Silicon

INSIGHTS FOR IT PROFESSIONALS

SPÉCIAL CLOUD

Silicon.fr

> STRATÉGIE CLOUD
QUELLE MÉTHODE POUR MIGRER SES APPLICATIONS

> SERVERLESS
POURQUOI FAUT-IL Y CROIRE

> CLOUD SOUVERAIN
UNE RÉALITÉ SEMÉE D'EMBUCHES

No Code
Des promesses et des limites

Rencontre
Farid Illikoud, CISO de Decathlon Technology

N° 13 - Décembre 2022

L 314277 - 7 - F: 25 € - RD

L'agence B2B au service de vos stratégies

Envie de booster votre performance marketing ? Contactez-nous !

WE FACTORY &co

hello@we-factoryandco.fr
01 41 31 72 44

MULTICLOUD CONFIANCE ET SOUVERAINETÉ

Depuis plus d'une décennie, on relève invariablement une croissance annuelle à deux chiffres du taux d'adoption du Cloud public. Et selon les prévisions, de Gartner à IDC, elle ne devrait pas faiblir au cours des cinq prochaines années. Pour un DSI, la question n'est donc plus de savoir s'il va adopter le Cloud mais quand il l'adoptera. Alors que les années 2010 ont vu l'essor des stratégies cloud hybride, nous sommes désormais résolument entrés dans l'ère du multicloud. Si ce choix n'est pas techniquement le plus simple à gérer (voir notre dossier page 25), il présente beaucoup d'avantages, en particulier celui d'échapper au piège du vendor lock-in ; traduction IT de l'expression « ne pas mettre tous ses œufs dans le même panier ». Mais ce n'est pas la seule problématique. Dans une Union Européenne qui a imposé la protection des données avec l'adoption du « Règlement Général sur la Protection des Données » (RGPD), les notions de confiance et de souveraineté se sont invitées dans un débat technologico-diplomatique qui place le Cloud au cœur du sujet. (voir notre dossier page 40). Le DSI doit-il accepter le « contrat de confiance » d'un hyperscaler américain qui dispose d'une région France/Europe ? Doit-il privilégier le choix d'un prestataire de l'UE, synonyme de souveraineté pour ses données ? On peut dire aujourd'hui, sans trop de se tromper, qu'il y a autant de réponses que de stratégies d'entreprise. Mais la question revêt une dimension stratégique pour l'avenir qui dépasse largement le seul cadre de la DSI.

Philippe LEROY
Rédacteur en chef
pleroy@netmedia.group

©Antoine Levesque

SOMMAIRE

FOCUS

LES TEMPS FORTS DE L'ACTUALITÉ

Cloud ..... p. 6-7
Cybersécurité ..... p. 8
Logiciels ..... p. 10
Data ..... p. 12
Carrière - formation ..... p. 14
Gestion des API, où en sont les principaux fournisseurs? ..... p. 16

MANAGER IT 2022

David Guillot de Suduiraut, AXA France ..... p. 18

ZOOM

Orange : les six femmes du COMEX ..... p. 19

DOSSIER

STRATÉGIE CLOUD

Migrer son portefeuille applicatif : un défi ! ..... p. 20
Retour d'expérience : Nexity ..... p. 25
Comment le multicloud s'est imposé comme le modèle dominant de l'IT ..... p. 26
Multicloud, pourquoi il faut miser sur le serverless ..... p. 32

PROGRAMMATION

Les langages sécurisés, prochain grand saut ? ..... p. 35

INTERVIEW

Farid Illikoud, Group Chief Information Security Officer (CISO) de Decathlon Technology ..... p. 36

CLOUD SOUVERAIN

Les mille et une voies du cloud de confiance ..... p. 40
VMWARE parie sur les partenariats locaux ..... p. 44

DÉVELOPPEMENT

Le no code : ses promesses, ses limites ! ..... p. 46
Finops, du bon usage des étiquettes ..... p. 52

CYBERSÉCURITÉ

Comment la menace change de visage ..... p. 56

Éditialis

98, rue du Château,
92645 Boulogne-Billancourt Cedex
Pour envoyer un e-mail à votre correspondant, suivre le modèle : pleroy@netmedia.group

NETMEDIA GROUP

PRÉSIDENT
Pascal Chevalier

DIRECTEUR GÉNÉRAL ET DIRECTEUR DE LA PUBLICATION
Hervé Lenglart

ÉDITORIAL

RÉDACTEUR EN CHEF
Philippe Leroy (01 53 32 10 08) pleroy@netmedia.group

RÉDACTION
Clément Bohic (cbohic@netmedia.group)
Ariane Beky (abeky@netmedia.group)

ONT PARTICIPÉ À CE NUMÉRO
Alain Clapaud, Xavier Biseul

RESPONSABLE DU STUDIO
Catherine Saulais

Réalisation - CONCEPTION GRAPHIQUE
Bench Media Factory
Direction : Christophe Gaillard
Maquette : Sylvain Giovagnoli
Secrétariat de rédaction : Philippe Legrain

COUVERTURE Antoine Levesque
CRÉDITS PHOTOS Adobe Stock

PUBLICITÉ

DIRECTEUR COMMERCIAL
Simon Leprat (01 41 31 72 41) sleprat@netmedia.group
DIRECTRICE DU DÉVELOPPEMENT COMMERCIAL
Cindy Martinez (01 53 32 10 07) cmartinez@netmedia.group

CHEF DE PUBLICITÉ
Mathilde Poirot (01 46 99 22 95) mpoirot@netmedia.group
Melissa Gomis (01 46 99 22 90) mgomis@netmedia.group

ABONNEMENT ET MARKETING

RESPONSABLE MARKETING et ABONNEMENT
Nicolas Cormier (01 41 31 72 44) ncormier@netmedia.group

CHARGES DE TRAFIC et RESPONSABLE DES PARTENARIATS
Irène Lemenager (01 46 99 72 40) ilemenager@netmedia.group

IMPRESSION
Léonce Deprez, allée de Belgique, 62128 Wancourt

TARIFS
Prix au numéro : France 25 €
Abonnement 1 an. France métropolitaine 120 € (TVA 2,10 %)
L'abonnement comprend le magazine en versions print et digitale accessible sur PC, tablettes et smartphones, la newsletter quotidienne et l'accès au site silicon.fr
4 numéros par an. Trimestriel
Abonnement 1 an. Étudiant, DOM-TOM et étranger : nous contacter

Silicon est édité par Éditialis, SAS au capital de 136 000 €
Actionnaire NetMedia Group
N° ISSN : 2681-1006
Numéro de commission paritaire : 1221T94134
Dépôt légal : novembre 2019
Origine du papier : Hallsta, Suède
Eutrophisation des eaux : 50 g
Gaz à effet de serre : 969 kg

PEFC 10-31-1495 Cette entreprise a fait certifier sa chaîne de contrôle. pefc-france.org

L'éditeur décline toute responsabilité en cas de perte, détérioration ou non-retour des documents qui lui sont confiés. Il se réserve le droit de refuser toute demande d'insertion sans avoir à motiver son refus.

IMPRIM'VERT

Cloud XPR

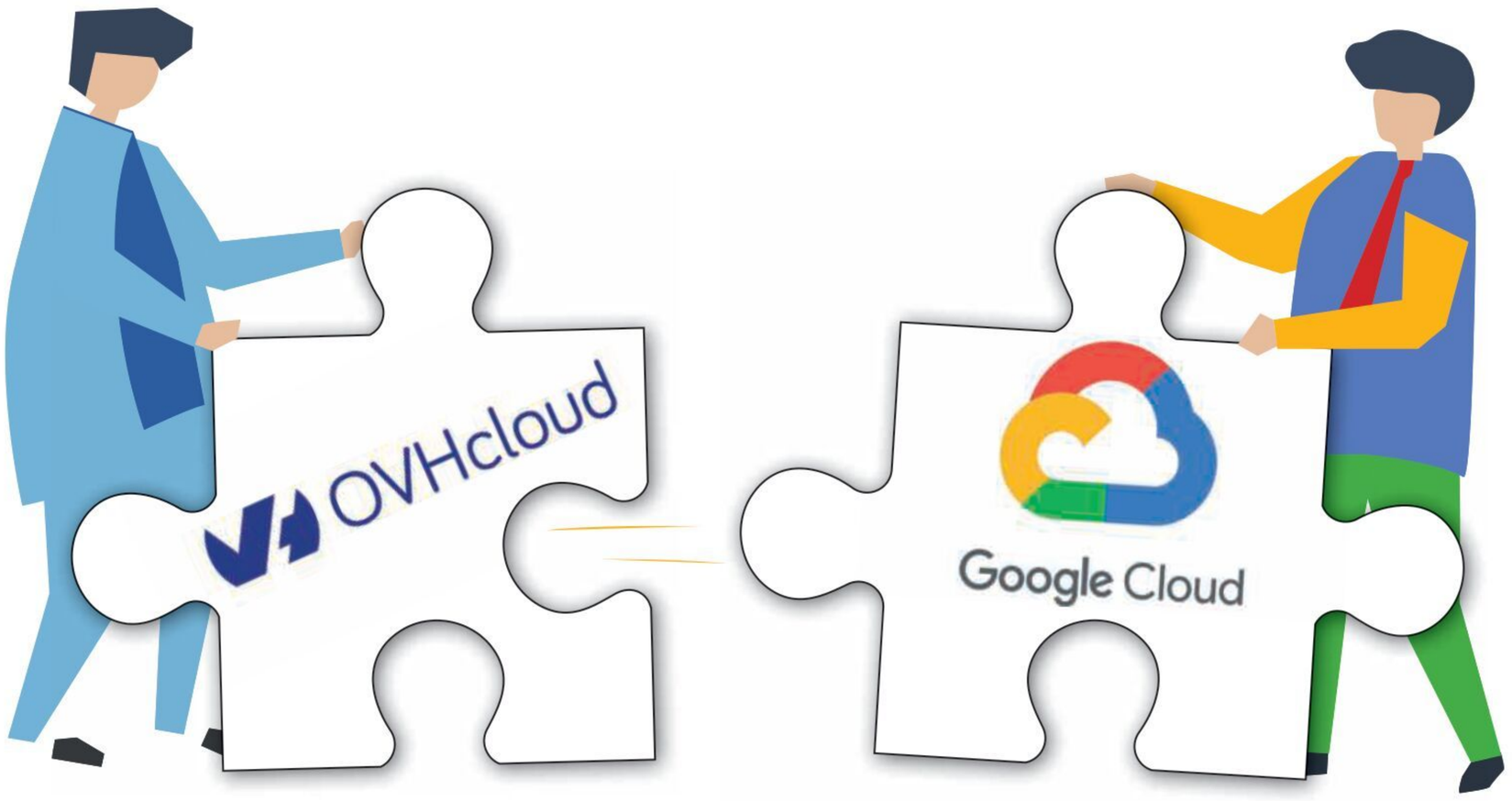
SIMPLIFIEZ LA MIGRATION ET L'EXPLOITATION DE VOS APPLICATIONS CRITIQUES DANS LE CLOUD

Jaguar network

JAGUAR-NETWORK.COM

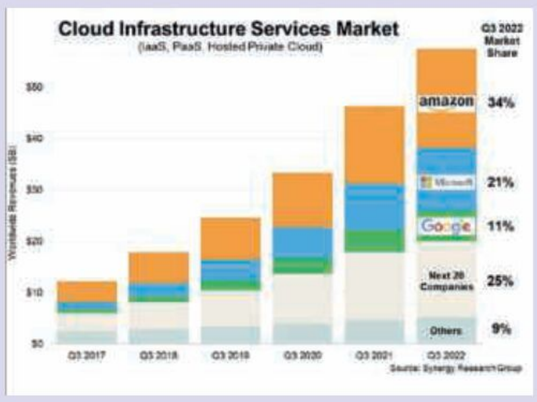
Restez connectés >

CLOUD SOUVERAIN : OVHCloud et Google Cloud se séparent



Le partenariat entre OVHCloud et Google Cloud sur l'utilisation d'Anthos – la plateforme kubernetes de gestion d'applications sur site et dans le cloud – est terminé. *« Cette décision résulte d'un constat conjointement partagé (...) mais ne remet en cause ni les technologies développées ni les possibilités de futures collaborations »*, ont annoncé les deux groupes, deux ans après son lancement. Ce sont les conditions d'exploitation et de gestion d'Anthos sur l'infrastructure du fournisseur roubaisien qui aurait fait capoter l'accord : *« Le groupe français OVHCloud a renoncé à utiliser un logiciel de Google pour son offre de cloud, faute d'accord sur les conditions de mise à jour du produit »*, ont-elles indiqué. Selon leur explication, l'hyperscaler américain souhaitait que les mises à jour s'effectuent directement via une connexion informatique quand le groupe français voulait procéder par ses propres moyens.

INFRASTRUCTURE CLOUD : AWS, MICROSOFT ET GOOGLE CAPTENT 66 % DU MARCHÉ



Les trois hyperscalers maintiennent à distance la concurrence avec 34 % du marché revenant à AWS, 21 % à Microsoft et 11 % à Google Cloud. Leur domination est plus marquée sur les segments IaaS et PaaS publics dont ils contrôlent 72 %. *« Tous les autres fournisseurs voient reculer leur part de marché »*, explique John Dinsdale, analyste chez Synergy Research Group.

NUMSPOT : nouvel acteur pour un cloud de confiance

Dix ans après Cloudwatt et Numergy, voici Numspot. Le premier comptait Orange dans ses rangs ; le deuxième, SFR. Cette fois, c'est Bouygues Telecom qui s'implique. Pour un objectif similaire : constituer une offre de cloud « souverain ». Dassault Systèmes est aussi de l'initiative, comme la Banque des territoires (Caisse des dépôts). L'un pour l'infrastructure (Outscale). L'autre comme investisseur. Docaposte est le chef de file. Le lancement des services est annoncé pour 2023.

NUMÉRIQUE DE CONFIANCE : OVHCloud va impulser le comité

Michel Paulin est chargé par le gouvernement de constituer un comité de filière « numérique de confiance ». Le directeur général d'OVHCloud devra, sous six mois, soumettre une proposition sur la composition, la gouvernance et les objectifs de cette entité. En l'articulant avec les comités existants, en particulier pour les industries de sécurité et les industries du futur. Une création qui s'inscrit dans la « stratégie nationale pour le cloud » présentée début 2021.

Cloud Seed
le joker de GitLab et Google

Cette collaboration entre la plateforme devops et l'hyperscaler a été présentée à l'écosystème de développeurs et partenaires lors de l'événement Google Next'22. Cloud Seed permet aux développeurs de déployer des applications web dans Google Cloud sans quitter GitLab.

Red Hat
investit le projet CoCo

Le projet Confidential Containers (CoCo) est soutenu par la Cloud Native Computing Foundation (CNCF) avec un niveau de maturité « sandbox » (non incubé donc). Red Hat a confirmé s'y investir.

Cloudflare
1,25 Md $ pour financer des start-up

Le spécialiste du NaaS promeut le programme Workers Launchpad. Jusqu'à 1,25 milliard $ est dévolu à des jeunes pousses en phase d'amorçage qui devront utiliser la plateforme Cloudflare Workers pour leurs développements applicatifs. Elles seront sélectionnées et financées par 26 capital-risqueurs partenaires.

ALLOY, atout souverain pour Oracle ?

Le groupe américain a annoncé Alloy dans le cadre de son événement CloudWorld 2022. L'offre permettra aux clients d'héberger les services OCI (Oracle Cloud Infrastructure) dans leurs datacenters sur le modèle des « régions dédiées ». Surtout, il leur procure de quoi « devenir des fournisseurs cloud ». D'un côté, les outils pour développer leurs propres services sur ce socle ; y compris en intégrant des ressources externes, jusqu'aux mainframes. De l'autre, pour gérer la commercialisation. Avec, notamment, une instance de l'ERP Fusion Cloud et des capacités de personnalisation (marque blanche). Oracle annonce l'échéance d'avril 2023 pour une première version expérimentale d'Alloy. On surveillera, en parallèle, le lancement des « régions cloud souveraines », qui restent sa principale réponse aux enjeux de souveraineté à l'échelle européenne.

GITHUB REVENDIQUE 94 MILLIONS DE DÉVELOPPEURS

La filiale de Microsoft a révélé quelques chiffres clés dans son rapport Octoverse. GitHub affiche une communauté de 94 millions de développeurs et contributeurs de l'écosystème open source, dont 20,5 millions de nouvelles recrues en 2022. Par ailleurs, la plateforme a récemment atteint un chiffre d'affaires annuel récurrent de 1 milliard $,

KYNDRYL + MICROSOFT : passer du mainframe au cloud

Les deux sociétés ont annoncé une initiative conjointe visant à faciliter la migration de données mainframe vers le cloud. L'accord porte sur la création de canaux de données entre des grands systèmes ou ordinateurs centraux (mainframes) utilisés par des clients Kyndryl et le cloud de Microsoft. Les systèmes et logiciels mainframes concernés sont les IBM des gammes iSeries et zSeries, ainsi que zCloud, l'infrastructure en tant que service managé par Kyndryl pour IBM Z.

DAAS : Red Hat Enterprise Linux rejoint AWS

Le système d'exploitation Red Hat Enterprise Linux for Workstations est disponible en mode « desktop-as-a-service » (DaaS) sur AWS. Pour l'exécuter, Red Hat recommande aux utilisateurs de s'appuyer sur le protocole d'affichage à distance haute performance NICE DCV fourni par Amazon. NICE DCV est disponible avec des clients natifs pour Windows, Linux et MacOS. Les utilisateurs peuvent aussi accéder à RHEL WS depuis le navigateur web de leur choix.

Cloud sectoriel

Le boom

Gartner

Selon Gartner, plus de 50 % des entreprises dans le monde seraient amenées à utiliser des plateformes cloud « sectorielles » pour soutenir leur activité commerciale d'ici à 2027. Combinant logiciels et infrastructures en tant que service (SaaS, PaaS et IaaS), elles permettent de répondre aux attentes spécifiques de différentes industries.

Sophie Papillon

rejoint Cloudera en France

En provenance de Veeva où elle pilotait les équipes commerciales en Europe du Sud, Sophie Papillon dirige les activités en France avec le titre de Regional Vice-President.

VMware France

Marc Dollois, nouveau DG

Entré en 2015 chez le spécialiste de la virtualisation comme responsable de compte, il a évolué dans différentes fonctions commerciales en France et en Europe. VMware est en procédure de rachat par Broadcom après s'être émancipé de Dell en 2021.

LE CAMPUS CYBER de Nouvelle-Aquitaine sur la rampe de lancement

Annoncée en mai 2022, la création d'un Campus Cyber Nouvelle-Aquitaine est sur les rails. Il sera ouvert d'ici à la fin de l'année au sein du parc Ampéris, à Pessac, un ancien site industriel de Thalès, regroupant 20 000 m² dédiés à la filière cyber. Le Campus Cyber Nouvelle-Aquitaine sera piloté par une association rassemblant les quatre structures fondatrices : le GIP Cybermalveillance, l'Agence de développement et d'innovation de Nouvelle-Aquitaine (ADI-NA), le CLUSIR et la Région Nouvelle-Aquitaine. Cette dernière lui a accordé 370 000 € pour l'année 2022 et a engagé un million pour lancer le projet dans le cadre de sa feuille de route pour la cybersécurité. Selon le conseil régional, une cinquantaine d'entreprises, associations, collectivités, écoles, universités, laboratoires de recherche, ordres professionnels ont déjà adhéré à l'association.

17 PROJETS CYBER CLÉS INVESTIS PAR LA FRANCE

Jean-Noël Barrot, ministre délégué chargé de la Transition numérique et des Télécommunications a dévoilé la liste de 17 nouveaux projets « d'envergure » associés au plan France 2030. Sélectionnés dans le cadre de cinq appels à projets et à manifestation d'intérêt, les projets lauréats vont bénéficier de 39 millions € de financements publics.

GARTNER distingue les leaders du SIEM

Ils sont cinq à figurer au carré des « leaders » du Magic Quadrant 2022 du SIEM. : Exabeam, IBM, Microsoft, Securonix et Splunk. Leur position résulte de la combinaison d'évaluations sur deux axes. L'un prospectif (« vision »), centré sur les stratégies (sectorielle, géographique, commerciale, marketing, produit...). L'autre axé sur la capacité à répondre effectivement à la demande (« exécution » : expérience client, performance avant-vente, qualité des produits/services...).

XDR : Tehtris lève 44 millions €

Tehtris annonce une deuxième opération de 44 millions. Les fonds qui avaient mené la série A – Tikehau Ace, Open CNP le fonds de Corporate Venture de CNP Assurances, et de Nouvelle-Aquitaine Co-Investissement (NACO) – participent à cette nouvelle levée menée par Jolt Capital, spécialiste du capital-investissement dans les entreprises deeptech. Tehtris propose une plateforme xDR (extended detection and response) qui regroupe plusieurs solutions de cybersécurité (EDR, MTD, SIEM...) au sein d'un socle unique.

Pradeo s'offre la start-up Yagaan

Pradeo, axée sur la protection de flottes mobiles, acquiert Yagaan Software Security qui a développé une offre logicielle de sécurité applicative. La jeune pousse fondée en 2017 accompagne des équipes DevSecOps dans leurs activités d'audit et de revue de code source.

Adrien Vandeweeghe à la direction de Trellix en France

En provenance de CS Group, auquel il avait cédé sa société de conseil et d'intégration Novidy's, le nouveau directeur de Trellix a pour mission de développer commercialement la filiale française.

La cyber toujours peu féminisée

Selon des données agrégées par l'International Information Systems Security Certification Consortium (ISC), les femmes représentent 25 % de la main-d'œuvre au sein de la cybersécurité mondiale. Une proportion équivalente ou presque à celle du secteur IT dans son ensemble.

GESTION IT : faire rimer simplicité et performance

De la PME aux grands comptes, aucune entreprise n'échappe à ce triple phénomène de digitalisation accélérée, de rationalisme économique et de pragmatisme environnemental. Alexis Valero, co-fondateur et CEO de Rzilient revient sur l'importance d'une gestion informatique optimisée.

« *Tout le problème de l'IT,* indique Alexis Valero, co-fondateur et CEO de Rzilient, *c'est que trop souvent les entreprises ne mesurent pas l'importance d'une gestion rigoureuse et pragmatique de leur parc, et l'opportunité qu'elle représente* ». Mais, à l'heure où la digitalisation des activités devient la norme, la dépendance des entreprises, quelle que soit leur taille, à l'IT est considérable. En jeu — pour les IT managers, Office Managers ou Tech Leads, comme pour les infogérants et leurs clients — des gains de temps et d'efficacité et une réduction de budget considérables. C'est en réponse à ce constat qu'est née Rzilient, une plateforme de gestion informatique tout-en-un qui répond à une triple promesse : simplifier et centraliser le pilotage informatique, allonger la durée de vie du matériel, et automatiser les opérations IT. Si l'on se réfère aux chiffres de l'ADEME, le nombre d'équipements IT augmente de 50 % par an et la durée d'utilisation d'un ordinateur a été divisée par 3 depuis 1985. « *Des rotations de matériel toujours plus nombreuses, un enrôlement aux outils de pilotage à distance et de sécurisation toujours plus fréquent et chronophage, la gestion de parc IT devient un exercice à part entière et nous avons cherché à développer un outil sur mesure* », indique Alexis Valero.

silicon

Une promesse de simplicité

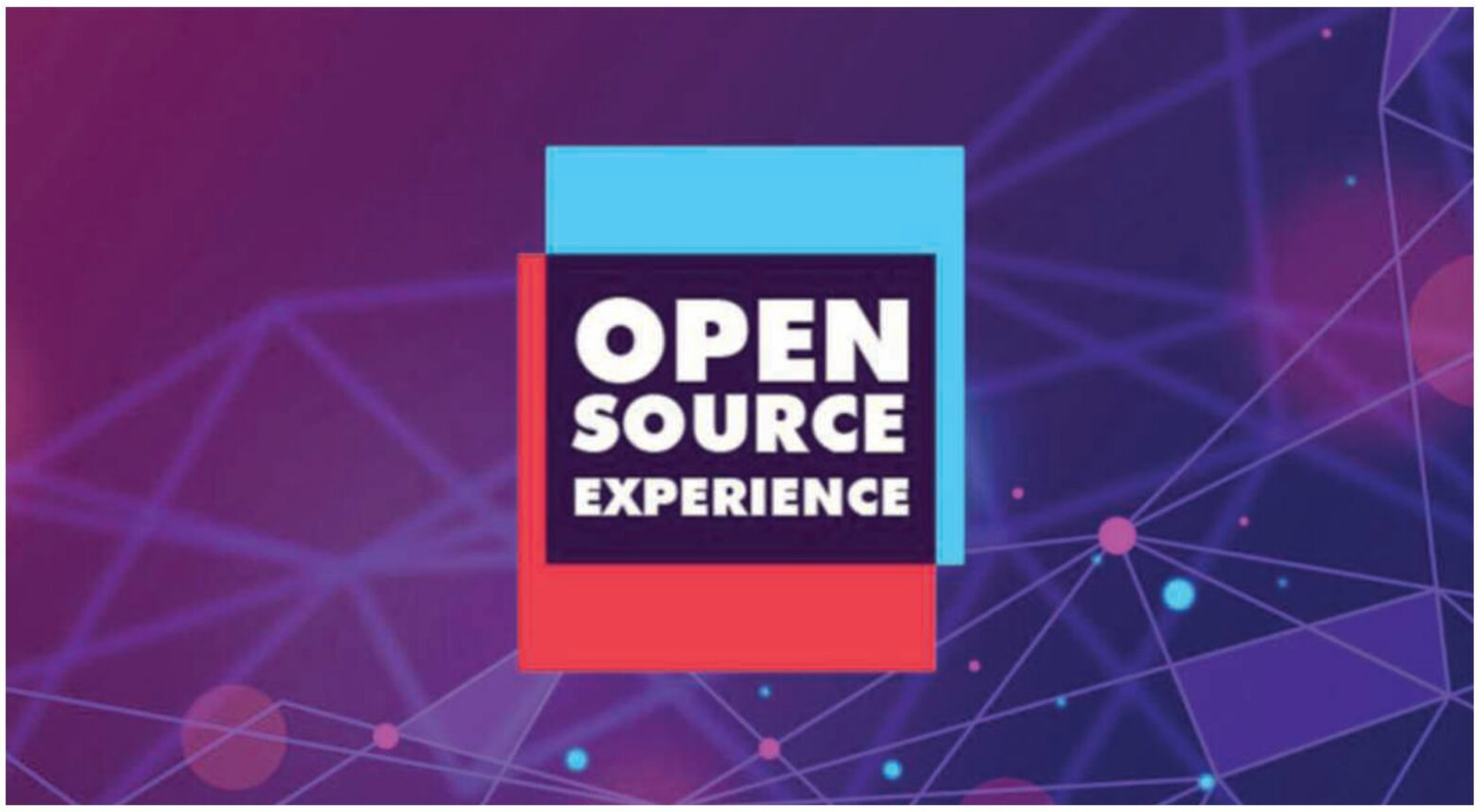
Le concept de Rzilient est simple. Une plateforme unique qui permet de centraliser l'ensemble des tâches liées à la gestion d'un parc informatique, depuis l'approvisionnement, en passant par l'inventorisation et la sécurisation des postes de travail, le pilotage des opérations de maintenance ou encore l'automatisation des déploiements : tout peut être administré depuis une interface unique. « *La visibilité à 360 degrés sur les assets disponibles et l'offre servicielle permet de s'assurer que chaque salarié possède la machine et les services adaptés à ses besoins comme à ses missions* », précise Alexis Valero. Les fonctionnalités d'onboarding et d'offboarding de Rzilient adressent pertinemment cet enjeu. Mais, la gestion IT, c'est aussi la maîtrise des coûts ! Là encore, Rzilient offre une visibilité optimale sur la réalité du parc informatique tant sur le plan fonctionnel que financier et même sur le plan environnemental. « *Tout doit être mis en œuvre pour allonger la durée de vie des parcs informatiques car les ressources ne sont pas inépuisables, c'est pourquoi nous proposons l'intégration de matériels reconditionnés à l'achat ou en leasing car c'est une demande des collaborateurs* ».

La proactivité : le grand défi de 2023 !

Alexis Valero dresse un constat sans appel : « *L'IT est au cœur de tous les enjeux de compétitivité des entreprises. Une gestion optimisée, simplifiée, consolidée des parcs informatiques agit comme une perspective d'économies financières, d'économies de temps et d'économies carbone* ». La solution de Rzilient, qui s'adresse autant aux managers non-experts qu'aux DSI ou acteurs de l'infogérance, a été pensée pour répondre à ces différents enjeux à la confluence de la performance, de la RSE et du pragmatisme économique. « *L'infogérance est encore trop souvent inscrite dans une dimension réactive, face aux pannes, aux incidents, aux déploiements… Notre solution ouvre la voie à une gestion proactive, plus efficace, plus stratégique au bénéfice des collaborateurs comme de l'entreprise* », conclut Alexis Valero. ■

rzilient

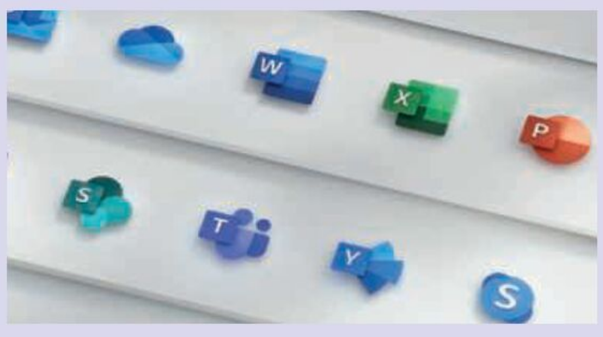
OPEN SOURCE
Un écosystème prospère en France



Le CNLL, Numeum et Systematic Paris-Region ont livré les résultats d'une étude Markess sur l'open source en France et en Europe dans le cadre du salon Open Source Experience. Dans l'Hexagone, le marché du logiciel libre et open source pèse 5,9 milliards € et représente plus de 60 000 emplois directs en 2022. Le secteur devrait croître en moyenne de 7,8 % par an d'ici à 2027 pour atteindre 8,7 Md€. À cette échéance, le nombre d'emplois équivalents temps plein (ETP) augmenterait de 26 400, passant de 63 800 à 90 200 ETP qui développent et intègrent des solutions open source. Développeurs, devops, marketeurs, architectes et consultants métier constituent le top 5 des profils les plus recherchés par l'écosystème open source. L'IoT, les API et les conteneurs forment le top 3 des domaines de compétences les plus prisés.

MICROSOFT 365 REMPLACE (TOUT) OFFICE

Ne l'appelez plus Office, mais Microsoft 365. Certes, dès 2017, l'éditeur américain avait renommé Office 365 en Microsoft 365, sa plateforme logicielle de productivité basée dans le cloud. Mais dorénavant, Microsoft 365 devient la marque phare qui succède à Office dans son ensemble. La bascule débutera en novembre 2022 pour Office.com, et en janvier 2023 pour les apps Office sur smartphones et ordinateurs personnels.



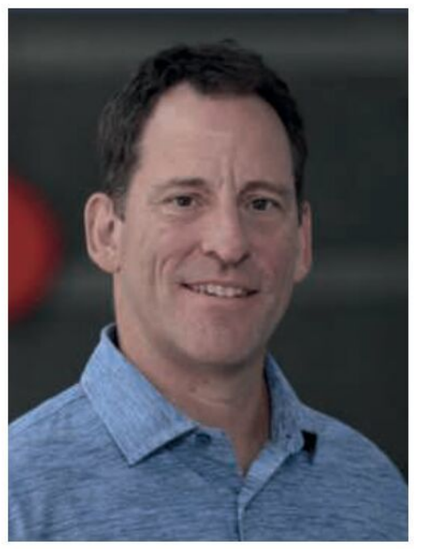
LINUS TORVALDS veut tourner la page i486

Introduit au printemps 1989, le microprocesseur i486, également nommé Intel 486 ou 80486, n'est plus produit par Intel depuis 2007. Le noyau Linux doit-il alors toujours prendre en charge ces puces exploitant le jeu d'instructions x86 (CISC) ? Linus Torvalds a son idée. « Nous nous sommes débarrassés de la prise en charge d'i386 en 2012. Peut-être est-il temps de nous défaire du support d'i486 en 2022 », s'est interrogé, sur la Linux Kernel Mailing List (LKML), le créateur du noyau Linux et de Git.

CLOUD SEED : le joker de GitLab et Google

Cloud Seed, projet de collaboration entre la plateforme devops GitLab et de Google Cloud, prend forme. Une solution stable a été présentée lors de l'événement Google Next' 22. Solution open source, Cloud Seed est directement intégrée à l'interface utilisateur web de GitLab et exploite ses pipelines d'intégration et de déploiement continus (CI/CD). L'objectif est de simplifier, automatiser et accélérer le déploiement et la configuration de ressources cloud.

Nouveau DSI chez Red Hat



Jim Palermo prend le relais de Mike Kelly, parti chez a16z (Andreessen Horowitz). Profil « maison », il a rejoint Red Hat en 2010 comme responsable IT infra pour les Amériques. Dernièrement, il était VP chargé de la livraison de solutions numériques (DSD) au siège de l'entreprise, à Raleigh (Caroline du Nord).

Firmware propriétaire pour Debian

debian

Debian 12 va officiellement inclure du microgiciel propriétaire. Un coup de canif dans le « contrat social », une avancée pour les nouveaux utilisateurs de l'OS libre.

Olvid-Oodrive-Tixeo alliance pour une « bureautique souveraine »

Le consortium a monté le projet « TOO 2022 » pour proposer une alternative française à Teams. Tixeo fournira la brique visio ; Olvid, la messagerie instantanée ; Oodrive, l'édition et le partage de documents. La commercialisation est envisagée au deuxième semestre 2023.

AGIR AVEC CERTITUDE
grâce aux données

Prendre les bonnes décisions au bon moment est un défi toujours plus complexe pour les chaînes d'approvisionnement. Mais en plaçant la donnée au cœur de sa transformation, et en tirant profit des nouvelles capacités des plateformes data intégrées, des améliorations significatives sont au rendez-vous.

Volatilité des prix, pénurie des ressources, nouvelles exigences de la demande... Les circuits d'approvisionnement sont plus que jamais mis à mal, obligeant les entreprises à trouver des solutions innovantes pour décider plus rapidement, mieux anticiper, mieux s'organiser. *« Dans un contexte d'internationalisation et d'externalisation des productions, la dépendance à des aléas extérieurs est d'autant plus forte. Obtenir une vision globale, transversale, pouvoir piloter les activités et prédire l'impact des événements à venir deviennent des défis majeurs que seule la maîtrise intelligente de la donnée permet de relever »*, indique Valérie Soubiran, Directrice Marketing du fournisseur de solutions de Business Intelligence Qlik. Ces enjeux s'inscrivent par ailleurs dans une évolution où la maîtrise des coûts et les impératifs RSE doivent également être mieux pris en compte.

Valérie SOUBIRAN
Directrice Marketing de Qlik

Spécialisée dans les solutions d'analyse des données et de datavisualisation, Qlik a étendu ces dernières années son offre à la partie amont de la chaîne de transformation de la donnée, avec des outils d'intégration et de catalogue de données, et d'automatisation de la création des datawarehouses et des data lakes. *« Notre mot d'ordre aujourd'hui est la maîtrise de l'information de bout en bout. Pour gérer au mieux les climats de crise, anticiper les risques et favoriser l'aide à la décision, il faut accélérer la mise à disposition des bonnes informations aux métiers, en disposant d'un pipeline de données de bout en bout »*, assure Valérie Soubiran. Un changement qui passe par l'intégration des solutions analytiques à l'ensemble de l'écosystème des entreprises, dans des environnements forcément hétérogènes incluant les fonctionnements cloud, on-premise, avec souvent de multiples fournisseurs.

Technologies innovantes et acculturation

L'intégration de fonctionnalités d'intelligence artificielle et de machine learning font partie des clés de l'évolution des plateformes analytiques. Elles aident à la prédictibilité des phénomènes, comme le risque de départ d'un salarié, la prédiction des ventes ou l'évolution des comportements clients. Il s'agit aussi de pouvoir déclencher des actions au niveau opérationnel : *« si l'analyse des livraisons en cours montre que les capacités d'un livreur à un temps donné se trouvent dépassées par la demande, on peut imaginer envoyer directement les commandes concernées vers un deuxième transporteur, et déclencher en même temps une alerte vers le responsable du transport »*, illustre Valérie Soubiran.
L'avantage d'une solution agile d'exploration des données s'illustre notamment avec la fusion entre le géant de l'industrie ferroviaire Alstom et Bombardier, annoncée en 2021. Le développement d'une application Qlik a permis en quelques semaines de consolider les données issues de deux systèmes d'information différents et de fournir une vision précise des activités une fois celles-ci réunies, pour une prise de décision éclairée par la donnée. En matière d'achats par exemple, cette application permet aux utilisateurs métiers de connaître, pour un fournisseur particulier, le volume d'achat de Bombardier et d'Alstom, ainsi que les prix négociés pour chaque produit par les deux acteurs.
Les cas d'usages sont innombrables. Pour se lancer, les entreprises doivent identifier le périmètre d'exploitation de la donnée qui leur apportera le plus de valeur, mettre en place les bonnes règles de gouvernance et impliquer les métiers au plus tôt pour qu'ils imaginent de nouveaux processus imbriqués entre l'analytique et l'opérationnel, en profitant des nouvelles capacités des plateformes data modernes. ■

KYNDRYL + MICROSOFT ou comment passer du mainframe au cloud

Le partenariat stratégique négocié l'an dernier entre Microsoft et Kyndryl prend forme. L'accord porte sur la création de canaux de données entre des grands systèmes ou ordinateurs centraux (mainframes) utilisés par des clients Kyndryl et le cloud de Microsoft. Les systèmes et logiciels mainframes concernés sont les gammes iSeries et zSeries, ainsi que zCloud, l'infrastructure en tant que service managée par Kyndryl pour IBM Z. Les données mainframe seront associées à d'autres sources de données internes et externes accessibles en mode cloud. Il s'agit de soutenir la création et l'analyse de flux et applications data par des utilisateurs métiers. Pour ce faire, la suite d'applications « low code » Microsoft Power Platform sera employée.

OPEN WEB SEARCH : VERS UN GOOGLE EUROPÉEN ?

En gestation depuis 2019, le projet Open Web Search se lance officiellement, à l'appui d'un financement européen de 8,5 M€. Le projet compte notamment exploiter Galileo et Copernic pour traiter la dimension des données géospatiales. Il fait aussi référence aux moteurs de recherche expérimentaux Chat Noir et Args (Argument Search). Et à Open Console pour les webmasters.

IBM PREND LA MAIN sur les technologies Red Hat

Le portefeuille stockage de Red Hat va fusionner avec celui d'IBM. En première ligne, Ceph et OpenShift Data Foundation. Une « semi-acquisition » ? IBM emploie ce terme à propos de l'absorption des solutions et des équipes associées. Ceph, tout comme OpenShift Data Foundation, *« restera 100 % open source »,* nous assure-t-on. Red Hat continuera par ailleurs à vendre les deux produits, qui resteront respectivement à la base de son OpenStack et d'OpenShift.

STOCKAGE COMPUTATIONNEL : une spécification émerge

Les principaux travaux réunissant l'industrie IT autour du stockage dit « computationnel » ont abouti à la publication d'une spécification qui balaye quatre axes majeurs : découverte, configuration, sécurité et utilisation. Elle ne restreint ni le choix des interfaces physiques ni celui des protocoles de stockage. Son objectif : poser un socle commun pour l'intégration de capacités de calcul au plus près du stockage pour maximiser les performances.

DALL·E est disponible

Le modèle génératif d'images d'OpenAI, est désormais accessible par API. Trois options : créer des images, en éditer ou en faire des variations. Sur la question des droits d'exploitation : on peut republier et commercialiser, sans limites, toute image conçue avec DALL·E.

Capgemini acquiert Quantmetry

Fondé en 2011, Quantmetry s'est spécialisé dans la modélisation mathématique des données et le développement de solutions d'intelligence artificielle (IA) au service de la gouvernance et de la prise de décision. Ses 120 collaborateurs vont renforcer Capgemini Invent, la marque de data science, d'innovation numérique et de design créatif du groupe Capgemini.

PyTorch passe à la Fondation Linux

Meta confie PyTorch à la Fondation Linux. Cinq industriels vont le rejoindre au comité de pilotage : AMD, AWS, Google Cloud, Microsoft et NVIDIA.

Hexadrone cible la data publique

Cette coentreprise détenue par Orange et la Banque des territoires va cibler les collectivités. Sa promesse : les aider à collecter, sécuriser, traiter et valoriser leurs données, dans des formats « standardisés », avec une plate-forme « ouverte ». Le lancement commercial est prévu au deuxième semestre 2023.

QUAND

VOUS REFERMEZ

UN

UNE NOUVELLE VIE

S'OUVRE À LUI.

EN TRIANT VOS JOURNAUX,
MAGAZINES, CARNETS, ENVELOPPES,
PROSPECTUS ET TOUS VOS AUTRES
PAPIERS, VOUS AGISSEZ POUR UN MONDE
PLUS DURABLE. DONNONS ENSEMBLE
UNE NOUVELLE VIE À NOS PRODUITS.

CONSIGNESDETRI.FR

CITEO

Le nouveau nom d'Eco-Emballages et Ecofolio

LES 10 MÉTIERS IT les mieux payés en 2023

Selon le « guide des salaires 2023 », établi par le cabinet de recrutement spécialisé Robert Half, le niveau des rémunérations reste le premier critère pour attirer et retenir les professionnels IT les plus demandés, devant l'équilibre entre activité professionnelle et vie privée, sans oublier la flexibilité (des horaires jusqu'au travail hybride).

1. **Directeur des systèmes d'information (DSI) :** 115 500 €
2. **Responsable de la sécurité des SI (RSSI) :** 94 500 €
3. **Ingénieur DevOps :** 78 750 €
4. **Architecte logiciel :** 73 500 €
5. **Lead développeur :** 68 250 €
6. **Responsable infrastructure IT :** 68 250 €
7. **Chef de projet maîtrise d'ouvrage/assistance à maîtrise d'ouvrage (MOA/AMOA) :** 66 150 €
8. **Responsable SI :** 65 100 €
9. **Manager IT :** 63 000 €
10. **Expert cybersécurité :** 63 000 €

CISCO VEUT RAPPROCHER OFFRE ET DEMANDE

L'équipementier souhaite étendre la portée de la Cisco Networking Academy (CNA), son programme mondial de formation professionnelle dans les technologies de l'information et la cybersécurité. Objectif : contribuer à la formation de quelque 25 millions de personnes en l'espace de dix ans. La CNA a été lancée en 1997, aux États-Unis et en 2001 en France.

RECORD D'EMBAUCHES de cadres dans le secteur IT

Selon les données de l'Apec, le niveau d'emploi cadre dans l'informatique a battu des records entre le premier semestre 2021 et le premier semestre 2022 : +27 % de recrutements de cadres informaticiens. C'est 34 % de plus qu'en 2020. Le taux progresse plus vite que pour l'ensemble des recrutements de cadres. Six recrutements sur dix sont réalisés dans la région Île-de-France et 79 % des cadres informaticiens sont recrutés par des entreprises du secteur informatique et télécoms.

RED HAT opte pour le « office-flex »

La filiale open source d'IBM propose à la plupart de ses 19 000 employés dans le monde, d'effectuer tout ou partie de leur travail au bureau ou de ne pas s'y rendre du tout. Ceux qui viennent au bureau réservent leur poste de travail en ligne. Le dispositif avait été initié avant la crise sanitaire mondiale de 2020, avec plus de 30 % des employés qui travaillaient déjà à distance. Il a été étendu depuis.

Timothy Campos

nouveau DSI d'Apple

Il dirigera le département des systèmes d'information et des technologies (IS&T), chargé de la gestion de l'infrastructure soutenant les services en ligne, le site web ainsi que le support client, depuis le siège à Cupertino (Californie).

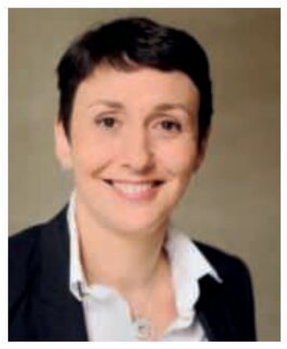
Cegid s'offre

DigitalRecruiters

L'éditeur lyonnais ajoute à ses actifs HCM la plateforme cloud de recrutement multisite et multimarque DigitalRecruiters. Celle-ci propose en mode SaaS des sites de gestion de carrière et de candidatures en marque blanche.

Groupe Bouygues

Marie-Luce Godinot prend la direction des SI



Au sein du groupe depuis 20 ans, elle prend la responsabilité de l'innovation, du développement durable (climat et biodiversité) et des SI (cybersécurité, digitalisation, IA). Marie-Luce Godinot est rattachée à Edward Bouygues, DG délégué de Bouygues SA et, par ailleurs, président de Bouygues Telecom.

DESIGN, ROBUSTESSE, SÉCURITÉ ET ASSISTANCE

Avec du style, un design fin et un traitement puissant, la série ThinkBook est conçue pour impressionner : performances remarquables, conception solide et fonctionnalités intelligentes.

Depuis 2020, tout ce qui concerne le travail a changé. En effet, qu'il s'agisse de l'endroit où nous travaillons, de la façon dont nous accomplissons le travail ou de la raison pour laquelle nous le faisons en premier lieu. Que les collaborateurs travaillent à domicile, dans un café ou dans un espace de travail en coworking, Lenovo propose des solutions technologiques hybrides pour vous aider à rester connecté.

La collaboration étant plus importante que jamais pour les collaborateurs hybrides, les équipes ont besoin d'une puissance informatique dotée d'une conception axée sur les personnes et des performances axées sur l'innovation pour être plus compétitive.

Dotés de fonctionnalités intelligentes, les ordinateurs portables ThinkBook vous offrent, à vous et à votre équipe, la technologie dont vous avez besoin pour transformer votre passion en productivité.

En effet, les PC portables ThinkBook de Lenovo sont les outils essentiels pour les petites et moyennes entreprises. Alliant élégance et fonctionnalités pensées pour les employés modernes, ces ordinateurs hybrides permettant de doper la productivité en toute situation. Conçus pour les nouveaux collaborateurs, les PC portables de la gamme ThinkBook vous offrent tout ce dont vous avez besoin dans un appareil de travail, et bien plus encore. Puissants, polyvalents et ultraportables, ces appareils s'adaptent à tous les styles de travail. Avec des appareils convertibles et 2-en-1 qui simplifient la vie professionnelle moderne et des innovations qui augmentent la productivité, la série de PC portables ThinkBook vous fait bénéficier d'une informatique plus intelligente.

Les ordinateurs portables ThinkBook de Lenovo sont conçus pour vous offrir sécurité, fiabilité et robustesse. Ces ordinateurs portables vous permettent de travailler en tout confiance, où que vous soyez. En effet, les ThinkBook sont dotés d'une sécurité intégrée et d'un service assistance de niveau professionnel destinés à stimuler le développement des entreprises en pleine croissance dans un monde toujours connecté. De plus, avec leur format de 15 pouces au maximum, vous pouvez emporter ces ordinateurs portables avec vous, n'importe où.

Propulsé par Windows 11 Professionnel, vous pouvez doper la productivité de toute votre équipe et concentrer tous vos efforts sur votre entreprise sans vous préoccuper de votre matériel informatique. C'est la définition même du "gagnant-gagnant".

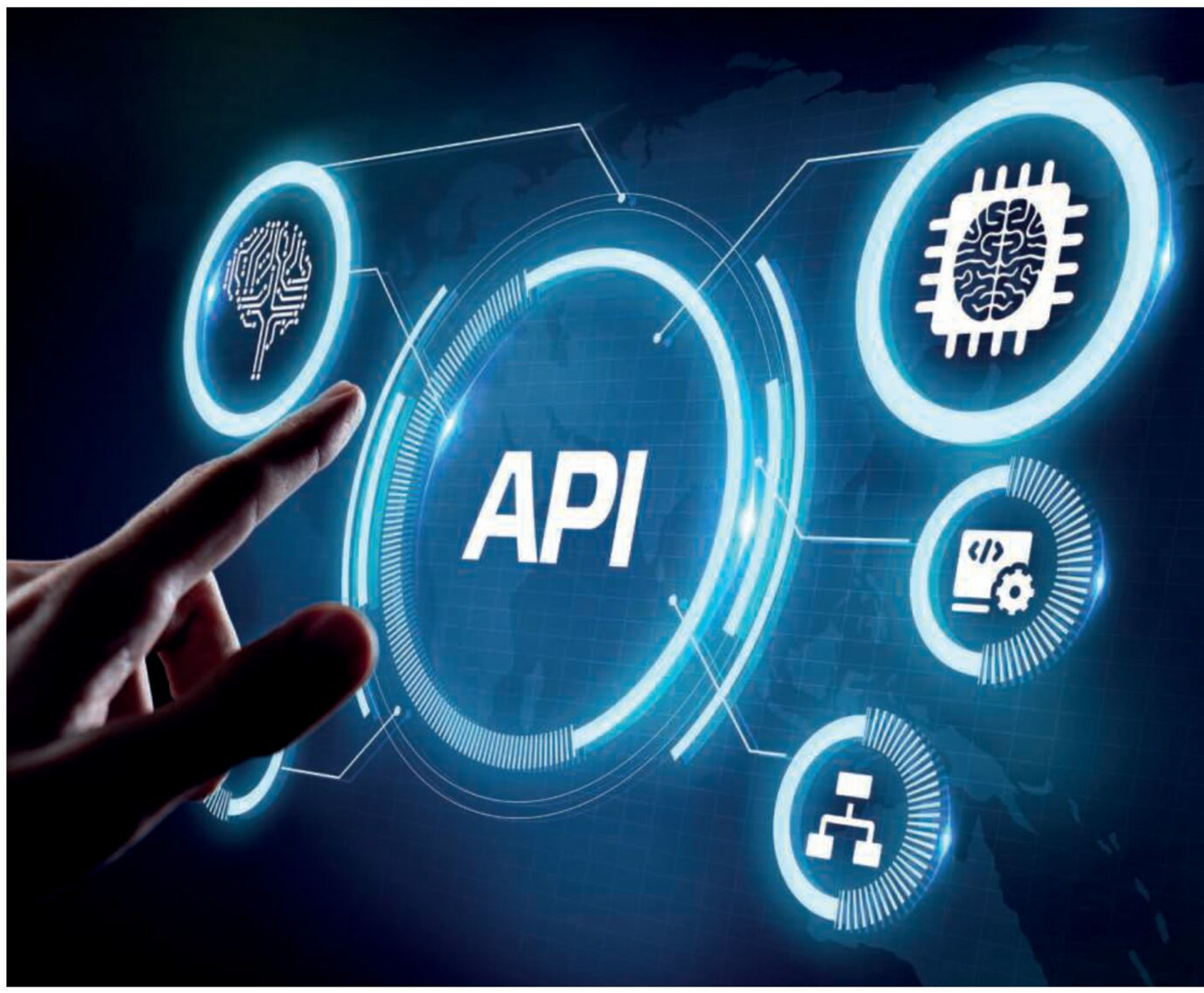
Les ThinkBook vous aident à réaliser des avancées que vous n'auriez jamais cru possibles. ■

GESTION DES API

OÙ EN SONT LES PRINCIPAUX FOURNISSEURS ?

Sept fournisseurs se positionnent comme « leaders » dans le dernier Magic Quadrant de Gartner dans le domaine de la gestion des API. À quels titres ?

Par Clément Bohic



Google, IBM et Microsoft, pas assez innovants ? Tous ont droit à un mauvais point à ce sujet dans le dernier Magic Quadrant de la gestion des API. Le premier, parce que ses travaux sur la partie intégration ont limité l'enrichissement du cœur fonctionnel de son offre. Le deuxième, parce qu'il a du retard sur ses principaux concurrents au niveau des jonctions avec les maillages de services. Le troisième, dans la mesure où il a généralement moins progressé que ses concurrents. Google, IBM et Microsoft figurent parmi les « leaders » du Quadrant version 2022. Il en était de même l'an dernier. Plus globalement, tous les « leaders » de 2021 le restent. Axway, Kong, Salesforce et Software AG en font aussi partie. Absorbé par IBM, Red Hat ne figure plus dans le Quadrant. Solo.io, au contraire, fait son apparition, dans la catégorie « acteurs de niche ». SAP et TIBCO Software en sortent, pour passer respectivement chez les *« challengers »* et les *« visionnaires »*.

IBM ET GOOGLE PLUS « VISIONNAIRES » QUE MICROSOFT

Gartner juge les offreurs sur deux axes. L'un prospectif *(« vision »),* centré sur les stratégies (sectorielle, géographique, commerciale, marketing, produit…). L'autre focalisé sur la capacité à répondre effectivement à la demande *(« exécution » :* expérience client, performance avant-vente, qualité des produits/services…). Sur l'axe *« vision »,* les fournisseurs classés au Quadrant se placent dans cet ordre :

LE MULTICLOUD OUI, MAIS NON

Gartner salue l'étendue de l'offre d'Axway, en particulier sur les cas d'usage et les modes de déploiement pris en charge. Le groupe américain se distingue aussi par son approche du multicloud (traduite par des ponts avec les passerelles API d'autres fournisseurs). Ainsi que son business model, nourri de partenariats avec, entre autres, Ping Identity (pour la détection de menaces), Stoplight (conception d'API) et Cloudentity (gestion du consentement). C'est moins positif sur la partie commerciale : la transition vers le modèle sur abonnement implique une normalisation du pricing… à suivre de près. Côté marketing, malgré une notoriété croissante, Axway reste perçu comme un vendeur spécialisé sur l'intégration. Et en dépit de sa stratégie multicloud, près des trois quarts de ses clients sont encore on-prem.

GOOGLE : LE SAAS PRIORITAIRE

Google se distingue sur la stratégie produit. Autant pour la qualité de ses services d'accompagnement que ses portails développeurs personnalisables et ses fonctionnalités de monétisation des données. La stratégie sectorielle est un autre point fort. En particulier dans le retail, dans la santé… et dans la finance, avec la solution Open Banking APIx. Bon point également sur le pricing, simple et qui ne restreint pas le nombre d'API ou d'utilisateurs. Apigee reste principalement conçu pour la gestion d'API : on pourra trouver le procédé limité si on cible des cas d'intégration. Attention, par ailleurs, au focus de Google sur Apigee X, c'est-à-dire la version SaaS sur GCP. S'y ajoute le point sus-évoqué en matière d'innovation.

IBM : FLEXIBLE… MAIS PAS POUR LES MISES À JOUR

Point positif chez IBM : la flexibilité de déploiement des composantes de son offre. Idem pour les fonctionnalités de sécurité (serveur d'autorisation OAuth intégré, prise en charge des certificats eiDAS…). Et pour les passerelles montées avec d'autres de ses technologies (App Connect pour l'intégration de données, Aspera pour leur transfert…) dans le cadre du Cloud Pak for Integration. Moins positif : l'expérience client ; en tout cas pour ce qui est des mises à jour de certaines versions. Outre le point innovation sus-évoqué, Gartner constate qu'IBM a enregistré en 2021 une croissance inférieure à celle du marché, quand bien même il reste le troisième plus gros fournisseur.

KONG : DÉVELOPPEURS D'ABORD

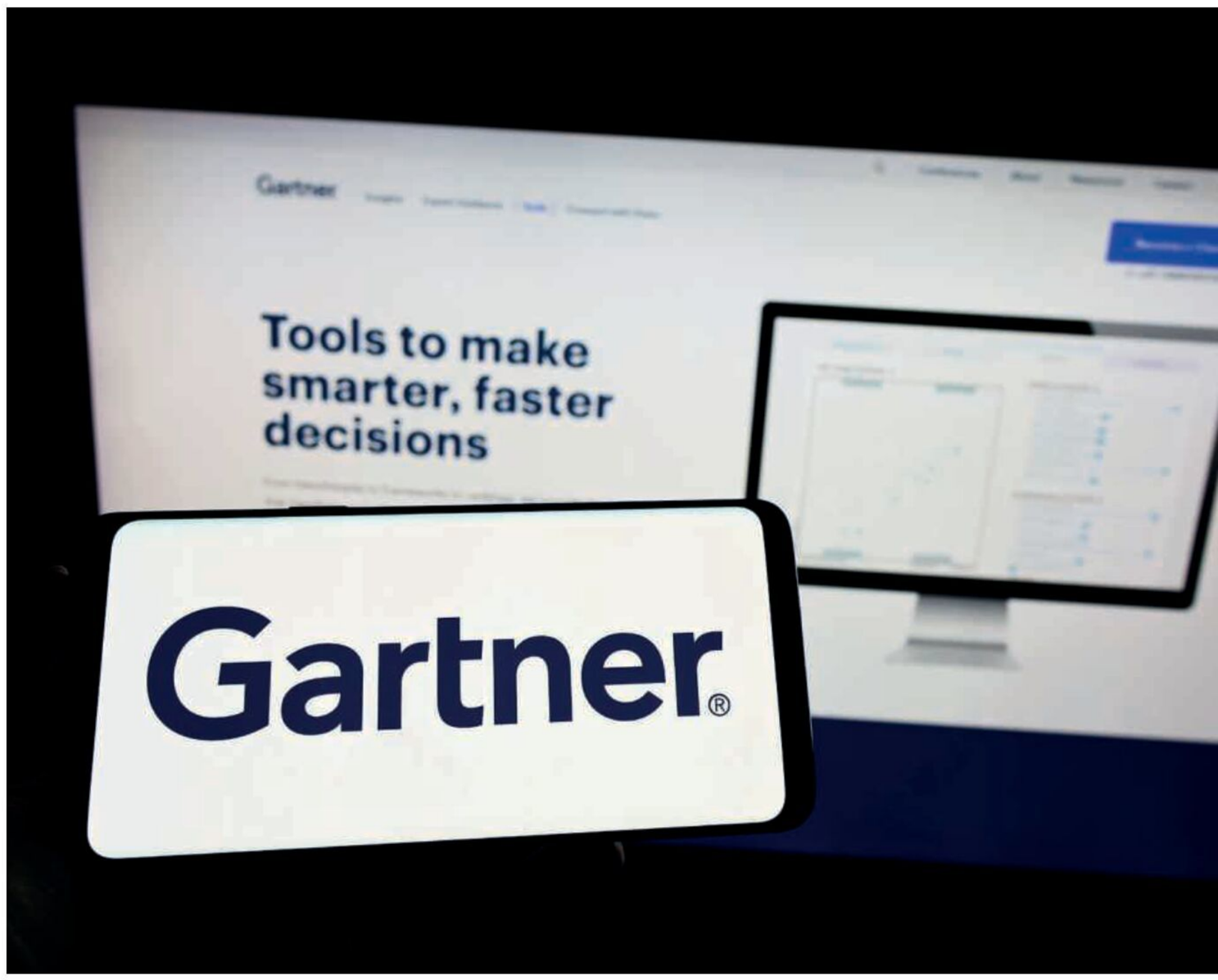
L'approche « less is more » de Kong à destination des développeurs (dev/test, service mesh, passerelle distribuée…) séduit Gartner. Même chose pour l'architecture de la solution, extensible et personnalisable par plug-in. La faible empreinte de la passerelle et son niveau de performance sont un autre point positif. Le focus sur les développeurs attire moins les métiers, fait remarquer Gartner. Qui souligne aussi l'écart fonctionnel entre la version open source gratuite de Kong et les formules payantes (pas d'admin web, d'analytics…). Le pricing, axé sur la notion de service, n'est par ailleurs pas le plus lisible qui soit.

MICROSOFT : LE BARYCENTRE AZURE

Les outils de gestion d'API de Microsoft sont le choix *« par défaut »* pour beaucoup de clients Azure. De manière générale, le niveau de satisfaction est élevé. L'interface d'administration, *« relativement simple et intuitive »,* en est un emblème. Gartner souligne aussi la couverture géographique du produit, disponible sur toutes les régions et zones Azure, avec un portail en 18 langues. L'offre a toutefois une visibilité encore limitée, étant marketée principalement dans le contexte d'autres services Azure. Et dans les faits, elle est vendue presque exclusivement en conjonction avec ces services. Se greffe le point innovation sus-évoqué, en dépit de l'ajout de la prise en charge de WebSocket et de GraphQL.

SALESFORCE : LES API ET PAS QUE

Salesforce fait figure de *« leader d'opinion »* à travers ses publications, ses événements, ses équipes d'évangélistes… et plus globalement sa capacité à accompagner l'usage de la plate-forme MuleSoft Anypoint. Le réseau de partenaires est un autre point fort, tout comme la jonction avec les composants RPA et l'intégration en low code. Comme chez Kong et Axway, Gartner ne salue pas le pricing. Il note que certains clients se montrent concernés sur la flexibilité de la contractualisation et les augmentations de prix au renouvellement, notamment sur les cas d'usage simples sans intégrations ou automatisations. Le support pourrait par ailleurs gagner en réactivité et assurer une meilleure disponibilité géographique de ses compétences. ■



Manager IT 2022

David Guillot de Suduiraut, directeur de la transformation et des technologies d'AXA France

À l'issue du vote des lecteurs de Silicon et de la communauté des professionnels de l'IT, David Guillot de Suduiraut, directeur de la transformation et des technologies d'AXA France, est élu Manager IT 2022.

Dans le cadre de la cérémonie de remise du prix Manager IT 2022 organisée par Silicon, c'est David Guillot de Suduiraut, directeur de la transformation et des technologies d'AXA France, qui a été désigné lauréat de l'édition 2022 par le vote des lecteurs de Silicon et de la communauté des professionnels de l'IT. Sur le podium, on retrouve Sophie Viger, directrice générale de l'École 42 (Argent) et Céline Stenger, directrice stratégie et gouvernance IT chez Fnac Darty (Bronze).

Il y a un an, David Guillot de Suduiraut décide de créer la fonction « stratégie » et il la fusionne avec la DSI qu'il dirige. « *On opère une transformation à l'échelle de toute l'entreprise,* insiste-t-il. *Il faut que tout le monde perçoive l'intérêt de monter sur le bateau »,* résume David Guillot de Suduiraut qui définit son rôle de leader comme celui « *qui balaie devant son équipe pour lever les obstacles* ». Et d'évoquer la métaphore du projet data qu'il assimile à une descente en rafting qui se joue en trois temps : se jeter à l'eau, faire équipe et oser prendre de la vitesse. Pour cet ancien X-Ponts qui a occupé, entre 2011 et 2016, le poste opérationnel de directeur général de la région Sud-Ouest, ce storytelling n'a rien d'anecdotique. « *Tous les processus sont passés au crible et revus de A à Z. Ce sont 3 000 personnes qui marchent main dans la main »,* souligne-t-il.

Une vision data en trois phases

Pièce maîtresse de cette stratégie : passer de l'expérience à l'impact. C'est ce chemin qu'il a tracé pour porter sa vision data en trois phases. « *La première a été de rentrer dans le vif sur nos sujets de prédilection. On a mis 40 personnes sur le sujet de la tarification des assurances automobile.* » Résultat : l'élaboration d'un pricing plus précis a permis de gagner des clients. Enfin, pour passer à l'échelle, c'est le domaine de l'assurance collective qui a été retenu. « *Avec notre datamap, nous pouvons produire des statistiques à grande échelle pour les DRH des collectivités. Avant, on assurait. Aujourd'hui, on donne des conseils pour des programmes de prévention »,* détaille David Guillot de Suduiraut.

L'horizon est aussi marqué du sceau du Web 3.0 et du métavers. « *On ne sait pas où ça va aller, mais il y a déjà des millions d'utilisateurs »,* rappelle-t-il. Des expérimentations ont commencé : l'ouverture de deux agences (qui ont déjà trouvé quelques clients), des opérations de recrutement pour l'équipe IT et même une réunion interne de 300 personnes. Il y a aussi ce terrain acheté sur The Sandox pour lequel il va falloir définir une « *mission* ». Ce sera notamment la mission des « *catalyseurs* ». « *Ce sont des collaborateurs, dont 40 % de femmes, qui ont pour rôle de proposer des changements. 70 personnes sont nommées chaque année »,* se réjouit David Guillot de Suduiraut. ■

Mari-Noëlle Jégo-Laveissière,
DGA des activités opérationnelles en Europe

➔ **Sa mission :** depuis le 1er septembre 2020, elle est directrice générale adjointe, chargée de superviser les activités opérationnelles d'Orange en Europe (hors France), en particulier le déploiement de la 5G et de la fibre. Entrée dans le groupe en 1996 pour gérer un réseau de boutiques à Paris, elle a ensuite multiplié les postes à responsabilités, tant dans le lancement de nouveaux services que le marketing, la R&D et la gestion commerciale. Elle est également aujourd'hui à la tête de la division Technology and Global Innovation.

Christel Heydemann,
directrice générale du groupe Orange

➔ **Sa mission :** objectif 2030. C'est l'horizon que la DG doit dessiner pour le premier opérateur français. Un plan d'action, annoncé pour le mois de février 2023, qu'elle a promis plus humain que comptable. Parmi les dossiers prioritaires : la gestion de fin du réseau de cuivre, la situation d'Orange Bank, la rationalisation de son réseau de boutique et les axes de développement pour ses infrastructures, en particulier les tours et le réseau de fibre.

Fabienne Dulac,
DGA, CEO Orange France

➔ **Sa mission :** à la tête d'Orange France depuis 2015, elle dirige ses activités sur le marché le plus concurrentiel d'Europe qui compte quatre opérateurs. Donnée partante après la démission de Stéphane Richard qui l'avait nommée, elle a été renouvelée par la nouvelle DG. Entrée en 1997 chez l'opérateur au sein de la division multimédia nouvellement créée, elle a ensuite occupé différentes fonctions dans le marketing, le business développement et la relation client. En 2011, elle avait dirigé la région nord de France avant d'assurer la direction de la communication de l'opérateur en France en 2013.

ORANGE

LES SIX FEMMES DU COMEX,

VERSION CHRISTEL HEYDEMANN

Nommée en avril 2022, Christel Heydemann s'appuie sur un Comex qui compte cinq directrices exécutives, sur 11 membres, pour piloter le premier opérateur français.

Caroline Guillaumin,
directrice exécutive de la communication

➔ **Sa mission :** Sa mission : En provenance de la Société Générale où elle gératit la communicatioon et les RH depuis 2010, elle doit déployer la communication du prochain nouveau plan stratégique Objectif 2030. Un rôle essentiel selon la nouvelle DG qui lui confie la communication auprès des salariés et de l'ensemble des parties prenantes externes du groupe. Au fil de sa carrière, démarrée en 1989, cette diplômée de l'IEP de Bordeaux et d'un Master of Arts en relations internationales de l'université de Boston a occupé diverses fonctions dans les domaines de la communication et du marketing, notamment au sein de Alcatel, SFR puis Alcatel-Lucent.

Aliette Mousnier-Lompre,
directrice générale Orange Business Services

➔ **Sa mission :** Sa mission : Elle a pris officiellement la direction de la filiale de services aux entreprises en mai 2022 après une période d'interim qui avait démarré en janvier. Elle doit réinventer pour 2023 une stratégie centrée sur le modèle des ESN afin de développer l'activité services IT, notamment le Cloud, la cybersécurité et l'IA, face au recul des activités télécom traditionnelles telles que la téléphonie fixe et les réseaux privés d'entreprise. Egalement sur sa feuille de route : le développement de Bleu, une offre de «cloud de confiance» proposée avec Capgemini et basée sur des services Microsoft dans le cadre d'une co-entreprise. Lancement prévu : 2024.

Elizabeth Tchoungui
Présidente déléguée de la Fondation Orange

➔ **Sa mission :** depuis septembre 2020, elle supervise, notamment, la politique de responsabilité sociale d'Orange dans le cadre des objectifs du plan stratégique Engage 2025. Et assure la présidence déléguée de la Fondation Orange qui soutient des actions qui combinent numérique et développement social. Avant de rejoindre Orange, elle a exercé comme journaliste à France Télévision et a dirigé le service culture de France 24.

STRATÉGIE CLOUD

MIGRER SON PORTEFEUILLE APPLICATIF DANS LE CLOUD : UN DEFI !

Lift and Shift, refactoring ou redéveloppement complet… la migration d'une application vers le cloud peut être rapide ou extrêmement coûteuse. Chaque option a ses avantages et ses inconvénients, mais ce choix doit avant tout s'inscrire dans la stratégie de digitalisation de l'entreprise.

Par Alain Clapaud

Migrer vers le cloud public est une problématique qui est à l'ordre du jour de tous les DSI. Outre les grands projets de « Move to cloud » des Veolia, Engie ou Carrefour, une récente étude IDC France montre que les PME et ETI se sont elles aussi engagées dans cette voie : 34 % des entreprises interrogées sont dans une approche « cloud also ». C'est-à-dire que le cloud est systématiquement analysé, mais pas privilégié : 23 % optent pour le cloud projet par projet et 15 % sont dans une approche « cloud first ». 14 % en approche « cloud last » : le cloud n'est retenu que s'il n'est pas possible de traiter le besoin en interne. Seulement 14 % proscrivent encore totalement le cloud de leur environnement informatique. *« La première question qu'un DSI doit se poser, c'est pourquoi aller vers le cloud »,* souligne

Mohammed Sijelmassi, CTO du Groupe Sopra Steria. « *Souvent, la raison n'est pas économique et le cloud peut être parfois plus coûteux qu'une approche on-premise. Il peut s'agir d'une volonté d'innovation afin de bénéficier de fonctionnalités disponibles dans le cloud.* »

Ainsi, hormis une volonté stratégique d'aller vers le zéro datacenter, migrer une grosse application legacy en lift and shift ne présente aucun véritable intérêt et peut induire des problématiques de performance, de latence et de coûts... À l'autre extrémité du spectre de l'innovation, pour le développement des nouvelles applications digitales, le cloud est la solution la plus évidente.

Pour Éric Salviac, Business Value Senior Consultant chez Cisco Appdynamics, un important travail préparatoire est indispensable à tout projet Move to cloud : « *Lorsque l'entreprise a détouré le périmètre applicatif qui doit basculer dans le cloud, il faut toujours passer par une étape d'inventaire et de diagnostic. Les applications legacy étant structurées par couches successives, il faut mener un mapping fonctionnel puis technique pour décider de la façon dont on va les migrer dans le cloud. Ou simplement la déplacer dans le cloud en l'état ou ne la redévelopper qu'en partie.* »

Mohammed Sijelmassi, CTO du Groupe Sopra Steria

"Il faut apporter plus de flexibilité"

« Les entreprises doivent élaborer ce que nous appelons une "transformation journey", une stratégie en plusieurs phases où l'intérêt de migrer chaque composant doit être évalué, ainsi que la façon dont il faut faire. Certaines ne présentent pas d'intérêt à être refondues. En outre, il est possible d'expérimenter les infrastructures cloud dans son propre datacenter, cela permet de monter en maturité sur les technologies cloud sans avoir à se poser de questions quant à la localisation des données. On peut développer sur des infrastructures modernes sans être chez AWS ou GCP. Assez souvent, les entreprises veulent mener un "lift and shift" de type "quick and dirty", puis, une fois que le SI est dans le cloud, adopter une trajectoire de modernisation de type 5R ou 6R. Certaines applications n'ont pas à être modifiées, car l'entreprise n'a pas d'intérêt immédiat à le faire, mais il faut les ouvrir à l'extérieur via une APIsation. C'est important, car les processus actuels sont beaucoup moins linéaires que par le passé : il faut apporter plus de flexibilité via des appels d'API possible tout au long du processus. »

LES CINQ MODÈLES DE MIGRATIONS SELON GARTNER

Dès 2010, le Gartner a défini le modèle des 5R, c'est-à-dire les cinq stratégies de migration vers le cloud : Rehost avec les projets de type « lift and shift », le refactoring et la modernisation des architectures jusqu'au rebuild et au remplacement pur et simple d'une application obsolète ne pouvant migrer vers le cloud. L'effort en termes d'ingénierie est bien évidemment croissant. Les projets de « lift and shift » sont relativement simples à mener, la durée reste limitée et le risque faible. En contrepartie, l'application ne tire pas profit des capacités offertes par le cloud provider, notamment ses services cloud. D'autre part, l'application et son architecture ne sont pas optimisées pour le fonctionnement du cloud et un mode de facturation à l'usage. L'application va donc être plus coûteuse à l'exploitation qu'une application « cloud native ».

À l'inverse, une application réarchitecturée et redéveloppée va pouvoir bénéficier des capacités offertes par le cloud cible, notamment les services PaaS et Serverless. L'approche présente des atouts certains en termes d'agilité et de productivité des DevOps. En outre, une application conçue pour le cloud ne va consommer que les ressources strictement nécessaires à son fonctionnement, à l'inverse d'applications legacy qui vont demander de multiples instances en production H24. La contrepartie de cette optimisation, c'est un important et coûteux travail d'ingénierie et des délais importants avant de pouvoir disposer d'une application réellement « cloud

> *Souvent, la raison de la migration n'est pas économique et le cloud peut être parfois plus coûteux qu'une approche on-premise. Il peut s'agir d'une volonté d'innovation afin de bénéficier de fonctionnalités disponibles dans le cloud.* »
>
> ***Mohammed Sijelmassi - CTO du Groupe Sopra Steria.***

ready ». La complexité des projets de rebuilt qui peuvent s'avérer extrêmement complexes. Il n'est pas étonnant que les programmes de « move to cloud » s'étalent sur plusieurs années.

DES MIGRATIONS "LIFT AND SHIFT" PLUS SIMPLES À MENER

Bien souvent, les DSI doivent panacher avec ces différents modèles de déploiement, en fonction des contraintes technologiques de certaines applications. Le « lift and shift » est un moyen de migrer assez rapidement un grand nombre de workloads dans le cloud et fermer les datacenters. Cette approche que certains peuvent appeler « quick and dirty » est considérablement simplifiée par la présence d'outils de migration tels que ceux proposés par les fournisseurs cloud, comme cloudEndure chez AWS ou Azure Migrate chez Microsoft.

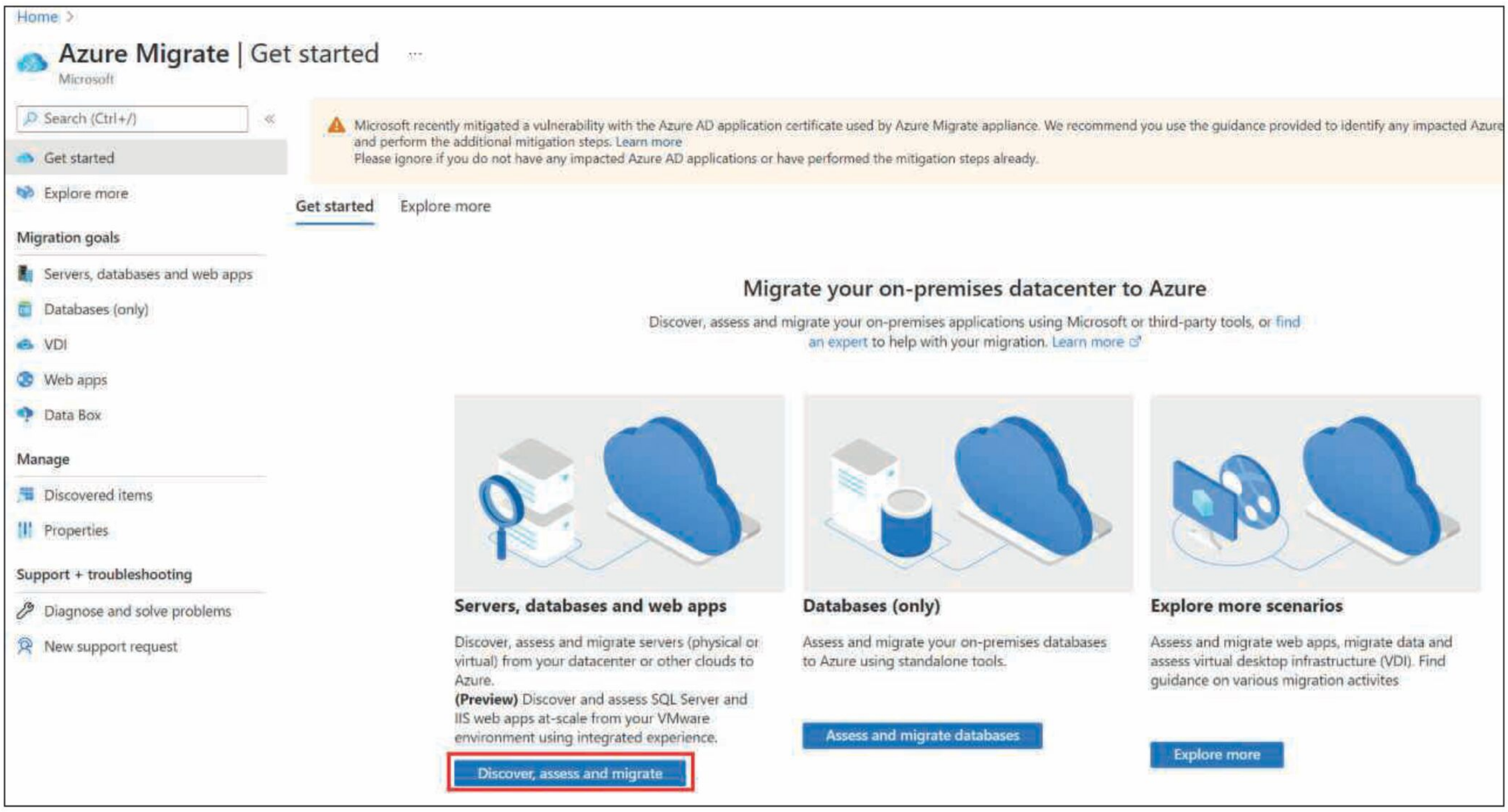
Depuis, le modèle 5R s'est enrichi, on parle désormais des 6R ou même des 7R. L'approche relocate définir ainsi une migration de type « lift and shiftt » réalisée non plus au niveau de l'OS, mais de l'hyperviseur. De facto, VMware, un acteur très présent dans les infrastructures on-premise a réussi à se poser en tant que pivot dans la migration de ces infrastructures virtualisées vers le cloud public. Chaque fournisseur cloud majeur dispose d'une offre VMware. Qu'il s'agisse de VMware cloud on AWS, d'Azure VMware Solution, de Google Cloud VMware Engine ou encore Oracle Cloud VMware Solution et IBM Cloud for VMware Solutions toutes ont pour vocation de faciliter le transfert de workloads du datacenter privé de l'entreprise aux infrastructures cloud public. L'éditeur avance des chiffres éloquents, avec un coût de migration de 100 VM qui passe de 412 400 $ en approche cloud classique à seulement 178 500 $ via VMware cloud on AWS et des délais réduits de 46 %. Cette approche qui peut rassurer les DSI habitués à gérer des infrastructures virtualisées.

23 %

Des PME et ETI optent pour le cloud projet par projet.
Source : IDC.

L'ÉPINEUX PROBLÈME DES APPLICATIONS LEGACY

S'il est possible d'industrialiser la migration de workload en mode « lift and shift », profiter réellement des capacités de scaling automatique et de l'allègement des tâches d'administration des plateformes passe par une réarchitecturation plus ou moins profonde des applications, voire un redéveloppement des plus obsolètes. Une récente étude menée par Vanson Bourne auprès de 1104 développeurs, architectes et DSI dans 49 pays estime à plus de 800 milliards de lignes Cobol encore en production dans le monde.



Des applications dont beaucoup des concepteurs sont aujourd'hui à la retraite et qu'il sera extrêmement compliqué de porter sur des architectures modernes. Eric Salviac, Business Value Senior Consultant chez Cisco Appdynamics souligne : « *Pour profiter des apports du cloud, il faut casser l'architecture de l'application, la porter en microservices et la conteneuriser, appeler les services Paas de la plateforme. Modifier ainsi une application legacy peut devenir rapidement très complexe : on va bouleverser l'architecture et l'effort à consentir devient comparable à redévelopper une application from scratch.* »

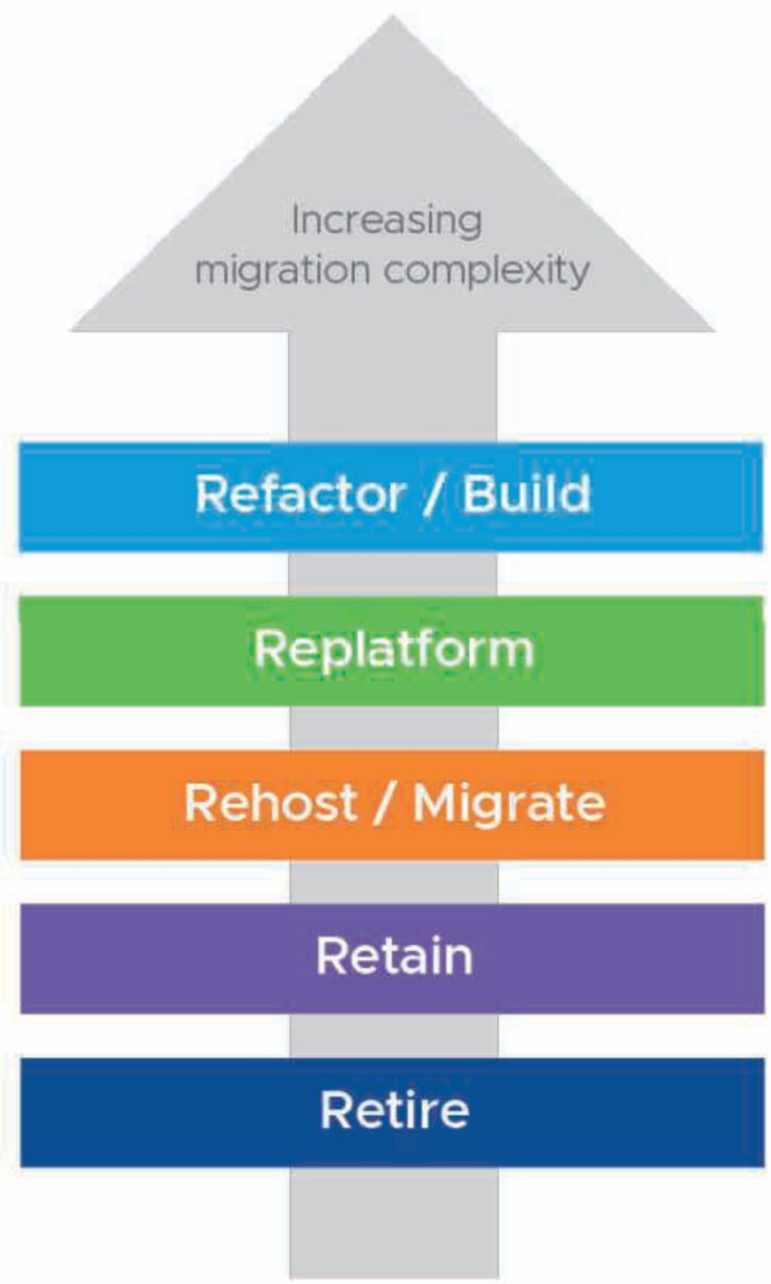
Plutôt que de lancer des projets de redéveloppements aux coûts et délais pharaoniques, Mohammed Sijelmassi suggère plutôt d'ouvrir ces applications legacy généralement très silotées : « *Le monde tend aujourd'hui à être de plus en plus transversal : l'utilisateur ne veut pas savoir que certaines opérations sont possibles sur le Web, mais pas sur mobile. Pour adopter une vision transverse, il faut être capable de donner de la valeur aux données produites au-delà des applications elles-mêmes.* » Après un « lift and shift », le CTO conseille de passer par une phase d'ouverture des applications, « APIser » ces applications afin de pousser les données hors des applications et, à terme, mieux les exploiter. Enfin, il faudra redévelopper certaines applications ou certains modules d'application si le projet peut dégager suffisamment de valeur ajoutée pour justifier un tel projet. Tout est alors question d'équilibre entre l'apport business de la transformation, le budget et l'effort que l'entreprise est prête à consentir, mais aussi le souci du DSI de ne pas laisser la dette technique s'accumuler dans son SI. ■

> *Les applications legacy étant structurées par couches successives, il faut mener un mapping fonctionnel, puis technique pour décider de la façon dont on va les migrer dans le cloud.* »
>
> ***Éric Salviac, Business Value Senior Consultant chez Cisco Appdynamics.***

Yan Morvan, Principal Cloud Engineer, Amadeus

"Nos 10 Po de données historiques ont été transférés par camions entre notre datacenter et celui de Microsoft"

Leader mondial des solutions informatiques pour le secteur du voyage, Amadeus dispose d'un datacenter en Allemagne, mais s'appuie aussi sur plusieurs clouds publics. L'entreprise gère 800 millions de requêtes par jour et traite un volume de données considérable, de l'ordre de 10 Po, stocké dans ses systèmes analytiques. Yan Morvan, Cloud Data Platform Principal Engineer chez Amadeus : « *En 2021, Amadeus a signé un partenariat stratégique avec Microsoft Azure. Le but est de migrer toutes les applications d'Amadeus vers le cloud Azure, non seulement les applications transactionnelles, mais également les applications big data. C'est le plus gros projet entrepris par les équipes R & D d'Amadeus et il est encore en cours de réalisation. Avec ce projet Amadeus ne veut pas seulement migrer vers le cloud, mais aussi déclencher une vague d'innovations sur le secteur du voyage. Cette migration représente déjà une année et demie d'efforts pour commencer à onboarder les applications. Il a fallu faire des choix : les infrastructures cloud ne permettent pas tout et il a fallu trouver des compromis. Nous avons adapté notre design en fonction des capacités de notre cloud provider. Nous comptons aujourd'hui entre 60 à 100 Application Workspace, c'est déjà considérable. Sur le plan de l'automatisation, cela implique de gérer une plateforme déjà très imposante et complexe.* »
Une seule issue pour administrer une telle infrastructure cloud, une automatisation systématique de la gestion des workloads.



Dès 2010, le Gartner a défini le modèle des 5R, c'est-à-dire les cinq stratégies de migration vers le cloud.

RETOUR D'EXPÉRIENCE

COMMENT NEXITY A ENGAGÉ SA TRANSFORMATION CLOUD

Le groupe immobilier s'est engagé dans une migration complète de son infrastructure dans le cloud en plusieurs étapes. Témoignage de Laurent Dirson, son directeur des solutions business et des technologies.

Par Alain Clapaud

Laurent Dirson, directeur des solutions business et des technologies.

Nexity a commencé à utiliser le cloud en 2016, mais cette adoption a connu une forte accélération en 2018, avec le programme « Go to cloud ». Quatre cent quatre-vingts applications ont été migrées sur un mode « lift and shift » sur douze mois : six mois de préparation, six mois d'exécution. *« Mon approche a consisté en une transition vers le cloud avant d'engager une transformation. Nous avons mis nos applications dans le cloud sur un mode lift and shift le plus rapidement possible pour bénéficier de la valeur ajoutée du cloud public. Ensuite, sur un temps nettement plus long, de l'ordre de trente-six mois, nous menons une transformation qui s'achèvera en décembre 2022 »,* explique Laurent Dirson, directeur des solutions business et des technologies – DSiN – de Nexity.

UN VASTE PROGRAMME SERVERLESS

« L'objectif de ce programme, baptisé Transform, est maintenant de rationaliser, d'optimiser et, surtout, d'utiliser le plus de services managés possible afin de nous concentrer sur les activités plus différenciantes, à plus forte valeur ajoutée. Nous avons encore un peu de IaaS, mais en très faible proportion, 1 500 bases de données ont ainsi été migrées vers des bases managées, poursuit-il. *La partie move to cloud de ce programme de transformation a été menée par une équipe AMF (Application Migration Factory), dite core, de sept personnes seulement. Pour garder de l'agilité, il faut concentrer le travail de migration sur une petite équipe, je crois beaucoup aux vertus de la notion de pizza team, une équipe soudée, pluridisciplinaire et qui maîtrise la majorité des stacks techniques. »* Après ce vaste programme datacenter-less, un autre chantier a été lancé par Laurent Dirson, celui de l'agence serverless. *« Nous avions énormément de serveurs déployés dans notre réseau de trois cents agences. En fin d'année 2022, nous n'aurons plus aucun serveur en agence, tout leur fonctionnement sera porté par le cloud. »* La démarche permet de réduire l'empreinte carbone de manière drastique ainsi que la consommation électrique des agences, tout en réglant tous les problèmes d'approvisionnement en matériel informatique qui affectent tant de DSI. *« Nous sommes passés d'un monde où nous devions supporter des infrastructures à un monde où la DSIN est devenue force de proposition et conduit l'innovation avec les métiers. Nous ne sommes plus une simple DSI et ce programme a grandement contribué à cela »,* conclut Laurent Dirson. ■

COMMENT LE MULTICLOUD S'EST IMPOSE COMME LE MODÈLE DOMINANT DE L'IT

Après des débuts timides en France, le cloud public s'est finalement imposé dans pratiquement toutes les entreprises et institutions françaises. Ce mouvement de fonds passe désormais par plus de diversité d'acteurs, mais aussi par une plus grande complexité à gérer ces écosystèmes.

Par Alain Clapaud

Si le cloud public est officiellement né en 2004, avec l'arrivée d'AWS sur le marché américain, les années 2010 ont vu l'essor du cloud hybride dans de nombreuses entreprises, les années 2020 seront celles du multicloud. Le benchmark Digital Benchmark1 de VMware, publié en août 2021, fait état de 73 % de décideurs qui souhaitent adopter cette approche multicloud. Les raisons de ce nouveau virage sont bien connues : gagner en agilité pour déployer des applications modernes, réduire les coûts liés aux infrastructures IT et, évidemment, faire gagner en productivité les collaborateurs avec des solutions SaaS à l'état de l'art. Les métiers eux-mêmes ont poussé les DSI dans cette voie du multicloud en optant pour des solutions SaaS ou en faisant porter leurs projets digitaux par des infrastructures de cloud public.

73%

Le nombre de décideurs prêts à se tourner vers une approche multicloud.

Jean-Pierre Chamarande, Directeur général de Skale-5

Bien choisir son fournisseur

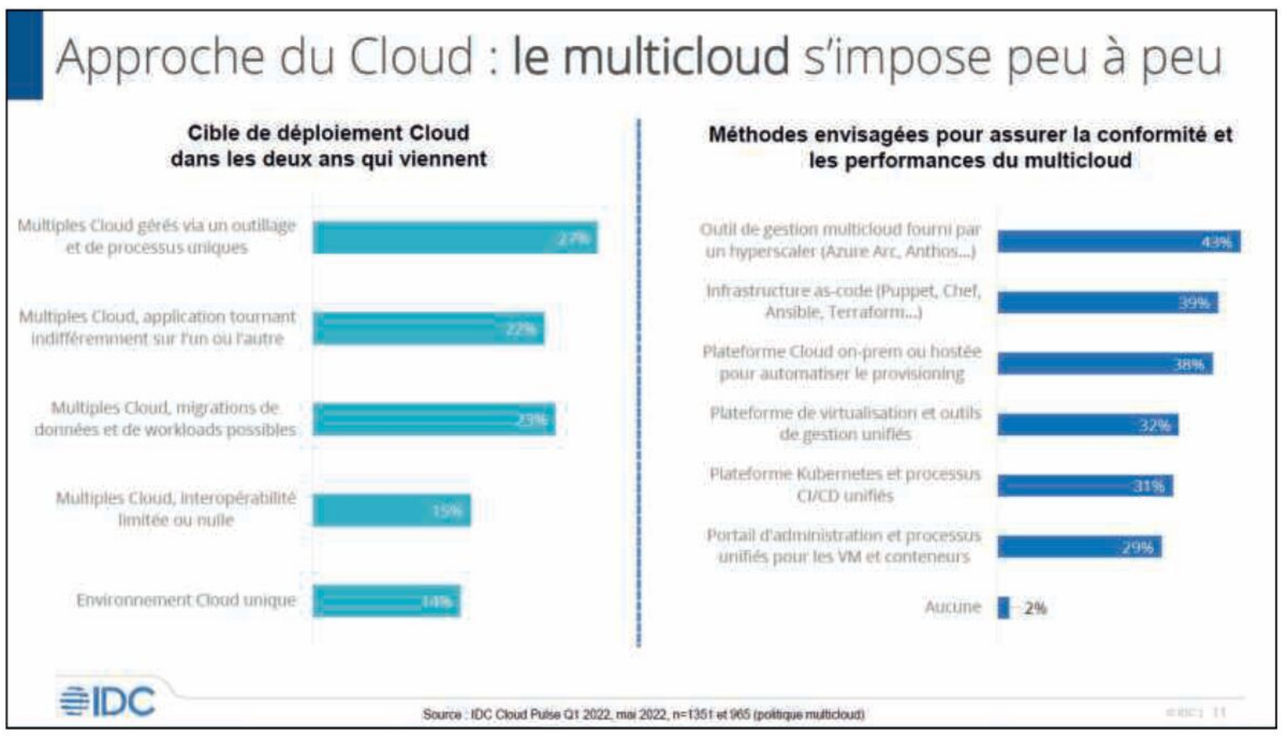
« Le choix d'un fournisseur cloud est soit technologique, soit dogmatique. L'entreprise peut souhaiter confier ses données à un fournisseur cloud, d'autres workloads à un deuxième et son ERP auprès d'un troisième. C'est quelque chose de très courant aujourd'hui. Certains peuvent privilégier un fournisseur pour bénéficier de fonctionnalités très pointues, mais en règle générale, les fournisseurs cloud ont tendance à converger. Une application réellement multicloud en production, cela n'existe pas. Il peut néanmoins être pertinent de charger de fournisseur cloud, en particulier lorsqu'il s'agit de mener de gros calculs, notamment l'apprentissage de modèles d'intelligence artificielle, mais pour des applications classiques, les mécanismes et efforts à déployer pour basculer une workload d'un fournisseur à l'autre ne sont pas justifiés par des écarts de prix souvent minimes. »

Reynald Fléchaux, analyste recherche senior chez IDC France, souligne aussi la volonté des DSI de contrebalancer la toute-puissance des hyperscalers en diversifiant leur portefeuille de solutions cloud : « *Initialement, le recours à plusieurs fournisseurs cloud en parallèle s'est imposé aux entreprises, car différentes unités ont exprimé des besoins différents. Sur le plan stratégique, les entreprises ont aussi cherché à équilibrer leurs relations avec leurs fournisseurs. Face aux hyperscalers le risque de dépendance est rapidement apparu aux yeux des DSI, avec le corollaire du prix et d'une dépendance aux prix pratiqués par tel ou tel acteur. Le multicloud s'est imposé comme un moyen de rééquilibrer cette relation client/fournisseur et de conserver une certaine indépendance.* »

Mohammed Sijelmassi, CTO du Groupe Sopra Steria confirme cette montée en puissance du modèle multicloud dans les entreprises : « Signer des accords avec plusieurs hyperscaler est devenu très courant. Aux États-Unis, 75 % des entreprises ont plus de deux fournisseurs cloud. Ce n'est pas parce qu'une entreprise utilise Google Workspace qu'elle porte ses applications sur GCP, de même que des banques emploient Teams, mais développent des services en ligne sur AWS. Le multicloud est aujourd'hui une réalité. »

CONVERGENCE DES ACTEURS DU CLOUD

La configuration la plus fréquente est de s'appuyer sur un cloud provider principal, éventuellement un second pour bénéficier de fonctionnalités ou d'une localisation géographique particulière et bien évidemment d'un cloud privé interne ou dans un datacenter en colocation pour les applications « legacy ». Si on observe une certaine convergence des hyperscalers qui présentent des catalogues produits de plus en plus larges, on observe quelques tendances fortes. Si aucun acteur du retail n'opte pour AWS, la filiale cloud d'Amazon pionnière du cloud public s'est attiré bon nombre de start-up, puis les divisions métiers des grandes entreprises en quête d'innovations.
Azure a séduit bon nombre de DSI déjà adeptes des technologies Microsoft, mais au-delà de ces clichés, les portefeuilles des hyperscalers ont aujourd'hui convergé et les positionnements de chacun sont beaucoup moins marqués. « *On peut encore observer quelques spécialisations comme le choix de la Google Cloud Platform pour les projets data,* ajoute Reynald Fléchaux. *Lors du dernier Salon Big Data Paris, de nombreuses entreprises ont témoigné sur la migration de leurs data lake on-premise vers le cloud Google, à l'image de ce que vient de réaliser Renault. Ce type de spécialisation se retrouve sur d'autres cloud et d'autres applications. Toute la question est, aujourd'hui, de faire fonctionner ces cloud de manière cohérente dans un système d'information.* »



LA CONFORMITÉ EN QUESTION

À cet écosystème des hyperscalers est venue se superposer la notion de cloud souverain. AWS, Microsoft, Google ou Oracle ont, certes, déployé des infrastructures cloud dans l'Hexagone, mais bon nombre d'organisations rechignent à confier leurs données confidentielles à des acteurs soumis à des réglementations américaines extraterritoriales comme le cloud Act. Même l'hébergement de données personnelles soumises au RGPD auprès de ces acteurs pose aujourd'hui question alors que la CNIL a mis en demeure plusieurs organismes de se mettre en

Le multicloud s'est imposé comme un moyen de rééquilibrer cette relation client/fournisseur et de conserver une certaine indépendance."

Reynald Fléchaux, analyste recherche senior chez IDC France.

conformité concernant l'utilisation de Google Analytics. Les services de l'État et les collectivités ont recours au cloud de manière souvent très prudente et pourraient franchir le pas auprès d'acteurs souverains disposant du label SecNumcloud délivré par l'ANSSI. « SecNumcloud est un jalon intéressant » note Reynald Fléchaux « Néanmoins, le catalogue de services reste peu étoffé et le surcoût est important, de l'ordre de 30 %. Ce surcoût s'explique par le niveau d'exigence très élevé de l'ANSSI, mais la qualification SecNumcloud n'est valable qu'en France et n'est pas alignée avec les autres certifications européennes, ce qui reste un sérieux handicap pour les entreprises. Cette problématique de cloud souveraine sera d'autant plus critique à l'avenir que de plus en plus de pays travaillent sur des réglementations locales comparables au RGPD européen.

Les architectures multicloud du futur risquent d'être modelées par ces notions de conformité, avec un fournisseur cloud pour la zone Europe, un autre pour la Chine, mais aussi pour les pays sud-américains, peut-être aussi un fournisseur américain qui sera capable d'assurer la conformité avec les différentes réglementations en train d'émerger dans certains états américains. Un futur casse-tête se constitue pour les DPO et les architectes. Le modèle de la centralisation de toutes les données et applications auprès d'un hyperscaler unique va être sérieusement battu en brèche dans les prochaines années.

KUBERNETES, L'OS DU MULTICLOUD ?

Face à cet accroissement de la complexité des architectures cloud, les entreprises cherchent des solutions. Avec Azure Arc ou Anthos de Google, les hyperscalers ont commencé à leur proposer des outils permettant la gestion d'infrastructures hybrides, voire multicloud, mais la solution la plus fréquemment utilisée pour à la fois abaisser la dépendance au fournisseur cloud, mais aussi donner de la cohérence à une architecture multi-cloud, ce sont les conteneurs, et plus particulièrement Kubernetes.

Thomas Poindessous, directeur général adjoint de Skale-5, ESN spécialisé dans les infrastructures

Bruno Delibanti, directeur des opérations et services informatiques de la Cnav

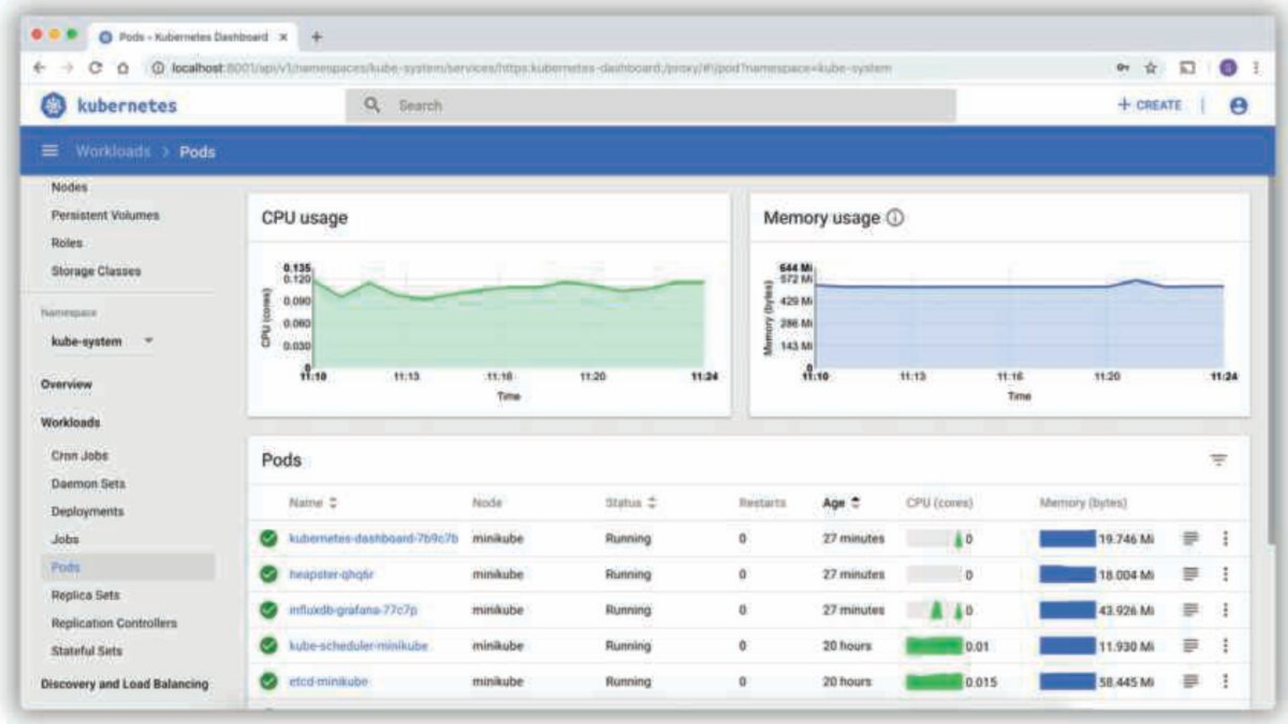
"Notre stratégie peut être qualifiée d'hybride"

« Nos activités recouvrent la gestion des infrastructures, l'intégration, la mise en production, l'exploitation des applications et le support utilisateur. Cela représente plus de 350 collaborateurs internes et une centaine d'externes, soit environ 30 % des ressources de la DSI. À partir de 2018, nous nous inscrivons dans une trajectoire qui nous mène vers le cloud, passant de 17 datacenters dans les années 2000 à trois aujourd'hui. Le principal, situé à Tours, abrite nos applications métiers, nos services en ligne et nos plateformes d'échanges sécurisés avec nos partenaires. Celui-ci est redondé en "RPO zéro" avec un second datacenter dans la même région. Un troisième, localisé à Lyon, est dédié aux environnements des projets et des régions. Notre stratégie peut être qualifiée d'hybride. Nous avons créé un cloud interne dédié à nos applications et données métiers, des données personnelles sensibles que la CNAV ne souhaite pas confier à un tiers. La version 1 de ce cloud privé offre aux exploitants, intégrateurs, testeurs et développeurs un portail sur lequel ils peuvent rapidement provisionner des VM avec un OS en mode IaaS et des services PaaS comme JBoss, PostgreSQL ou Oracle. Cette ressource est mise à disposition dans un délai très court, de l'ordre de l'heure. Nous avons développé ce cloud interne nous-mêmes à base de scripts Ansible/AWX. Pour obtenir des composants d'infrastructure non standards, le processus de provisioning reste classique et manuel.

Un premier bilan du fonctionnement de ce cloud a montré le succès de l'initiative et a confirmé la stratégie cloud interne dans notre prochain schéma directeur pour la période 2023/2027. Dans une version 2, nous allons enrichir le portefeuille de services PaaS avec d'autres middlewares, la gestion de conteneurs et une offre "infrastructure as a code" en soutien d'une démarche DevSecOps. Cette approche cloud privé ne signifie pas que nous avons fermé la porte au cloud public. En dehors de nos applications métiers où l'enjeu de souveraineté et de confidentialité est très fort, nous avons des besoins génériques, comme la bureautique et le collaboratif, qui sont couverts par Microsoft Office 365. Pour des usages transversaux, hors de notre cœur de métier, nous pouvons utiliser des ressources du cloud public en mode SaaS : nous nous appuyons sur la gestion de projet Orchestra de Planisware, le SIEM avec Rapid7, ou la solution Security Service Edge de Netskope. À moyen terme, les acteurs de l'écosystème ont commencé de réfléchir à un cloud « Sécurité sociale » appuyé sur les fournisseurs de cloud souverains. Nous aurons peut-être matière à exploiter de telles offres pour une partie de nos activités. Nous sommes encore au début des réflexions sur ce que sera, à l'avenir, ce cloud communautaire.

cloud et Kubernetes souligne : *« Kubernetes permet d'amoindrir la zone d'adhérence avec le fournisseur cloud. Cela permet notamment aux éditeurs de rendre leur application compatible avec plusieurs fournisseurs cloud. Cette approche a de quoi rassurer les DSI. »* Déployer des clusters Kubernetes sur plusieurs zones géographiques auprès de fournisseurs cloud différents est possible tout en profitant des gains de productivité liés aux approches modernes de type « infrastructure as code » et aux services Kubernetes managés proposés par tous les grands fournisseurs.

L'enjeu est d'avoir une chaîne CI/CD capable de gérer ces différents fournisseurs et un stack de monitoring unique qui puisse être déployés sur l'ensemble des clusters, quel que soit le cloud provider qui va les porter. L'expert ajoute : *« En règle générale, pour tirer profit du choix d'un cloud provider, il faut maximiser le recours aux services managés. Sur ce plan, on peut distinguer les composants d'infrastructure classiques comme MongoDB, PostgreSQL ou Elastic Search qui sont proposés en mode managé. Sur de tels composants, il n'y a aucune adhérence au fournisseur. D'autres services sont plus différenciants. C'est le cas des services Serverless, des conteneurs en mode managé. »* Faut-il pour autant ne pas exploiter les innovations fournies par un fournisseur cloud, car celles-ci n'ont pas d'équivalent chez ses concurrents ? La réponse va dépendre de l'entreprise et de sa stratégie d'innovation. Pour Mario Arnautou, consultant chez Neoxia, *« Il s'agit d'un compromis à réaliser entre des services très innovants proposés par le fournisseur cloud et le vendor lock-in que cela induit si on les utilisent. Avoir une forte adhérence à son fournisseur cloud n'est pas une chose nécessairement à éviter si on peut en tirer un gros avantage sur le marché. Il faut maximiser l'intérêt de mettre en œuvre telle ou telle fonction du fournisseur cloud, c'est un choix stratégique à réaliser. »* ■



30 %

Le surcoût du label SecNumcloud.

Xavier Pestel, Lead SRE (Site Reliability Engineering) chez Weborama

"Nous faisons maintenant du Kubernetes au quotidien"

« L'infrastructure DMP de la R&D de Weborama s'appuie sur deux fournisseurs cloud publics, avec plusieurs centaines et une dizaine de GKE sur GCP, deux clusters Kubernetes et une centaine d'instances sur notre second cloud provider. Tous ces clusters sont managés par les cloud providers. En parallèle, nous avons nos deux datacenters où nous disposons de plusieurs centaines de serveurs et VM, deux clusters Kubernetes sur un premier et un troisième cluster sur le second datacenter. Cela représente beaucoup de machines. Avant Kubernetes, nous avions des machines virtuelles, des machines physiques, avec une part plus importante en datacenter. Nous étions dans une approche de type "Excel as a Service" avec un suivi manuel de nos applicatifs et nos services. Ce fut le point de départ en 2018 d'une expérimentation de Kubernetes, avec une volonté d'éliminer au maximum les traitements manuels. Le premier volet de cette transformation est organisationnel. Lorsqu'on a plusieurs clusters Kubernetes situés dans différents cloud, il faut une grande rigueur. Sur GCP, on fonctionne par projet, l'idée étant de créer un cluster pour chacun d'entre eux et disposer de notre stack de monitoring complète pour collecter les métriques avant de les centraliser. L'approche est la même chez notre autre fournisseur cloud avec du Kubernetes managé. Nous appliquons ce même principe dans nos datacenters. L'ensemble de ces clusters sont répartis sur deux environnements différents. La règle, c'est que lorsqu'on veut déployer des applications qui ont besoin de monitoring comme des clusters Couchbase ou Redis ou MySQL, on les exporte dans Kubernetes. Les déploiements des clusters sont menés en Terraform pour le volet cloud et Salt/Kubadm sur nos datacenters. Pour les applicatifs, c'est du mode "gitops" pour combiner Flux et Helm et disposer d'un déploiement totalement automatisé. Le bilan, c'est que nous faisons maintenant du Kubernetes au quotidien. L'autoscaling et l'autoguérison règlent certains problèmes et ont permis de réduire les volumes d'astreintes, mais peuvent poser d'autres problématiques à traiter sur le long terme. Nous avons résolu notre problématique d'homogénéisation de services, avec des déploiements facilités avec le passage au GitOps. Nous avons automatisé notre monitoring. Et l'ensemble des services sont autodécouverts à l'échelle de tout le parc grâce à consul (dans ou hors Kubernetes). »

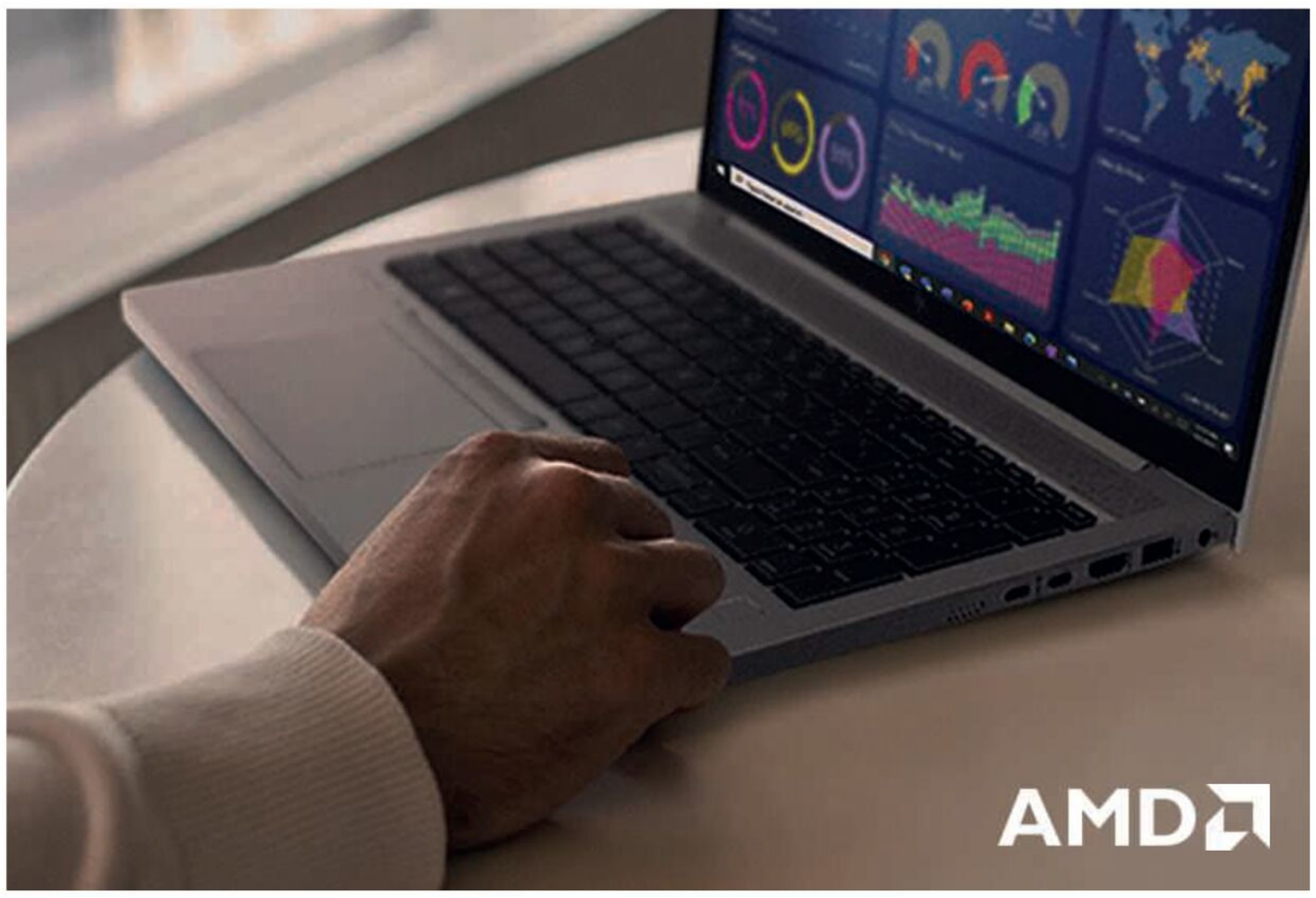
COMMENT FAIRE DES CHOIX PLUS DURABLES lors de la mise à jour de votre matériel ?

Bien que cela ne semble pas être une mesure évidente à prendre, les entreprises devraient également s'intéresser à parc informatique afin de vérifier qu'elles utilisent des équipements respectueux de l'environnement.

Cependant, choisir le bon matériel – comme un PC portable économe en énergie – pourrait vraiment permettre à votre entreprise de se rapprocher de ses objectifs de développement durable.
Les processeurs Ryzen™ 6000 PRO d'AMD rendent la tâche plus facile que jamais. Basés sur l'architecture "Zen 3+", les CPU utilisent les fonctionnalités de gestion de la consommation énergétique adaptative qui adaptent rapidement la vitesse pour assurer une bonne efficacité énergétique, AMD réduisant de 50 % la consommation énergétique entre 2018 et 2022 .

Par rapport aux processeurs AMD Ryzen™ de dernière génération, les processeurs AMD Ryzen™ PRO Série 6000 peuvent utiliser jusqu'à 30 % d'électricité en moins pour la visioconférence et jusqu'à 45 % d'autonomie en plus pour Microsoft Teams par rapport à l'Intel Core i7-1260P . Cela signifie que les CPU AMD Ryzen™ PRO Série 6000 peuvent offrir jusqu'à 26 heures d'autonomie sur un PC portable professionnel haut de gamme, garantissant ainsi que vos employés n'ont pas besoin d'être connectés à une prise.
Il ne s'agit pas là de compromettre les performances. Par rapport à la concurrence, les processeurs AMD Ryzen™ PRO Série 6000 offrent 2 fois plus de performances par watt, en utilisant jusqu'à 67 % de watts par cœur en moins et un rendu jusqu'à 39 % plus rapide .

Les processeurs Ryzen™ PRO Série 6000 d'AMD se retrouvent déjà dans de nombreux PC portables fins, légers et puissants pour qui l'écologie est essentielle. Le HP EliteBook G9, qui intègre un processeur AMD Ryzen™ 7 PRO 6850U, a été conçu pour les utilisateurs écoresponsables. Il est produit en utilisant de l'aluminium fabriqué avec des plastiques océaniques récupérés. Il utilise des plastiques recyclés dans le cadre de l'écran et les capuchons, et est expédié dans un emballage complétement recyclable.



De même, le Lenovo ThinkPad Z – qui intègre un CPU AMD Ryzen™ 7 PRO 6860Z dans son châssis fin et léger – est doté d'un cadre en aluminium recyclé élégant. Les matériaux respectueux de l'environnement vont au-delà du PC portable lui même avec un emballage en bambou et canne à sucre compostables et 100 % recyclables et un adaptateur CA qui est fait de 90 % de matières recyclées post consommation. Ces PC portables, grâce à leurs processeurs hautes performances AMD Ryzen™ PRO 6000, sont également conçus pour durer, ce qui signifie que vous n'aurez pas à remplacer votre matériel.

En outre, les processeurs pour PC portable d'AMD sont non seulement conçus pour durer, mais ils sont également entièrement optimisés pour les logiciels modernes et existants, ce qui signifie que vous n'avez pas à mettre en œuvre une stratégie de remplacement complet. ■

[1]D'après les tests réalisés par AMD le 14/12/2021.

[2]D'après les tests réalisés par AMD le 01/04/2022.

[3]Basé sur des mesures effectuées par AMD.

AMD

silicon

MULTICLOUD

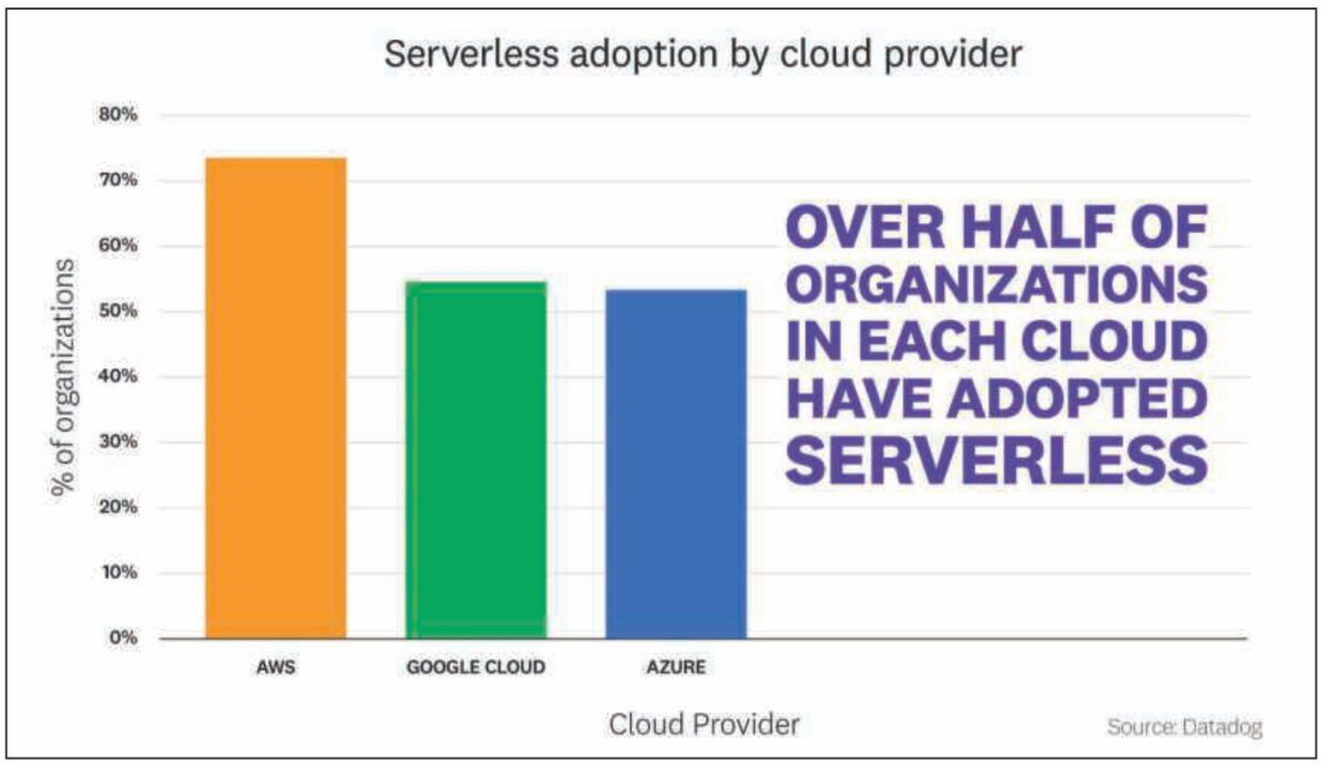
POURQUOI FAUT-IL MISER SUR LE SERVERLESS

Le serverless se pose comme la technologie qui permettra un nouveau bond en avant en termes d'efficacité et de baisse du coût des applications. Malgré ses avantages, l'approche pâtit de quelques contraintes, dont une adhésion plus forte au cloud provider. Un mal nécessaire pour passer à l'étape supérieure ?

Par Alain Clapaud

Airbus, L'Oréal, Air France, toutes les grandes entreprises y viennent... Architectures Web hautement scalables, développements d'API, manipulation de données IoT, la liste des applications qui peuvent être traitées par des appels de fonctions serverless s'allonge à l'infini. L'écosystème serverless va désormais bien au-delà du Functions as a Service (FaaS), avec des bus d'événements, des orchestrateurs, du Kubernetes et des bases de données serverless qui permettent d'imaginer des architectures complexes.

Lors de l'AWS Summit 2022, François Le Gac, Head of Cloud Product and Service Line chez Airbus soulignait la synergie entre les services managés et le serverless dans le cadre de la transformation digitale de l'avionneur : *« Nous sommes aujourd'hui capables de livrer des projets en trois mois contre vingt-quatre par le passé. Nous avions besoin de douze à dix-huit mois pour déployer un stack technologique dans nos datacenters. Sur AWS, il nous faut que trois mois pour mettre en compliance un stack sur notre "landing zone". Un deuxième aspect, c'est la scalabilité : nous n'avons plus de problèmes de provisioning, plus de diffi-*



cultés de capacity planning. Le troisième bénéfice porte sur la protection. Le cloud nous permet d'atteindre des niveaux de sécurité qu'il serait beaucoup plus compliqué d'atteindre sur un datacenter classique. » Airbus annonce des économies de l'ordre de 25 % à 40 % de ses coûts d'exploitation, selon l'application.

LE RISQUE DE VENDOR LOCK-IN

Si les gains générés par le serverless sont spectaculaires, beaucoup de DSI s'alarment sur un risque de vendor lock-in. Mehdi El Kouhen, architecte cloud devops chez Ippon Technologies estime qu'il est possible de passer outre cette contrainte : *« Le vendor lock-in peut être facilement contourné par la mise en œuvre d'une bonne structuration du code et aller vers des architectures tolérantes au changement, à l'image des architectures hexagonales. Seules les couches*

Mehdi El Kouhen, architecte cloud devops chez Ippon Technologies

Coût, sécurité et scalabilité : les trois atouts du serverless

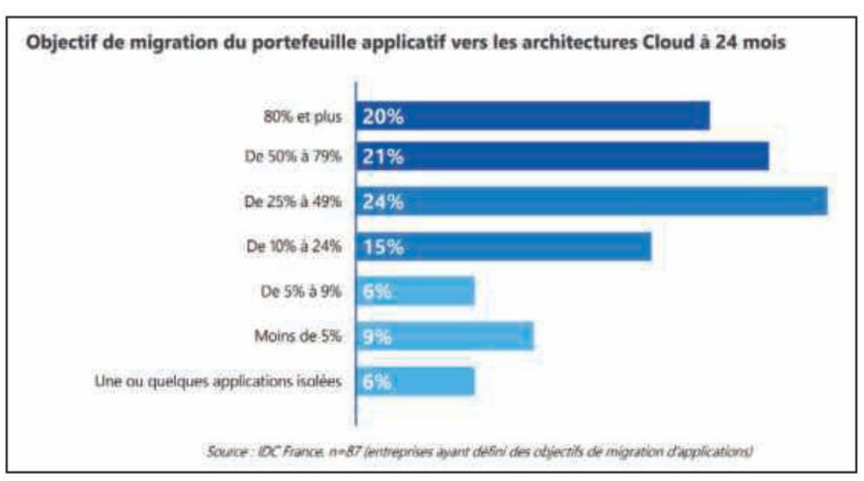
« Le coût est sans doute l'atout le plus évident du serverless : il s'agit du mode de facturation pay as you go le plus optimisé qui soit. On atteint des coûts de « run » extrêmement faibles, de l'ordre de quelques dizaines d'euros seulement dans le cadre d'un projet que nous avons mené pour un énergéticien. Ce coût aurait été très largement supérieur si nous avions mis en œuvre des instances. Le volet sécurité est un autre atout majeur du serverless. La responsabilité de la sécurité de l'application bascule du côté du fournisseur cloud et les tâches de sécurisation, côté entreprise, sont grandement allégées. Enfin, le serverless est scalable à l'infini, le dimensionnement des fonctions Lambda par AWS est automatique. Si on se place du côté des développeurs, l'approche présente de nombreux avantages : le serverless pousse les développeurs à adopter des patterns d'architecture beaucoup plus performants. Le serverless n'a que très peu d'impact sur le code lui-même. Les coûts d'exécution des applications sont très faibles et celles-ci sont beaucoup plus simples à gérer. »

Nous sommes capables de livrer des projets en trois mois contre vingt-quatre par le passé. Nous avions besoin de douze à dix-huit mois pour déployer un stack technologique dans nos datacenters. Sur AWS, il nous faut que trois mois pour mettre en compliance un stack sur notre landing zone. »

François Le Gac, Head of Cloud Product and Service Line chez Airbus.

basses qui reçoivent les événements vont être affectées par une migration vers un autre fournisseur cloud. Toute la partie de l'application qui relève du métier ne sera pas impactée. »

Il existe aujourd'hui des fonctions serverless chez tous les hyperscalers, ainsi que chez Scaleway qui se pose en alternative souveraine. L'adoption du serverless est d'autant plus simple que la méthode n'implique pas de devoir former à nouveau les développeurs. Et qu'il est possible de conserver des pratiques en place, dont la conception pilotée par les domaines (DDD). Toutes les applications ne sont pas adaptées à une approche serverless. Le modèle est particulièrement approprié pour développer des API REST stateless, mais dans d'autres contextes, il sera moins le cas et il faudra composer avec les limites techniques définies par le fournisseur cloud en termes de mémoire, d'espace disque et de durée d'exécution maximale. Le rapport annuel produit par Datadog fait apparaître une adoption extrêmement rapide par les entreprises déjà utilisatrices d'un hyperscaler. Elles emploient plusieurs langages à la fois, mais aussi de nombreux services serverless chez leur cloud provider, preuve d'un usage de plus en plus extensif de cette nouvelle façon de concevoir des applications. ■



Simon Parisot, CEO et co-fondateur de Blank

Pourquoi Blank a choisi les technologies serverless

Filiale à 100 % du groupe Crédit Agricole, Blank est une néobanque qui propose divers services financiers à destination des professionnels. « Dès la création de Blank, fin 2019, j'ai fait le pari de construire nos services avec des technologies que l'on appelle « serverless » ; c'est-à-dire déléguer une partie importante des aspects d'infrastructure à AWS : sécurité, scalabilité, disponibilité… Aujourd'hui, encore peu d'entreprises ont fait ce choix, il était audacieux, mais je suis convaincu qu'il s'agit d'une transformation majeure qui va attirer de plus en plus de start-up. Il y a dix ans, le cloud computing a permis aux entreprises d'externaliser des tâches critiques pour leur activité, mais à faible valeur ajoutée pour leurs clients (la gestion d'un datacenter, par exemple). Le serverless nous permet de franchir une étape supplémentaire dans cette direction. Le temps qu'un ingénieur Blank ne passe pas à configurer de nouveaux serveurs pour tenir la charge, il peut l'utiliser à développer une nouvelle fonctionnalité directement profitable pour nos clients ! »

PROGRAMMATION

LES LANGAGES SÉCURISÉS, PROCHAIN GRAND SAUT ?

Avec l'open source en ligne de mire, les appels à l'adoption des langages de programmation « sécurisés » se multiplient.

Par Clément Bohic

Ruby, Swift, C#... Prière d'envisager sérieusement l'adoption de ces langages de programmation sécurisés. La NSA vient d'émettre une note d'information qui va dans ce sens. Cette publication s'inscrit, notamment, dans la lignée d'un atelier organisé il y a quelques semaines sous la bannière de l'Open Source Software Security Initiative. Un projet qui associe, sous l'impulsion de la Maison-Blanche, les principales agences américaines impliquées dans le domaine de la cyber (CISA, NIST, NTIA).

GOOGLE, MICROSOFT : DES STATS QUI DONNENT LE TON

L'atelier s'est structuré autour de trois grands axes. En l'occurrence, les leviers économiques, la gestion des dépendances... et les langages de programmation sécurisés. Plus précisément, ceux qui gèrent automatiquement la mémoire. En la matière, le consensus s'est porté sur Rust. Avec Java, Python et Go comme options, lorsque les exigences de performances sont moins importantes. Parmi les démarches souhaitables à court terme pour pousser ces langages, financer le développement de l'outillage attenant. On peut aussi envisager de compartimenter les bases de code pour favoriser leur migration incrémentielle. À plus long terme, se posent en particulier des questions de formation. L'aspect économique n'est pas à négliger, tout du moins si on croit le constat selon lequel les équipes Java et Rust sont plus petites que les équipes C/C ++. La note de la NSA fait référence à un autre événement, organisé plus tôt cette année : l'Open Source Software Security Summit II. C'était en mai, sous la houlette de la Fondation Linux et de l'OpenSSF. Il en est ressorti un plan d'action en dix points. Parmi eux, la signature de code, l'amélioration de l'outillage SBOM... et, à nouveau, les langages sécurisés. Au gré de ces événements revient une statistique : 70 % des vulnérabilités logicielles sont dues à des problèmes de mémoire. Les données de Google concernant Chrome la corroborent. Chez Microsoft aussi, on est autour des 70 %. En tout cas, sur la foi de données que le groupe américain a communiquées début 2019 et couvrant une douzaine d'années. La NSA fait remarquer que le développement des outils de fuzzing a simplifié la découverte de telles failles. Dans le même temps, l'agence reconnaît que les langages sécurisés ont leurs contraintes en matière de performance et de souplesse (nécessité fréquente d'un ramasse-miettes, poids de la vérification des accès potentiellement hors limites...). Elle affirme toutefois qu'il peut en coûter autant de sécuriser ceux qui ne le sont pas nativement. D'autant plus que ce palliatif a ses inconvénients, entre le taux de faux positifs de l'analyse statique et la couverture limitée de l'analyse dynamique. ■

Farid Illikoud

CISO chez
Decathlon Technology

« C'est une difficulté d'être multicloud, mais cela assure une résilience. »

Farid Illikoud est Group Chief Information Security Officer (CISO) de Decathlon Technology. Pour *Silicon,* il explique comment la cybersécurité est intégrée à la stratégie multicloud de l'équipementier sportif.

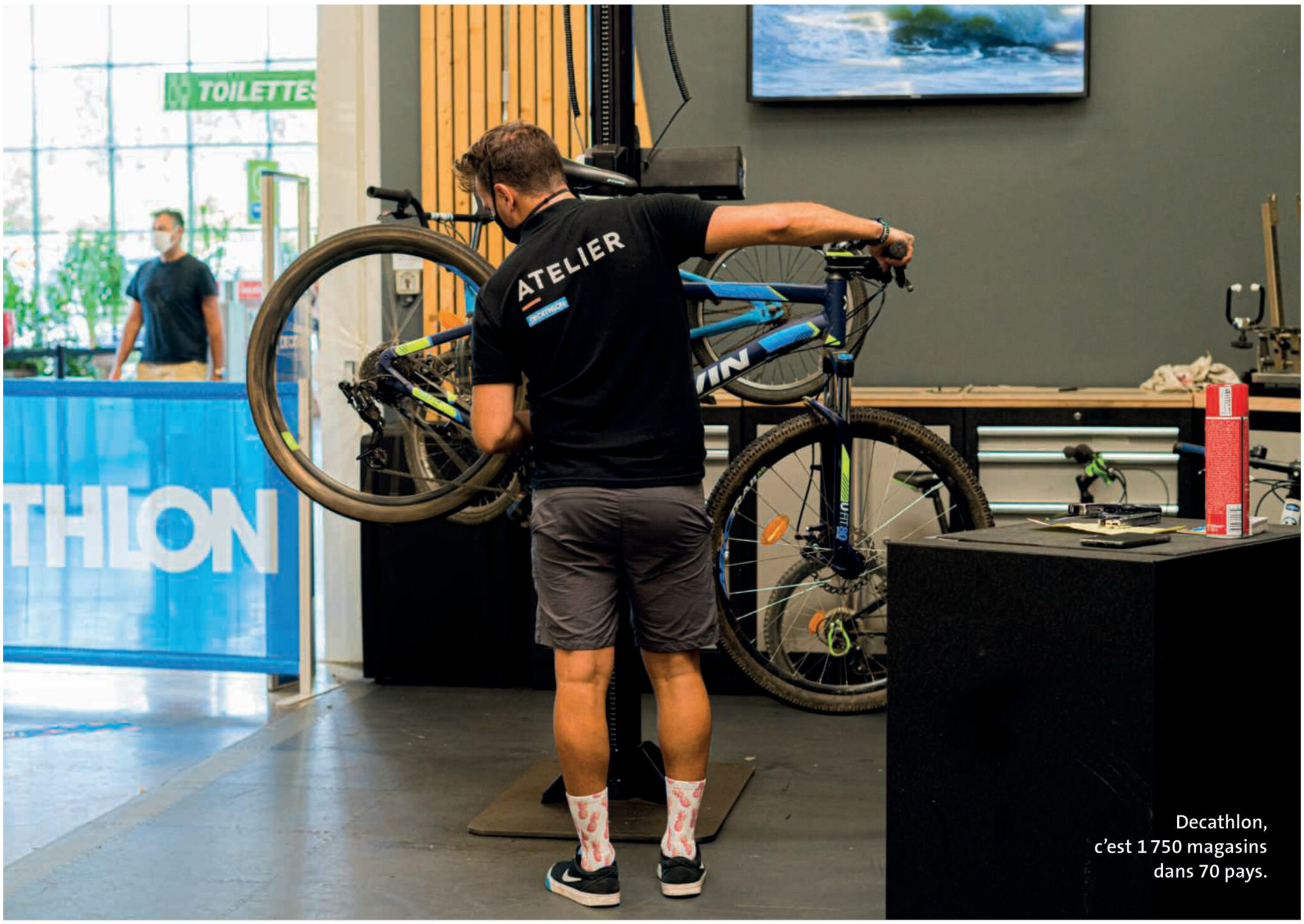
Propos recueillis par Clément Bohic

Qu'implique plus précisément, en matière juridique, cette présence internationale ?
Farid Illikoud Une surveillance continue de l'évolution de la conformité. En Californie, par exemple, le CCPA (California Consumer Privacy Act) évoluera début 2023. Depuis deux ans, on travaille sur le PIPL (Personal Information Protection Law) en Chine. Comme le RGPD, cette loi impose la localisation d'un certain type de données. Cela soulève de vrais sujets : comment réarchitecture-t-on nos systèmes et nos solutions ? Comment imaginer l'expérience utilisateur de bout en bout ? Comment gérer des solutions de big data ? On a la chance d'avoir des équipes juridiques dédiées sur le sujet data, au sens large, dont la privacy et les lois locales. On rêverait, effectivement, d'une forme de normalisation… Il y a aussi un réel sujet de guerre économique entre les États, qui nous dépasse. Il faut être prêt à transférer ses données d'une région vers une autre. C'est, quelque part, la chance du cloud. On n'avait pas nécessairement cette possibilité auparavant, avec des datacenters locaux. Au quotidien, je ne sais pas si on prend vraiment toute la mesure de la dimension géopolitique : une entreprise multinationale comme la nôtre s'expose à plusieurs types d'attaques. Depuis cette année, nous avons rédigé notre plan de gestion de crise dédié à ce sujet au même titre que nous avons des plans de gestion de crise « vol de données », « ransomware » ou « déni de service ». Nous avions des points de présence au Kazakhstan, où il y a eu des émeutes… Nous avons beaucoup travaillé sur le cloisonnement réseau, ce qui nous donne la capacité d'isoler un pays.

Quelle place pour l'open source et sa sécurité ?
F. I. historiquement, Decathlon est une boîte de builders. C'est 3 500 personnes dans la tech et beaucoup de développeurs… qui privilégient tout naturellement l'open source. Depuis l'an dernier, grâce à nos équipes juridiques, nous avons recruté quelqu'un de dédié sur le sujet. Parce qu'au-delà de l'aspect cyber, la question est légale. Les briques qu'on emploie sont-elles conformes du point de vue juridique ? Parfois, vous utilisez des briques logicielles qui deviennent payantes. Avec l'arrivée de cette personne, on a posé un framework : qu'est-ce que l'open source ? Quelles sont les règles à adopter ? On a considéré ce sujet comme un risque, donc on l'a traité tel quel.

La notion de zero trust parle-t-elle au RSSI que vous êtes ?
F.I. Le zero trust ? C'est un buzzword. Comme on parlait, il y a cinq, six ans, de « composants next-generation », par exemple pour les firewalls. Le sujet, pour l'avoir traité longuement dans mon ancienne expérience, est un sujet de contrôle d'accès logique. On revient juste sur la gestion

« Nous avons beaucoup travaillé sur le cloisonnement réseau », Farid Illikoud.



Decathlon, c'est 1 750 magasins dans 70 pays.

« Au quotidien, je ne sais pas si on prend vraiment toute la mesure de la dimension géopolitique : une entreprise multinationale comme la nôtre s'expose à plusieurs types d'attaques. »

des identités et on se dit : « Chaque composant doit être trusté et on sait que tel composant a le droit d'appeler tel autre parce qu'on a établi une relation de confiance. » Ça n'est pas plus que cela. Après, effectivement, lorsqu'on décline ce concept sur d'autres couches et notamment le network, c'est du cloisonnement, de la segmentation : quelle zone a le droit d'appeler quelle zone, avec quel type de protocole, sur quel port réseau ? Là-dessus, vous venez poser des règles, de sécurité, et surtout d'alertes : ça doit sonner tout de suite au niveau de votre SOC.

Un SOC dont vous aimez rappeler le degré d'automatisation…

F. I. Pour au moins deux raisons ! D'abord, la limitation des ressources. On est sur un marché de pénurie. Decathlon a noué des partenariats avec des écoles et des universités. On investit beaucoup dans l'apprentissage et dans l'alternance. On appelle ça « l'école de la seconde chance ». Ensuite, les attaques deviennent nombreuses. Même si vous avez un SOC hyper bien dimensionné, vous ne pouvez pas faire face à un tel volume. Donc, oui à l'automatisation. Mais là aussi, pas de buzzword. Tout en reconnaissant que ça reste compliqué : il faut gérer de faux positifs parce que les patterns d'attaque évoluent très vite. On a investi dans un EDR – et donc un SOAR – depuis 18 mois. Aujourd'hui, on maîtrise bien le D de détection. Mais le R de réponse est très sensible. Soit vous le surcalibrez et, potentiellement, vous lancez de faux positifs et vous bloquez des ressources. Soit vous le sous-dimensionnez et, probablement, vous laissez passer des attaques.

Le zero trust ? C'est un buzzword. Comme on parlait, il y a cinq ou six ans, de "composants next-generation" pour les firewalls, par exemple. C'est un sujet de contrôle d'accès logique. »

Nous-mêmes, nous nous cherchons encore après 18 mois. Notre modèle de SOC, qui existe officiellement depuis le mois de mai, est hybride. Pour plusieurs raisons, nous avons posé comme postulat que les outils et les solutions sont les nôtres. Nous avons des ressources en interne et si demain nous devions remettre en question notre partenariat avec le SOC, nous garderons la maîtrise de nos solutions, sans devoir repartir de zéro. La culture de la boîte, c'est très peu d'externalisations.

La cyber offensive fait-elle partie de votre arsenal ?

F. I. On réalise des exercices très spécifiques. Dernièrement, il s'agissait d'un scénario de vol de clé d'un compte cloud : une attaque « niveau zéro » qui arrive quasiment tous les jours. D'un côté, nous avons une red team qui prépare le scénario, sous l'impulsion de notre Cloud Security Officer. En face, une blue team (des personnes de notre SOC) à qui on a simplement dit : « Vous allez faire face à un incident. » Et c'est la red team qui a gagné. Entre autres points positifs, cela nous permet de développer des patterns d'automatisation : on détecte un leak de clé et on a une remédiation automatique. Le prochain exercice est prévu en décembre. Les moyens sont un non-sujet. C'est juste une question de temps. On se reconnaît beaucoup dans ce que fait ManoMano. C'est ce que j'appelle de la sécurité innovante. Avec beaucoup de transparence, de communication et de partage de bonnes pratiques. ■

Decathlon

- 1 750 magasins dans 70 pays
- 320 magasins en France
- 14 milliards € de CA (25 % en France)
- Plus de 100 000 collaborateurs

Decathlon a noué des partenariats avec des écoles et des universités.

CLOUD SOUVERAIN

LES MILLE ET UNE VOIES DU CLOUD DE CONFIANCE

Des espoirs qu'il porte à la réalité à laquelle il se heurte, le concept de cloud « souverain » est, pour l'heure, sujet à de multiples incarnations.

Par Clément Bohic

Les fournisseurs cloud américains, obligés de « *courber l'échine* » pour rester actifs sur le marché européen ? C'est un fait, estime Édouard de Rémur. Le cofondateur et directeur général d'Oodrive y voit, entre autres preuves, les alliances que Google et Microsoft ont respectivement nouées – en France – avec Thales et le duo Orange-Capgemini. Leur forme : des coentreprises appelées S3NS et Bleu. De doctrine en texte de loi, les règles du jeu se durcissent au nom d'un dénominateur commun : la « souveraineté ». Pour Yann Lechelle, DG de Scaleway, il n'en va pas d'une logique de protectionnisme ou d'isolationnisme. Mais d'un rééquilibrage des rapports de force, pour « *faire entendre la voix de l'Europe* ». La récente rupture du partenariat entre OVHcloud et Google est emblématique des tensions. Le premier aura hébergé, pendant deux ans, une offre fondée sur le « *socle multicloud* » du second : la plate-forme de conteneurs Anthos. Officiellement, le groupe français a considéré que son vis-à-vis avait franchi une ligne rouge en voulant imposer des mises à jour distantes et non plus « locales » (par clé USB).

8 M €
Le coût du projet lancé par l'État pour développer une « suite bureautique cloud souveraine »

DETTE AMÉRICAINE…

Est-ce pragmatique de remettre en cause de telles alliances ? Dans l'absolu, il est « *difficile de se dire qu'on peut tout faire nous-mêmes* », recon-

naît Stanislas de Goriainoff. Le CTO du groupe Sewan – qui a acquis Ikoula l'an dernier – donne l'exemple des logiciels de virtualisation. Passé VMware, « les [offres européennes], je ne dis pas que cela n'existe pas, mais c'est beaucoup moins déployé », constate-t-il. Même son de cloche chez Christophe Lesur. *« Dans l'industrie, il y a une réalité : le barycentre des systèmes d'information, c'est Microsoft. »* Le directeur général de Cloud Temple élargit son propos : « Le marché utilise des technologies américaines, sauf qu'il le fait sans aucune garantie de sécurité. » Et d'avancer, dans un tel contexte, l'argument SecNumCloud. L'obtention de cette certification ANSSI a représenté *« le travail d'une équipe de plus de 20 personnes pendant deux ans et demi »*. SecNumCloud, c'est aussi le graal de Bleu et de S3NS. Qui, plus généralement, promettent une immunité face à l'extraterritorialité des lois américaines. En théorie… mais *« en réalité, pas du tout »,* à en croire Me Julie Jacob. L'avocate, dont le numérique est l'une des spécialisations, qualifie d'*« extrêmement risqués »* ces modèles hybrides. À commencer, au-delà même des considérations de localisation ou de structure capitalistique, par le simple fait d'employer des technologies américaines. *« Plutôt que des solutions de contournement, il faut développer l'écosystème français »,* résume-t-elle, allant jusqu'à plaider pour l'utilisation exclusive de softwares et de matériels nationaux ou européens.

… JUSQU'AU LOGICIEL

Au niveau européen, justement, plusieurs membres tricolores de l'alliance Euclidia font écho à Me Julie Jacob. Il en est ainsi de Clever Cloud, dont le P.-D.G., Quentin Adam, appelle plus globalement à percevoir la valeur du logiciel. *« En le sous-traitant, on cède de facto la partie la plus stratégique et la plus rentable »,* clame-t-il. Et d'exemplifier : *« Ce qu'on achète chez AWS, ce ne sont pas les VM, tout le monde sait en faire. C'est l'IAM, la facturation à la demande, etc. : tous les services additionnels. »*

Nexedi aussi est membre d'Euclidia. Et son P.-D.G., Jean-Paul Smet, est sur la même ligne que Quentin Adam. *« Si on n'a pas accès au code source des logiciels, est-ce vraiment du cloud de confiance ? »* s'interroge-t-il. Son point de vue est tranché : le FISA (Foreign Intelligence Surveillance Act, loi US qui régit les activités de renseignement extérieur) s'applique aux logiciels américains, quelle que soit la nationalité de l'entreprise qui les utilise. Yann Lechelle ne pense pas différemment : *« Pour moi, Bleu, ce n'est pas souverain, car le logiciel ne l'est pas. »* Dans ce cadre, le risque est aussi géopolitique : les États-Unis ont un *« droit de vie ou de mort »* sur l'exploitation des licences. On se souviendra, remarque-t-il, des déboires de Huawei avec Android. Ou des conséquences de la coupure du réseau Visa en Russie après l'ouverture du conflit contre l'Ukraine.

30 mois
Le temps de travail de 20 personnes pour obtenir la certification ANSII.

OFFICE 365 POUR L'EXEMPLE ?

« Si on veut acquérir un jour une forme d'autonomie numérique, on doit avoir une filière du logiciel forte », martèle Édouard de Rémur. *« Si on se limite à héberger […] demain, les acteurs étrangers imposeront leur loi. Aujourd'hui, ils acceptent les contraintes […] parce qu'il y a une alternative. Entreprendre en France est assez facile et on est beaucoup aidé »,* affirme le DG d'Oodrive. *« Là où on a des progrès énormes à faire, c'est sur la commande publique. Elle est totalement désorganisée, il y a très peu de directives, chaque administration est complètement autonome. »*

L'État a bien une doctrine cloud, appuyée de documents tels que la note de la Dinum relative à Office 365. Mais juridiquement, l'ensemble est non contraignant : il ne fait que donner une direction. Bruno Le Maire a laissé entendre, lors de l'inauguration du dernier datacenter d'OVHcloud, à Strasbourg, que la France pourrait légiférer. Cela impliquera néanmoins de préciser des notions. Parmi elles, celle de *« document sensible »*. Ce sera l'une des missions du nouveau CSF (comité stratégique de filière) *« Numérique de confiance »,* annoncé en parallèle de cette même inauguration et que préside Michel Paulin (DG d'OVHcloud). Quentin Adam l'admet : la commande publique

sera peut-être un levier de collaboration « *forcée* ». Mais elle impulsera, en tout cas, une « *culture du travail en commun* ». Et si les produits qui en résultent ne couvraient pas tout le spectre fonctionnel souhaité, on serait bien inspiré de découpler les appels d'offres, glisse Yann Lechelle. Du côté de Clever Cloud, on a, par exemple, intégré les DPU de l'entreprise grenobloise Kalray [trophée de bronze des Silicon Awards Data 2022]. Sur le volet software, dans la lignée de l'appel du Cigref à rechercher une « troisième voie » entre Office 365 et Google Workspace, l'État a lancé un projet à 8 millions € pour développer une « *suite bureautique cloud souveraine* ». Oodrive y a répondu avec Olvid (pour la brique messagerie) et Tixeo (visioconférence). Édouard de Rémur souligne, à cet égard, l'importance d'aller vers une interface utilisateur unique. « *On ne peut pas avoir juste un partenariat entre des acteurs français ou européens qui proposent une interconnexion entre leurs offres.* »

IMPOSSIBLE(S) CONSENSUS ?

En bureautique, mais pas que, les passerelles transnationales restent rares. Il faut dire, comme le fait remarquer Me Julie Jacob, que le schéma de qualification des services cloud [EUCS] n'est pas encore harmonisé à l'échelon européen. SecNumCloud ne vaut pour le moment qu'en France, comme C5 ne vaut qu'en Allemagne, GovCloud au Royaume-Uni, etc. « *Là encore, on se bat contre les Américains* », déplore Édouard de Rémur concernant ce processus d'harmonisation. « *Ils [font pression] pour que, au niveau européen, il n'y ait pas de critères réglementaires.* » Les Allemands aussi font blocage, prétend-il : « *Des acteurs comme SAP exportent beaucoup aux États-Unis et n'imaginent pas d'avoir le niveau de sécurité le plus élevé dans leurs offres.* » Ses propos ne sont pas plus favorables en ce qui concerne l'initiative Gaia-X. Les Américains y ont « *placé leurs pions : [au conseil d'administration] des intégrateurs avec lesquels ils travaillent de façon très proche.* » Au contraire d'Oodrive, Scaleway a participé à l'aventure. Mais la filiale d'Iliad en est revenue. « *Gaia-X ne cherche qu'une chose : trouver le tronc commun qui fait plaisir aux grands acheteurs. Et qui inscrit les fournisseurs majeurs pour sédimenter le marché sur ce tronc commun* », regrette Yann Lechelle. On pourrait penser Cloud Temple plus aligné sur les intérêts du projet. C'est le cas, non sans bémols. « *Le marché débat beaucoup de technologies, mais les communications ne sont pas client-centric* », avance Christophe Lesur. Pour lui, les discussions ne tournent pas suffisamment autour d'un aspect clé : l'interopérabilité. « *La couche technologique qui va la porter, le client saura, pour peu que le marché soit pluriel, ce qu'il a besoin de consommer [...] : la bonne architecture pour la bonne application.* » Stanislas de Goriainoff invite pour sa part à ne pas perdre de vue le potentiel antagonisme entre les garde-fous que posent l'Europe et la compétitivité de ses entreprises. En l'occurrence, le risque que ces dernières adoptent des technologies en décalage par rapport à leurs concurrents étrangers. Il précise qu'en matière de souveraineté, la proximité fait partie des axes qui résonnent auprès d'une clientèle comme celle de Sewan/Ikoula. « *Moins pour ceux qui achètent en ligne, mais dès qu'on va construire l'infrastructure avec un client, s'intégrer dans leur plan informatique global, il y a de l'intérêt.* » ■

> *Dans l'industrie, il y a une réalité : le barycentre des systèmes d'information, c'est Microsoft. Le marché utilise des technologies américaines, sauf qu'il le fait sans aucune garantie de sécurité.* »
>
> ***Christophe Lesur, directeur général de Cloud Temple.***

CLOUD SOUVERAIN

VMWARE PARIE SUR LES PARTENARIATS LOCAUX

Les fournisseurs hyperscale ont-ils leur place sur le marché du cloud souverain ? C'est oui pour VMware... à condition de les inscrire dans des stratégies multicloud et de ne leur confier que des données non sensibles.

Par Clément Bohic

Le groupe américain VMware a exprimé ce point de vue il y a quelques semaines. Il a reconnu, en parallèle, l'attrait des joint ventures qui émergent actuellement, à l'image de Bleu et de S3NS, en France. En faisant toutefois remarquer qu'un tel modèle doit encore prouver sa pertinence. Le contexte ainsi posé, VMware avance sa propre approche de la souveraineté, fondée sur des partenariats avec des fournisseurs cloud locaux. Depuis environ un an, ceux-ci peuvent bénéficier du sceau « Sovereign Cloud ». La condition : déclarer leur conformité au framework du même nom.

Ce framework, essentiellement technique, apporte un certain niveau de souplesse pour permettre des offres adaptées aux typologies de clients et de données. Certains critères annexes sont, au contraire, inflexibles. En particulier concernant la structure juridique des fournisseurs. Ces derniers doivent être des « entités autonomes » (aucun

lien avec des entités localisées hors du territoire) enregistrées et établies dans la région où elles souhaitent commercialiser leurs offres. L'Union européenne compte pour une seule région. Le cercle « Sovereign Cloud » approche de la trentaine de membres. Une dizaine de fournisseurs européens en sont, dont un qui couvre le territoire français : OVHcloud. Sopra Steria est aussi dans la liste, mais pour la Norvège, avec sa plate-forme SolidCloud.

ZERO TRUST ET DISPONIBILITÉ

Au cœur de la notion de souveraineté selon VMware, il y a la résidence des données. Dans les grandes lignes, elles doivent rester soumises aux lois de la juridiction dans laquelle elles ont été créées ou collectées. Cet aspect s'étend à la gestion et à la gouvernance des clouds. Deuxième point clé : l'accès aux données et leur intégrité. Le fournisseur doit proposer son offre sur au moins deux datacenters Tier III (disponibilité : 99,982 % ou plus). Et fournir, entre autres services, de la sauvegarde, de la récupération après sinistres, de la microsegmentation et de multiples options de stockage. Troisième point : la sécurité des données et la conformité des infrastructures. Il s'agit ici d'obtenir les certifications industrielles ou gouvernementales adéquates pour les systèmes de contrôle de sécurité mis en place. Le chiffrement fait aussi partie des exigences, au minimum avec les fonctionnalités natives de vSphere et de vSAN. Tout comme le zero trust, au minimum avec NSX-T. Quatrième point : l'indépendance et l'interopérabilité des données. Avec deux consignes : architecture de conteneurs et capacité de migration bidirectionnelle des charges de travail.

Techniquement, le framework exige une architecture en deux zones de confiance (aussi appelées domaines de sécurité). Une « souveraine » et une « résidente ». La première fait l'interface avec le monde extérieur. La seconde est isolée. Le framework impose aussi une stack technologique minimale. En tête de liste, Cloud Foundation Enterprise (pile SDDC), vSAN (stockage), NSX-T Data Center Advanced ou Enterprise (réseau) et Cloud Director (gestion). S'y adjoignent plusieurs composantes du portefeuille Tanzu, dont Data Management Services (services de données) et Application Catalog (registre de composants open source prévalidés). L'approche cloud souverain implique le fonctionnement de certaines solutions en mode hors ligne. Avec des différences par rapport à la version classique. L'outil de monitoring vCloud Usage Meter, par exemple, ne transfère pas automatiquement ses données vers vCloud Usage Insight. Concernant la souplesse que laisse

le framework, elle touche par exemple à la sauvegarde : au niveau des VM, c'est bien, au niveau des applications, c'est mieux. Idem pour le contrôle d'accès : préférentiellement à base de rôles, mais éventuellement à base d'attributs. Les options sont particulièrement nombreuses sur la sécurité zero trust. VMware considère qu'utiliser NSX-T pour segmenter les flux dans le domaine souverain suffit. Il recommande toutefois d'autres de ses produits pour étendre la démarche zero trust aux appareils, aux utilisateurs et aux données. Parmi eux, son SASE, son EDR Carbon Black et sa plateforme Workspace ONE.

SOLUTIONS SOUVERAINES

L'adaptation des services VMware en mode hors ligne se fait progressivement. La gamme Tanzu l'illustre. La transition est faite pour le runtime (Kubernetes Grid) comme pour l'outillage DevOps (Application Platform). Elle ne l'est pas encore pour le plan de contrôle Mission Control (bêta privée). Et elle l'est partiellement pour les services de données : c'est bon pour le serveur de messagerie RabbitMQ, ça le sera avant la fin de l'année pour le module DBaaS (sur MySQL ou Postgres), puis en 2023 pour Greenplum (data warehouse) et Gemfire (cache). Les services de données ont leur guide technique dédié pour le cloud souverain. On y parle haute disponibilité pour Postgres, chiffrement sur MySQL, fédération et contrôle d'accès sur RabbitMQ, etc. Pour compléter ses outils, VMware pousse plusieurs « solutions souveraines » tierces : Caveonix Cloud (pour l'évaluation continue de conformité) et Fortanix DSM pour chiffrement (BYOK et gestion des secrets). ■

LE NO CODE

SES

PROMESSES

SES

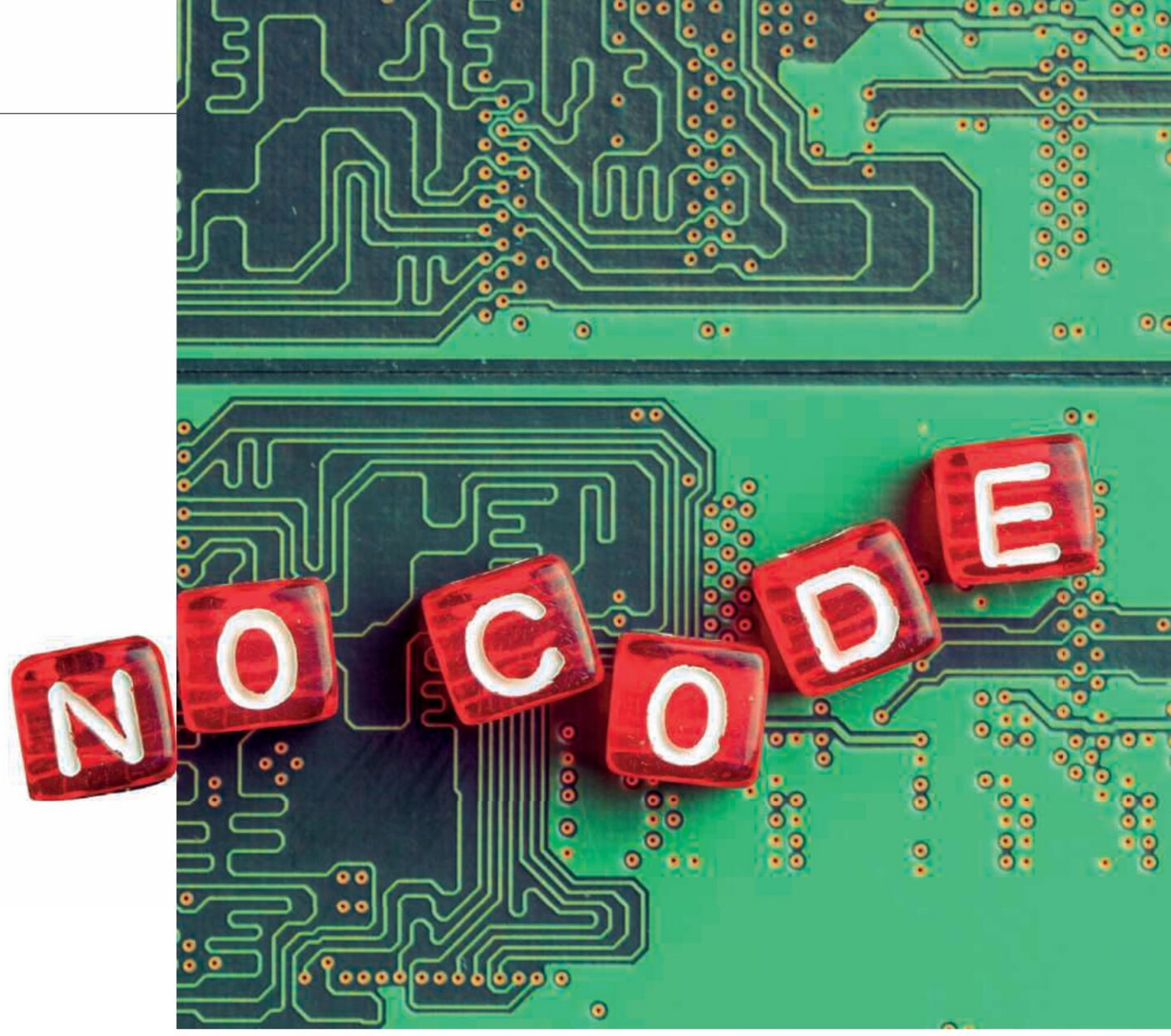
LIMITES !

En autorisant la conception d'applications sans avoir à écrire une ligne de code, le no code accélère les développements tout en réduisant fortement les coûts. Quels sont les cas d'usage éligibles ? Quelles entreprises ont recours à cette approche ? Quels sont les freins à lever ? Éléments de réponse.

Par Xavier Biseul

Le no code est appelé à rebattre les cartes du développement. En évitant le recours aux langages informatiques traditionnels, cette approche permet d'élaborer des sites et des applications web jusqu'à trois plus rapidement, pour un coût divisé au moins par deux. Le no code constitue une des réponses à la pénurie de développeurs et à la volonté de réduire le « time to market », facteur clé de la transformation numérique. Il participe, par ailleurs, à la digitalisation des TPE et PME aux budgets contraints. Selon le cabinet d'études Gartner, 80 % des produits et services technologiques pourraient être conçus par des non-informaticiens à l'horizon 2024. Depuis une interface 100 % graphique, un « maker » ou un « product builder » assemble des briques fonctionnelles préparamètres à la manière d'un Lego, établit

le workflow de la future solution, puis la relie à une base de données. En soi, la volonté de créer des applicatifs en utilisant le moins de code possible n'est pas nouvelle. Le phénomène remonte à quelques dizaines d'années avec les environnements de développement intégré (EDI) et les ateliers de génie logiciel comme Visual Basic de Microsoft ou WinDev. Comment, dès lors, expliquer l'explosion du no code ? Pour Maxime Topolov, cofondateur de l'agence code.store, *« le phénomène profite de la multiplication des APIs permettant à des applications front end ou à des tableaux de bord d'interagir avec les applications et les données de l'entreprise. »*



DISPOSER D'UN CRM DÉDIÉ

Quels sont les cas d'usage éligibles ? De la simple feuille de calcul au CRM sur mesure en passant par l'automatisation des processus métiers, le spectre est large. *« Dans le domaine de la gestion de la relation client ou de l'e-commerce, il y a beaucoup de niches verticales qui ne sont pas complètement couvertes par les solutions du marché comme Salesforce ou HubSpot,* poursuit Maxime Topolov. *Le no code va, par exemple, permettre à un barbier de disposer d'un CRM dédié. »* Un des premiers projets no code sur lequel a travaillé Christelle Curcio, cofondatrice et Chief makers officer du groupe Alegria, portait également sur un CRM, mais destiné, cette fois, à un cabinet d'avocats. *« Il s'agissait de déterminer quels étaient les trois prospects les plus pertinents à inviter à déjeuner au cours du mois. Aucun logiciel du marché ne répondait à cette question. »* Le no code permet aussi de pallier les lacunes fonctionnelles des progiciels métiers et autres ERP. *« Pour combler les trous dans la raquette, les opérationnels emploient, faute de mieux, Microsoft Excel ou Google Sheets »,* note Maxime Topolov. Christelle Curcio abonde dans son sens. *« Une solution sur étagère ne couvre pas 100 % des besoins d'une entreprise et celle-ci n'utilise vraiment que 10 % de ses fonctionnalités. L'éditeur déroule sa feuille de route produit et ne peut se permettre du faire du sur-mesure. »* Le recours au no code favorise également l'automatisation de tous les processus manuels en parti-

> *Il s'agissait de déterminer quels étaient les trois prospects les plus pertinents à inviter à déjeuner au cours du mois. Aucun logiciel du marché ne répondait à cette question. »*
>
> ***Christelle Curcio, cofondatrice et Chief makers officer du groupe Alegria.***

culier dans les métiers support de la finance, du marketing, de la communication, de l'IT ou des RH. Une entreprise se dotera, par exemple, d'un outil de réservation de salles de réunion ou d'un workflow interne pour valider les notes de frais. *« Cela permet à la fois de réaliser des gains de productivité et de libérer les énergies en déchargeant les collaborateurs qui effectuaient ces tâches répétitives et chronophages »*, observe Christelle Curcio. Maxime Topolov cite comme autre exemple le cas d'une application développée pour gérer les petits-déjeuners au sein d'une chaîne d'hôtels. *« Au lieu d'imprimer tous les matins une feuille A4 et de barrer les noms des clients présents, le personnel hôtelier utilise une tablette. Le nom du client associé à son numéro de chambre remonte automatiquement depuis l'ERP. »* Cofondateur et P.-D.G. de Cube, Pierre Launay s'est, lui, mis à Airtable et Make (ex-Integromat) en souhaitant justement maximaliser les processus de son agence. *« J'ai rapidement perçu la valeur de ces outils. Une fois que l'on a goûté au no code, on cherche à optimiser toutes les tâches à faible valeur ajoutée comme réconcilier une facture et un devis. »* Le no code permet aussi, selon lui, de tester l'appétence d'un nouveau marché à un produit ou à un service. Il cite le cas de l'agence d'intérim

> *J'ai rapidement perçu la valeur de ces outils. Une fois que l'on a goûté au no code, on cherche à optimiser toutes les tâches à faible valeur ajoutée comme réconcilier une facture et un devis. »*
>
> ***Pierre Launay, cofondateur et P.-D.G. de Cube.***

Gojob qui souhaite exporter son modèle. *« Elle a pu rapidement voir que le marché américain répondait favorablement à son offre, mais pas le marché britannique. »*

GAGNER EN AGILITÉ

Plus généralement, Christelle Curcio estime que la culture no code libère le potentiel de créativité. *« Combien de fois j'ai entendu : si je savais coder, je ferais plein de choses. Designer de formation, j'étais, à titre personnel, frustrée de devoir m'arrêter au stade de la maquette. Aujourd'hui, je peux aller jusqu'au bout de mes idées sans dépendre du service IT. »* En ce sens, le no code représente, à ses yeux, une vraie révolution technologique et sociétale. *« Les ingénieurs ne sont plus les seuls à régir le monde numérique. Tout le monde peut devenir acteur de sa vie digitale. »* Elle y voit aussi un levier d'inclusion et de féminisation. Le groupe Alegria emploie 30 % de femmes et sa filiale formation, Alegria Academy, propose des promotions composées pour moitié d'étudiantes. L'apprentissage est à la fois plus facile et moins long. *« Il ne s'agit pas d'apprendre*

un langage, mais de comprendre les principes de modélisation et de base de données, la logique d'interface et d'intégration. » Pour autant, le no code n'est pas appelé à se substituer au codage en dur, mais à le compléter. Il y aura toujours besoin de développeurs traditionnels, ne serait-ce que pour maintenir des systèmes critiques de type ERP, reposant sur un existant fort (legacy). À défaut de tout basculer en no code, la méthode low code permet d'introduire un peu de code traditionnel dans un ratio de 90/10 ou de 80/20. « *Il est plus facile de mettre un bout de JavaScript que de tout coder en dur* », poursuit la dirigeante. Autre avantage du no code : sa capacité à transposer rapidement un besoin utilisateur en solution applicative. Pour Maxime Topolov, l'approche est inhérente aux procédés agiles. « *En supprimant beaucoup d'étapes, le no code permet d'avoir des itérations de l'ordre de la journée. Il est, par ailleurs, possible de concevoir une application in situ à côté des utilisateurs. Cette co-construction éradique les erreurs de communication, les phases de formation et de conduite du changement.* » Pour Jean-Michel Maillet, User eXperience Digital Officer chez Colas Digital Solutions, l'approche low code-no code permet d'aller rapidement sur une maquette. « *Proposer une restitution visuelle est beaucoup plus parlant pour l'utilisateur final. Il est aussi plus facile de se tromper. Si on fait un mauvais choix, on ne perd qu'une semaine et non pas des mois de développement. Revers de la médaille, il faut freiner les ardeurs du métier qui multiplieraient sinon les réajustements.* »

LE CŒUR DE CIBLE : LES PME

Quel est le profil type de l'entreprise qui a recours au no code ? « *Les start-up sont très au fait des possibilités des technologies du low/no code*, juge Maxime Topolov. *Mais elles les utilisent parfois de manière anarchique et il faut les freiner. À l'inverse, les DSI des grands comptes sont encore réticentes et se posent pas mal des questions en termes de*

> *Proposer une restitution visuelle est beaucoup plus parlant pour l'utilisateur final. Il est aussi plus facile se tromper. Si on fait un mauvais choix, on ne perd qu'une semaine et non pas des mois de développement. Revers de la médaille, il faut freiner les ardeurs du métier qui multiplieraient sinon les réajustements.* »
>
> ***Jean-Michel Maillet, User eXperience Digital Officer chez Colas Digital Solutions.***

sécurité et de conformité. » Entre les deux, « *les PME voient, depuis la crise sanitaire, les bénéfices de la digitalisation et souhaitent optimiser leurs process tout en ayant des contraintes de coût. Pour de 3 à10 K€, elles peuvent avoir une application sur mesure pour traiter les tickets de support ou superviser leur workflow financier.* » Le premier obstacle sur le chemin d'une entreprise qui s'initie au no code porte sur le choix d'outil. Comme toute industrie naissante, il existe une multitude de solutions - Alegria en a recensé plus de 800 ! – ce qui poste question de leur pérennité. « *Tous les éditeurs ne vont pas survivre* », estime Maxime Topolov qui conseille de privilégier les systèmes bien installés. « *En même temps, la solution peut se faire racheter et le coût de migration d'un outil à un autre est relativement faible.* »

En attendant qu'un mouvement de consolidation s'opère, quelques noms se détachent comme Webflow pour la conception de site web, Adelo ou Bubble pour le développement full stack d'applications web, Notion pour la gestion de contenu, Shopify dans l'e-commerce, Make et Zapier pour l'automatisation des processus. Se présentant comme des Excel 2.0, Airtable ou Smartsheet permettent, eux, de créer des tableaux de bord personnalisés et d'automatiser les flux de travail. Une entreprise sélectionnera le meilleur outil en fonction de la typologie de projet ou de la présence ou non de compétences internes. Elle tiendra aussi compte de ses contraintes en termes de sécurité et de conformité. S'agissant de solutions cloud distribuées par des éditeurs pour la plupart américains se pose, en effet, la question de la confidentialité des données personnelles au regard du RGPD. Si Bubble ou Airtable proposent, moyennant un coût supplémentaire, de basculer sur la région Europe de leur cloud provider, d'autres éditeurs comme Retool ou n8n permettent d'héberger les données dans un serveur d'entreprise. Il est aussi possible de recourir à une solution open source comme Appsmith et BaseRow ou de faire le choix du made in France avec des acteurs tels que WeWeb ou Fortia, dédié au monde de la finance.

POSER UN CADRE DE GOUVERNANCE

Enfin, il convient pour une entreprise de poser des règles de gouvernance. En fonction de l'existant et du niveau d'intégration au système d'information, quels projets sont éligibles ou non au low code-no code ? Pour répondre à cette question,

> *Le phénomène profite de la multiplication des APIs permettant à des applications front end ou à des tableaux de bord d'interagir avec les applications et les données de l'entreprise.* »
>
> ***Maxime Topolov, cofondateur de l'agence code.store.***

le groupe Colas *(lire encadré),* a fondé un centre d'excellence dédié et ouvert une usine de développement consacré au low code-no code à côté de celles pour les environnements PHP et. Net. Colas mène, en parallèle, une politique en faveur des citizen developers, ces experts métiers qui, grâce au low code-no code, créent en toute autonomie leurs applications. Le leader mondial du BTP identifie les collaborateurs qui ont conçu des applications utilisées par plus d'une personne afin de les accompagner, les guider dans leurs choix, mais aussi les sensibiliser aux risques. « *Quand une application devient critique, il faut pouvoir la reprendre en central afin de la maintenir en cas de départ ou de congé de son créateur* », avance Jean-Michel Maillet. Un projet low code-no code reste un projet comme les autres avec ses exigences de qualité et de maintenabilité. ■

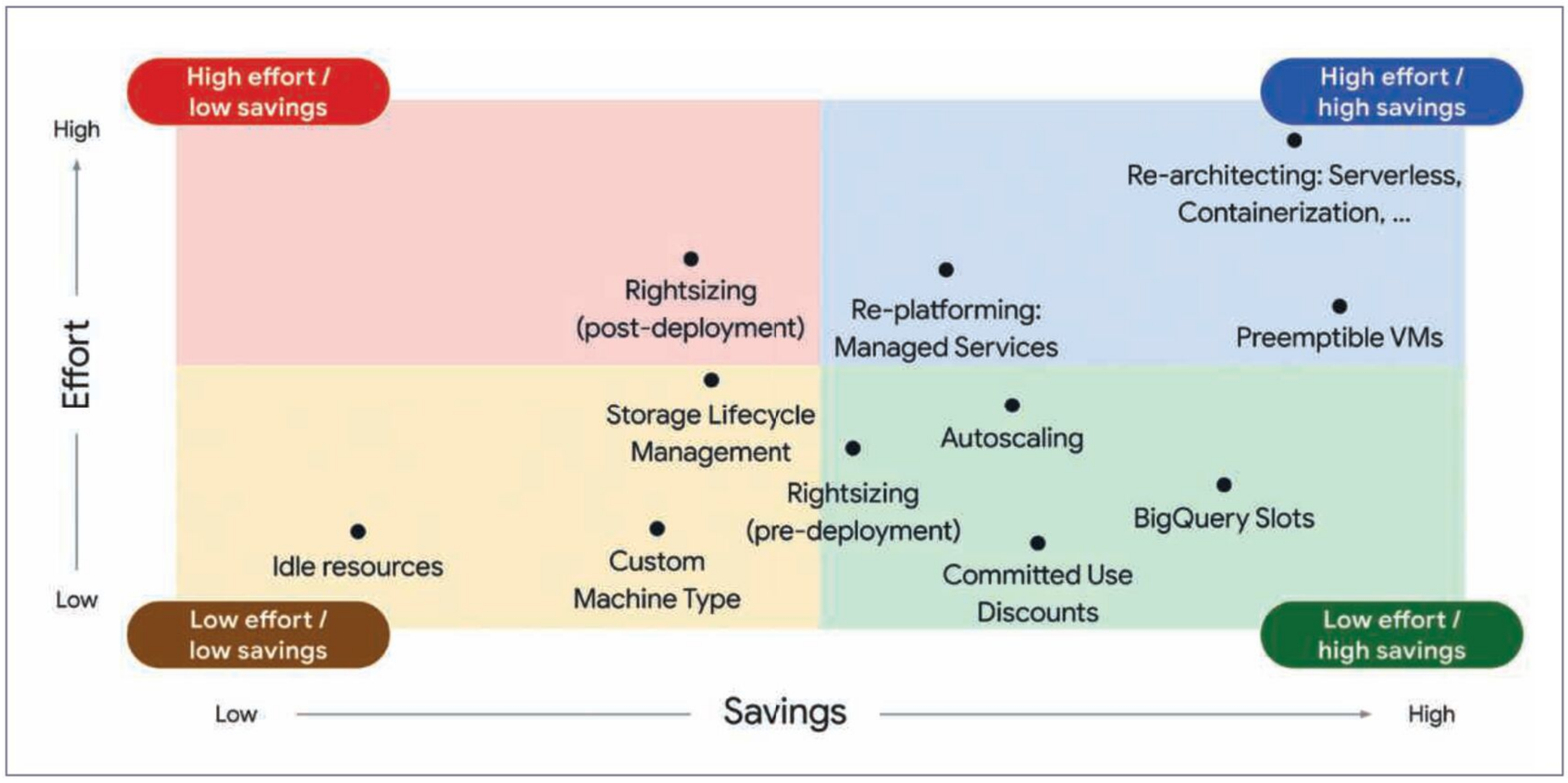
FINOPS

DU BON USAGE DES ÉTIQUETTES

L'étiquetage des ressources IT apparaît comme un élément clé pour la mise en action d'une démarche de gestion financière du cloud d'infrastructure.

Par Clément Bohic

Avez-vous bien étiqueté vos ressources ? Les « trois grands » du cloud d'infrastructure le conseillent fortement dans le contexte des stratégies FinOps. La logique ? Davantage de précision dans le contrôle des coûts. En tout cas, une fois les projets lancés. En amont, chacun possède ses simulateurs, ses outils d'aide à la migration et, plus largement, son framework d'architecture englobant cette même dimension. Laquelle, rappelons-le, ne consiste pas tant à diminuer le coût total que les coûts unitaires – ou comment tirer parti de l'élasticité du cloud pour lisser au mieux la demande. La « partie amont » implique un enjeu en particulier : l'optimisation du code (FinOps by design). Avec une question centrale : l'opportunité de (re) structurer ses applications afin qu'elles tirent parti de technologies potentiellement sources d'économies, comme les conteneurs, l'autoscaling et le serverless.



Quels efforts pour quelles économies ? La matrice de Google.

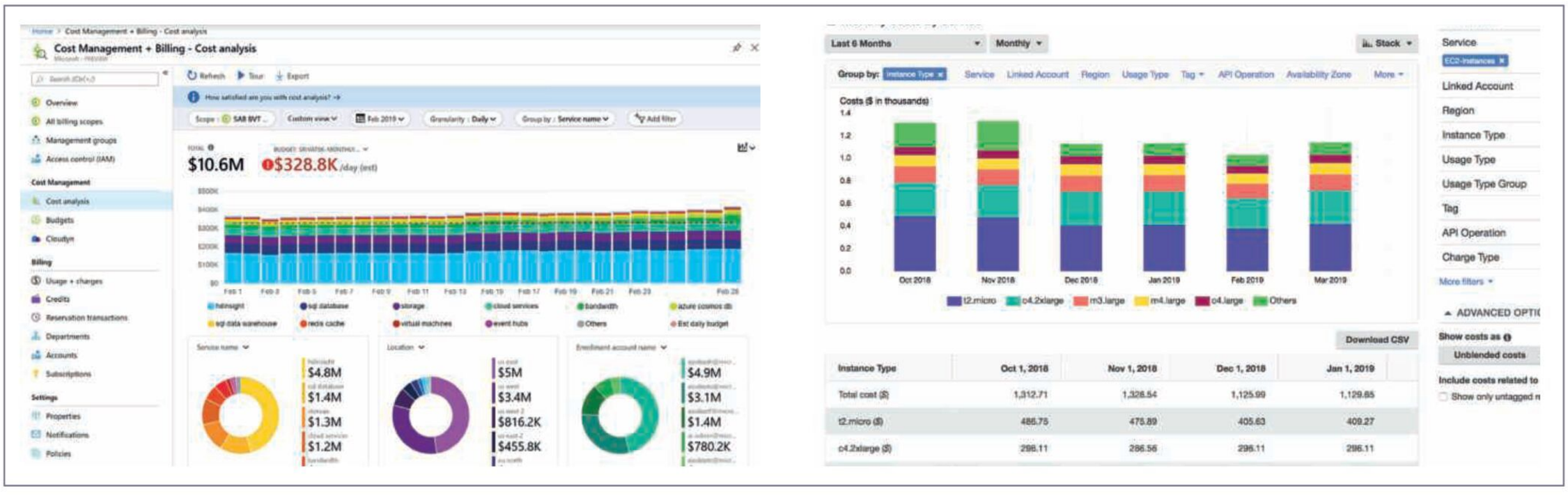
Sur la « partie aval », les hyperscalers disposent aujourd'hui de boîtes à outils exhaustives. Cela commence au niveau de la visualisation des coûts.

VISUALISER ET ATTRIBUER

Point d'entrée : la console cloud. L'exploration peut se poursuivre, d'une part, dans les outils internes de dataviz (QuickSight chez AWS, Data Studio chez Google Cloud, Power BI chez Microsoft) ; y compris par l'intermédiaire de dashboards préconçus qui dépassent, pour certains, la sphère FinOps. D'autre part, en exportant les données, par exemple vers des systèmes de reporting. De palier en palier, on gagne en finesse. Et on peut d'autant plus contextualiser les dépenses, en les corrélant à la valeur dégagée (agilité, productivité, résilience...). Ces visualisations et les rapports qui en résultent sont perfectibles. Azure, notamment, n'affiche pas les charges additionnelles de type support, et certaines solutions achetées par l'intermédiaire de la marketplace. Surtout, par défaut, ils s'alignent sur la topologie des projets tels que structurés chez le fournisseur. L'étiquetage trouve là son intérêt, pour rattacher des ressources à des unités organisationnelles qu'on n'a pas pu représenter directement sur l'architecture cloud. Le processus peut s'automatiser en partie au travers de stratégies et de modèles de déploiement. Ou encore en exploitant – comme plusieurs outils tiers – les services natifs de monitoring et d'exécution de fonctions sans serveur.

RESSOURCES TAGUÉES ET AGILES

Par rebond, les étiquettes sont aussi un renfort pour la définition de budgets et d'alertes. Elles aident également à gérer l'état des ressources. En tête de liste, l'arrêt et le redémarrage des VM



(voir le cas de Médiamétrie ci-contre). Là encore, pas de couverture intégrale. Certaines ressources échappent encore aux tags, tels les IP externes chez Google Cloud et les éléments internes aux déploiements VMware sur Azure. Il peut par ailleurs exister des conflits, comme sur Amazon EC2, où l'autoscaling a la priorité sur les règles de start/stop. Il arrive que les fournisseurs cloud recommandent explicitement des outils externes. Google pointe ainsi les utilisateurs vers Forseti, un projet open source qu'il sponsorise. Et plus précisément vers l'une de ses briques : Config Validator, pour la détection continue des ressources mal étiquetées (au run, donc, Terraform pouvant intervenir au déploiement).

PENSER AUX MODÈLES ÉCONOMIQUES

Avant d'optimiser les usages, on peut chercher à les cadrer. L'application de quotas au niveau des ressources (appels API par seconde, quantité de données par jour...) fait partie des solutions à disposition. Comme la mise à l'arrêt de projets lorsqu'on dépasse un plafond budgétaire. Moins radical, mais qui requiert plus d'efforts : adapter le dimensionnement des ressources. Les économies les plus « évidentes » sont liées essentiellement aux ressources de calcul inactives et sous-utilisées. Les autres pans de l'infrastructure peuvent demander davantage de réflexion : cycle de vie des objets stockés, intérêt des liens dédiés face aux VPN et au réseau Internet... Une règle commune : surveiller la variation des tarifs entre régions cloud. On y associera un travail au niveau des métiers. L'analyse de données est emblématique des gains réalisables sur ce plan, avec de nombreux leviers à actionner : partitionnement des tables, limitation du périmètre de requête, mise en cache, tâche en lot plutôt qu'en flux, etc. Optimiser l'usage de l'infrastructure est une chose. Le faire pour le modèle de facturation en est une autre. Là aussi, les leviers sont multiples. À commencer par les remises forfaitaires et sur engagement. Sur la partie compute, il y a les instances personnalisées et les VM préemptives, idéales pour les charges de travail prévisibles. On aura aussi un œil sur la possibilité de transférer des licences. En la matière, Microsoft permet d'utiliser, sur Azure, des licences on-prem de Windows Server et de SQL Server. Pour apporter une dimension multicloud au FinOps, on ne se tournera pas vers les hyperscalers. Même si Microsoft a la particularité de prendre en charge – avec un surcoût – les infrastructures AWS. Chez ce dernier, tout n'est pas non plus gratuit. On paye, entre autres services, l'accès API aux métriques de coûts et les automatisations adossées aux budgets. ■

COMMENT MÉDIAMÉTRIE FAIT DU FINOPS BY DESIGN

En 2014, le spécialiste de la mesure d'audience prend la décision de basculer son système d'information sur AWS. Une démarche aujourd'hui bouclée à 80 %, qui doit s'achever en 2023. Médiamétrie produit des études d'audience TV, radio et Internet. Avec une DSI de 130 personnes (sur 700), elle fonctionne en 24/7 pour collecter les résultats d'audience quotidiens qui sont évalués en flux et réalise une centaine de mises en production par mois. En 2014, une stratégie « cloud first » est adoptée et le choix se porte sur AWS.

Premier axe de cette démarche

Le FinOps by design. Il implique la prise en compte des bonnes pratiques dans les dossiers d'architecture technique. Et la réalisation de tous les développements et tests dans le cloud AWS, jusqu'aux tests. L'étiquetage en est une fondation. À deux échelons. D'un côté, les tags techniques, destinés notamment à gérer les plages d'arrêt et de redémarrage hors prod. De l'autre, les tags de facturation. De trois types, servant à définir le domaine applicatif, à préciser le rôle des ressources dans l'architecture globale (collecte, traitement ou restitution) et à identifier des sous-domaines applicatifs ou des couches d'infrastructure.

Deuxième axe

L'automatisation des procédures d'optimisation. Au centre du dispositif, le tag autostop. Et un outil open source pour l'exploiter : Cloud Custodian. Sur un domaine applicatif, l'arrêt des VM le soir et les week-ends hors production a fait économiser 40 % du coût des ressources. Médiamétrie a opté pour une politique stricte : hors production, les ressources non étiquetées sont automatiquement supprimées. Trusted Advisor, l'outil de recommandation d'AWS, aide à la détection des instances sans connexion pendant plus de deux semaines.

Optimisation tarifaire

Médiamétrie recourt aussi à l'optimisation tarifaire. En particulier avec les remises sur engagement pour EC2, RDS et ElastiCache. Parallèlement, elle adapte les ressources aux usages : avoir telle machine en prod n'oblige pas à avoir la même sur l'environnement de développement. Elle exploite aussi l'autoscaling quand c'est possible : certaines de ses applications peuvent employer quatre instances en période creuse et monter jusqu'à vingt selon la demande. Au global, le taux d'utilisation des ressources atteint 98 à 100 %.
Troisième axe : la supervision. Les alertes sur budgets réels ou prévisionnels en sont la composante centrale. Avec le renfort d'un des dashboards que fournit AWS et de rapports personnalisés. La détection d'anomalies a par exemple permis de repérer un coût de transfert inter-régions qui, sur un mois, avait coûté près de 5 000 $. Médiamétrie est parvenu à diviser ce coût par dix. Soutenue par cette politique d'étiquetage, la démarche FinOps de Médiamétrie a permis de réduire de 20 % le coût annuel du cloud chez AWS. Et, mécaniquement, l'empreinte carbone... L'approche FinOps by design, aujourd'hui bouclée à 80 %, devrait s'achever en 2023.

CYBERSÉCURITÉ

COMMENT LA MENACE CHANGE DE VISAGE

Le panorama annuel de l'ENISA sur la menace cyber illustre l'évolution des cibles, des outils et des techniques d'attaque.

Par Clément Bohic

Le mot ransomware rime-t-il forcément avec chiffrement ? De moins en moins, à en croire l'agence européenne ENISA qui mentionne la montée en puissance du phishing. Du côté des cybercriminels, on joue de plus en plus, lors des négociations, sur la couverture assurantielle des victimes. L'ENISA évoque deux groupes en particulier : Karakurt et LAPSUS$. Ce dernier est entré dans la lumière au printemps avec le piratage d'Okta. LockBit, Conti et ALPHV/BlackCat ont été les ransomwares, les plus « actifs » au premier semestre 2022.

NOUVELLES ATTAQUES

Qu'en est-il si on élargit le champ d'analyse à l'ensemble des malwares ? On constate que l'IoT y est pour beaucoup dans la croissance globale du volume d'attaques. L'usage des macros Office, au contraire, recule depuis que Microsoft a resserré l'étau. En parallèle, il augmente sur une voie alternative : les images disque (ISO, VHDX). Avantage, on ne peut leur apposer l'indicateur MotW (« Mark of the Web »), ce qui favorise le contournement de filtres tels que SmartScreen. Le mode opératoire Nobelium, qui a ciblé la France l'an dernier, a exploité cette technique. Conséquence du développement de l'authentification à facteurs multiples (MFA), les attaquants tendent à délaisser la compromission de comptes de messagerie au profit des plates-formes. La compromission des serveurs Exchange a eu le vent en poupe ces derniers temps, avec l'appui de failles comme ProxyLogon et ProxyShell. Le ciblage de l'IoT se répand aussi dans le cadre des attaques en déni de service (DoS). L'ENISA l'avait déjà constaté dans son panorama 2021. Il faut dire que la sécurité est généralement moins robuste sur ces appareils, aussi bien par défaut (il est, entre autres, parfois impossible de modifier le mot de passe) que tout au long du cycle de vie (correctifs plus rares et moins souvent appliqués).

UN DDOS ? NON, JUSTE UN POC

Emblème : le botnet Mozi, qui exploite des vulnérabilités vieilles de plusieurs années. S'en prendre aux modèles IA qui gouvernent les décisions de cybersécurité est un levier émergent pour le déni de service. L'ENISA constate aussi le développement du RDoS. En d'autres termes, du déni de service avec rançon. Et parfois, sans attaque. Juste avec un PoC (un « mini-DoS ») en soutien d'une injonction à payer… Il arrive que des cybercriminels avancent l'argument des conséquences juridiques : nous avons compromis votre infrastructure, et vous êtes responsable de toute attaque DDoS qu'elle permettrait de mener. Parfois, cette intimidation n'est qu'une première étape. L'ENISA en réfère à un cas rencontré l'an dernier : les cibles recevaient un avertissement de compromission de leur infrastructure, assorti d'un lien vers un dossier cloud censé contenir des preuves. Il contenait en fait la charge malveillante BazarLoader. Dans le même esprit, on nous mentionne un cas de phishing en deux temps. Les attaquants se faisaient passer pour un employé de l'ambassade de Belgique en Irlande. C'est uniquement une fois répondu au mail qu'un malware, est envoyé, intégré dans un fichier zip. ■

Silicon DAY CYBERSECURITE

ANTICIPER LES CYBERATTAQUES & SOIGNER SA RÉSILIENCE IT

27 SEPTEMBRE 2022

Retour sur les prises de paroles des partenaires

En partenariat avec

COHESITY · COMMVAULT · jamf · LastPass · FORTINET · SOPHOS · tenable · VEEAM · WatchGuard

Cohesity place son cluster au service de la cyber-résilience

Données, métadonnées et traitements cruciaux sont protégés et orchestrés par le cluster de Cohesity qui consolide les sauvegardes, pour une reprise d'activités fiable et rapide à la fois.

« *Lorsqu'on veut sanctuariser son infrastructure, mieux vaut la simplifier. Si on a de multiples silos avec plusieurs serveurs de médias, passerelles et solutions de stockage répartis sur divers réseaux et dans le cloud, cela crée de nombreux points de faiblesse. Cohesity permet d'unifier ces environnements pour sécuriser au maximum la sauvegarde,* » explique François-Christophe Jean, directeur technique de Cohesity.

La cyber-résilience se distingue d'un plan de reprise complet en cas de sinistre, nuance-t-il : « *On doit se concentrer sur le noyau dur du S.I., c'est-à-dire les applications et données vitales pour l'entreprise. Nous permettons de remettre en route ce cœur MVC (Minimum Viable Company) le plus vite possible, en éliminant les goulets d'étranglement des architectures traditionnelles.* » précise-t-il.

Un cluster évolutif conçu pour la reprise rapide

Le cluster Cohesity accompagne l'évolution des volumes de sauvegarde tout en apportant des facultés de traitement également évolutives, cette montée progressive en capacité et en puissance s'effectuant simplement par ajout de nœuds. L'architecture autorise des traitements analytiques et de restauration répartis, tant en mode physique, qu'en mode virtuel ou dans le cloud. « *Grâce aux traitements massivement parallèles, nous pouvons booter un millier de VMs directement dans notre cluster, pour relancer provisoirement les applications sur ce stockage secondaire, avant de proposer une migration de type VMotion visant à replacer les machines virtuelles sur l'infrastructure de production, dimensionnée pour tenir les engagements de niveaux de services.* »

Les entreprises ciblées ne sont pas uniquement de très grandes organisations puisque la grappe de serveurs Cohesity démarre à partir de trois nœuds de 12 To chacun et qu'il est aussi possible de bénéficier des avantages de la plateforme en mode SaaS : « *Une entreprise peut démarrer avec un cluster de 36 To, et/ou souscrire à notre offre BaaS (Backup as a Service) afin de bénéficier de la détection d'anomalies et de s'armer face aux ransomware, à moindre coût. Avec l'offre DMaaS (Data Management as a Service), le client s'abonne à un service de sauvegarde, de Disaster Recovery, d'isolation de données (FortKnox) tandis que Cohesity s'occupe des automatismes nécessaires.* »

Si l'immuabilité des données reste un élément fondateur de l'infrastructure résiliente, cette pierre d'angle s'avère nécessaire, mais insuffisante, souligne cependant François-Christophe Jean : « *Nous considérons l'immuabilité des métadonnées et des traitements, pas uniquement celle des données. Si un malware a détruit le catalogue de sauvegarde, il faut analyser les data, afin de reconstruire le catalogue. L'objectif de notre cluster consiste à récupérer workloads et données, avec un délai de restauration aussi rapide que possible. Pour y parvenir, il faut être en mesure de détecter des anomalies. Et, à ce niveau, toutes les architectures ne se valent pas.* » ■

COHESITY

La méthode Commvault pour se prémunir des cybermenaces

Une protection efficace des données d'entreprise commence par bien les identifier, les localiser et les trier. Commvault aide ses clients à maîtriser leurs sauvegardes, sur site et dans le cloud.

« *L'important, c'est de pouvoir compter sur ses données prioritaires à tout moment pour pouvoir repartir au plus vite après une attaque cyber. Nous accompagnons nos clients et partenaires dans la mise en place de solutions pérennes incluant des backups résilients et efficaces,* » explique Sébastien Weber, ingénieur avant-vente Commvault.

Avant de restaurer les fichiers de sauvegarde, la suite Activate de Commvault aide à bien identifier les données et à en faire le tri. Comment ? En détectant les fichiers sans accès afin de les archiver avant de mener une migration vers le cloud, par exemple. « *La connaissance et la classification des données sont deux préalables nécessaires à une bonne protection. Deux modules de notre suite Activate, respectivement File Storage Optimisation et Sensitive Data Governance, sont associés pour mener ce tri conformément aux priorités de l'entreprise,* » précise-t-il.

Réduire le délai d'indisponibilité du S.I.

Sébastien Weber partage volontiers une expérience vécue dans une structure internationale, avant qu'il n'entre chez Commvault : « *Quand l'attaque par ransomware frappe, l'administrateur est réveillé en pleine nuit par ses collègues à l'étranger qui ne peuvent plus accéder aux serveurs à distance. Faute de plan d'actions et d'identification des données minimales pour travailler, nous avons subi une forte pression des métiers et du management. Il a fallu deux semaines pour retrouver un fonctionnement très dégradé, puis un mois avant de repartir en production. Depuis, un grand ménage a été fait dans les données stockées, réduisant la surface d'attaques et le temps de restauration des sauvegardes. C'est l'un des enseignements tirés de cet incident.* »

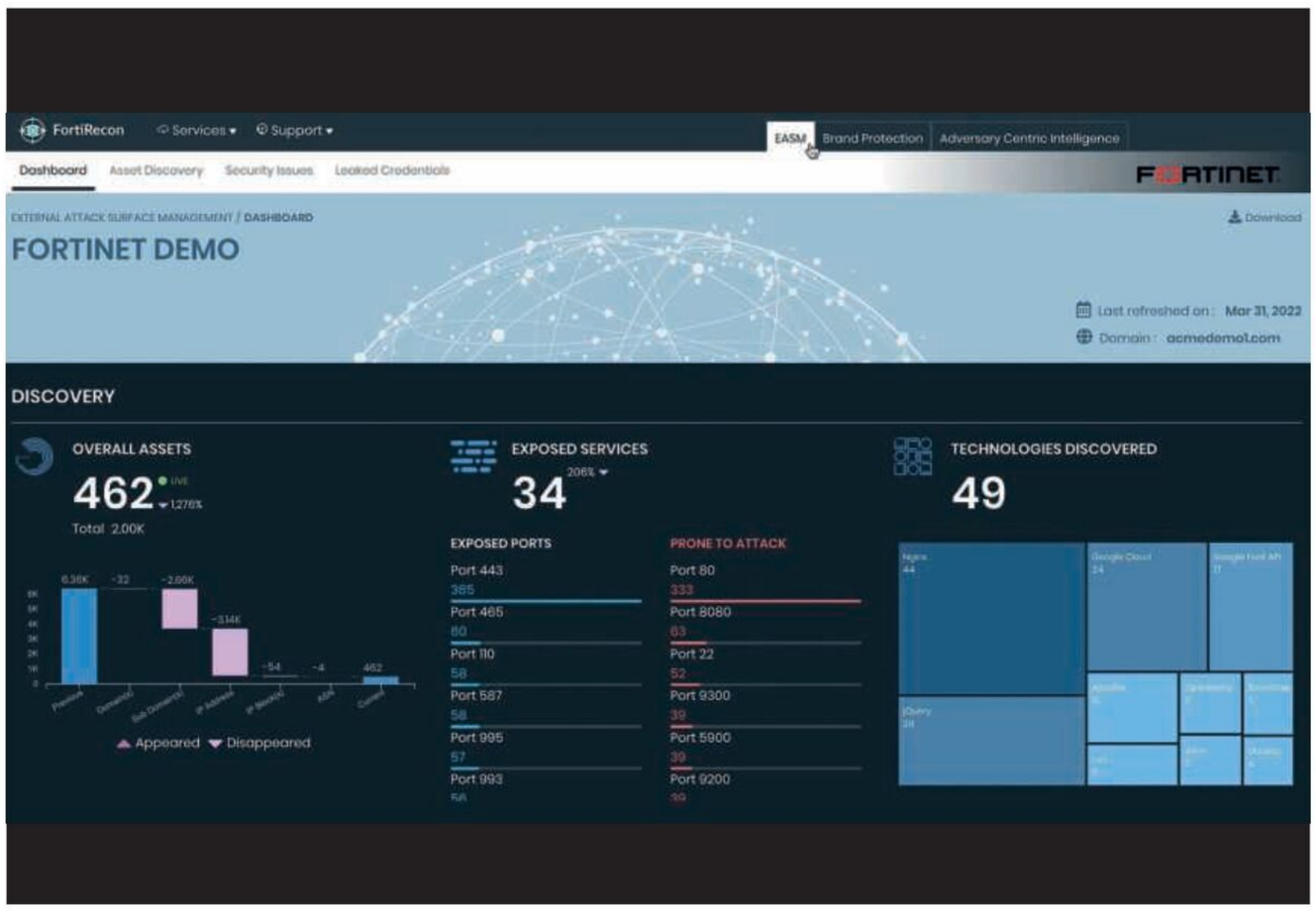
Depuis 25 ans, Commvault a développé des connecteurs pour protéger les principaux formats de données et gagner en agilité, en facilitant la bascule de VMware vers HyperV ou Nutanix, voire vers un cloud public. « *Ces ponts aident nos clients à s'affranchir d'une technologie de virtualisation, y compris en mode Disaster Recovery. Ils peuvent répliquer des données entre plusieurs environnements physiques, virtuels ou cloud, tout en ordonnançant la reprise d'activités en cas d'incident majeur sur la production.* »

Une autre précaution consiste à bien tester le plan d'identification des sources de données, afin de restaurer les bonnes sauvegardes et de redémarrer les serveurs dans le bon ordre. « *Commvault facilite le pilotage de la reprise d'activité en apportant une orchestration et une consistance lors de la remise en état des machines ; l'offre Metallic propose ces services en mode SaaS. La solution ThreatWise positionne des leurres sur le réseau, des systèmes complets surveillés à distance pour retracer le cheminement de l'attaque et permettre de réagir au plus vite.* » ■

COMMVAULT

Fortinet modélise la Cyber Kill Chain pour contrer les attaques en progression

Grâce à l'examen détaillé d'une cyberattaque, Fortinet trace les vulnérabilités exploitées, et signale les outils pertinents, étape par étape, pour se prémunir de fuites de données numériques.



Suivant un scénario d'attaque/défense sur une société fictive, Guillaume Cherruau et François Vinel, deux ingénieurs avant-vente de Fortinet ont proposé une démonstration concrète du vol d'identifiants et de leur commercialisation à l'occasion du récent Silicon Day Cybersécurité. En modélisant chaque étape de la Cyber Kill Chain, ils ont analysé l'attaque, vérifié les brèches retenues et montré les outils de défense complémentaires pour y faire face.

La phase de reconnaissance intervient avant même l'attaque. Durant cette première étape, l'attaquant s'appuie sur le social engineering, sur les réseaux sociaux, articles de presse, sites Web d'entreprise et recherches de fichiers via le web. La simple détection d'une adresse e-mail, à joindre en cas d'erreur de livraison, peut être mise à profit.

L'outillage consiste à retenir, parmi une kyrielle de frameworks et de malwares personnalisables, les briques logicielles à réunir pour mener une attaque ciblée. Par exemple, l'outil evil-pdf pourra incruster un keylogger (un logiciel malveillant d'interception de frappes au clavier), au sein d'un fichier bureautique. L'attaquant n'a plus qu'à préparer son email, en se faisant passer pour un manager et en exigeant, dès que possible, une intervention sur l'erreur de livraison jointe.

Face à cette stratégie offensive, l'entreprise peut recourir aux services de pentest, s'équiper de scanners de vulnérabilités ou faire appel aux services SaaS FortiRecon ; dans ce dernier cas, une console de supervision améliore la visibilité sur les attaques en cours, précisant les comptes ciblés. Mieux, elle aide à réduire les risques numériques, grâce à une liste d'actions correctives.

Pendant l'attaque, le malware est remis à la victime par téléchargement automatique, ou via une clé USB infectée ou encore via un simple e-mail ; c'est la phase de delivery. L'attaque peut être bloquée à ce stade par un moteur antivirus. Pour lutter contre le phishing, FortiMail identifie les messages malicieux et leurs attachements suspects, rejetés automatiquement.

La phase d'exploitation détermine les dégâts résultant de l'attaque. Les mécanismes exploités sont le centre de Command and Control pour exfiltrer des fichiers partagés, le Reverse Shell pour gagner un accès distant à un poste client, ou le keylogger pour récupérer les identifiants saisis au clavier. Un logiciel EDR (Endpoint Detection and Response) bloquera ces malwares, FortiEDR offrant des défenses en prévention, en temps réel, et en réponse sur incident.

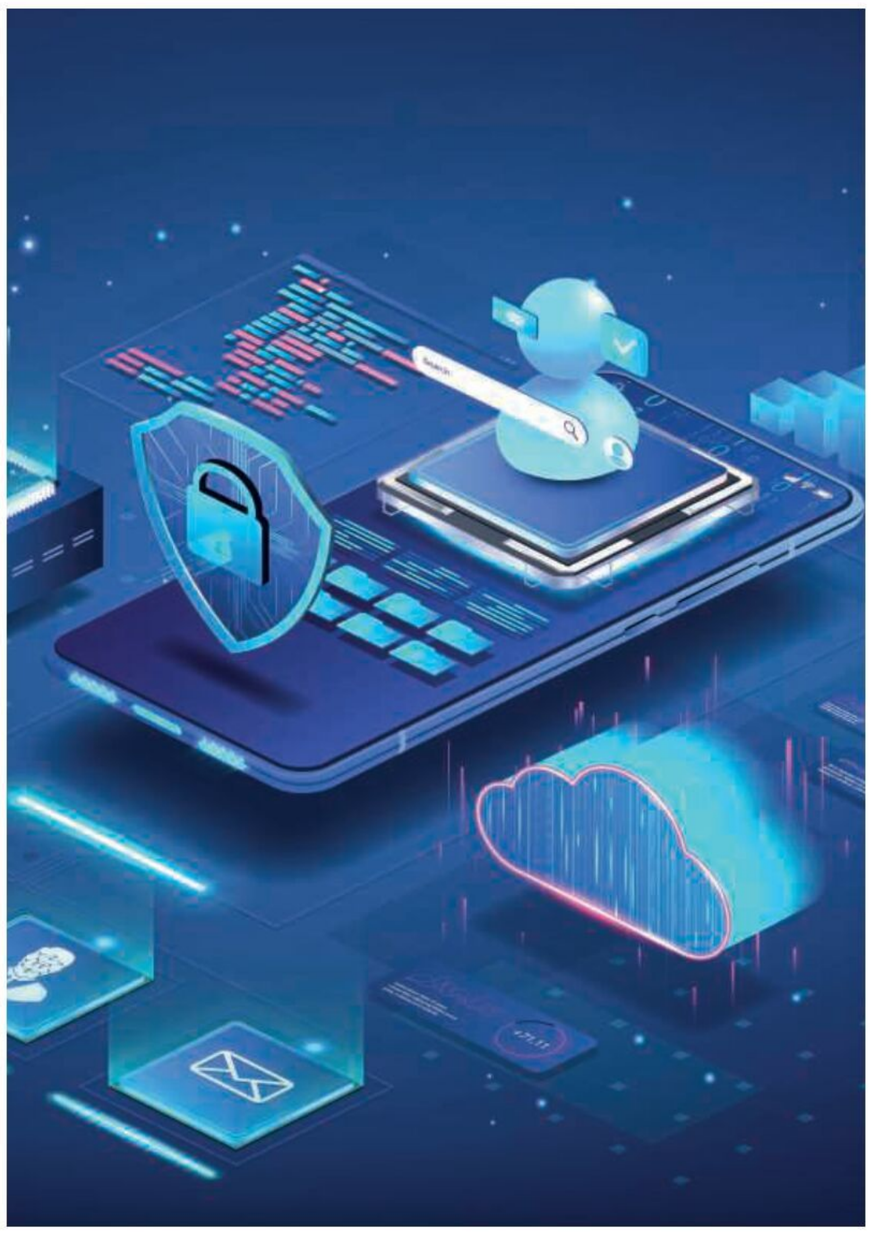
La dernière étape consiste à mener les bonnes actions, selon les motivations de l'attaquant. Pour se prémunir de la fuite de mots de passe et de leur commercialisation, la console FortiRecon améliore la posture de sécurité, dès la détection d'une tentative de vol d'identifiants. ■

FORTINET

silicon

Jamf protège les terminaux Apple en préservant la vie privée des utilisateurs.

Les solutions Jamf sécurisent et gèrent les environnements macOS, ainsi que les parcs mobiles hétérogènes composés de smartphones et tablettes sous iOS et Android.



« Le malware *Pegasus a impacté des milliers de terminaux mobiles iOS et Android dans le but d'espionner des responsables politiques. Plus récemment, Uber a subi une attaque par ingénierie sociale, cherchant à dérober des identifiants et mots de passe via les consoles d'administration de l'entreprise. Il faut sécuriser tous les environnements mobiles à présent,* » souligne Aurélien Autin, Senior Key Account Manager, Systems Engineer de Jamf.

Jamf Protect est la seule solution EDR (Endpoint Detection and Response) protégeant spécifiquement les ordinateurs Apple sous macOS. Pour les parcs mobiles Apple et Android, Jamf propose une solution unifiée de MDM (Mobile Device Management), qui permet d'établir des règles et contrôles pour différents terminaux, bloquer les contenus à risque et le shadow IT.

« *L'une des grandes forces de nos solutions est le lien entre l'EDR et la MDM, en particulier lorsque l'on doit remédier aux vulnérabilités détectées,* » poursuit Aurélien Autin.

Des logiciels en phase avec chaque version de macOS

Selon les entreprises, le niveau de maturité vis-à-vis de la sécurité des postes de travail fixes et des terminaux mobiles varie. Or, les cyberattaques font feu de tout bois, ciblant chaque environnement. L'équipe de soutien aux utilisateurs a donc besoin de solutions de sécurité adaptées à chaque système d'exploitation : « *Des malwares s'exécutent sur tous les OS à présent. Cependant, les solutions déportées de Windows sur Mac consomment trop de ressources sur les ordinateurs Apple et peuvent engendrer des problèmes de compatibilité lors des mises à jour du système d'exploitation,* » prévient Aurélien Autin.

Jamf prend en compte le dernier environnement système disponible dès le jour de sa sortie.

Les solutions Jamf sont en phase avec les dernières fonctionnalités de macOS pour ne pas freiner la productivité des administrateurs et des utilisateurs qui veulent disposer de la dernière mise à jour système.

Une autre différence importante tient au choix de microprocesseurs du constructeur : « *Depuis l'arrivée des puces M1 et M2 d'Apple, le Mac perce nettement en entreprise. Ce matériel requiert cependant des outils de sécurité compatibles avec ses composants internes. De plus, deux autres aspects ne doivent pas être négligés : la confidentialité des données privées et l'expérience utilisateur.* »

Les utilisateurs disposant de la solution de filtrage web Jamf profitent d'une navigation plus sereine, sans compromettre leur vie privée. Quant à la solution d'accès zero-trust ZTNA, elle remplace un réseau privé VPN, sécurise les accès distants, chiffre le trafic et révoque les terminaux à risques. ■

silicon

Un coffre-fort de mots de passe pour chacun avec LastPass

Le logiciel LastPass aide à sensibiliser à la cybersécurité chaque salarié de l'entreprise, à autoévaluer ses règles d'hygiène informatique pour améliorer la gestion des identités numériques.

« *Actuellement, plus de quatre brèches de sécurité sur cinq sont liées à des problèmes d'identités numériques et de gestion des mots de passe, 83 % précise même le cabinet d'études IDC. Si les administrateurs informatiques ont bien conscience du problème, ils ne sont pas les seuls à partager des informations sensibles dans l'entreprise. Les services financiers, les ressources humaines et d'autres départements gagnent à s'équiper d'un gestionnaire de mots de passe. Pour être efficace, il faudrait que tous les utilisateurs utilisent LastPass et suivent ses recommandations,* » souligne Patrick Brennan, le directeur des ventes indirectes de l'éditeur éponyme.

Avec l'essor des services web et des ressources dans le cloud, chaque utilisateur exploite en moyenne 197 comptes en ligne. Comment retenir autant d'identifiants et accéder rapidement à chaque application ? Si le problème n'est pas nouveau, force est de constater que les stratégies pour *y pallier doivent progresser : « il n'est pas rare de croiser un simple tableau bureautique stockant les mots de passe, ou encore des notes manuscrites proches du clavier. Les sésames restent souvent trop simples à deviner, fondés sur une suite alphabétique, le nom d'un animal domestique ou celui d'un enfant avec sa date de naissance. Deux fois sur trois, on note qu'un même mot de passe est réutilisé pour accéder à plusieurs services en ligne. Ces mauvaises pratiques génèrent un risque énorme pour l'entreprise,* » poursuit-il.

L'usurpation d'identité peut mener à une fuite d'informations, voire à l'immobilisation de services essentiels et à une demande de rançon. D'où l'importance d'offrir un gestionnaire de mots de passe compatible avec tous les terminaux de l'utilisateur et d'y associer des protections d'accès de type SSO (Single Sign On) et MFA (Multi-Factor Authentication). « *À présent, il y a toujours des applications non gérées en interne, du shadow IT ou des comptes d'accès et des mots de passe partagés entre collaborateurs. Dans ce cas, l'authentification à multiples facteurs aide à valider que la personne qui accède à l'application est vraiment la bonne personne,* » précise Patrick Brennan.

LastPass peut être déployé sur les principales plateformes et navigateurs du marché. Les mots de passe sont stockés dans le cloud via une technologie dite *"zero knowledge"* empêchant quiconque d'accéder aux identifiants secrets.

Quelle bonne pratique retenir pour le dernier mot de passe à retenir, celui permettant d'ouvrir le coffre-fort numérique ? « *Nous recommandons plutôt une phrase de passe, un extrait de poème, de chanson ou une citation à laquelle personne ne penserait, sauf l'utilisateur. Il faut proscrire les dates d'anniversaire, prénoms de la famille, et leur préférer quelques chiffres et caractères spéciaux.* » ■

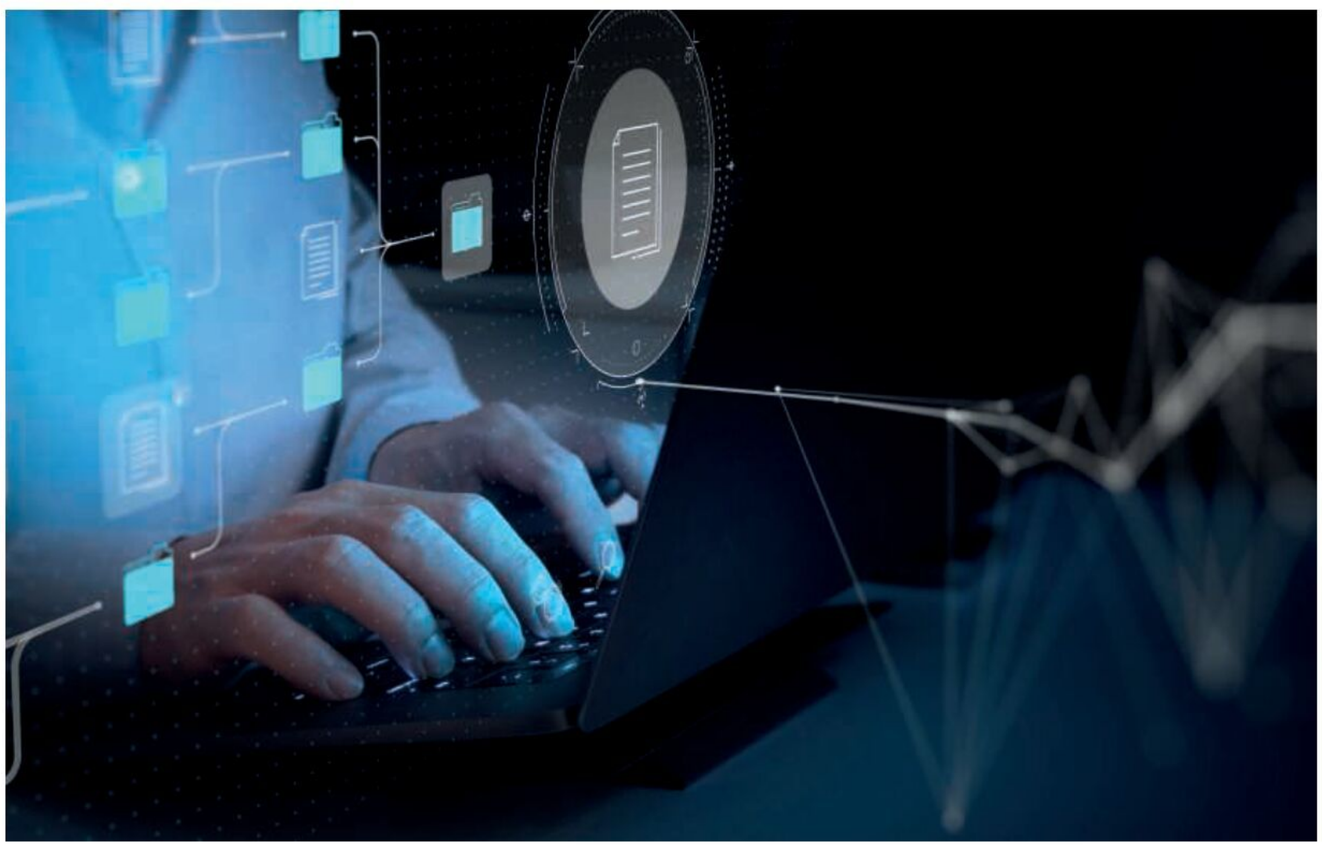
LastPass •••

Ransomware : Sophos fournit une réponse instantanée via son SOC externalisé

L'offre Cybersecurity as-a-Service de Sophos combine des équipes réparties sur ses centres opérationnels de sécurité aux automatismes traitant en masse les tentatives de cyberattaques.

Le rapport sur l'état des ransomwares 2022 remis par Vanson Bourne à Sophos est sans appel : deux tiers des sondés ont subi au moins un ransomware en 2021, contre 37 % en 2020, sur un total de 5 600 professionnels informatiques issus de 31 pays ; avec, deux fois sur trois, des données numériques bel et bien chiffrées malgré eux. En moyenne, la rançon payée par leur entreprise a presque quintuplé en un an pour atteindre 703 341€.

Face au succès croissant des kits d'attaques dans le cloud et du modèle RaaS (Ransomware-as-a-Service) qui étend considérablement la portée des ran¬somwares, Benjamin Mercusot, ingénieur avant-vente cybersécurité de Sophos souligne les bénéfices d'un centre d'opérations de sécurité (SOC) externalisé : *« les laboratoires Sophos Labs analysent plus d'un demi-million de menaces par jour. Les attaquants s'efforcent de rendre leur progression difficilement décelable ; dorénavant 75% des attaques sont uniques, personnalisées. Avec l'offre CaaS (Cybersecurity as a Service), Sophos affecte un interlocuteur à chaque client, qui analyse les besoins, prodigue de bons conseils et aide à répondre en cas d'attaque. »*



Une solution adaptée à l'entreprise

L'éditeur britannique accompagne des entreprises de toutes tailles avec des offres aussi cohérentes que possible, en tenant compte de l'évolution des solutions en place dans l'organisation et des tentatives déjà enregistrées dans son écosystème. En effet, il faut un ensemble de bonnes pratiques, d'expertises et de logiciels capables d'interagir pour fournir une cybersécurité globale. Le CaaS remonte des indices de suspicion de plusieurs sources contribuant à mener des enquêtes qualifiées, en évitant les faux positifs.

Plusieurs formules sont proposées pour bénéficier des services du SOC externalisé, dont un service par abonnement et un service à la demande délivrant une réponse rapide pendant 45 jours, quelles que soient les solutions de sécurité en place dans l'entreprise.

« Des collecteurs et des API Restful complètent le système Sophos Central pour procurer une vision globale du périmètre et du système d'information. La grande force du SOC instantané est d'associer des IA et des compétences humaines pour qualifier les attaques, apprendre continuellement, et apporter la bonne réponse en 24/7. Déjà 12 000 clients ont souscrit à cette offre pour améliorer la continuité de leurs services hors des heures ouvrées, ou pour un accompagnement temporaire devenu nécessaire. »

En soutien du SOC, plusieurs datacenters basés en Europe hébergent le datalake conçu pour l'analyse de métadonnées des sites surveillés, avec une ségrégation par client. Une corrélation d'indices détermine le facteur de risques de l'entreprise et déclenche uniquement des alertes pertinentes. ■

SOPHOS

Tenable One gère l'exposition cyber sur toute la surface d'attaque IT, OT et cloud

L'informatique industrielle, de gestion et les services cloud peuvent à tout moment être cible d'une attaque via une faille non identifiée ou corrigée. Tenable propose une visibilité complète des vulnérabilités, pour améliorer la posture de sécurité globale.

« *Tous les secteurs d'activités sont concernés par la transformation numérique ; l'éducation, la finance, l'industrie... La surface d'attaque évolue aussi avec le télétravail qui concerne tout le monde à présent. Il faut se soucier des réseaux domestiques, des environnements industriels (l'OT), des identités numériques, jusqu'aux code de développement des ressources déployées sur les infrastructures cloud* » recommande Bernard Montel, directeur technique EMEA de Tenable.

Avec les applications distribuées qui empruntent de nombreuses bibliothèques et frameworks intégrées, les brèches subsistent très longtemps avant d'être comblées. Les attaquants se font fort de les détecter, pour glisser des logiciels malveillants dans le système, prendre des données sensibles en otage ou bloquer une production.

Disponibilité et améliorations continues

« *Il y a toujours eu des menaces ciblant les actifs de l'entreprise. Ce qui change, ce sont les chemins d'attaque exploités pour aller d'un point A à un point B dans l'infrastructure. L'attaquant d'aujourd'hui peut profiter des faiblesses des applications cloud ou de celles des accès du télétravail. Or, dans le monde industriel, la disponibilité continue est primordiale. Le moindre arrêt d'une chaîne de production a de lourdes conséquences financières.Connaître tous les actifs de l'entreprise (IT,OT, Cloud) pour identifier tout chemin d'attaque est indispensable* » poursuit-il.

La plateforme Tenable One propose un suivi dynamique de l'exposition aux risques IT et OT ; elle unifie la découverte et la visibilité de tous les actifs jusqu'aux ressources cloud. Disponible sur site ou via le cloud, elle fournit une évaluation de l'exposition et des vulnérabilités sur l'ensemble de la surface d'attaque et permet une amélioration continue de la sécurité.
Plutôt qu'une approche photographique assemblant de simples scans de vulnérabilités par nouvelle application d'entreprise, Tenable défend un modèle holistique de gestion des risques par les signaux faibles et phénomènes isolés qui s'inscrivent désormais dans la sécurisation du système d'information et de production.

Tracer chaque changement de configuration

« *Nos clients industriels nous demandent de casser les silos, que l'on agrège pour eux les données de sécurité et qu'on les analyse afin que le RSSI dispose d'une vue de la surface d'attaque complète, avant de redescendre sur chaque périmètre à optimiser,* » rapporte Bernard Montel.

Il ajoute qu'une bonne communication entre les outils d'administration reste déterminante. En effet, la première tâche de nombreux malwares consiste à accéder à l'annuaire partagé de l'entreprise afin de le compromettre. C'est pourquoi Tenable analyse en temps réel les problèmes de configuration sur tous les objets de l'AD (Active Directory) afin de remonter la moindre anomalie dans un SOC (Security Operation Center). ■

VEEAM prône l'immuabilité des données et la bande pour vaincre le ransomware

Adapter les bonnes pratiques de sauvegarde 3-2-1 permet de contrer les cyberattaques du moment. Veeam prône une variante avec une copie hors ligne, immuable, aérienne et vérifiée.

La méthode 3-2-1 devrait parler à tous les administrateurs de sauvegardes informatiques. Elle prône 3 copies des données sur 2 supports différents avec 1 copie hors site, dans le cloud par exemple. L'éditeur Veeam conseille une copie hors ligne, en mode air-gapped ou immuable et recommande la vérification préalable de la restauration SureBackup pour garantir l'absence d'erreur. Deux adjonctions essentielles aujourd'hui pour contrer les ransomwares.

« Les équipes informatiques ne vivent pas très bien les jours suivants une cyberattaque par ransomware, souvent déclenchée en fin de semaine. Pour y faire face, il faut un vrai travail d'équipe et mobiliser les bonnes personnes pour rétablir les services. Les notions d'immuabilité et d'air-gap redonnent confiance, en particulier au moment de restaurer les données. En pratique, c'est souvent une sauvegarde sur bande magnétique qui sauve l'entreprise, » témoigne Yoann Castillo, Team Lead, Systems Engineering France et l'Afrique francophone chez l'éditeur Veeam.

Une cellule de confiance à instaurer

Suivre cette méthode n'impose pas d'investir dans de nouveaux supports de sauvegarde. En revanche, une organisation rigoureuse et des procédures bien documentées s'avèrent indispensables. *« Il faut préparer une cellule de crise pour rétablir les services après une cyberattaque. Nous sommes un maillon de cette chaîne seulement, mais un maillon vital pour récupérer des workloads et des données non corrompues, »* précise-t-il.

Au moment où les applications cloud-natives et les containers sont fréquemment ciblés par les attaquants, la solution Backup & Replication de Veeam interdit la suppression de données de son référentiel de sauvegarde en les rendant temporairement immuables.

« Une protection globale devient nécessaire. Avec les plateformes cloud et les applications SaaS, de nouvelles façons de consommer les données sont apparues. La data voyage entre plusieurs infrastructures. Du coup, la visibilité de l'état des sauvegardes compte plus que jamais pour restaurer les données et les charges applicatives, le jour j. »

L'éditeur Veeam est réputé pour protéger les environnements virtualisés et les micro-services, des workloads maintenant critiques pour de multiples entreprises. Les dernières fonctionnalités de Backup & Replication v12 procurent plus de visibilité et une gestion avancée des sauvegardes. L'authentification des utilisateurs est renforcée, via plusieurs facteurs (MFA).

Tandis que des comportements imprévus se manifestent lors des restaurations ou du redémarrage d'un serveur, et peuvent empêcher la restauration de se dérouler comme prévu, Veeam améliore la résilience du système d'information en assurant la récupération possible de données saines après une attaque par ransomware. ■

WATCHGUARD ET AVA6 unis pour réduire l'exposition aux vulnérabilités

Combinant les analyses automatiques et humaines, la solution EDR de WatchGuard managée par Ava6 procure une réactivité optimale, une réponse adaptée à chaque contexte et organisation.

« *Il existe un fossé colossal entre l'anti-malware et l'EDR (Endpoint Detection and Response) qui offre un niveau de protection supérieure avec des réponses automatisées. Avec l'EDR managé, le fossé est encore plus important car aux fonctionnalités de blocage de l'outil s'ajoutent la connaissance des infrastructures, celle des applications et celle des métiers du client, sans oublier l'expertise des threat hunters* », affirme Pascal Le Digol, Country Manager France chez WatchGuard Technologies.

En dépit de ses algorithmes d'IA et de ses facultés d'apprentissage, le logiciel EDR n'offre pas de réponse universelle. Si personne ne vérifie les comportements signalés suspects, l'attaquant sera ralenti mais aucune solution ne l'empêchera d'identifier un autre angle d'attaque grâce auquel il réussira peut-être à parvenir à ses fins.

Des threat hunters en soutien

Associé à l'équipe de threat hunters de l'intégrateur Ava6, l'EDR WatchGuard devient un service managé qui compense les effectifs réduits de l'entreprise pour contrer les cyberattaques. Sur une centaine de salariés, Ava6 mobilise une douzaine d'experts à la surveillance continue des infrastructures de ses clients. « *Nous analysons en profondeur les alertes en 24/7, 365 jours par an, pour comprendre jusqu'où l'attaque est parvenue, contenir sa progression, et éviter toute nouvelle occurrence,* » précise Sylvain Gouillat, le DG d'Ava6.

La proximité entre l'équipe qui gère la solution EDR et l'équipe informatique du client reste essentielle : « *Il faut une compréhension fine des métiers et des impacts en cas d'interruption de services. Conduire une réponse adaptée dépend d'un accord avec la direction de l'entreprise et avec le RSSI,* » poursuit-il.

Chaque attaque est contextualisée

WatchGuard et son partenaire recommandent la surface de protection la plus large possible autour d'un seul EDR pour tous les segments de réseau. « *Pour être efficace, l'IA doit analyser de nombreux événements en temps réel. Moins on a de zones d'ombre, plus l'EDR sera pertinent. Les analyses en profondeur et la corrélation d'alertes menées par l'équipe d'experts Ava6 fournissent une vision très fine de ce qui se passe sur l'infrastructure,* » souligne Pascal Le Digol. Cette surveillance continue soutenue par l'œil humain permet un engagement de réponse en 15 minutes, avec un plan d'action adapté à la sévérité de l'attaque. Un rapport détaille précisément ce que l'équipe d'experts a observé, comment elle a réagi pour endiguer la menace, et comment l'entreprise pourrait dorénavant réduire sa surface d'exposition aux vulnérabilités. « *Les meilleures réponses à une attaque cyber sont des méthodes plutôt que de nouveaux outils. On peut souvent renforcer la sécurité de son S.I. sans proposer une armada de solutions onéreuses,* » conclut Sylvain Gouillat. ■

Silicon DAY DATA

COMMENT DÉVELOPPER UNE APPROCHE DATA DRIVEN ?

20 OCTOBRE 2022

Retour sur les prises de paroles des partenaires

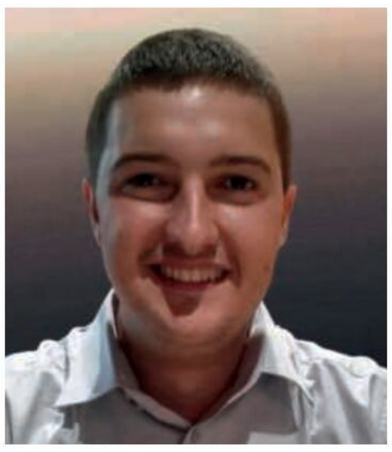
En partenariat avec

boomi · COMMVAULT · Fivetran · NetApp · opendatasoft · Quantum · rubrik · scasicomp · Stordata · vmware

La plateforme iPaaS de Boomi consolide les donées

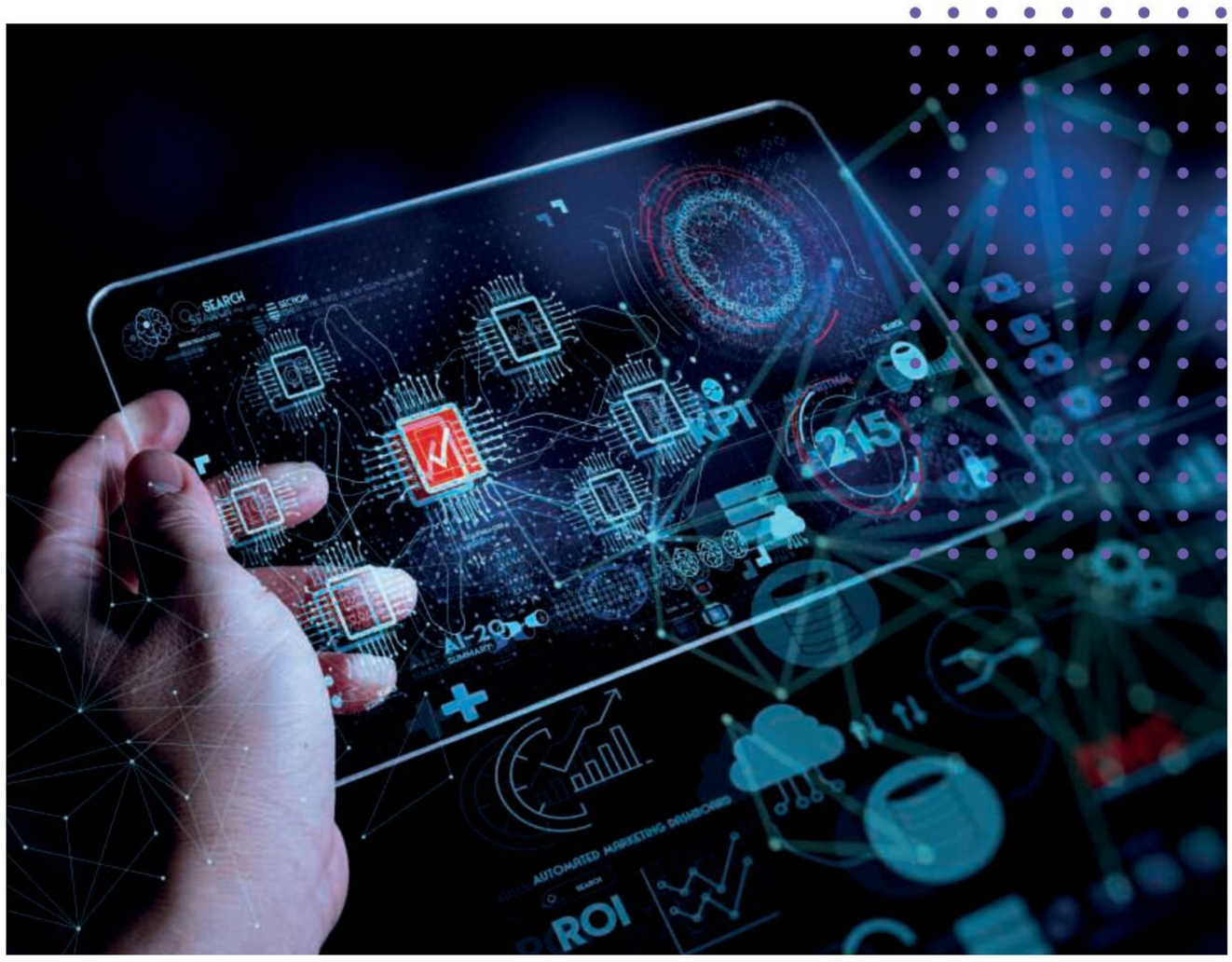
A l'instar du groupement Les Mousquetaires, plus de 20 000 clients dans le monde font confiance à Boomi pour synchroniser leurs données et améliorer ainsi leurs résultats commerciaux.

« *De plus en plus d'applications historiques installées sur site cohabitent avec d'autres applications SaaS, nécessitant d'héberger de vastes volumes de données sur plusieurs infrastructures. Ces solutions doivent communiquer entre eux pour que les utilisateurs puissent travailler de façon efficace. La synchronisation des données devient cruciale et elle doit être orchestrée avec soin,* » recommande Arnaud François, Ingénieur Avant-Vente chez Boomi.



Arnaud FRANCOIS
Solution Engineer,
EMEA Presales team

Pour l'utilisateur, la gestion de plusieurs formats de fichiers distincts et plusieurs bases de données hétérogènes devrait rester transparente. Mais, en pratique, les adaptations techniques s'avèrent nombreuses et chronophages car chaque application dispose de sa propre architecture. Les flux de synchronisation conçus en interne restent souvent incomplets, et peu flexibles. Or, il en va de la qualité des données : certaines analyses se basant sur ces dernières, guidant de plus en plus les décisions quotidiennes des décideurs et le pilotage de l'entreprise.



L'enseigne Les Mousequetaires gagne en réactivité

Le groupement Les Mousquetaires a cassé ses silos de données dans un environnement hybride et multicloud grâce à la plateforme iPaaS, précieuse pour accélérer ses projets ERP. Les données de l'enseigne transitent, de façon continue, des magasins aux sites de commerce en ligne, avec une synchronisation instantanée entre les canaux de vente. Finies les extractions périodiques de données suivies de traitements par lots qui ne convenaient plus aux attentes de réactivité des managers et des clients.

La plateforme iPaaS de Boomi facilite la transition des applications et de leurs données. « *Il s'agit d'une plateforme d'intégration proposée en tant que service. Elle propose un mode de fonctionnement agnostique par rapport au lieu d'exécution des applications, simple et rapide à implémenter, conçue pour les utilisateurs métiers,* » assure Arnaud François.

Composée de modules fonctionnels prêts à assembler, la plateforme Low Code n'exige pas de compétences spécifiques en développement. Une bibliothèque de connecteurs natifs facilite la connexion aux principales applications du marché (NetSuite, Salesforce, SAP, Workday, etc.). Ses principaux modules aident à aller chercher l'information à la source, à l'enrichir ou à la filtrer, puis à pousser les résultats vers leur destination.

Parmi les bénéfices de la plateforme iPaaS, « *sa mise en production rapide procure, en moyenne, un retour sur investissement de l'ordre de six mois. Elle répond aux évolutions techniques de l'entreprise, aux migrations vers les solutions SaaS, et aux besoins de synchronisation avec les applications historiques. Elle propose un tableau de bord unifié, centralisé et transparent sur un périmètre qui peut évoluer, quels que soient les prochains choix de solutions IT de l'entreprise,* » conclut-il. ■

boomi

Pas de gouvernance
sans connaissance fine des données

L'éditeur Commvault et son partenaire intégrateur Stordata guident un nombre croissant d'entreprises vers un stockage dynamique et une gouvernance des données numériques.

« *Connaissez-vous l'empreinte de vos données numériques en termes de valorisation, d'efficacité du stockage et de suivi des risques ? La plupart des entreprises reconnaissent avoir de vastes zones d'ombres dans un à plusieurs domaines, avant même d'aborder l'empreinte carbone,* » signale Bruno Gauthier, ingénieur avant-vente Commvault, éditeur spécialisé en gestion et protection des données.

La gestion des données numériques comporte plusieurs volets, au même titre que la gestion des risques recouvre leur protection, le suivi des droits d'accès et la conformité juridique. Commvault aide les organisations à retrouver automatiquement des données à caractère personnel réparties sur plusieurs infrastructures. L'éditeur sait aussi déplacer les fichiers peu utilisés vers des espaces de stockage moins coûteux, via des contrôles HSM associés à son data mover.

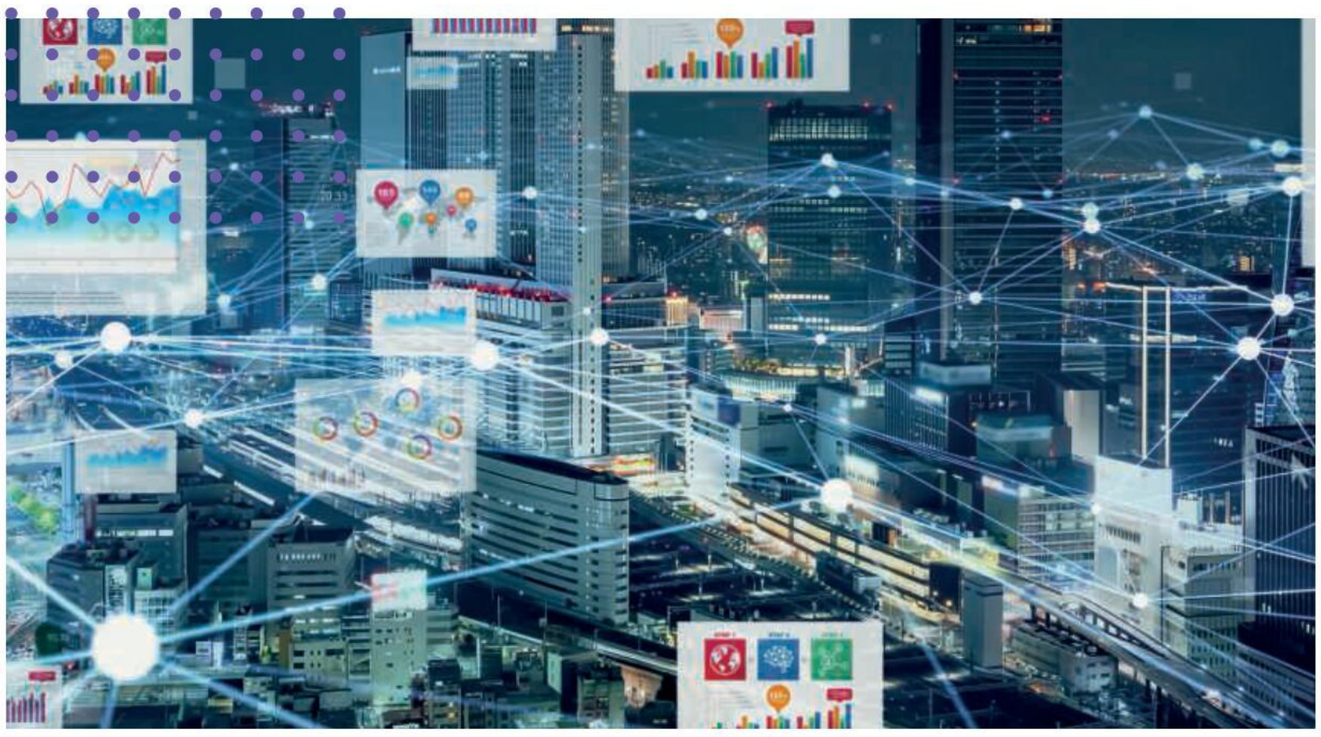
Comprendre ses données s'avère essentiel

Huit données numériques sur dix seraient des dark data, sur un total de 59 Zettaoctets générés en 2022 ; ces données obscures ne sont ni analysées ni même utilisées par les métiers. Elles sont hybrides, résident dans le cloud, sur des espaces de stockages partagés entre les utilisateurs, ainsi que sur les postes de travail.

« *On se retrouve avec un melting pot de données disponibles dans plusieurs environnements de stockage, auquel on souhaite accéder avec nos téléphones portables et nos applications personnelles. Or, de 40 % à 80 % des fichiers n'ont pas de propriétaire assigné, s'avèrent obsolètes ou redondants, évalue le Gartner.* »

Une simple sauvegarde de la messagerie électronique peut déboucher sur un projet plus ambitieux. Un exemple de découverte automatique des données et de la vérification de leur conformité est illustré par Patrick Dufour, Directeur stratégie et alliances partenaires de Stordata : « *Un établissement financier avait besoin d'auditer ses messages électroniques en temps réel. Commvault nous a permis de les stocker, avant même que l'utilisateur en prenne connaissance, sur un espace conçu pour leur analyse. L'entreprise conserve ainsi une trace de tout ce qui se passe.* »

L'intégrateur Stordata assure le bon dimensionnement des infrastructures de stockage, ainsi que le maintien en conditions opérationnelles des solutions de sauvegarde et de pilotage des données numériques. Ses missions dépassent la simple protection des données pour fournir une connaissance fine des données numériques et permettre la prise de décisions en temps réel autour de trois suites complémentaires Data Governance, Discovery & Compliance et File Storage Optimization de Commvault. Ce triptyque assure un soutien précieux au DPO, au RSSI et aux administrateurs du S.I. ■



COMMVAULT

Stordata

MisterTemp' double le taux de placement des intérimaires grâce à Fivetran

Clients, intérimaires, et franchisés MisterTemp' profitent des connecteurs prêts à l'emploi de Fivetran qui facilitent l'accès aux données, même lorsque les schémas de données ou les API changent.

Avec 45 000 travailleurs placés auprès de 10 000 clients, le réseau d'agences d'intérim MisterTemp' génère 310 millions d'euros de chiffre d'affaires. Créé en 2009, il compte 170 agences en franchise en France, plus une dizaine en Italie et trois au Canada. Grâce à la direction Data et à son organisation mise en place fin 2019, la mise en relation gagne en efficacité.
« Les équipes avaient très peu de visibilité sur l'ensemble des données numériques du réseau, il y a trois ans. Il leur était difficile d'avoir une vision macro avec des informations en silos, associées à plusieurs services SaaS, » retrace David Milosevic, Head of Data MisterTemp'.

Dès 2017, l'offre digitalisée est lancée en laboratoire avant de gagner tous les services et les outils mis à la disposition des franchisés. Mais, faute d'outillage efficace et d'équipe dédiée, la valorisation des données les plus récentes atteint trop rarement les clients et les candidats.

Une data stack procure l'agilité requise

La création d'une direction des données apporte un nouveau souffle à l'automne 2019. David Milosevic pilote le nouveau service et compose une architecture autour de la data stack de Fivetran pour disposer d'un endroit unique où manipuler, enrichir et redistribuer la donnée. Il explique : *« Lorsqu'un candidat s'inscrit chez MisterTemp', il confirme un certain nombre de métiers compatibles avec son expérience. Le rapprochement avec les besoins exprimés par les clients et prospects enregistrés dans le CRM Salesforce doit s'effectuer rapidement. Reste à envoyer une série de messages personnalisés, avec les détails du candidat, invitant les destinataires à vérifier ce profil. Après plusieurs itérations, nous avons réussi à doubler le taux de placement des intérimaires. »*

Tant au niveau du choix des outils que du choix des profils de ses propres collaborateurs, David Milosevic voulait se concentrer sur l'apport de valeur, plutôt que sur la mise en place, la maintenance et l'évolution de la solution technique. A présent, sur les cinq personnes de l'équipe data, 3,5 ETP (équivalents temps plein) soutiennent les métiers avec des rapports d'analyse tandis que 1,5 ETP s'attelle aux tâches sous-jacentes d'ingénierie des données.

Trois outils principaux composent la suite analytique retenue par MisterTemp' : Fivetran assure l'intégration automatisée des données avec plus de 40 formats sources reconnus, facilite leur transformation, et leur consolidation au sein du datawarehouse Snowflake où elles sont analysées. La phase de visualisation des résultats d'analyse s'appuie sur l'outil de Business Intelligence Looker. Deux briques logicielles ont apporté leurs fonctions complémentaires récemment ; il s'agit de Dbt pour la transformation de données et Atlan pour le catalogue de données. ■

Fivetran

Opendatasoft : l'organisation data-driven partage des compétences spécifiques

En 10 ans, la plateforme Opendatasoft s'est glissée au cœur de plus de 3 000 projets data à travers le monde et référence plus de 28 000 datasets publics. Avec des gains d'efficacité opérationnelle et de nouveaux revenus générés en écosystème pour plus de 500 clients dans 25 pays.

« *Les entreprises data-driven ont une longueur d'avance. Elles sont 8,5 fois plus susceptibles d'enregistrer une croissance annuelle d'au moins 20 %, évalue précisément le cabinet d'études Forrester Research. C'est la preuve qu'il existe bien une corrélation directe entre l'exploitation des données dans tous les compartiments de l'organisation et la croissance de l'entreprise,* » démontre Jean-Marc Lazard, co-fondateur et Président d'Opendatasoft, l'éditeur français d'une plateforme de partage d'expériences autour des données.

À présent, huit décideurs sur dix estiment que la donnée est une ressource stratégique de l'organisation, susceptible d'améliorer l'efficacité opérationnelle. Pourtant, une société sur deux seulement est engagée dans une démarche de transformation via la data, révèle une autre étude récente d'Opendatasoft et l'Usine Digitale. Pour vérifier les étapes du pèlerinage numérique restant à franchir, Jean-Marc Lazard recommande de sonder chacun des collaborateurs et des partenaires de l'entreprise sur son autonomie réelle vis-à-vis des données : peut-il toujours y accéder sans effort ? En chemin, on rencontre souvent trois principaux obstacles : les solutions de data management accessibles à quelques experts seulement dans les organisations, des projets data longs et difficiles à déployer, et sous l'angle de l'acculturation, des services métiers qui ont une connaissance très limitée du stock de données réellement disponible.

Trois axes de travail pour devenir data-driven

Que l'on prenne le projet sous l'angle de la culture, de la gouvernance ou des technologies de la donnée, il s'agit souvent de rassembler dans un même endroit les data de l'organisation et de son environnement, comme on rassemble des actualités derrière un intranet ou un extranet.

Par exemple, grâce à la plateforme Opendatasoft, Schneider Electric a d'abord bâti sa data library comme un self-service interne, avant de créer une place de marché Data as a Service destinée aux partenaires technologiques. Ces derniers peuvent ainsi comparer, de façon anonyme, les consommations d'énergie de points de vente concurrents afin d'optimiser leurs installations.

« *Notre plateforme aide à mettre en place un portail de data, à se connecter sur les fabriques de données, à les mettre en perspective pour chaque métier et à industrialiser des tableaux de bord de pilotage élaborés autour de ces data. Comme on se passe la balle dans un sport d'équipe, on doit pouvoir se passer la donnée dans l'entreprise. Nos clients les plus avancés dans l'implémentation d'une stratégie data-driven, notent que leurs collaborateurs deviennent eux-mêmes contributeurs,* » observe le président d'Opendatasoft, avant de présenter le cas d'usage concret de Schneider Electric.. ■

opendatasoft

Quantum combine l'immuabilité de la bande avec le stockage objet multisite

En fonction des accès et du volume de données à sauvegarder, Quantum oriente ses clients vers ses librairies de bandes et/ou vers une architecture de stockage objet répartie sur plusieurs sites.

« *Nos clients et prospects veulent protéger leur IT contre les cyberattaques, dont les ransomwares. Ils veulent gérer aussi de grands volumes de données à moindre coût. Il n'existe pas de solution miracle, mais de bonnes pratiques à mettre en place au moyen de plusieurs outils,* » souligne Stéphane Cardot, Directeur avant-ventes de Quantum EMEA.

Le groupe breton de travaux publics Le Du, quelques mois après avoir refondu son ERP, souhaitait pouvoir redémarrer rapidement en cas d'attaque, avec des données saines, non chiffrées. Il a retenu un partenaire local de Quantum pour renouveler son architecture de sauvegarde, en suivant les recommandations de la CNIL pour garantir l'immuabilité des données numériques. « *Nous avons mis en place des périphériques intelligents protégeant les données sauvegardées. Au-delà des sauvegardes effectuées sur disques, une rétention longue s'appuie sur une librairie de bandes magnétiques Quantum capable de déplacer la bande vers une partition invisible du logiciel de sauvegarde. Le hacker prenant le contrôle de l'outil de sauvegarde ne verra pas ces données et ne pourra donc pas les chiffrer,* » explique-t-il.

Une bonne pratique consiste à entraîner les équipes IT à la restauration depuis cette librairie, pour qu'elles maîtrisent le processus en cas d'attaque et qu'elles puissent assurer la continuité des activités informatiques.

300 à 600 Peta-octets à stocker et protéger

De nombreuses entreprises génèrent de grandes quantités d'informations non structurées qu'elles doivent protéger sans multiplier les copies. Ainsi, l'institut européen de biotechnologies EBI et Genomic England mènent-elles de nombreuses simulations autour du génome humain, outre-Manche. Confrontées à une volumétrie croissante, elles devaient s'affranchir de la limite de capacité de baies NAS. Quantum les aide à protéger 300 à 600 Po de données actives, autour d'un stockage objet, une solution flexible et évolutive, incluant une administration simple, tout le stockage restant visible au travers d'un même espace de nom.

« *Nous avons mis en place un référentiel objet, un datalake et des clusters répartis sur trois sites, pour que tous les contenus soient toujours accessibles. Notre mécanisme d'Erasure Coding (codage par effacement) protège des pannes de disque par répartition de segments. L'intérêt est aussi économique, avec 70 % de gains par rapport à une réplication classique,* » détaille Stéphane Cardot. Lorsque l'archivage de données froides sur un cloud public n'est pas envisageable, pour des raisons de souveraineté, l'organisation doit créer son propre service de rétention longue, pour 5 ans, 10 ans et au-delà. Quantum suggère alors la combinaison du stockage objet en frontal associé à une librairie de bandes pour conserver la donnée à moindre coût, en mode cloud privé. ■

Quantum

silicon

Cyber resilience : Scasicomp donne aux entreprises les clés de la sécurité de leurs données avec NetApp et Rubrik.

Comment minimiser l'impact d'un ransomware et poursuivre ses activités numériques au plus vite ? Scasicomp fait équipe avec les DSI grâce à ses services d'accompagnement B-Zen, bâtis sur des solutions NetApp et Rubrik.

Le cabinet Deloitte a sondé les entreprises ayant subi des cyberattaques pour distinguer les coûts directs et indirects auxquels elles sont confrontées. Pas moins de 14 facteurs sont à prendre en compte, des violations de données à caractère personnel, à la dévalorisation financière de la marque, en passant par la perte de propriété intellectuelle ou l'augmentation du coût des assurances.

« Outre l'arrêt de production informatique, une communication trop tardive, supérieure à 72 heures, au sujet des données à caractère personnel exposées peut coûter jusqu'à 4 % du chiffre d'affaires annuel, depuis la mise en place du RGPD (Règlement Général sur la Protection des Données), » rappelle Benjamin Durand, CTO & Alliance Manager Scasicomp.

Architecte et intégrateur en infrastructures cloud, Scasicomp a combiné les solutions complémentaires de NetApp et de Rubrik pour tirer la quintessence d'une résilience des données optimale. *« En cas de cyberattaque, l'entreprise a très peu de temps. Elle doit se concentrer sur la valeur des données ciblées. L'offre B-Zen de Scasicomp prend la main sur les environnements distants, de façon à les exploiter. Avec une équipe de soutien en France, toutes les remontées d'alertes sont analysées en 24/7, afin de traiter à temps les informations cruciales, »* décrit-il.

Dans cette alliance technologique, Rubrik s'engage sur le fait que les données ne seront pas compromises, et que les métiers pourront les utiliser en cas d'attaque. Jean Lafargue, Sales Engineering Manager, de Rubrik France précise : *« La finalité consiste à gérer la remédiation de manière orchestrée pour relancer les services rapidement. Cela passe par trois étapes pour assurer que seules des données saines seront remises en production : la détection d'anomalies d'usage, la recherche de données sensibles qui auraient pu être exposées (bancaires, de santé, à caractère personnel) et la recherche d'indices de compromission. »*

Côté NetApp, l'approche zéro trust consiste également à ne faire confiance à personne, pas même à l'administrateur qui n'acquiert jamais tous les droits sur toutes les données : *« Le mal peut venir de l'intérieur comme de l'extérieur. Nos solutions à base d'IA identifient et bloquent les cyberattaques. Nous nous assurons que les données sauvegardées et externalisées soient saines, non corrompues et non exposées à tous les vents »* explique Guillaume Sowinski, Partner Technical Lead de NetApp.

« Notre technologie de snapshot a fait ses preuves depuis trois décennies. Elle est mise en lumière à présent comme le premier rempart pour pouvoir restaurer les données après une cyberattaque, avec un point de restauration en local ou à distance, » conclut-il.

En plus de la protection des données contre les menaces croissantes, la gouvernance des données passera enfin par la prise en compte des contraintes règlementaires pour éviter d'avoir à régler des amendes qui seraient subies comme une double peine en passant de victime à coupable. ■

Olivier Bouzereau.

Pour VMware, moderniser la pile de données passe par l'open source

Renforcée par Pivotal début 2020, VMware modernise les piles de données d'entreprise autour du SGBD PostgreSQL et de Greenplum pour l'analytique, l'apprentissage automatique et l'IA. .

« *L'entreprise doit fournir à ses utilisateurs des dizaines de services distincts, opérés en cloud privé et dans un ou plusieurs clouds publics. L'enjeu pour l'IT consiste à proposer le même modèle opérationnel quel que soit le service et le cloud. Il s'agit d'offrir partout les bons engagements de disponibilité et de performances, avec des volumes croissants de données et des contraintes de sécurité et de respect de la vie privée,* » résume Franck Sidi, Directeur Data de VMware Tanzu.

Pour faire face à ces enjeux, les technologies open source viennent s'immiscer au cœur des infrastructures de données, orientant la stratégie IT pour plusieurs raisons : « *la première raison est l'accès à l'innovation et aux nouvelles technologies, la deuxième concerne la baisse des coûts IT et la troisième raison est la modernisation de la stack logicielle complète,* » précise-t-il en s'appuyant sur une étude Open Logic récente, menée auprès de 2 500 responsables informatiques.

Clusters de données à la demande

VMware propose avec PostgreSQL un système de gestion de bases de données relationnel et objet, complété de services de caching, de messaging, de streaming et, avec Greenplum, l'analyse de données massives indépendante du matériel.

« *Des clients français tel qu'un institut national, une mutuelle ou un assureur ont retenu Greenplum pour combiner les fonctions d'un datawarehouse et celles d'un datalake,* » illustre Franck Sidi.

La stratégie multicloud de VMware se concrétise avec la distribution d'applications et de grands volumes de données répartis sur une combinaison de clouds privés et publics. Avec l'offre DBaaS (Database as a Service), les clouds publics ont simplifié la façon de consommer des services de données. L'offre DMS, développée par l'équipe du projet VSAN de VMware, cherche à offrir la même simplicité d'utilisation du cloud public au niveau du cloud privé et en cloud hybride. « *Nous avons commencé avec MySQL et PostgreSQL, d'autres services suivront dans le cadre du projet ambitieux de VMware dénommé Moneta. Notre approche consiste à automatiser complètement l'ensemble des tâches, de la mise à disposition du service jusqu'aux sauvegardes, en passant par l'application des mises à jour,* » révèle-t-il.

VMware et de son écosystème combinent leur valeur ajoutée durant les phases d'analyse, d'architecture, et d'accompagnement. « *Le principal avantage d'une solution open source comme Greenplum est de pouvoir passer librement à la version commerciale, et vice-versa, de revenir à la version communautaire sans impact, en évitant toute nouvelle forme de verrouillage au client. Cheops, l'un de nos partenaires français, est ainsi en mesure d'automatiser la migration complète des bases de données et des codes applicatifs associés en Java, Windev ou Powerbuilder.* » ■

vmware®

silicon

Faciliter la migration **DES APPLICATIONS CRITIQUES**

La migration vers le cloud est devenue un enjeu essentiel pour les entreprises. À fortiori lorsque les applications sont critiques. Pour faciliter cet accès au “nuage”, Cloud XPR de Jaguar Network mise avant tout sur la sécurité et la confiance.

Les besoins en cloud sont en pleine essor, les entreprises souhaitent rattraper leur retard. *« Pour 2/3 d'entre elles, la migration vers le cloud est une priorité absolue. Or, on s'aperçoit que pour 80% leurs applications critiques n'ont pas été portées dans le cloud. Par ailleurs, elles doivent faire face à de nombreux défis : conformité aux contraintes réglementaires, transparence tarifaire, sécurité des systèmes, complexité d'intégration, manque de compétences internes, souveraineté des données, disponibilité… »*, souligne Laurent Cheyssial, CTO Jaguar Network filiale B2B du Groupe iliad. Des solutions existent pour aider les entreprises à migrer leurs applications critiques dans le cloud. À commencer par Cloud XPR.

Démocratiser la migration vers le cloud

Sécurité et confiance sont souvent les maîtres mots pour un passage à l'acte. Idem dans l'univers cloud ! *« Nous voulons démocratiser l'accès à une connectivité sécurisée et des services cloud de confiance pour toutes les entreprises. Avec Cloud XPR, nous avons conçu une offre clé en mains pour rendre accessible aux entreprises la migration et l'exploitation des applications critiques dans le cloud (applications métiers, techniques ou transverses) »*. Cette offre est le fruit de trois années de co-innovation avec les clients de Jaguar Network. Elle réunit toutes les ressources indispensables pour accompagner les DSI dans la mise en œuvre de leurs environnements dans le cloud et leur sécurisation (sauvegarde des données, immutabilité des données pour lutter contre les rançongiciels. *« Nous l'avons souhaitée non seulement simple à déployer, à superviser tout en étant bien positionnée sur le plan tarifaire. Nos coûts sont prédictibles et la facturation se fait à l'unité. Ces coûts incluent le service, le support ainsi que le trafic entre datacenters »*.

Laurent Cheyssial
CTO Jaguar Network

Les atouts de la solution Cloud XPR

En appuyant son socle technologique sur VMware, l'hébergeur garantit une réponse aux besoins de sauvegarde et de traitement de données sensibles. *« Nous avons articulé l'offre autour de cinq services : la puissance de calcul, le stockage, le réseau, la sécurité et l'exploitation »*.

En outre, les données sont hébergées dans des datacenters certifiés HDS (hébergement Données de Santé) et ISO 27001, situés en France. Ce qui permet à Jaguar Network un accompagnement pragmatique de ses clients vers la souveraineté. Mieux, une géoredondance des données est possible dans des régions distantes et l'hébergeur se distingue par une mise en place de Plan de Continuité d'Activité et de Plan de Reprise d'Activité automatisés directement au travers de son portail. Sans oublier l'expertise des équipes, *« Avec un support technique qui fonctionne en 24/7, 365 jours par an, nous garantissons un temps d'intervention de 10 minutes, avec un suivi opérationnel via des responsables de comptes dédiés ainsi qu'un SOC (détection des cybermenaces, gestion des vulnérabilités, audits et tests d'intrusion) »*, conclut Laurent Cheyssial, CTO Jaguar Network. ■

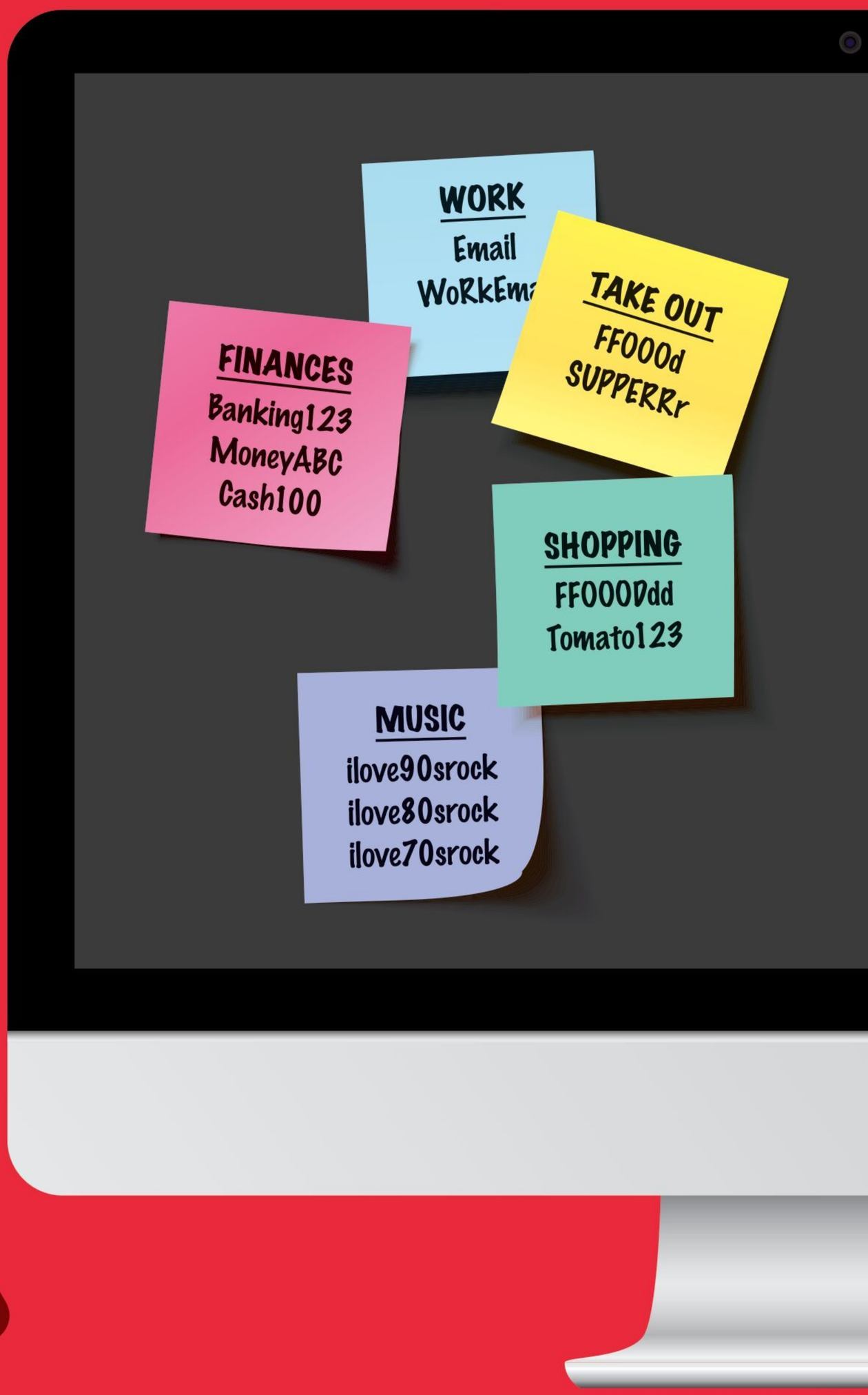
Jaguar network

LastPass •••|

Il existe une meilleure façon de gérer les mots de passe de votre organisation.

#BeCyberSmart

Plus de vigilance. Plus de
#CyberIntelligence.



Un tour d'essai ?

LastPass.com