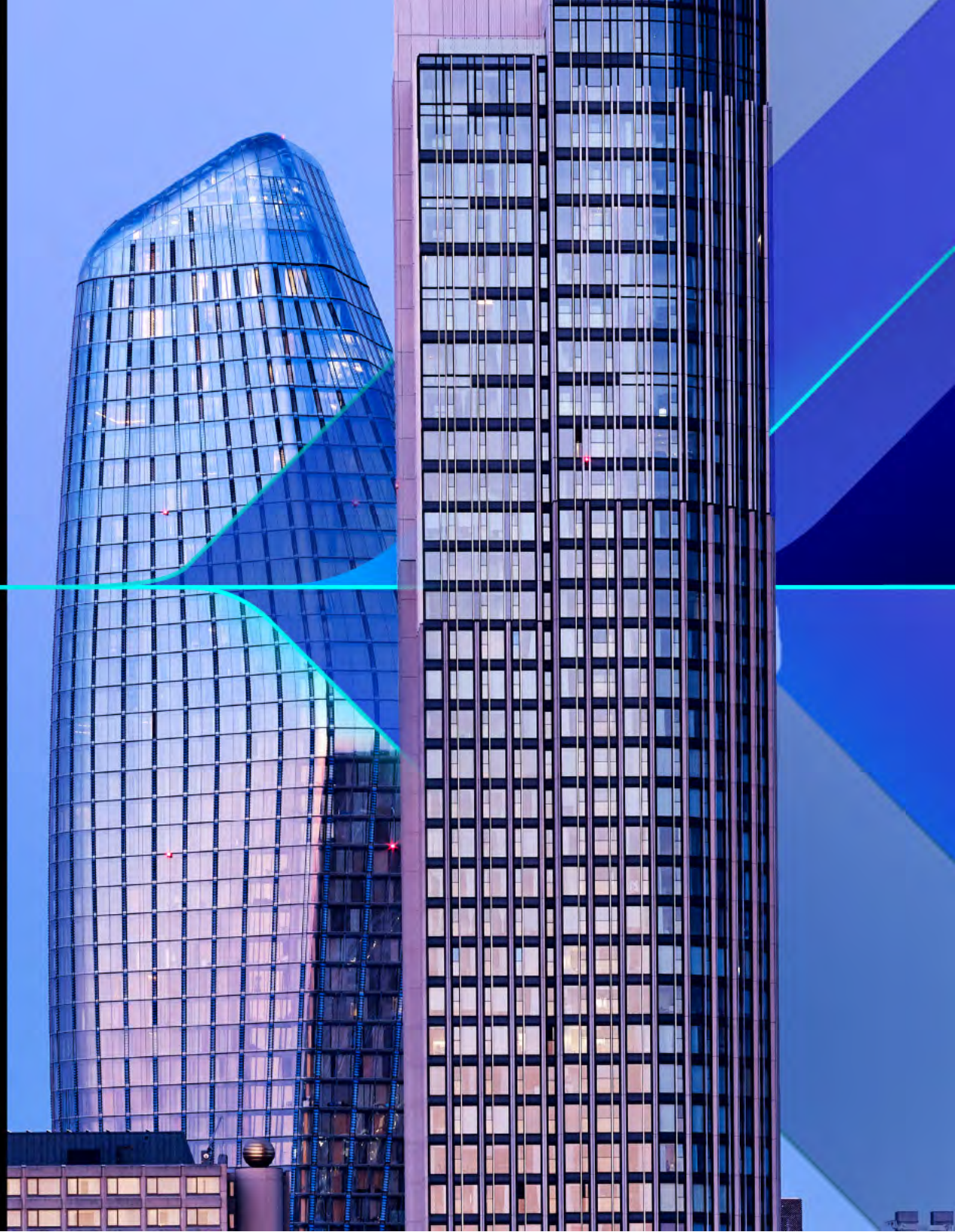
zscaler™

# ZSCALER

## POUR LES SERVICES FINANCIERS

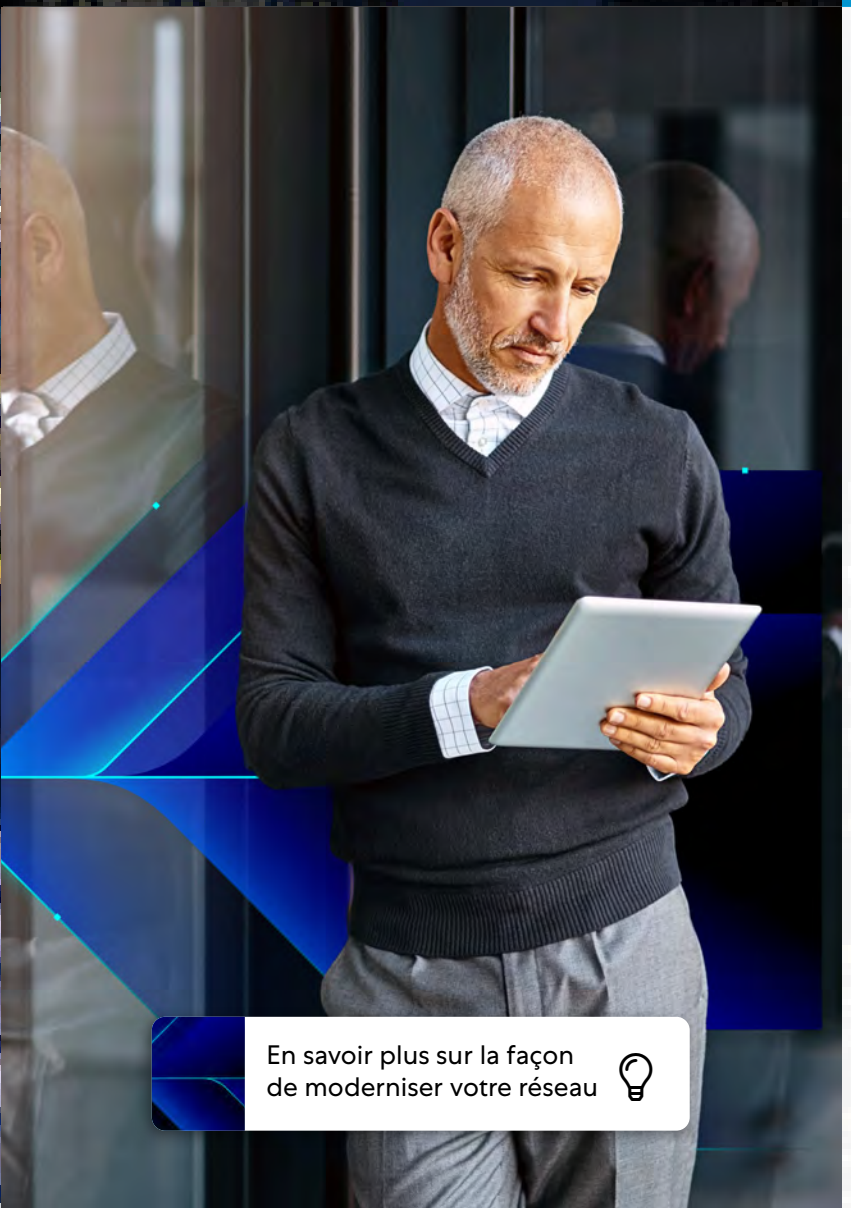


# SOMMAIRE



# 1 L'ÉVOLUTION RAPIDE DU PAYSAGE TECHNOLOGIQUE

Quels que soient les effets déstabilisants qui se produisent dans le monde, le baromètre le plus sensible, le plus quantitatif, et le plus pertinent de la situation mondiale reste la santé du secteur des services financiers.



En savoir plus sur la façon de moderniser votre réseau

**Pour pouvoir survivre et prospérer dans un paysage économique international en pleine mutation, le secteur a adopté une approche holistique et stratégique, en se réinventant et en adoptant de nouvelles plate-formes FinTech basées sur le cloud computing, l'ubiquité du mobile et les dernières avancées en matière d'automatisation de l'intelligence artificielle (IA).**

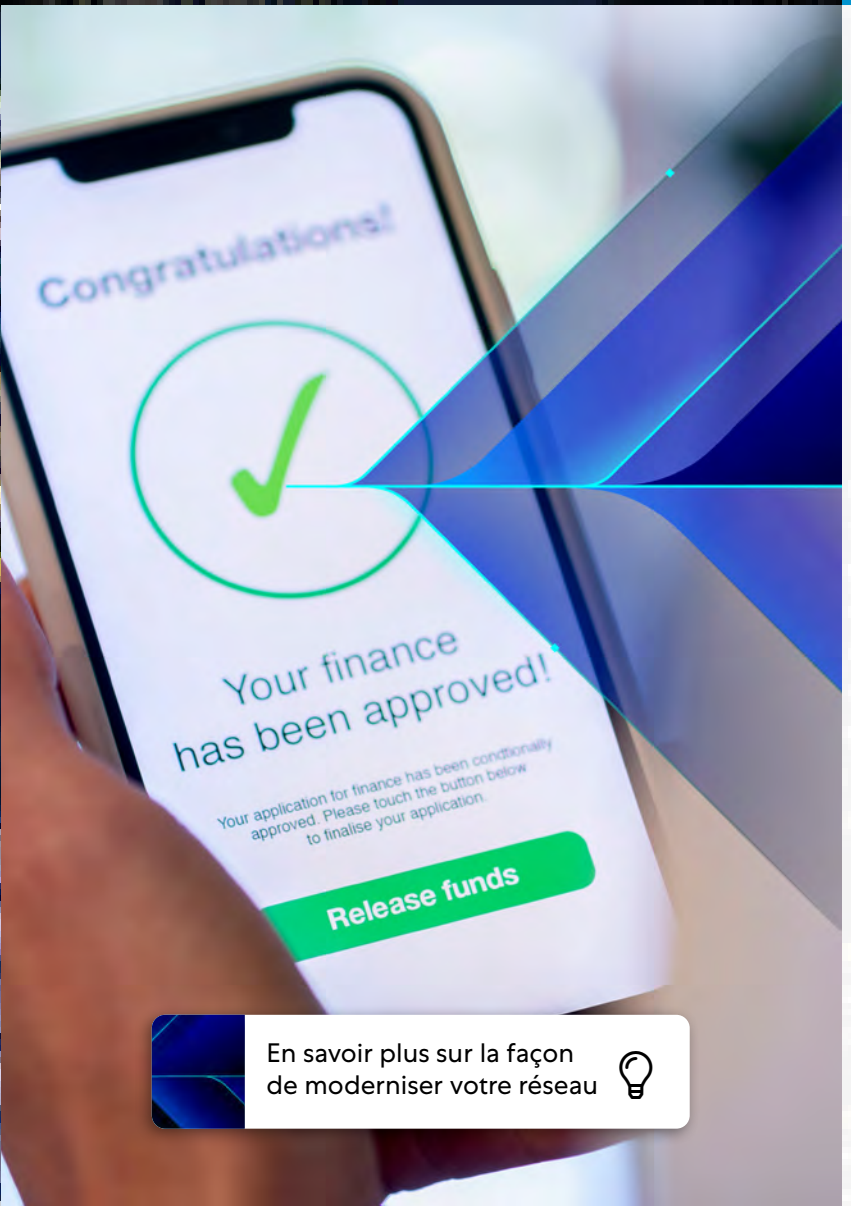
Jusqu'en 2020, les jeunes de la « génération Y » étaient les principaux adeptes des nouvelles technologies bancaires telles que les systèmes de paiement sans contact, mais la courbe d'apprentissage s'est considérablement stabilisée et élargie, toutes les tranches d'âge trouvant désormais pratique cette forme de paiement. L'ère du Coronavirus (COVID-19) a évidemment accéléré le passage à la banque en ligne et à une société sans argent liquide.

Dans le même temps, les avancées technologiques ont ouvert le marché à des concurrents perturbateurs 100% digital. C'est en droite ligne avec l'empressement des consommateurs à adopter le commerce électronique grâce à l'utilisation du smartphone et à un plus large usage des paiements électroniques que s'est développée l'expansion des banques « challengers », comme on les appelle.

Qu'il s'agisse d'une hypothèque, d'une police d'assurance, d'un plan d'investissement ou simplement d'un transfert de fonds et d'une opération normale sur son compte courant, l'exécution de ces tâches en mode numérique devient très rapidement la norme. Les changements ainsi que les circonstances imprévisibles du marché ont donné lieu à de nouvelles façons de faire, rendant les clients extrêmement exigeants ; ils attendent des services non seulement instantanés mais aussi optimisés et immédiatement accessibles.

# 2 L'ÉTAT DE LA TRANSFORMATION DIGITALE

L'innovation digitale et l'agilité commerciale sont essentielles pour attirer de nouveaux clients, accroître la part de marché et saisir les opportunités de croissance dans de nouveaux secteurs commerciaux.




**Mais au cœur de la plupart des entreprises financières matures se trouvent des systèmes centraux, souvent basés sur des technologies exclusives sur site qui ont été au fil des ans personnalisées en profondeur, créant de multiples dépendances et de nombreux niveaux de fonctions informatiques interconnectées. Citant les réglementations financières, les contrôles de gouvernance et les lois sur la confidentialité des données comme un autre inhibiteur clé de l'adoption du cloud, il est compréhensible que la plupart des entreprises de services financiers aient traîné la patte ou pris du retard pour tirer parti de l'efficacité et de l'agilité fournies par le cloud public.**

Depuis ses débuts, les organismes de réglementation financière ont établi des normes et des directives sur l'utilisation du cloud computing pour la sécurité et la confidentialité. Cela a permis au cloud de devenir un catalyseur de la conformité réglementaire, permettant aux institutions financières de développer des approches efficaces en matière de gestion des risques, d'intégrité et de confidentialité des données, sans pour autant freiner l'innovation.

Bien que la plupart des institutions financières vivent aujourd'hui dans un environnement hybride avec une certaine infrastructure obsolète, le cloud gagne progressivement le paysage informatique avec des plates-formes et des applications pour tout, de l'ERP aux données de marché, en passant par la recherche et le CRM, les garanties de vente, les études de marché et bien plus encore. Même les simples formations pour les qualifications de la FINRA ont été transférées en ligne et **la FINRA elle-même a transféré 100 % de ses propres applications vers le cloud.**

Selon une enquête menée par Zscaler auprès de 600 directeurs informatiques sur la région EMEA en 2020, la transformation digitale est en bonne voie dans le secteur des services financiers. De nombreuses entreprises ont désormais adopté une stratégie centrée sur le cloud, en s'appuyant sur plusieurs clouds publics et applications SaaS (Software as a Service) pour les solutions orientées client, les opérations de back-office et l'intégration avec des partenaires dans l'écosystème financier : le secteur bancaire, les fournisseurs FinTech, etc.

**L'enquête indique que deux tiers des entreprises ont transféré 50 % de leurs applications vers le cloud et un quart des entreprises ont transféré 75 % de leurs applications vers le cloud.**

En savoir plus sur la façon de moderniser votre réseau

# 3 LA TRANSFORMATION DIGITALE BIEN FAITE, LA TRANSFORMATION DIGITALE MAL FAITE

Au fur et à mesure que les services financiers évoluent des rues commerciales à la Toile, les fournisseurs sont confrontés au défi de devoir reproduire le même niveau de service client auparavant livré dans leurs filiales, dans un format en ligne.

**Afin d'atténuer le risque de perdre des clients, l'expérience client s'est hissée en tête de liste des priorités de l'entreprise pour la plupart des institutions financières. Lorsque les services sont fournis correctement et en toute transparence, le client en demande davantage, interagit davantage et investit potentiellement dans de nouveaux services. Si par contre les services sont mal assurés, lents et n'inspirent pas confiance... le client dès lors s'éclipse en un clin d'œil.**

Résolument tournées vers l'avenir et la concurrence émergente, les entreprises de services financiers progressistes se projettent d'ores et déjà vers les technologies basées sur la 5G, l'IA, la blockchain, l'automatisation des processus robotisés (RPA) et l'utilisation de plus en plus large de l'Internet des objets (IoT).

Les progrès réalisés dans l'adoption, la mise en œuvre et le déploiement de ces technologies ont été brusquement stoppés dans leur élan du fait de la pandémie du Covid-19, qui a eu à tous les niveaux un impact très perturbateur sur les stratégies de développement commercial et organisationnel. Partout, les entreprises ont été rapidement contraintes de changer de vitesse et de se concentrer sur la poursuite des activités. En l'espace de quelques jours, la plupart des départements informatiques ont relevé le défi et démontré leur maîtrise de la gestion de projet, en redéfinissant les priorités et en accélérant les projets qui ont permis aux économies locales et internationales de continuer à fonctionner. Des milliers d'employés basés dans des bureaux ou des filiales ont pu travailler à distance, tandis que les paiements sans argent liquide et d'autres formes de **processus fluides et à distance** ont été très rapidement déployés, parfois avant les délais de mise en service prévus.

En savoir plus sur la façon de moderniser votre réseau

# 4 L'INFRASTRUCTURE EXISTANTE – CATALYSEUR OU INHIBITEUR ?

Alors que les entreprises de services financiers ont réalisé d'importants progrès en adoptant le cloud et la mobilité dans le cadre de leur parcours de transformation digitale, l'évolution a posé plusieurs nouveaux défis.

**Les investissements existants, qui continuent de favoriser les opérations commerciales au quotidien, sont souvent pressurés jusqu'à leur durée de vie maximale afin d'obtenir le meilleur retour sur investissement. Le hic est que l'infrastructure en place n'a jamais été conçue pour répondre aux exigences transactionnelles, analytiques et procédurales du monde moderne mobile et tourné vers le cloud. C'est avec la pandémie que ces insuffisances ont été mises en évidence.**

Avant la crise, la plupart du personnel du secteur des services financiers était basé dans une filiale ou dans un bureau. Un pourcentage négligeable d'entre eux se déplaçaient pour des réunions sur le terrain ou travaillaient à domicile, se connectant aux systèmes bancaires et d'assurance centraux de l'entreprise via des VPN (Virtual Private Networks) ou des VDI (Virtualized Desktop Interfaces). Dans le sillage de la crise, les services informatiques ont dû faire face à un défi : permettre un accès distant sécurisé à un nombre record de télétravailleurs, bloqués à domicile.

Même si le personnel mobile pouvait toujours accéder aux systèmes d'entreprise et aux applications cloud, les VPN n'étaient pas conçus pour être utilisés par la majorité du personnel, ce qui obligeait le trafic à traverser une pile d'appliances comme les équilibreurs de charge, les DDoS, les pare-feux et les concentrateurs VPN. Le routage du trafic via le réseau existant et l'infrastructure obsolète ainsi qu'à travers de multiples appliances causait de la latence, la frustration des utilisateurs et une baisse de productivité. Dans le pire des cas, les employés contournaient les politiques de sécurité et les contrôles VPN, générant ainsi des failles de sécurité.

La technologie VDI a permis aux utilisateurs distants de se connecter aux principaux systèmes, à la messagerie électronique et à d'autres applications dans le cadre de l'utilisation du BYOD (Bring Your Own Device), ce qui a permis d'atténuer les problèmes classiques tels que l'exposition et le vol des données. Non seulement ces solutions sont manifestement difficiles à mettre en place et coûteuses à entretenir, mais elles ont également été utilisées de manière excessive et sont devenues un risque supplémentaire pour la sécurité durant la pandémie.

En savoir plus sur la façon de moderniser votre réseau

**En général, c'est par une infrastructure supplémentaire que les services informatiques résolvent un problème de rendement insuffisant au niveau du réseau. Ceci non seulement génère une complexité et un coût supplémentaires, mais également augmente les risques de sécurité. Au fur et à mesure que les entreprises dévalent la pente de 'voraces investissements', elles perdent en agilité, et deviennent autant moins innovantes que compétitives.**

**Au cours des derniers mois, cette tendance s'est accélérée en raison du Covid-19, amenant une majorité du personnel vers le télétravail et le secteur des services financiers à accélérer son déploiement de Microsoft 365.**

## DES POINTS FAIBLES SPÉCIFIQUES EN DÉCOULENT :

- Les solutions d'accès à distance basées sur les VPN n'ont pas été en mesure de fournir les niveaux de service requis par l'entreprise, générant de la latence et une médiocre expérience utilisateur
- L'accès à distance basé sur VPN qui place les ordinateurs distants sur le réseau d'entreprise est depuis longtemps considéré comme le principal vecteur d'infection des terminaux. L'expansion du télétravail n'a fait qu'envenimer la situation.
- Microsoft 365 est un protocole « bavard » qui nécessite une bande passante plus élevée et une plus faible latence afin d'offrir des niveaux de service acceptables.
- L'extension de l'architecture en étoile est très coûteuse et ne permet pas à terme d'obtenir les SLA nécessaires.
- L'extension de la surface des architectures de sécurité existantes rend les entreprises plus vulnérables, notamment aux attaques de chevaux de Troie, tout en ne protégeant pas complètement la menace interne.

De nombreux responsables informatiques reconnaissent que l'architecture en étoile n'est plus adaptée à l'environnement distribué cloud et mobile d'aujourd'hui, et qu'elle peine à prendre en charge les utilisateurs distants ou à démontrer une capacité d'évolution qui réponde à la croissance du trafic réseau. Mais ce n'est pas simplement les efforts et le coût de sécurisation de l'infrastructure ancienne qui rendent nécessaire la transformation de l'architecture ; le service informatique doit concevoir et mettre en œuvre une architecture qui sous-tend une multitude de nouvelles innovations dans des environnements divers, dynamiques et complexes.

L'objectif est de créer un monde digital capable de comprendre et de traiter le langage naturel, de rassembler des mégadonnées, d'identifier des modèles, d'interpréter, de percevoir, de raisonner et de conseiller en temps réel pour prendre en charge l'apprentissage guidé de nouvelle génération, la technologie opérationnelle, la robotique, les objets connectés et bien plus encore.

# 5 L'ART DE CONCILIER SÉCURITÉ ET EXPÉRIENCE UTILISATEUR

Les banques, les compagnies d'assurance et les autres organismes de services financiers sont bien sûr responsables de la possession et de la gestion de considérables sommes d'argent et d'informations financières de leurs clients.


**Face au défi en constante évolution de garder une longueur d'avance sur les criminels et de respecter de strictes réglementations financières, il n'est pas surprenant que les entreprises financières se retrouvent parmi les plus gros investisseurs en cybersécurité.**

Les nouveaux développements digitaux créent des opportunités pour les criminels qui sont prêts à exploiter des vulnérabilités. En quelques secondes, un personnel répondant à un e-mail d'hameçonnage peut voir ses informations d'identification compromises et faire l'objet d'une violation de données, d'une attaque de ransomware voire les deux. Mais il faut trouver un équilibre. Comment transmettre de manière rentable et en toute sécurité les processus et applications essentiels de l'entreprise à un personnel mobile et distant, sans compromettre l'expérience utilisateur ?

De multiples étapes de sécurité peuvent ajouter beaucoup de frictions à l'expérience utilisateur. Cela peut frustrer autant les clients que les employés et porter un coup à la productivité. Les responsables des services informatiques reconnaissent qu'ils ont une mission d'offrir la sécurité et l'expérience utilisateur à la fois, mais qu'il est difficile d'atteindre ces deux objectifs ensemble.

En savoir plus sur Zscaler Zero Trust Exchange

# 6 CONCILIER SÉCURITÉ ET EXPÉRIENCE UTILISATEUR AVEC UNE APPROCHE **SASE ET ZERO TRUST**

Le modèle SASE (Secure Access Service Edge) est un modèle de sécurité défini par Gartner dans l'optique spécifique de répondre aux défis de sécurité que suscitent les applications, les appareils et les utilisateurs fonctionnant en dehors du périmètre traditionnel du réseau.

En savoir plus sur Zscaler Zero Trust Exchange

**L'architecture SASE combine des fonctionnalités WAN complètes et des fonctions de sécurité réseau telles que Secure Web Gateway, CASB, le pare-feu de nouvelle génération et ZTNA (Zero Trust Network Acess) pour répondre aux besoins dynamiques d'accès sécurisé des entreprises digitales.**

Contrairement à l'accès réseau traditionnel, les processus opérationnels adaptatifs de Zero Trust établissent des connexions et accordent l'accès en fonction de l'utilisateur, de l'appareil, de l'emplacement et de l'application, offrant un accès rapide et sécurisé aux utilisateurs autorisés, peu importe leur position géographique et sans placer les utilisateurs sur le réseau. Avec ZTNA, le Web devient un transport non fiable et l'accès aux applications se fait par le biais d'un service cloud intermédiaire contrôlé par un fournisseur tiers ou un service auto-hébergé.

Puisque ce modèle élimine la nécessité d'un matériel et de processus VPN traditionnels encombrants, il crée pour l'utilisateur un processus fluide ainsi qu'une meilleure expérience globale.

ZTNA fournit un accès contrôlé aux ressources, améliore la connectivité et supprime la nécessité d'exposer directement les applications à Internet, ce qui réduit la surface d'attaque. Cette solution a été largement adoptée face à la pandémie, permettant aux travailleurs à distance et à domicile d'accéder aux applications essentielles avec le même niveau de contrôle de sécurité que les travailleurs basés au siège de l'entreprise. À ce jour, ZTNA est rapidement en train de devenir une norme de bonne pratique que les entreprises adoptent dans toute leur activité. Que les utilisateurs accèdent au data center, aux applications privées ou au cloud public, qu'ils soient au bureau ou en télétravail, l'expérience sera identique.

## ZERO TRUST EXCHANGE

Zero Trust Exchange est la plate-forme SASE de Zscaler spécialement conçue et basée sur le cloud, qui connecte en toute sécurité les utilisateurs, les appareils et les applications en utilisant des politiques de sécurité d'entreprise sur n'importe quel réseau. Rapide, sécurisée et évolutive, elle équilibre les priorités de sécurité de l'entreprise avec l'expérience utilisateur pour faire du cloud et d'Internet un endroit sécurisé pour la gestion des affaires.

# 7 POURQUOI ZSCALER ?

Qu'il s'agisse de développer de nouvelles solutions bancaires qui fonctionnent avec la cryptomonnaie, de nouveaux services transfrontaliers, de limiter les fraudes ou de gérer de nouveaux processus de conformité réglementaire, les entreprises de services financiers doivent mettre en œuvre leur stratégie à l'aide d'une plate-forme moderne, robuste, agile et évolutive qui permet à l'entreprise d'être à jour en matière d'innovation et d'atténuer la concurrence.


En savoir plus sur Zscaler Zero Trust Exchange

**Avec plus de dix années d'expérience et répartie sur plus de 150 data centers à travers le monde, Zero Trust Exchange, la plate-forme de Zscaler basée sur le modèle SASE, est la plus grande plate-forme de sécurité cloud au monde, bloquant plus de 100 millions de menaces par jour. La plate-forme traite plus de 150 milliards de transactions et 175 millions de mises à jour de sécurité par jour, soit 10 fois plus le nombre de recherches Google par jour dans le monde.**

Zscaler a fait ses preuves dans le secteur des services financiers avec plus de 500 clients, six des dix plus grandes banques américaines, sept des dix plus grandes banques européennes et deux des cinq plus grandes banques australiennes soutenant leur infrastructure bancaire avec Zero Trust Exchange de Zscaler. Globalement, Zscaler est un partenaire de confiance pour 5 000 clients dans 185 pays, dont 500 des meilleures entreprises du classement Forbes 2000.

Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte de données en connectant en toute sécurité les utilisateurs, les appareils et les applications, peu importe leur emplacement, grâce à des politiques de sécurité d'entreprise.

Au nombre des principaux avantages de la plate-forme, évoquons sa capacité à superposer l'architecture existante pour instantanément accélérer la transformation digitale et fournir des services efficaces, sécurisés, centrés sur le client et évolutifs :

- **Efficace :** simplifie l'informatique, réduit la complexité et les coûts.
- **Sécurisé :** améliore la résilience et la posture de sécurité, atténue les risques de perte de données et de sécurité grâce à une vue unique de la posture de sécurité sur plusieurs divisions.
- **Centré sur le client :** prend en charge l'environnement du télétravail, augmente la capacité, réduit la latence et crée une expérience utilisateur cohérente pour améliorer la productivité.
- **Évolutif :** une plate-forme moderne et agile qui sous-tend l'innovation digitale, accélère la transformation digitale et crée une capacité de croissance.

La NAB (National Australia Bank) offre une gamme complète et intégrée de produits et services bancaires et financiers, y compris la gestion de patrimoine, avec des opérations en Australie, en Nouvelle-Zélande, dans certaines parties de l'Asie, au Royaume-Uni et aux États-Unis.

## Steve Day

National Australia Bank,
Melbourne, Australie

nab.com.au

**Face au confinement consécutif au COVID-19, la banque devait rapidement permettre au personnel d'adopter le télétravail tout en continuant à fournir des services à plus de 9 millions de clients.**

« Avant la pandémie du Covid-19, nous n'avions jamais eu plus de 5 000 de nos employés travaillant à distance », a déclaré Steve Day, EGM Infrastructure, Cloud & Workplace chez NAB. « Nous devions trouver rapidement un moyen d'équiper le personnel du centre d'appels afin qu'il puisse traiter les appels depuis le domicile et accéder à distance à nos applications et à nos entrepôts de données », a-t-il déclaré. « Tout ceci en gérant quatre fois plus de volumes d'appels qu'à l'accoutumée ».

En collaboration avec Zscaler, la NAB a fourni un accès distant sécurisé à plus de 32 000 employés, y compris les équipes du centre d'appels, en seulement trois semaines. La NAB a adopté Zero Trust pour réduire à la fois les coûts et la surface d'attaque, tout en créant une infrastructure qui prendrait en charge les opérations futures.

« Zero Trust présente deux avantages majeurs. Tout d'abord, nous n'avons plus besoin de gérer un réseau d'entreprise distinct, ce qui permet de réaliser d'importantes économies. Dans le nouveau modèle, nous proposons uniquement un accès à l'Internet public dans nos bureaux. Deuxièmement, nous avons renforcé notre dispositif de sécurité, non pas en installant davantage d'infrastructures de sécurité plus coûteuses, mais en supprimant toutes les données et applications de l'environnement de l'entreprise afin de réduire notre surface d'attaque. Nous disposons désormais d'une infrastructure réseau sécurisée qui peut prendre en charge la NAB pendant la crise actuelle de même que lorsque les opérations reviendront à la normale ».

« Les gens rentrent chez eux, allument leur PC et travaillent exactement de la même manière qu'au bureau. Ils n'ont pas à se soucier d'étapes de connexion supplémentaires ou à gérer des jetons de sécurité - tout fonctionne tout simplement », a déclaré Steve Day, EGM Infrastructure, Cloud & Workplace.

# 8 FUSIONS ET ACQUISITIONS

Les fusions, acquisitions et cessions sont courantes dans le secteur des services financiers, mais constituent un défi pour les équipes réseau et de sécurité chargées de garantir la connectivité des utilisateurs aux applications internes et la sécurité des données sensibles.

**La convergence de réseaux disparates, la gestion d'adresses IP qui se chevauchent et la création de normes de sécurité cohérentes ne sont que quelques exemples des défis auxquels les services informatiques sont confrontés. Les projets demandent beaucoup de temps et de ressources, et leur réalisation prend souvent des mois, voire des années.**

La vitesse, la sécurité et l'expérience utilisateur sont primordiales lors de ces transitions complexes. En travaillant avec Zscaler, les entreprises peuvent énormément simplifier les projets de fusions, acquisitions et de cessions :

- Déployer simplement des logiciels et orienter les utilisateurs vers des applications en quelques minutes sans la moindre convergence des réseaux.
- Sécurité standardisée pour tous les actifs. Les applications ne sont visibles que pour les utilisateurs autorisés et les utilisateurs ne sont jamais sur le réseau.
- Les utilisateurs bénéficient d'une expérience d'accès cohérente, quel que soit le périphérique, l'application ou le lieu.

En savoir plus sur Zscaler Zero Trust Exchange

# 9 À QUOI S'ATTENDRE AVEC LA TRANSFORMATION DIGITALE ?

Si les entreprises financières ont pu réagir rapidement à la pandémie, les équipes chargées de l'informatique et de la sécurité jettent un œil au rétroviseur pour s'assurer qu'elles se sont bien adaptées à la nouvelle norme.

Explorez d'autres ressources sur le télétravail

**Une fois les solutions temporaires prises en compte, l'attention se tournera vers la prochaine étape du parcours de transformation digitale. Il est primordial de construire une infrastructure moderne pour soutenir l'innovation future.**

À mesure que la 5G se déploie et que le secteur des services financiers adopte davantage de technologies opérationnelles, la robotique de pointe, des dispositifs mobiles et d'autres innovations centrées sur le client, de nouveaux défis et de nouvelles vulnérabilités en matière de sécurité apparaissent. La cybersécurité restera l'un des principaux risques auxquels sont confrontées les institutions financières.

Au fil du temps, il devient de plus en plus important de s'associer à des fournisseurs d'infrastructure fiables, qui non seulement sont bien équipés pour répondre aux demandes modernes, mais qui ont également la vision et la capacité de piloter et de porter vers le haut les entreprises financières à l'échelle mondiale.

Nous avons demandé aux leaders informatiques visionnaires quelles étaient les prochaines étapes de leur parcours de transformation digitale ?

# 10 POURQUOI AGIR MAINTENANT ?

Il est très coûteux de ne rien entreprendre, qu'il s'agisse d'une simple augmentation des coûts d'infrastructure et de MPLS, d'une perte de productivité ou du coût pour se remettre d'une cyberattaque.

**En agissant maintenant, votre entreprise peut immédiatement améliorer sa posture de sécurité et bénéficier d'une vision unique sur la sécurité dans toute l'entreprise, tout en implémentant efficacement la nouvelle norme du télétravail.**

Dans le même temps, les investissements informatiques deviennent tournés vers l'avenir et sont canalisés vers une nouvelle architecture évolutive qui peut accélérer les priorités et les nouvelles innovations.

## CONFORMITÉ RÉGLEMENTAIRE

Les autorités bancaires indépendantes s'efforcent de garantir une réglementation et une surveillance efficaces et cohérentes du secteur des services bancaires et financiers. Ces organismes, avec la contribution d'entreprises leaders du secteur, ont élaboré des conseils et des recommandations sur l'adoption des technologies cloud, le processus et la pratique de l'externalisation vers des fournisseurs de services cloud (CSP) et l'adoption d'une approche basée sur des principes pour gérer et mesurer les risques dans les environnements de technologies cloud.

Zscaler s'engage à aider ses clients dans leur démarche de conformité en leur fournissant une sécurité et une protection de la vie privée solides, et en les aidant à répondre aux obligations réglementaires actuelles et émergentes en matière de risque. Zscaler fournit des informations transparentes et un soutien en matière de meilleures pratiques pour garantir que le déploiement et la gestion des solutions Zscaler respectent le cadre de gouvernance.

Explorez d'autres ressources sur le télétravail

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com