Business
Magazine

U & US

By Telindus

Paypal
At the crossroads of convenience and security

Palo Alto - John Kindervag
The Art of Healthy Skepticism

Microsoft - Neobanks
Leveraging the Cloud to change the Game

More inside

#10

SPECIAL ISSUE

FINTEXPLORATION 2020

HOW COMPANIES CREATE NEW OPPORTUNITIES & USAGE THROUGH DIGITALIZATION?

U&US #10

Dear friends, customers and partners,

Technology changes our reality profoundly. Used separately, IoT, AI, blockchain or cloud, (...) have the potential to change the way we do business. But when used jointly, they become truly transformational. Imagine how these technologies could change your customers', suppliers', employees' and business partners' experience.

This U&US magazine's special edition is dedicated to our annual FinteXploration innovation event. As the Covid-19 situation forced us to postpone our 2020 immersive tour in San Francisco, I thus invite you to travel with us along the magazine pages to the cradle of innovation: Silicon Valley. Take a look at this year's agenda and discover the next-generation of digital solutions that will reshape our economy and see how innovative companies are creating opportunities through digitalization.

Join us to keep up with the rapid innovation and disruption happening across all industries and discover how to leverage them to drive your business innovation.

Enjoy the reading!

GÉRARD HOFFMANN
CEO, Proximus Luxembourg

SOMMAIRE

U&US #10

PROXIMUS LUXEMBOURG S.A.
18, rue du Puits Romain
Z.A. Bourmicht 8070 Bertrange
Tél :+352 450 915-1

GESTION ÉDITORIALE
Michaël Renotte

CONCEPTION GRAPHIQUE
Deuux

POUR ÉCRIRE À LA RÉDACTION
marketing@telindus.lu

@ telindustelecom
/Telindus-luxembourg
/Telindus_lu

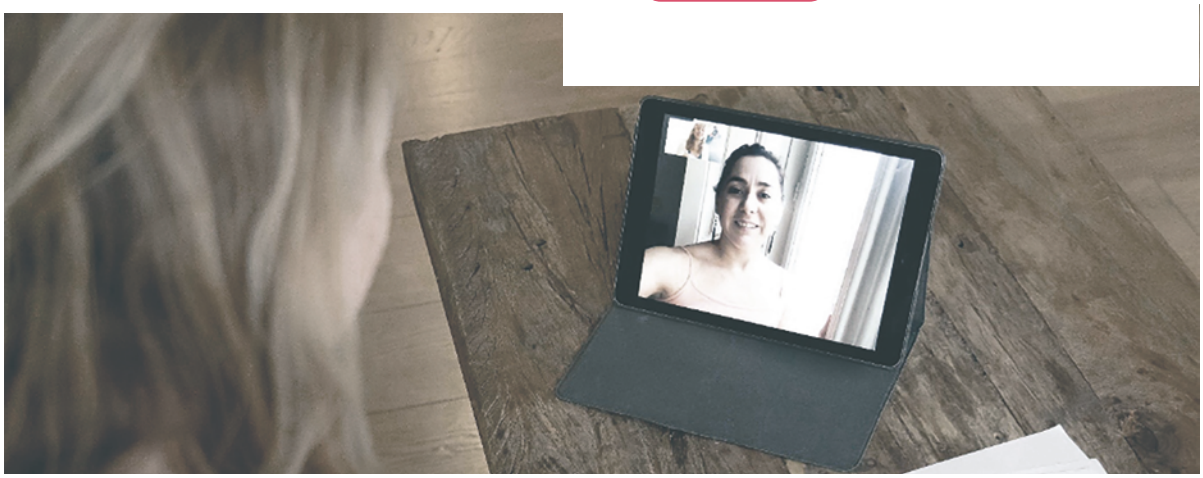
À LA UNE

Time to work together

Dans le cadre de la pandémie qui touche la quasi-totalité du globe, les entreprises et organisations tentent d'assurer la continuité de leurs activités. Un environnement de travail numérique qui aide les salariés à collaborer à distance peut faire une différence de taille.

Afin de répondre aux entreprises cherchant des solutions simples et sécurisées pour accompagner le télétravail de leurs collaborateurs, nous avons regroupé certaines de nos solutions sur cette page web :

DÉCOUVRIR



FINTEX-PLORATION

A BRIDGE BETWEEN LUXEMBOURG & SILICON VALLEY

Through numerous years of collaboration with Silicon Valley enterprises, Telindus has built a sound network of innovation leaders, inspiring technologists, and industry experts. We leverage these connections to bring our clients in Luxembourg the transformative power of innovation.

For us, "Silicon Valley" stands for a uniquely ambitious, easy-going spirit, unlimited possibilities and world-changing technologies. We understand that Silicon Valley attracts ideas, talent and capital like no other region in the world and determines technological development worldwide.

A few years ago, we came up with the idea of sharing these privileged relationships with our customers and partners.

We then realized there would be value in inviting our clients to visit the places where our future is designed, learn what makes Silicon Valley companies unique, how we can get inspired by the Valley's go-getting mentality and combine it with our own strengths. After all, if Silicon Valley is a leading location for the tech industry, Luxembourg is for sure one of the world's most successful financial centres!

This is how we gave birth to FinteXploration, a five-day immersion into Silicon Valley and San Francisco Bay ecosystem. There, we seek to create a bridge between Luxembourg CXOs and technologists, entrepreneurs, managers, startupers, and researchers from this region of the world regarded as the cradle of innovation.

Since 2017, FinteXploration has given participants a shortcut to the opportunities and benefits of emerging industry trends. The program brings executives into contact with corporations and start-ups leading disruptive innovation, allowing them to see how their own enterprise's practices and processes need to change if they are to compete and grow over the long-term.

Over the recent years, FinteXploration has offered participants the opportunity to visit world-class companies such as Apple, Cisco, Darktrace, Facebook, Google, Hewlett Packard Enterprise, Microsoft, Oracle, PayPal, Stanford University, Symantec, not forgetting Plug&Play, one of the largest start-up incubators in the world.

Visitors were presented with technology trends being developed in Silicon Valley that will surely impact their businesses and industries in the near future, including Blockchain, IoT, Digital Networks, Big Data, Mobile Identity Management, Biometrics, Hybrid IT, Cloud Intelligence, Open Banking, Zero Trust networking, with a special focus on Artificial Intelligence applied to Financial Services, an industry that can expect to benefit particularly from this promising technology.

FinteXploration is above all an immersive journey that allows our clients and partners to get closer than ever before to the world's most disruptive enterprises, an inspirational experience punctuated with numerous interaction opportunities with Silicon Valley professionals with whom they can discuss future projects, which is certainly one of the best ways to boost even the most ambitious digital transformation agenda.

Silicon Valley in a few figures

- **2.6** million people live in the Silicon Valley, and 39% of them are aged between **20** and **40**
- Silicon Valley is home to approximately **11,500** high-tech companies that employ **420,000** people and generate around $ **100 billion** in sales
- Every week, **11** new companies are created in Silicon Valley
- If Silicon Valley were to be an indepedent territory, it would be the **12**th economic power in the world
- **160** venture capital companies are located in the Valley region
- More than **15**% of United States patents are filed by companies, universities or laboratories located in Silicon Valley.

Source: frenchdistrict.com

LES TECHNOLOGIES EMERGENTES FACE AU COVID-19

UNE OPPORTUNITÉ DE CROISSANCE?

Cette année, l'épidémie mondiale de coronavirus nous a contraints à annuler notre voyage de découverte des entreprises les plus innovantes de la Silicon Valley, FinteXploration. Parmi les technologies émergentes dont nous comptions explorer le potentiel, certaines ont été mises à contribution pour aider les soignants, les gouvernements et les citoyens à faire face à l'impact de la pandémie. Pour ces technologies, la pandémie est une extraordinaire mise à l'épreuve du fait des conditions les plus difficiles qu'il nous ait été donné de vivre depuis plusieurs décennies. Et certaines d'entre elles pourraient sortir de la crise avec des niveaux de maturité et des taux d'adoption bien supérieurs à ce qu'ils étaient il y a quelques mois encore.

En dépit de la situation, la 3D fait bonne impression

Produisant valves de ventilateur, filtres respiratoires, kits de test ou fermoirs pour masques faciaux, les industriels et les FabLabs du monde entier ont mobilisé leurs systèmes d'impression 3D pour compenser les déficits d'approvisionnement liés à la pandémie de Covid-19. Certains ont également pris l'initiative de créer des produits entièrement nouveaux, comme des adaptateurs en plastique qui permettent d'ouvrir une porte avec le coude et de limiter ainsi la propagation du virus. Réagissant à la l'appel de la Commission européenne à mettre en œuvre des modes alternatifs de production d'équipements, l'Association Européenne des Industries de la Machine-Outil – ce qui inclut l'impression 3D - a incité ses membres à produire les équipements qui font défaut aux hôpitaux européens en raison de la crise sanitaire. Parallèlement, les initiatives d'impression d'équipements médicaux en 3D se sont multipliées.

> “ La crise sanitaire changera radicalement la donne pour l'impression 3D et stimulera son adoption dans de nombreux secteurs

Mais au-delà, l'impression 3D présente également un fort potentiel d'adoption *"post-pandémique"* à travers de nouveaux scénarios d'utilisation. Des industries majeures, dont le secteur automobile et l'industrie aérospatiale, ont intégré l'impression 3D dans leurs flux de production depuis plusieurs années déjà. Les ruptures dans les chaînes d'approvisionnement provoquées par l'épidémie de coronavirus pourraient cependant conduire ces entreprises à investir plus massivement dans la fabrication additive et amener de nouveaux utilisateurs à adopter l'impression 3D. Au fil de la crise sanitaire, certains fabricants ont également fait le constat qu'imprimer des pièces en 3D permettait de produire des structures plus légères.

Pour Venkata Naveen, spécialiste des technologies de rupture auprès du cabinet GlobalData, l'impression 3D ne devrait pas connaître un fort ralentissement en 2020, malgré la pandémie de Covid-19. Elle fait le constat que *"l'impression 3D est passée du statut de proof-of-concept à celui d'alternative viable aux procédés de fabrication traditionnels, démontrant son potentiel dans des environnements réels, notamment dans les secteurs de l'aérospatiale, de la défense, de la construction et de l'automobile."* Venkata Naveen considère encore que *"la crise sanitaire mondiale de 2020 changera radicalement la donne pour l'impression 3D et stimulera son adoption dans de nombreux secteurs. Le scénario actuellement vécu de chaînes d'approvisionnement fragilisées accélérera le développement d'un écosystème de fabrication numérique dont la technologie d'impression 3D sera le moteur."*

L'avènement de la blockchain ... logistique

Dans des circonstances telles qu'une infection virale pandémique, où un grand nombre de données entrantes sont publiées en temps réel, recourir à la blockchain permet de réduire l'incertitude et de renforcer la confiance. La technologie blockchain autorise en effet la création de plateformes automatisées d'enregistrement et d'échange d'informations factuelles cohérentes entre plusieurs parties. Au-delà de son utilisation en tant qu'outil de surveillance et de suivi des données de santé, la blockchain peut encore aider à relever le défi de l'interopérabilité des soins de santé et à garantir la fiabilité des données des essais cliniques.

En ces temps de crise mondiale, la blockchain présente cependant une opportunité particulière à travers sa capacité à permettre l'automatisation des chaînes logistiques mises à mal par la pandémie. La possibilité de créer des contrats intelligents sécurisés et décentralisés grâce à la blockchain offre aux entreprises un moyen d'automatiser certains de leurs processus sans prendre de risques supplémentaires en matière de sécurité.

Pour Indira Mysore, directrice du Healthcare Community Development au sein de l'Austin Blockchain Collective, *"avec le COVID-19, la Chine s'est révélée être le principal point de défaillance dans les chaînes d'approvisionnement à l'échelle mondiale*". Selon elle, la pandémie obligera les entreprises à repenser leur chaîne logistique et à répartir les risques entre différentes sources d'approvisionnement. Indira Mysore pense que *"la blockchain peut jouer un rôle central dans la mise en place d'un nouveau modèle logistique parce que celui-ci nécessitera une collaboration étroite et un partage de données sans faille entre les partenaires de l'écosystème afin d'être capable de réagir rapidement si une catastrophe similaire se reproduit."*

> “ La blockchain peut jouer un rôle central dans la mise en place d'un nouveau modèle logistique

Marquis Allen, membre associé de la Government Blockchain Association, un organe international de promotion de la technologie blockchain, considère quant à lui que les efforts déployés pour contenir la propagation du Covid-19 a mis en évidence l'inefficacité des processus et des systèmes de traitement des données dans de nombreuses industries. Selon lui, *"les promesses d'efficacité, de transparence, de sécurité et d'immuabilité des transactions portées par la blockchain soulèvent en ce moment beaucoup d'intérêt. La blockchain connaît déjà un grand succès en matière de gestion des chaînes d'approvisionnement dans l'agriculture et l'industrie manufacturière. De nombreux efforts seront prochainement déployés dans d'autres secteurs pour adopter l'innovation que constitue cette technologie."*

Cybersécurité: Le Jour d'après

Une étude réalisée par le cabinet Gartner révèle qu'une fois la crise du Covid-19 surmontée, 48% des employés sont susceptibles de conserver les différentes formes de télétravail adoptées pendant la pandémie. En fait, pas moins de 74% des entreprises interrogées par la firme déclarent avoir l'intention d'étendre le télétravail après la crise sanitaire.

Cette dépendance croissante à la connectivité Internet – le trafic de données a augmenté de 50% sur certains marché - exige d'accorder une importance particulière à l'amélioration des solutions de cybersécurité qui protègent les systèmes et leurs utilisateurs, lesquels sont plus que jamais exposés aux risques d'escroquerie par hameçonnage et autres formes d'attaques par ingénierie sociale.

Depuis le début de la crise, les cyberattaques se sont multipliées dans le monde entier, notamment envers les services de santé qui ont été la cible d'attaques de type ransomware. Zoom, qui est devenu une plateforme de communication incontournable pendant la pandémie, a connu une augmentation considérable de cas de cyberattaques ciblées, surnommées *"Zoombombing"*. L'analyse de données Google a révélé une augmentation de 350% des sites d'hameçonnage depuis le début de la pandémie. La Grande-Bretagne et les États-Unis ont signalé qu'un nombre croissant de cybercriminels et autres groupes malintentionnés exploitent la situation et profitent des mesures de soutien économique pour perpétrer des tentatives d'hameçonnage.

Nous sommes mis au défi de repenser et d'améliorer la résilience de l'infrastructure numérique qui sous-tend notre environnement économique.

Cependant, le Covid-19 n'est pas la seule menace susceptible de déstabiliser rapidement et durablement nos vies personnelles et nos activités professionnelles. Selon le Forum Economique Mondial, la crise actuelle indique clairement que notre monde est beaucoup plus exposé aux impacts des pandémies, des catastrophes environnementales et des cyberattaques que nous ne le pensions. Une cyberattaque qui priverait les entreprises, les services publics et les individus de l'accès à leurs appareils, à leurs données ou à Internet pourrait être dévastatrice.

Le magazine spécialisé Dark Reading y voit cependant une opportunité pour les professionnels et l'industrie de la cybersécurité de tirer des leçons utiles pour l'avenir. *"A la lumière de la crise du coronavirus"*, écrit le capital-risqueur Robert Ackerman, *"les vulnérabilités de l'économie numérique et de la chaîne logistique mondiale nous apparaissent désormais clairement. Nous sommes mis au défi de repenser et d'améliorer la résilience de l'infrastructure numérique qui sous-tend notre environnement économique."*

L'intelligence artificielle sous surveillance

Dans le cadre de la pandémie, l'IA a été mise à contribution de multiples façons, notamment pour détecter des signes d'infection sur base d'images tomodensitométriques et de capteurs de température portables. Des applications d'intelligence artificielle aident à livrer des fournitures médicales par drone, désinfecter les chambres des patients et rechercher dans les bases de données de médicaments des traitements qui pourraient être efficaces contre le coronavirus. Les technologies de l'IA sont aussi exploitées pour découvrir de nouvelles molécules qui pourraient permettre de produire des médicaments ou même pour aider à prédire la structure secondaire de l'ARN du virus.

> “ En Chine, des entreprises déploient des solutions capables de reconnaître les visages malgré le port d'un masque

La reconnaissance faciale, l'une des applications les plus médiatiques de l'IA, offre des avantages indéniables en matière de sécurité, de surveillance et d'identification biométrique. Mais ces mêmes avantages en font également l'une des technologies les plus controversées. En Chine, des entreprises comme Hanwang Technology déploient des solutions capables de reconnaître les visages malgré le port d'un masque. En utilisant des détecteurs de température, des systèmes d'IA peuvent également repérer dans une foule des citoyens ayant une température corporelle supérieure à la normale. Le géant de la technologie Alibaba revendique quant à lui le développement d'un système capable de détecter le coronavirus chez un patient en 20 secondes avec une précision de 96% à partir d'un scanner des poumons!

Mais l'utilisation massive d'outils de suivi et de surveillance basés sur l'IA dans le contexte de la pandémie, combinée à la fragmentation actuelle de la gouvernance éthique en la matière, pourrait ouvrir la voie à une utilisation plus large et plus permanente de ces modes de surveillance. L'Union européenne s'en inquiète et projette d'intégrer cette problématique dans les initiatives législatives en cours afin d'empêcher que l'IA puisse contribuer à la mise en place de nouvelles formes de contrôle social automatisé qui pourraient persister après la fin de l'épidémie.

Les robots, conquérants du post-Covid

Dans le monde entier, des robots sont déployés pour lutter contre la pandémie de coronavirus. Ils désinfectent des hôpitaux, décontaminent des sites publics comme privés, manipulent des déchets biologiques dangereux, livrent de l'alimentation et des médicaments. Certains robots prennent même la température des patients.

Les contraintes liées à la pandémie, comme les mesures de distanciation sociale, offrent par ailleurs aux entreprises spécialisées dans l'automatisation de nouvelles opportunités de développement. Takeoff Technologies a par exemple mis au point des entrepôts miniatures et automatisés dans lesquels des robots préparent des commandes d'épicerie pour que celles-ci puissent être livrées rapidement aux clients. L'entreprise s'attend à ce que l'adoption de l'automatisation s'accélère dans le secteur de la vente au détail suite à la pandémie.

En juin 2020, Takeoff a été qualifié de *"Pionnier Technologique"* par le Forum Economique Mondial.

La robotique appliquée aux soins de santé, qui a fait ses preuves pendant la pandémie, devrait également sortir de la crise du Covid-19 par le haut. Les robots chirurgicaux télécommandés et les robots de téléprésence épaulent déjà utilement les médecins, le personnel médical et les services sanitaires. Knightscope, un producteur de robots de sécurité automatisés, a ainsi détourné l'usage habituel de ses machines et leur fait dorénavant diffuser des messages d'intérêt public et des conseils sanitaires sur le coronavirus dans les espaces publics. 20 ans à peine après son émergence, le marché mondial de la robotique chirurgicale devrait passer de 6,7 milliards de dollars en 2020 à 11,8 milliards de dollars en 2025, ce qui représente un taux de croissance annuel de 12,1%.

"A long terme", estime Rian Whitton, analyste chez ABI Research, *"le développement de la robotique devrait connaître une croissance importante. A l'issue de la crise sanitaire, les entreprises auront d'avantage recours à l'automatisation pour accélérer le retour à la normale. Les nouvelles chaînes d'approvisionnement mettront l'accent sur la fabrication locale, sur la relocalisation et sur une production plus automatisée."*

> “ A l'issue de la crise sanitaire, les entreprises auront d'avantage recours à l'automatisation pour accélérer le retour à la normale

5 TENDANCES TECHNO-LOGIQUES

À SUIVRE DE PRÈS

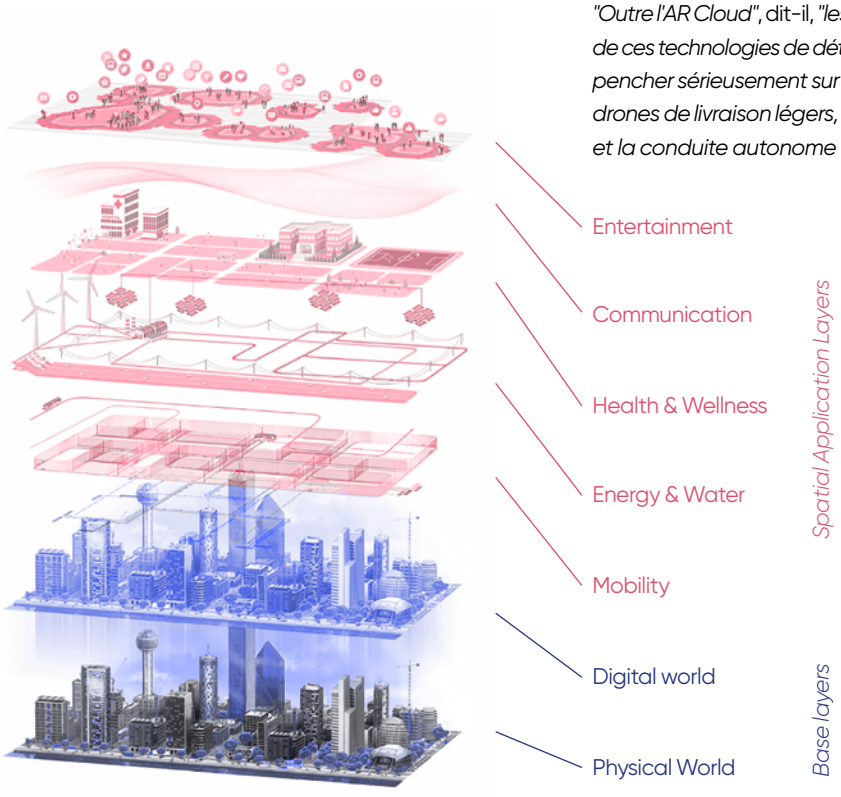
Détection et Mobilité, Humain Augmenté, Informatique et Communications Postclassiques, Ecosystèmes Numériques, IA et Analytique Avancées, voici les tendances clés qui se dégagent du dernier "Hype Cycle" consacré aux technologies émergentes par le cabinet Gartner.

Brian Burke, *Reaserch Vice President chez Gartner*

Les Hype Cycles de Gartner fournissent chaque année une évaluation de la maturité et de l'adoption des technologies et des applications, ainsi que de leur pertinence pour résoudre des problèmes réels et exploiter de nouvelles opportunités. Les 29 technologies émergentes étudiées par Gartner ont été regroupées en cinq tendances distinctes pouvant donner lieu à de nouvelles initiatives, créer de nouvelles expériences ou permettre aux entreprises d'exploiter à leur avantage les nouveaux écosystèmes numériques au cours des cinq à dix années à venir.

Pour **Brian Burke**, Research Vice President chez Gartner, *"l'innovation technologique est plus que jamais ce qui permet aux entreprises de faire la différence. Le rythme auquel s'enchaînent les progrès technologiques continue de s'accélérer et ceux-ci posent sans cesse de nouveaux défis aux entreprises, même aux plus innovantes d'entre elles"*.

Exemple d'AR Cloud – Les couches applicatives du Magiverse de Magic Leap



Détection et Mobilité

Aujourd'hui, en combinant les technologies de détection et l'intelligence artificielle, on peut donner aux machines une meilleure compréhension du monde qui les entoure et donc des capacités de mobilité et de manipulation d'objets inédites. Les technologies de détection forment également une composante essentielle de l'Internet des Objets et sont à la source des immenses quantités de données collectées par l'IoT. Y injecter de l'intelligence permet de récolter divers types d'informations pouvant être appliqués à de nombreux scénarios.

Selon Brian Burke, l'AR Cloud, un système de systèmes faisant le pont entre le physique et le numérique, permettra dans les années à venir de créer une carte du monde en 3D superposée au monde réel. Ce jumeau numérique à grande échelle autorisera de nouveaux modèles d'interaction qui, à leur tour, donneront naissance à de nouveaux modèles économiques qui permettront de monétiser l'espace physique.

"Outre l'AR Cloud", dit-il, *"les entreprises qui veulent tirer parti de ces technologies de détection et de mobilité devraient se pencher sérieusement sur les caméras de détection 3D, les drones de livraison légers, les véhicules autonomes volants et la conduite autonome de niveaux 4 et 5"*.

L'Humain Augmenté

"Pour détecter les fraudes, les compagnies d'assurance doivent analyser les déclarations de sinistre, établir des recoupements à l'aide de logiciels spécialisés ou faire appel à des enquêteurs privés. Mais une technologie émergente - l'intelligence artificielle émotionnelle - pourrait bientôt permettre de détecter la fraude à l'assurance en se basant sur l'analyse des signaux audio à l'occasion d'un simple contact téléphonique", explique Brian Burke. Dans un avenir proche, L'IA émotionnelle pourrait être utilisée pour améliorer l'expérience client en détectant l'humeur d'un consommateur, en dirigeant plus précisément les utilisateurs d'un centre d'appel, en détectant les conducteurs distraits ou même en adaptant un programme éducatif à l'état émotionnel d'un élève.

Les avancées en matière d'augmentation de l'être humain permettent aujourd'hui d'intégrer au corps humain des améliorations tant cognitives que physiques. Il est par exemple possible de créer des prothèses dotées de capacités qui dépassent les performances humaines naturelles les plus élevées. *"Les technologies émergentes pouvant contribuer à surmonter les limites actuelles du corps humain et à en étendre les capacités englobent entre autres l'intelligence augmentée, l'IA émotionnelle, la personnification, les espaces de travail immersifs, les biopuces, et la biotechnologie avec les tissus artificiels ou mis en culture"*, énumère Brian Burke.

Informatique et Communications Postclassiques

Pendant des décennies, l'informatique et les communications classiques - ainsi que leur intégration - ont connu des progrès considérables en grande partie grâce aux perfectionnements apportés aux architectures traditionnelles : conformément à la loi de Moore, les CPU devenaient sans cesse plus rapides, la mémoire plus dense et les débits plus élevés. Les technologies de nouvelle génération adoptent quant à elles des architectures complètement inédites, ce qui ouvre non seulement la voie à des approches entièrement nouvelles mais également à des améliorations en cascade dont les impacts promettent d'être très importants.

Les satellites LEO – c'est-à-dire en orbite basse - peuvent par exemple fournir une connectivité Internet à faible latence à l'échelle mondiale. Ces constellations de petits satellites seront ainsi capables d'offrir de la connectivité aux 48% des foyers qui en sont actuellement dépourvus et, par là, de nouvelles opportunités de croissance économique aux pays et régions non desservis. *"Seuls quelques satellites ont été lancés jusqu'à présent"*, admet Brian Burke. *"La technologie en est encore à ses balbutiements"*, dit-il, *"mais, dans les années à venir, elle devrait avoir un impact social et commercial spectaculaire. Les entreprises intéressées par le sujet devraient évaluer des technologies telles que la 5G, la mémoire de nouvelle génération, les systèmes LEO et l'impression 3D nanométrique"*.

Les Ecosystèmes Numériques

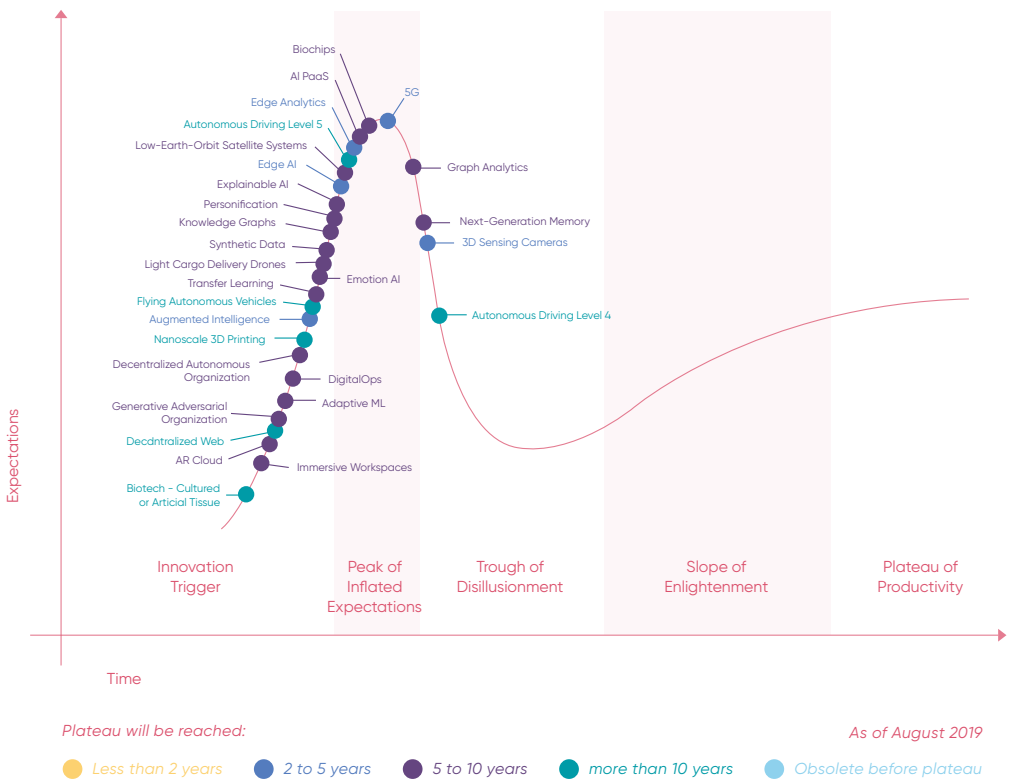
L'écosystème numérique s'appuie sur un groupe interdépendant d'acteurs - entreprises, personnes et objets – qui partagent des plateformes numériques pour atteindre un objectif mutuellement avantageux. La numérisation ayant facilité la déconstruction des chaînes de valeur classiques, celles-ci cèdent progressivement la place à des réseaux de création de valeur plus forts, plus flexibles et plus résilients qui se transforment constamment pour créer de nouveaux produits et services. Les technologies et les concepts à prendre en compte dans ce domaine sont les opérations numériques (DigitalOps), les graphes de connaissances, les données synthétiques, le web décentralisé et les organisations autonomes décentralisées (DAO).

L'IA et l'Analytique Avancées

Selon Brian Burke, "*l'adoption de l'intelligence artificielle de proximité – où les algorithmes d'IA sont traités localement sur un matériel qui n'a pas besoin d'être connecté pour effectuer sa tâche – est en augmentation pour les applications sensibles à la latence, comme la navigation autonome, sujettes à des interruptions de réseau, telles que le contrôle à distance, le traitement du langage naturel et la reconnaissance faciale, ou gourmandes en données, comme l'analyse vidéo*". Quant à l'analytique avancée, elle recouvre l'exploration autonome ou semi-autonome de données ou de contenus à l'aide de techniques et d'outils plus sophistiqués que ceux utilisés en Business Intelligence traditionnelle.

Les technologies à suivre dans ce segment incluent l'apprentissage automatique adaptatif, l'IA de proximité, l'analytique de proximité, l'IA explicable, la plateforme d'IA en tant que service (AIPaaS), l'apprentissage par transfert, les réseaux antagonistes génératifs et l'analytique des graphes (GAN).

Gartner Hype Cycle for Emerging Technologies, August 2019



COMMENT PAIERONS-NOUS DEMAIN ?

Payer d'un sourire, d'une parole, en tapotant. Avec l'essor du paiement mobile et digital, les jours du portefeuille physique semblent comptés. Mais comment réglerons-nous nos achats demain ? Quel est le niveau de maturité du paiement mobile ? Quel rôle la biométrie et l'Internet des Objets sont-ils appelés à jouer ? Allons-nous assister à la fin de l'argent liquide ? Face à ces interrogations, nous avons sélectionné, parmi les nouveaux moyens de paiement, 5 tendances susceptibles de s'affirmer dans les années à venir.

1. Le paiement mobile et sans contact

Le paiement sans contact n'est pas une nouveauté, mais la crise du Covid-19 marquera sans doute le véritable décollage de ce mode de paiement, que ce soit par carte ou à l'aide d'un téléphone mobile. Ainsi, au cours des quatre premiers mois de 2020, les mesures de distanciation sociale mises en place dans les pays nordiques (Danemark, Finlande, Islande, Norvège et Suède) pour combattre la pandémie ont engendré une augmentation sans précédent de 12% des paiements sans contact[1]. Du jamais vu, même pour cette région connue pour utiliser le moins d'argent liquide au monde.

Apple Pay, Android Pay, Samsung Pay,... le paiement sans contact à l'aide d'un smartphone gagne sans cesse du terrain. Comme les cartes bancaires sans contact, les téléphones mobiles utilisent la technologie NFC (Near Field Communication), qui permet l'échange de données sur de très courtes distances, pour communiquer avec les terminaux de paiement.

Les consommateurs apprécient de plus en plus de ne pas avoir à saisir leur code PIN au terminal et de pouvoir laisser leur carte bancaire à la maison. Au Pays-Bas, le nombre de clients d'ING qui ont recours au paiement mobile a ainsi presque quadruplé entre 2018 et 2019[2].

2. Le rôle croissant de la biométrie

La biométrie est déjà utilisée à des fins d'authentification sous la forme d'une empreinte digitale, d'une empreinte vocale ou d'une reconnaissance faciale comme c'est le cas, par exemple, avec Apple Pay. A l'usage, l'authentification biométrique s'avère peu contraignante et rend le paiement plus transparent. En Chine, près de 300 restaurants KFC ont testé le smile-to-pay, une technologie de reconnaissance faciale développée par Ant Financial, la filiale d'Alibaba dédiée aux paiements, et qui consiste à faire comparer par le terminal le visage du client à une photographie liée à un compte de paiement sécurisé. En Chine encore, le Groupe Carrefour a déployé, en partenariat avec Tencent via WeChat, le paiement par reconnaissance faciale dans la totalité de ses points de vente locaux, soit 210 hypermarchés.

Importance du paiement mobile pour les commerçants

80%

Des commerçants considèrent que le paiement mobile occupe une place fondamentale dans leur stratégie

92%

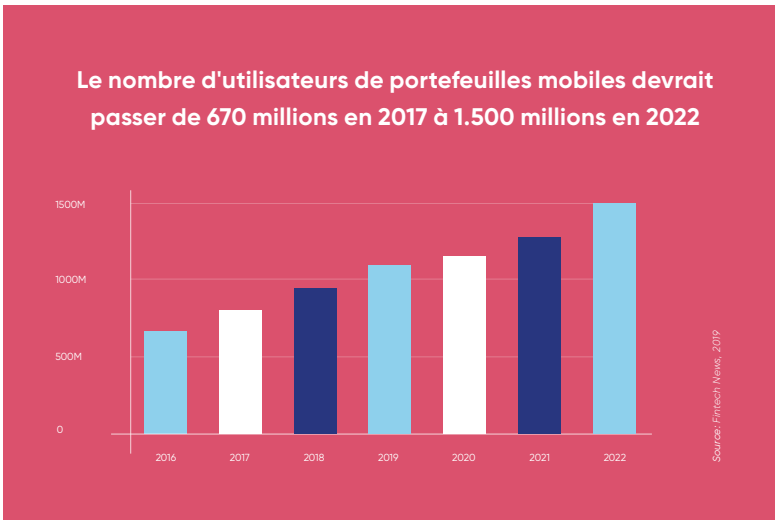
Des commerçants s'attendent à maintenir au niveau actuel ou à augmenter leurs investissements dans les infrastructures mobiles dans les 12 à 18 mois

80%

Des répondants citent la demande des consommateurs comme l'une des raisons principales pour l'adoption du paiement mobile

Source : Finextra, 2018

[1] *www.nets.eu*
[2] *www.ing.com*



> La part des transactions par carte physique devrait passer de **46**% à **34**% en Europe occidentale d'ici 2022
>
> ***Source: McKinsey, 2019***

3. Payer avec un objet ... connecté

L'IoT est en plein essor. Il est désormais possible de payer un achat avec sa montre, son bracelet de fitness ou un bijou comme la K Ring, la bague connectée développée par Mastercard. Les montres connectées et les traqueurs d'activité Garmin Pay et Fitbit Pay sont deux autres concrétisations de solutions IoT permettant de payer partout où il est possible de payer sans contact. Fitbit Pay, par exemple, est supporté dans plus de 20 pays et par plus de 160 banques et établissements de paiement, dont les réseaux Mastercard et Visa.

Des partenariats entre les réseaux de paiement et l'industrie se créent pour intégrer les paiements à l'aide de l'Internet des Objets (IoT). MasterCard, IBM et General Motors se sont ainsi associés pour intégrer la technologie de paiement sécurisée Masterpass à une nouvelle plateforme de mobilité cognitive appelée OnStar Go. Depuis 2017, les propriétaires de véhicules GM aux Etats-Unis peuvent effectuer certains achats, comme faire le plein de carburant ou payer un repas au drive, sans quitter le confort de leur voiture, ni même ouvrir leur portefeuille. Ce service est appelé à s'étendre progressivement à d'autres pays.

4. Le développement du paiement P2P

Les services de paiement peer-to-peer sont des applications - ou des fonctionnalités d'application - qui permettent à un particulier d'envoyer de l'argent à d'autres personnes rapidement et généralement gratuitement, en utilisant un numéro de téléphone, une adresse e-mail ou un nom d'utilisateur. Les plus connus de ces services sont Venmo (PayPal), Cash App (Square) et Zelle aux Etats-Unis. En plus de ses services de paiement pour les achats en ligne, PayPal offre également à ses utilisateurs enregistrés une solution de transfert d'argent P2P. Les portefeuilles numériques Google Pay et Apple Pay Cash offrent également de telles fonctionnalités à leurs utilisateurs. Certains réseaux sociaux, dont Facebook Messenger et Skype, permettent aussi d'effectuer des transferts d'argent entre pairs.

Par ailleurs, le paiement peer-to-peer fait progressivement son chemin dans le secteur de la vente aux consommateurs (B2C). Aux Pays-Bas, par exemple, les détaillants qui veulent intégrer le paiement directement dans leur propre parcours client se voient proposer par ING une solution qui leur permet d'envoyer à leurs clients une demande de paiement au moment de la livraison.

5. L'argent liquide n'est pas mort !

Demain, les paiement en espèces se feront moins fréquents, c'est une évidence. Dans certains pays scandinaves, les paiements électroniques sont devenus la norme[3]. La Suède, premier pays à introduire les billets de banque en 1661, pourrait bien aussi devenir le premier à se passer de liquide : les 56 milliards de couronnes qui circulent encore dans le pays ne représentent plus que 1,2% du PIB, le plus bas niveau du monde - la moyenne dans la zone euro étant de 10%, et le cash n'y est plus utilisé que dans 6% des transactions[4].

Mais l'argent liquide ne disparaitra pas complètement pour autant, loin s'en faut. Les régulateurs comme les citoyens sont préoccupés par la disparition éventuelle des espèces. Comment, par exemple, payer un achat en cas de panne généralisée des systèmes ? Que deviendrait un pays privé de tout moyen de paiement si une guerre ou une cyberattaque devait survenir ? Certains considèrent que l'instauration d'une société sans espèces nous soumettrait au monopole de l'industrie bancaire. Lors d'une crise financière, la seule défense du citoyen ordinaire consiste à retirer son argent de la banque: dans une société sans argent liquide, cela serait impossible. D'autres craignent des ponctions arbitraires sur les comptes des citoyens ou davantage de surveillance sous prétexte de lutte contre la fraude ou le terrorisme.

Utilisation du portefeuille numérique

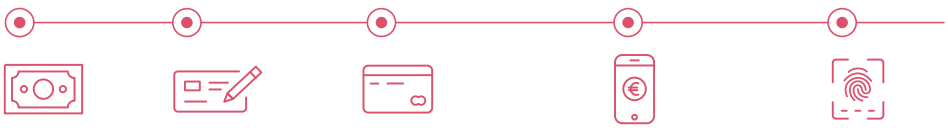
55% Utilisent leur portefeuille numérique car c'est l'option la plus rapide

51% Utilisent leur portefeuille numérique en raison d'une commodité accrue

Source : PaymentsSource, 2019

Une société sans argent liquide est-elle souhaitable ? On ne peut que s'interroger quand on apprend que la Suède, pays pourtant le plus avancé en matière de paiement numérique, vient d'adopter, au mois de janvier de cette année, une nouvelle loi visant à obliger les banques à fournir des services en liquide afin de protéger les plus âgés et les défavorisés, et d'être en mesure de faire face à de possibles cyberattaques.

Historique des supports de paiement



Espèces
- *Permet de payer partout*
- *Contrôle des dépenses*

Chèque
- *Sécurité accrue*
- *Commodité*

Carte de paiement
- *Sécurité accrue*
- *Argent accessible 24/7*
- *Commodité*

Appareil mobile
- *Sécurité accrue*
- *Personnalisation, fidélité et cashback*
- *Un objet de moins à emporter*

Pas de support

Les experts de l'industrie prédisent que l'identité biométrique aura un impact substantiel sur les futures expériens d'achat en magasin

[3] *www.nets.eu*
[4] *www.letemps.ch*

DIGITAL CLIENT MANAGEMENT

RÉINVENTER LA RELATION CLIENT

En ces temps de transformation technologique accélérée, les organisations qui ne progressent pas au rythme imposé par la révolution digitale en payent chèrement le prix. Dorénavant, les entreprises les plus performantes sont celles qui accompagnent leurs clients au quotidien et sont à l'écoute pro-active de leurs besoins. Cela, à toutes les étapes de leur parcours et sur tous les canaux de communication. Consciente de ces enjeux, Telindus a constitué une équipe multidisciplinaire d'experts capable d'offrir aux entreprises les outils les plus innovants pour réussir leur transition vers le Digital Client Management.

Frank Roessig, *Fintech Lead chez Telindus*

L'expérience digitale change la donne et offre de nouvelles opportunités pour acquérir, développer ou conserver une clientèle. Nouveaux processus d'achat, de conversion, de vente ... le digital offre à l'entreprise des outils aussi innovants que performants pour réinventer la relation qu'elle entretient avec ses clients. "Nous observons que, dans tous les secteurs, la gestion du client se fait de plus en plus de façon digitale", confirme **Frank Roessig**, Fintech Lead chez Telindus. "Cette relation se fait même 'phygitale', ce qui signifie qu'il faut être capable de créer un lien fort entre le canal de distribution briques et mortier et son alter ego digital. En effet, une porosité de l'information ainsi qu'une continuité des services au travers les canaux de distribution optimisent l'expérience des clients ", ajoute-t-il.

Une expérience full-service et omnicanal

"Qu'il s'agisse d'un consommateur ou d'une entreprise", poursuit Frank Roessig, "le client veut non seulement bénéficier d'une offre de services en ligne complète mais aussi pouvoir y accéder par tous les canaux de communication dont il dispose. Il veut avoir la possibilité de consommer un service indifféremment sur son mobile, sa tablette, son PC, ou en se rendant dans un lieu physique quand il en éprouve le besoin. De plus, au sein de cet environnement omnicanal et full-service, le client s'attend à pouvoir chater, échanger des messages, avoir un entretien en face-à-face ou par vidéoconférence. L'approche omnicanal repose donc sur deux composants : l'appareil proprement dit et le média utilisé sur cet appareil."

L'offre de services en ligne se doit également d'être aussi étendue que son équivalent dans la sphère physique. *"Au cours des 5 dernières années, le taux d'utilisation des services bancaires digitaux est passé de 65% à 86%. Certains services en lignes sont bien sûr plus sollicités que d'autres : si 90% des clients bancaires recourent aux services digitaux pour consulter leur compte, les conseils en investissement en ligne ne touchent que 20% d'entre eux"*, explique Frank Roessig. *"Aujourd'hui – et d'autant plus suite à la pandémie de coronavirus – les clients veulent pouvoir effectuer en ligne tout type d'opération, et à n'importe quel moment. Ces nouvelles attentes remettent en cause le modèle économique de beaucoup d'entreprises. Et pour que cela fonctionne, la confiance est un élément indispensable"*, insiste-t-il.

Etendre et sécuriser les nouveaux services

C'est là que Telindus entre en scène. La mission que s'est donnée la société est de faire en sorte que ces nouveaux services digitaux soient rendus de manière efficace, sécurisée, et conforme aux lois et réglementations. *"En matière de conseil financier, par exemple, la Directive MiFID II requiert des institutions financières qu'elles assurent la traçabilité de toute communication en lien avec une transaction entre elles et leurs clients. Cette obligation d'enregistrement – et d'extraction aisée si le client en fait la demande – s'applique à tous les moyens de communication : réunion physique, email, appel depuis une ligne fixe ou mobile, SMS, chat, ou encore vidéo. Pour aider le secteur financier à rencontrer les exigences de la directive, Telindus a développé un outil intégré qui permet d'enregistrer et de tracer les échanges entre un investisseur et son fournisseur"*, explique Frank Roessig.

Jusqu'il y a peu, les services en ligne s'adressaient essentiellement aux jeunes générations. Ici aussi, la crise sanitaire a changé la donne et les seniors se sont découvert un intérêt pour ce type de services. Ce saut générationnel implique des adaptations du design et de l'ergonomie des applications. *"Dans le monde physique"*, dit encore l'expert de Telindus, *"il serait très difficile de concevoir un point de vente pouvant convenir à différents publics. Par contre, dans l'univers digital, décliner un service sous plusieurs formes adaptées à des publics variés est non seulement facilement réalisable, mais aussi beaucoup moins coûteux."*

"Nous assistons également à de grands efforts de digitalisation de la part des acteurs du marché interentreprises", ajoute-t-il. *"D'abord, parce que les digital natives veulent travailler comme ils vivent; mais également parce que beaucoup de services s'avèrent inefficaces. Le secteur de la logistique, par exemple, consomme encore d'énormes quantités de papier. Des secteurs aussi variés que la construction, le tourisme, l'agriculture, la métallurgie, l'aide aux personnes, sans oublier les PME, accusent un retard important en matière de transformation digitale."*

La gamme d'outils digitaux développée par Telindus va du digital onboarding - l'accueil client sécurisé - jusqu'aux solutions de self-service omni-device, en passant par une gestion documentaire qui donne au client final un accès direct à ses factures, sa consommation, etc. *"Si l'entreprise qui fait appel à nous est active dans le secteur interentreprise"*, explique Frank Roessig, *"la solution d'accueil client que nous lui proposons prend la forme d'un corporate KYC. Cette solution repose sur une plateforme d'enregistrement automatique qui permet de collecter et de rassembler les données de la société cliente, telles que statuts, informations légales, comptes annuels, etc. Les informations nécessaires à l'accueil sont ainsi rassemblées sans que le client final ait à faire quoi que ce soit, si ce n'est valider les informations."*

En matière de Digital Client Management, la gestion de l'identité constitue un élément clé. En effet, plus l'accès aux services digitaux est aisé et convivial, plus le danger de piratage des informations augmente. *"Si les systèmes que nous mettons en place sont accessibles à partir de n'importe quel appareil, ils n'en sont pas moins fortement sécurisés"*, souligne Frank Roessig. *"Pour cela, nous avons recours à différentes technologies : identification de l'appareil par son adresse IP, authentification multi-facteurs, biométrie, ou encore intelligence artificielle. Certains opérateurs du secteur financier, ont ainsi commencé à appliquer des modèles comportementaux pour protéger leurs clients. A terme, la généralisation de cette pratique permettra de vérifier l'identité d'un client en détectant des comportements anormaux ou inhabituels"*, prédit-il.

L'intelligence artificielle au cœur de la relation avec le client

L'intelligence artificielle et ses sous-disciplines, le machine learning et le deep learning, sont devenues des technologies essentielles pour sécuriser les transactions en ligne. L'IA permet notamment de lutter efficacement contre la fraude, le blanchiment d'argent et l'abus d'identité. *"Nous pratiquions déjà la détection de fraude aux paiements pour des banques européennes majeures"*, rappelle Frank Roessig. *"Ce qui est nouveau, c'est que Telindus a décidé de développer davantage ses capacités en intelligence artificielle. Il s'agit, par exemple, de développer des systèmes capables de détecter les risques d'attrition de la clientèle"*, indique-t-il. Certains comportements, certains signes, permettent en effet à un système d'IA de déduire qu'un client risque de quitter son fournisseur. En poussant plus loin l'analyse, on s'aperçoit que ces mêmes technologies permettent également de détecter, directement en ligne, de nouvelles opportunités commerciales.

Les demandes des clients parviennent de plus en plus souvent à l'entreprise sous forme de chat, d'email, mais aussi de courrier postal et d'échanges téléphoniques ou en face-à-face. Déployer des systèmes intelligents, qui scannent et interprètent ces

> “ Telindus travaille étroitement avec des équipes basées à Los Angeles, qui développent des solutions de pointe en intelligence mobile et en identification sécurisée. Ces solutions sont notamment utilisées par de grandes banques aux Etats-Unis, en Europe et, depuis peu, en Amérique latine.

demandes avant de les attribuer aux personnes qualifiées pour les traiter, permet d'automatiser les processus de traitement. Ces systèmes d'IA rendent les réponses plus efficaces, plus rapides, et permettent de réaliser d'importantes économies d'échelle.

"Aujourd'hui, le client passe bien plus de temps sur la plateforme digitale de son fournisseur que dans les locaux de celui-ci", constate Frank Roessig. C'est donc sur la sphère digitale qu'il faut faire porter les efforts : observer les activités des clients, détecter les comportements significatifs, en tirer les enseignements et agir pour fournir un service personnalisé. Qui plus est, les informations recueillies dans l'espace digital peuvent aider à enrichir la gestion de clientèle. *"Ces processus basés sur l'IA sont à l'origine d'un véritable cercle vertueux d'amélioration des services et de développement de la clientèle"*, insiste-t-il. *"Travailler sur les données permet d'améliorer le service, ce qui donne la possibilité d'acquérir davantage de clients, lesquels génèrent plus de données qui permettent d'enrichir à nouveau le service, et ainsi de suite."*

Concrétiser les promesses du digital

"Pour concrétiser le potentiel des nouvelles technologies et faire bénéficier les entreprises d'une approche complète en la matière, nous avons choisi d'organiser à leur intention des workshops spécifiques", explique Frank Roessig. *"Nous mettons à profit ces espaces de rencontre pour analyser le cycle de leurs processus clients, imaginer comment rendre ces expériences plus fluides, et identifier la manière de leur procurer un avantage compétitif."*

Ces workshops intègrent de nombreuses parties prenantes car toute la chaîne de valeur de l'entreprise cliente doit être représentée. S'y ajoutent des experts de Telindus en design-thinking, en solutions digitales, des spécialistes-métiers, sans oublier les experts techniques chargés d'évaluer les infrastructures nécessaires selon les besoins identifiés. *"Il nous arrive d'y inviter des clients finaux pour recueillir leurs réactions face aux idées proposées"*, ajoute Frank Roessig. *"Sur cette base, nous pouvons ensuite faire monter en puissance la solution – ou une partie de celle-ci - en fonction des leçons apprises."*

PAYPAL

AT THE CROSSROADS OF CONVENIENCE AND SECURITY

PayPal

Frank Keller, Vice President, Europe & Global Inside Sales of Paypal

PayPal has been providing an alternative to traditional payment methods for over two decades now. The company has grown significantly since the days when it was best known as a way to make purchases on eBay, expanding to hundreds of countries around the world with millions of active customers. We asked ***Frank Keller****, Vice President, Europe & Global Inside Sales of PayPal, to give us some insights on the future of the global payments space.*

AS THE PAYMENTS UNIVERSE EXPANDS, CUSTOMER EXPERIENCE IS BECOMING A KEY COMPETITIVE DIFFERENTIATOR. HOW DO YOU DESIGN NEW PAYMENTS EXPERIENCES?

F.K. At PayPal, we have a customer-centric approach for designing and delivering new products. The product development journey is iterative and starts by identifying customer pain-points. We continuously meet with existing and potential customers to learn more about their behaviors, preferences and challenges.

Once we have identified an issue or a customer pain-point, we focus on finding the right solution. We count on open stack shared services that are easy to integrate, reusable across different contexts and have global compatibility. For product design, our approach is to "design globally, optimize locally", which allows us to launch simultaneously in many markets.

Our recent QR code payments launch in 28 markets around the globe is a good example of this approach. In a response to the COVID-19 pandemic and the increasing demand to buy and sell in a touch-free way, we introduced a QR code functionality to our app. This feature provides a quick and safe way to complete a transaction in-person utilizing PayPal and eliminating the need to handle cash.

A STUDY CONDUCTED BY AMERICAN EXPRESS SHOWS THAT WHILE MERCHANTS LOOK TO ENHANCE PAYMENT SECURITY, CONSUMERS DESIRE TO SPEED UP THE CHECKOUT EXPERIENCE ACROSS ALL PAYMENT CHANNELS, INCLUDING ONLINE TRANSACTIONS. HOW DO YOU ADDRESS THIS BATTLE BETWEEN CONVENIENCE AND SECURITY?

F.K. Security is a top priority for PayPal, as we are securing the world's digital operating system for commerce. We are committed to continuously making significant investments in security to protect our complete ecosystem: consumers, merchants and employees. We process more than 33 million transactions per day and 22,000 USD in payments every second, which enables us to learn about our customers' spending patterns, behavior, location and more. This data is used privately to verify customer identities implicitly, so they do not need to identify explicitly every time they transact. With that, we are giving our customers the confidence of security while shaving valuable seconds off purchase time. Data closes the loop between speed and safety: within a two-second transaction, PayPal will conduct hundreds or even thousands of risk checks.

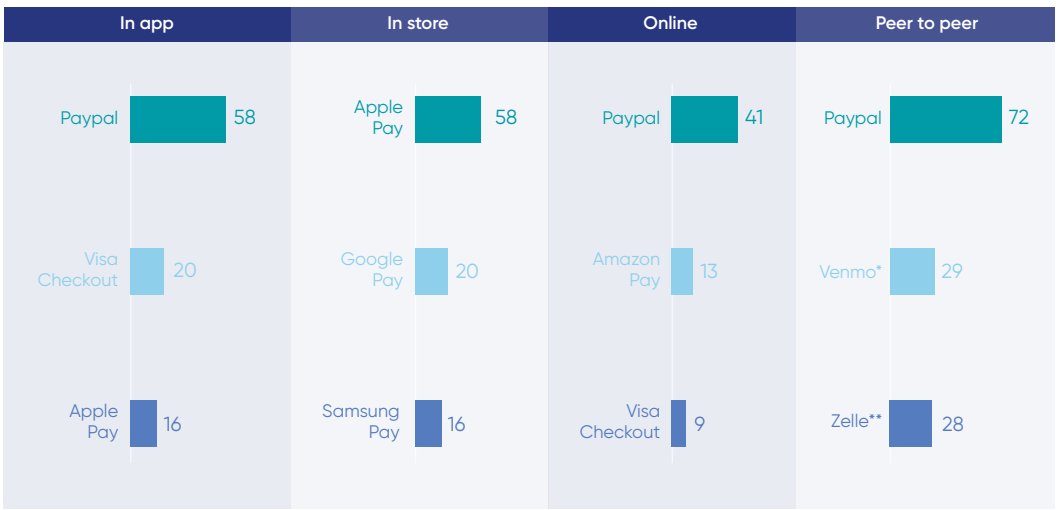
> "We are committed to continuously making significant investments in security to protect our complete ecosystem: consumers, merchants and employees

WITH ALL THE FOCUS ON THE COMING OF AGE OF MILLENNIALS, LESS ATTENTION HAS BEEN GIVEN TO GENERATION Z. GEN Z - THOSE WHO WERE BORN BETWEEN 1995 AND 2015 - CURRENTLY MAKES UP 24% OF THE GLOBAL POPULATION AND IS SET TO HAVE SIGNIFICANT SPENDING POWER[1]. WHAT ARE YOUR PLANS FOR REACHING OUT TO THIS FINANCIALLY POWERFUL GENERATION OF YOUNG CONSUMERS?

F.K. Today, mobile and app-based services that especially the younger generation are using on a daily basis, such as food delivery, public transport tickets or music streaming services, require secure online payments. Being available

Digital wallet wars are still raging, but clear leaders exist by environment

Popular payment method *(% penetration)*



Source: McKinsey, 2019 Digital Payments Survey

* Venmo is a subsidiary of Paypal ** Zelle is available in the US only

[1] Source: *Research and Markets*

> “ Our peer-to-peer payment offer is another key driver for digital natives across Europe

as a payment method for these new experiences increases our visibility among younger consumers. Another key driver for digital natives across Europe is our peer-to-peer payment offer. The fact that you can use PayPal to send money to your friends and family has been a huge driver of new customers as well as keeping them engaged, especially in Europe. When it comes to addressing Gen Z via marketing, we focus on products and experiences that are relevant to this target group and communicate through channels that match their media consumption habits.

WILL THE COVID-19 CRISIS ACT AS AN ACCELERATOR FOR THE END OF CASH? WHICH ALTERNATIVE PAYMENT MODES ARE IN THE BEST POSITION TO TAKE OVER?

F.K. We have seen three big shifts coming out of the global pandemic: First, the world is moving from physical to digital. There has long been a distinct long-term trend towards digital payments, but the current environment has rapidly accelerated that movement.

Second, we are seeing the face of retail fundamentally changing, moving more and more to online ecommerce at a much more rapid pace. The impact of COVID-19 has accelerated the shift from physical to online commerce by two to five years.

Third, we are seeing the rise of digital payments. Digital payments have gone from a nice-to-have to a must-have. We are fortunate to be in a position where we can help our merchant customers move online and help our customers leverage digital payments in a safe way. As consumers and businesses are moving online, we have seen our customer base rise to more than 325 million customers, the average daily usage across our base is up well over 20% and the new cohorts of users are 30% more engaged than previous ones.

People are embracing digital payments and we believe that this trend will only continue. Digital payments, whether online or in-store, will become an integral part of our daily lives, even when shelter-in-place restrictions lift. People do not want to handle money, touch screens or pick up pens to complete their in-store transactions. Given the demand for contactless and digital payments, we expect a continued rise in ecommerce activity. We recently rolled out an in-app QR code feature that allows consumers and businesses to conduct in-person transactions at a safe distance, touch-free, using PayPal. We expect to see more touch-free payments such as this to be used by retailers of all sizes.

BLOCK-CHAIN

L'INTERNET DE LA VALEUR

Cyril Paglino, Co-Fondateur chez The Garage

Selon le dernier rapport de Forrester Research consacré à la blockchain , la frénésie du milieu de la décennie a cédé la place à une approche plus pragmatique et réaliste de la "technologie du registre distribué". Le cabinet souligne que si les projets aujourd'hui en cours en Amérique du Nord et en Europe sont moins nombreux qu'il y a quelques années, ils relèvent d'initiatives sérieuses et non plus d'hypothèses hasardeuses.

Après avoir fondé en 2017 Starchain Capital, un fond d'investissement dédié aux actifs numériques et à la blockchain, l'entrepreneur du numérique **Cyril Paglino** a ainsi récemment lancé The Garage, un incubateur DLT aux ambitions européennes et résolument tourné vers les nouveaux usages de la chaîne de blocs.

QUELLE EST VOTRE DÉFINITION PERSONNELLE DE LA BLOCKCHAIN ?

C.P. Wikipedia dit qu'il s'agit d'un registre comptable. Pour ma part, je décrirais la blockchain comme une technologie assez nouvelle, qui a un peu plus d'une dizaine d'années, et qui été rendue célèbre car elle est utilisée par le protocole Bitcoin. La blockchain permet la désintermédiation dans tout type d'échange. Qu'est-ce que cela veut dire ? Cela signifie que, dans une multitude de blockchains, les transactions sont plus sécurisées, plus rapides, moins coûteuses et sans intermédiaire.

QUEL EST VOTRE VISION DE L'AVENIR DE LA BLOCKCHAIN ?

C.P. Il est certain que la blockchain va s'immiscer dans toutes les industries, dès lors que des échanges de valeur ou des transactions interviennent. Les transferts d'actifs, quels qu'ils soient, les marketplaces, le vote, le message, sont des transactions ou des services transactionnels. Je suis convaincu que nous allons assister à une adoption lente mais certaine des systèmes de blockchain au cours des prochaines années.

QUE REND-ELLE POSSIBLE ?

C.P. Elle rend possible la décentralisation d'une base de données et donc sa mise à jour en temps réel et ce, pour tous les acteurs concernés. Maintenant que nous sommes capables de transférer de la valeur de façon sécurisée, rapide et sans intermédiaire, nous pouvons imaginer quantité de services et d'outils nouveaux.

L'arrivée de la musique, de la photo et de la vidéo dans le cyber espace a été le point de départ de la révolution Internet de ces deux dernières décennies. Maintenant que nous pouvons transférer de la "valeur" sur Internet, un nouveau champ des possibles s'offre à nous. Des milliers d'ingénieurs, d'entrepreneurs et d'investisseurs l'ont bien compris et y consacrent tous leurs efforts. L'automatisation via les smart contracts, la tokenisation d'actifs peu liquide comme l'immobilier, l'art, la joaillerie, ou la création, les économies et places de marché basées sur les services pair à pair sont des cas d'usage que l'on peut d'ores et déjà considérer comme pertinents. Mais les innovations les plus importantes restent à venir. Au même titre qu'en 1995, il était impossible d'imaginer Twitter, Uber ou Instagram, il est aujourd'hui très difficile d'imaginer les "trillion dollar protocols" de demain.

QUELLES ACTIVITÉS SONT SUSCEPTIBLES D'ÊTRE LE PLUS IMPACTÉES ?

C.P. En premier lieu, l'industrie financière avec notamment le mouvement DeFi de décentralisation de la finance, mais aussi l'immobilier, le notariat et les services de certification. Dans un second temps, tous les types de marketplaces et de services seront impactés.

Dès leurs premiers balbutiements, les systèmes blockchain ont apporté des améliorations majeures. Nous avons assisté à des améliorations d'un facteur 10 pour le réseau interbancaire SWIFT par exemple, mais aussi pour le crowdfunding à travers les ICOs. Au Delaware, il est désormais possible de créer en quelques secondes une société dotée d'une adresse de facturation et d'y percevoir de l'argent, grâce au réseau Ethereum.

QUELLES SONT LES AMBITIONS DE VOTRE DERNIÈRE INITIATIVE EN DATE, THE GARAGE ?

C.P. L'idée à l'origine du Garage est de créer un lieu et une infrastructure réunissant des experts sur les sujets que nous venons d'évoquer, afin de conseiller et d'accompagner dans les meilleures conditions les innovations blockchain, françaises comme européennes. Nous aidons aujourd'hui 20 sociétés à se développer. Nos actions portent sur des besoins liés au recrutement, au produit, à la technique, au financement, au marketing, ou encore aux aspects réglementaires et légaux.

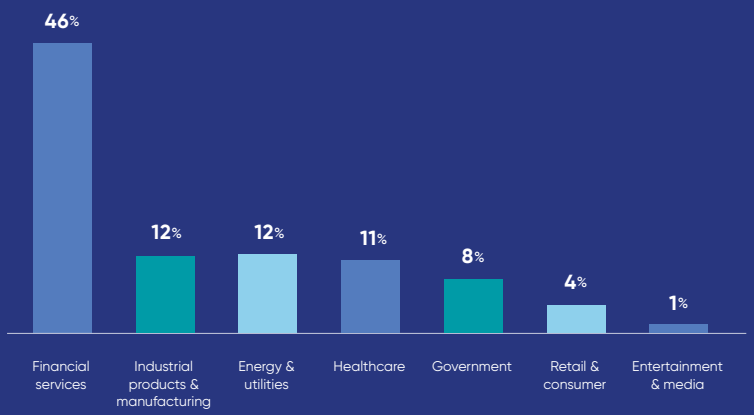
> “ Plus de **80**% des déploiements blockchain seront hybrides ou multicloud - ou les deux
>
> ***Source: Forrester Research***

Né le 1er juillet **1986**, **Cyril Paglino**, est un entrepreneur français. Après une première carrière artistique et médiatique, il s'établit à Los Angeles et se tourne vers le monde de l'entrepreneuriat, dans les domaines de la communication et du numérique.

Cyril Paglino participe en **2009** à la création de **Wizee**, une agence de communication digitale spécialisée dans la mise en relation de célébrités. En **2015**, il co-fonde **Tribe**, une application de messagerie vidéo instantanée.

En **2017**, il crée **Starchain Capital**, un fond d'investissement dédié à la Blockchain et, en novembre **2019**, il lance **The Garage**, un incubateur dédié exclusivement à la blockchain et basé à Paris.

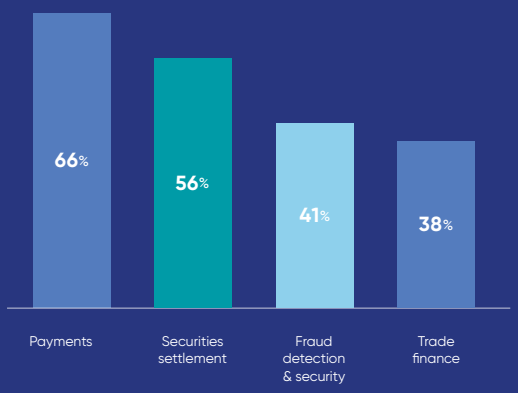
Industries That Global Executives Think Are Most Advanced In Blockchain Development



Source: Business Insider Intelligence

Note: Percentage don't sum to 100% because industries with less than 1% of votes are excluded. Source: PwC Global Blockchain survey, n=600, 2018

Primary Benefits Of Blockchain According To FIs Exploring Or Using The Tech



Source: Business Insider Intelligence

Note: Respondents are representatives of US banks with assets of over $100 billion that are evaluating, piloting, or implementing blockchain. Source: UBS Evidence Lab, 2019, n=40

JOHN KINDERVAG:

THE ART OF HEALTHY SKEPTICISM

BANKS USED TO BE BUILT TO LAST. TODAY, THEY NEED TO BE BUILT TO CHANGE.

John Kindervag, *Field CTO, Palo Alto Networks*

With its principle of user, device and infrastructure verification before granting conditional access to enterprise resources, the Zero Trust security model is growing in popularity as a new approach to cyber risk mitigation. But while Zero Trust holds the promise of enhanced usability, data protection and governance, many security professionals are not confident in their ability to apply this type of architecture in today's IT environments. In order to demystify perceptions and beliefs about Zero Trust, we met ***John Kindervag*** *who first came up with the idea of eliminating the concept of trust from an organization's network architecture.*

John Kindervag *created the concept of Zero Trust in 2010 during his tenure as a vice president and principal analyst for Forrester Research, when it became clear to him that traditional security models operated on the outdated assumption that everything inside an organization's network should be trusted. Having joined Palo Alto Networks as Field CTO in 2017, he currently advises both public and private sector organizations with the design and building of Zero Trust networks and other cybersecurity topics.*

ZERO TRUST HAS BECOME ONE OF THE LATEST BUZZWORDS IN THE CYBERSECURITY CIRCLES, TO SUCH AN EXTENT THAT NON-SPECIALISTS OFTEN STRUGGLE TO GET A CLEAR UNDERSTANDING OF THIS MODEL. CAN YOU TELL US IN SIMPLE TERMS WHAT IS - AND WHAT IS NOT - A ZERO TRUST ARCHITECTURE?

J.K. We have to distinguish between Zero Trust and the architecture that comes out of it. Zero Trust is a cybersecurity strategy which identifies that the fundamental problem in cybersecurity is the broken trust model where it is said that the trusted side of the network goes to the internal network and the untrusted side goes to the external network. And if you are on the internal network, you can have access to any resource based upon that trust model. Identifying that the fundamental flaw was trust, a human emotion injected into a digital system for no reason, was the foundation for Zero Trust.

And then, of course, you need a way to make that thing happen, bring it into action. That's where architecting a Zero Trust environment comes in. All this was extensively described in the second report I wrote back in 2010, called Build Security Into Your Network's DNA.

There are four design principles when you are building a Zero Trust environment. The first step is focusing on the business outcomes. What is the business trying to achieve? That's the question we ask. Typically we didn't do that in traditional cybersecurity. We used to build networks for our organization based upon certain standards, or what we thought were standards but were in fact ideas created by vendors for the purpose of selling equipment.

The second thing that we do in Zero Trust is design the network or the environment from the inside-out instead of the outside-in. GDPR, for example, says that you need to know where all your data and assets are, but no one knows because the networks were built the wrong way, from the outside-in instead of the inside-out. If you're going to protect something, you need to know what it is, you need to know where it is, you need to know who should have access to it.

> “ There are no prerequisites for doing Zero Trust

Start Zero Trust environments with the thing that you want to protect. Deploying Zero Trust environments is based upon the concept of protect surfaces, the smallest possible reduction of the attack surface. A protect surface contains a single DAAS element - Data, Assets, Applications and Services - and these vary as far as how sensitive or critical they are. There are data types that you need to protect like credit card data, health data, PII, or intellectual property. There are applications that you need to protect like HR applications, CRM applications, or applications that use sensitive data. There are assets that

you need to protect, places where sensitive data is stored, or assets that highly impact the availability of systems. And then finally, there are services that you need to protect, services like DNS, DHCP, Active Directory, Network Time Protocol, things that are very fragile but integral to your business. So, we take a single DAAS element, we put it into a single protect surface, and we start building the Zero Trust network from there going out.

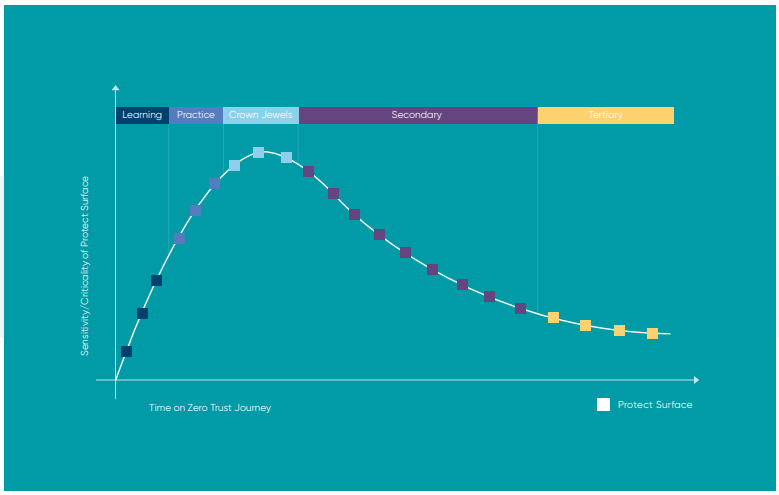
The third design principle is to control access to the DAAS element in the protect surface, based upon need to know and least privileged concepts. Abuse of trust is at the heart of many of the data breaches making news headlines on an almost daily basis.

And then finally, we inspect and log that access all the way through layer 7 of the packet to make sure that it doesn't have threats embedded in it, that it behaves appropriately, and that it meets policy. Ultimately, Zero Trust is a layer 7 policy statement but I must have layer 7 technology in order to enforce that policy statement. And that's why I joined Palo Alto Networks, because what their core technology does is enforce these types of Zero Trust layer 7 policy statements. Using this technology, it was very easy for me to deploy Zero Trust environments, whether on premises, in public or private clouds.

> “ Zero Trust makes cybersecurity a business enabler instead of an inhibitor

WHAT ARE THE BUSINESS BENEFITS OF ADOPTING A ZERO TRUST APPROACH?

J.K. There are several business benefits in using Zero Trust. I identified them when I was still at Forrester. There is, first, a reduction in capital expenditures. You have too much technology now that doesn't integrate. So, by collapsing a lot of that you get savings in capital expenditures. Palo Alto Networks, for instance, have gathered all of the disparate independent components that you would use in cybersecurity - like firewalls, IPS, content filtering, or sandboxing - and collapsed them into a single unified architecture that applies each of those components as a service, in real time, in a single pass of the packet. This is where the value of Zero Trust lies from a CAPEX perspective.



> “ In cybersecurity, we can't settle for keeping things the way they are

This automatically leads to a reduction in operational expenditures. With Zero Trust, we reduce complexity, which results in an equivalent reduction in operational costs. We lower the number of rules that we need to manage and smaller rule sets are easier to maintain, monitor and update. Typically, there is a 7 to 10 times reduction in the policy space when applying Zero Trust.

By placing the security controls very close to the assets that you are protecting - the protect surface - you also reduce the ability of lateral movement of malware. This results in blocking the ability of attackers to exfiltrate data, which is actually the situation that leads an organization to having a breach. With Zero Trust, the limitations on the possibility for bad actors to get access and exfiltrate the data are huge.

The thing that surprised me the most when I started working on this is the reduction in audit costs generated by Zero Trust, especially as it relates to compliance. By implementing a Zero Trust approach, you end up with a less complex environment and doing less work overall. Once you know what your data is, where it is and how important it is, you can then put your efforts towards it. Adopting a Zero Trust mindset is also a really strong way to show auditors that you are doing your part. It also means that compliance becomes far easier as a result of best-in-class documentation and records at every stage.

All these things taken together become a huge benefit for the organization, and make cybersecurity a business enabler instead of a business inhibitor by helping to keep the business operational because it doesn't have to contend with disruptive cybersecurity events.

WHAT ADVICE WOULD YOU GIVE AN ORGANIZATION THAT WANTS TO GO ZERO TRUST?

J.K. I have worked in Zero Trust environments for well over a decade. I used to think that we should start deploying Zero Trust with the most sensitive data an organization needs to protect because those things are the most important. Experience now tells me that that thinking was wrong, and we need to change it.

The trouble with starting with the most sensitive protect surfaces is that they are often too fragile and many people don't know how they work. Starting there with Zero Trust frequently results in failures. Too often, when this happens, organizations blame these failures on Zero Trust. In fact, the problem is that no one in the organization has experience building Zero Trust environments.

To start out deploying Zero Trust environments, an organization should first of all consider building what I call a Zero Trust Centre for Excellence – gathering business and IT leaders – where everybody talks to each other about the problems they face, because what is missing from a lot of cybersecurity initiatives is the involvement of the business.

And then you build it. You start small. You start by working on what I call learning protect surfaces. You need to start with a low sensitivity environment because you have to give people the ability to fail without retribution. Once you are comfortable with the basic concepts of Zero Trust environments, you can move on to the practice protect surfaces. These are a little more sensitive, a little more critical, but they are not the "crown jewels" of your organization. This way, before you touch the most sensitive protect surfaces in your environment, you have practiced and gained confidence in the mindset of Zero Trust. This is the peak of the Zero Trust learning curve.

Once you have protected your high-value assets, the remainder of the journey becomes easier. From there, you can focus on less important assets, the secondary and tertiary protect surfaces. Eventually, you will end up in a place where you don't have anything left that is important enough to go into a Zero Trust environment.

The Zero Trust Learning Curve is an important thing to understand. When I first started talking about Zero Trust, many people didn't understand what it was or why they should deploy it. The Zero Trust principles didn't match what they were familiar with. Now that more people understand what Zero Trust is about, I'm more likely to hear the objection that deploying it sounds overwhelming and that people are not sure where to start. But in cybersecurity, in a threat environment that is constantly escalating, we can't settle for keeping things the way they are. The thing I fight against now is doing nothing.

DOES ZERO TRUST MAKE TRADITIONAL SECURITY TECHNOLOGIES – SUCH AS VPN - COMPLETELY OBSOLETE OR SHOULD ENTERPRISES PREPARE THEMSELVES TO OPERATE IN A HYBRID ENVIRONMENT MADE OF A MIX OF TRADITIONAL AND NEWER SECURITY DESIGN PRINCIPLES?

J.K. One of the most common mistakes is to say that Zero Trust is going to kill the VPN. This is one of the myths or deceptions propagated by people who don't have the technological background to understand how VPNs work. No, you are never going to get rid of it. VPN is definitely part of Zero Trust.

There are only two ways to send traffic across the public Internet - encrypted or in clear text - and if it's encrypted, it's in a VPN. There are no Zero Trust products or technologies. What we do is use existing technologies in Zero Trust ways. There are products that work well in Zero Trust environments and those that don't. When I hear someone saying "we have a Zero Trust product", that's always a red flag to me that these people don't understand Zero Trust. Zero Trust is built upon your existing architecture and does not require you to rip and replace existing technology.

IS ZERO TRUST ADAPTED TO ALL TYPES OF ENTERPRISES REGARDLESS OF THEIR SIZE AND BUSINESS SECTOR?

J.K. There are no prerequisites for doing Zero Trust. Zero Trust is suitable for businesses of any sector and any size, be they small, medium, large, even extra-large. It doesn't matter. The reason is - and this has to be reinforced - that everybody is much more the same than they are different. There are two things that really impact the way your network is designed. The first one is TCP/IP, a standardized way of transporting packets that everybody uses. In that way, everybody is exactly the same. The second thing that impacts it relates to the compliance mandates that you need to protect.

What makes up the specificity of your organization is determined more by how your network gets designed than anything else. It doesn't relate to your size. It doesn't relate to your sector. If you understand what you are protecting, that's all that matters. At Palo Alto Networks, we make products that work for any size company. You won't get less because you are a small company, it's all the same technology under the hood.

NEOBANKS

LEVERAGING THE CLOUD TO CHANGE THE GAME

BANKS USED TO BE BUILT TO LAST.
TODAY, THEY NEED TO BE BUILT TO CHANGE.

In the age of the great customer experience, customers have high expectations – and the expectations keep increasing. Today's bank customers expect to engage meaningfully with their financial services provider using channels and touchpoints that best suit them, when it suits them. In this context, a new breed of banks - neobanks - has emerged as a disruptive force that threatens to turn the entire banking industry on its head.

Christian Sarafidis, *Senior Director Business Strategy Financial Services at Microsoft*

These neobanks – also called digital-only banks, online banks or mobile banks - offer a unique digital banking experience that is difficult to match for traditional, brick-and-mortar financial institutions.

The term neobank became prominent a few years ago to describe FinTech providers challenging traditional banks. Simply put, a neobank is a 100% digital direct bank that reaches customers on mobile apps and personal computer platforms only. Not operating traditional physical branch networks unburdens them from the legacy systems and processes that incumbent players must maintain.

In return, these newcomers must find ways to stay at the forefront of agility and flexibility, get to market faster, develop their customer base, and ultimately serve their customers better. And this is where public cloud platforms such as Microsoft Azure come in. **Christian Sarafidis**, Senior Director Business Strategy Financial Services at Microsoft, explains why and how the public cloud can provide the neobanks with the modern tooling and innovation capabilities they need to develop new business models.

> “ Microsoft has committed to build a cloud platform the financial services industry can trust

IN THE PAST, FINANCIAL REGULATORS HAVE SHOWN CONCERNS ABOUT BANKS USING THE PUBLIC CLOUD FOR CUSTOMER DATA, DUE TO PERCEIVED PRIVACY AND DATA PROTECTION RISKS. THEY ALSO WORRIED ABOUT THE IMPLICATIONS OF SO MUCH DATA BEING CONCENTRATED IN THE HANDS OF A FEW GLOBAL TECH GIANTS. WHAT IS THE CURRENT SITUATION REGARDING THESE MATTERS?

C.S. Financial institutions are facing three major forces of change: rising customer expectations, advancement in technology, and regulatory scrutiny. Artificial intelligence can help financial institutions as they face the challenges they are confronted with. AI can enable the transformation of critical business functions, from helping financial organizations fully understand their customers to identifying fraud and security breaches more quickly and efficiently, and to offering new innovative services to their clients.

While AI obviously presents game changing opportunities for financial institutions, it's also critical to understand and manage the privacy and data protection-related risks. It's up to technology providers to ensure that those risks are managed.

To support the financial services industry in its data and privacy protection risks, Microsoft has made a commitment to build a cloud platform they can trust. By listening to

> “ The cloud has allowed us to create sophisticated tools to guard against attackers

the concerns and objectives of financial regulators and by building a comprehensive contractual framework compliance program that reflects our engagements in terms of transparency, liability, and obligations specific to the industry, we are able to address data and privacy protection concerns and provide a high level of security and resilience, becoming a partner that neobanks can trust.

FOR A LONG TIME, SECURITY WAS THE MOST OFTEN-CITED REASON FOR JUSTIFYING BANKS' RELUCTANCE TO ADOPTING PUBLIC CLOUD STRATEGIES. TODAY, THE POSITION TOWARDS DATA SECURITY IN THE CLOUD OF THE BANKS AND THAT OF THE SUPERVISORY AUTHORITIES THEY ANSWER, TO SEEMS TO HAVE EVOLVED IN A POSITIVE DIRECTION. WHAT ARE THE REASONS FOR THIS CHANGE OF ATTITUDE?

C.S. For financial institutions, the security management paradigm has completely shifted. The traditional perimetric defense that many financial institutions still rely on, is not sufficient anymore to protect their data from the new cyber risks.

With the rise of data input to the cloud, we have also ushered in a new era of cybersecurity. On the one hand, individuals and companies

have had to give up a measure of physical control, but on the other hand, the cloud has allowed us to create much more sophisticated tools to guard against increasingly cunning attackers. That means that instead of banks having to manage security completely on their own, they also can rely on cloud service providers who have only one job – to keep their data secure.

> “ The possibilities of the cloud are endless

At any point in time on any day of the week, Microsoft's cloud computing operations are under attack: The company detects a 1.5 million attempts a day to compromise its systems. We aren't just fending off those attacks. We are also learning from them. All those foiled attacks, along with data about the hundreds of billions of emails and other pieces of information that flow to and from our cloud computing data centers, are constantly being fed into an intelligent security graph. This graph is a massive web of data that can be used to connect the dots between attacks from across the globe, thwarting one attack for one customer and applying that knowledge to every customer.

HOW CAN PUBLIC CLOUD SERVICES HELP NEOBANKS TO BENEFIT FROM SUPERIOR FLEXIBILITY AND SCALABILITY?

C.S. For financial services organizations, success in the coming decade will depend on how well they transform "business as usual" with technology to create new value, becoming indispensable partners in increasingly interdependent networks and complex value chains that cross business and industry boundaries. To get there, they must embrace entirely new business models that combine agility and security in dynamic tension, with trust at the center. And this goes for all segments of the industry - from retail to wholesale banking, and from neobanks to wealth management services.

The cloud can help the finance sector do just that. The possibilities are endless. What if a bank combined data from multiple sources to predict when a small business would need to expand and proactively extended credit? Or, what if a bank used telemetry, biometrics, and AI-powered facial recognition to immediately identify a customer and offered customized products and services? Customers are looking for an intuitive experience - a partner who understands their needs and offers anticipatory assistance.

Financial institutions, including the neobanks, are using cloud services primarily for the development of new business models. They bring business value in different ways: scalability and cost optimization by transforming the management of the technical resources, flexibility, and speed to market by empowering developers with modern tooling and innovation capabilities, from big data to artificial intelligence.

Adopting secure and scalable solutions allows for advanced analytics and augmented intelligence capabilities - simultaneously removing inefficiency and permitting greater customization and improved customer experience. With such capabilities, regulatory complexity can be managed and threats such as fraud, money laundering, and cybercrime detected and suppressed.

> “ McKinsey estimates there are 5,000 startups worldwide offering new and traditional financial services, up from 2,000 just three years ago **Forbes**

Two major conditions need to be addressed to succeed in the cloud adoption journey: the transformation of the workforce mindset by moving from traditional operating models to digital ones, and the risk management transformation by including the modern security principles and controls.

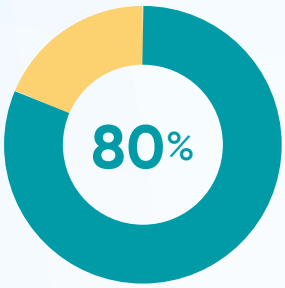
TO WHAT EXTENT CAN THESE SERVICES ALLOW DIGITAL-ONLY FINANCIAL INSTITUTIONS TO STREAMLINE THEIR OPERATIONS AND BOOST THEIR EFFICIENCY?

C.S. Cloud computing offers all businesses increased efficiency, flexibility, and cost-savings. Companies don't need to spend as much on equipment, infrastructure and software and only use the amount of cloud services that they need. The pay-as-you-go model, combined with other advantages such as scalability, enhanced security and flexibility of workplace, have transformed the cloud into an invaluable asset for businesses across the globe and sectors. What I find an extremely interesting bonus for financial institutions is the opportunities that it provides for blockchain.

The financial services industry is fundamentally about facilitating the trusted exchange of value between multiple, untrusting parties. Brokering that trust is an enormous responsibility and carries significant risk, which is why the industry has had to adopt multi-factor authentication processes over the years that have become increasingly costly, manual and error-prone. Over the past years, blockchain has emerged as a viable technology for addressing multi-party business processes and value exchange without complex shared data schemes and third-party intermediaries.

> "Cloud computing provides interesting opportunities for blockchain

At its core, a blockchain is a secure, shared, distributed ledger - a new shared data structure where banks can record transactions and work together to validate updates. Smart contracts act as a shared tool to govern changes to the underlying ledger in accordance with pre-agreed rules or terms. This shared record enables organizations to collaborate more efficiently, and because every member of the network holds a record of every transaction, it is nearly impossible to manipulate data undetected.



By 2030, 80 percent of heritage financial services firms will go out of business, become commoditized or exist only formally but not competing effectively

Gartner

While cryptocurrencies like Bitcoin were responsible for popularizing blockchain technology, blockchain protocols with business-oriented uses are now proliferating, revealing the value of this innovative technology to disrupt business models and transform operations. This offers financial institutions three key benefits: risk mitigation, cost reduction and improved customer outcomes.

CHECK POINT

WORKING IN THE CLOUD WITH CONFIDENCE

Peter Sandkuijl, *Security Engineer Director EMEA, Check Point Software Technologies*

Digital transformation has reshaped enterprise IT as we knew it. The ease and availability of the cloud provides businesses with dynamic options for developing and deploying services and applications at a fast pace. These advances drive business performance, but they have also resulted in security that just can't keep up. We held a discussion with Peter Sandkuijl, Security Engineer Director EMEA at Check Point Software Technologies, on how to secure cloud environments at scale, provide protection to IoT networks, and in what way AI actually helps improve an organization's security posture.

1. There is no question that cloud computing offers numerous advantages to those who adopt it, not the least of which being lower cost, faster time to market, and increased worker productivity. However, the security of data in the cloud is a key concern for IT departments. What are the specific risks associated with cloud computing and how do you address them?

P.S. Cloud computing is all around us and there is no doubt it comes with a large amount of opportunity and promise. For the last five years, we have been closely following this movement, applying dedicated resources to better understand customer needs and tooling. Cloud providers speak about a shared responsibility model, whereas a better term would be a split responsibility model. The cloud provider takes care of the infrastructure, but the applications and data storage you run on top is your sole responsibility.

Next to the traditional security topics to be addressed such as access control, intrusion prevention and other advanced threat prevention technologies, new challenges have arisen. Since the move to the cloud is often not handled by the traditional network and security team, we have a different audience to speak to. Who knew the term DevSecOps five years ago? They have different KPI's and don't necessarily have the same security background that we can assume when talking to the former group. This brings us back to the need to discuss why dedicated and focused security technologies are required rather than using native controls only.

> " Next to the traditional security topics, new challenges have arisen

Next to that, we also see new needs as we are no longer in full control of the infrastructure. That means a focus on cloud security posture management, for instance, or CPSM which continuously monitors the state we expect the cloud compute to be in. This will help ensure least privileged accounts and access, the need to have data encrypted, specific version control and such like. Check Point offers a lot of canned checks - i.e. GDPR and PCI - and reports but also offers a user-friendly language to write one's own checks.

Lastly, as everything gets automated, traditional change management procedures go out of the window and security has to become an integral part of the deployment cycles. All of this has to be applied in cloud technology in on-premise and public cloud deployments. More often than not, we see multi-cloud deployments and this is where we offer a lot of value: the ability to create a consistent implementation of appropriate security across any environment, cloudy or not cloudy.

2. In 2025, more than 24.9 billion Internet of Things connections are forecasted, compared to the estimated human population of 8.1 billion people. The future of IoT has the potential to be limitless. This potential is not just in enabling billions of devices simultaneously but also and above all in leveraging the huge volumes of actionable data that can automate diverse business processes. On the other hand, due to their inherent vulnerability and growing use, IoT devices also extend the attack surface. What do you recommend to better protect IoT devices, networks and data?

P.S. The numbers vary depending on the research you read: in our recent press release on this topic we mentioned 41 billion. The fact remains that they are so high that traditional approaches alone will not be enough. With the introduction of Check Point IoT Protect, we allow our customers to address the key topics. We roughly see the needs segmented across traditional industrial control systems, building automation and healthcare. From IP cameras to smart elevators, medical devices and industrial controllers, many IoT devices are inherently vulnerable and easy to hack. The challenge lies in their diversity and sometimes limited control over the actual application or OS. With the sheer volume of devices, focus is shifting towards discovery, automatic categorization and having the security solution suggest a security policy. The discovery is performed by partners and we created an API to allow a continuous update of the currently live devices.

Consuming this information bridges the gap between the teams deploying these devices and the teams managing security in IT networks. It even allows a seamless integration without any human interaction, providing zero day protection from the get go. This decreases the need for policy changes and allows for the addition of ThreatCloud intelligence around the vulnerabilities surrounding these devices. Doing this provides both an overview of exactly what a customer is operating, a graphical overview of how that relates to their IT network, in addition to a fine grained policy as to expected behavior and enforcement of that.

3. While cyber attacks continue to evolve at an accelerating pace, threats have become more sophisticated and dangerous compared to just a few years ago, making it impossible for human-created models to provide comprehensive and up-to-date protection. This is where advanced technologies such as artificial intelligence, machine learning or deep learning come into the equation, helping under-resourced security operations analysts fight the new generations of threats. How does Check Point leverage advanced technologies to strengthen its cyber security solutions?

P.S. Personally I started in this market in 1995, so I have seen many evolutions pass by. In recent years, both the way we publish and consume applications, and how we need to secure them, has changed faster and faster. We actually started categorizing them into five generations; on average, we see that enterprises are running behind two generations. Doing what we did before will not mitigate that or close the gap. Check Point has been collecting threat information for many years and is making that available as a service through an online portal called ThreatCloud.

It's important to highlight here this crosses platforms such as regular gateways, cloud based security, SaaS environments up to endpoints and mobile devices. Correlation is a keyword to analyze everything we learn and technologies such as machine learning - the market likes calling this AI - are key. It's not a single technology however; we use up to 64 technologies to ensure our hit rate is high with the least amount of false positives possible. We frequently get tested on that by external organizations such as NSS Labs. For a customer, after all, this is not a one-time prize. This is about continuously enabling and securing business operations.

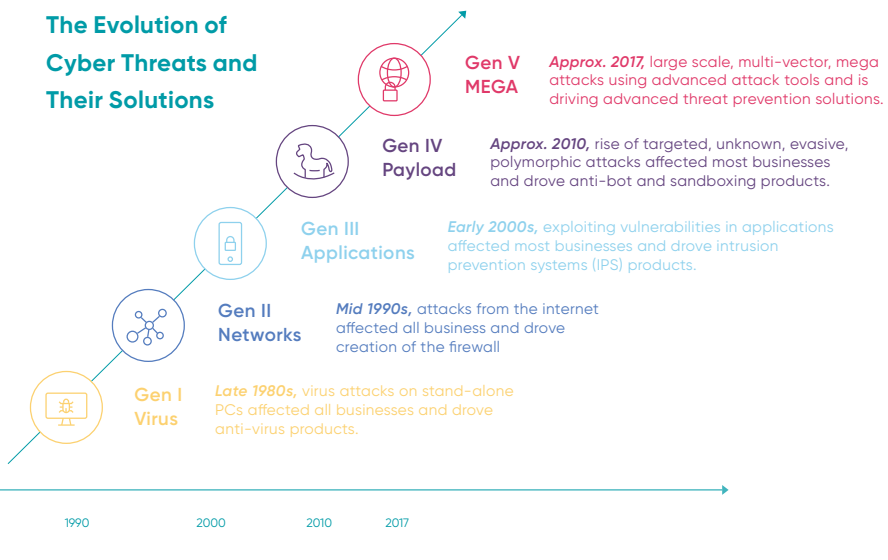
> “ Many IoT devices are inherently vulnerable and easy to hack

4. Now that they have overcome the worst effects of the Covid-19 crisis, organizations of all shapes and sizes are starting to return to some degree of normalcy. However, it appears that some of the measures adopted during the crisis – like the large-scale use of remote working – are here to stay. What is your view on the post-Covid cyber security landscape and what advice would you give an organization that seeks to navigate safely through the coming months and years?

P.S. First of all we cannot declare victory too early and I would urge each and every one to stay as safe and well as possible. Where lots of roadblocks have forcefully been removed, a lot of business leaders and executives have realized that there is opportunity in change and disruption, isn't there always? Once the pressure is off, things will go back to the "new normal". No-one actually knows what that looks like and what I have been telling both my teams as well as customers is the fact that it is up to us to shape that future. The forgiveness for things that happen right now will decrease, people will start physically meeting again. We are social animals and it's in our nature, and that is all good. I do expect that a new balance will be agreed upon, what it will look like will depend on each company.

> "We are digitally transforming and that is not simply lifting and shifting the datacenter to the cloud

With regards to working remotely, how we spend our time efficiently and run the business, this crisis has shown, on the plus side, that we can survive even when we work from home and hardly meet in person at all. That balance will attempt to get back to the center but never as far back as where it was. That will be a good thing. On a security level it should open the discussion about the fact that we are digitally transforming and that is not simply "lifting and shifting" the datacenter to the cloud. It's a cultural and technical change, and a big one at that. Further dissolving the perimeter as we think about it, we need to consider how to secure beyond that perimeter. This means how we do secure data, applications and identities on a plethora of devices, especially considering these live outside of our building and potentially outside of our managerial control. For instance, did we take any shortcuts on GDPR that we really need to address now? Connecting all the dots, providing continuous protections, while allowing our customers to sit in the driver's seat doing their business, is the promise we will deliver on.



Source: www.checkpoint.com

AFTER-WORD

THE TECHNOLOGY REVOLUTION

CHECK POINT
CloudGuard™

CLOUD WITH CONFIDENCE

CLOUD SECURITY SOLUTIONS

SECURITY - AUTOMATED - EVERYWHERE

The Check Point Cloudguard platform provides you cloud native security, with advanced threat prevention for all your assets and workloads — in your public, private, hybrid or multi-cloud environment — providing you unified security to automate security everywhere.

Advanced Threat Prevention

Advanced threat prevention for all your cloud assets

Automated Security

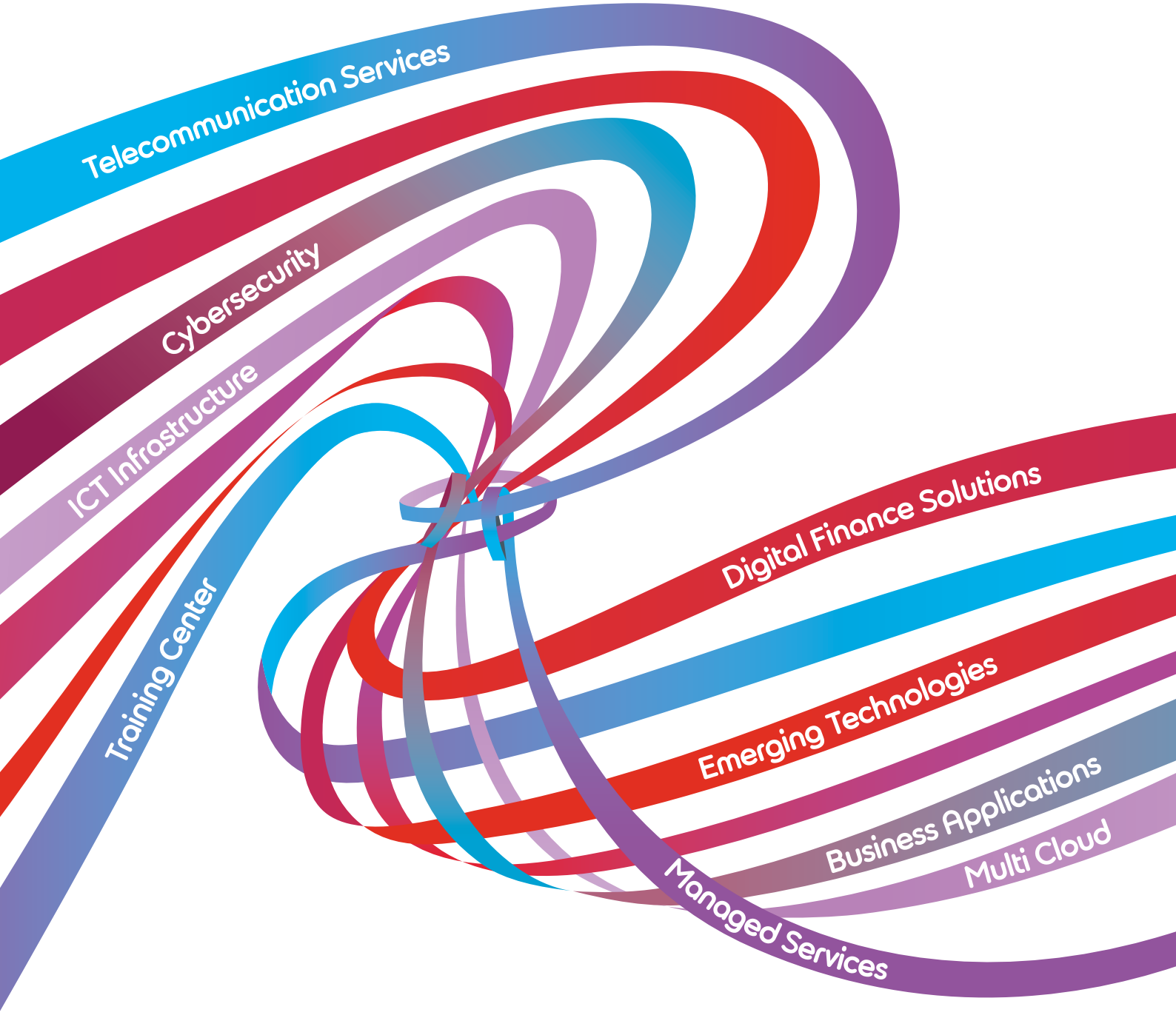
Automated security across your cloud environment

Unified Security for Multi-Cloud

Visibility & control across your entire multi-cloud environment

FOR MORE INFORMATION, A DEMO OR A FREE TRIAL, PLEASE VISIT:

www.checkpoint.com/solutions/cloud-security/



SHARE MORE THAN TECHNOLOGY

Since 1979, we accompany all organizations in their digital transformation, by providing holistic ICT & Telecommunication solutions, as well as tailored support services.

More than just technology, we share our passion and know-how to simplify, connect and secure your business.

www.telindus.lu

telindus