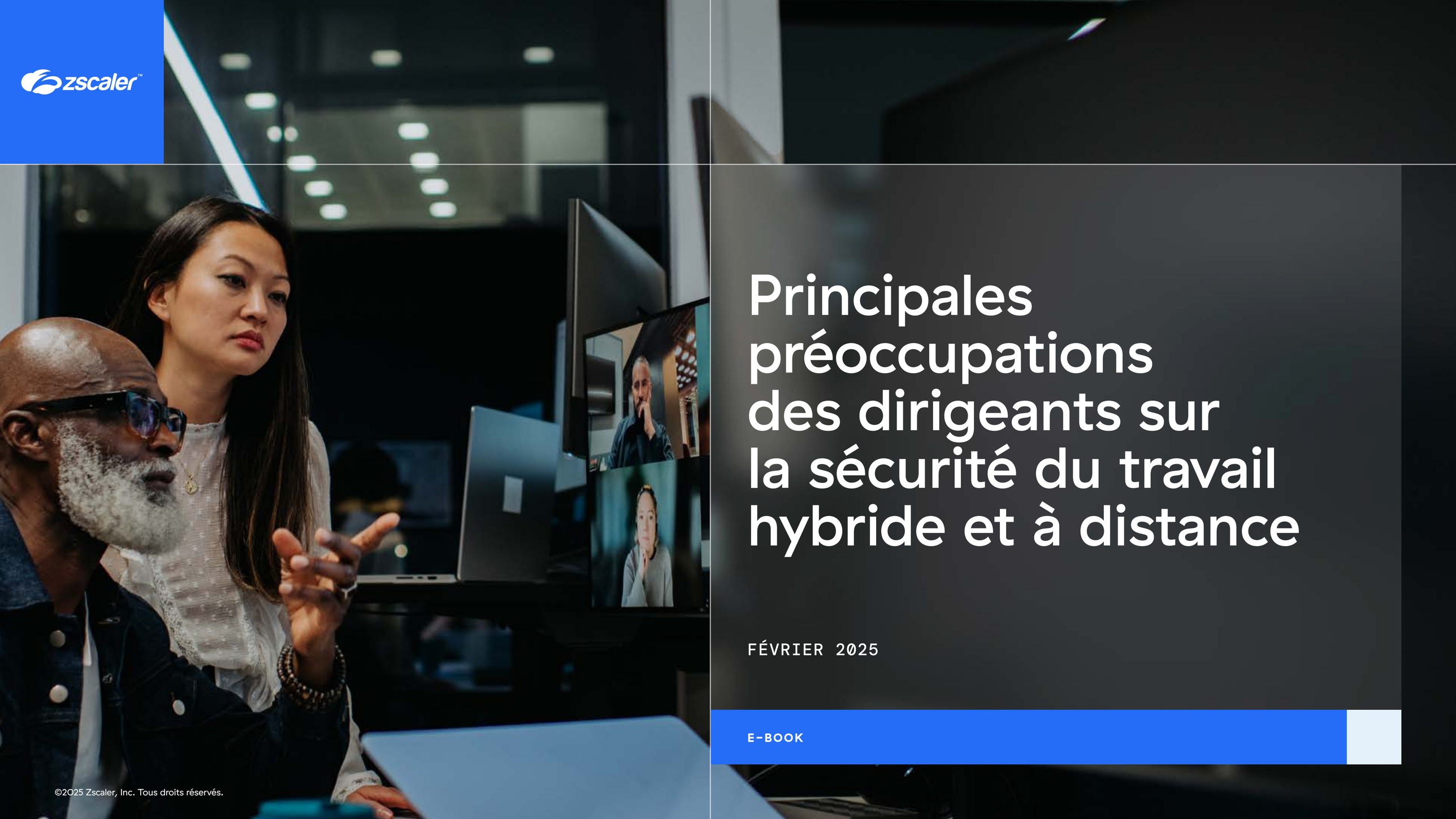


Principales préoccupations des dirigeants sur la sécurité du travail hybride et à distance

FÉVRIER 2025

E-BOOK

Sommaire

Introduction

Les cyberattaques ont bondi à un rythme annuel de 30 % par an[1] dans le monde au deuxième trimestre 2024. L'adoption croissante du télétravail a élargi la surface d'attaque et rendu les entreprises vulnérables à un large éventail de menaces. Selon le rapport ThreatLabz de Zscaler sur les attaques chiffrées, Zscaler Cloud a neutralisé un nombre record de 32,1 milliards d'attaques intégrées dans un trafic TLS/SSL. Les menaces chiffrées représentent 87,2 % de toutes les attaques déjouées, un chiffre qui s'est apprécié de 10,3 % sur un an.[2] Ces données mettent en évidence le recours croissant des assaillants au chiffrement pour dissimuler leurs activités malveillantes.

Les technologies traditionnelles telles que les pare-feu et les réseaux privés virtuels (VPN) ne suffisent plus à protéger les données, les applications et les réseaux des entreprises, ce qui inquiète les décideurs et les dirigeants par rapport à la sécurisation des environnements de télétravail. Les dirigeants sont soumis à une pression constante pour minimiser le risque d'incident, assurer la conformité aux réglementations et aux normes du secteur, et empêcher le vol de données de valeur (éléments de propriété intellectuelle, données métiers confidentielles, données de clients...)

Heureusement, les solutions Zero Trust basées sur le cloud sont conçues pour protéger les réseaux des entreprises qui gèrent des collaborateurs en télétravail ou hybrides. Avec la bonne technologie, les dirigeants peuvent répondre à ces préoccupations majeures.

Enjeux critiques de la sécurité réseau et du télétravail

Le télétravail peut amoindrir le contrôle des entreprises sur les données et l'intégrité de leur architecture de sécurité. Les collaborateurs peuvent utiliser des appareils non gérés, dépourvus de logiciel de sécurité et sans surveillance active, pour accéder aux ressources d'entreprise, y compris aux applications critiques.

De plus, les professionnels de la sécurité ignorent généralement la manière dont les télétravailleurs gèrent les données sensibles et s'ils les suppriment après utilisation. Les collaborateurs peuvent également stocker des données sur leurs appareils personnels, ce qui les expose à des attaques de ransomware, à des piratages de données et à d'autres menaces.

L'adoption d'applications basées sur le cloud élargit encore davantage la surface d'attaque, ce qui rend la sécurité de votre infrastructure numérique plus complexe.

Évolution du paysage de la sécurité numérique

Avant la pandémie, les pare-feu et les VPN auraient pu suffire à sécuriser les réseaux et les données sensibles d'une entreprise. Cependant, le télétravail et le travail hybride ont contraint les entreprises à transformer radicalement leur façon de protéger leurs environnements numériques.

Dernières tendances en matière de sécurité numérique et de télétravail

Les télétravailleurs ont inévitablement besoin des ressources de leur entreprise pour mener leurs tâches et de nombreuses entreprises ont adopté des applications SaaS (Software-as-a-Service) dans le cloud pour faciliter le télétravail et améliorer la productivité. Le déploiement d'applications SaaS sur un réseau de collaborateurs disséminés élargit la surface d'attaque et accentue le risque d'accès non autorisés et de failles de sécurité.

Les cybercriminels ont également développé des tactiques plus sophistiquées, notamment le credential stuffing et les attaques de type « zero-day », ce qui accentue les enjeux de cybersécurité pour les dirigeants. Les États-Unis demeurent la principale cible des ransomwares, avec 49,95 % du total des attaques, suivis par le Royaume-Uni, l'Allemagne, le Canada et la France.[3] En plus de ternir l'image de marque et la confiance des clients, ces attaques exposent votre entreprise à un risque de non-conformité aux réglementations en matière de confidentialité et de sécurité des données, ainsi qu'à des risques financiers.

À la lumière de ces tendances, les cadres dirigeants et les responsables de la sécurité adoptent de nouvelles mesures de sécurité :

- **Architecture Zero Trust**, qui fonctionne selon le principe « ne jamais faire confiance, toujours vérifier ». Tous les utilisateurs et appareils, y compris les appareils BYOD (appareils personnels), doivent être vérifiés.
- **Détection des menaces optimisée par l'intelligence artificielle (IA) et l'apprentissage automatique (AA)**, qui permet d'identifier et d'atténuer de manière proactive les cyber-attaques sophistiquées.
- **Segmentation des applications**, qui empêche le déplacement latéral des menaces.
- **Sécurité des terminaux**, qui se concentre sur la protection des appareils des employés distants, permet de détecter et de bloquer les menaces avant qu'elles n'affectent les terminaux, garantissant ainsi une meilleure protection aux équipes disséminées.

Principales préoccupations des dirigeants en matière de sécurité d'entreprise

Avec la prévalence du télétravail et du travail hybride, et la dépendance croissante aux solutions basées sur le cloud, les dirigeants d'entreprise et les RSSI doivent penser au-delà d'une sécurité périmétrique.

Protection des données sensibles

Les collaborateurs qui accèdent aux données d'entreprise via des réseaux non sécurisés et les enregistrent sur leurs appareils personnels amplifient le risque d'un accès non autorisé et d'une utilisation abusive des données. La protection des données sensibles dans les environnements de télétravail implique les éléments suivants :

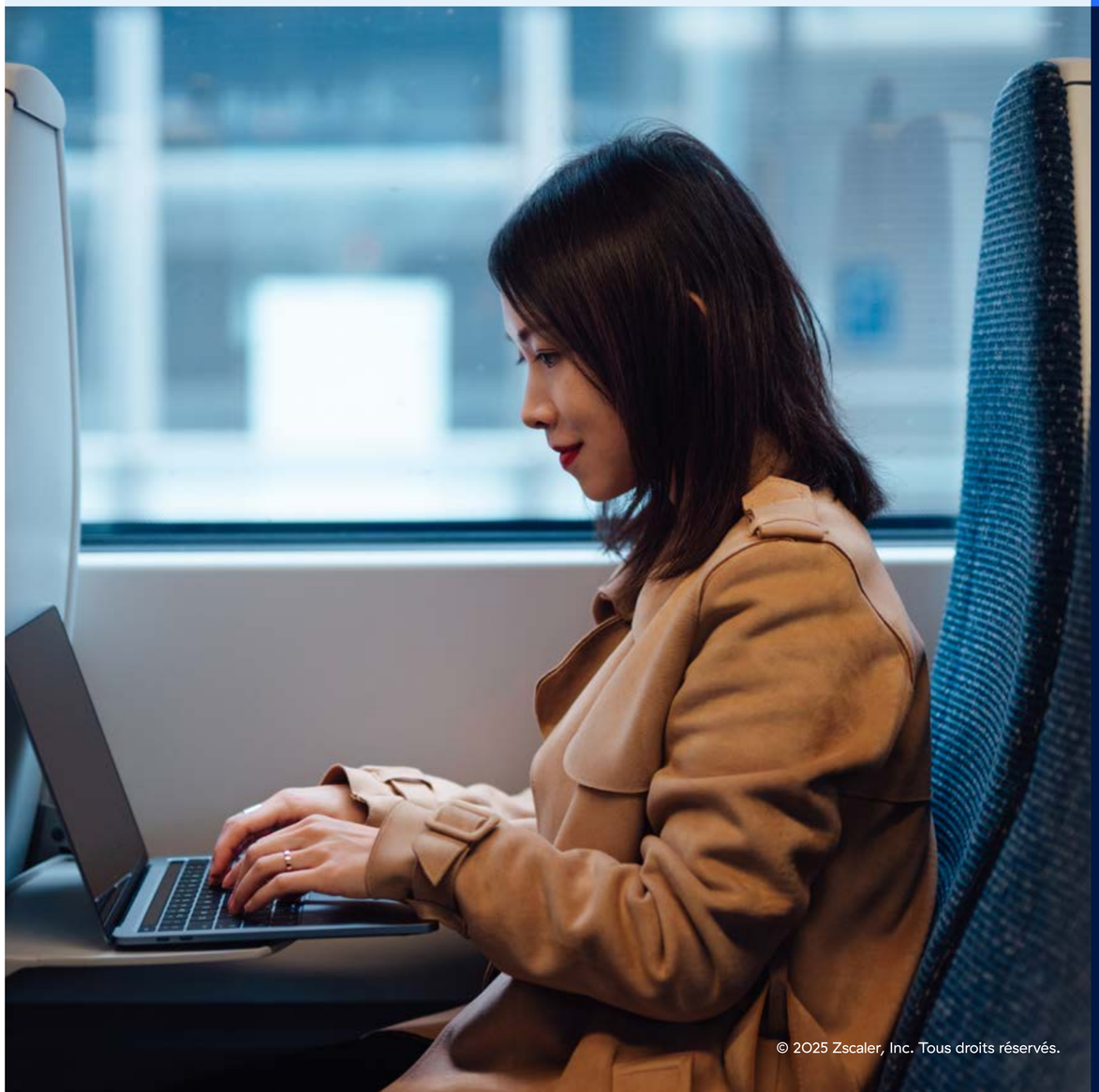
- **Chiffrement de bout en bout** pour protéger les données au repos et en transit, en particulier lorsqu'elles sont transférées sur des canaux non sécurisés.
- **Gestion des identités et des accès** pour garantir que seuls les employés autorisés peuvent accéder et utiliser les données nécessaires.
- **Techniques de prévention de la perte de données** pour atténuer l'exposition accidentelle des données et les violations.

Gérer les menaces internes

Des actions fortuites ou intentionnelles de colaborateurs sur site et à distance peuvent compromettre la sécurité des systèmes. Par exemple, un nouveau collaborateur peut être victime d'une escroquerie par phishing, ou un collaborateur mécontent peut utiliser à mauvais escient des données confidentielles d'entreprise. Le contrôle d'accès basé sur les rôles, les politiques d'accès sur la base du moindre privilège et l'analyse comportementale peuvent contribuer à minimiser le risque de menaces internes.

Conformité réglementaire

De très nombreux gouvernements ont instauré des lois sur la protection des données et la confidentialité pour protéger les informations personnelles des consommateurs, à l'image du règlement général sur la protection des données (RGPD) et du California Consumer Privacy Act (CCPA). En outre, il existe des réglementations sectorielles spécifiques à l'instar de la loi HIPAA (Health Insurance Portability and Accountability Act). Dans les environnements de télétravail, le respect de ces exigences réglementaires implique des stratégies de gouvernance rigoureuses.



Stratégies pour répondre aux préoccupations des dirigeants

Les cadres dirigeants peuvent opter pour plusieurs stratégies en réponse aux défis complexes liés à la sécurité dans l'environnement de travail moderne.

Mise en œuvre d'une gestion robuste des identités et des accès

La gestion des identités et des accès (IAM) constitue une méthode efficace pour prévenir les accès non autorisés au réseau et aux systèmes de votre entreprise. Elle garantit que seules les personnes autorisées accèdent aux applications et aux données dont elles ont besoin pour travailler.

L'IAM minimise la surface d'attaque, réduisant ainsi l'exposition inutile des données sensibles. Contrairement aux méthodes de sécurité périmétrique, l'IAM applique des contrôles d'accès plus stricts, quels que soient le dispositif et l'emplacement de l'utilisateur. Les dirigeants devraient envisager de déployer une plateforme qui propose une solution IAM, en natif ou après intégration.

Amélioration des capacités de détection et de réponse aux menaces

À mesure que les cybercriminels font évoluer leurs stratégies, les responsables de la sécurité doivent également actualiser leurs propres stratégies afin de déjouer les attaques, grâce à des capacités avancées de détection et de réponse aux menaces. Déployez des solutions qui utilisent des modèles IA et AA pour surveiller le trafic réseau et le comportement des utilisateurs afin de détecter automatiquement les éléments suspects.

L'IA et l'AA viennent également au renfort des solutions Zero Trust qui isolent les appareils et les fichiers compromis en temps réel, permettant ainsi de réagir rapidement aux menaces et d'encourager une cybersécurité plus proactive. En outre, les algorithmes d'AA peuvent mettre en évidence les vulnérabilités potentielles tout en identifiant et en neutralisant les menaces émergentes.

Programmes réguliers de formation et de sensibilisation à la sécurité

L'efficacité des politiques et des outils de sécurité dépend de leurs utilisateurs. En effet, 80 % des RSSI estiment que la négligence des collaborateurs et le risque humain constitueront des risques de cybersécurité majeurs d'ici 2026[4]. Les télé-travailleurs sont particulièrement vulnérables, car ils ne peuvent pas toujours demander de l'aide en personne aux professionnels de la sécurité, ce qui entraîne des retards et des dommages irréversibles.

Pour atténuer ces risques, les entreprises peuvent instaurer des programmes de formation continue à la sécurité qui sensibilisent les collaborateurs aux menaces existantes, émergentes et versatiles, ainsi qu'aux bonnes pratiques qui assurent leur vigilance face à des menaces en constante évolution. Formez votre équipe aux bonnes pratiques de télétravail, d'utilisation de mots de passe et de gestion sécurisée des données. Organisez également régulièrement des sessions de formation pour informer vos équipes des protocoles de cybersécurité en vigueur dans l'entreprise et des ressources disponibles sur les mesures à prendre en cas de compromission de leurs appareils, de leurs données ou de leur accès aux applications.

Les solutions Zscaler pour la sécurité des collaborateurs au bureau, à distance et hybrides

Les solutions Zero Trust basées sur Zscaler Cloud sont conçues pour aider les dirigeants d'entreprise à sécuriser tous les environnements de travail, aujourd'hui comme demain, à mesure que les menaces évoluent. Zscaler Zero Trust Exchange™ propose les solutions suivantes pour garantir aux équipes une sécurité complète :

Zscaler Internet Access (ZIA)

Zscaler Internet Access est une solution Zero Trust cloud native, optimisée par l'IA, qui contribue à renforcer la sécurité numérique des télétravailleurs. Grâce à une architecture proxy Zero Trust qui inspecte 100 % du trafic TLS/SSL, ainsi que des connexions directes entre l'utilisateur et l'application sur la base de l'identité, le contexte et les politiques métiers, ZIA garantit un accès fluide et sécurisé aux applications SaaS et Web. La solution fournit les fonctionnalités clés suivantes :

- **Le Secure Web Gateway (SWG) cloud-native** fournit une expérience Web sûre et rapide tout en détectant et en prévenant les attaques avancées grâce à une analyse en temps réel et au filtrage d'URL optimisés par l'IA.
- **La détection des menaces avancées optimisée par l'IA/AA** neutralise les menaces avancées tels que les botnets, les ransomwares, l'infrastructure Commande et Contrôle (C&C), le partage de fichier à risque, le contenu actif malveillant, les scripts intersites, les sites frauduleux, etc.
- **Le filtrage d'URL optimisé par l'IA** garantit à vos utilisateurs des sessions de navigation sécurisées sur les applications Web en arrêtant les menaces avancées, telles que le phishing et les ransomwares, et en appliquant une politique d'utilisation acceptable.
- **Le Cloud Access Security Broker (CASB)** sécurise les applications cloud, protège les données, bloque les menaces et garantit la conformité dans vos environnements SaaS et IaaS avec une protection intégrée.
- **La prévention de la perte de donnés (DLP)** protège les données en mouvement avec une inspection inline complète, y compris la correspondance exacte des données (EDM), la correspondance des documents indexés (IDM) et l'apprentissage automatique.
- **La politique dynamique basée sur les risques** stoppe les attaques actives et pérennise vos défenses grâce à l'analyse continue des risques liés aux utilisateurs, aux appareils, aux applications et aux contenus, alimentant les contrôles d'accès dynamiques.
- **Le pare -feu Zero Trust** établit des connexions rapides et sécurisées sur le réseau et hors réseau, ainsi que des points locaux d'accès à Internet pour le trafic des utilisateurs à travers tous les ports et protocoles, sans avoir à gérer de mises à jour matérielles ou logicielles.
- **L'isolation du navigateur optimisée par l'IA** restitue les sessions Web uniquement sous forme de pixels dans le navigateur de l'utilisateur, offrant une expérience Web quasi native sans risque de perte de données ni d'infection de l'appareil.
- **DNS Security** filtre les domaines à risque et malveillants et empêche l'utilisation du tunneling DNS pour transférer des payloads malveillants et des données sensibles.

Zscaler Private Access (ZPA)

Zscaler Private Access est la première solution d'accès réseau Zero Trust (ZTNA) optimisée par l'IA du secteur. Cette offre cloud native fournit un accès Zero Trust à tous les utilisateurs. En assurant une connectivité directe aux applications privées tout en minimisant la surface d'attaque, ZPA élimine le déplacement latéral des menaces à l'aide d'une segmentation utilisateur–application optimisée par l'IA. La solution protège également les entreprises contre les attaques sophistiquées grâce à une inspection intégrée du trafic et à une protection des applications et des données. Voici quelques-unes des principales fonctionnalités de ZPA qui permettent de sécuriser les environnements de travail hybrides :

- **La segmentation d'applications optimisée par l'IA** découvre automatiquement les applications et fournit des recommandations générées par l'IA sur les segments d'applications et les politiques afin de réduire votre surface d'attaque et empêcher les déplacements latéraux.
- **La segmentation de workload à workload** sécurise les communications des workloads cloud dans les environnements hybrides et multicloud tels qu'AWS et Azure.
- **L'accès distant privilégié** permet aux collaborateurs distants et aux tiers d'accéder à distance et sans client aux systèmes de production RDP, SSH et VNC sensibles.
- **Private Service Edge** apporte ZTNA aux utilisateurs sur site avec un accès utilisateur–application direct et basé sur le moindre privilège aux applications privées.
- **Business Continuity** garantit un accès ininterrompu et conforme aux politiques aux applications critiques pendant les interruptions de connectivité et les événements catastrophiques.
- **La prise en charge des applications extranet** permet un accès Zero Trust aux applications des partenaires commerciaux et des fournisseurs hébergées sur leurs réseaux.
- **La surveillance de l'expérience numérique** optimise vos expériences numériques pour préserver la productivité des utilisateurs en détectant et en résolvant rapidement les problèmes liés aux applications, au réseau et aux appareils.

Fonctionnalités de sécurité avancées

Zscaler propose plusieurs fonctionnalités avancées, parmi lesquelles :

- **L'inspection SSL/TLS** à grande échelle pour une protection complète des données et une inspection de l'utilisateur à l'application.
- **Détection des menaces inline optimisée par l'IA** pour neutraliser les vecteurs d'attaque avant qu'ils n'atteignent leur cible.
- **Risk360™** qui propose une visualisation intuitive et détaillée des facteurs des risques. Vous pouvez ainsi prendre des mesures immédiates pour maîtriser les risques.

Comment sécuriser votre équipe avec Zscaler

Si vous souhaitez renforcer la sécurité de votre environnement de télétravail, vous devez envisager de remplacer les solutions de cybersécurité traditionnelles. La plateforme Zero Trust Zscaler offre plusieurs moyens de simplifier ce remplacement.

Migrer des pare-feu vers le Zero Trust

Les pare-feu et les VPN sont peu efficaces dans les environnements business modernes : ils étendent votre réseau d'entreprise, offrant aux assaillants davantage de passerelles d'intrusion. En revanche, Zscaler Zero Trust Exchange™ agit comme un commutateur intelligent, qui inspecte le trafic entrant et sortant des dispositifs des utilisateurs afin de détecter et neutraliser les menaces, tout en négociant en toute sécurité des connexions directes vers les applications et ressources cloud.

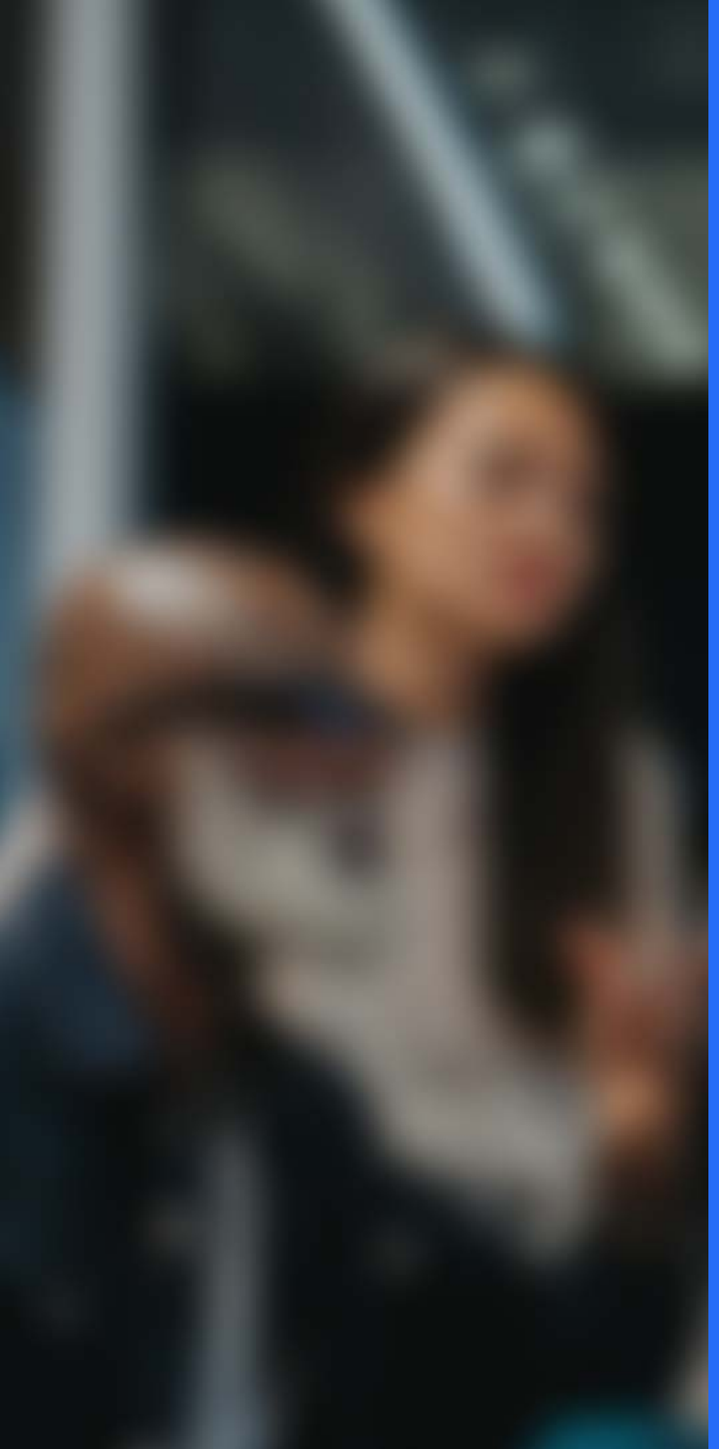
Une approche Zero Trust intégrale

Une véritable approche Zero Trust en matière de sécurité requiert des politiques d'accès contextuelles et centrées sur l'identité, adaptées à chaque utilisateur, appareil ou application. L'objectif ? Garantir que seuls des utilisateurs de confiance accèdent à des ressources spécifiques, et que ces utilisateurs et ressources sont désignés par les fonctionnalités établies par votre entreprise. Vous pouvez définir, dans votre cadre de sécurité Zero Trust, des règles qui accordent aux utilisateurs un accès en fonction de leur emplacement, de leur identité, de l'heure/la date, etc. Zscaler peut vous accompagner tout au long de ce processus.

Découvrez comment Zscaler peut vous aider à optimiser votre posture de sécurité et protéger vos équipes disséminées en demandant une démonstration.

SOURCES :

1. Intelligent CISO, Check Point Research unveils Q2 2024 cyberattack trends, highlighting global and UAE increases, 29 juillet 2024.
2. Zscaler, Rapport ThreatLabz 2024 sur les attaques chiffrées, 2024.
3. Zscaler, Rapport ThreatLabz 2024 sur les ransomwares, 2024.
4. Infosecurity Magazine, 70% of CISOs Expect Cyber-Attacks in Next Year, Report Finds, 21 mai 2024.



zscaler™ | Experience your world, secured.™