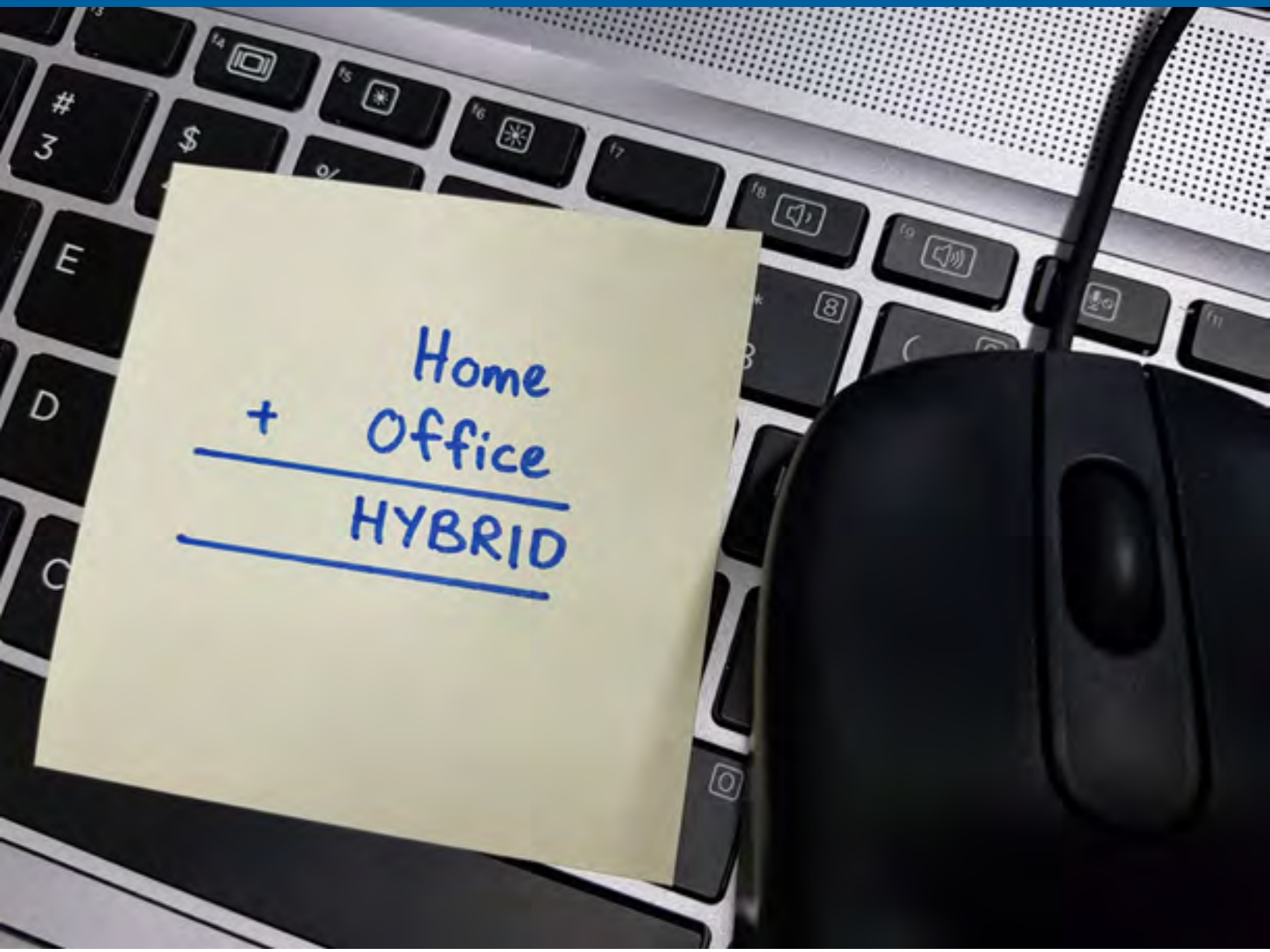
Protéger votre personnel hybride avec une approche Zero Trust

Découvrez comment une stratégie Zero Trust peut protéger plus efficacement l'environnement de travail hybride



RAPPORT DE RECHERCHE DE HMG STRATEGY SOUTENU PAR ZSCALER

HMG STRATEGY

zscaler™

NOTE DE SYNTHÈSE

Lorsque le monde a changé en mars 2020, les RSSI et les équipes de sécurité de l'information se sont retrouvés confrontés à une multitude de nouveaux défis. Alors que des millions d'employés ont soudainement commencé à travailler à domicile, toute notion restante basée sur des entreprises ayant un périmètre défini à défendre a été écartée.

Alors que la pandémie mondiale progressait et que la plupart des équipes des entreprises ont continué à travailler à distance, il est également devenu évident que les architectures réseau existantes ne suffisaient plus à protéger les employés et les entreprises sur un lieu de travail extrêmement distribué. Parallèlement, la migration des applications du data center au cloud et aux plateformes SaaS, s'est accélérée à un rythme sans précédent et continue d'augmenter. Une étude menée par O'Reilly Media révèle que 48 % des entreprises prévoient de migrer 50 % ou plus de leurs applications vers le cloud en 2022 [1].

À ces défis d'un personnel hybride s'ajoute l'augmentation des problèmes de sécurité associés aux appareils personnels non gérés dans un contexte de télétravail. La dépendance permanente à l'égard des réseaux privés virtuels (VPN) a exposé de nombreuses entreprises.

Ce ne sont là que quelques-unes des raisons pour lesquelles la majorité des RSSI et des responsables de la sécurité des entreprises adoptent des architectures modernes de Zero Trust pour renforcer leurs défenses et protéger l'entreprise de bout en bout.

« *L'un des principaux atouts d'une méthodologie Zero Trust est la faculté d'adapter vos contrôles de sécurité aux niveaux de risque spécifiques et à la hiérarchisation de chaque cas d'utilisation* », a déclaré **Lisa Lorenzin**, directrice technique, Amériques, chez Zscaler. « *Avec une solution Zero Trust moderne, vous pouvez le faire à un niveau d'abstraction approprié. Vous pouvez appliquer ces contrôles inline pour un utilisateur se connectant à une application, plutôt que pour un terminal se connectant à un réseau.* »

À mesure que les entreprises étendent leurs empreintes numériques et étoffent leurs portefeuilles de produits et services numériques, une architecture Zero Trust est indispensable pour protéger toutes les couches du modèle économique numérique d'une organisation. **Cela explique en partie pourquoi 61 % des RSSI et des responsables de la sécurité des entreprises pensent qu'un modèle de sécurité Zero Trust constitue une approche efficace pour sécuriser l'écosystème numérique d'une entreprise**, selon une enquête récente menée par HMG Strategy et Zscaler auprès de 118 responsables de la sécurité.

HMG Strategy s'est associé à Zscaler pour mieux comprendre comment le paysage des menaces a évolué depuis que les entreprises sont passées à des espaces de travail hybrides, où ces vulnérabilités critiques existent, et pour appréhender les avantages et les opportunités de l'application d'une architecture Zero Trust. Dans ce rapport de recherche détaillé, vous découvrirez les sujets suivants :

- Principaux risques et défis de sécurité associés à l'environnement de travail hybride
- Pourquoi les architectures actuelles sont insuffisantes pour protéger l'entreprise, ainsi que les pertes économiques qu'elles génèrent
- Récents exemples d'attaques par ransomware et de violations de la sécurité du réseau
- Urgence liée à l'adoption d'une architecture Zero Trust
- Exemples concrets d'entreprises qui tirent profit de l'adoption d'un modèle de sécurité Zero Trust
- Recommandations concernant la mise en œuvre d'une architecture Zero Trust pour un personnel hybride

[1] *Adoption des technologies cloud 2021, O'Reilly Media.*

Évaluer ce qu'est réellement Zero Trust

Lequel des énoncés suivants est la définition exacte des modèles de sécurité Zero Trust ?

GRAPHIQUE 1 :

Zero Trust est un cadre de sécurisation des entreprises dans un monde basé sur le cloud et la mobilité qui part du principe qu'aucun utilisateur ou application ne devrait être considéré comme fiable par défaut, avec la conviction supplémentaire que le périmètre du réseau n'existe plus dans le monde numérique.

Il s'agit d'un concept de sécurité centré sur la conviction que les entreprises ne doivent faire confiance à rien ni à personne, que ce soit à l'intérieur ou à l'extérieur du périmètre de leur réseau, et qu'elles doivent vérifier toute personne ou tout objet qui tente de se connecter à leurs systèmes avant de lui accorder l'accès.

Ne faire confiance à personne. Jamais.

Aucune de ces réponses

Source : Comprendre le Zero Trust - Protéger le personnel hybride ; étude HMG Strategy/Zscaler ; 118 RSSI et cadres supérieurs en sécurité

Zero Trust est une stratégie de cybersécurité dans le cadre de laquelle la politique de sécurité est appliquée en fonction du contexte établi par des contrôles des accès basés sur le moindre privilège et une authentification stricte de l'utilisateur, et non sur la base d'une confiance implicite. Une architecture Zero Trust bien ajustée permet de simplifier l'infrastructure réseau, d'améliorer l'expérience des utilisateurs et de renforcer la défense contre les cybermenaces.

« L'un des principaux atouts d'une méthodologie Zero Trust est la possibilité d'adapter vos contrôles de sécurité aux niveaux de risque spécifiques et à la priorisation de chaque cas d'utilisation. »

LISA LORENZIN
Directrice technique, Amériques
Zscaler

Relever les principaux défis de sécurité de l'environnement de travail hybride

Bien que le télétravail et les problèmes de sécurité associés aux réseaux domestiques non sécurisés et aux appareils personnels non gérés soient monnaie courante depuis des années, le passage spectaculaire des organisations à un environnement de télétravail depuis mars 2020 a augmenté de façon exponentielle l'empreinte numérique de chaque entreprise, ainsi que les vulnérabilités associées, y compris la surface d'attaque.

La plupart des employés ne connaissent pas grand-chose à la sécurité des réseaux ou aux mesures qu'ils doivent prendre pour se protéger, et protéger les données sensibles et confidentielles des clients. Les utilisateurs se connectent simplement aux services via les pare-feu et les VPN de leur réseau d'entreprise, convaincus qu'ils sont en sécurité. Mais la sécurité réseau basée sur le périmètre les rend vulnérables.

De plus, bien que certaines équipes de sécurité effectuent des tests de simulation de phishing pour aider les employés à mieux comprendre et reconnaître une campagne de phishing, il existe toujours un niveau de fragilité qui a mis de nombreuses organisations dans une situation à risque. Cela contribue à expliquer pourquoi 72 % des dirigeants craignent que les VPN ne compromettent la capacité des services informatiques à assurer la sécurité de leurs environnements, selon le rapport 2021 de Zscaler sur les risques liés aux VPN.

Vulnérabilités du VPN

La dépendance continue à l'égard des VPN pour protéger à la fois les employés et les données sensibles de l'entreprise rend les organisations vulnérables sur plusieurs fronts.

Lisa Lorenzin explique les trois lacunes fondamentales des VPN :

1. Chaque passerelle VPN possède un écouteur entrant qui en fait une surface d'attaque exposée en soi.
2. La passerelle VPN devient alors un point de départ pour des attaques plus sophistiquées menées par des hackers.
3. Le VPN est intrinsèquement ouvert, ce qui oblige les équipes de sécurité à bloquer explicitement l'accès des employés aux applications et systèmes auxquels ils n'ont pas ou ne devraient pas avoir de droits d'accès.

La cyberattaque catastrophique de Colonial Pipeline en 2021 a été initiée via un VPN traditionnel qui ne prévoyait pas d'authentification multifacteur pour les utilisateurs. L'attaque est un exemple classique de déplacement latéral effectué par un cybercriminel dans le réseau d'une entreprise. Dès que le hacker a dérobé les informations d'identification VPN d'un utilisateur, il a obtenu l'accès au réseau de Colonial Pipeline, s'est déplacé latéralement pour accéder aux applications financières critiques, a dérobé des données sensibles et a exigé une rançon.

L'attaque a temporairement interrompu la livraison de carburant pour la majeure partie de la côte Est et du sud des États-Unis, et a forcé l'entreprise à payer une rançon de 4,4 millions de dollars en bitcoins.

De nombreuses autres organisations ont été victimes de ransomware et autres cyberattaques dans un environnement de travail hybride, notamment Brenntag, un distributeur allemand de produits chimiques qui a également payé une rançon de 4,4 millions de dollars en bitcoins, en l'occurrence au gang du ransomware Darkside après que celui-ci ait chiffré des appareils sur le réseau nord-américain de Brenntag et dérobé des fichiers non chiffrés.

Alors que les cybercriminels s'attaquent à des organisations de tous secteurs et de toutes tailles, Accenture estime dans son rapport « The Cost of Cybercrime » que 57 % de toutes les cyberattaques sont dirigées contre des entreprises. Selon un autre rapport d'Accenture, « How Aligning Security and the Business Creates Cyber Resilience », le nombre moyen d'attaques par entreprise a fait un bond énorme de 31 % en 2021 par rapport à 2020. Par ailleurs, le préjudice moyen par entreprise d'une violation de données se chiffrait à 3,86 millions de dollars, incluant l'interruption de l'activité, les paiements de ransomware, les mesures de restauration, les frais juridiques et autres.

Appliquer une meilleure approche, moins coûteuse

Heureusement, l'adoption d'une architecture Zero Trust permet aux entreprises de se protéger contre des violations coûteuses, mais aussi de réduire la complexité, d'améliorer l'expérience utilisateur et de protéger leurs données, tout en éliminant la surface d'attaque.

Sanmina, l'un des principaux fournisseurs de solutions intégrées pour le secteur de la fabrication qui dessert les segments à croissance rapide du marché mondial des services de fabrication électronique, en est un excellent exemple. Bien que l'entreprise ait adopté les principes de Zero Trust et ait commencé à réarchitecturer ses systèmes tout au long de sa transformation cloud pour prendre en charge les pratiques de fabrication avancées de l'industrie 4.0, l'équipe de sécurité de l'entreprise a rapidement réalisé qu'elle ne pouvait pas appliquer le principe de Zero Trust en utilisant la technologie VPN traditionnelle.

« *Nous avions besoin d'une solution d'accès adaptée à un monde moderne, sans périmètre* », a déclaré **Matt Ramberg**, vice-président de la sécurité informatique chez Sanmina.

Comme de nombreuses entreprises, le personnel de Sanmina, qui compte plus de 35 000 personnes, est de plus en plus mobile et distant, en particulier à la suite de la COVID-19, faisant de Zero Trust une priorité.

« *Chaque jour, plusieurs milliers de personnes travaillent à distance et doivent accéder à des dizaines de milliers d'actifs* », explique Matt Ramberg. « *L'utilisation de VPN était une pratique dépassée qui augmentait les risques de cybersécurité en créant des surfaces d'attaque.* »

Après avoir évalué plusieurs options, Sanmina a décidé d'étendre les capacités de sa plateforme Zscaler Zero Trust Exchange™ en adoptant Zscaler Private Access™ (ZPA).

Élément fondamental de Zero Trust Exchange, ZPA connecte les utilisateurs et les appareils aux applications, plutôt que de les connecter au réseau. Contrairement aux pare-feu et aux VPN,[2] qui créent des portes dérobées permettant aux menaces de s'introduire, Zero Trust Exchange rend les utilisateurs et les applications invisibles pour les menaces externes, tout en empêchant le déplacement latéral des menaces. En effet, les entreprises ont la possibilité de limiter l'accès des utilisateurs, en les connectant uniquement aux applications dont ils ont besoin et en ne les plaçant pas sur le réseau de l'entreprise.

> ***« Nous avions besoin d'une solution d'accès adaptée à un monde moderne, sans périmètre .»***
>
> **MATT RAMBERG**
> *Vice-président de la sécurité de l'information*
> **Sanmina**

[2] *Les cinq principaux risques des pare-feu de périmètre et comment les surmonter - Zscaler*

La décision de Sanmina d'adopter Zero Trust Exchange a généré de nombreux dividendes. Grâce à Zero Trust Exchange, l'équipe de cybersécurité de l'entreprise peut contrôler et protéger de manière granulaire tout le trafic entre les utilisateurs et les applications, contrairement aux VPN, tout en protégeant les applications internes contre les failles de sécurité.

De plus, les retours sur les investissements de Sanmina dans le cadre de Zero Trust Exchange ont rapidement augmenté. Les utilisateurs des entreprises bénéficient désormais d'un accès plus rapide et homogène aux applications publiques et privées que lorsqu'ils utilisaient des pare-feu et des VPN.

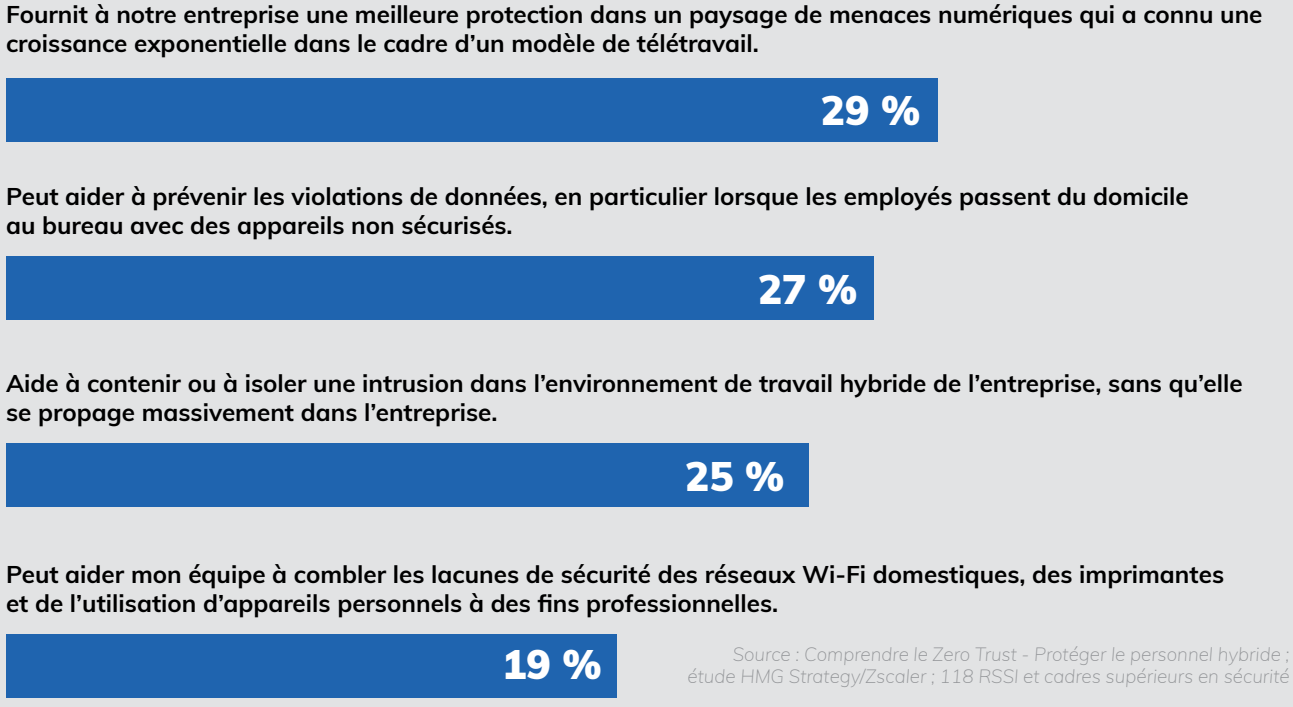
En outre, les dépenses d'administration informatique sont moindres par rapport à l'acquisition, la configuration, la gestion et la mise à jour des pare-feu, VPN et passerelles Web traditionnels. « *Nous disposions de plusieurs appliances physiques réparties dans le monde entier, chacune d'entre elles nécessitant ses propres configurations, règles, correctifs, mises à jour et contrats de maintenance* », explique Matt Ramberg.

L'adoption d'une architecture Zero Trust a aidé Sanmina à étendre en toute sécurité son utilisation des technologies de l'industrie 4.0, à réduire ses coûts d'administration informatique et à accélérer ses processus de fusion et d'acquisition pour une plus grande agilité, tout en améliorant l'expérience utilisateur. Dans la prochaine section du rapport, nous aborderons les facteurs qui motivent l'urgence liée à l'adoption de cette méthodologie de sécurité éprouvée, ainsi que des exemples d'autres entreprises de premier plan qui tirent profit de cette transition.

Renforcer la sécurité grâce à Zero Trust

Quels sont les principaux avantages en matière de sécurité de l'adoption d'un modèle de sécurité Zero Trust pour un environnement de travail hybride ?

GRAPHIQUE 2 :



Source : Comprendre le Zero Trust - Protéger le personnel hybride ; étude HMG Strategy/Zscaler ; 118 RSSI et cadres supérieurs en sécurité

Le plus grand avantage de l'adoption d'un modèle de sécurité Zero Trust pour un environnement de travail hybride, tel que cité par les RSSI et les responsables de la sécurité, est le renforcement de la protection qu'il offre dans un paysage de menaces numériques qui a connu une croissance exponentielle dans le cadre d'un modèle de télétravail.

Urgence liée à l'adoption d'un modèle Zero Trust

Le nombre croissant d'employés qui reviennent au bureau ou qui partagent leur temps entre des environnements de télétravail et de bureau a élargi la surface d'attaque et crée des vulnérabilités supplémentaires dans l'empreinte numérique de chaque entreprise, et toujours plus de défis pour les RSSI et les équipes de sécurité.

La constante transition des employés entre les environnements de travail au bureau et à distance avec des appareils non sécurisés augmente la probabilité de violations de données et d'autres types de cyberattaques lancées par des cybercriminels et des acteurs étatiques. Il s'agit de l'une des principales raisons pour lesquelles les responsables de la sécurité interrogés dans le cadre de l'étude HMG Strategy-Zscaler déclarent adopter une architecture Zero Trust.

« *Que je sois dans mon bureau chez moi, dans un café, dans un bureau d'entreprise, sur mon ordinateur portable, ou que je me connecte par le biais d'une fonctionnalité Desktop-as-a-Service basé sur le cloud, j'ai toujours besoin du même accès aux ressources, et j'ai évidemment toujours besoin de la même protection pour mon trafic sortant* », a déclaré Lisa Lorenzin. « *Zero Trust constitue l'approche la mieux adaptée car elle vous permet de disposer d'une politique et d'une visibilité centralisées et cohérentes, plutôt que de devoir compter sur plusieurs solutions disparates qui peuvent ne pas être coordonnées et manquer de visibilité et de contrôle* », a-t-elle ajouté.

Careem protège l'expansion mondiale de son personnel distant

Un modèle de sécurité Zero Trust s'est imposé comme le choix le plus évident pour **Careem**, le principal fournisseur de services de covoiturage du Moyen-Orient.

À sa création en 2012, Careem utilisait une approche de sécurité informatique cloisonnée traditionnelle. Mais comme l'entreprise basée à Dubaï a connu ces dernières années une croissance exponentielle dans tout le Moyen-Orient et l'Afrique du Nord avec son personnel essentiellement distant, les dirigeants ont réalisé que son modèle de sécurité traditionnel entravait sa fulgurante croissance.

« *Notre activité étant en voie de quadrupler, nous nous sommes rendu compte que notre infrastructure de sécurité traditionnelle représentait une charge considérable pour nos ressources, nous empêchant de recruter efficacement des collaborateurs et nous empêchant d'atteindre nos objectifs commerciaux* », explique **Peeyush Patel**, DSI et RSSI chez Careem. « *Nous devions moderniser l'ensemble de notre approche de la sécurité.* »

Pour soutenir son modèle de développement d'applications basé sur le cloud, son personnel distant et sa trajectoire de croissance explosive, Careem a décidé de remplacer son infrastructure de sécurité traditionnelle, comprenant plus de cinquante pare-feu et des dizaines d'appliances de réseau privé virtuel (VPN), par une approche Zero Trust optimisée par la plateforme Zscaler Zero Trust Exchange.

« *La plateforme Zero Trust Exchange était le choix évident pour créer un modèle SSE (Security Service Edge) Zero Trust afin de protéger nos données, nos employés et nos clients* », a déclaré Peeyush Patel.

Pour rationaliser et simplifier son infrastructure de sécurité, Careem a adopté plusieurs services au sein de Zero Trust Exchange. À la base, Careem a déployé Zscaler Internet Access™ (ZIA) pour sécuriser l'accès aux applications SaaS et à Internet ; Zscaler Private Access (ZPA) pour sécuriser l'accès à ses applications privées exécutées sur l'infrastructure de cloud public et au sein de son data center ; et Zscaler Digital Experience (ZDX) pour détecter et résoudre de manière proactive les problèmes d'accès avant qu'ils n'affectent les utilisateurs.

Au sein de la plateforme, Careem utilise également Cloud Access Security Broker (CASB) pour protéger les données au repos en examinant les applications SaaS et les environnements IaaS, ainsi que Cloud Data Loss Prevention (DLP) pour assurer la conformité réglementaire lors de la manipulation de données personnelles sensibles dans le cloud.

Une fois la plateforme Zero Trust Exchange déployée, Careem a immédiatement bénéficié d'avantages en termes d'agilité, de productivité et de ressources dans toute son entreprise, à commencer par l'élimination des frustrations et des coûts liés à la sécurité du réseau.

« *Nos collègues ont exprimé haut et fort leur mécontentement à l'égard de l'accès VPN* », a déclaré Peeyush Patel. « *L'adoption de la plateforme, y compris ZPA, a non seulement supprimé ces plaintes, mais l'expérience utilisateur globale s'est considérablement améliorée, avec une augmentation correspondante de 70 % de notre Net Promoter Score (NPS) parmi nos collègues et nos CSR.* ».

En outre, Careem a réalisé des économies de ressources considérables, qu'il a depuis réinvesties dans ses projets de développement. « *En simplifiant l'accès aux applications d'ingénierie, nous avons regagné environ 20 000 heures de développement par an* », a déclaré Peeyush Patel. « *Nous avons recentré ces ressources sur la création de valeur commerciale.* »

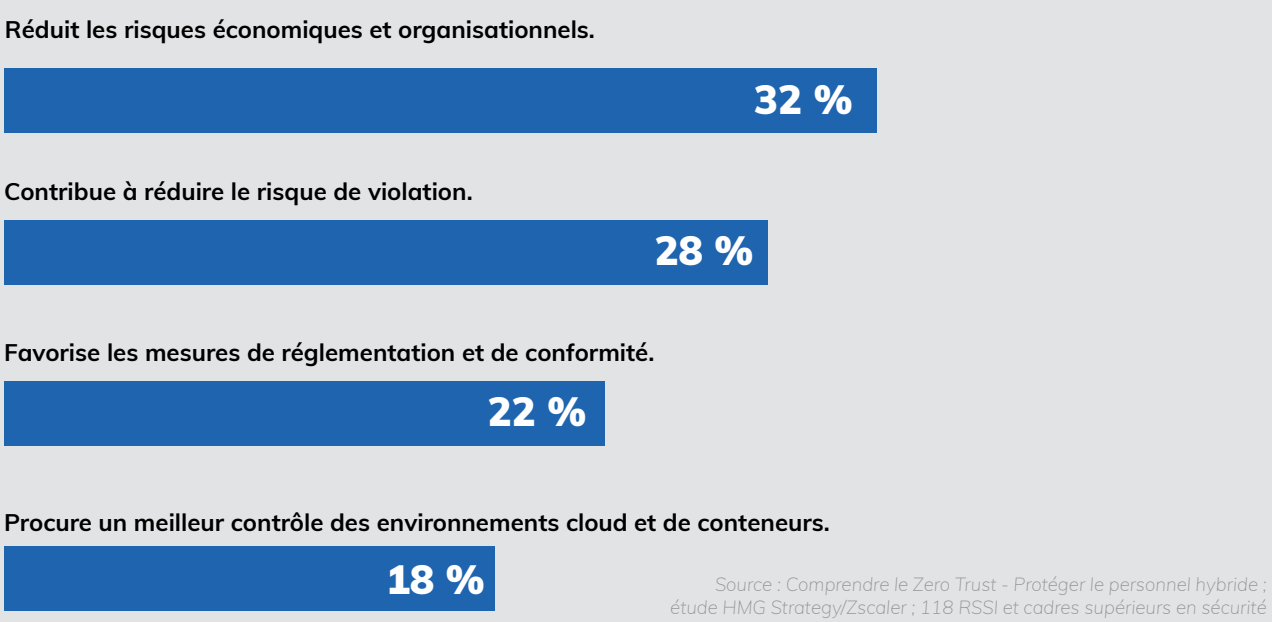
Comme Careem en a fait l'expérience, une approche Zero Trust apporte non seulement des contrôles et des sauvegardes plus solides dans son environnement de travail hybride, mais elle a également permis de gagner en agilité, en productivité et en rentabilité. Dans la dernière section du rapport, nous partagerons des recommandations concernant le déploiement d'une architecture Zero Trust pour mieux protéger le personnel hybride d'une entreprise.

> ***« La plateforme Zero Trust Exchange était le choix évident pour créer un modèle SSE (Security Service Edge) Zero Trust afin de protéger nos données, nos employés et nos clients. »***
>
> **PEEYUSH PATEL**
> *DSI et RSSI*
> **Careem**

Avantages de Zero Trust : Réduction des risques, meilleur contrôle

Quels sont les principaux avantages commerciaux et opérationnels de l'adoption d'un modèle de sécurité Zero Trust ?

GRAPHIQUE 3 :



Source : Comprendre le Zero Trust - Protéger le personnel hybride ; étude HMG Strategy/Zscaler ; 118 RSSI et cadres supérieurs en sécurité

AVANTAGES COMMERCIAUX ET OPÉRATIONNELS D'UN MODÈLE ZERO TRUST

Les avantages commerciaux et opérationnels que Sanmina, Careem et d'autres entreprises ont retirés de l'adoption d'une approche Zero Trust concordent avec les expériences que Lisa Lorenzin a pu observer chez d'autres clients de Zscaler.

« Quatre avantages principaux sont liés à l'utilisation d'un modèle Zero Trust », a déclaré Lisa Lorenzin. **« Le premier est la flexibilité et la résilience.** Cela inclut un déploiement rapide et la capacité de s'adapter rapidement aux changements au fur et à mesure de l'évolution de votre entreprise. ».

« Le deuxième avantage réside dans une meilleure sécurité », a ajouté Lisa Lorenzin. « Cela inclut la capacité de supprimer la surface d'attaque externe, ainsi que les moyens de réduire et potentiellement d'éliminer les déplacements latéraux non autorisés. »

Le troisième avantage consiste en une amélioration de l'expérience utilisateur. Cela inclut un accès plus rapide, plus facile et plus cohérent aux applications.

Le quatrième avantage principal est la réduction des coûts.

« Vous pouvez éliminer les CapEx (dépenses d'investissement) non seulement pour les multiples passerelles VPN déployées dans le monde entier, mais également pour les piles des appliances et des fonctions (équilibrage de charge, pare-feu DMZ, protection DDoS) qui entourent ces passerelles VPN », conclut Lisa Lorenzin.

Les quatre avantages d'une architecture Zero Trust

Démarrer votre parcours Zero Trust

Pour les RSSI et les responsables de la sécurité qui se lancent dans l'aventure Zero Trust, un bon point de départ consiste à identifier un cas d'utilisation simple et direct auquel vous pouvez appliquer les principes de Zero Trust, à déterminer les contrôles déjà en place dans votre entreprise, puis à exécuter ce cas d'utilisation pour en démontrer le bien-fondé.

« *Trouvez un cas d'utilisation facile. Accordez-vous la permission d'essayer quelque chose de nouveau. Ne vous attaquez pas au problème le plus difficile en premier* », conseille Lisa Lorenzin.

À partir de là, les responsables de la sécurité peuvent rencontrer le PDG et le conseil d'administration pour leur expliquer ce qu'est une architecture Zero Trust et comment elle est conçue pour réduire les risques, faciliter les activités et apporter à l'entreprise plus de flexibilité et d'agilité que les approches traditionnelles de sécurité centrées sur le réseau. Cela peut inclure l'utilisation d'analogies qui aident à dépeindre une approche Zero Trust afin de rendre le concept plus facile à comprendre pour les membres non techniques du conseil.

Les responsables de la sécurité peuvent également partager les succès obtenus dans le cadre du projet pilote afin de démontrer la valeur ajoutée d'une approche Zero Trust et d'obtenir un soutien financier pour une stratégie Zero Trust plus large.

Il est également utile de recueillir les retours d'information et les idées de collègues concernant leurs propres expériences de déploiement du Zero Trust. Parmi les forums populaires pour ce type de connexions figure le forum CXO REvolutionaries. Ces interactions peuvent également fournir des recommandations concernant la collaboration avec un partenaire Zero Trust de confiance dont la plateforme est la mieux adaptée pour répondre à chaque cas d'utilisation prioritaire tout en offrant à l'entreprise la possibilité d'atteindre ses objectifs stratégiques de Zero Trust.

« *Profitez des connaissances techniques des personnes qui sont plus avancées dans cette voie* », ajoute Lisa Lorenzin.

Comme nous l'avons dit, l'adoption d'une architecture Zero Trust n'est pas seulement opportune, elle est vitale pour la protection du personnel hybride et des activités numériques. Mais le jeu en vaut la chandelle, c'est certain.

À propos de HMG Strategy

HMG Strategy est la principale plateforme numérique au monde qui met en relation les cadres technologiques afin de repenser l'entreprise et de remodeler le monde des affaires. Nos conférences régionales et virtuelles sur le leadership exécutif des DSI et des RSSI, nos livres d'auteurs et notre centre de ressources numériques proposent des recherches uniques, menées par des homologues, des DSI aux RSSI, en passant par des directeurs techniques et des cadres technologiques, sur le leadership, l'innovation, la transformation et l'ascension professionnelle.

Le réseau mondial de HMG Strategy est composé de plus de 400 000 cadres supérieurs en informatique, d'experts du secteur et de leaders d'opinion de renommée mondiale.

Pour en savoir plus sur les 7 piliers de confiance du modèle économique unique de HMG Strategy, cliquez ici.

HMG Strategy : Votre plateforme numérique de confiance n° 1 qui met en relation les cadres technologiques afin de repenser l'entreprise et de remodeler le monde des affaires.

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale afin que les clients puissent être plus agiles, plus efficaces, plus résilients et plus sécurisés. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur zscaler.fr ou suivez-nous sur Twitter @zscaler.