écosystème blockchain, accessible via FUSE ou à travers HTTP. Mais IPFS présente un défaut pour certains cas d'utilisation : le stockage n'est pas assuré dans le temps. C'est là qu'Arweave entre en jeu. Son principe est de récompenser les nœuds qui conservent les données de manière permanente, et ainsi réconcilie le meilleur des deux mondes. En l'occurrence, la populaire blockchain Solana est l'une des premières à avoir fait le choix d'Arweave pour le stockage de l'ensemble de sa chaîne, via le protocole KYVE.
La notion de permanence des données est donc cruciale pour les entreprises, mais aussi dans le Web3, notamment vis-à-vis des NFT. Rappelons qu'un jeton non-fongible est en fait « juste » un lien entre un jeton et son URI (Uniform Resource Identifier), permettant d'identifier le fichier contenant les métadonnées (les propriétés et le lien pointant vers le média). Ainsi, plusieurs projets NFT utilisant IPFS ont vu leur média associé (une image, un GIF, *etc.*) disparaître du jour au lendemain… d'où l'apparition du stockage permanent, et donc d'Arweave.

DU PC AUX PÉRIPHÉRIQUES

L'environnement de travail s'adapte à de nouveaux besoins

Les nécessités au moment de la pandémie et de sa sortie toujours repoussée ont remanié durablement les organisations du travail avec le télétravail ou de tout autre lieu susceptible d'accueillir les salariés et une connexion Wi-Fi. Plus discrètement, des impacts importants ont accompagné ce phénomène sur tous les matériels qui composent les espaces de travail, du PC aux écrans en passant par les souris, tous les périphériques ont connu d'importantes évolutions. Point sur les différentes tendances qui marquent ces changements.

Pas toujours simple de pouvoir proposer des conditions et des outils pour travailler de manière optimale lorsque le contexte fait que l'utilisateur n'aura pas forcément l'environnement adéquat pour bénéficier à plein de ce qui est proposé. Bande passante, réseau faible, espace de travail limité ou bruyant sont les problèmes le plus souvent rencontrés par les salariés confinés ou en télétravail.



Un exemple des nouvelles ergonomies des postes avec un Latitude 9430, très plat et permettant de multiples usages.

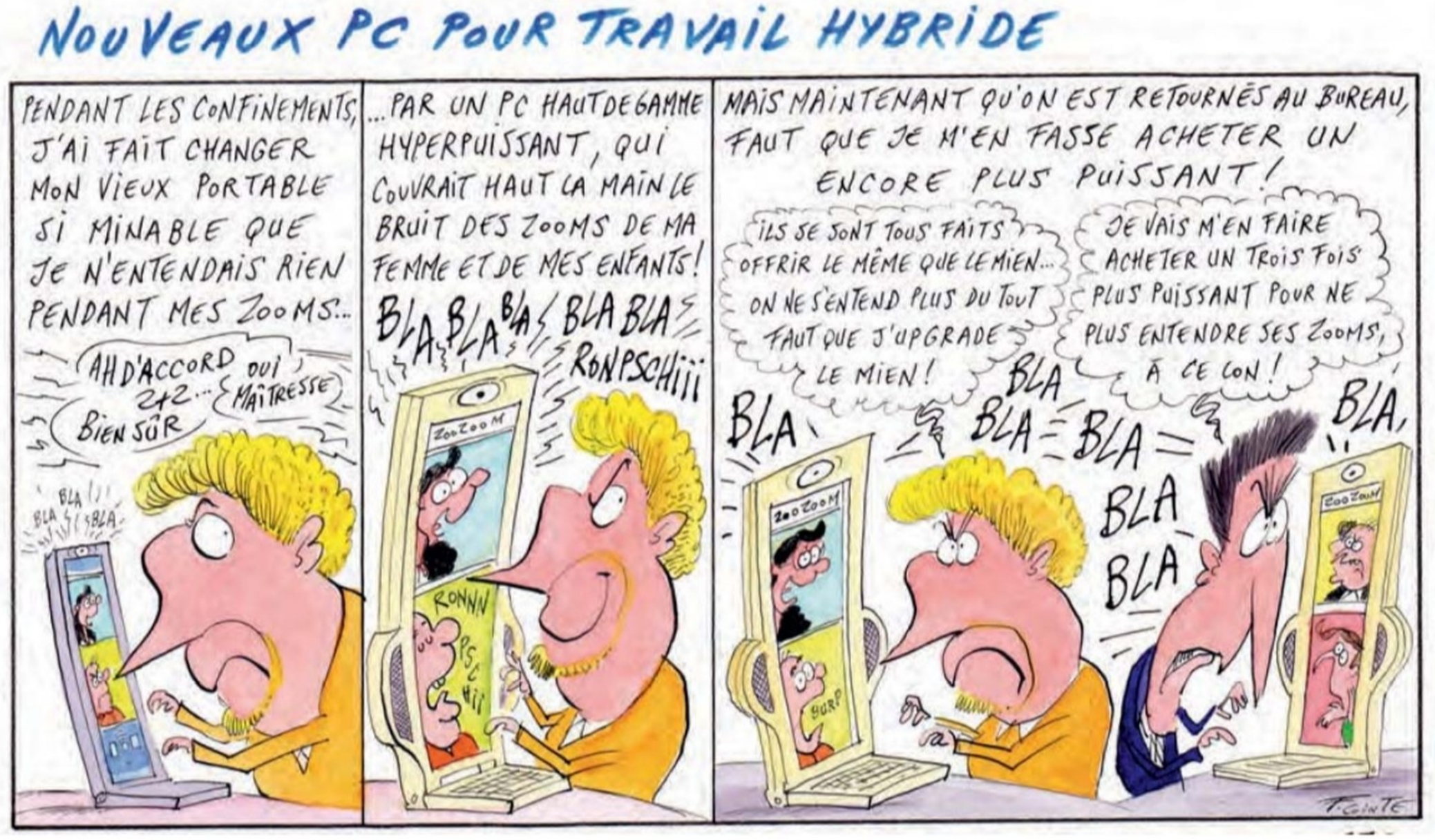
Les constructeurs de Hardware ont bien compris ces problèmes et ont adapté leurs produits pour répondre aux besoins des utilisateurs finaux. Performance, encombrement, simplicité d'utilisation et sécurité sont les principaux thèmes qui conduisent l'évolution des matériels qui composent les environnements de travail actuels.

Performance et autonomie

Kristel Delnesse, manager des chefs de produits postes clients chez Dell, constate : *« Les grands axes depuis trois ans, avec une accélération durant la pandémie ont été de faire des machines plus performantes et avec plus d'autonomie. La philosophie est de coller aux besoins des utilisateurs »*. Mustapha Nhari, DG d'Asus France, ajoute : *« Les utilisateurs sont moins patients et demandent toujours plus de performance pour obtenir des temps de réponse sur leurs actions les plus bas possibles. D'ailleurs, pour cela, tout le monde est passé aux disques SSD, on ne trouve plus beaucoup de disques durs mécaniques dans des appareils qui demandent à être plus que des tablettes ou des téléphones, lesquels ne suffisent pas pour les tâches demandées. »* Il continue : *« Cette puissance est aussi corrélée avec la mobilité »*.

La performance a aussi besoin d'être optimisée selon les usages ou les utilisateurs. Kristel Delnesse souligne : *« L'avenir du hardware c'est le software »*. *A priori* cela semble cryptique. Elle détaille ensuite les différents modules logiciels installés sur les postes comme Express Response qui analyse les applications utilisées ou les ressources allouées pour automatiquement voir les priorités de performance même si l'utilisateur ouvre une autre application. Il en est de même avec Express Connect qui va rechercher la borne de connexion la plus large mais aussi la plus stable.

Il en est de même pour l'autonomie. Un logiciel comme Dell Power Manager autorise l'utilisateur à gérer sa consommation pour obtenir une autonomie optimale.



Si des constructeurs annoncent 24 heures d'autonomie, la réalité tourne cependant aujourd'hui à la durée de la journée de travail de 8 heures, même connecté à Internet ou en utilisant des applications gourmandes. De même, Express Charge permet de recharger la batterie à 80 % en une heure.

Il faut y ajouter les nouvelles générations de processeurs, que ce soit chez Intel ou AMD, dans les améliorations des performances des portables.

De plus, la plupart des périphériques, comme les écrans, embarquent de plus des ports USB-C qui en « pass through » facilite la recharge des équipements reliés dont les postes de travail comme les laptops. Miguel Limones, responsable Category Manager chez Fujitsu France, précise : *« Comparativement aux générations précédentes, nous intégrons maintenant les batteries 65 Watts qui apportent plus d'autonomie, quasiment deux heures, sans alourdir les machines. On prévoit d'arriver à onze ou douze heures dans les prochaines générations »*.

Kristel Delnesse, manager des chefs de produits postes clients chez Dell.



« Beaucoup d'éléments visent à simplifier la vie de l'utilisateur et à lui rendre la machine agréable. »

Rendre l'utilisation simple

Tous les salariés ne sont pas des informaticiens et ils n'ont pas forcément une culture étendue sur les branchements, déploiements ou utilisation des matériels mis à leur disposition. La simplicité et l'ergonomie des équipements sont donc indispensables si l'on veut conserver le niveau de productivité des utilisateurs. Kristel Delnesse précise : *« Beaucoup d'éléments visent à simplifier la vie de l'utilisateur et à lui rendre la machine agréable »*.

L'automatisation de certaines fonctions entrent aussi dans cette catégorie de la simplification des usages. Autre élément déterminant pour le déploiement des environnements de travail, le sans-fil, Bluetooth principalement, se généralise pour ne pas avoir à brancher. Les réplicateurs USB-C autorisent le branchement de plusieurs matériels externes tout en alimentant les matériels depuis une seule source de courant.

L'expérience utilisateur = confort et bien-être

Un autre axe de progrès sur les matériels dans les environnements de travail concerne tout ce qui peut rendre confortable l'utilisation ou le bien-être de

l'utilisateur. Dell a ainsi mis en place sur ses matériels la fonction ConfortView + qui atténue la lumière bleue nocive sans jaunir les écrans pour plus de confort visuel. Le tactile s'impose peu à peu. Sur les ordinateurs portables, les écrans migrent du 16/9 au 16/10 pour apporter une vision plus large. De plus, ils se réduisent. Kristel Delnesse, mais aussi les autres personnes interrogées lors de cette enquête, ont noté que le 13 ou 14 pouces devient le standard devant le 15 pouces habituel. Qu'il soit externe ou intégré, les machines intègrent de plus en plus un pavé numérique bien utile pour certaines tâches. Sur certains modèles, Asus le propose en pavé virtuel. Il en est de même avec les équipements Audio devenu indispensables avec l'utilisation massive des logiciels de communication ou de collaboration durant la pandémie. L'annulation de bruit est devenue une fonction recherchée. Orosound est une jeune entreprise française qui s'est spécialisée dans ce domaine et ses casques embarquent cette fonction par des algorithmes directement sur ses produits. Il est aussi possible de moduler cette fonction par une molette.

Les écrans des équipements s'améliorent avec quasiment partout du Full HD. Mustapha Nhari indique : *« Les utilisateurs évoluent entre plusieurs usages professionnels et personnels. Les demandes s'orientent vers le full HD, grand angle et cela va continuer à évoluer vers le 4K et au-delà du fait de l'utilisation de plus en plus massive des réunions virtuelles »*.

Les souris connaissent aussi de véritables progrès en ce sens au-delà des touches programmables. Des souris verticales remplissent un office intéressant en travaillant une ergonomie verticale pour éviter les problèmes du canal carpien du fait d'une utilisation intensive.

La réduction de la taille des portables se conjugue avec une réduction de poids avec des ergonomies différentes. Miguel Limones précise : *« Nous avons commencé avec nos différentes gammes à mettre le clavier sur les bords afin de réduire l'encombrement en largeur et en profondeur. Le poids est aussi déterminant. Nous sommes de toute façon dans une semi-mobilité même pour les sédentaires. Ainsi, sur les 14 pouces nous arrivons aujourd'hui à 1,5 kilo et en dessous avec 1,2 kilo pour certains modèles destinés à l'ultra-mobilité. »*

La maintenance des matériels devient aussi plus simple et facile avec moins de vis et des éléments encastrables comme les claviers, ce qui simplifie leur remplacement en cas de besoin. Il en est de même pour le remplacement des batteries et même de composants primordiaux comme la carte-mère ou le processeur.

Du fait des multiples déplacements des utilisateurs, les postes se durcissent et se veulent plus résistants aux chocs. Par exemple, Fujitsu travaille sur des coques en magnésium avec des renforts sur les bords. Résultat : les postes sont résistants, mais restent légers selon Miguel Limones.

Miguel Limones, responsable Category Manager chez Fujitsu France.



« Comparativement aux générations précédentes nous intégrons maintenant les batteries 65 Watts qui apportent plus d'autonomie. »

La sécurité s'installe sur les postes

Miguel Limones met en avant les ajouts autour de la sécurité sur les machines, que ce soit directement par le processeur, comme le TPM dans les équipements recevant Windows 11, ou le service VPro chez Intel, ou sur des lecteurs intégrés comme les lecteurs d'empreintes digitales, mais aussi des lecteurs de paumes ou de veines de la main. S'y ajoute les filtres de confidentialité afin que l'écran ne soit pas vu par d'autres personnes que l'utilisateur.

Chez Dell, un verrouillage automatique permet de quitter son poste de travail sans avoir à s'inquiéter de qui regarde ce que vous faites. Dans les modèles de portables Latitude haut de gamme, une fonction ferme la caméra embarquée par une touche sur le clavier.

Des efforts environnementaux

Suivant les tendances du marché et pour remplir leurs objectifs ESG (données environnementales, sociales et de gouvernance) les fournisseurs de matériels essaient d'oublier les errances passées d'obsolescence programmée et d'utilisation de produits nocifs ou difficiles à recycler. Kristel Delnesse rappelle le nouveau concept Luna chez Dell qui vise à créer un ordinateur portable véritablement durable, évolutif, réparable et recyclable, en tenant compte de l'ensemble de sa durée de vie lors de son développement. Le résultat final est un ordinateur portable dont l'empreinte carbone a été réduite de 50 %. Dell et Intel ont réussi à atteindre cet objectif grâce à des éléments de conception tels qu'une carte mère 75 % plus petite. Ce concept s'applique à toute la chaîne de fabrication de la conception à la livraison du produit avec des emballages en carton recyclé.

Miguel Limones ajoute : *« Nos éléments les plus compacts sont consciemment dans cette tendance durable en utilisant moins de matériaux »*. □

B.G

TANIUM

2021 PALMARÈS L'INFORMATICIEN

The Power of Certainty

Les organisations IT font face à de multiples défis : des environnements de plus en plus étendus et changeants, une actualité sécurité oppressante, un manque de ressources IT, et une gestion quotidienne complexe.

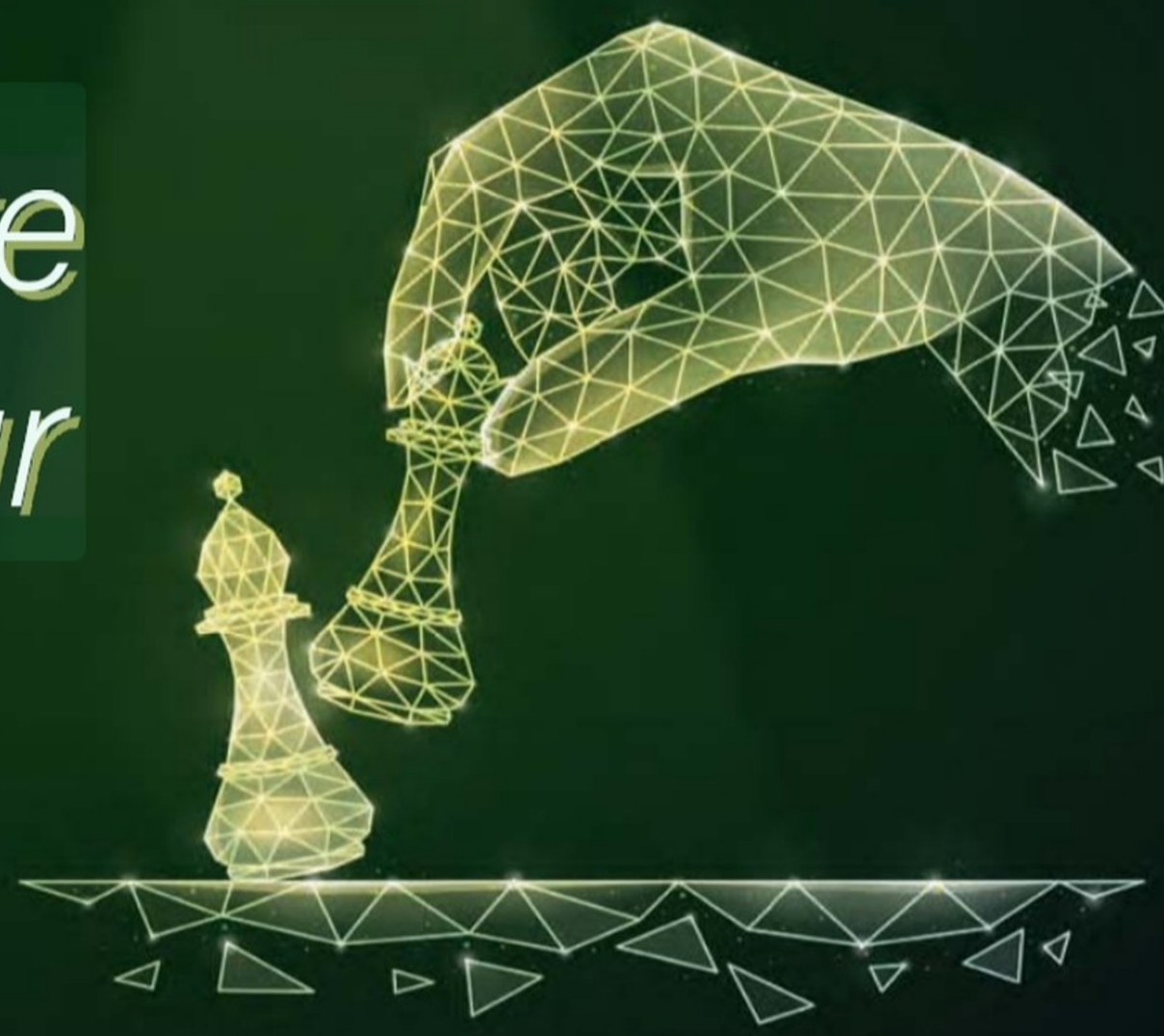
Avec Tanium, ayez connaissance de tout ce qui se passe sur l'ensemble de vos endpoints, afin d'anticiper les problèmes ou de les résoudre rapidement lorsqu'ils se produisent.

tanium.com/fr



© Tanium 2022

La dictature du bonheur



par Bertrand Garé

Depuis quelques années, l'entreprise s'est emparée d'un espace qui était jusqu'à présent dévolu au domaine politique ou aux gouvernements : le bonheur ! Cela a commencé par une période gadget avec sucreries et tables de ping-pong à volonté dans des espaces non plus remplis de bureaux et d'écrans mais de poufs, de canapés et d'autres impedimenta voulant prouver le côté « cool » de l'entreprise. Bon, tout cela commençait cependant à partir en vrille, il a donc fallu nommer une personne en charge de gérer ce nouveau bazar, le CHO ou Chief Hapiness Officer.

Bon, si beaucoup raillent cette fonction, il en est quelques-unes qui le font sans le « bullshit » associé au bonheur des salariés dans l'entreprise. Ils sont plutôt là pour rendre plus simple l'intégration de nouveaux salariés et du développement de la « marque employeur », le marketing des ressources humaines dans le but d'attirer des talents, recrues rares et de leur apporter un cadre où ils se sentent dans de bonnes conditions pour faire leur travail.

Tout cela n'est pas fait pour rien. Comme le capitalisme sauvage avait découvert au XIXe siècle qu'un travailleur en bonne santé apportait plus à l'entreprise qu'un pauvre souffreteux, les entreprises sont maintenant conscientes qu'un salarié en pleine possession de ses moyens et heureux dans son travail est moins malade, moins absent, plus productif qu'un salarié en « burn-out » ou « désengagé ». Plusieurs études récentes démontrent d'ailleurs un lien entre « l'épanouissement » du salarié et la performance économique de l'entreprise.

Devant la pénurie de « talents » et la course au recrutement, la mariée se veut belle et engageante et revient aux bonnes vieilles recettes des entrepreneurs pour apporter plus de productivité. Ce n'est pas le seul élément à prendre en compte. La pénurie a retourné le rapport de force entre les entreprises et les salariés. Les salariés ont un peu le choix et les métiers porteurs comme l'informatique voit une vague de démission ou de course à un meilleur poste de grande ampleur avec souvent à la clé, pour le salarié, une augmentation de son salaire et des perspectives d'évolution.

Jamais la « recherche de sens » et « l'épanouissement personnel » n'ont été autant mis en avant dans les entreprises. Entre les cours de yoga et les heures de méditation, des entreprises vont un peu plus loin avec un intérêt pour l'expérience du salarié dans l'entreprise afin de lui apporter ce dont il a besoin pour optimiser son travail et son confort dans la réalisation de celui-ci. Ce joli tableau a cependant pas mal de revers. Ainsi, la pandémie a déjà rapidement fait tomber les frontières ente vie personnelle et vie professionnelle. Le fait que plus que dans sa vie personnelle, le salarié connaisse son épanouissement dans l'entreprise accentue encore ce phénomène. Mais cela est antinomique avec ce qu'expriment les salariés eux-mêmes : plus d'autonomie, de sens et de compréhension dans les tâches qu'ils doivent effectuer. En quoi ce travail contribue-t-il à la réussite de l'entreprise, du salarié… Bref, quel est le but de mon travail quotidien à défaut de me voir seulement comme un rouage dans la matrice ?

De l'armée à la secte ?

Tout ce changement s'est accompagné d'un changement dans le « management » et du modèle sur lequel se construit l'entreprise. Jusqu'à présent, le système était assez pyramidal avec des « N+x » sur plusieurs couches assez comparables avec ce que l'on retrouve dans la chaîne de commandement d'une armée. Du grand stratège au piéton de base. D'ailleurs, on parlait de ressources même si cela était des

êtres humains. Cela faisait moins ancillaire que la gestion du personnel, mais cela semblait tout de même faire peu de cas des employés qui se comparaient ainsi à des cartouches d'imprimantes ou autres ressources nécessaires au fonctionnement de l'entreprise. Cette notion change aujourd'hui avec le déploiement d'une organisation plus horizontale ou en râteau. De ressources, le salarié devient un « asset », un actif dans tous les sens du terme. Car comme il est valorisé comme un actif, il se doit de l'être et aussi de s'engager dans le but et la structure de l'entreprise. Il se doit de montrer qu'il est un bon équipier ou un leader, un coach quand il est aux commandes d'une équipe de salariés. Il doit le montrer tous les jours sans connaître de mauvais jours, de saute d'humeur et bien suivre la ligne blanche s'il ne veut pas faire ostraciser comme *« l'empêcheur de tourner en rond »* ou de se faire qualifier au mieux de « talentueux mais ingérable ».

Sur le site d'un éditeur spécialisé dans l'engagement des salariés, celui-ci est défini comme suit : *« Un état de fonctionnement dans une organisation, dans lequel les employés sont motivés pour contribuer au succès de l'entreprise. Ils donnent le meilleur d'eux-mêmes et font des efforts supplémentaires afin d'atteindre leurs objectifs »*. Sic.

Comme les légionnaires romains dans Asterix, le « engagez-vous, rengagez-vous » a des beaux jours devant lui et c'est là que le modèle mis en place glisse vers des comportements proches de ceux des sectes. La quête du bonheur se joue sur fond d'une sorte de séduction et de réconfort face à une situation ou une réalité plus ou moins douloureuse. La deuxième est un processus identificatoire au but, à l'image, aux comportements demandés dans l'entreprise avec une idéalisation de celle-ci et de sa « mission ». Suit ensuite un processus de socialisation différent de ceux habituels.

Mais cela entre en confrontation avec la persistance du modèle « armé » qui de manière sous-jacente existe toujours. Donc, entre illusion du bonheur apporté et modèles ayant assez peu évolué, on retrouve une entreprise qui oscille de l'un à l'autre suivant les circonstances. Les conséquences peuvent être graves.

Une enquête Opinion Way du dernier trimestre de l'année dernière affirme que plus de trois salariés sur 10 sont en « détresse psychologique », comprenez burn-out. Cela touche toutes les couches de salariés dont les managers qui, à 18 %, seraient dans cette situation. 20% de l'ensemble des salariés ayant répondu à l'enquête ont déjà été en arrêt maladie pour des raisons psychologiques et un tiers sont en dépression et sous traitement médical. Et la situation est en passe d'empirer dans les mois à venir.

L'étude explique le phénomène par *« des amplitudes horaires très importantes pendant le télétravail imposé, des difficultés aussi à différencier la vie professionnelle et la vie personnelle d'un point de vue psychologique »*. *« Les salariés pâtissent d'un manque de repères avec le travail à distance et expérimentent surtout une perte de sens, avec un décalage croissant entre leurs attentes et ce que propose leur entreprise »* est le leitmotiv de ce sondage.

Avouez que tout cela est loin de votre image du bonheur ni du « management bienveillant » dont on nous rebat les oreilles. Il est surtout le moyen le plus sûr de mettre sous le tapis la gestion des conflits inévitables dans tout environnement social sauf quand il est trop tard. Mais il ne faut pas fâcher les talents, sauf quand vous n'en avez plus besoin. □

B.G



« Comment déployer la technologie
et transformer la société pour créer
le meilleur avenir possible ? »

Ayana Elizabeth Johnson, Ph.D.
Biologiste marine et experte en politique océanique



Quand la technologie rend le progrès possible, ESET est là pour le protéger.

eset.com/fr/progress

eset®
Digital Security
Progress. Protected.

Un nouveau modèle économique

GreenLake : Toute l'IT peut-elle basculer en mode « As a Service » ?

La vente des équipements informatiques va-t-elle changer de modèle comme pour le logiciel qui a basculé vers le SaaS ? L'essor du « Hardware as a Service » et de l'approche GreenLake accélère et HPE pousse aujourd'hui le concept à son paroxysme.

Souscrire à des serveurs, des switchs, des balises Wi-Fi ou des baies de stockage comme on lance à la demande un service AWS ou Microsoft Azure, c'est la promesse du *« Hardware as a Service »*. Bien évidemment, l'instantanéité du Cloud n'est pas tout à fait au rendez-vous, il faut bien livrer et installer les équipements, mais la promesse de basculer ces investissements en frais d'exploitation est tenue. De quoi faire saliver les DAF des grandes entreprises qui veulent rendre les comptes de leur entreprise plus séduisants aux yeux des investisseurs mais le DSI y trouve aussi son compte. Dans certaines limites, ces infrastructures « as a Service » offrent une certaine flexibilité et peuvent accompagner une montée ou une descente en charge.



Avec GreenLake Central, HPE a mis en ligne une console de gestion de l'ensemble des ressources IT de l'entreprise, que celles-ci soient en on-premise « classique », des ressources GreenLake en mode As a Service, mais aussi des ressources consommées dans le Cloud public avec un pilotage par leurs API.

Pour toutes ces raisons, le modèle *« Hardware as a Service »* est en plein boum. Selon le cabinet d'études Persistance Market Research, celui-ci connaîtra une croissance annuelle totalement extravagante de +28.5% par an entre 2021-2031 ! *De facto*, de plus en plus d'équipements informatiques basculent dans ce mode locatif. C'est le cas des PC, des serveurs, des équipements réseaux, des SAN, mais aussi d'équipements plus annexes comme les téléphones et autres équipements de visioconférence. En juillet 2020, Zoom proposait l'offre Zoom Hardware as a Service afin de proposer ses Zoom Phone et Zoom Rooms en mode « as a Service » …

HPE passe à une nouvelle étape de sa stratégie GreenLake

Parmi les pionniers de l'approche HaaS, HPE a lancé ses premières offres Flexible Capacity il y a maintenant 5 ans. Charles Henry, Directeur de la division Transformation, Solutions et Services Cloud d'HPE France explique la démarche : *« Il ne s'agissait encore que de solutions de type « Hardware as a service », avec différents mécanismes qui permettaient de moduler le cash flow. Ce qui allait devenir GreenLake intégrait une réserve capacitaire que le client ne payait pas tant que celle-ci n'était pas consommée. La facturation à l'usage s'appuyait sur une métrologie et un Capacity Planning automatisés avec l'outil Cloud Cruiser que nous avons acquis en 2017. »* Depuis, l'Américain a été rejoint par de nombreux constructeurs, au premier rang desquels Cisco avec son offre Cisco+, ainsi que Dell, Lenovo et bien évidemment IBM dont les principes de location et de réserve capacitaire remontent à l'ère des mainframes !

Il y a trois ans, HPE a très largement élargi le portefeuille de ses offres GreenLake et vient de frapper un grand coup au premier trimestre 2022 en dévoilant pas moins de 12 nouveaux services Cloud. Son portefeuille GreenLake compte

plus de 50 offres et va bien au-delà des seules solutions *« Hardware as a Service »*. L'Américain propose des offres de partenaires de type Azure Stack HCI avec Microsoft, des solutions de Nutanix, Scality, Veeam, *etc.* Un troisième type de service porte sur des solutions complètes dédiées à un type de besoin. C'est par exemple l'offre MLOps, ou encore de la version 2 de l'offre HPC qui inclut des API de connexion multi-Cloud qui permet de faire très simplement du débordement auprès des hyper-scalers. Le quatrième étage de l'offre GreenLake HPE est constitué des Cloud Services, des services sur étagère qui sont commercialisés sous forme de souscription. HPE vient d'annoncer un service de Stockage en mode bloc et une offre de « Backup & Recovery » hybride.



Louer une VM chez HPE plutôt que chez AWS ou Azure, c'est possible ! L'offre GreenLake correspondante s'appuie sur des configurations HPE Synergy embarquant HPE Primera ou HPE Nimble Storage.

Si HPE vise les grandes entreprises qui peuvent se laisser tenter par ces grandes offres packagées, le midmarket et les PME sont tout autant dans le viseur de l'Américain. Ces dernières opteront sans doute pour les ressources *« Hardware as a Service »* pour remplacer leurs serveurs ou leurs équipements réseau.

HPE veut faire converger toutes les ressources IT sur sa console

À la manière de la console d'un hyper-scaler depuis laquelle on accède à tous les services, HPE veut proposer une interface unifiée pour gérer l'ensemble des 50 services GreenLake.

CHARLES HENRY, DIRECTEUR DE LA DIVISION TRANSFORMATION, SOLUTIONS ET SERVICES CLOUD CHEZ HPE FRANCE



« Pour HPE, GreenLake constitue une transformation majeure de notre business interne, la manière dont sont rémunérées les forces commerciales, à travers la manière dont nous gérons nos partenaires. Il s'agit d'une réelle transformation d'entreprise et je pense que nos concurrents accusent un gros retard sur nous. Nous avons commencé cette transformation beaucoup plus tôt, nous sommes plus matures et c'est ce qui explique aujourd'hui la très forte croissance que nous connaissons actuellement sur ce modèle, même si le modèle traditionnel reste encore très important. »

Celle-ci a été construite sur le code d'Aruba Central, plateforme qui compte environ 2 millions de devices gérés pour 120 000 clients. *« Nous avons construit une plateforme Cloud commune pour gérer l'ensemble des services GreenLake »* détaille Charles Henry. *« L'entreprise dispose de la visibilité de l'ensemble de ses devices, de son infrastructure serveur, stockage et réseau. Une authentification unique donne accès à l'ensemble des services provisionnés, y compris sur les Cloud publics. »* Un autre point-clé dans la réussite d'une telle approche est de convaincre les partenaires et distributeurs de la pertinence de ce changement de paradigme car une bonne partie du chiffre d'affaires d'HPE est réalisée en indirect. HPE mise là encore sur l'approche plateforme et donne les moyens à ses partenaires de piloter les infrastructures de leur client depuis sa console. De même, le constructeur peut compter sur des partenaires Service Providers qui s'appuient sur GreenLake pour délivrer leurs services à leurs propres clients. C'est notamment le cas de Cheops Technology en France.

Au premier trimestre 2022, HPE affichait une croissance de 136% de ses offres GreenLake, soit 6,5 milliards de dollars de contrats pour 1 400 clients et 900 partenaires signés. Ces chiffres sont à comparer aux 2% de croissance et 7 milliards de dollars de chiffre d'affaires d'HPE sur la période. Le responsable des services Cloud précise : *« En France, le chiffre d'affaires a été doublé sur ces six derniers mois de même que nous avons doublé le nombre de références clients. Le marché est prêt à basculer et il y a eu une prise de conscience des entreprises les plus matures qui sont engagées dans des stratégies multiclouds qu'elles n'iront pas jusqu'au bout. Elles auront toujours des infrastructures on-premise et doivent se doter d'un modèle opérationnel hybride qui englobera des ressources du cloud public, mais aussi des ressources Cloud privées. »* HPE espère bien pouvoir placer sa plateforme GreenLake en tant que système d'exploitation de cette infrastructure hybride et, par la même occasion, continuer à livrer ses équipements dans les datacenters de ses clients. □

A.C

Mainframe

Z16 : le nouveau monstre d'IBM

IBM a annoncé début avril un nouveau mainframe, le Z16, qui offre une configuration et des performances hors normes.

Les mainframes sont régulièrement sur des configurations musclées. Ainsi, en 2003, IBM avait sorti une machine dont le nom de code était T-Rex tirant parti des performances et de la vélocité de la machine. Il semblerait qu'il n'existe pas de noms de bestiole de l'ère tertiaire pour qualifier le dernier d'IBM, le Z16.

Ce mainframe est conçu pour les très grandes entreprises en environnement hybride comme les banques, les assurances ou toutes celles qui doivent traiter des données en temps réel. Lors de la présentation, IBM a insisté sur les différentes applications de la machine comme la détection de la fraude à la carte bancaire. IBM indique ainsi que la machine est capable de traiter 300 milliards de requêtes d'inférence avec moins d'une milliseconde de latence par jour. La puissance de la machine peut aussi être utile dans d'autres usages comme la revue de prêts, la gestion des risques...

Une bête de course

Le serveur s'appuie sur les processeurs Telum et différents accélérateurs. Chaque module embarque un de ces processeurs de 16 cœurs gravés en 7nm à une fréquence de 5,2 GHz. La machine peut se décliner en différentes versions selon les besoins en nombre de cœurs. Elle embarque, de plus, jusqu'à 40 To de Redundant Array of Independent Memory (RAIM). Un coprocesseur pour les applications d'intelligence artificielle est directement placé sur la puce. Tout un jeu entre les différents niveaux de cache accélère encore les performances. La connectivité est pensée pour partager les communications entre les mémoires qui sont partagées. Sur la génération précédente, le Z16 apporte des performances améliorées de facteur 20 à 30 mais surtout apporte une meilleure consistance et précision sur les résultats des opérations d'intelligence artificielle.

Une sécurité post-quantique

IBM présente ce mainframe comme la première machine avec une sécurité post-quantique. Ainsi, la machine repose sur un chiffrement en treillis, une nouvelle approche pour construire une sécurité originale afin de protéger les données et les systèmes contre les attaques actuelles, mais aussi celles du futur. Le boot ou démarrage est sécurisé pour éviter une injection de malware durant ce processus. Le Z16 inclut un module de sécurité hardware, Crypto Express 8S (CEX8S), qui offre des technologies de chiffrement classiques et quantiques pour protéger la confidentialité des données. La machine sera en disponibilité générale à la fin du mois de mai.



Une vue de face du nouveau monstre d'IBM, le Z16.

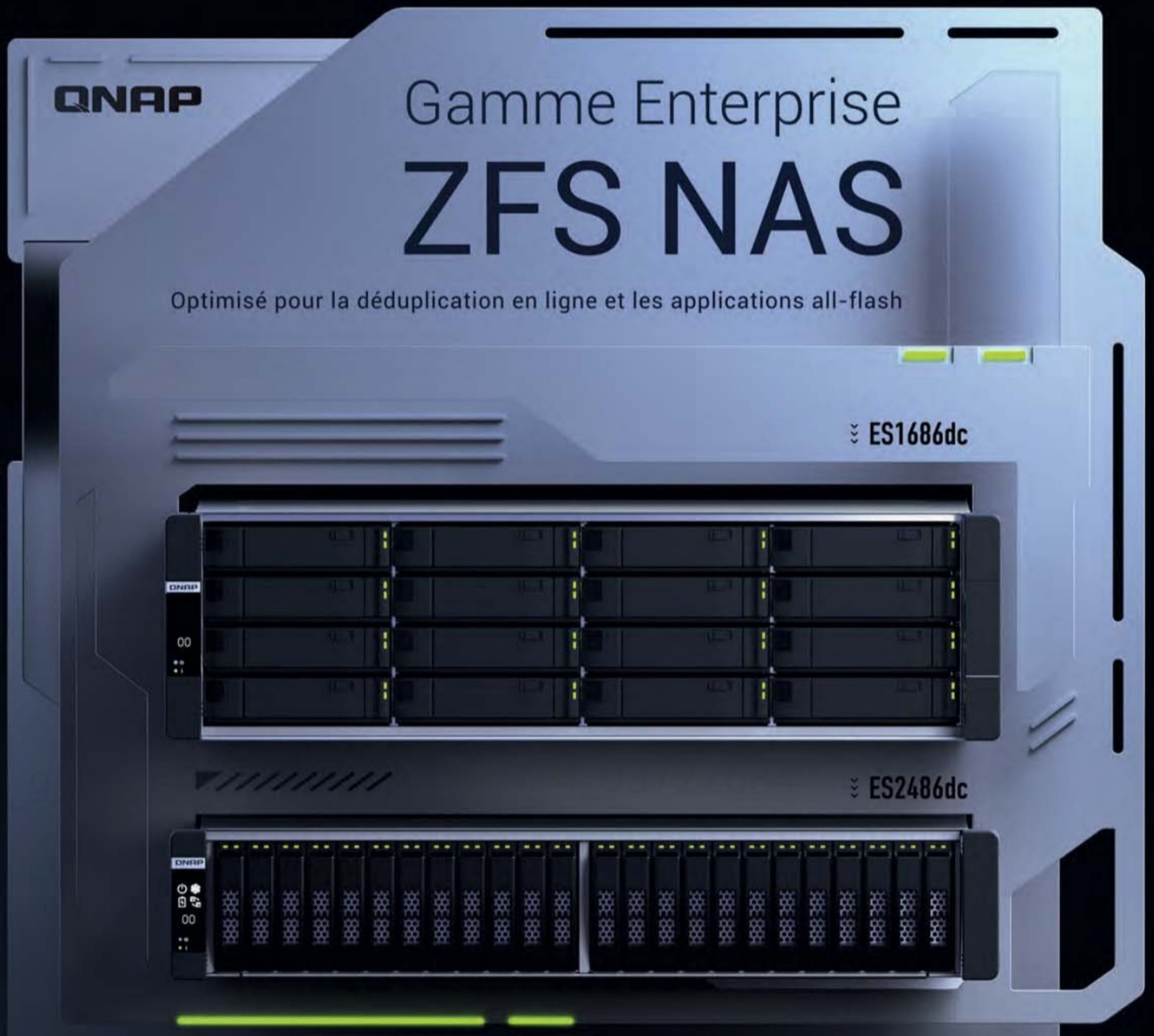
À l'analyse, une fois de plus, IBM réussit le pari de relancer le mainframe sur de nouvelles approches plus proches des problématiques de ces grands clients comme la détection de la fraude dans les institutions financières ou les entreprises nécessitant des calculs sur des données en temps réel pour leur activité. Cela va donc concerner qu'un faible nombre d'entreprises souvent déjà clientes de Bigblue. Par ailleurs, IBM positionne la machine pour les environnements hybrides, l'architecture devenue de fait l'architecture moderne des grandes entreprises avec des capacités flexibles et un mode de facturation qui se rénove régulièrement pour que le mainframe maintienne ses positions mais pas forcément une ligne de business d'avenir. □

B.G

QNAP

Gamme Enterprise
ZFS NAS

Optimisé pour la déduplication en ligne et les applications all-flash



Réplication à distance haute performance

Reprenez rapidement les services essentiels en cas d'arrêt imprévus en utilisant des snapshots quasi illimités et SnapSync pour la sauvegarde à distance des snapshots.

Capacités d'E/S exceptionnelles avec l'extension PCIe

L'extensibilité PCIe permet d'utiliser des adaptateurs 10GbE/25GbE/40GbE pour augmenter les performances des applications.

Modules NVRAM pour des performances de niveau entreprise

La protection des données en écriture DRAM en cache et l'accélération de la lecture Flash offrent des performances d'accès aléatoire à la pointe de l'industrie.

Haute disponibilité avec les processeurs Intel® Xeon® D

Les processeurs Intel® Xeon® D sont dotés d'une architecture à double contrôleur actif-actif pour assurer la continuité des activités et offrir aux entreprises une haute disponibilité avec des temps d'arrêt quasi nuls.

QNAP SYSTEMS, INC.
Copyright © 2021 QNAP Systems, Inc. All rights reserved.

www.qnap.c
frsales@qnap.com

Puces graphiques

GPU : Intel tente de revenir dans le « game »

Que ce soit pour jouer ou faire de la conception 3D, des calculs de simulation ou de l'apprentissage machine, le choix est clair : c'est soit un GPU NVidia, soit un AMD. Un duopole qu'Intel n'arrive pas à briser depuis plusieurs décennies. Les GPU Intel Arc parviendront-ils à faire mieux ? Pas si sûr !

Les derniers chiffres publiés par Jon Peddie Research sont sans appel : Intel a livré au quatrième trimestre 2021, 62% de l'ensemble des GPU vendus, contre 19% pour NVidia et autant pour AMD. Intel domine largement le marché en nombre de puces, mais le hic, c'est qu'il s'agit essentiellement de composant de type intégré, les iGPU. Il s'agit des puces Intel HD Graphics et Iris Xe que l'on trouve par défaut dans bon nombre de desktop et autres portables. Sur le marché des puces de grande puissance, les dGPU (discrete GPU), AMD détient 19% des parts de marché, NVidia en glane 81% ! Intel est littéralement absent du marché le plus lucratif, un marché où la demande excède largement l'offre comme en témoignent les prix très élevés des composants qui évoluent en fonction des livraisons des fondeurs.



Après les Arc 3 d'entrée de gamme pour les laptops, Intel veut lancer des modèles plus puissants, les Arc séries 5 et 7 qui seront disponibles sous forme de cartes PCIe.

Le constat d'échec des multi-cœurs x86

Intel n'a pas laissé ce duopole s'installer sans étudier de son côté des GPU puissants. On se souvient notamment du projet Larrabee annoncé en 2008 et ce pari un peu fou d'Intel d'implémenter des cœurs x86 dans un GPU. L'idée est de disposer d'un maximum de cœurs x86 sur la puce et dédier ces cœurs au rôle de CPU ou de GPU en fonction du besoin de la charge demandée. Une brillante idée qui n'a jamais pu aller jusqu'à la commercialisation à grande échelle. En 2010/2011, apparaissait Knights Ferry, une grosse puce (684 mm^2) gravée en 45 nm offrant 32 cœurs x86. On commençait à parler de ray tracing temps réel, de la science-fiction à l'époque ! Des versions 64 cœurs et même 80 cœurs sont alors évoquées, mais Intel n'ira pas jusqu'à la commercialisation. Néanmoins, la lignée Larrabee et son architecture « Many Integrated Core » a connu un ultime rejeton avec le Knights Corner, une puce que l'on va retrouver dans les cartes Xeon Phi, commercialisée en 2012. Intel a alors renoncé à renverser le marché des GPU avec ses cœurs x86 : le Xeon Phi se destinant exclusivement au marché HPC.

Intel repart à l'assaut avec l'architecture Xe-HPG

L'approche « Many Integrated Core » s'étant révélée une impasse, Intel a dû revoir sa copie. Lors de l'Architecture Day 2020, Intel avait détaillé sa stratégie Xe pour disposer d'une gamme complète de GPU qui devait répondre à tous les besoins du marché, depuis l'iGPU de base jusqu'à la puce de force puissance destinée au marché HPC, en passant par des composants destinés aux gamers ou encore des puces plus spécifiquement dédiées aux datacenters et à l'accélération IA. Gravés en 10 nm, ses composants devaient submerger le marché en 2021… on attend encore les cartes

4_93722684



L'architecture Xe-HPG qui anime les puces Intel Arc se décompose en un nombre variable de Slice, selon le modèle. Ces structures contiennent les cœurs de rendu/IA et de ray tracing. Le volet codage/décodage des médias est assuré séparément, par les unités MFX.

Intel Xe-HPG (High Performance Gaming) sensées rivaliser avec les GeForce RTX 3070 ou 3090 de NVidia… Aujourd'hui rebrandée Intel Arc, la microarchitecture Xe-HPG semble enfin s'approcher de la commercialisation.

Le lancement officiel fut réalisé virtuellement le 30 mars dernier, avec la présentation des puces Arc 3, une gamme dédiée aux laptops. Roger Chandler, Vice Président et General Manager en charge des produits graphiques et Gaming d'Intel a souligné : *« Arc 3 représente une nouvelle étape dans notre voyage. Il vient doubler la puissance des Intel Irix Xe pour un même encombrement. Les premiers laptops Arc 3 sont disponibles et seront suivis par les modèles Arc 5 et Arc 7 cet été. »* Intel a annoncé la disponibilité immédiate de 2 composants, les A350M et A370M, avec 6 et 8 cœurs graphiques et 6/8 unités de raytracing pour 4 Go de ram GDDR6. Avec les séries 5 et 7, le nombre de cœurs grimpe à 16 pour Arc 5 et à 24/32 pour Arc 7. Ces modèles plus puissants seront disponibles au format PCIe : ils seront en concurrence frontale avec NVidia et AMD.

Ces 3 gammes s'appuient sur la même microarchitecture Xe-HPG qui a été conçue dès le départ pour les gamers et les créateurs de contenu. Celle-ci intègre des cœurs graphiques et les cœurs IA baptisés XMX. Ceux-ci accélèrent les workloads IA mais aussi la fonction d'upscaling XeSS (Xe SuperSampling) que met en avant Intel auprès des gamers. Un nouveau moteur de médias supportant la 8K mais aussi une accélération hardware du codec AV1 de l'Alliance for Open Media. Celui-ci est annoncé par ses concepteurs comme 50% plus efficace que le H.264 et 20% de plus que HEVC. Roger Chandler a ajouté : *« Toutes les puces Intel Arc supportent DirectX 12 Ultimate, dont l'accélération hardware du raytracing. Couplé aux coprocesseurs Intel de 12ième génération, Intel Arc aura des capacités d'écriture directe de données dans le stockage. »* Intel Arc est désormais intégré avec l'Evo Design, la plateforme matérielle poussée par Intel auprès des constructeurs de portables.

Des premiers benchmarks plutôt décevants…

Officiellement, Intel vise les professionnels de la création de contenus et les gamers, mais avec ces premiers composants, il sera difficile de séduire les « hardcore gamers ». Le premier Laptop disponible est le Samsung Galaxy Book2 Pro et les premiers benchmarks ne sont guère flatteurs pour l'Intel Arc A350M qui l'équipe. Le 3DMark classe le GPU sous une GTX 1650 de 2019… En outre, un Intel Arc A770, le haut de gamme Intel Arc a pu être évalué sous OpenCL et les résultats ne sont pas transcendants ; le Geekbench le place au niveau d'une GeForce RTX 2070 de Nvidia, soit le modèle de moyenne gamme NVidia avec une génération de retard…

Pire, une semaine seulement après le lancement officiel, un tweet du support Intel révélait que le lancement des premier laptops Intel Arc était décalé au second trimestre 2022, sans autre explication. La disponibilité effective des Intel Arc 3 est donc pour l'instant incertaine, quant à celle des Arc 5 et 7, initialement annoncés pour cet été, elle devient très hypothétique.

À force de retards et de performances en retrait, Intel risque de se retrouver à jouer en deuxième division alors qu'une nouvelle menace point à l'horizon : le chinois Moore Threads vient de dévoiler la MTT S2000, un GPU de 12 TFLOPS, soit pratiquement déjà au niveau de l'Intel Arc 7… □

A.C



Intel mise sur la fonction XMX de son Intel Arc pour accélérer les inférences de modèles d'IA. L'américain assure être en contact avec les éditeurs d'Adobe Premiere Pro, Video Enhance AI de TopazLabs et Gigapixel Ai pour le support de cette accélération matérielle.

Expérience utilisateur

Juniper étend le LAN au WAN

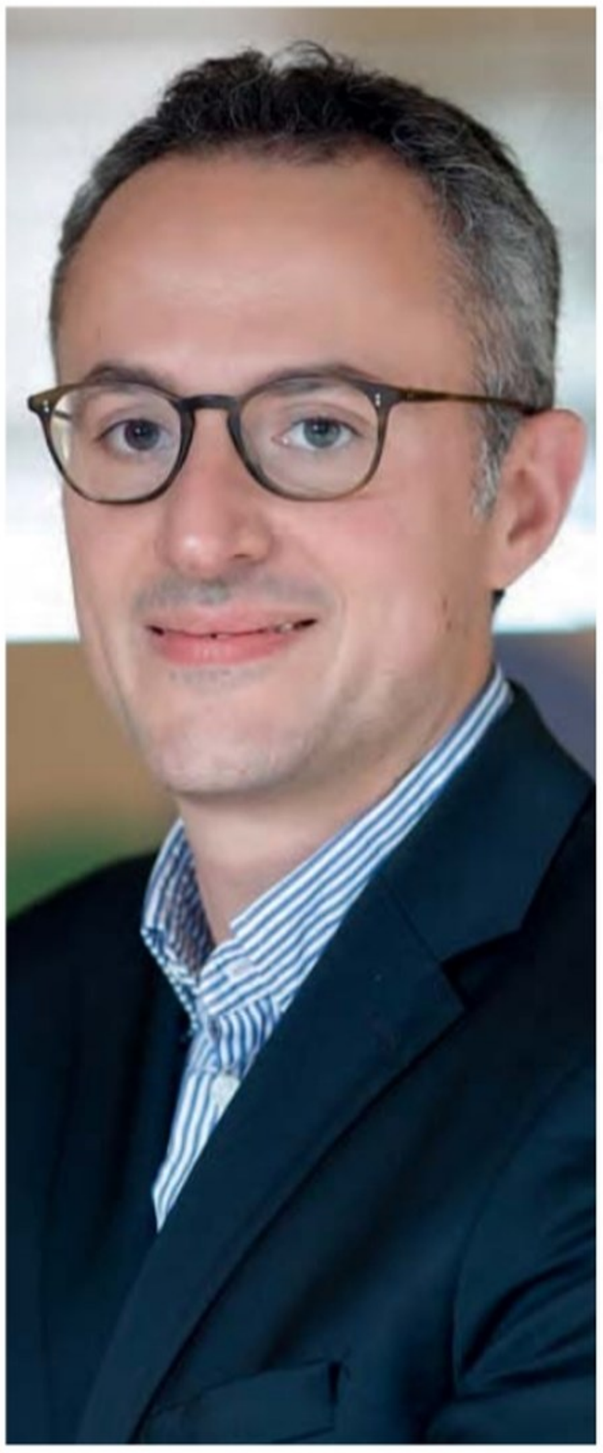
Sur le marché émergent du SD-WAN, Juniper Networks veut faire entendre sa différence en apportant une expérience utilisateur comparable à celle sur le réseau local (LAN ou Local Area Network).

Michael Melloul, Systems Engineering Director chez Juniper Networks, affirme que l'expérience utilisateur sera le principal différenciateur et que Juniper a une importante carte à jouer en apportant une expérience comparable à celle du LAN, où l'entreprise fait partie des principaux acteurs, au WAN.

Une nouvelle étape

Dans le futur, Juniper Networks vise à apporter un ensemble de ses services par un portail unifié avec l'ajout de la sécurité apporté par l'acquisition de 128 T. Cette solution, purement software apporte, une technologie « tunneless » qui évite d'avoir à rechiffrer les données ou de le faire que lorsque c'est nécessaire. Les performances sont d'autant améliorées. Cette technologie sera d'ailleurs portée sur les appliances SRX. Le portail s'appuie sur Mist pour l'offre WAN Assurance. Michael Melloul le décrit comme *« la WAN Assurance 2.0 »*, avec une expérience optimale pour les utilisateurs.

Concrètement, le portail permet de déployer et de suivre les opérations sur le WAN tout en apportant une visibilité complète sur l'expérience des utilisateurs et réduit le temps de résolution des incidents. Il apporte aussi des informations sur l'état des routeurs et des appliances SRX déployées. Il identifie automatiquement les erreurs de configuration et des interfaces sur la passerelle. Des fonctions d'intelligence artificielle évaluent les impacts sur la latence, la gigue, les paquets perdus et sur toutes les autres métriques choisies. La solution embarque, de plus, l'interface conversationnelle de Marvis qui permet aux équipes IT de rechercher en langage naturel les causes d'incidents pour y remédier plus rapidement. Une fonction de déploiement « zero touch » simplifie et unifie le déploiement des réseaux SD-WAN par des templates de configuration pour des déploiements larges.



Michael Melloul, systems engineering director chez Juniper Networks.

Reprendre la main

Michael Melloul indique : *« Cela va nous permettre de reprendre la main sur les services de contournement »* (OTT ou Over the Top). Sur ce point particulier, Juniper veut se placer comme une surcouche sur ces services.

Une sécurité zero trust

Avec 128 T et Apstra, la sécurité de la Data Center Fabric va être étendue du centre de données privé aux environnements multiclouds par des règles qui pourront être déployées pour des groupes. Pour les applications, cela s'appliquera flux par flux. Security Director, le portail d'accès aux services SASE de Juniper va être cloudifié pour des services de sécurité déployés au plus près des utilisateurs un peu comme le réalise Zscaler avec ces caches déployés au plus près des utilisateurs. Autre intérêt de la solution, le chiffrement est un chiffrement TLS et non IPSEC apportant une meilleure performance.

RIC n'est pas un hochet

Pour les environnements mobiles, Juniper pousse comme beaucoup Open RAN et possède un RIC (RAN Intelligent Controller) qui contrôle et optimise les fonctions RAN. Ce contrôleur embarque à la fois des fonctions temps réel et non temps réel avec un framework de gestion et d'orchestration comme défini par l'alliance Open RAN.

Juniper ne lâche pas l'affaire et étend ses points forts sur les environnements WAN avec une vision logicielle. L'entreprise se place sur un marché qui frémit en France, mais qui devrait finir par décoller du fait des avantages de coûts et de gestion que cela apporte. □

B.G

Cloud XPR de Jaguar

Une solution clé en main souveraine



La filiale du Groupe Iliad a lancé récemment sa propre offre de Cloud souverain XPR pour apporter une solution clé en main dans ce domaine.

Jaguar constate un retard des entreprises françaises dans la migration de leurs applications vers le Cloud comparativement aux autres pays européens. Selon un classement établi par la Commission européenne (DESI), 80% des entreprises françaises n'ont pas encore franchi le pas. Elles seraient deux fois plus nombreuses à utiliser le Cloud aux Pays-Bas, en Italie et en Belgique. Jaguar Network veut aider les entreprises à combler ce fossé avec une offre souveraine qui se veut innovante, simple et abordable. Cloud XPR a demandé trois années de recherche et de développement. L'offre se veut, non seulement, complète pour faciliter la migration et proposer un service clé en main, mais aussi, multi-usage et compatible avec les environnements hybrides avec des instances mutualisées. Elle vise aussi à héberger des applications critiques pour un public d'ETI et de PME.

Des services pour le Cloud de confiance

Cloud XPR orchestre plus de vingt modules standardisés qui couvrent tous les aspects d'infrastructure : calcul, stockage, réseau... La solution donne l'accès à une marketplace de plus de cent cinquante applications tierces. Au-delà de garantir une très haute disponibilité grâce à la géo-redondance et la réplication des données sur trois sites dans les douze centres de données de Jaguar. Des plans de continuation ou de repise (PCA/PRA) sont inclus. Cette offre permet d'accéder à un portail intuitif pour piloter aisément les projets, visualiser la performance des environnements ou encore gérer les plans de sauvegarde et de continuité grâce aux outils de métrologies intégrés. Plus globalement, Jaguar Network mobilise une équipe de plus de cent experts Cloud et sécurité pour apporter des services à valeur ajoutée avec une supervision active qualifiée par l'ANSSI. La solution est certifiée ISO 27001 et Jaguar Network est hébergeur de données de santé. Pour la sécurité, Jaguar Network va mobiliser plus d'une centaine d'experts pour offrir des services dont un de supervision, certifié par l'ANSSI.

Lors de l'annonce, aucun tarif n'a été donné, mais Jaguar Network veut proposer une tarification prévisible et allant, sur certains services, à moins de 50 % que chez les grands fournisseurs de Cloud public.

Une stratégie convergente

La nouvelle offre de Jaguar Network qui cible les environnements hybrides et le Cloud privé se retrouve très complémentaire de ce qu'offre une autre filiale d'Iliad, Scaleway, sur le Cloud public. Les deux vont donc avancer de concert pour offrir des services de Cloud correspondant aux besoins des différentes tailles d'entreprises sur un ensemble d'environnement. En tout cas, cela ne peut que contribuer aux différents objectifs dans le secteur B2B d'Illiad qui vise les 500 millions de chiffre d'affaires sur ce segment dans les années à venir. □

B.G

TELEHOUSE S'ÉTEND À MARSEILLE AVEC JAGUAR NETWORK

Telehouse va s'implanter à Marseille en s'appuyant sur Jaguar Network. Depuis Marseille, Telehouse peut proposer aux entreprises qui lui externalisent leur infrastructure informatique, une capacité de transit de leurs données bien plus rapide vers certains continents qu'il ne peut le garantir depuis ses autres implantations européennes du fait de l'arrivée de câbles sous-marins avec des bandes passantes très larges dans cette ville.

Convergence sécurité et réseau

La dernière version de FortiOS, la 7.2, apporte de nouvelles fonctionnalités qui renforcent la convergence entre réseau et sécurité en unifiant SD-Wan et Approche Zero Trust.

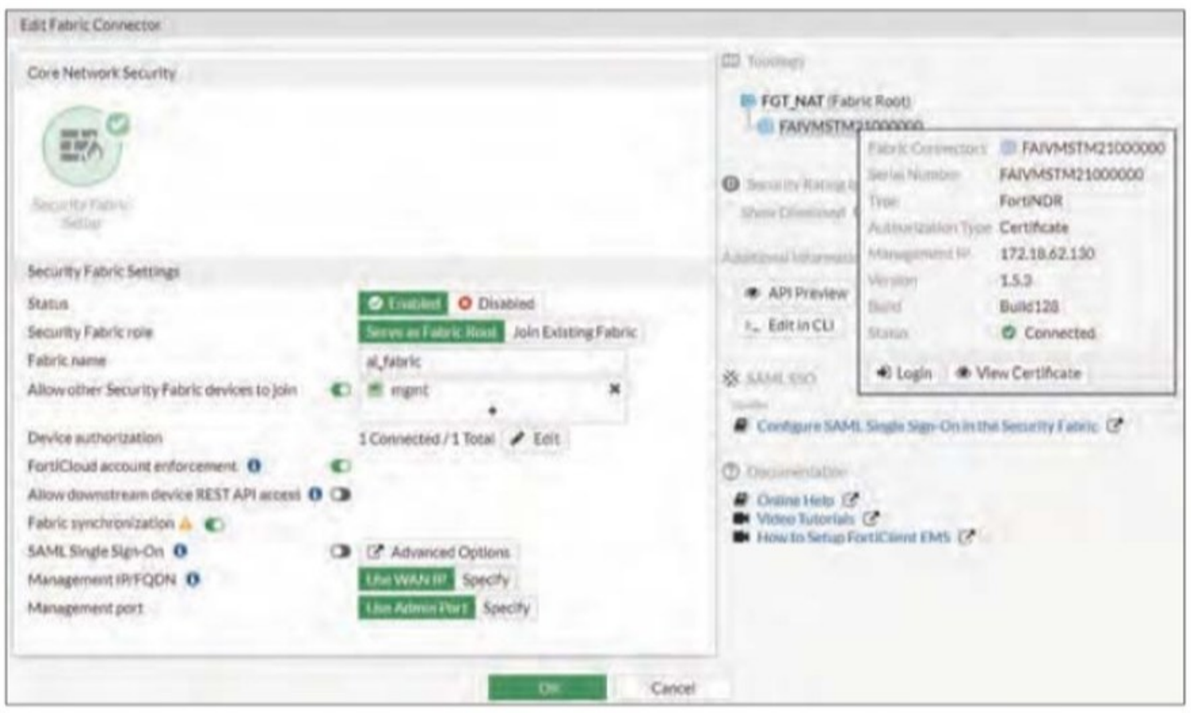
Fortinet annonce la disponibilité de FortiOS 7.2, nouvelle version de son système d'exploitation, clé de voûte de la Fortinet Security Fabric. La version comprend plus de 300 nouvelles fonctionnalités visant à apporter une sécurité optimale sur la périphérie du réseau.

FortiOS 7.2 propose de nouveaux services de sécurité FortiGuard, optimisés par l'Intelligence Artificielle pour sa plateforme convergente de sécurité et réseau, tout en consolidant davantage des produits de sécurité distincts sur les réseaux, les Endpoints et les environnements cloud. Le panel des services de sécurité FortiGuard, piloté par FortiGuard Labs, est intégré en natif sur l'ensemble de la Fortinet Security Fabric pour fournir une sécurité automatisée et coordonnée en temps réel. Les fonctions d'apprentissage machine et d'intelligence artificielle pour analyser les données en provenance du réseau, des terminaux et du Cloud enrichies par des données issues de sources indépendantes.

De nouveaux services

Le bac à sable classique devient une fonction temps réel, étroitement intégrée au réseau, pour neutraliser les malware connus et inconnus, avec un impact maîtrisé sur l'opérationnel. Il en résulte une protection renforcée contre les ransomwares par rapport aux solutions qui acceptent des fichiers suspects au sein du réseau et qui, par la suite, doivent tracer le malware une fois identifié.

Un service de protection avancée contre les menaces détecte automatiquement et segmente les dispositifs IT et OT compte tenu de leur fonction sur le réseau. Ce service procède également à un inventaire des ressources et utilise le pattern matching pour appliquer les règles pertinentes et automatiser la remédiation. Ce service est actif sur la solution de firewall de nouvelle génération de l'éditeur et sur le LAN Edge grâce à une intégration avec FortiNAC. L'utilisation de playbooks dédiés au contrôle d'accès au réseau (NAC – Network Access Control) permet de détecter et de traiter les menaces au plus proche des ressources protégées. Les autres nouvelles fonctions concernent la détection des malwares provoquant des épidémies par des scripts qui vérifient la présence de ses menaces, un service De SOC (Security Operation Center) managé, un nouveau service de CASB intégré dans le firewall FortiGate qui collabore avec Fabric Agent pour inspecter le trafic selon les principes de ZTNA, et vérifier le statut ZTNA. Plusieurs autres services connaissent des améliorations comme la sécurité Web.



La nouvelle fonction de FortiOS intégrée à FortiGate.

Une convergence renforcée entre sécurité et réseau

La solution de SD-WAN sécurisée de Fortinet bénéficie d'améliorations qui accélèrent et automatisent la couche d'orchestration et encouragent l'évolutivité des architectures WAN. Grâce à un monitoring des analyses des données applicatives et de la note moyenne d'opinion pour les applications voix et données, les entreprises peuvent mesurer la qualité d'expérience d'une application du point de vue de l'utilisateur final. Une solution SD-Branch de sécurisation des sites distants, du WAN edge au LAN Edge, propose des fonctions de WAN sur 5G, de SD-WAN, de sécurité par pare-feu NGFW, ainsi que des équipements LAN, à partir d'une seule solution unifiée et convergente. FortiOS 7.2 propose de plus des fonctions automatisées de déploiement et d'orchestration qui sécurisent la gestion des réseaux sur les sites distants. Les nouvelles fonctions d'intégration permettent d'identifier les dispositifs et de mettre en œuvre un accès à privilège moindre au niveau de l'edge du LAN, sans avoir à déployer de nouveaux systèmes.

Cette version très riche suit le modèle SASE prôné par le cabinet Gartner, et Fortinet a désormais toutes les fonctions qui y correspondent. ☐

B.G

HarfangLab
Deep Integrity | Paramount Security

HarfangLab EDR
Souverain
Certifié
Offert*

VISA DE SÉCURITÉ

*Le seul EDR certifié par l'ANSSI, offert pendant 3 mois !

Pour en profiter, scannez ce QR code et remplissez le formulaire de demande lié

HarfangLab | EDR

- + 25 ans d'expérience en cybersécurité auprès du ministère des armées, de l'ANSSI et de grandes entreprises de cybersécurité.
- Déploiement Cloud ou On-Premises.
- Agents déployés sur les postes de travail et serveurs.
- Moteur d'intelligence artificielle basé sur l'analyse comportementale.
- API ouverte pour s'intégrer aux autres solutions de sécurité.
- HarfangLab EDR a été sélectionné par Safran, Nexter, Thalès et le ministère des armées.
- **EDR souverain certifié par l'ANSSI.**

La souveraineté n'a jamais été aussi importante.

Les tensions internationales actuelles provoquent une accélération des opérations cybercriminelles.

Pour y faire face, L'**ANSSI** recommande fortement d'accroitre la supervision de sécurité et de s'équiper d'un **EDR**.

Dans une démarche de solidarité et pour aider les organisations à s'équiper, **HarfangLab** met à disposition son **EDR** souverain certifié par l'**ANSSI** gratuitement pendant 3 mois.

CYBERSECURITY MADE IN EUROPE

www.**HarfangLab**.io

Applications

F5 analyse la **transformation numérique**

Dans la huitième édition de son étude, le fournisseur de solutions de sécurité et d'équipements réseau présente les défis auxquels sont confrontées les organisations lorsqu'elles transforment leurs infrastructures informatiques pour déployer et sécuriser des services numériques devenus indissociables des activités quotidiennes, comme la réalisation de tâches professionnelles ou la consultation d'un médecin.

Les résultats de l'enquête indiquent également des écueils à venir qui, s'ils sont ignorés, empêcheront les organisations de gagner en réactivité et en agilité. Les personnes interrogées ont classé la visibilité dans différents environnements comme étant le principal défi à relever pour les équipes qui déploient des applications dans plusieurs Clouds, suivie de près par une sécurité cohérente. Pour les aider, 90 % des organisations, tous secteurs confondus, prévoient de mettre en œuvre l'IA pour mieux servir les clients et obtenir des informations précieuses. Cependant, une IA efficace exige une transparence, une intégration et une gouvernance des données supérieures à ce qu'offrent les solutions actuellement disponibles. De même, l'enquête identifie l'ingénierie de la fiabilité des sites (SRE ou Site Reliability Engineering) comme une pièce essentielle du puzzle, 77 % d'entre eux adoptant des approches SRE pour leurs applications et systèmes. Néanmoins, l'architecture d'entreprise doit évoluer en parallèle pour prendre en charge des modèles distribués et centrés sur les applications et faire progresser les efforts de transformation numérique des organisations.

D'autres résultats notables

Plus des deux tiers des entreprises réalisent que la création d'interactions numériques supérieures pour les clients implique également de moderniser des processus commerciaux moins visibles et des fonctions de back office. Dans le même ordre d'idées, les personnes interrogées considèrent la convergence des systèmes de technologie de l'information (IT) et de technologie opérationnelle (OT) comme l'évolution la plus prometteuse des années à venir. L'intégration des systèmes OT qui gèrent les opérations industrielles et d'entreprise avec les systèmes IT centrés sur les données contribuera à boucler la boucle de l'automatisation et à rendre les entreprises numériques plus adaptatives, afin qu'elles puissent mieux anticiper et répondre à l'évolution des attentes des



clients et des conditions du marché. Un nombre écrasant d'organisations (95 %) ont prévu d'exploiter les données opérationnelles en vue d'obtenir des informations qu'elles espèrent utiliser pour améliorer l'expérience client et stimuler la croissance de l'entreprise. Cependant, 98 % des personnes interrogées indiquent qu'elles sont actuellement incapables d'extraire les informations nécessaires de leurs systèmes existants.

Plus des trois quarts (76 %) des personnes interrogées admettent que, si elles avaient le choix, elles désactiveraient les mesures de sécurité pour améliorer les performances. La gestion d'un spectre de risques avec des objectifs réels montre que les entreprises adoptent une approche modifiée de la gestion des risques. Plus important encore, plus des deux tiers des entreprises (67 %) rapatrient actuellement des applications, c'est-à-dire qu'elles les déplacent du Cloud vers un environnement de centre de données ou prévoient de le faire dans les 12 prochains mois. Un chiffre en hausse par rapport aux 27 % de l'année précédente. □

B.G

Visite de la start-up Nation

ITPT 43 : Infrastructure et software

Cela faisait plus de deux ans que l'IT Press Tour n'était pas allé en Israël. Le mois dernier, il redevenait possible d'y retourner après la période de pandémie et de découvrir, ou redécouvrir les start-ups qui comptent dans différents domaines.

Pliops

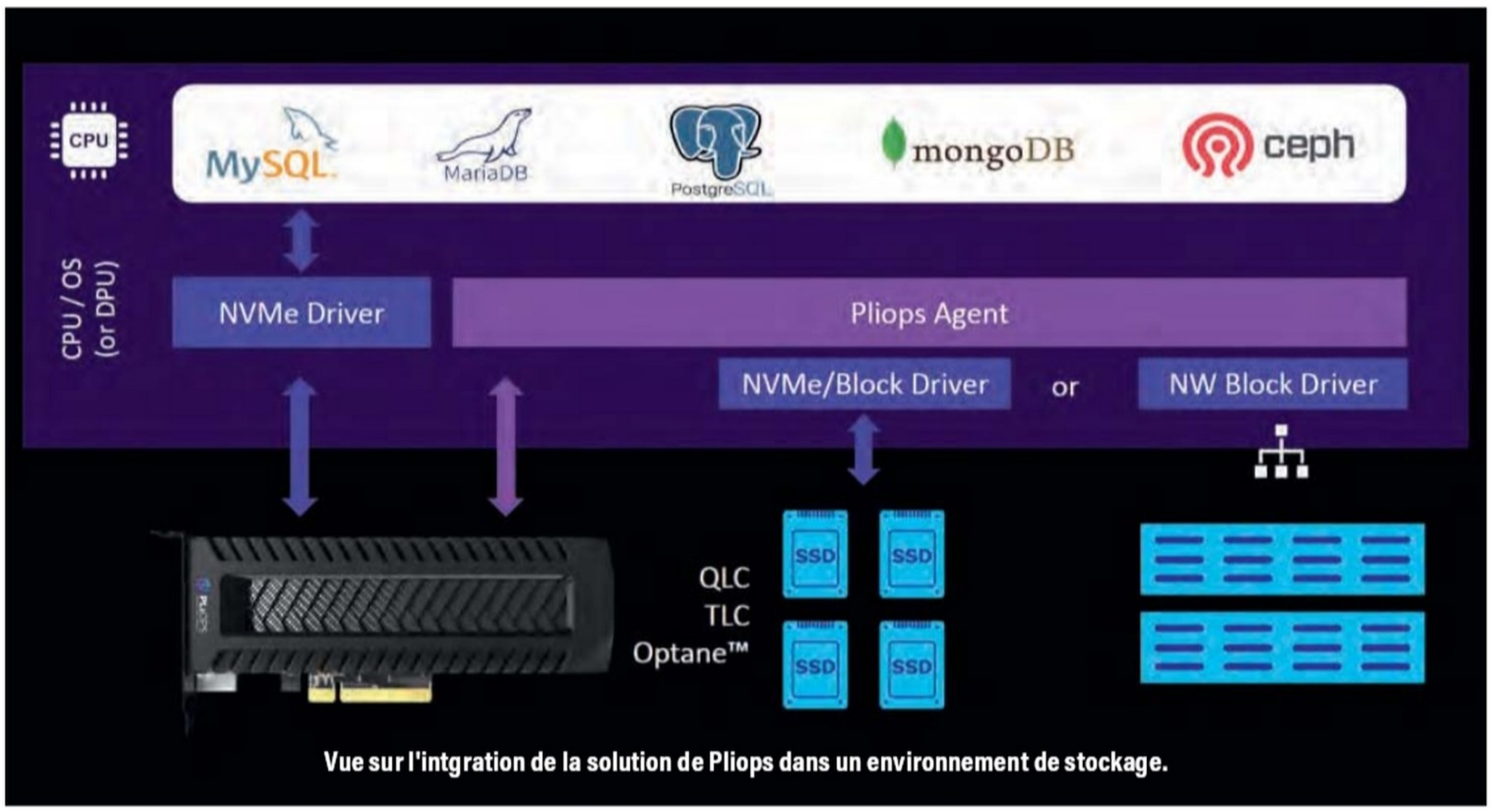
Pliops est une start-up ambitieuse qui se donne pour mission de devenir le Nvidia du stockage en autorisant par sa solution une mise à l'échelle massive des infrastructures pour les bases de données, l'analytique ou d'autres workloads avec des traitements massifs de données. Pour y parvenir, la société a développé Pliops XDP, un processeur de traitement de données extrême. Dans le contexte contraignant des centres de données et du fait de la pénurie de puces, XDP apporte sa différence avec des augmentations de performance d'un facteur de 3 à 15 avec une disponibilité deux fois supérieure à un environnement RAID 0 en consolidant les capacités d'un facteur 6, tout en assurant un coût de possession beaucoup plus bas. XDP se veut le maillon le plus récent sur les processeurs et se positionne face aux GPU, CPU et autres DPU en se voulant plus performant. Le système de Pliops s'appuie sur un cœur ARM avec des interfaces NVMe, des librairies clé/valeur et des fonctions d'accélération pour le stockage et l'analytique.

La solution est idéale pour éviter les problèmes d'amplification des données que connaissent les moteurs de stockage comme RocksDB en limitant celle-ci à un facteur allant de 1 à 3, soit son minimum théorique. La solution consolide de plus les différentes couches nécessaires sur un matériel optimisé. Cela permet des mises à l'échelle extrêmes sur à peu près tous les environnements NVMe. D'après Pliops, les performances sont consistantes même sur des disques ayant quasiment leur capacité maximale.

Intel, Nvidia, Inspur et Percona sont des partenaires et Western Digital et Sakura Internet sont des clients de Pliops.

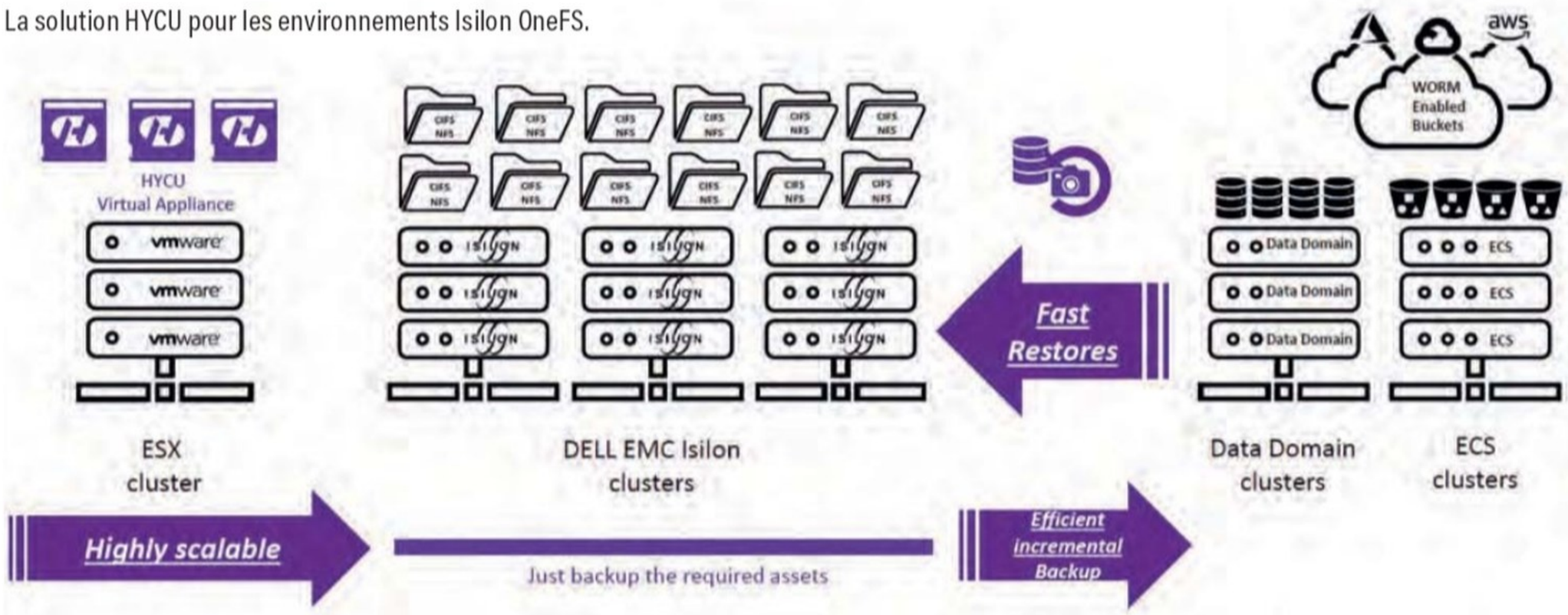
HYCU

L'Informaticien a souvent rencontré HYCU lors des IT Press Tour. Le fournisseur de solutions de sauvegarde natives pour les environnements Cloud et hyperconvergents avait plusieurs annonces à partager lors de notre rencontre. Récemment, l'éditeur avait annoncé une de ses solutions Protégé for Kubernetes afin d'assurer la protection des données dans cet environnement cloud natif. La solution propose un service de sauvegarde en ligne unifiée qui protège toutes les sources de données dans Kubernetes.



Vue sur l'intgration de la solution de Pliops dans un environnement de stockage.

La solution HYCU pour les environnements Isilon OneFS.



Autre innovation récente, R-Score permet à l'utilisateur ou au client de faire une analyse de sa préparation en cas d'attaque de rançongiciel en évaluant les processus de backup, leur infrastructure, la sécurité et le réseau associé, le processus de restauration et l'organisation autour d'un plan de reprise. R-Score copie FICO Score et se décline en deux versions : Web et pour un consulting avancé. Le logiciel délivre des recommandations et est versionné pour des mises à jour continues. La solution est proposée maintenant sous la forme d'un service en ligne.

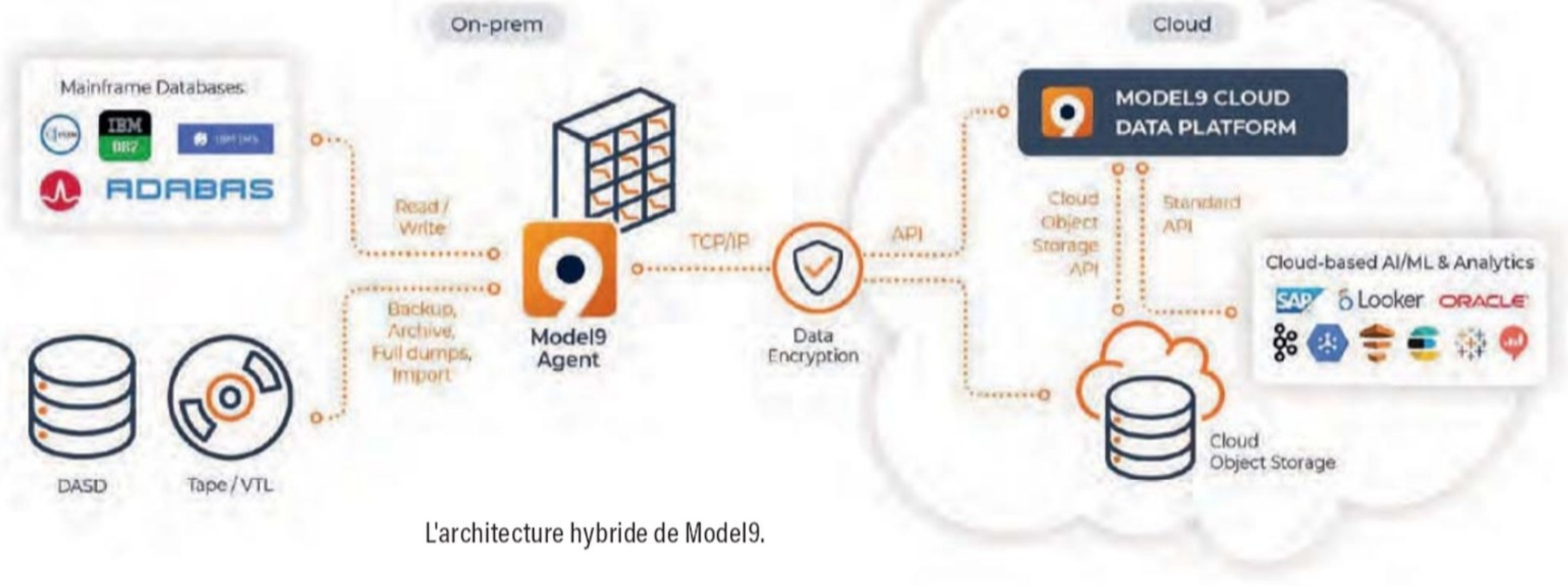
La principale annonce de cette visite est le lancement de HYCU Protégé Ransomware Release qui apporte une extension de la couverture des tâches prises en charge avec le support de PowerScale One FS de Dell EMC, le support étendu de la fonction WORM, de fonctions de sécurité Zero Trust par la prise en charge des systèmes de gestion des clés tiers, de fonctions de déduplication efficaces et de la possibilité de migrer les données en un clic pour les données Azure Gov Cloud.

Model9

Cette entreprise s'attache à une nouvelle approche de la gestion des données sur les mainframes dans le Cloud. Model9 se positionne sur la modernisation du mainframe et est soutenue par Intel Capital, Stage One, North First Ventures, et Glenrock Israel. La société est partenaire d'IBM, Microsoft Azure et AWS. L'éditeur met en avant différents bénéfices de sa solution en proposant un stockage objet à la place de stockage sur disques onéreux ou d'environnements de bandes lourds à gérer. L'approche de Model9 permet de supprimer de nombreux frais de licences et décharge les processeurs du mainframe en passant les charges sur des puces qui ne sont pas facturées par IBM. La solution se révèle performante et annonce pouvoir migrer quatre fois de plus de données en utilisant 40 % de traitement processeur en moins.

Shield est une fonction en ligne pour protéger les données sur mainframes qui, contrairement à l'idée reçue, peuvent être victimes de rançongiciel. Le logiciel fournit une copie immutable dans un environnement « air gap », de la compression et du chiffrement de bout en bout, des fonctions de reprise, des tests périodiques, des fonctions forensiques et le maintien de la conformité sur les périodes de rétention des données.

Gravity est une autre fonction de Model9 qui rend les données du mainframe accessibles aux environnements IA/ML et analytiques pour tous les environnements Cloud



L'architecture hybride de Model9.

et transforme les données sur un format ouvert qui peut être consommé par ces environnements. Gravity utilise un système ELT qui transfert et transforme les données dans le Cloud cible, ce qui est plus rapide et moins cher que sur le mainframe.

SpeeDB

SpeeDB est très jeune et n'a que 18 mois d'existence. Sa solution souhaite faire bouger les lignes sur les moteurs de données, dans les bases de données clé/valeur. Sa vision est ambitieuse et vise à lever toutes les contraintes que connaissent actuellement les bases clé/valeur : capacité, échelle, performance. La solution s'attaque aux différents problèmes que sont la croissance des métadonnées et le coût induit pour y faire face. Les moteurs de stockage connaissent des limitations sur plusieurs niveaux comme la limitation de la taille des données à 100 Go, mais aussi la forte utilisation de CPU lors des écritures provenant de l'amplification des données... Pour Adi Gelvan, CEO et fondateur de SpeeDB, ces moteurs clé/valeur sont devenus le maillon faible des opérations dans les environnements hyperscale et deviennent le véritable goulet d'étranglement pour les nouvelles bases de données.

SpeeDB se veut le premier moteur qui apporte la dimension hyper-scale à ce type de moteur en délivrant des jeux de données à l'échelle du pétaoctet en demandant peu de ressources hardware pour traiter des milliards d'objets avec de très hautes performances et totalement conforme avec le leader de ce secteur, RocksDB. SpeeDB est une solution de remplacement de RocksDB sans avoir à changer le code ou l'architecture. Le moteur permet aux utilisateurs de RocksDB de gérer des jeux de données multipliés par 100 avec des traitements multipliés par 10 en utilisant 80 % de ressources en moins. Pour y parvenir le moteur utilise de nouvelles méthodes de compactage qui réduisent drastiquement les amplifications en écriture. Il élimine le besoin de faire du sharding par une croissance sans limite sur une seule instance tout en minimisant l'utilisation de la mémoire. Un contrôle des flux élimine les pics de latence pour les utilisateurs et une méthode d'indexation nouvelle supporte le stockage des index avec les données pour parvenir à de très hautes performances sur de grands environnements.

Data Dynamics

Piyush Mehta, le CEO de Data Dynamics s'est fixé un but ardu : structurer les données non structurées pour faire face au déluge de celles-ci dans les entreprises pour faciliter la prise de décision par une plate-forme centralisée, une tâche herculéenne ! Le pari est en passe de réussir. La société revendique plus de 300 clients dont 26 Fortune 100, banques, industriels ou dans le secteur de l'énergie. La plate-forme dans le Cloud est sécurisée et permet d'enrichir les données et de les partager à partir d'un point central. Elle apporte des informations pertinentes pour une prise d'actions ou de résolution de problème tout en maintenant la conformité autour des données.

La solution a déjà analysé et migré plus de 400 Pétaoctets de données et connaît un succès grandissant. Data Dynamics a obtenu de nombreux prix et reconnaissance sur le marché que ce soit par des organisations professionnelles, des cabinets d'analystes ou des médias.



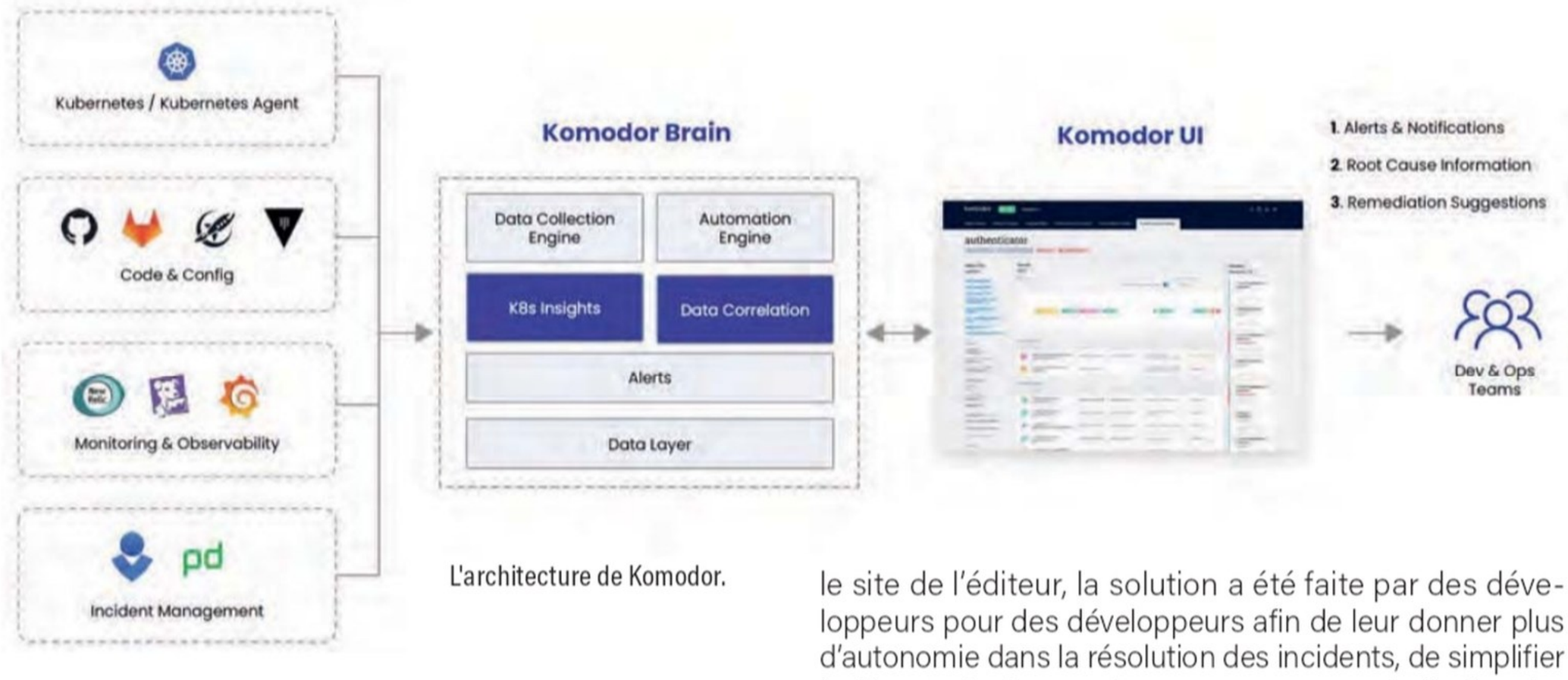
Piyush Mehta, CEO de Data Dynamics.

Ctera

Nous avions rencontré CTera l'année dernière et la priorité de l'entreprise était les environnements de périphérie. Lors de notre visite, cette priorité s'est déplacée vers les données et la présentation de CTera Data Services Platform. Elle s'appuie sur une structure de microservices et est programmable pour des workflows automatisés, la sécurité et l'analyse des données. L'éditeur a aussi présenté Ctera DevOps SDK pour accélérer les déploiements et leur automatisation qui prend en charge Ansible et Python. La solution peut ainsi automatiser des migrations d'un NAS (Network Attached Storage) vers le Cloud.

Comme l'ensemble des acteurs dans la protection des données, Ctera a renforcé les fonctions de sécurité avec des réplications continues vers des stockages cloud immutables, des restaurations rapides, des alertes proactives et des analyses en temps réel. La plate-forme est elle aussi sur une architecture Zero Trust avec sa propre défense contre les attaques de virus ou de rançongiciels. Les fonctions de respect de la conformité pour les données s'appuient sur une classification des données et des fonctions d'audit.

Ctera se dirige clairement vers une stratégie mettant le cloud en avant. Les récents partenariats avec Backblaze, et certainement d'autres à venir, devraient concrétiser ce virage.



L'architecture de Komodor.

Infinidat

Le spécialiste du stockage haute performance connaît une belle croissance avec un doublement depuis 2020 de ses clients sur des affaires à plus de 10 M$ et une croissance des ventes de 40 % d'une année sur l'autre en particulier sur le segment des plus grandes entreprises dans le Fortune 100.

Phil Bullinger, le CEO de la société, voit dans le logiciel développé par Infinidat les principaux différenciateurs qui expliquent le succès de l'entreprise sur ces environnements exigeants. Ainsi, son Neural Cache avec ses fonctions de parallélisme dans le moteur de traitement des métadonnées et sa mémoire cache sur le front-end séparé du backend media apportent un plus dans les performances.

Le Neural Cache est aussi très utile pour les fonctions d'Aiops et de STaaS embarquées dans les machines. Il y ajoute les fonctions de disponibilité et de protection des données avec une fonction d' « air gap » virtuel avec des snaps immutables, des synchronisations actives/actives ou asynchrones avec des RPO de quelques secondes. Le système breveté InfiniRaid élimine le point unique de panne et réduit le coût de support. Supportant des applications critiques comme SAP ou Oracle, Infinidat propose des cas d'usages pour consolider des environnements de stockage à l'échelle des Pétaoctets. De plus, Infinidat supporte la plupart des protocoles comme FC, iSCSI, NFS, SMB.

Komodor

Komodor est une toute jeune entreprise créée en 2020. Son logiciel est sorti en version beta en novembre de la même année pour être lancée officiellement en mars 2021 et de lever 25 M$ quelques semaines plus tard. En février dernier, la société a lancé un premier projet open source, ValidKube. La solution cherche à simplifier la résolution des incidents qui surviennent dans les environnements de containers opérés sous Kubernetes. Comme le proclame le site de l'éditeur, la solution a été faite par des développeurs pour des développeurs afin de leur donner plus d'autonomie dans la résolution des incidents, de simplifier la découverte des « root causes » par une centralisation des informations et de réduire le temps passé à résoudre les problèmes. Il est vrai que du fait de la complexité technique et des barrières organisationnelles parfois, la recherche des causes d'un incident dans ce type d'environnement peut revenir à chercher une épingle dans une botte de foin. Pour parvenir à son but, le logiciel collecte toutes les données, analyse le contexte et permet aux développeurs de résoudre le problème de manière professionnelle. La solution apporte beaucoup d'automatisation avec l'infusion de toute l'expertise de Komodor sur Kubernetes dans le logiciel. Komodor ne veut pas s'arrêter en si bon chemin et souhaite développer un produit complet pour améliorer la fiabilité de Kubernetes, s'agrandir et servir encore plus de clients ! □

B.G



Ben Ofiri, CEO de Komodor.

Au bonheur des **DAM**

Le Digital Asset Management, c'est le référentiel unique de tous les médias produits et exploités par l'entreprise. D'abord, chasse gardée des marketeurs et des communicants, ce domaine voit peu à peu revenir l'IT.

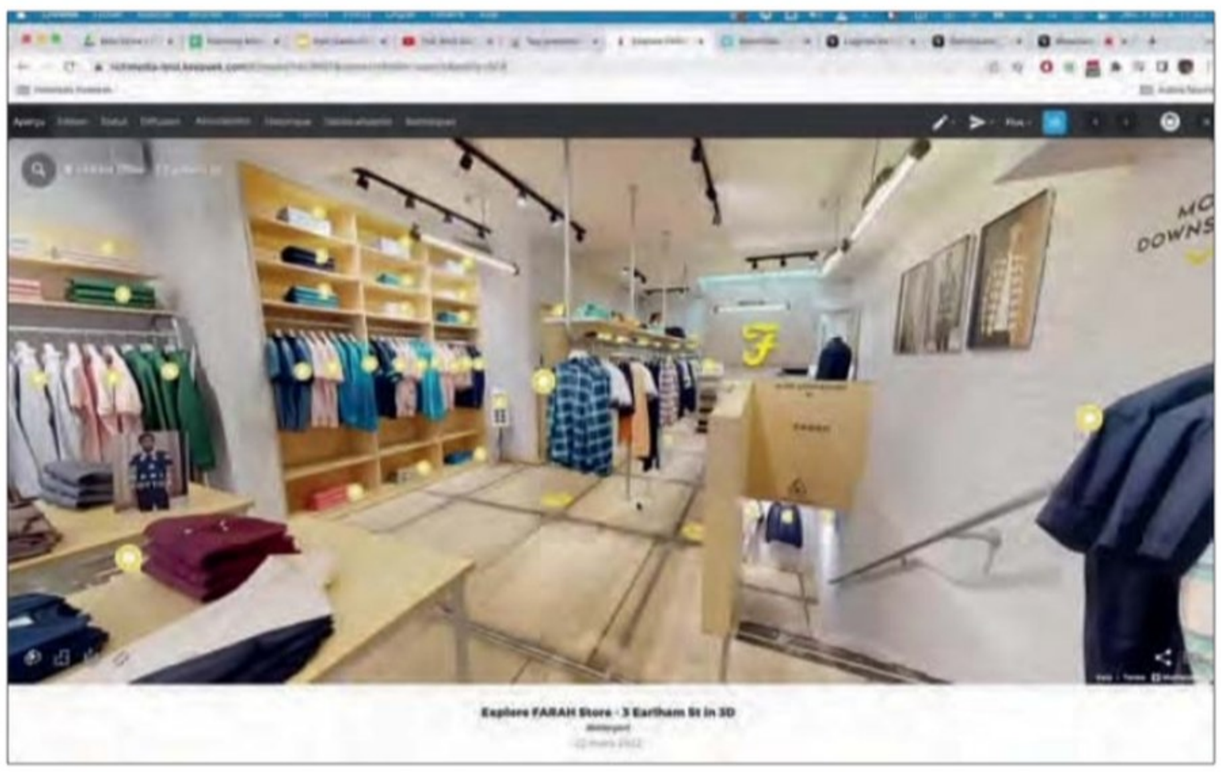
C'est un pan des activités des entreprises que nous négligeons peut-être un peu dans nos pages. Pourtant, les départements marketing et communication sont des décideurs IT, au même titre que de nombreux autres métiers. Eux aussi participent à la transformation numérique des entreprises et, parmi leurs outils, on trouve le DAM ou Digital Asset Management. Très schématiquement, il s'agit du registre unique où sont centralisés tous les médias, les contenus produits par (et pour) l'entreprise.

Thomas Larzillière a fondé Keepeek en 2008. De simple photothèque, la plateforme est devenue un DAM qui revendique 350 clients dans des secteurs comme la distribution *« où Keepeek remplace les mails et WeTransfer pour canaliser les médias produits dans le cadre d'un processus beaucoup plus industrialisé »* ainsi que le luxe, mais aussi l'industrie avec Stellantis, Eiffage ou encore un Airbus. Évidemment, les médias d'une entreprise sont mis à contribution pour renforcer l'image de marque, développer la notoriété, soit des activités de communication, mais aussi pour la formation ou encore l'e-commerce.

Du WeTransfer à l'industrialisation

« L'e-commerce représente chaque jour des milliers de photos, le DAM va avoir pour rôle de prendre en charge la captation via des plateformes spécialisées ainsi que le dépôt de médias de la part des producteurs internes et externes » explique Thomas Larzillière. Concentrateur de médias, le DAM doit venir alimenter des outils tels que des PIM (Product Information Management) afin de placer la photo sur le bon site à côté du bon produit, par exemple. Une tâche difficilement gérable manuellement. Le DAM s'intègre donc aux PIM… mais pas seulement puisque c'est l'ensemble de la chaîne de valeur autour des contenus de l'entreprise qui doit être prise en compte. Donc, en aval, des intégrations avec des outils tels que Trello *« pour la validation des étapes d'un projet vidéo par exemple »* indique le dirigeant de Keepeek.

« Pour adresser ces projets e-commerce, il faut gérer de nombreuses applications en entrée et en sortie. Nous avons dès le départ une culture d'ingénierie, ce qui nous a incité à développer des API pour simplifier l'automatisation » raconte Thomas Larzillière. *« Le DAM est un outil assez central dans l'urbanisation du SI, au même titre que le CRM »*. Et pour cause : il s'agit de rassembler des milliers, des dizaines de milliers de médias photos, vidéo, audio, *etc.*, de normaliser leur production et leur validation et d'automatiser leurs utilisations. On est loin du PDF raturé que l'on s'envoie par mail. D'autant que Keepeek s'attaque désormais à centraliser sur sa plateforme les Rich Media, ces contenus produits sur des plateformes en ligne tels que YouTube, TikTok ou encore Acast, et même des mini-sites de l'entreprise. *« Sur Keepeek, on peut agréger ces contenus, les référencer, les classer, mettre des métadonnées, mettre des droits d'accès et de les partager dans le reste de l'entreprise mais sans qu'elles quittent leurs plateformes natives, grâce à une récupération de l'URL et des API pour récupérer les statistiques et autres interactions utilisateurs »*.



Keepeek a récemment lancé la prise en charge sur sa plateforme des Rich Medias, récupérant non seulement les contenus mais aussi les interactions avec les utilisateurs.

Les API motivent les services informatiques

API, droit d'accès, automatisation, industrialisation des processus… autant de termes qui parleront aux DSI. Car le DAM n'est plus la chasse gardée des communicants et des créatifs. *« En 2008, on est né comme outils SaaS multi-tenant, auquel les départements communication et marketing pouvaient s'abonner sans rien demander à personne »* souligne Thomas Larzillière. *« Pendant des années, on ne voyait pas l'IT, mais ils réapparaissent désormais, par le biais du SSO et des questions de sécurité, et de plus en plus du fait des intégrations. L'IT revient donc au centre des discussions et des prises de décisions »*. □

Guillaume Périssat

Data lakes

BigLake : **Google Cloud** unifie l'accès aux données

Rejoignant des acteurs spécialisés dans la gestion de données, tel Snowflake, Google Cloud veut à son tour unifier data lakes et data warehouses. Le 6 avril, le géant de Mountain View a dévoilé BigLake, son nouveau moteur de stockage qui entend effacer les frontières entre lacs et entrepôts. En parallèle, Google a annoncé une Data Cloud Alliance, autour de l'interopérabilité et l'accessibilité des données entre les environnements des divers partenaires de cette initiative.

À l'occasion de son Data Cloud Summit, Google Cloud a présenté sa réponse aux vastes et épineux problèmes des silos de données. Et par silos, le géant entend la multiplication des data lakes, des bases NoSQL et des data warehouses. À en croire Mountain View, plusieurs centaines de ses clients ont plus d'un pétaoctet de données. Et entre les entrepôts, qui conservent des données transformées, nettoyées et structurées pour les traiter au plus vite, et les lacs qui stockent des données brutes, non transformées et malléables, sans compter que chacun recouvre des méthodes de traitement et des finalités différentes, il y a de quoi se perdre. On passera sur la longue liste de problématiques inhérentes au silotage (coûts, risques, *etc.*).

Ce créneau de l'accès unifié est déjà occupé par des acteurs spécialisés tels que Snowflake et Databricks mais Google Cloud, avec son poids et sa politique de partenariats, entend bien fournir LA réponse aux environnements hétéroclites qui augmentent les risques et les coûts alors que les volumes de données à stocker, traiter et déplacer croît à un rythme effréné. Pour Sudhir Hasbe, Directeur Senior des solutions Analyse de données chez Google Cloud, il s'agit de fournir *« un seul lieu depuis lequel accéder à toutes vos données, de sorte que vous ne soyez pas obligés de les copier à travers vos environnements de stockage comme Google Cloud Storage, AWS S3 ou Azure »*.

Sudhir Hasbe, Directeur Senior des solutions Analyse de données chez Google Cloud.



« Nous étendons nos innovations au monde de l'open source et les ouvrons pour tous. »

Multicloud

Ce lieu unique, c'est BigLake, un moteur de stockage permettant d'unifier l'accès aux entrepôts de données et aux data lakes. Annoncé lors du Data Cloud Summit le 6 avril, cet outil fournit un contrôle d'accès unifié sur les magasins d'objets contenant des données, tels que Google Cloud Storage, évidemment, mais aussi Amazon S3 ou encore Azure Data Lake Storage Gen 2. BigLake dissocie en effet l'accès à la table des données sous-jacentes stockées sur le cloud grâce à la délégation d'accès, et abstrait, pour les administrateurs, la gestion de ces accès des fichiers vers les tables, de sorte à accorder un accès au niveau des lignes et des colonnes. Plus schématiquement, il n'est pas nécessaire de donner accès à l'ensemble de la table à un utilisateur, simplement aux ressources dont il a besoin.

Pour les tables BigLake définies sur Google Cloud Storage, les paramètres de sécurité sont appliqués de manière cohérente sur Google Cloud et les moteurs open source pris en charge à l'aide de connecteurs BigLake. Pour les tables BigLake définies sur Amazon S3 et Azure Data Lake Storage Gen 2, il faudra passer par BigQuery Omni pour traiter les données en appliquant lesdits contrôles de sécurité. Ainsi, les utilisateurs n'ont à conserver qu'une copie unique des données, qui couvre aussi bien BigQuery que les data lakes tout en appliquant des contrôles d'accès cohérents et unifiés sur les moteurs d'analyse choisis.

Un BigQuery dopé à l'ouverture

La création de tables sur BigLake ne dépaysera pas les utilisateurs de BigQuery : le processus est identique, à la différence près qu'il faut dans BigLake préciser la connexion

à la ressource cloud associée. Une fois créée, la table peut être interrogée comme n'importe quelle table BigQuery, les deux sont d'ailleurs soumises aux mêmes limitations. À noter que les utilisateurs peuvent accéder aux tables BigLake sur Cloud Storage en utilisant d'autres outils de traitement de données que BigQuery (Apache Spark ou Hive ou encore Trino) grâce à l'API BigQuery Storage (voir schéma ci-contre). Les connecteurs de BigLake couvrent en outre plusieurs formats de fichiers ouverts, dont Parquet, et divers formats de tableaux à l'instar d'Iceberg. En résumé, Google Cloud veut son BigLake aussi ouvert que possible. *« Nous étendons nos innovations au monde de l'open source et les ouvrons pour tous »* souligne Sudhir Hasbe.

Bref, Google souhaite que BigLake devienne le point d'accès unique aux données, indépendamment de leur stockage en data lake ou en data warehouse, et grâce à son ouverture, permette les analyses sans avoir à déplacer ou copier les données. D'où une concentration des efforts du géant sur ce nouvel outil. Sudhir Hasbe précise que Mountain View s'assurera que *« tous nos différents composants fonctionnent de manière fluide avec BigLake »*. C'est également le sens de cette nouvelle alliance lancée par Google, la Data Cloud Alliance. L'entreprise a battu le rappel et a réuni, surtout autour de ses outils, son écosystème de partenaires. Ainsi, Dataiku, Fivetran, MongoDB, Redis, Elastic ou encore Neo4j ont rallié l'initiative, de même qu'Accenture et Deloitte. Même Databricks, pourtant en concurrence frontale avec BigLake, a rejoint cette alliance.

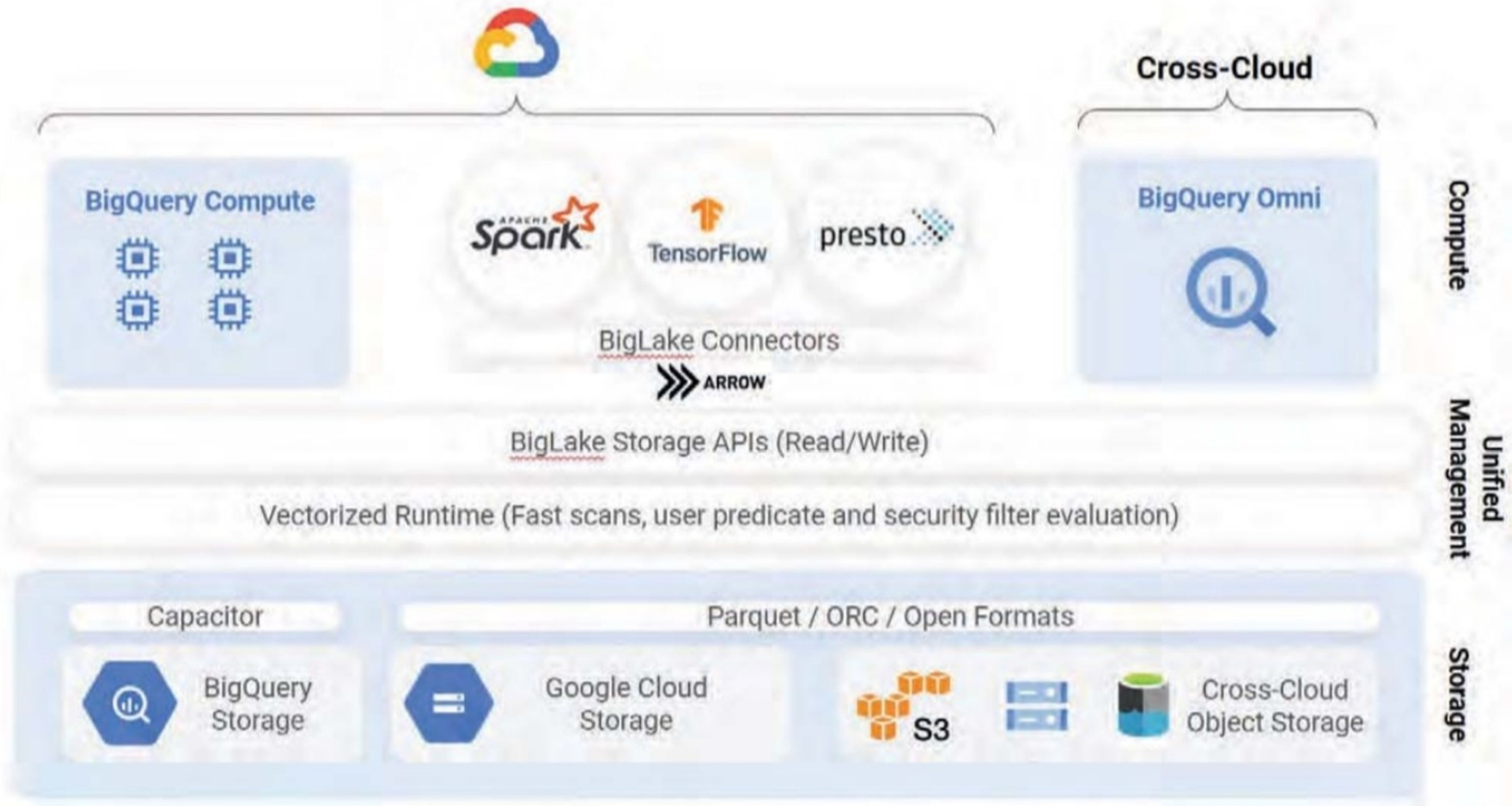
Data Cloud Alliance

Ce groupe a pour grand dessein de *« supprimer les obstacles à l'accessibilité des données »*, selon Gerrit Kazmaier, Directeur Général Base de données, Analytique et Looker chez Google Cloud. Ses membres travailleront à l'interopérabilité, ou plutôt à la portabilité, des données entre leurs produits et leurs environnements, et à la réduction de la complexité de leur gouvernance. Ils élaboreront et fourniront donc infrastructures dédiées, API et un support d'intégration des données, tout en travaillant sur des processus et des modèles de données communs. *« Nous nous sommes engagés à faire en sorte que les données puissent être accessibles et traitées entre les produits, et à placer le client au centre de nos innovations »*, poursuit Gerrit Kazmaier. Les premières initiatives ont été annoncées en amont. Ainsi, Databricks travaille à porter sa solution Databricks SQL sur GCP, tandis que Neo4j met au point la version Google Cloud de son service Graphe Data Science. Starburst, pour sa part, doit rendre prochainement disponible une offre de Trino fonctionnant avec DataPlex et BigQuery. ☐

Guillaume Périssat

VERTEX AI EN MODE WORKBENCH

Annoncé lors du Google Cloud Next 2021, Vertex AI Workbench est désormais disponible. La plateforme de création et de déploiement de modèles de machine learning se renforce de l'intégration native au sein d'une même interface de plusieurs outils : BigQuery, Serverless Spark et Dataproc. Selon Google Cloud, Workbench permet de concevoir des modèles cinq fois plus vite qu'avec les notebooks classiques, tout en offrant la possibilité de mettre à jour les modèles à l'aide de données stockées dans le cloud. En outre, la suite de solutions de machine learning se dote d'un référentiel, d'une librairie de modèles : Vertex AI Model Registry. Celui-ci permet selon le géant d'ajouter, de modifier ou de partager des modèles en quelques clics.



L'architecture de BigLake.

Antivirus

Kaspersky sous haute surveillance

Depuis l'invasion de l'Ukraine, l'entreprise russe Kaspersky est dans le collimateur de plusieurs administrations européennes. Lesquelles lui prêtent d'éventuelles connivences avec Moscou ou la jugent possiblement incapable d'assurer ses services au regard du contexte et des sanctions. Kaspersky dément et s'efforce de rassurer ses utilisateurs.

Alors que la guerre fait rage en Ukraine et que les tensions diplomatiques entre la Russie et l'Ouest rappellent les heures les plus chaudes de la guerre froide, le conflit s'est invité sur une autre scène, celle de la cybersécurité.

Dans un contexte de sanctions économiques à l'encontre de la Russie et face au risque cyber que le Kremlin fait potentiellement peser sur les secteurs politiques, économiques et financiers des pays de l'Union européenne et des États-Unis, certains acteurs sont dans le collimateur des autorités. C'est le cas de l'entreprise russe Kaspersky basé à Moscou, spécialisée dans la sécurité des systèmes d'information et qui développe des outils de sécurité informatique.

Une méfiance grandissante

Les États-Unis ont d'ailleurs placé récemment la société sur la « liste noire » de la Federal Communications Commission (FCC). Kaspersky ne peut donc plus vendre ses produits ou ses services aux administrations américaines, ni bénéficier de subventions fédérales pour des achats.

Le 15 mars dernier, près de trois semaines après l'invasion de l'Ukraine, l'Office fédéral de la sécurité de l'information (BSI), l'agence allemande chargée de la cybersécurité, a recommandé aux entreprises et aux administrations sensibles de remplacer le logiciel antivirus de Kaspersky – si elles en étaient équipées – par « des produits alternatifs ». Une déclaration faite en réaction au risque « considérable » d'attaques informatiques par Moscou.

Inquiète, l'institution craint, en effet, que cette entreprise serve de passerelle et que le Kremlin subtilise des données potentiellement sensibles. *« Un fabricant informatique russe peut lui-même mener des opérations offensives, être contraint d'attaquer des systèmes cibles, être victime d'une cyber-opération, être espionné ou utilisé comme outil pour lancer des attaques contre ses propres*



Eugène Kaspersky, emblématique patron de la société de cybersécurité qui porte son nom.

clients », a-t-elle expliqué. Ce qui, disons-le, s'apparenterait à un suicide commercial si ces allégations venaient à se confirmer.

Et, pour ajouter encore à l'inquiétude de l'office allemand, les logiciels antivirus, pour fonctionner correctement, doivent accéder aux moindres recoins des terminaux qu'ils sont censés protéger et doivent communiquer avec leurs serveurs pour être mis à jour.

« Du jour au lendemain, la BSI, avec qui nous avions de très bonnes relations, a suggéré de désinstaller Kaspersky et de trouver des alternatives. Mais il s'agissait d'un avis pris pour des raisons politiques, qui n'apportait aucuns

faits techniques », regrette Bertrand Trastour, directeur général de Kaspersky pour la France, l'Afrique du Nord, de l'Ouest et du Centre.

Moscou n'est pas le centre de tout

La société assure être transparente avec ses clients, ses partenaires, et tout l'écosystème cyber en général. D'autant plus que, depuis 2017, les autorités américaines avaient pris des mesures pour bannir l'entreprise des réseaux fédéraux, de peur que les renseignements russes n'utilisent le logiciel à des fins d'espionnage.



Des accusations que le principal intéressé balaie d'un revers de la main. La Russie a effectivement mis en place une législation de surveillance, officiellement destinée à lutter contre le terrorisme (SORM). Mais celle-ci s'applique aux opérateurs de télécommunications et aux fournisseurs d'accès internet (FAI). *« Ne fournissant pas de services de télécommunications, Kaspersky n'est pas soumise à cette législation ni à d'autres outils employés par les autorités (russes, ndlr) »*, justifie l'entreprise.



Bertrand Trastour, General Manager France, Afrique du Nord, de l'Ouest et du Centre chez Kaspersky.

« Nos clients peuvent venir auditer nos solutions, le code source, ainsi que les mécanismes de mises à jour et voir comment fonctionne notre chaîne d'approvisionnement logiciel et quelles briques de software sont utilisées. »

Et pour prouver sa bonne foi, la société a mis en place, depuis 2017, une série de mesures, comme l'ouverture de Transparency Center en Suisse, en Espagne, en Italie et au Canada. Des centres où *« nos clients peuvent venir auditer nos solutions, le code source, ainsi que les mécanismes de mises à jour, et voir comment fonctionne notre chaîne d'approvisionnement logiciel et quelles briques de software sont utilisées pour parvenir au produit final »*, décrit Bertrand Trastour.

Et notre interlocuteur d'enfoncer le clou en regrettant que le BSI, *« en dépit des invitations »* de Kaspersky à venir auditer le code source (bien avant la guerre en Ukraine), ne se soit jamais déplacé. L'entreprise rappelle, par ailleurs, ses deux certifications — ISO 27001 et SOC 2 type 1 —, qui attestent de l'intégrité et de la fiabilité des produits. Tous les mécanismes qui alimentent ses systèmes ont été audités et certifiés par des éléments tiers comme le cabinet de consulting et de certification TÜV Austria (ISO 27001).

Si le siège social du groupe est effectivement basé dans la capitale de la Fédération de Russie, ses données les plus sensibles, elles, ont déménagé. *« Nous avons renforcé nos processus internes et la distribution géographique de notre architecture technique »*, indique Arnaud Dechoux, responsable des Affaires Publiques et des relations institutionnelles de Kaspersky France.

Depuis 2017, les données de ses clients, auparavant stockées à Moscou, ont été relocalisées en Suisse. Bertrand Trastour le confirme : *« Toutes les données clients d'origines européenne, américaine, asiatique, moyen-orientale et d'Amérique du Sud, sont désormais en Suisse. »*

La France sur la retenue…

Sur l'autre rive du Rhin, l'Agence nationale de la sécurité des systèmes d'information (Anssi) a, elle aussi, exprimé quelques doutes dans une note publiée le 2 mars 2022. Plus mesurée que son homologue allemand, l'agence écrit que : *« Dans le contexte actuel, l'utilisation de certains outils numériques, notamment ceux de la société Kaspersky, peut être questionnée du fait de leur lien avec la Russie. »* Elle ajoute néanmoins qu' *« à ce stade, aucun élément objectif ne justifie de faire évoluer l'évaluation du niveau de qualité des produits et services fournis ».*

L'agence estime aussi que l'isolement de la Russie du fait des diverses sanctions économiques peut amoindrir la capacité de Kaspersky à mettre à jour ses outils. Ce qui, par ricochet, pourrait menacer les systèmes protégés par Kaspersky. Elle suggère donc de diversifier ses solutions de cybersécurité pour ne pas être dépendant de la seule entreprise russe.

Un discours sensiblement identique par-delà les Alpes, où les Italiens s'inquiètent également de la capacité des entreprises de fournisseurs liées à la Fédération de Russie, à assurer un support adéquat pour leurs produits et services.

L'Agence pour la cybersécurité nationale italienne (ACN) a donc émis une recommandation, dans laquelle elle invite les utilisateurs à *« examiner les implications en matière de sécurité découlant de l'utilisation des technologies de l'information fournies par des sociétés liées à la Fédération de Russie »*, dont Kaspersky fait partie. Mais à l'instar de l'ANSSI, l'ACN précise qu'il n'existe aucune preuve objective d'une baisse de la qualité des produits et services technologiques fournis.

Bertrand Trastour, de son côté, affirme : *« Aujourd'hui, nos opérations fonctionnent parfaitement. Nous avons réalisé de nombreux stress tests de nos infrastructures, pour nous en assurer ».* Même en cas de coupure totale de la Russie de l'internet mondial, l'entreprise dit être en mesure de garantir la résilience de ses opérations. Étant donné le contexte actuel, des stress tests sont toujours en cours et des équipes en interne contrôlent que les services fournis par Kaspersky sont bien délivrés à ses clients *« et que la chaîne d'approvisionnement n'est corrompue en aucune manière »*, ajoute Bertrand Trastour.

Arnaud Dechoux rappelle, en outre, que Kaspersky n'est pas ciblé spécifiquement par les sanctions. *« Eugène Kaspersky (fondateur de l'entreprise, ndlr) n'est pas un proche du Kremlin et la société travaille avec des banques françaises et européennes. Nous ne sommes pas non plus impactés par les sanctions à l'encontre des banques russes. »*

L'ITALIE ENQUÊTE.

L'Autorité italienne de protection des données personnelles a annoncé avoir ouvert une enquête sur les « risques potentiels » liés à l'utilisation des solutions de Kaspersky.
L'enquête doit *« approfondir les alertes lancées par de nombreux organismes italiens et européens spécialisés dans la sécurité informatique, sur la possible utilisation de ce produit pour des attaques cybernétiques contre des utilisateurs italiens »*, détaille l'autorité.
Kaspersky devra fournir *« le nombre et la typologie de ses clients italiens, ainsi que des informations détaillées sur le traitement des données personnelles effectué à travers divers produits et services de sécurité »*. Elle devra aussi « clarifier » certains éléments, notamment les données *« transférées hors de l'Union européenne »*.



Rassurer la clientèle

Cela dit, Kaspersky reconnaît qu'elle perçoit de l'inquiétude chez ses partenaires et dit se tenir à disposition pour lever toutes les interrogations. *« Nous n'avons rien à cacher. Nos clients à l'échelle responsable sécurité ou DSI nous disent qu'ils n'ont pas de soucis et connaissent la qualité de nos solutions. Est-ce que le board (direction, ndlr) nous suivra ? »*, s'interroge Bertrand Trastour. Alors que la guerre en Ukraine sévit depuis déjà sept semaines, difficile, selon lui, de mesurer avec certitude l'étendue des dégâts collatéraux sur la société. □

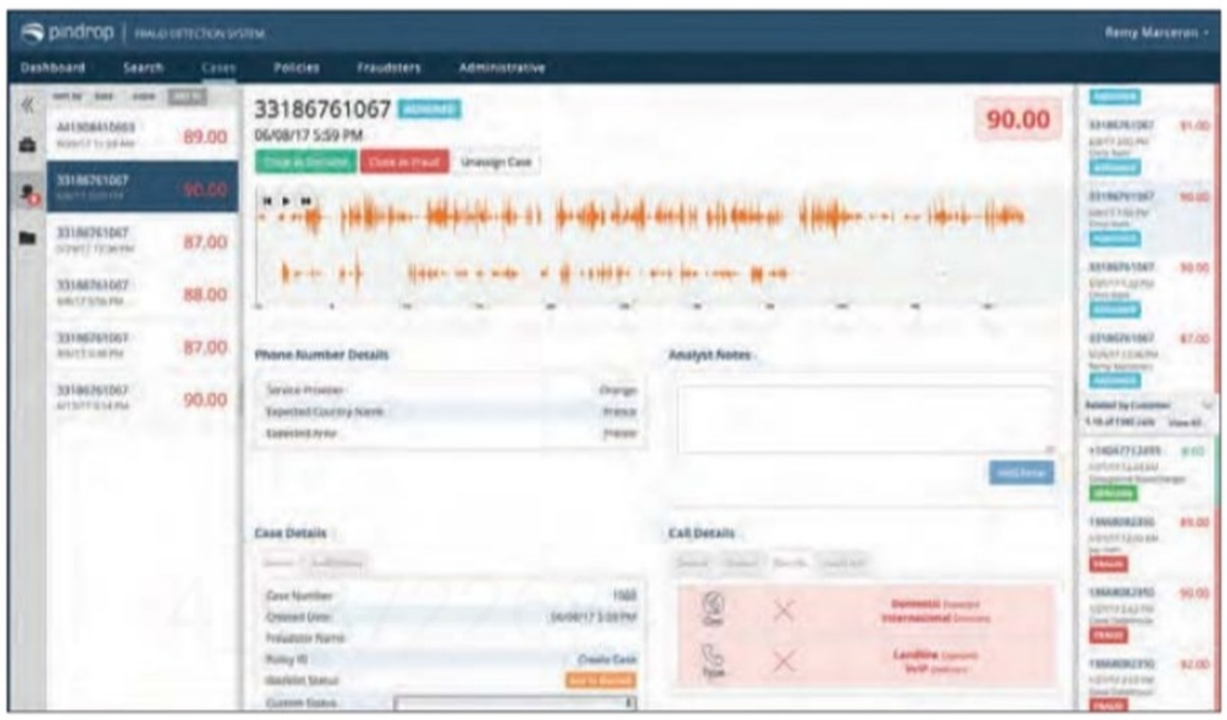
V.M

Attaques méconnues

Pindrop traque la **fraude téléphonique**

Une récente attaque par le canal téléphonique au Moyen-Orient a remis sur le devant de la scène ce type d'arnaque qui arrive plus souvent qu'on ne le croit.

Dominique Ango, DG pour la France de Pindrop, réagit : *« Cela fait beaucoup de bruit, et souvent, la façon de sa réalisation est spectaculaire mais c'est de l'épaisseur du trait sur les fraudes qui utilisent le canal téléphonique. C'est la difficulté qu'il y a à discerner la petite fraude de ces gros coups. »* Il ajoute que des applications gratuites sur le store d'Apple permettent de réaliser le spoofing de numéro de téléphone et d'utiliser des numéros d'autres personnes en y ajoutant des bruits de fond ou de faire croire que la personne est dans un certain endroit.



L'interface de la solution de Pindrop

Pindrop s'est fait une spécialité de traquer les fraudes et de sécuriser le canal téléphonique dans les centres de contacts ou d'appels. La solution tend à séparer le bon grain de l'ivraie en identifiant les utilisateurs légitimes d'une banque par exemple. Dominique Ango donne un ordre d'idée de l'ampleur de cette fraude. *« Un appel sur mille participe à une fraude. 90% d'entre elles se réalisent à partir de numéros de téléphone détournés. 60% des fraudes sur Internet qu'elles soient directes ou indirectes passent à un moment donné par le canal téléphonique, le moins sécurisé depuis 30 ans »*.

De nouveaux terrains de chasse

Si Pindrop est bien implanté dans le secteur financier, assurances comprises, la solution s'ouvre maintenant sur d'autres secteurs comme la distribution, la santé ou l'automobile. Plus généralement, Pindrop se positionne sur les domaines où les appels sont en masse ou sur la sécurisation de transactions sensibles. Dominique Ango explique : *« Il est possible de contrôler de manière précise la voix des personnes et un simple bonjour suffit à contrôler que c'est bien la bonne personne »*.

Une approche multi-facteurs

La solution de l'éditeur utilise plusieurs vecteurs qui traquent des signaux faibles pour construire le profil de l'appelant. Ces éléments analysent le matériel (codecs utilisés, les fréquences…) et certaines caractéristiques comme la vitesse et la fréquence des frappes sur les touches du matériel, ou le réseau utilisé. Le dirigeant le précise : *« Les fraudeurs ont souvent la tentation d'utiliser des réseaux alternatifs comme des MVNO ou des solutions de VoIP »*. Avec la capture de ces différents signaux faibles, la solution arrive à un niveau de fiabilité intéressant avec 80% de détection des fraudes mais aussi l'assurance d'avoir servi le bon client et donc d'améliorer sa satisfaction. Sur les cas restants, une alerte est émise vers des équipes dédiées pour investigation et vers le conseiller avec la possibilité de passer sur une procédure d'identification différente.

Dominique Ango précise : *« les données collectées sont des données techniques et à part le numéro de téléphone il n'y a pas de données personnelles dans le référentiel qui reste sous le contrôle du client »*. Il est possible de déployer la solution sur AWS, et le backend de Pindrop est sur les infrastructures de cet hyper-scaler, et le but est de devenir Multi plate-forme rapidement.

Dominique Ango concède cependant que la détection des fraudes téléphoniques est peu avancée en France et qu'un travail de préparation comme aider à construire un historique des appels, et d'évangélisation sont nécessaires. ☐

B.G

AWS Summit

AWS veut rassurer son écosystème

Pour son événement français, AWS avait choisi le cadre du Palais des Congrès pour rassembler l'ensemble de son écosystème, clients, prospects, partenaires… Lors de cette manifestation, AWS a tenu à répondre aux différents points de critiques que sa plateforme peut rencontrer et a largement mis en avant les réalisations de ses clients.

Avec plus de 130 sessions, une cinquantaine de témoignages de clients et un panel de sponsors et de partenaires, AWS a vu les choses en grand, un peu à l'échelle de l'entreprise. Julien Groues, directeur général d'AWS pour la France, est revenu sur le contexte de la pandémie qui affecte toujours notre quotidien et la tendance forte des entreprises à se lancer dans une vaste transformation numérique qui a créé une sorte de « distorsion du temps » où tout s'accélère sur de nouveaux outils.

Un contrat de confiance

Il a ensuite énuméré les différents avantages d'AWS mais aussi évoqué les buts de l'entreprise. *« Nous devons gagner la confiance de nos clients, c'est le fondement de notre activité »*. Et de poursuivre avec les avantages dont les clients peuvent bénéficier : des coûts trois fois moins chers que dans leurs centres de données, une simplification du stack avec des services managés et la création de la région de Paris qui redonne au client le contrôle dont celui sur le chiffrement. Le client peut utiliser les outils d'AWS ou d'autres mais garde le contrôle sur les clés. Il a de plus mis en avant le garde-fou que crée les clauses contractuelles types qui vont au-delà du RGPD et des demandes du droit européen.



Julien Groues, directeur général d'AWS pour la France.

Démocratiser l'informatique

Il a poursuivi son intervention avec les différentes actions d'AWS autour de la formation et de la durabilité. Ainsi pour aider à améliorer la compétitivité des entreprises, AWS s'emploie à offrir des opportunités de formation. L'entreprise a déjà prodigué plus de 29 millions de formation dans 200 pays. Un demi-million de celles-ci sur la France. La société propose de plus des cours gratuits en ligne pour des formations plus ou moins intensives à travers 11 programmes dont le programme re/Start annoncé en début d'année. Pour rappel, ce programme est un ensemble de formations et réinsertions des personnes éloignées de l'emploi dans une carrière dans le cloud. Le programme a pour objectif de fournir des opportunités professionnelles à des personnes sans emploi ou sous représentées dans le milieu de la technologie, tout en répondant aux besoins de recrutement des employeurs. Le programme s'adresse aux personnes sans emploi, y compris aux anciens combattants, à leurs familles et aux jeunes.

DES ANNONCES DE PARTENAIRES

Toucan Toco a profité de l'événement pour intégrer le programme ISV Workload Migration qui aide les clients à migrer leurs solutions vers AWS via un processus de migration reproductible. Alter Way, dans le giron de Smile, a présenté un mini Green Book pour ses offres sur AWS respectant une approche durable sous le vocable Green Ops. Centreon a annoncé un accord de collaboration stratégique avec Amazon Web Services (AWS) pour héberger Centreon Cloud, sa nouvelle plateforme de supervision en mode SaaS (Software as a Service). Annoncée lors du Centreon Summit 2021, Centreon Cloud est une nouvelle plateforme de supervision informatique en mode SaaS pour les organisations quelle que soit leur taille. Après une phase bêta réussie en collaboration avec des clients sélectionnés, Centreon Cloud est entré dans une phase de Controlled Availability pour six mois et est désormais commercialisée dans certaines régions depuis le 1er mars 2022. Cette offre SaaS sera disponible sur tous les marchés dans le courant de l'année.

Au secours de la planète

Il a continué sur les avantages environnementaux et les engagements d'AWS en la matière. Selon lui, l'infrastructure AWS est cinq fois plus économe en énergie qu'un centre de données moyen européen. Il a évoqué le processeur maison, le Graviton qui est deux à plus de trois fois plus efficace que les autres CPU en termes de consommation électrique. Amazon a annoncé ainsi 37 nouveaux projets d'énergie renouvelable à travers le monde, marquant ainsi son objectif d'alimenter 100% de ses opérations à l'aide d'énergies renouvelables d'ici 2025 - cinq ans avant l'objectif initial de 2030. Pour la France, Amazon a annoncé son deuxième projet solaire à Préchac, en Gironde, ce qui porte à 38 MW la capacité totale d'énergie renouvelable annoncée à ce jour par l'entreprise en France. Il complète le site de Saint-Frichoux près de Carcassonne.

Le Cloud pour le long terme

Après le Directeur général, Sébastien Stormacq, Principal Developer Advocate, est monté sur scène pour lancer un appel : *« Ne laissez pas le passé pour définir votre futur »*. Pour lui, il se place évidemment dans le Cloud qui est un choix de moyen ou long terme. Il a insisté sur la puissance et les bénéfices que les clients peuvent tirer des offres d'AWS. D'ailleurs, il remarque que 90 % des innovations sur la plate-forme proviennent des demandes des clients. Au centre des innovations apportées par AWS, Sébastien Stormacq a évidemment fait l'article de la nouvelle puce Graviton que nous avons présenté dans un article précédent à la fin de l'année dernière. Les économies sont aussi

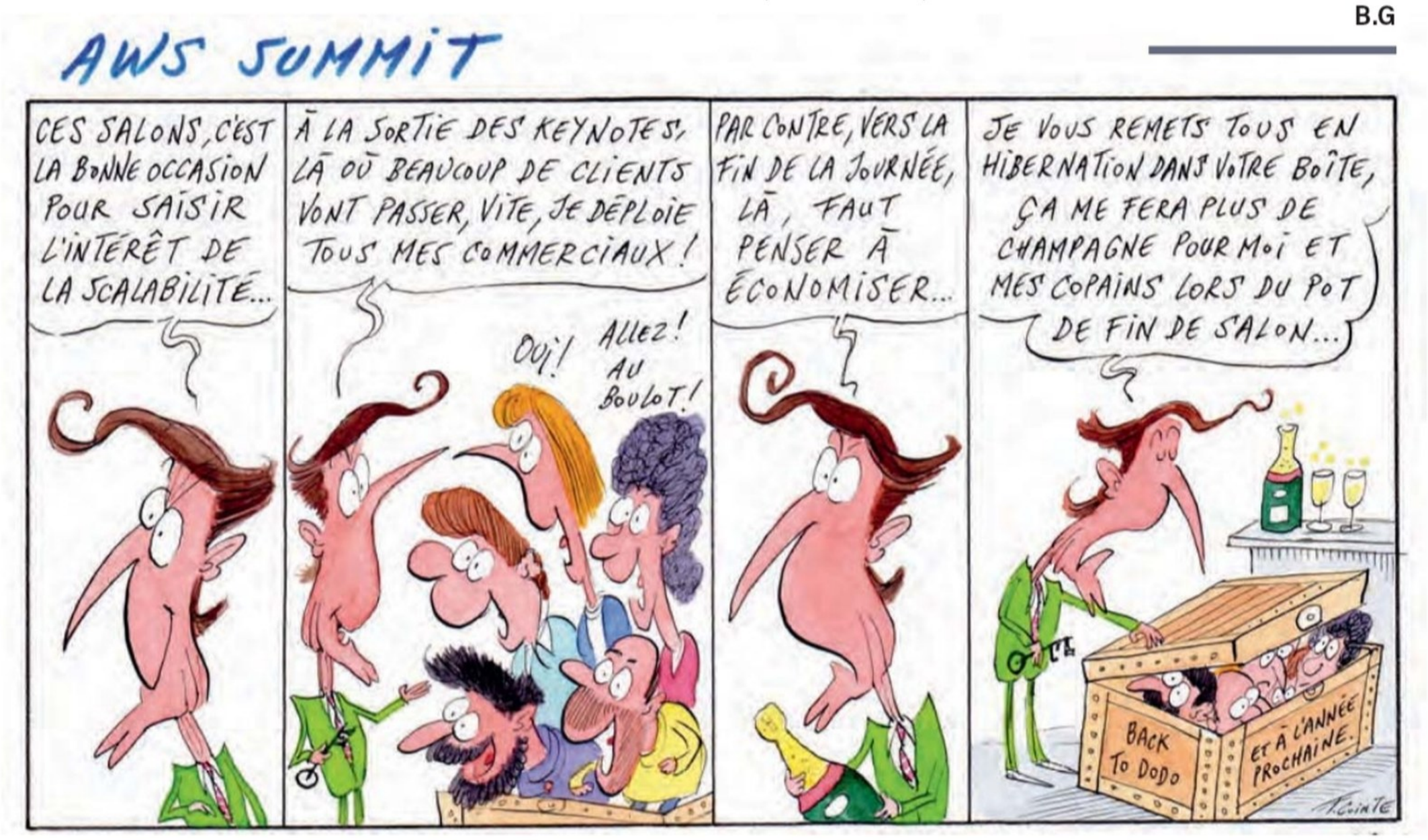


Ambiance de l'exposition durant l'AWS Summit.

un point fort pour le fournisseur de cloud public dont les workloads permettent de réduire de 80 % la consommation d'énergie comparativement à un centre de données habituel. Il a ensuite insisté sur le nombre d'instance utilisé par les clients en citant l'exemple d'EC² qui a été utilisé 60 millions de fois, soit deux fois plus qu'en 2019 et de la possibilité de les utiliser dans des zones localisées pour une moindre latence, ainsi que la combinaison avec Outpost pour les environnements hybrides pour le même résultat.

Au final, AWS a mis l'emphase sur le green et a tenu à répondre aux principales critiques qu'on peut lui adresser sur la protection des données personnelles ou sa propension à enfermer le client en étalant ses partenariats pour prouver son ouverture et avec moult clients aux grands noms sur scène ou dans les sessions pour démontrer les capacités de la plate-forme. □

B.G



RPA no code

Ideta : une solution no code pour créer des chatbots

Le marché des chatbots a littéralement explosé ces dernières années et touche désormais la quasi-totalité des secteurs d'activités. Outre les progrès technologiques de l'intelligence artificielle et du machine learning qui améliorent sans cesse leur fiabilité, les robots conversationnels sont devenus de plus en plus simples à créer grâce notamment aux technologies no code.



L'histoire des chatbots remonte aux prémices de l'informatique avec « ELIZA » qui avait été créé en 1966 pour simuler un psychothérapeute rogérien. Il s'agissait d'un programme informatique chargé d'analyser les mots clés de phrases écrites par des patients pour les reformuler sous forme de questions et instaurer un dialogue avec eux. Aujourd'hui, ces programmes ne sont plus seulement conçus sous la forme de questions/réponses. Grâce aux évolutions technologiques, les plus sophistiqués sont devenus de véritables assistants virtuels capables d'apprendre par eux-mêmes, interagir en langage naturel avec les utilisateurs, les conseiller, leur faire des suggestions, *etc.* Disponible 24h/24 et 7j/7, ils constituent désormais un outil de communication indispensable pour les entreprises que cela soit pour le support client de leur site Internet, leurs réseaux sociaux, ou leur Intranet. Face à la demande croissante des chatbots, des start-ups comme Ideta ont développé des solutions innovantes permettant de développer un agent conversationnel sans avoir à écrire une seule ligne de code. □

« Selon les prévisions de Research and Markets, le ***marché ultra concurrentiel des chatbots*** *qui a généré plus de 17 milliards de dollars en 2020* ***pourrait atteindre 102 milliards de dollars*** *en 2026 »,*

Sarah Martineau, cofondatrice et CEO d'Ideta, a développé une plateforme qui permet d'aider les entreprises à créer très facilement des agents conversationnels.

Pouvez-vous nous présenter Ideta ?

Ideta est un logiciel qui permet de créer facilement des chatbots («voicebot» ou «callbot») de manière très simple, mais avec quelques particularités. On est multicanal, donc on va pouvoir créer son bot et ensuite le déployer sur à peu près tous les canaux possibles de communication, dont, Facebook, Messenger, Teams, Slack (pour les bots en interne), etc. Il peut s'agir de «callbot» pour les «call center», ou juste d'un petit «live tchat» pour un site web. Le point important, c'est que l'on peut mettre de l'IA, et on est indépendant de la technologie que l'on utilise, car il existe plusieurs algorithmes de reconnaissance du langage. On

propose à nos clients les algorithmes les plus performants, dont ceux de Google, Amazon, et Microsoft. Nos clients peuvent choisir l'IA avec laquelle ils veulent travailler et la changer à tout moment.

L'utilisation de ces IA est-elle payante ?

Lorsque l'un de nos clients comme Carrefour par exemple connecte son propre compte « Dialogflow Google » sur notre plateforme, il paye directement l'IA, si toutefois celle-ci devient payante. Pour tous ces algorithmes-là, il faut savoir que c'est gratuit tant que vous ne franchissez pas un certain seuil d'échange avec les utilisateurs. Ce seuil est grand, car nous avons de gros e-commerçants avec un important trafic comme Alinéa qui utilisent « Dialogflow » et qui ne payent toujours pas. Pour l'instant, on peut donc dire que l'accès à ces IA n'est vraiment pas cher, voire gratuit.

Quel est l'intérêt pour les entreprises de passer par votre plateforme ?

Notre force réside dans le fait que notre outil est « no code » et qu'il permet vraiment à n'importe qui de créer son chatbot. À l'inverse, si on veut créer directement un chatbot avec « Dialogflow », cela signifie qu'il faut recréer toute une infrastructure autour. C'est juste un algorithme, donc on ne peut pas s'en servir facilement. Il faut développer l'infrastructure pour envoyer et recevoir des messages, les interpréter, les envoyer à l'IA, faire en sorte que l'IA donne une réponse, programmer quel message choisir en fonction de cette réponse, etc. Toute cette partie-là, c'est nous qui nous en occupons. Tout se passe dans la plateforme d'Ideta dans laquelle notre client va venir programmer son flot de chatbot, mettre des conditions et faire aussi de l'automatisation. Nous avons tout fait pour simplifier au maximum l'usage de l'IA. C'est-à-dire que nos clients peuvent faire apprendre de nouvelles phrases à leur chatbot sans être « data scientist » ou développeur. La plus-value d'utiliser Ideta, c'est aussi que si un jour « Dialogflow » ou une autre IA devient payante ou moins performante que la solution de RazrCorp ou Stanford par exemple, il est possible de modifier l'algorithme en un clic ! L'apprentissage de l'IA se fait sur Ideta et non sur l'algorithme.

Quels sont les différents types de chatbot et à quoi servent-ils ?

Il existe trois grands types de chatbot avec pour chacun des usages très différents. Le premier est un chatbot dit « scénarisé » dans lequel il n'y a pas d'intelligence artificielle. Ce sont des « clics boutons » sous forme de questions/réponses : « Êtes-vous une femme ou un homme ? » , puis un bouton pour « Femme » et un autre pour « Homme ». On clique sur l'un ou sur l'autre et on avance dans des scénarios. C'est ce que nous appelons les chatbots scénarisés, et cela fonctionne très bien. Le deuxième type de chatbot est celui qui intègre de l'IA. Ce n'est pas uniquement du clic bouton, on laisse l'utilisateur parler. Cela nécessite d'utiliser des algorithmes d'IA que l'on appelle « NLP ». Le dernier type de chatbot, c'est celui qui va faire en plus de l'automatisation. On programme des choses dans le chatbot pour qu'il fasse des actions. Imaginons par exemple que la personne a fait une demande de livre blanc, on va programmer le chatbot pour qu'il envoie lui-même un email afin que la personne reçoive son livre blanc par email. On va pouvoir ainsi automatiser plein de tâches, mettre des informations dans un CRM, aller chercher des informations dans une base de données, etc. Ce chatbot avec de l'automatisation est vraiment selon moi le plus pertinent et le plus intelligent. Après, il y a les cas d'usages très variés. Cela peut être du simple « live chat » sur une page web où il n'y a même pas de bot. C'est juste un échange entre un humain et un autre. On peut dire qu'il s'agit de la première étape, mais celle-ci est tout à fait réalisable avec Ideta. La seconde étape permet de programmer par exemple quelques bulles sur un site internet pour récolter des adresses email, aider à naviguer sur le site, etc. Après, on a des cas d'usage beaucoup plus variés dans des grandes entreprises comme des « chatbot RH ». Ils vont servir à renseigner les collaborateurs sur des questions telles que : « Combien de jours de congés il me reste », « Je vais être papa, à quoi j'ai droit ? » , etc. Dans ce cas, on se connecte aux outils internes du service « RH » de l'entreprise pour aller chercher les informations et les donner aux employés qui en font la demande. Il y a bien sûr aussi le chatbot pour le support client que les entreprises peuvent utiliser sur leur site web et/ou leur intranet. Je dirais que 70% de nos clients sont plutôt sur du support que ce soit en interne pour du RH ou autres, ou sur de l'externe.

Quel est le coût pour développer un chatbot sur Ideta ?

Nos coûts sont parmi les plus bas du marché, car on considère que nos clients sont autonomes pour créer des chatbots sur notre plateforme. Avec la plupart de nos concurrents, la programmation d'un « setup » peut coûter jusqu'à 100 000 €. Ce qui fait monter le prix, c'est toujours l'accompagnement. En fonction de la demande de l'entreprise, cela peut faire grossir l'assiette. Malgré cela, notre prix initial, qui se situe autour de 17 000 € par an, est vraiment très faible par rapport à la moyenne des solutions de chatbot. □

J.C



Sarah Martineau, cofondatrice et CEO d'Ideta.

Partage de données

Le **Samusocial de Paris** centralise ses données

Pour le groupement d'intérêt public, acteur de la lutte contre la grande exclusion, le partage des informations relatives aux personnes et aux familles rencontrées est un enjeu majeur, pour des questions notamment de suivi. Le Samusocial s'appuie depuis 2019 sur le Français NetExplorer, qui lui fournit une plateforme de stockage et de collaboration autour de ces données.

On trouve des cas d'usage de la donnée là où on ne l'attend parfois pas. C'est le cas au Samusocial, dont la parenté revient à Xavier Emmanuelli, créateur des équipes Mobiles d'Aide en 1993 et fondateur du Samusocial de Paris, constitué en groupement d'intérêt public (GIP) l'année suivante. Sa mission, depuis ses débuts, est de venir en aide aux personnes en détresse physique et sociale, à l'aide de maraudes et d'un numéro d'urgence, le 115. Afin de lutter contre la grande exclusion, le GIP et les nombreuses entités partenaires en Île-de-France, de la Croix Rouge à l'Ordre de Malte en passant par les Restos du Cœur ou encore la Protection Civile, produisent et échangent des données sur les personnes et les familles rencontrées. *« Pour la faire courte et simple, on a besoin d'un "CRM" comme n'importe quelle entreprise, à la différence qu'on ne vend rien : nous avons besoin d'informations pour comprendre la situation de la personne, avoir un meilleur suivi et coller au mieux aux besoins »* détaille Frédéric Lamagdelaine, chef de projet informatique au Samusocial de Paris.



ORASH est le portail de NetExplorer utilisé par le Samusocial, les huit Plateformes départementales d'accompagnement social à l'hôtel et l'opérateur de réservation Delta.

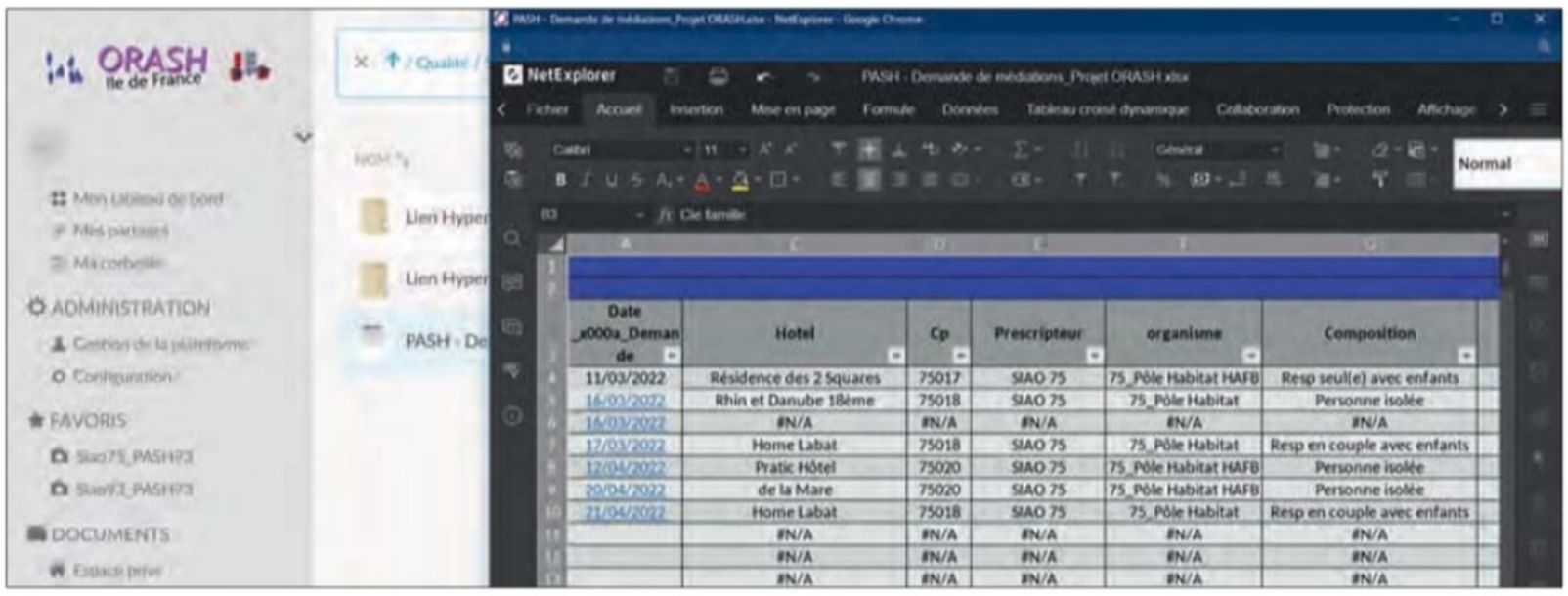
Du mail au Cloud

« Initialement, les équipes partageaient leurs données par des feuilles Excel déposées sur l'Intranet » nous explique-t-il. Un Intranet qui requiert une connexion VPN, posant des problèmes en termes d'usages à des médecins, infirmières et travailleurs sociaux qui, non seulement, ne sont pas formés à l'informatique, mais en plus, travaillent bien souvent sur le terrain, avec leur smartphone pour seul terminal à disposition. Sans compter les accès à ouvrir pour les tiers, associatifs notamment, qui ont eux aussi besoin de communiquer des informations sur les personnes rencontrées lors de leurs maraudes. Frédéric Lamagdelaine poursuit : *« À la demande de la Cnil, ces feuilles Excel ont été compressées, protégées par mot de passe et envoyées par mail »*. Ce qui oblige à de nombreux allers-retours, d'autant qu'il ne suffit pas d'envoyer un seul mail. Le mot de passe du fichier était communiqué dans un second mail.

Or, la masse de données à partager est conséquente : le Samusocial de Paris représente plus de 28000 rencontres avec des personnes et des familles en difficulté, plus les 685 hôtels partenaires et les 660 places d'hébergement réparties dans 219 communes. Et de nombreuses actions allant de l'accompagnement social à la médiation en passant par le 115, les soins en Lits Halte Soins Santé (LHSS) et Lits d'Accueil Médicalisés (LAM) ou encore l'hébergement, que ce soit en Centre d'Hébergement d'Urgence ou à l'hôtel. Pour cette dernière partie, les réservations sont effectuées par l'opérateur spécialisé Delta, qui lui aussi utilise ces données, et en produit en retour. C'est dans ce contexte qu'arrive, en 2019, NetExplorer, une PME française d'une vingtaine de salariés, spécialisée dans la gestion de documents dans le cloud, qui met en place pour le Samusocial de Paris une plateforme de partage documentaire.

4_93722684

Simplicité d'usage et d'accès



La plateforme permet de travailler à plusieurs sur un même tableur, sans avoir à télécharger le document. Ce qui évite d'avoir à souffrir de l'hétérogénéité des versions d'Excel utilisées par les agents du Samusocial.

« Ce qui nous a plu chez NetExplorer, c'est la coédition. En effet, le parc Excel chez nous est très hétéroclite, on doit encore pouvoir trouver du Excel 2003 » raconte Frédéric Lamagdelaine. La plateforme Cloud mise en place par l'entreprise permet ainsi à plusieurs personnes de collaborer en même temps sur le même tableur OnlyOffice intégré, après avoir uploadé sur le service leurs propres fichiers Excel. *« Chaque mission fait un import simple, bête et méchant, depuis la trame qu'ils ont l'habitude d'utiliser »* indique le chef de projet. L'outil n'est pas sans défaut, puisque si un utilisateur choisit d'ouvrir le fichier en local, il est alors impossible de travailler à plusieurs sur le document. Heureusement, l'outil de NetExplorer prévient les autres utilisateurs et, pour le service informatique, *« il suffit de simplement demander d'utiliser directement le tableur intégré »*, précise Frédéric Lamagdelaine, ajoutant au passage que les sauvegardes automatiques sont un gros plus : personne n'est à l'abri d'une suppression maladroite. Le stockage centralisé et le partage ne sont toutefois pas les seuls avantages présentés par NetExplorer : l'entreprise est française et héberge les données en France, sur ses propres serveurs dans des datacenters *« Tier 3+ et 4 »*, avec une sauvegarde effectuée dans un second lieu, mais toujours sur le sol national.

La plateforme est en outre certifiée ISO 9001 et 27001, et surtout HDS, une quasi-obligation pour le Samusocial dont les équipes remontent fréquemment des données de santé dans le cadre de leurs missions. Ajoutons à cela que la solution fonctionne via un portail web mais aussi une application mobile, *« pratique car nous avons des missions sur le terrain et qui ont besoin d'avoir le service sur leur téléphone »*. Et ça reste toujours moins complexe à configurer qu'un tunnel VPN. Les données sont ainsi immédiatement accessibles aux équipes qui restent, elles, sédentaires et assurent notamment la demande de places d'hébergement, ainsi qu'un suivi sur la durée des personnes rencontrées. Les fonctionnalités de contrôles des accès et des groupes, de provisionnement, de suppression de comptes et des droits adaptés à la volée (et à distance) complètent l'ensemble, un ensemble commercialisé à un prix adapté au secteur du social, un menu détail qu'il serait dommage d'oublier.

Un outil déployé à l'échelle régionale

Tout n'est pas parfait cependant, les utilisateurs avancés au sein du Samusocial déplorent notamment que *« NetExplorer ne sache pas faire de RECHERCHE entre plusieurs feuilles Excel, c'est un peu dommage »* déplore Frédéric Lamagdelaine. Pour autant, l'outil convient en interne, tant et si bien que, début 2020, la solution est présentée à la DRIHL (Direction régionale et interdépartementale de l'hébergement et du logement) afin que les huit PASH (Plateformes départementales d'accompagnement social à l'hôtel) l'intègrent, de même que Delta, l'opérateur de réservation de chambres d'hôtel. Le portail ORASH est né. *« Nous avions proposé à la DRIHL un outil pour que les PASH et Delta puissent communiquer entre elles. Les PASH sont régionalisées : à Paris, nous n'avons pas forcément de place d'hébergement disponible pour répondre à toutes les demandes, ce qui nous oblige de les envoyer dans des hôtels en Seine-Saint-Denis ou en Seine-et-Marne, où les PASH les prennent en charge. Donc, bien sûr, il est nécessaire d'échanger des informations pour assurer le suivi des demandeurs »* note le chef de projet.

Dans ORASH, rien de compliqué, les fichiers sont partagés par le biais de dossiers, accessibles ou non en fonction des droits, fonctionnant sur le principe d'une arborescence comme sur tout système Windows ou Mac. Ainsi, en cas de problème d'une personne hébergée dans un hôtel, les médiateurs vont faire remonter vers Delta des données permettant d'identifier le demandeur, la date de la demande, l'hôtel, l'organisme prescripteur, les problèmes rencontrés. Inversement, Delta va sur le même document renseigner l'évolution de la situation : tout est ainsi centralisé de sorte à faciliter les démarches des agents et des entités impliquées. Autre point d'intérêt de la plateforme, ses API. Celles-ci sont principalement utilisées par Delta qui les exploite pour verser automatiquement sur ORASH ses PDF récapitulatifs. Car l'outil ne se limite pas qu'aux tableurs, mais permet le stockage et le partage de documents de tout type. *« Pour l'instant, les API sont utilisées dans le sens ascendant, et je ne pense pas que nous les exploiterons dans le sens descendant, de NetExplorer vers une application métier du Samusocial »* signale Frédéric Lamagdelaine. La principale évolution qu'il entrevoit à court terme est l'augmentation du nombre d'utilisateurs, plus d'une centaine au moment où nous écrivons ces lignes. Surtout, aux yeux du chef de projet, une chose compte plus que toute autre : *« Depuis 2019, la plateforme a toujours été accessible, nous n'avons jamais subi de coupure »*. ☐

Guillaume Périssat

4_93722684

Refonte SI

Papernest virtualise la gestion de son parc

Pour soutenir sa forte croissance, la jeune pousse française a refondu le parc informatique de certaines de ses équipes grâce à la solution ceBox de Wisper. Ainsi, quatre personnes à l'IT gèrent sans mal les postes de 300 salariés.

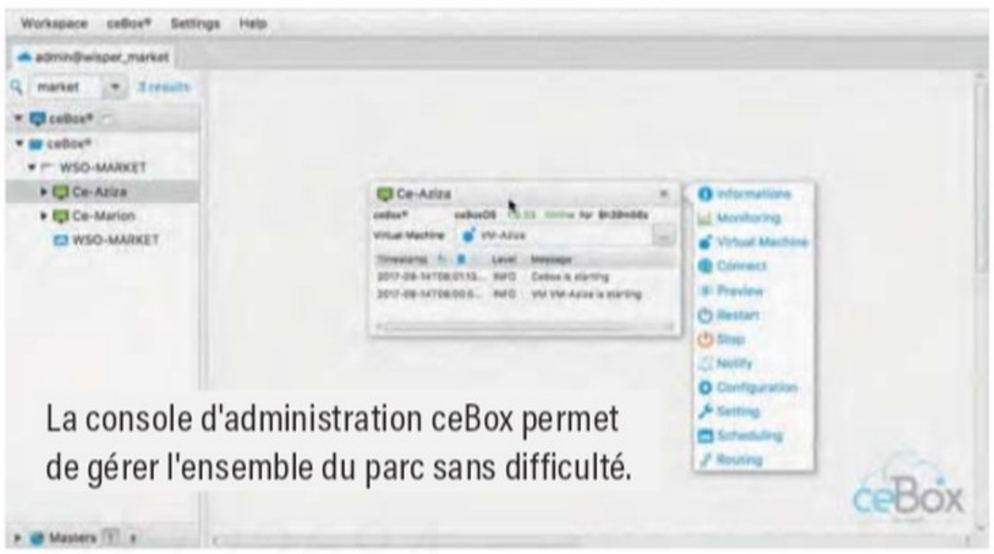
Jeune pousse née en 2015, Papernest aide les personnes qui déménagent à effectuer leurs démarches administratives et à gérer les contrats du foyer, par le biais d'une application web ou par téléphone. Depuis sa création, la scale-up a bien grandi : elle compte aujourd'hui un millier de collaborateurs à Paris, à Reims, à Barcelone et à Varsovie et a accompagné un million de clients en France mais aussi en Italie, en Espagne et en Grande-Bretagne.

Du fait de sa croissance, Papernest a dû très tôt repenser la gestion de son parc informatique. *« Au tout début, nous avions une politique assez simple : à chaque fois qu'un nouveau salarié arrivait, nous achetions une nouvelle machine dont le salarié était admin et qui avait sa procédure d'installation »* raconte Benoît Fabre, fondateur et CEO de Papernest. Une stratégie qui s'avère peu « scalable » à mesure que la société grossissait, d'autant que tous les salariés n'ont pas le même niveau d'engagement et de compétences sur ces sujets informatiques, d'où une perte de temps sur la maintenance.

Machine physique mais virtualisée

« En 2016, avec une quarantaine de postes, leur gestion devenait déjà compliquée » indique Benoît Fabre. Pour centraliser la gestion du parc, la jeune entreprise a envisagé trois solutions. D'une part, un serveur Windows avec une équipe IT compétente derrière, une option « vite éliminée ». De l'autre, du « full virtualisé », solution pour laquelle plusieurs tests sont effectués, mais qui posait une difficulté « majeure » en termes de bande passante. Finalement, c'est vers Wisper et sa solution ceBox que se tourne Papernest pour les postes de ses forces de vente et de support client.

ceBox, c'est d'abord une machine, un ordinateur, en l'occurrence des Intel NUC (Next Unit Computing) dans le cas de Papernest, fournie et louée par Wisper. Ce qui permet d'avoir un parc homogène. Ces terminaux tournent sous ceBox OS, un fork propriétaire de Linux installé par défaut sur toutes ces machines, mais au-dessus duquel peuvent être virtualisés d'autres systèmes d'exploitation, Windows par exemple. *« Wisper crée les masters et gère les licences. Nous avons ensuite une interface d'administration avec d'un côté les masters, de l'autre les machines »* explique le CEO de Papernest. *« La gestion du parc se fait alors par drag & drop d'un master vers une machine, ou par un simple système de règles »*.



La console d'administration ceBox permet de gérer l'ensemble du parc sans difficulté.

Rien sur le poste

Ainsi, et pour en détailler un peu le fonctionnement, la ceBox va télécharger à chaque démarrage les blocs du master dont elle a besoin. Des blocs qu'elle télécharge non pas sur Internet, mais via un serveur de cache local WSO2, équipé d'une version de ceBox OS dédiée WSO. En ce qui concerne les mises à jour, la console admin permet de déployer patchs et autres sur une seule machine, sur un groupe ou sur tout le parc. Il est en outre possible d'assigner un master différent en fonction des équipes et des rôles. L'utilisateur final n'a rien en local, à l'exception de quelques GPO de l'Active Directory.

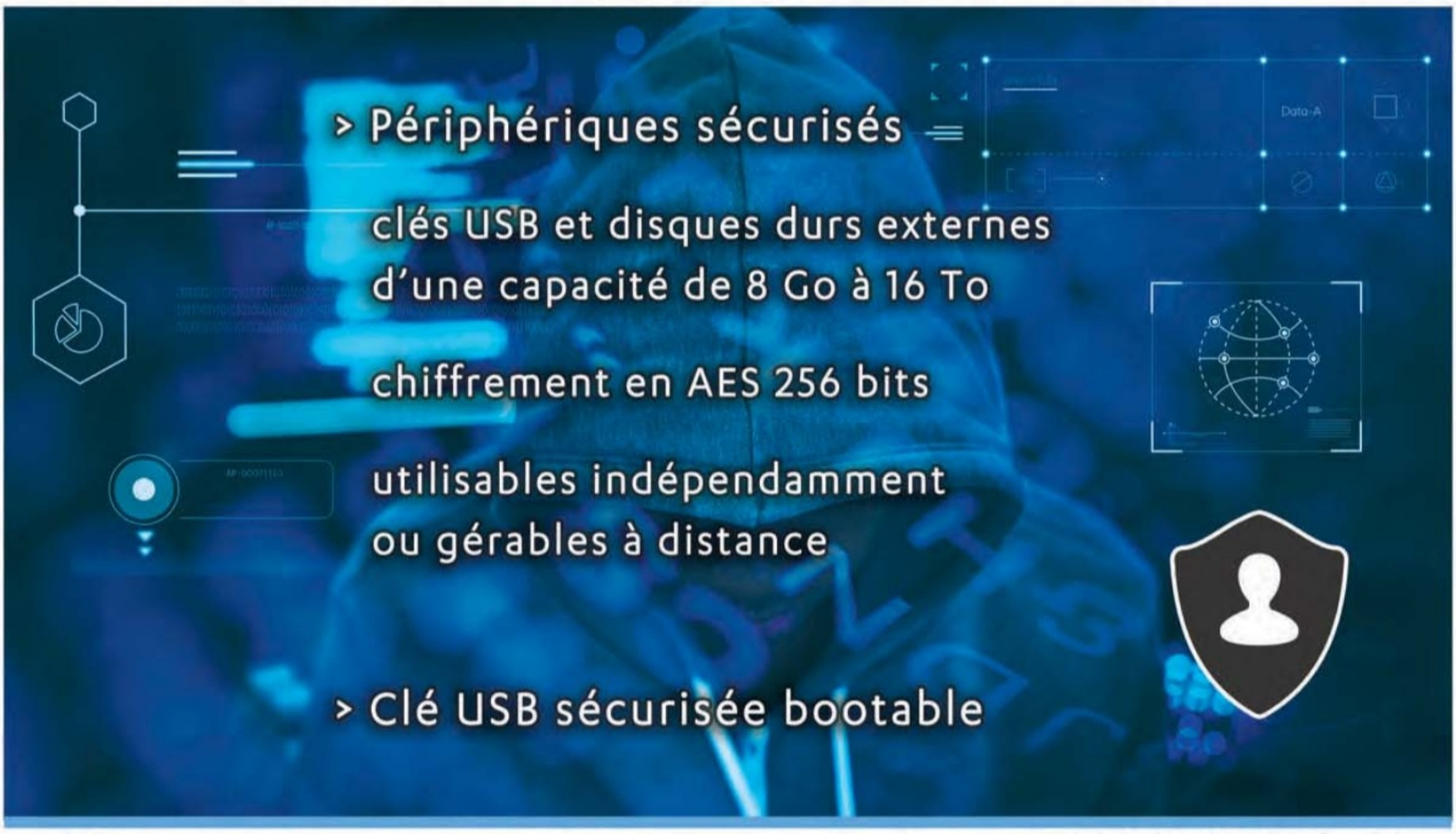
À partir de 2021, Papernest a mis en place la possibilité d'utiliser ceBox en télétravail, puisqu'il suffit au salarié de ramener chez lui son NUC, d'y brancher clavier, souris et écran et de pouvoir travailler. Puisqu'il n'est plus sur le réseau de l'entreprise, l'accès au WSO se fait via un tunnel VPN dont les paramètres sont récupérés sur le cloud de Wisper. L'employé n'a alors plus qu'à travailler sans autre réglage requis. *« Les ceBox sont utilisées par les équipes ventes et supports, soit plus de 300 personnes réparties sur plusieurs sites. Et les machines sont toutes gérées depuis une seule console, par une équipe IT de 4 personnes »* souligne Benoît Fabre. Et le nombre d'utilisateurs devrait à terme être étendu au centre d'appels commerciaux de Papernest, sans le moindre problème de mise à l'échelle du parc. □

Guillaume Périssat



Sécurisation des accès et des données

Solutions modulables protégeant de façon optimale votre parc informatique et vos informations numériques.



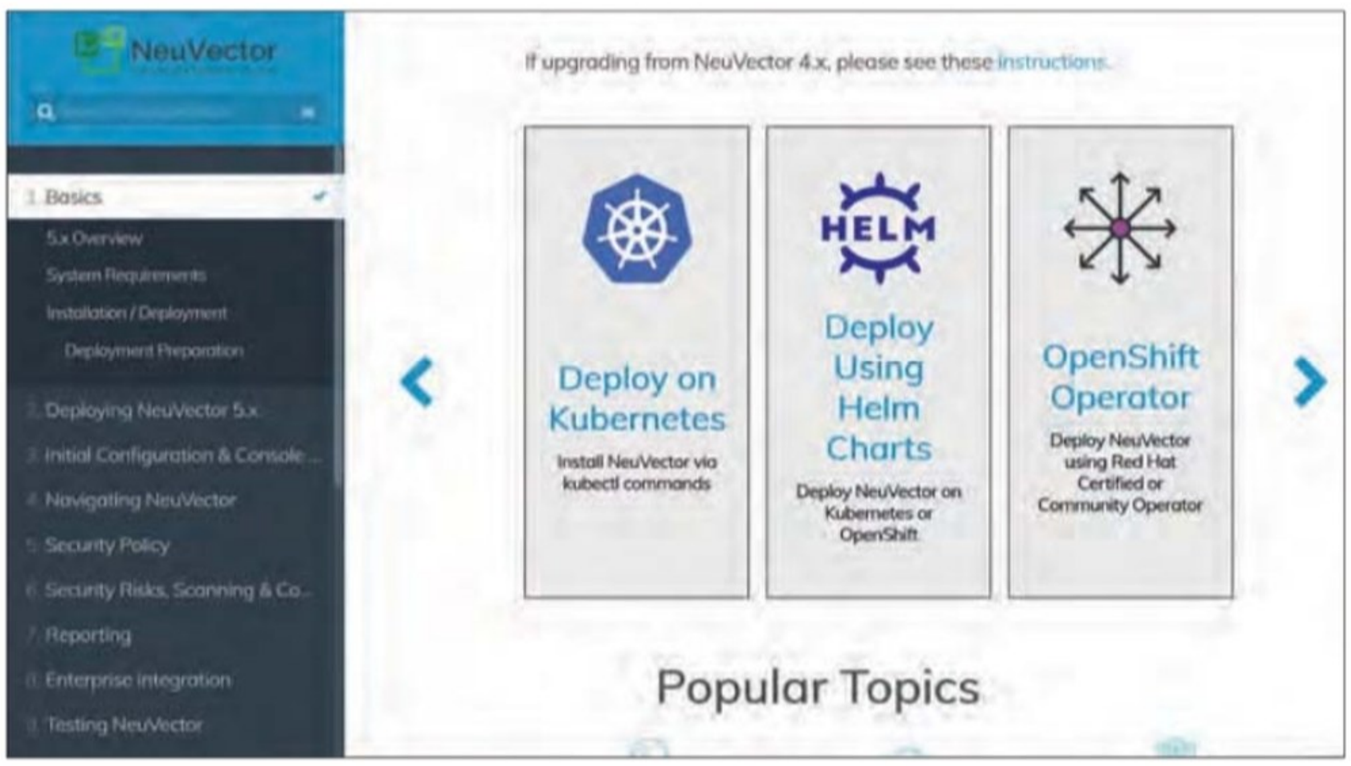
Query Informatique
www.query-informatique.com
1 bd Charles de Gaulle
92700 Colombes - FRANCE
Tél. : +33 (0)1 49 97 33 00

Renforcement de Kubernetes

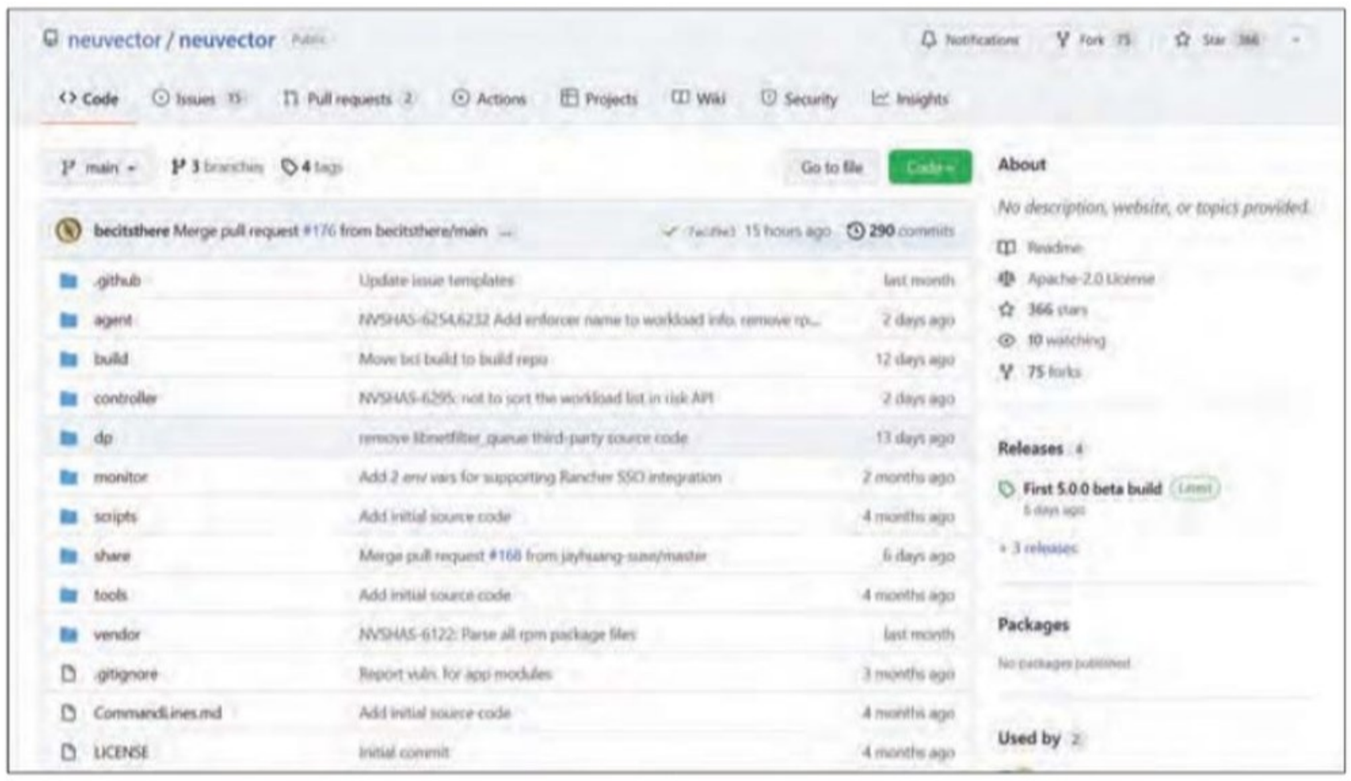
SUSE a fait basculer NeuVector dans l'open source

SUSE a annoncé que le code de base de NeuVector, la plateforme de sécurité de containers, est désormais passé en open source. Disponible sur GitHub, elle est sous licence Apache 2.0. Nous allons voir dans cet article ce que cela implique.

SUSE a fait l'acquisition en octobre 2021 de NeuVector, un logiciel offrant une sécurité de bout en bout pour les containers. Comme à son habitude après un rachat, le 18 janvier 2022, soit seulement 3 mois plus tard, SUSE a annoncé le passage de NeuVector en open source. SUSE a certainement fait cela pour en faire la technologie de prédilection dans ce domaine ainsi que pour contribuer à l'amélioration de la sécurité de Kubernetes. La version open-source de NeuVector peut être installée sur n'importe quel cluster Kubernetes. Il devrait également être possible, dans un futur proche, de l'installer depuis le catalogue d'applications Rancher. NeuVector devrait aussi supporter prochainement d'autres plateformes de gestion de containers comme Red Hat OpenShift, Google GKE, Microsoft Azure AKS et autres Amazon EKS. Le « modèle émergent » de la sécurité de l'exécution des conteneurs suscite un intérêt toujours croissant. En effet, les développeurs ont le devoir et surtout le besoin de protéger en permanence leurs charges de travail cloud-native éphémères – déploiement, testing et intégration. Il peut s'agir de « durcir » un cluster Kubernetes ou bien d'analyser de façon continue des comportements anormaux dans un conteneur après sa mise en production. Ce besoin, en termes de sécurisation des conteneurs, a donné lieu à une bataille en règle dans l'industrie avec, d'un côté, des startups bien dotées financièrement parlant telles qu'Aqua Security, Deepfence ou Sysdig et, de l'autre, des fournisseurs déjà très présents sur ce marché comme Palo Alto Networks avec TwistLock, Red Hat avec StackRox et, désormais, Suse avec NeuVector. Les fonctionnalités de NeuVector sont nombreuses et assez intéressantes : l'analyse en continu des vulnérabilités tout au long du cycle de vie des conteneurs, la segmentation des conteneurs pour une meilleure conformité, la sécurité d'exécution de bout en bout et, enfin, l'analyse réseau en profondeur à travers des terminaux mobiles (pods).



La documentation de NeuVector est disponible à l'adresse https://open-docs.neuvector.com.

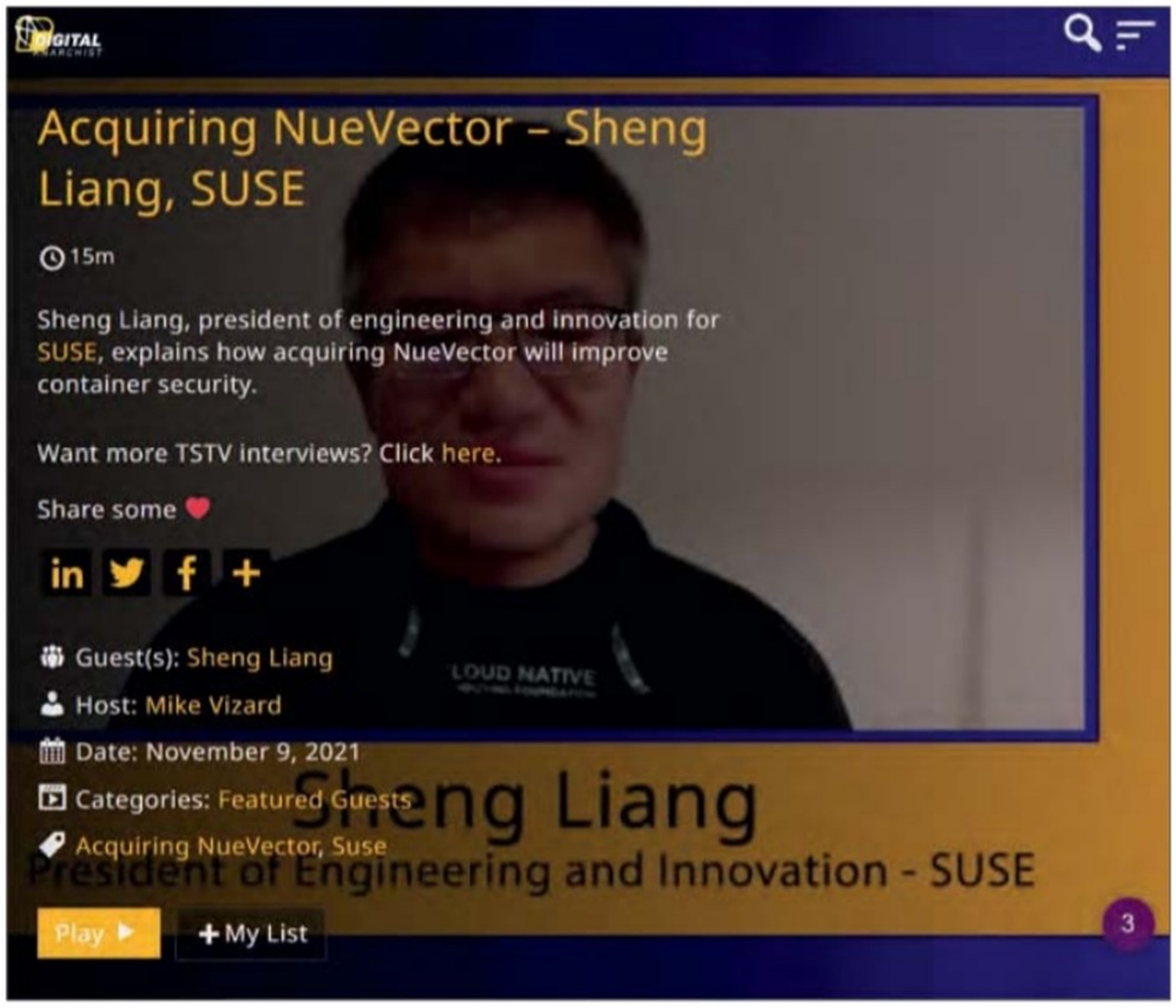


La plateforme de sécurisation NeuVector est disponible sur GitHub à l'adresse https://github.com/neuvector/neuvector) sous licence Apache 2.0.

À l'origine

La société NeuVector a été fondée en 2015 en Californie. Elle était spécialisée dans la sécurisation et la conformité des environnements Kubernetes. En plus d'un outil de scan des images intégré aux solutions CI du marché (comme CircleCI

ou Jenkins), l'éditeur a investi depuis ses débuts sur l'inspection approfondie des paquets réseau (Deep Packet Inspection ou DPI) jusqu'à la couche application afin de mieux surveiller les connexions entre les conteneurs ainsi que le trafic latéral. Conçu à l'origine pour les conteneurs Docker, NeuVector a étoffé sa solution afin qu'elle fonctionne aussi avec Kubernetes. NeuVector ne s'appuie pas sur un agent. Elle repose en fait sur plusieurs autres conteneurs (dont un contrôleur DaemonSet) compatibles avec la plupart des distributions Kubernetes et les CMP (Containers Management Platform) du marché que sont Amazon EKS, GKE, Microsoft Azure AKS, Red Hat OpenShift ou encore VMWare Tanzu. La condition à satisfaire est qu'elles soient associées à des plug-ins réseau (ou SDN pour Software Defined Network) tels que calico, flannel ou weave. Rappelons qu'un SDN est une architecture réseau « agile » qui sépare la gestion réseau de l'infrastructure réseau sous-jacente dans le but de simplifier la fourniture des ressources réseau.



Sheng Liang a également dit que *« l'un des aspects les plus impressionnants de l'approche de NeuVector était l'association de l'inspection réseau à la surveillance des comportements d'exécution de manière discrète »*.

Une plateforme de sécurisation complète

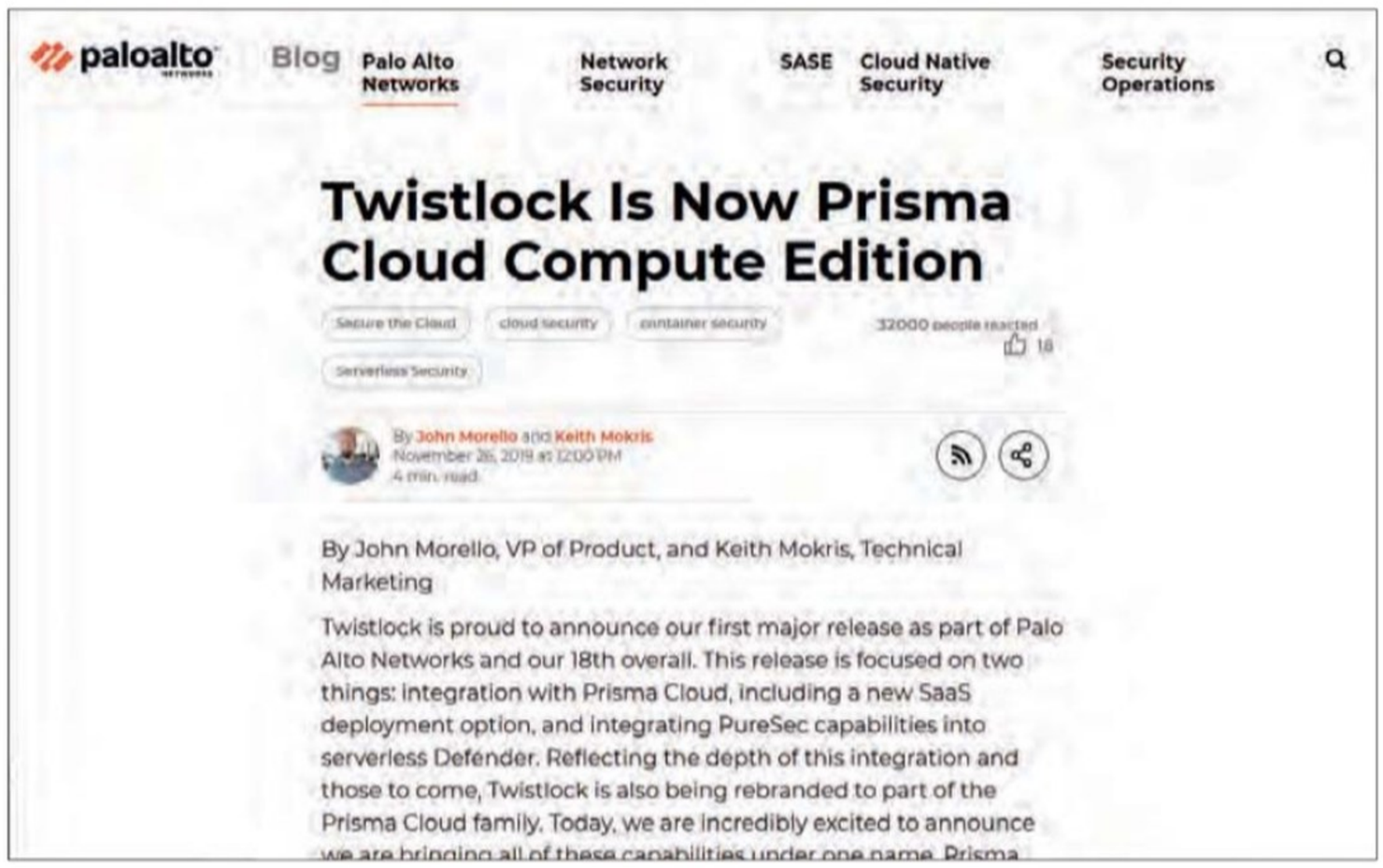
Même sans rentrer dans le détail de l'implémentation, la clef pour comprendre le fonctionnement de NeuVector est de savoir qu'il propose de nombreuses interfaces. Consoles web, API REST ou plugins CLI, elles permettent de surveiller et de protéger les activités réseau entre les différents nœuds d'un système conteneurisé. La plateforme découvre automatiquement les groupes d'hôtes ou de conteneurs internes et externes, comme ceux par exemple nécessaires à l'exécution d'une application ou qui permettent de configurer des règles de sécurité et de les appliquer.

Ces règles peuvent être créées aussi bien automatiquement que manuellement. Le logiciel est même capable de détecter des attaques DDoS, des tentatives d'injections SQL et du tunnelling. Son système de prévention de perte de données à base de filtres inspecte les paquets à la recherche de données sensibles qui ne seraient pas chiffrées. La plateforme peut aussi détecter automatiquement les tentatives d'escalades de privilèges, le scan des ports de la machine ainsi que le reverse Shell. L'outil procède en tentant d'identifier le comportement jugé normal de l'environnement de conteneur à surveiller et crée ensuite automatiquement des règles de whitelisting ou de blacklisting. Les équipes DevOps (et DevSecOps) peuvent importer ou exporter sous forme de CRDs (stockés dans des fichiers YAML) des règles depuis ou vers la plateforme afin de les faire appliquer dès la livraison en production.

INTÉGRATION AVEC RANCHER

Les images de conteneurs NeuVector peuvent désormais être installées sur presque n'importe quel cluster Kubernetes. La condition incontournable est que le cluster en question doit impérativement être certifié CNCF (Cloud Native Computing Foundation). NeuVector est également en cours d'intégration « en profondeur » avec la propre plateforme de conteneurs managés de Suse, Rancher, qui la proposera via son catalogue d'applications. *« Nous sommes convaincus que cette initiative participera à stimuler l'innovation dans le domaine de la sécurité de Kubernetes, secteur dominé traditionnellement surtout par des solutions propriétaires à code fermé »*, a déclaré dans un billet de blog le cofondateur de Rancher et désormais président de l'ingénierie et de l'innovation chez Suse, le sieur Sheng Liang. *« Cette décision de basculer en open source le code d'une technologie précédemment propriétaire montre clairement s'il en était besoin la culture communautaire de Suse et son engagement à fournir des solutions ouvertes, interopérables et innovantes »*, a encore déclaré M. Liang.

Tout un ensemble de tableaux de bord permet de visualiser depuis la console des scores de risques, les résultats des scans ou encore des benchmarks CIS (un conteneur nommé Updater contient une base de données CVE très régulièrement mise à jour). Un ensemble de filtres sert à vérifier la conformité à différents règlements (PCI, HIPAA, RGPD). Il est également possible d'intégrer NeuVector avec un SIEM (celui de Splunk, par exemple) ou avec des plateformes d'observabilité, même, éventuellement, des « maisons ». En effet, NeuVector dispose d'un exportateur vers Prometheus couplé à des tableaux de bord Grafana. SUSE a déclaré que lorsqu'il est question de sécurité de containers lors de la conception et l'exécution d'applications Kubernetes, le code de base de la plate-forme permettra aux utilisateurs de Rancher (l'outil de gestion de clusters Kubernetes) de résoudre les cas d'utilisation majeurs en termes de sécurité à travers le cycle de vie de l'application. Ceci inclut la visibilité, l'inspection et la segmentation en profondeur du réseau, la gestion des vulnérabilités, de la configuration et de la conformité, le profilage du risque, la détection de menaces et la réponse aux incidents. NeuVector a créé ce qu'il décrit comme un *« pare-feu de containers multi-vecteurs »* qui protège les réseaux de container de la couche 3 à la couche 7 du modèle OSI. Il détecte et affiche des informations sur les connexions en temps réel pour tout le trafic réseau des containers et peut facilement capturer des paquets réseau pour le débogage d'applications container et l'investigation. NeuVector segmente aussi automatiquement le trafic en se basant sur le comportement de la couche application, ce indépendamment des paramètres réseau. Cette fonctionnalité est particulièrement bien adaptée aux organisations qui s'orientent vers une approche zéro confiance en vue d'implémenter de bonnes pratiques DevSecOps à travers un environnement applicatif cloud-natif.



TwistLock de PaloAlto Networks est un des concurrents sérieux de NeuVector. Là aussi, il y a eu acquisition de technologie.

Sécurité et open source

Un doute plane en termes de sécurité concernant ce basculement dans l'open source du code. Si ce passage à une licence open source n'est qu'une étape de normalisation pour SUSE, il en est autrement chez NeuVector. Le 13 octobre dernier, l'éditeur annonçait l'obtention de deux brevets, le premier portant sur la notation des risques du cycle de vie des conteneurs et le deuxième sur la protection des Service Mesh (Istio et Linkerd 2). La société Neuvector se vantait d'être propriétaire de huit brevets. Si l'ouverture du code de NeuVector ne va pas forcément remettre en cause tous ces brevets, la plateforme de sécurité devra être compatible avec les distributions Kubernetes certifiées CNCF et son code accessible à tous depuis GitHub. Rappelons, côté concurrence, que Red Hat a acquis StackRox, un concurrent de NeuVector, en janvier 2021. L'éditeur au chapeau rouge a ensuite lancé la communauté open source liée à l'outil de sécurité en question en mai 2021. Cette première étape a précédé l'ouverture de la solution. Red Hat a, en parallèle, fait la promotion du projet KubeLinter, une solution d'analyse des fichiers YAML et des Helms charts mise aussi dans

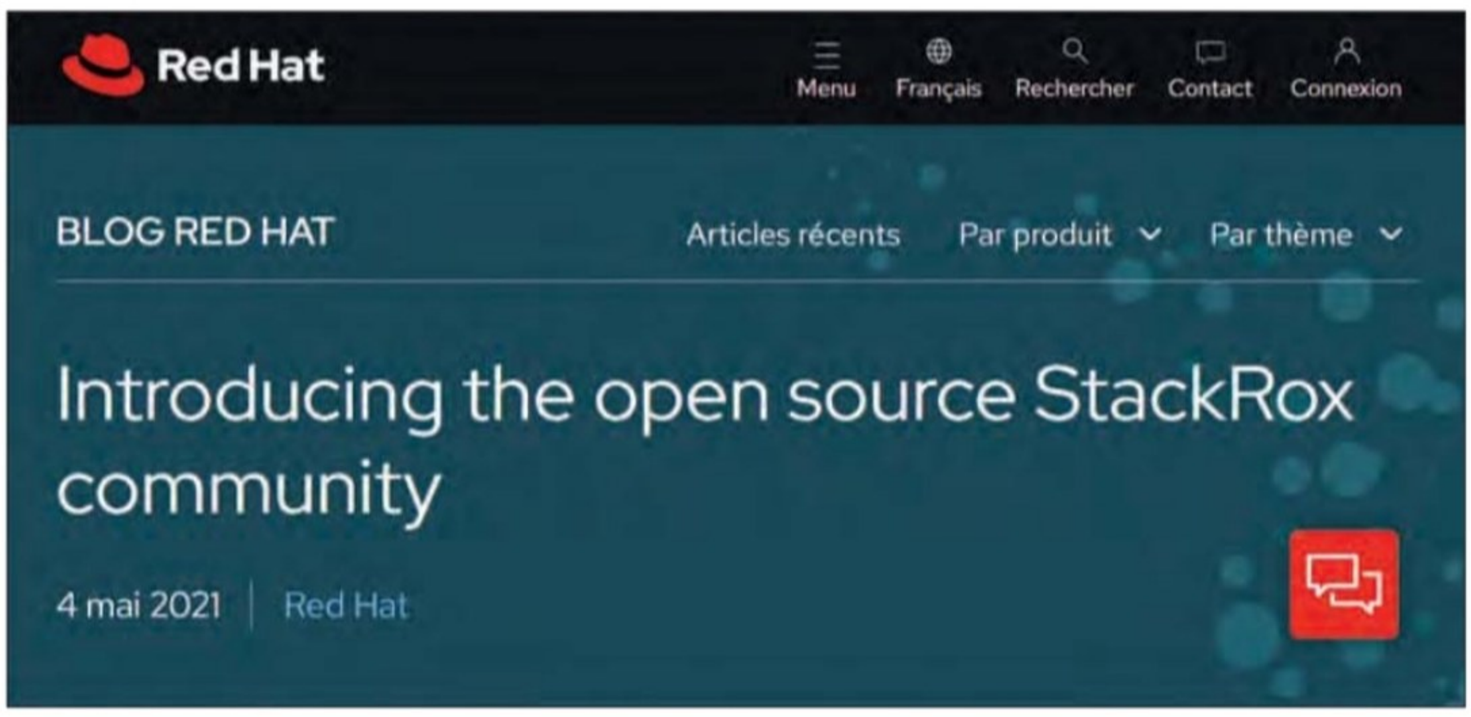
QUELLE ORIENTATION POUR SUSE ?

SUSE a acquis Rancher Labs fin 2020 pour obtenir un accès à la fois à un framework de gestion de clusters Kubernetes et à une instance organisée de la plateforme d'orchestration de container optimisée pour les environnements IT d'entreprise. L'entreprise d'outre-Rhin vise maintenant à étendre le champ d'action de son framework de gestion afin d'y inclure des plateformes de sécurité telles que NeuVector. *« Le défi et l'opportunité qui en découlent sont l'automatisation d'autant de processus de sécurité que possible d'une manière qui ne requière pas systématiquement des développeurs et des utilisateurs finaux pour implémenter manuellement un ensemble de bonnes pratiques DevSecOps »*, a déclaré Mister Liang. SUSE s'engage aussi sur le fait que NeuVector continuera à maintenir le support pour d'autres distributions Kubernetes telles que Red Hat, VMware et Mirantis. L'éditeur continuera à travailler en parallèle avec des vendeurs de solutions de sécurité cloud-natif tels que Aqua Security, Palo Alto Networks ou Sysdig.

RANCHER, LA **PLATE-FORME DE GESTION KUBERNETES PHARE** DE SUSE

Rancher est un logiciel SUSE de gestion de clusters Kubernetes multiples. Grâce à Neuvector, SUSE Rancher peut offrir une plateforme de sécurité intégrée à sa CMP (plateforme de gestion de contenu), conduisant à la monétisation du support associé. C'était déjà le cas avec SUSE Liberty Linux, une technologie mais aussi une offre de support permettant de mieux sécuriser différentes distributions Linux. NeuVector fournira aux clients employant une distribution Kubernetes certifiée CNCF une sécurité native pour leurs infrastructures et charges de travail de production. ***«Le projet NeuVector va permettre aux utilisateurs Rancher de résoudre des cas d'utilisation de sécurité majeurs à travers tout le cycle de vie de l'application. Le projet NeuVector sera le code derrière les fonctionnalités de sécurité de cluster avancées de Rancher»*** **a encore déclaré Monsieur Liang.**

l'open source mais cette fois par StackRox, juste avant son rachat. Néanmoins, même si le fournisseur germanique offre une solution avec un écosystème complet, il ne veut pas pour autant se fâcher avec des partenaires proposant des solutions similaires à ses clients. Que ce soit Aqua Security, Palo Alto Networks ou encore Sysdig — porteur du projet open source Falco incubé par la CNCF — tous proposent des offres de sécurisation des conteneurs. Pour, disons, ne pas les froisser, les responsables de SUSE et de NeuVector avancent prudemment leurs pions. Pour le moment, seul le code de la préversion de la v5 de NeuVector a été totalement ouvert. Il faut dire aussi que lors de l'annonce du rachat de StackRox par RedHat, certains clients communs à StackRox et la société rachetée par IBM s'étaient inquiétés des risques, en matière de sécurité, du passage à une licence open source. C'était notamment le cas de l'US Air Force, dont il est assez facile de comprendre les motivations sur ce sujet. Des produits comme ceux d'Aqua Security et Sysdig conservent des briques propriétaires pour cette raison essentielle. Le grave incident en matière de sécurité survenu avec Log4j (voir à ce sujet l'article paru dans le dernier numéro de CyberRisques) n'a laissé personne indifférent et a contribué aussi bien à des renfermements propriétaires qu'à des investissements massifs dans la sécurité des projets open source.

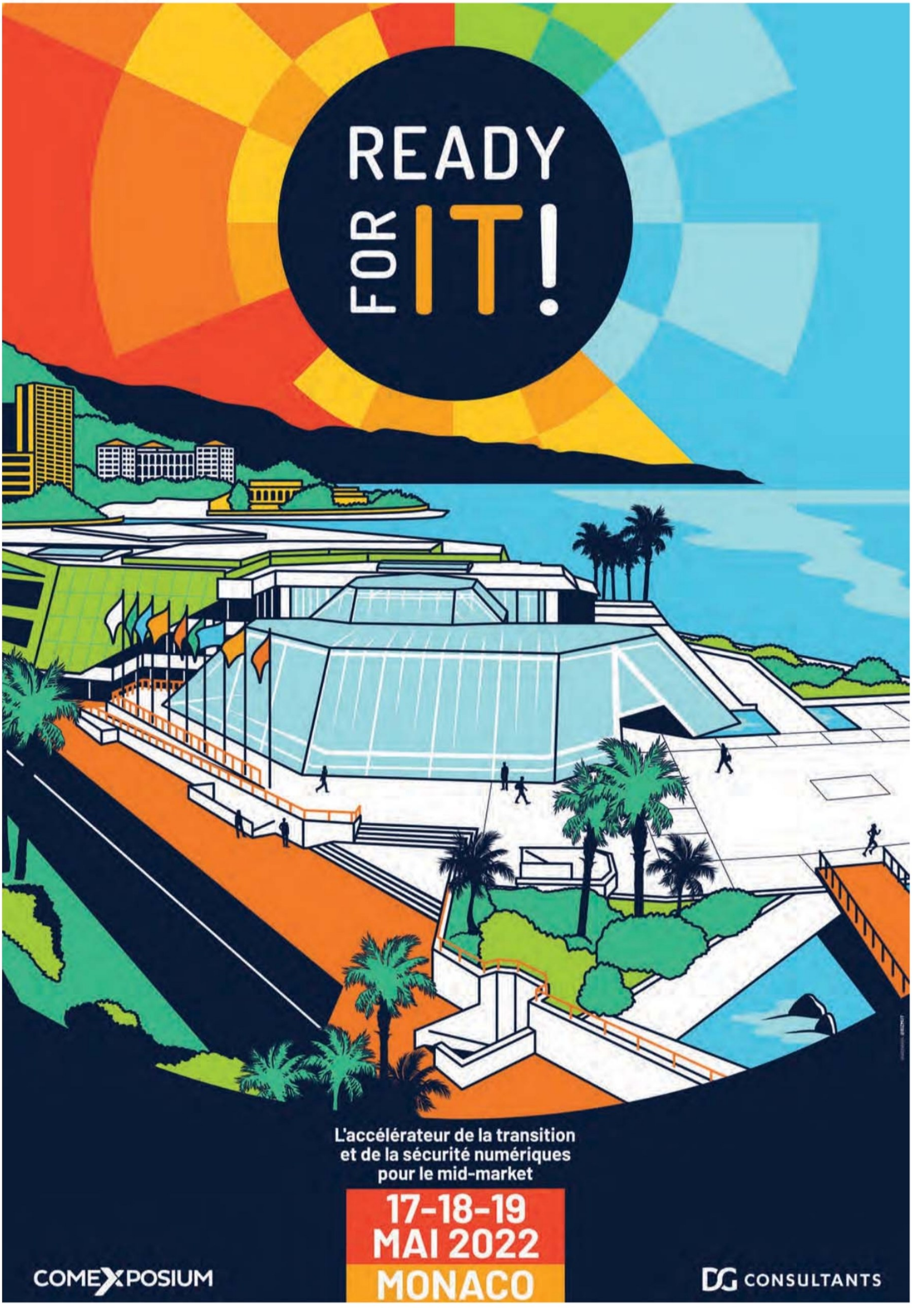


StackRox de Red Hat est un autre challenger, lui aussi incontournable en matière de sécurisation de containers.

La responsabilité des développeurs

La part de responsabilité qui incombe aux développeurs concernant la sécurité des applications n'est pas toujours – et même rarement – clairement définie. D'un côté, les développeurs sont vivement intéressés par la conception et le déploiement d'applications sécurisées. De l'autre, le problème est que la plupart du temps ceux-ci ne disposent pas de suffisamment de ressources pour maîtriser toutes les nuances de la sécurité des applications. Plus la sécurité des applications sera intégrée à la plateforme sur laquelle elles sont déployées, plus il sera facile de mettre en place et de maintenir la sécurité globale des containers. Certes, nombre de développeurs pensent que les containers ne fonctionnent pas suffisamment longtemps – du moins consécutivement parlant - pour être ciblés par des cybercriminels. En réalité, comme de plus en plus d'applications avec état sont déployées sur des plateformes telles que Kubernetes, les containers utilisés pour les concevoir fonctionnent sur d'assez longues périodes. Le risque est qu'une fois qu'un container est compromis, il est relativement aisé pour le malware l'ayant infecté de se propager latéralement (sur les autres containers) voire de prendre le contrôle de toute l'architecture en place. La plupart des problèmes de sécurité impliquant des containers concernent généralement des attaques de cryptojacking qui utilisent les containers pour miner de la crypto-monnaie. Bien que généralement considérés comme de simples crimes de nuisance, ces attaques peuvent également donner aux cybercriminels l'opportunité de créer des backdoors (portes dérobées) qui pourront être exploitées plus tard. Comme de plus en plus de ces charges de travail de type mission-critique basées sur des containers sont déployées sur ce type de plateformes, il devient relativement trivial pour les cybercriminels d'en garder l'accès. Le défi, en matière de sécurité, est donc d'éliminer autant d'attaques supposées anodines que possible afin d'éviter des intrusions plus sérieuses ne manquant pas, le plus souvent, de suivre. □

T.T


READY
FOR IT!
L'accélérateur de la transition
et de la sécurité numériques
pour le mid-market
17-18-19
MAI 2022
MONACO
COMEXPOSIUM
DG CONSULTANTS

Survivre dans la jungle des Cryptomonnaies



Blockchain et NFT affolent les gazettes mais, finalement, peu comprennent réellement ce dont il s'agit. Dans la collection « Pour les nuls », Daniel Ichbiah avec Jean-Martial Lefranc signent un ouvrage pour vous donner les éléments et les bases pour naviguer dans ce monde nouveau. Sans nul doute, nous avons affaire à une véritable révolution. Elle pourrait se résumer ainsi : pour la première fois dans l'histoire, nous voyons apparaître des monnaies d'envergure indépendantes des banques centrales et des États. Ce qui semblait relever de l'utopie est devenu réalité.

Pour autant, tout est-il vraiment si rose dans ce nouvel univers, qui s'apparente encore à un nouveau Far West ? Au contraire, les arnaques et les pièges abondent, et en face de gains mirobolants réalisés par certains, des milliers de particuliers ont été floués de leurs économies.

Pour s'aventurer dans ce qui s'apparente à une jungle, il est nécessaire de se former. C'est l'objet de la nouvelle édition de ce livre, avec une mise à jour quasiment intégrale de la précédente, tant ce domaine a évolué en trois ans.

Les auteurs se sont d'ailleurs engagés eux-mêmes dans la démarche avec un NFT sur le manuscrit du livre !

Les industries que la blockchain décentralisée va révolutionner

La révolution de la décentralisation est en cours dans de nombreux secteurs : entreprises établies et start-up préparent l'arrivée de la blockchain dans de nombreux secteurs. Quels sont les métiers où l'impact risque d'être le plus important ?

Le secteur bancaire

La blockchain est la technologie sous-jacente d'un système de monnaie virtuelle. Il est donc logique que les financiers soient les premiers à s'y intéresser. La première application pertinente serait de mettre en place une blockchain pour remplacer les systèmes de virements bancaires internationaux tels que Swift. On peut s'attendre à une baisse significative du coût des transactions bancaires.

Ce nouveau système Swift sur la blockchain est déjà mis en œuvre par la société Ripple qui a eu un succès certain pour convaincre de nombreuses institutions financières de premier plan d'utiliser ses services.

Depuis mai 2020, la Banque de France expérimente l'usage d'un euro numérique. Et la Banque centrale européenne envisage un stablecoin fondé sur la monnaie officielle à l'horizon 2025. On parle de MDBC : monnaie digitale de banque centrale.

La santé

La conservation des dossiers médicaux dans le temps et l'espace est une des préoccupations majeures des systèmes de santé. Placer ses dossiers sur une blockchain garantirait leur accessibilité dans le temps tout en y associant des permissions de consultation qui pourraient évoluer avec l'âge du patient ou la nature des soins qu'il doit recevoir.

DokChain, une entreprise basée en Californie, gère un registre unique de dossiers médicaux sur sa blockchain PokitDok.

Les institutions démocratiques

Jusqu'à présent, le comptage des votes exprimés par les citoyens n'était pas à l'abri des pirates informatiques. Une blockchain dédiée à la gestion et à l'authentification des listes électorales permettrait de sécuriser ce processus démocratique. De plus, un tel système simplifierait de manière radicale les opérations de vote et conduirait à une participation citoyenne plus ample et plus active.

Follow my vote, un projet d'applications décentralisées (DApps) qui vise dans un premier temps à sécuriser les votes électroniques.



L'immobilier

Avec la blockchain, les notaires pourraient avoir du souci à se faire. En effet, il est envisageable qu'à terme, il ne soit plus nécessaire de faire enregistrer ses transactions immobilières par ces officiers ministériels.

Lorsqu'un compromis de vente est signé, les dépôts de garantie pourraient être intégrés à un smart contract et le solde de la transaction serait payé une fois que toutes les conditions de la vente seraient remplies. Le paiement des taxes pourrait être intégré au contrat intelligent, il serait alors effectué au profit du trésor public à la date de finalisation de la vente.

Activités annexes des notaires, l'enregistrement des contrats de mariage ou la consignation des testaments pourraient aussi être transférés sur une blockchain.

Le cadastre de la ville de Chicago teste le transfert de ses registres sur une blockchain basée sur Bitcoin Core, le logiciel de base de Bitcoin. Les éléments enregistrant les droits de propriété deviendraient ainsi infalsifiables.

La diffusion de contenu vidéo

Si BitTorrent continue d'être utilisé largement pour diffuser des films piratés, la blockchain pourrait proposer des films ou des séries légalement à partir d'un système peer to peer.

L'intérêt ? Chaque ordinateur du réseau devient une unité de stockage pour les fichiers vidéo. Ce système permettrait aux ayants droit d'économiser les 30 milliards de dollars qui sont actuellement payés par les grands studios ou Netflix pour diffuser leurs programmes sur le Net.

La logistique

La blockchain pourrait remplacer les systèmes de codes à barres pour le suivi des colis. Dans le même ordre d'idées, pour la traçabilité et la sécurité alimentaire, il est facile d'imaginer comment une chaîne de blocs pourrait répertorier tout le cheptel d'animaux consommable et ainsi garantir l'origine des viandes dans une zone géographique donnée.

Le potentiel de la blockchain dans ce secteur est jugé tellement important qu'une association professionnelle dédiée regroupe déjà 85 % des transporteurs américains : Blockchain in Trucking Action (BiTA).

Le trésor public

Le transfert sur une blockchain des activités de collecte d'impôts peut entraîner de sérieuses économies pour le budget de l'état. L'établissement de contrats intelligents pour chaque contribuable simplifierait le processus de déclaration tout en assurant une perception plus efficace.



BiTA, les routiers aiment la blockchain !

Au Luxembourg, le gouvernement a investi dans une société dénommée LuxTrust dont l'objet est d'enregistrer les citoyens sur une blockchain en vue de faciliter les démarches de toutes sortes à l'aide d'identités numériques.

Les jeux vidéo

La GameFi ou Finance du Jeu est une tendance qui émerge dans le secteur des jeux vidéo. Avec les applications play to earn (*« jouer pour gagner de l'argent »*) comme Mobox ou Axie Infinity, le joueur accumule des tokens émis par le jeu pour le récompenser de ses performances.



LuxTrust ambitionne de simplifier et de sécuriser les activités numériques des citoyens et des entreprises en les équipant d'identités numériques vérifiées.

Ces tokens permettent d'acquérir des NFT, personnages uniques ou autres accessoires. Ces NFT peuvent générer des intérêts dans la monnaie du jeu.

Mobox.io propose ainsi une infrastructure complète qui permet à des développeurs de jeux de rendre leurs titres « GameFi compatibles ».

LE SPORT PROFESSIONNEL

Lors de la spectaculaire transaction qui a permis d'attirer Messi au PSG en août 2021, une part de la rémunération du joueur a été payée en « Fan Tokens ». Les Fan Tokens sont des tokens émis par un club de football spécifique. Produits par la société Socios.com, les « Fan Tokens » sont cotés sur Binance et échangeables dans un autre token dénommé Chiliz qui peut être échangé contre de la FIAT (monnaie traditionnelle).

À quoi servent les « Fan Tokens » ? À obtenir divers privilèges auprès du club, comme l'accès à du merchandising à tirage limité ou à des systèmes de cash back récompensant les plus fidèles des supporters.

Les « Fan Tokens » étant cotés sur certaines plates-formes d'échanges, la spéculation est aussi au rendez-vous.

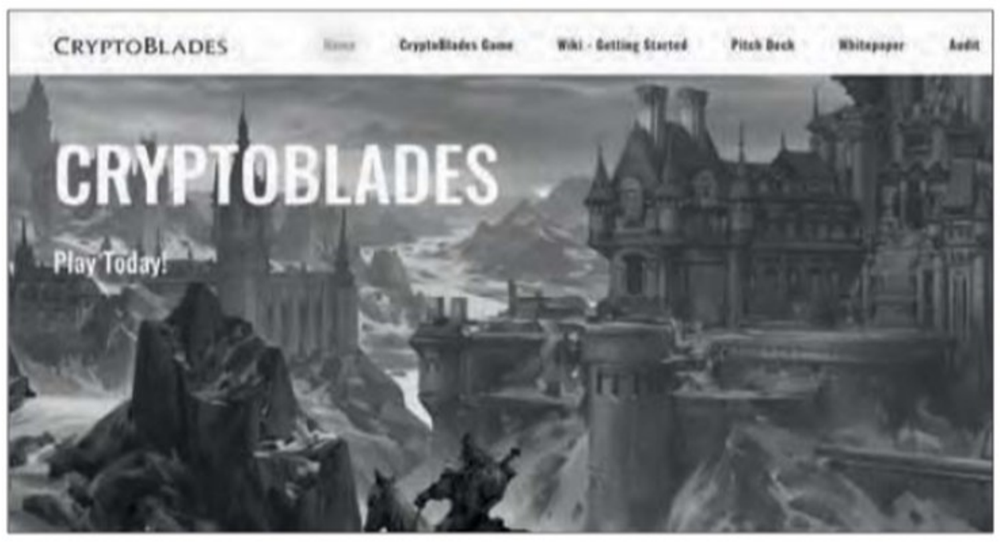
Émis à 2 dollars en 2018, le « Fan Token » du PSG est monté à 35 euros à l'annonce de l'arrivée de Messi pour jouer dans le club.

Chaque but de l'Argentin aux pieds d'or devrait permettre de valoriser la monnaie. Mais gare au match nul !

Justin Sun, le fondateur de TRON, a lancé un fonds de 300 millions de dollars pour investir dans les projets de GameFi.

La sécurité industrielle

Comme dans le secteur de la logistique, la traçabilité permise par la blockchain motive le déploiement d'applications dans le domaine de l'automobile ou de l'aéronautique.



Cryptoblades est l'un des jeux « GameFi » les plus populaires.

Ainsi, la plate-forme GoDirect Trade, mise en place sur une blockchain par la société Honeywell, permet de se procurer des pièces de rechange pour les avions en s'assurant de leur authenticité et de leur provenance.

Dans l'automobile, la blockchain sert à identifier chaque pièce d'un véhicule en circulation, ce qui permet de mieux cibler les propriétaires de voitures à alerter lorsqu'un défaut qui peut mettre en danger le conducteur et les passagers a été identifié.

Le continent obscur à la marge de la légalité

Aussi paradoxal que cela puisse paraître, il existe une relation symbiotique entre le continent clair et le continent obscur de la crypto. Chaque drame ou rebondissement sur le continent obscur fait progresser les innovations sur le continent clair et contribue à l'expansion de la décentralisation.

The Silk Road, première killer app de la cryptomonnaie

Le continent obscur de la crypto a émergé dès 2011 avec le supermarché illicite du Darknet, The Silk Road, mis en place par Ross Ulbricht, *« The Dread Pirate Roberts »*.

Grâce à quelques bitcoins, sur The Silk Road, il était facile de se procurer du cannabis, des drogues de synthèse, des armes, voire d'engager un tueur à gages.

Comme nous l'avons vu au Chapitre 1, le pirate Roberts a fait trop confiance aux capacités d'anonymat du Darknet et il s'est fait arrêter par le FBI en 2013 avant d'être condamné à la prison à vie en 2015.

Au cours de ses années d'activité, The Silk Road a généré plus de 1,2 milliard de dollars de chiffre d'affaires.

En 2020, le Département de la Justice américain a récupéré 69 000 bitcoins ayant appartenu au fondateur de The Silk Road représentant au cours actuel 3,22 milliards de dollars.

Malgré son activité infamante, Ross Ulbricht a certes contribué à faire connaître Bitcoin, au risque d'entacher son image, au grand désespoir des premiers supporters de cette monnaie.

Les attaques contre les exchanges, étapes de la sécurisation du continent obscur

Les exchanges tels que Coinbase, Kraken ou Binance ont été, depuis le début de la vague crypto, les cibles favorites des pirates. Il faut dire qu'un grand nombre de bitcoins sont stockés dans leurs serveurs et que, face à la ruée vers l'or virtuel, les promoteurs de certains exchanges n'ont pas toujours fait preuve d'une grande prudence.

Cependant, au fil des années, force est de constater que les attaques menées avec succès se font rares et surtout que les exchanges ont trouvé le moyen de riposter dans ce cas de hold-up virtuel.

Le festival des hacks a commencé avec l'attaque sur Mt. Gox en 2014, dont l'histoire est contée dans le Chapitre 1.

En 2018, un autre échange basé au Japon, Coincheck, a annoncé avoir perdu l'équivalent de 500 millions de dollars après le vol de 500 millions d'unités d'un nouvel altcoin dénommé NEM. Intervenant rapidement, les développeurs du NEM ont pu « marquer » les NEM dérobés par des hackers d'abord soupçonnés d'être originaires de Corée du Nord, puis identifiés comme russes.

Le crime contre Coincheck ne paie pas, les NEM détournés étant devenus inutilisables. La technologie a permis de neutraliser la monnaie mal acquise.

La série « crimes et châtiments » s'est poursuivie en Italie quelques mois plus tard avec le hack sur un exchange dénommé BitGrail sur un token appelé NANO. À l'époque, le préjudice a été estimé à 170 millions de dollars. La justice italienne s'est mêlée rapidement de l'affaire et a découvert que le patron de l'exchange avait commis différentes fraudes. Un jugement a déclaré la mise en liquidation de l'exchange et autorisé la saisie de ses biens pour rembourser les clients.

La résilience des exchanges a donc fait d'énormes progrès tandis que le cours du bitcoin s'est envolé.

En 2016, Bitfinex a perdu 70 millions de dollars en bitcoins, mais a fait une proposition originale à ses clients : les indemniser dans une nouvelle monnaie produite par l'échange lui-même, le Bitfinex token. Puis, sur une période de moins d'un an, l'exchange est parvenu à racheter les tokens en circulation afin de rembourser les clients de leur perte. Une telle démarche permet de prendre conscience de la rentabilité d'un des principaux exchanges qui, à l'époque, a généré ainsi des dizaines de millions de dollars de trésorerie en quelques mois.

Mais cela n'est pas fini

En 2019, Upbit en Corée du Sud et le fameux Binance se sont fait hacker pour respectivement 40 et 50 millions de dollars. Qu'à cela ne tienne ! Les deux exchanges ont indemnisé immédiatement leurs clients sans discuter. Désormais, il apparaît que les principales places de marché génèrent suffisamment de cash flow pour assumer sans sourciller ce genre d'incident.

Coinbase, qui publie des comptes trimestriels en tant que société cotée en Bourse, a ainsi annoncé pour le seul deuxième trimestre 2021 avoir encaissé 770 millions de dollars de bénéfice. Une performance qui fait tourner la tête !

L'autre phénomène spécifique au monde de la crypto est ce que l'on appelle « l'éthique du hacker ». Nous en avons vu un épisode dans l'histoire de The DAO, contée au Chapitre 2.

Le premier grand hack de la DeFi officielle a eu lieu en août 2021 avec le détournement de 600 millions de dollars des caisses de Poly Network, un système d'interopérabilité entre blockchains. Le hacker a exploité une faille importante dans le code du système. Mais quelques jours plus tard, il a rendu l'argent à son propriétaire, conformément à l'éthique du hacker « white hat » qui attaque pour identifier des faiblesses dans le réseau, pas pour s'enrichir. Poly Network a quand même décidé de récompenser son tourmenteur anonyme en lui accordant une prime de 500 000 USD.

Ainsi donc, dans la DeFi, un voleur peut se montrer gentil et rendre l'argent, et néanmoins recevoir une prime le félicitant d'être un bon citoyen ! □



Bitcoin et Cryptomonnaies pour les nuls

Daniel Ichbiah et Jean-Martial Lefranc

Format : Broché

Nb de pages : 338 pages

Poids : 723 g

Dimensions : 19cm X 23cm

Date de parution : 28/10/2021

ISBN : 978-2-412-07353-7

EAN : 9782412073537

Sécurisez votre avenir numérique

WALLIX PAM4ALL

Gardez la visibilité et le contrôle de vos accès !

Le télétravail, la migration vers le cloud, la multiplication d'équipements et les nouveaux usages numériques... engendrent une explosion du nombre et type d'accès aux actifs stratégiques des entreprises. Faites face à ce défi avec WALLIX PAM4ALL, la plateforme de gestion unifiée des privilèges qui vous permet de sécuriser, contrôler et manager l'ensemble de vos accès. PAM4ALL réduit les risques liés aux accès et aux privilèges associés, permet une gestion granulaire de vos accès distants et offre des accès uniquement pour des usages et durées spécifiques réduisant ainsi considérablement les surfaces d'attaques, sans affecter la productivité et en respectant les directives réglementaires.

WWW.WALLIX.COM



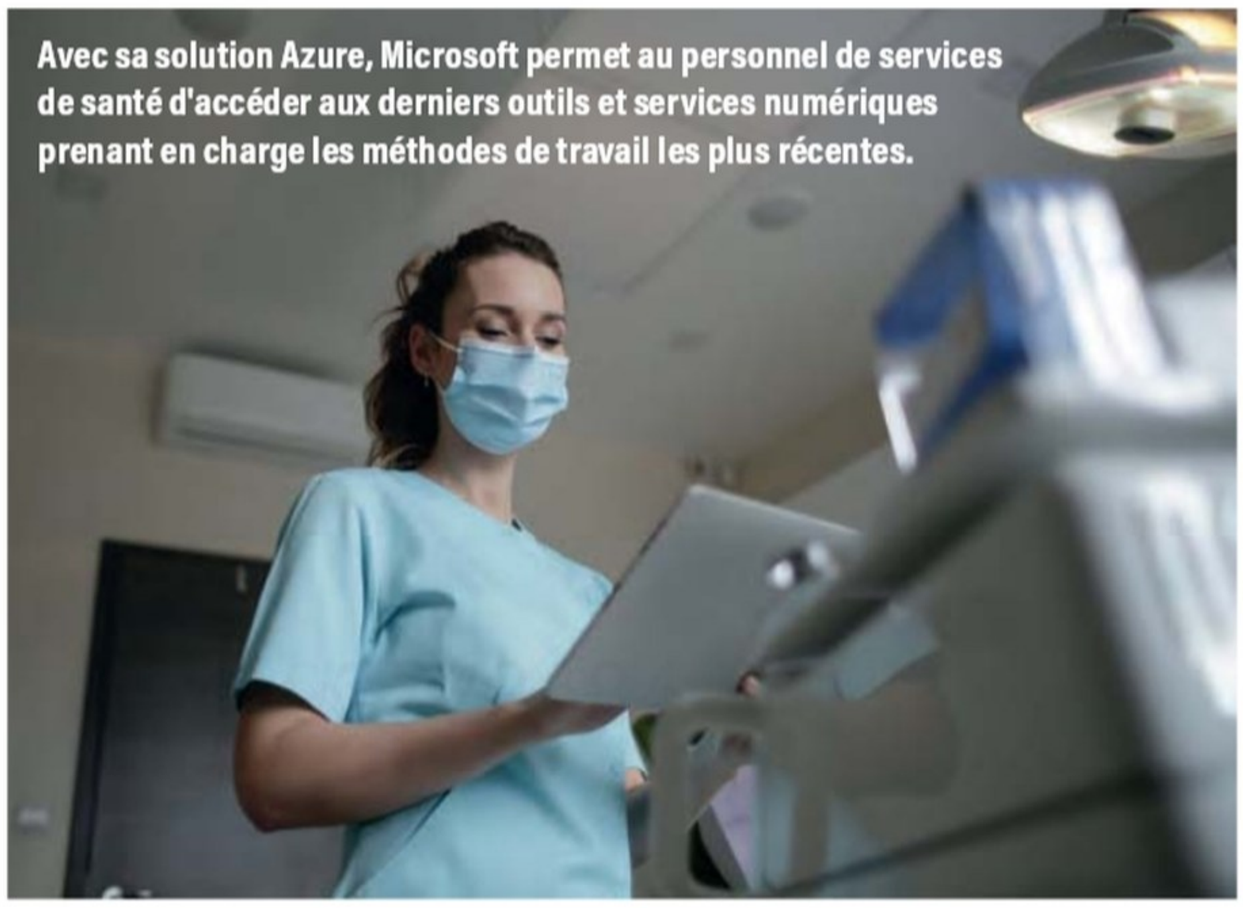
Pour plus d'informations
sur les solutions WALLIX contactez
Jean-Pierre Barré : jpbarre@wallix.com

WALLIX
CYBERSECURITY SIMPLIFIED

La **santé connectée** fait un grand pas en avant

En moins de deux ans, la santé connectée a connu un formidable essor aux États-Unis, mais aussi un peu partout dans le monde.

Avec la pandémie de Covid-19 et une demande accrue en matière de bien-être, les grands groupes pharmaceutiques, les géants de la tech et de nombreuses start-up ont investi dans ce secteur pour développer des solutions diverses et variées. Leur objectif : améliorer la santé de tout un chacun, faciliter la récolte et le transfert des données en toute sécurité et proposer une médecine prédictive avec le soutien de l'intelligence artificielle.



Avec sa solution Azure, Microsoft permet au personnel de services de santé d'accéder aux derniers outils et services numériques prenant en charge les méthodes de travail les plus récentes.

Poussée par la pandémie de Covid-19 et par la recherche accrue de bien-être, la santé connectée a fait un énorme bond en avant aux États-Unis et dans le monde. *« La santé est au centre de notre capacité à vivre une vie pleine, et l'accélération des technologies de la santé a le potentiel d'améliorer plus de vies dans plus d'endroits que jamais auparavant »*, a ainsi déclaré Robert B. Ford, directeur général du géant Abbott, durant le CES 2022. Une analyse partagée par Gary Shapiro, le P.-D.G de la Consumer Technology Association (CTA) et du CES. *« Plus que jamais, nous assistons à l'incroyable impact de la technologie sur l'amélioration des vies »*, relevait ce dernier à l'ouverture du salon de Las Vegas. Les différentes prévisions de marché semblent d'ailleurs leur donner raison. En effet, selon une étude menée par le cabinet Global Industry Analysts, le marché mondial de la santé numérique pourrait atteindre les 441 milliards de dollars (environ 407,8 milliards d'euros) à l'horizon 2026, dont une très large part outre-Atlantique.



Durant la pandémie de Covid-19, les solutions proposées par AWS ont permis à de nombreux pays, comme Singapour par exemple, de mieux prendre en charge la gestion des pics des vaccinations quotidiennes.

Des start-up américaines à la pointe de l'innovation

Au cours de ces deux dernières années, plusieurs start-up américaines sont sorties du lot à l'image de Northwell Health, d'Olive AI, Illumina ou Sleep Number. Cette dernière a montré son potentiel en matière d'innovation en présentant le lit intelligent Climate360 durant le CES. Tirant parti de l'architecture IoT, de l'apprentissage automatique et du tissu intelligent 3D, le matelas du lit s'ajuste automatiquement pour répondre aux besoins individuels et favoriser un sommeil réparateur.

Dans un autre registre, Northwell Health s'est fait remarquer en proposant un moyen autre que les tests pour détecter si un patient était positif à la Covid. Comment ? En menant une étude de validation d'un algorithme Fitbit pour détecter le virus avant que les symptômes ne commencent à apparaître. Illumina a travaillé sur les tests de séquençage pour suivre la propagation des différents variants. Pendant la pandémie, Illumina a développé le test COVIDSeq pour aider les laboratoires des pays sous-financés à décoder les séquences génétiques des variantes de la Covid-19. En 2021, l'entreprise a lancé Connected Analytics, une plateforme d'échange de données de séquençage et d'analyse utilisant le Cloud pour faciliter la gestion des données.

De son côté, la société Olive IA s'est spécialisée dans la conception de logiciels et de systèmes d'automatisation en direction des hôpitaux pour faciliter les opérations et améliorer les soins aux patients, et ce, en lien avec Amazon Web Services (AWS). En 2021, la technologie conçue par l'entreprise était utilisée par 1 000 hôpitaux. Olive AI a signé un partenariat avec Akava, un studio de développement de logiciels basé à San Francisco qui propose des produits cloud, web et mobiles natifs. Par ailleurs, Olive AI a lancé une « boutique » d'applications baptisée The Library. Cette plateforme de développement permet à des tiers de créer de nouvelles applications qui seront approuvées par Olive AI. Preuve de son succès, l'entreprise a levé 400 millions de dollars en juillet dernier, portant sa valorisation à 4 milliards de dollars.

Parmi les poids lourds de l'industrie de la santé comme Abbott, on peut aussi citer Johnson & Johnson MedTech. L'entreprise américaine a investi dans l'innovation chirurgicale en créant un logiciel de planification complet, une formation et une robotique chirurgicale pour les systèmes de santé. Avec sa plateforme C-SATS, la société propose des contenus de formation chirurgicale pour les médecins via une bibliothèque de 30 000 vidéos, dans lesquelles 350 chirurgiens enseignent de nouvelles techniques à d'autres chirurgiens. Par ailleurs, Johnson & Johnson MedTech a développé la plateforme Visible Patient, permettant aux chirurgiens de modéliser des chirurgies en 3D. En plus des États-Unis, cette plateforme s'étend désormais à 11 pays d'Europe, du Moyen-Orient et d'Afrique. Selon l'entreprise, plus d'un million de professionnels de la santé ont accédé aux cours en ligne de l'entreprise sur les protocoles spécifiques à la Covid-19.

Protéger les données et faciliter leur compatibilité

Hormis les start-up et les géants de l'industrie pharmaceutique, les entreprises de la tech comme Amazon avec AWS ou Microsoft avec Azure et Azure Health Data Services sont aussi sur les rangs avec des solutions pour protéger les données et faciliter leur accès comme l'explique Steve Kearney, directeur médical chez SAS. *« Malgré les nouveaux développements en matière d'imagerie, de diagnostic, de traitement et de techniques chirurgicales, le manque de normalisation des données dans l'industrie a enfermé les informations sur la santé*



Fin 2021, AWS a sélectionné dix entreprises pour participer à son programme AWS Healthcare Accelerator. Basées aux États-Unis, ces start-up issues du secteur des soins ont été choisies suivant des critères précis comme avoir une solution opérationnelle, des revenus et des clients.

dans des silos fonctionnels. Ainsi, les différents prestataires ont du mal à concilier manuellement les formats de fichiers incompatibles, ce qui ralentit le transfert d'informations. Cela a clairement un impact négatif sur la qualité des soins et l'expérience des patients », indique-t-il sur son blog. Selon lui, les entreprises comme Microsoft et ses partenaires tels que SAS travaillent à améliorer l'interopérabilité en permettant l'utilisation de normes telles que Fast Healthcare Interoperability Resources (FHIR). *« SAS et Microsoft Azure créent ainsi des intégrations technologiques approfondies qui libèrent de la valeur en rendant les données disparates et les analyses avancées plus accessibles aux organisations de santé. Avec de nouvelles fonctionnalités telles que l'intégration d'Azure Health Data Services à SAS sur Azure, les capacités d'IA intégrées de SAS Health sont plus efficaces et sécurisées »*, explique-t-il.

Intelligence artificielle : vers la santé prédictive

Toujours chez Microsoft, l'entreprise a annoncé une preview et des mises à jour de son outil Microsoft Cloud for Healthcare qui permettent d'avoir une vue à 360 degrés des patients. *« Cette version prend en compte les commentaires des clients et des partenaires et renforce notre engagement à aider les prestataires de soins de santé et les patients en garantissant une meilleure navigation dans les données, en renforçant la collaboration d'équipe et améliorant les connaissances cliniques et opérationnelles »*, souligne-t-on chez Microsoft. Il est aussi question de Microsoft Power Apps, la solution qui permet aux fournisseurs et aux partenaires de créer des applications personnalisées. La gestion et l'interopérabilité des données via le Cloud sont donc de plus en plus visibles dans la santé. Mais c'est aussi le cas de l'intelligence artificielle grâce à sa capacité à analyser d'énormes volumes de données, à les interpréter et à les comparer pour prédire des modèles, des possibilités et des résultats à tous les niveaux. À l'avenir, il ne fait aucun doute que l'association du Cloud, Big Data, intelligence artificielle ira plus loin que la récolte et le partage de données des patients. On peut dès lors parler de santé prédictive, répondant au vieil adage : mieux vaut prévenir que guérir. ☐ **Michel Chotard**

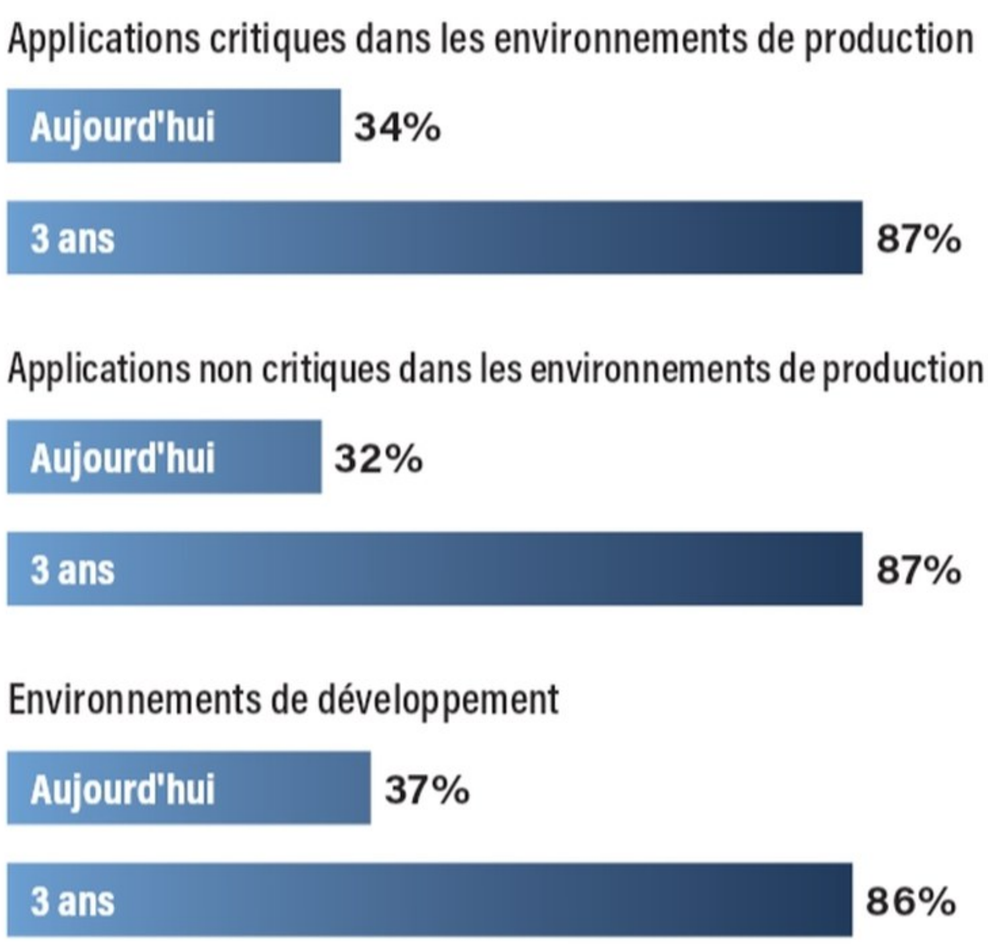
Containers

Kubernetes partout, sécurité nulle part

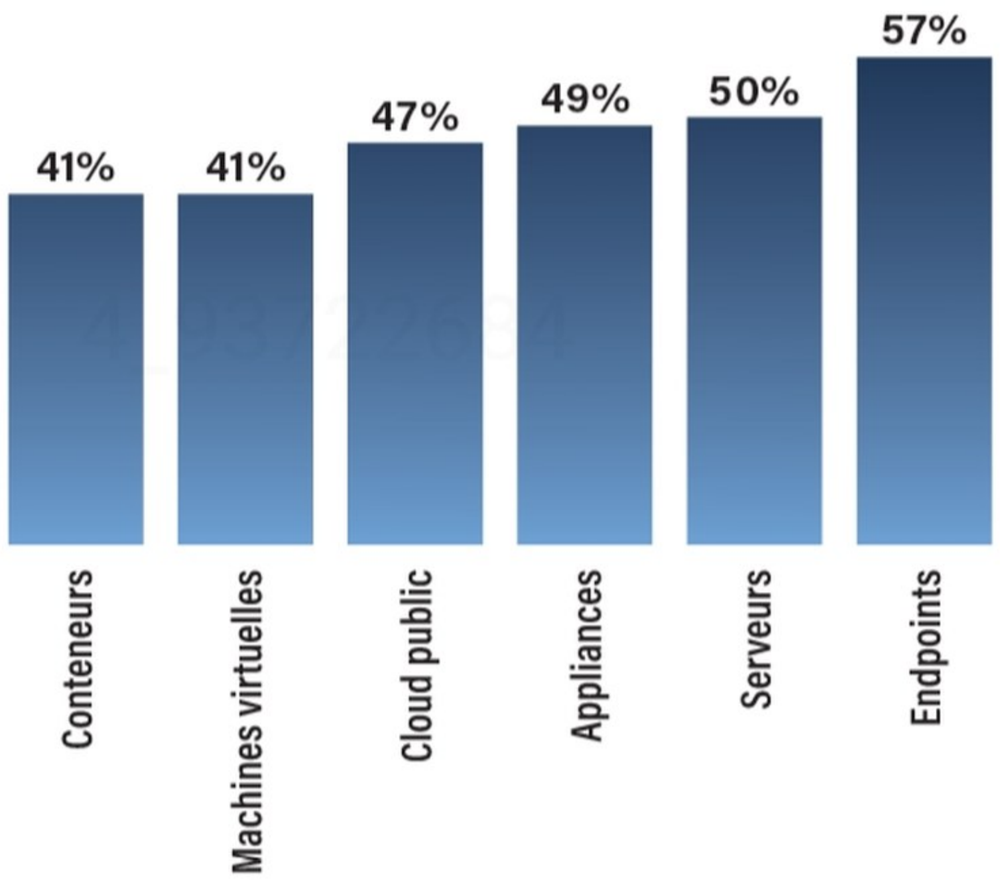
Les conteneurs sont-ils le prochain ventre mou des systèmes informatiques ? Alors que 87% des entreprises envisagent de déployer Kubernetes dans leurs environnements au cours des trois prochaines années, moins d'un tiers de celles qui l'ont déployé aujourd'hui dispose des outils nécessaires à sa sécurité.

La majorité des entreprises ne seraient pas suffisamment préparées pour faire face aux menaces qui peuvent peser sur leurs environnements Kubernetes. Tel est le sombre constat auquel parvient Veritas Technologies aux termes d'une enquête commandée à Opinium Research. L'étude a été menée en février dernier auprès de 1 100 décideurs IT dans 11 pays, dont la France. Première observation : l'adoption de Kubernetes devrait sensiblement accélérer lors des trois prochaines années. Alors qu'aujourd'hui, un tiers des entreprises ont déployé Kubernetes, tous environnements confondus, 87% des répondants assurent qu'ils utiliseront la solution d'orchestration de conteneurs dans les trois années à venir. *« Kubernetes passera rapidement du déploiement par la minorité des organisations à la grande majorité »* explique Veritas, qui souligne que seuls 3% des organisations ne prévoient pas, *in fine*, de déployer l'orchestrateur.

KUBERNETES AUJOURD'HUI ET DEMAIN



QUE VISENT LES RANSOMWARES ?



Dans le détail, les environnements de déploiement sont aujourd'hui ceux dans lesquels Kubernetes est le plus déployé, à hauteur de 37% des interrogés, contre 33% dans les environnements de production. D'ici à trois ans, le rapport s'inversera très légèrement, puis la solution d'orchestration de conteneurs sera déployée en production chez 87% des entreprises, un point de mieux qu'en ce qui concerne les environnements de développement. On note, en outre, que Kubernetes concernera aussi bien les applications critiques que non critiques.

« Kubernetes est une technologie facile à déployer pour les entreprises. Elle améliore rapidement la gestion des coûts, la flexibilité et l'évolutivité des environnements. Il n'est donc pas étonnant que les entreprises soient si nombreuses à adopter la conteneurisation. Cependant, la simplicité de déploiement de Kubernetes peut également induire les entreprises en erreur et les pousser à les déployer plus vite qu'ils ne les sécurisent » fait remarquer Jean-Pierre Boushira, VP EMEA et Benelux chez Veritas.

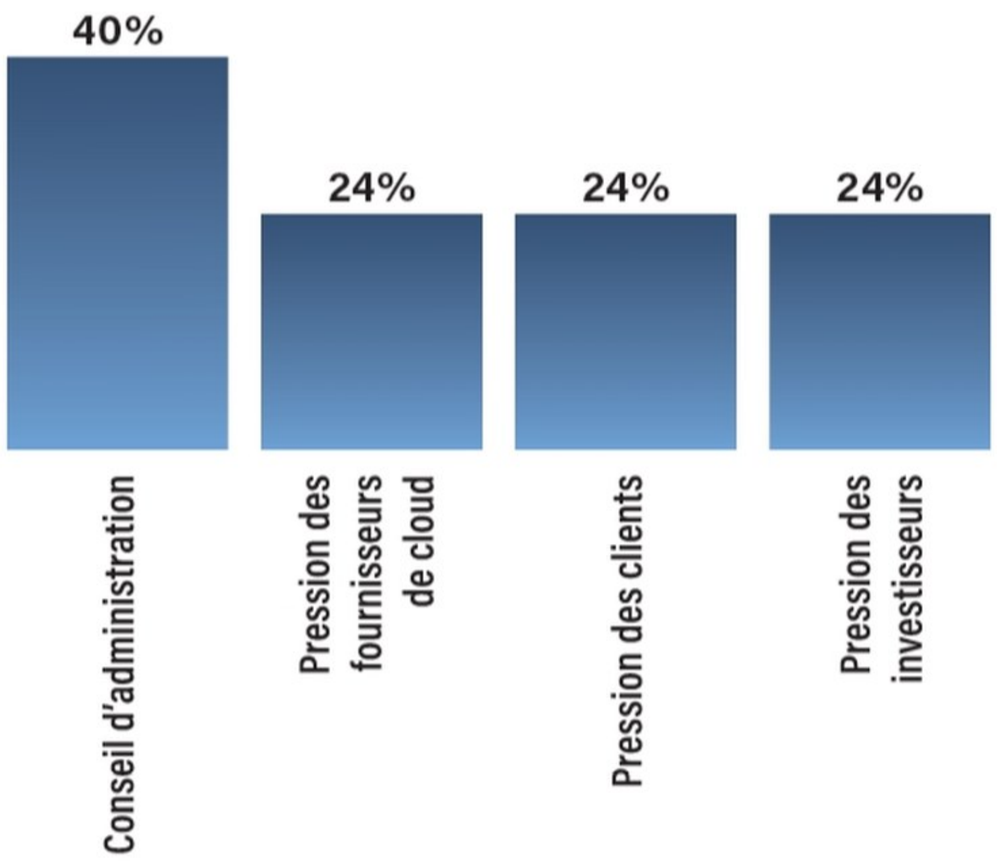


En effet, et c'est là que l'étude s'assombrit, 41% des entreprises déclarent avoir subi une attaque de ransomware sur leurs environnements conteneurisés. Un chiffre relativement bas, égal au pourcentage d'entreprises qui indiquent que leurs machines virtuelles ont été la cible d'attaque et bien en dessous de celles qui, à respectivement 57% et 50%, déplorent des attaques contre leurs terminaux et leurs serveurs. Pour autant, selon Veritas, ce chiffre de 41% demeure élevé compte tenu de la récente adoption de la technologie d'orchestration des conteneurs pour les données avec état. D'autant que, en considérant uniquement les entreprises ayant déployé à l'heure actuelle Kubernetes, ce sont près de la moitié d'entre elles qui signalent que leurs conteneurs ont été la cible d'attaques.

Pourquoi une telle fragilité ? La raison en est triviale : les environnements conteneurisés manquent de protection. Parmi les entreprises ayant déployé Kubernetes, moins d'un tiers ont mis en place des mécanismes de sécurisation des données dans leurs environnements Kubernetes en production. Ils sont 36% à protéger leurs environnements de développement. Les applications critiques sont à peine plus défendues que les applications non-critiques, 33% contre 30%. Néanmoins, les décideurs IT ont pleinement conscience des enjeux. 89% des organisations pensent que les attaques de ransomwares sur leurs environnements Kubernetes seront un problème pour elles l'année prochaine, 44% d'entre elles affirment qu'elles constitueront un « problème majeur ».

Ce manque de protection s'explique assez aisément. En effet, l'étude de Veritas pointe que les décisions liées à Kubernetes et à son déploiement échappent bien souvent à l'IT. À la question *« Qui a le plus d'influence dans le processus de prise de décision sur l'adoption ou non de Kubernetes dans votre organisation ? »*, le conseil d'administration arrive en tête dans 40% des réponses, suivi à égalité par les pressions des vendeurs de cloud, les pressions des clients et les pressions des investisseurs, à 24% chacun. En d'autres termes, les déploiements Kubernetes ne correspondent pas nécessairement à l'agenda des départements IT, avec les conséquences que l'on imagine sur les questions de sécurité qui se posent soudain.

LES DÉCISIONS LIÉES À KUBERNETES NE VIENNENT PAS TOUJOURS DE L'IT



Un autre problème porte sur les solutions de sécurité elles-mêmes, ou plus exactement la perception qu'en ont les décideurs IT. 45% des interrogés ont déclaré qu'ils savaient peu ou rien des solutions qui peuvent protéger les données à travers leurs différents environnements. En conséquence de quoi l'approche la plus courante, pour près de la moitié des entreprises protégeant leurs environnements Kubernetes, consiste à ajouter des solutions de protection des données autonomes supplémentaires, introduisant une nouvelle couche de complexité à leur sécurité. Elles ne sont que 40% à étendre leurs solutions de protection des données existantes pour leurs environnements traditionnels et virtualisés à leurs environnements Kubernetes. On peut comprendre ce faible pourcentage : 15% des répondants ne pensaient même pas qu'une telle solution soit disponible sur le marché aujourd'hui.

« À ce rythme, Kubernetes deviendra, en dépit de tous ses avantages, le talon d'Achille de la stratégie de défense des entreprises contre les ransomwares » s'inquiète Jean-Pierre Boushira. Mais qu'on se rassure ! À en croire l'étude de Veritas, 97% des organisations utilisant Kubernetes dans des environnements critiques considèrent qu'ils seront protégés d'ici à cinq ans. Mieux encore, en France, 76% des répondants pensent pouvoir sécuriser leurs environnements Kubernetes d'ici à l'année prochaine. La très grande majorité des entreprises dit certes s'attendre à ce que, dans cinq ans, les ransomwares seront toujours un problème. Toutefois, les entreprises s'attendent à dépenser en moyenne 49% de plus pour la protection des données de leurs environnements Kubernetes à l'horizon 2027, des investissements qui permettent à 61% d'entre elles d'estimer qu'elles seront « très bien préparées » pour faire face aux attaques contre leurs environnements Kubernetes sous cinq ans. □

G.P

CLUB DECISION DSI

1er Club Français de décideurs informatiques & télécoms
1250 MEMBRES



Véronique Daval
Présidente

Un réseau indépendant et privé au sein duquel siègent 11 DSI ambassadeurs de leur secteur d'activité



Julien Daval
Vice-Président

LES MEMBRES DU BUREAU ET AMBASSADEURS DU CLUB



Armand ASSOULINE
CIO
MSC FRANCE



Christian DOGUET
DSI
CHAINE THERMALE DU SOLEIL



Trieu HUYNH-THIEN
DSI ADJOINT
CENTRE GEORGES POMPIDOU



Dominique TROUVE
DSI
HÔPITAUX AVICENNE



Gilles BERTHELOT
RSSI
GROUPE SNCF



Damien GRIESSINGER
CTO
EPPO



Stéphane MALGRAND
DSI
Laboratoire national de Métrologie et Essais



Claude YAMEOGO
ARCHITECT SI
ALSTOM



Christophe BOUTONNET
SOUS-DIRECTEUR
SCHÉMA DIRECTEUR ET POLITIQUE SI



Christophe GUILLARME
DSI
GROUPE AB TÉLÉVISION



Lionel ROBIN
DSI
GROUPE LA RESERVE

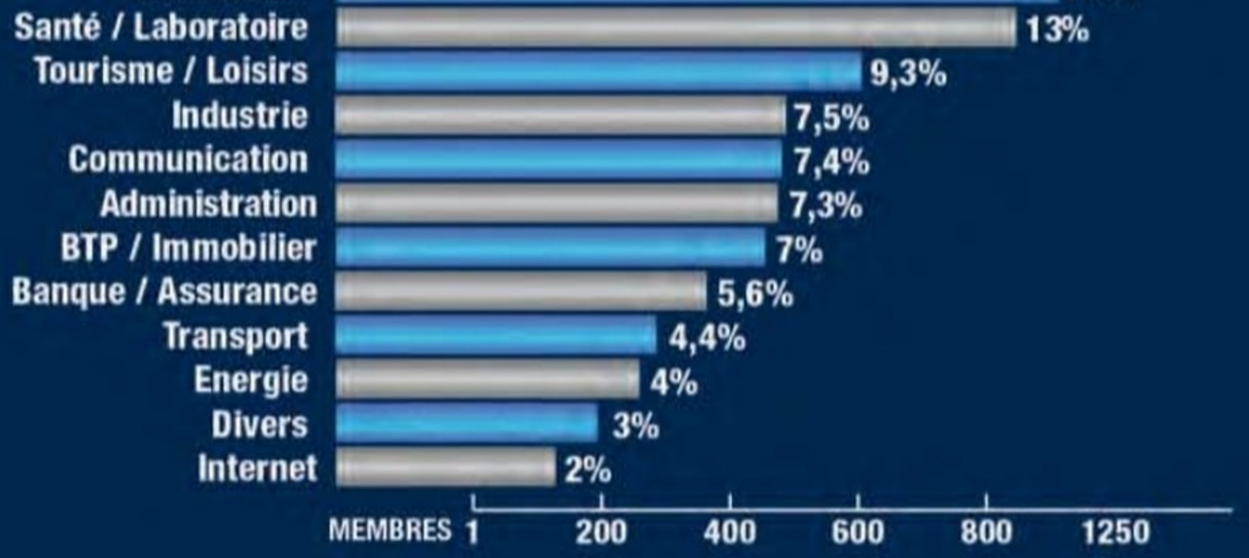
Le Club accompagne les DSI à faire les bons choix technologiques et aligner l'informatique sur la stratégie de l'entreprise



LES MEMBRES DU CLUB

1200 CIO, DOSI, DSI, DI Membres du Club, sociétés de + 300 salariés PARIS/IDF





CLUB DECISION DSI • 33, Rue Galilée 75116 Paris • Tél +33 1 53 45 28 65
www.clubdecisiondsi.fr
Contact : Véronique DAVAL - Présidente
veronique.daval@decisiondsi.com

@clubdecisiondsi

www.imstudio.fr

Inetum lance la **plus grande campagne de recrutement** de son histoire



L'ex-Gfi Informatique prévoit de recruter 7000 nouveaux collaborateurs en 2022, dont 3000 en France.

Un record historique pour l'ESN qui mise sur la diversité de ses activités et missions pour attirer des candidats, dont une majorité de profils expérimentés. Les postes à pourvoir sont très larges et vont de l'ingénieur au consultant, en passant par le développeur. Quelle est la proposition d'Inetum et quels sont les profils recherchés ?

L'année 2022 sera cruciale pour Inetum en matière de recrutements. L'ESN espère embaucher par moins de 3000 collaborateurs en France et 7000 au total. *« Cela représente cinquante recrutements par semaine dans l'Hexagone »*, explique l'ex-Gfi Informatique. Une campagne sans précédent pour l'entreprise qui compte aujourd'hui 27000 salariés dans 26 pays, dont environ 10000 en France. Ces embauches seront majoritairement réalisées en CDI (2400), avec également 600 CDD, contrats d'alternance et stages. Les recrutements en CDI sont répartis localement sur 5 grandes régions dans les agglomérations et bassins de Nantes, Lyon, Lille, Toulouse et Paris. Dans le détail, Inetum table sur 400 recrutements dans le Centre et l'Ouest, 300 en Auvergne-Rhône-Alpes, 350 dans le Nord et l'Est, 350 dans le Sud et 1200 en Île-de-France.

Accompagner les projets

Pourquoi l'entreprise a-t-elle besoin d'autant de nouvelles recrues ? Inetum ne possède pas de turn-over au-dessus de la moyenne (18,9% au niveau mondial et une ancienneté moyenne de 7 ans en France). Elle n'est pas non plus en perte de croissance. Son chiffre d'affaires atteint les 2,2 milliards d'euros en 2021. La principale raison est plutôt à trouver du côté de la crise sanitaire et de la vague de projets de transformation numérique qu'elle suscite. *« Au cours de ces dernières années, et d'autant plus dernièrement avec la crise sanitaire, le secteur des ESN a vu les besoins en recrutements connaître une croissance sans pareil, correspondant à l'accélération des projets de digitalisation des entreprises et des usages quotidiens du numérique »*, indique ainsi Inetum.

Ces embauches concernent toutes les activités de l'entreprise, dont l'édition de logiciels, qui est une des spécificités d'Inetum. L'entreprise possède en effet six activités : le conseil, les services applicatifs et d'infrastructure, l'intégration systèmes (Business Solutions, ERP, CRM, PLM…), l'outsourcing (infogérance), la revente à valeur ajoutée (accompagnement sur l'achat de matériel) et donc également l'édition de logiciels. Sur ce dernier point, Inetum édite une cinquantaine d'applications dont la plus connue est Chronotime Workplace (gestion RH), mais aussi Cleva Insurance Solution (assurance) ou encore Bdoc (dématérialisation des processus documentaires).

« Cette grande variété d'activités nous permet d'offrir un parcours de carrière très diversifié », met en avant Bruno Da Sola, directeur des ressources humaines d'Inetum.



« Nous intervenons également dans une grande variété de secteurs, comme la finance, la santé, la défense, la sécurité, le secteur public, l'énergie, l'aéronautique ou l'automobile ». Et comme toute ESN, Inetum propose des missions en prestation externe chez des clients (40%) mais aussi en interne (60%). *« Selon le plan de carrière du collaborateur, il peut passer de missions externes, chez le client, à des projets développés en interne. Nous cherchons la meilleure adaptation possible »*.

Recrutements tous azimuts

Quels sont les postes à pourvoir chez Inetum ? Le moins que l'on puisse dire est que la liste est longue. L'ESN évoque ainsi : les consultants business solutions confirmés (Salesforce, Microsoft Dynamics...), les ingénieurs commerciaux, Data ou DevOps, les architectes Cloud, les Product Owners ou Proxy Product Owners, les Scrum master... sans oublier les toujours incontournables développeurs Java Full Stack, développeurs Low Code et Tech lead Java.

Tous les profils sont recherchés, du junior au sénior, en passant par les professionnels en reconversion. Inetum recrute d'ailleurs majoritairement des profils expérimentés. Côté compétences, outre celles liées au poste, la maîtrise de l'anglais est demandée dans certaines fonctions, notamment celles à périmètre international. Et concernant les « soft skills », l'ESN évoque surtout « l'esprit entrepreneurial » qui est une de ses valeurs fondamentales. *« Il faut être entreprenant, c'est-à-dire force de proposition, autonome, centré sur la relation client, agile et à l'écoute »*, résume Bruno Da Sola.

Pour sourcer les candidats, Inetum mise principalement sur son site internet (www.inetum.com/fr/jobs) et les réseaux sociaux (notamment LinkedIn, qui représente 30% de son sourcing). L'ESN fait très peu appel à des cabinets de recrutements externes. *« Ce sont très majoritairement des embauches en direct encadrées par nos différentes business lines. La cooptation entre collaborateurs est également au cœur de notre stratégie. Nous proposons d'ailleurs une prime de cooptation à nos collaborateurs. Elle est aujourd'hui à l'origine de 27% de nos embauches »*, poursuit Bruno Da Sola.

Une fois la prise de contact réalisée, l'ESN préfère aller vite et ne pas multiplier les entretiens. Deux à trois entretiens sont ainsi réalisés, dont le premier à distance via Teams. Pour les postes techniques, des tests de compétences sont également réalisés. *« L'idée est de resserrer au maximum ces différentes étapes. Le marché est très tendu, et nous avons besoin de recruter avec des cycles courts »*. Pour garder le contact entre la signature du contrat et l'arrivée dans les locaux (onboarding), Inetum va proposer en 2022 une application mobile dédiée. Elle permettra de retrouver une présentation de l'entreprise, mais aussi ses actualités, ainsi que d'échanger avec le service qui va l'accueillir.

Télétravail et formations

Pourquoi venir travailler chez Inetum ? Outre la diversité des activités et missions, l'ESN met en avant un accord sur le télétravail datant de 2011 (et amendé en 2020). *« C'est une évolution incontournable du mode d'organisation de l'entreprise, qui est très demandée par les candidats »*, souligne le DRH du groupe. Selon cet accord, les salariés peuvent bénéficier jusqu'à 4 jours de télétravail par semaine, qu'ils peuvent gérer de différentes manières, car il s'agit d'un volant de jours à répartir sur l'année. Inetum est présent sur 45 sites en France, mais il entend ainsi laisser un maximum de liberté à ses collaborateurs sur le choix de leur lieu de travail.

Autre avantage mis en avant par l'ESN : la formation et les certifications. Sur ses 27000 collaborateurs, près de 10000 ont bénéficié de formations et de certifications en 2021. Il s'agit de formations techniques mais aussi managériales, en présentiel ou de plus en plus en e-learning. Parmi les certifications les plus suivies : GCP (Google Cloud Platform) et équivalent sur Microsoft Azur ou AWS, mais également ITIL, Oracle ou ISTQB.

Dernier atout évoqué par l'ESN pour séduire les candidats : sa solidité financière. Le groupe a donc généré 2,2 milliards d'euros en 2021, avec une croissance organique de « près de 5% ». Il y a dix ans, les revenus de l'ex-Gfi Informatique étaient plutôt de l'ordre de 750 millions d'euros. *« Nous sommes un groupe qui affiche une croissance et un développement constant. Ce qui est un gage de pérennité. Nos collaborateurs ont ainsi la garantie de pouvoir mener une carrière sur la durée, autour de projets variés, avec une montée en compétences régulière et des conditions de travail attractives »*, conclut Inetum. □

C.G

www.linformaticien.com

ABONNEZ-VOUS À L'INFORMATICIEN



linformaticien.com/abonnement

Une **offre triple** pour ne rien manquer
des dernières tendances
et innovations de la transformation numérique

MAGAZINE

Recevez chaque mois (10 numéros par an) le magazine «papier» et accédez également aux versions numériques des dernières publications.

1 AN FRANCE : 72 €
2 ANS FRANCE : 135 €
1 AN UE : 90 €
2 ANS UE : 171 €
1 AN HORS UE : 108 €
2 ANS HORS UE : 207 €

NUMÉRIQUE

Accédez chaque mois (10 numéros par an) à la version numérique du magazine et retrouvez également via votre compte en ligne les versions numériques des dernières publications.

1 AN : 49 €
2 ANS : 89 €

COUPLAGE

Recevez chaque mois L'Informaticien (10 numéros par an) et chaque trimestre L'Info CyberRisques (4 numéros par an) et accédez également aux versions numériques des dernières publications.

1 AN FRANCE : 99 €
2 ANS FRANCE : 179 €

Accès aux versions numériques seules des deux publications.

1 AN numérique : 75 €
2 ANS numérique : 135 €

Réalité virtuelle

Faire revivre le passé au présent

Qui ne s'est jamais demandé comment se passait la vie au Moyen-Âge ? Comment peignait Monet dans son atelier ? Si le voyage dans le temps n'existe pas... encore, il est possible avec la réalité virtuelle de faire ce type de voyage. De nombreux nouveaux titres sont disponibles. Tour de ce qui est paru récemment.

DreamAway, le réseau de salles de réalité virtuelle a enrichi son offre culturelle avec trois nouvelles rencontres. La première permet de rencontrer notre ancêtre Sapiens, une chasseresse du Paléolithique. Elle vous fera entrer dans son clan et vous présentera à une femme chamane qui vous enseignera les arcanes de la peinture rupestre. Vous pouvez apprendre à tailler vos propres outils dont une lance qui vous aidera lors d'une chasse au mammouth !

Développé avec l'aide de la Maison Anne Frank d'Amsterdam, un parcours vous conduit dans l'annexe secrète où elle a vécu ainsi que sa famille et quatre autres juifs. Moins dramatique, un parcours vous entraîne dans l'atelier de Claude Monet à Giverny pour un dialogue entre le peintre et son ami Georges Clemenceau, le célèbre homme d'Etat. On y découvre son atelier à la découverte de son obsession : les Nymphéas.

Les salles proposent aussi des parcours plus ludiques comme *« Prince of Persia : Dagger of time »* conçu en partenariat avec le studio français Ubisoft. L'enseigne offre une expérience de divertissement inédite permettant aux clients de vivre un « escape game » virtuel dans l'univers du célèbre jeu.

Des ateliers plus classiques tournent autour de la formation comme *« Sauver des vies en apprenant les gestes de premiers secours »*, un outil de formation au secourisme puissant, créé en partenariat avec D'un Seul Geste pour sensibiliser et former aux gestes simples qui pourraient sauver des vies chaque année.

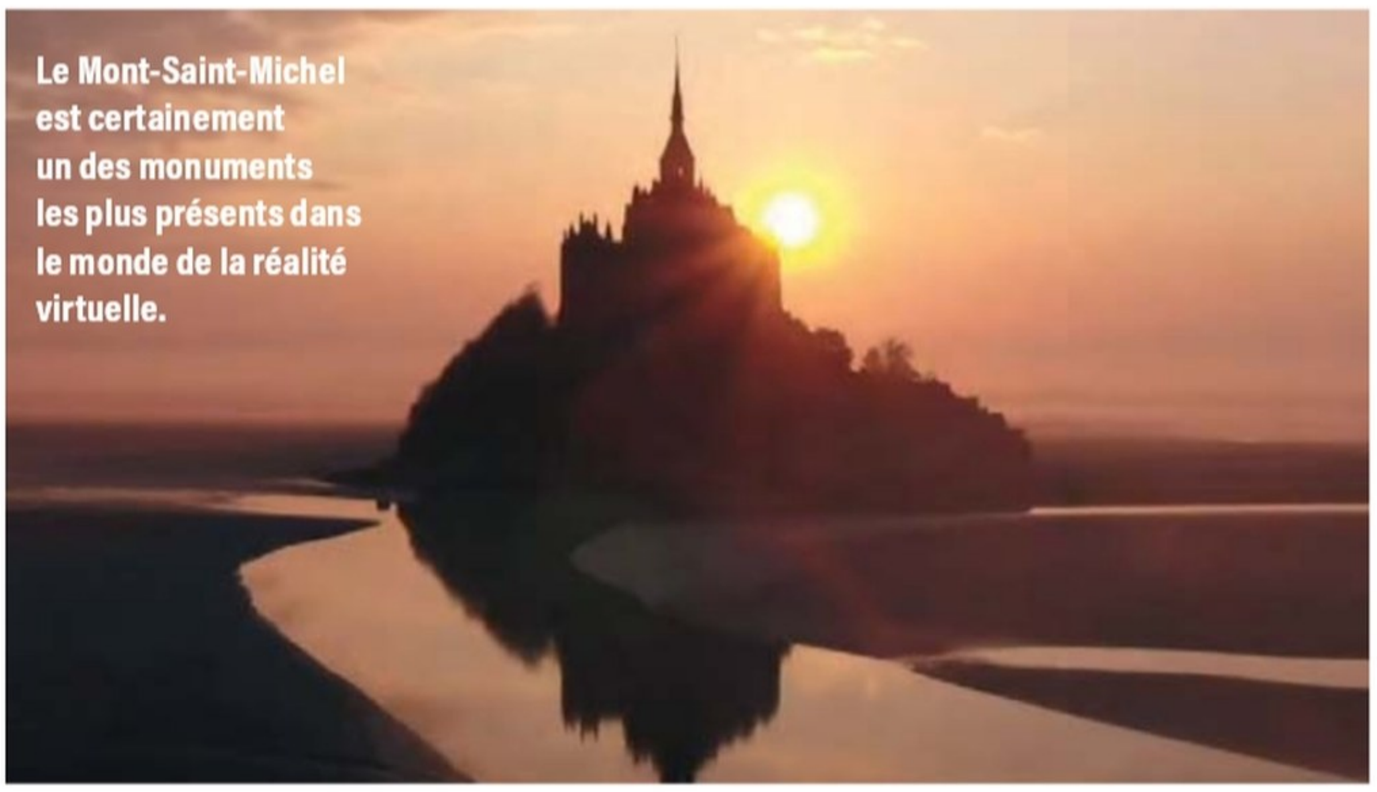
Un voyage dans la Grèce Antique...

Playful Culture, primé par le prix Pépite qui se définit comme un tremplin pour l'entreprenariat étudiant, développe de nombreux parcours virtuels pour les scolaires par des ateliers ludo-éducatifs avec réalité augmentée et gamification. Un des ateliers demande de ramener Emma, Sam et le chien Rocki qui ont été projetés dans la période archaïque de la Grèce antique. Les élèves doivent relever différents défis comme ceux du transport, de la nourriture et des jeux sportifs à l'aune des jeux qui se tiendront bientôt à Paris. L'idée de ces ateliers est venue lors du confinement à la fondatrice de Playful Culture pour aider les enfants à faire leurs devoirs d'histoire. La solution se présente comme un atelier d'une heure clé en main avec tablette et la présence d'un « médiateur culturel ». D'autres projets sont en cours avec pour thèmes un atelier sur la Commune de Paris et la Naissance de l'écriture.

Ou dans les plus grands monuments du monde

Il est, de plus, possible depuis quelques années déjà de visiter virtuellement les principaux monuments dans le monde et de revivre leur construction. Louvre, Château de Versailles, musée de l'Ermitage à Saint-Pétersbourg ou les grandes pyramides d'Égypte. Flyview, en collaboration avec une start-up française, propose cette expérience de réalité virtuelle à 360°. C'est le fruit d'une aventure entrepreneuriale et scientifique hors-norme qui a vu Iconem mener des campagnes de numérisation 3D à large échelle en Égypte à partir d'une technologie de radiographie haute définition composée de centaines de milliers de photos. □

B.G



Le Mont-Saint-Michel est certainement un des monuments les plus présents dans le monde de la réalité virtuelle.

FIC

Forum International
de la Cybersécurité

“Shaping Europe’s digital future”



7, 8 et 9 juin 2022

Lille Grand Palais

Organisé par

Gendarmerie nationale

avisa partners

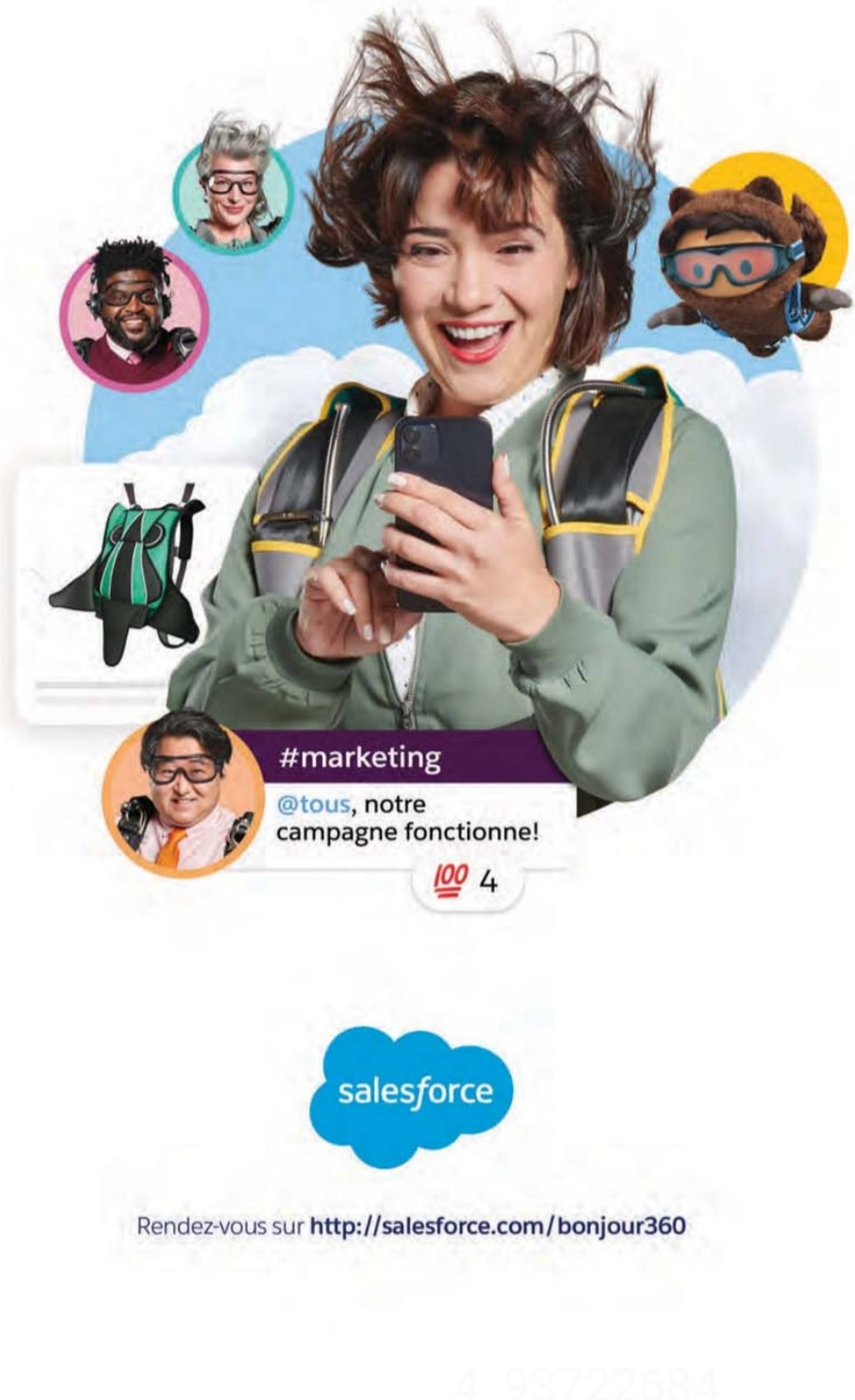
Avec le soutien de

Région Hauts-de-France

forum-fic.com

Mobilisez vos équipes autour de votre client

avec Customer 360 et Slack.



salesforce

Rendez-vous sur **http://salesforce.com/bonjour360**