Parcours Client

Découvrez des témoignages de transformation sécurisée, optimisées par les solutions Zero Trust + IA de Zscaler

Découvrez comment les entreprises ont élevé leurs postures de sécurité, favorisé des expériences utilisateur exceptionnelles, simplifié leurs fusions et acquisitions, et bien plus encore, grâce aux solutions Zero Trust + IA.

L'obsession du client est l'une de nos valeurs fondamentales chez Zscaler et, à ce titre, nous nous engageons à offrir le meilleur de l'innovation Zero Trust pour aider votre entreprise à atteindre ses objectifs. Grâce aux capacités fondamentales mobilisées par notre plateforme Zero Trust Exchange, optimisée par l'IA, nous avons aidé plus de 5 000 entreprises dans le monde à réduire leurs coûts et la complexité de leurs opérations, à simplifier leurs architectures réseau, à sécuriser leurs utilisateurs et à se protéger contre l'évolution des cybermenaces. Dans cet e-book, vous plongerez dans les études de cas de certaines des entreprises les plus performantes au monde et découvrirez comment elles ont transformé leur réseau, leur sécurité et leurs opérations avec Zscaler.

Pionnier du Zero Trust depuis plus de 15 ans, Zscaler s'engage à aider les entreprises de toutes tailles et de tous secteurs à atteindre et à dépasser leurs objectifs de Zero Trust. La seule constante que nous connaissons dans le domaine de la technologie est le « changement », et grâce à notre plateforme Zero Trust Exchange, les entreprises restent prêtes à faire face à toutes les éventualités, tout en continuant à innover et à transformer leur infrastructure informatique.

Mike Rich
CRO et Président des ventes mondiales

Sommaire

Condultez les témoignages de clients par secteur

AMS

Consultez les témoignages de clients par région

AMN Healthcare protège ses utilisateurs et ses données à l'échelle mondiale avec Zscaler Zero Trust Exchange

Zscaler sécurise l'expérience de télétravail de plus de 5 000 utilisateurs et protège les données des patients contre la multiplication des cybermenaces ciblant le secteur de la santé

AMN HEALTHCARE EN BREF

Fournit aux clients des solutions pour le personnel de santé afin d'améliorer les prestations aux patients

- Soins de santé et industrie pharmaceutique
- Dallas, Texas, États-Unis
- Plus de 10 000 clients répartis sur 24 sites

1,2 milliard
de transactions Web traitées mensuellement

7 M
de menaces bloquées en trois mois

Heures
pour déployer un edge sécurisé n'importe où

Défis

- Une infrastructure de sécurité traditionnelle n'était plus compatible avec l'évolution de l'écosystème opérationnel cloud-first de l'entreprise
- Les VPN traditionnels ne pouvaient pas répondre à la demande croissante d'accès à distance, exposant ainsi davantage les ressources privées aux cybermenaces
- Une architecture de sécurité complexe avec de multiples solutions ponctuelles compliquait la gestion de la visibilité et de la résolution des incidents

Parcours par étapes

1. **Fourniture d'un accès sécurisé et direct à Internet**, garantissant la flexibilité du télétravail à un personnel dispersé dans le monde entier
2. **Introduction d'un accès micro-segmenté et Zero Trust aux applications privées**, assurant un remplacement sécurisé des VPN traditionnels
3. **Rationalisation de la pile de surveillance et exploitation d'une visibilité complète de bout en bout** pour améliorer la résolution des problèmes des utilisateurs

Résultats

- **Sécurise la connectivité sortante et entrante pour plus de 5 OOO utilisateurs**, améliorant ainsi les capacités et l'efficacité du télétravail à l'échelle mondiale
- **Applique des politiques d'accès Zero Trust aux applications privées et aux produits numériques** utilisés par plus de 10 OOO clients dans le monde
- **Simplifie l'architecture et réduit les coûts technologiques** pour renforcer la sécurité tout en réduisant les frais généraux

L'approche de Zscaler est alignée sur notre philosophie globale de Zero Trust, et la plateforme Zero Trust Exchange incarnait notre vision d'une architecture Zero Trust chez AMN Healthcare.

Mani Massoud
Responsable de la sécurité de l'information, AMN Healthcare

Voir le témoignage client

ATN International sécurise ses opérations et optimise ses performances avec Zscaler Zero Trust Exchange

Zscaler améliore les capacités de télétravail de plus de 2 500 employés, élimine les problèmes d'utilisateurs liés au VPN et garantit une intégration et une prise en charge plus sécurisées des fusions et acquisitions

ATN INTERNATIONAL EN BREF

Fournit une infrastructure et des services de communication avec une expertise sur les marchés distants

- Télécommunications
- Beverly, Massachusetts, États-Unis
- 750 000 clients dans le monde

100 %

élimination des VPN et les demandes d'assistance liées au VPN

Tous

les employés sécurisés avec Zscaler

Minutes

vs. plusieurs heures pour atténuer les problèmes de l'utilisateur

Défis

- L'infrastructure de sécurité sur site ne pouvait pas efficacement prendre en charge les opérations commerciales cloud-first ni les futurs objectifs de fusions et acquisitions
- Les anciennes appliances VPN peinaient à s'adapter à l'augmentation du télétravail, ce qui entraînait une dégradation de l'expérience utilisateur et une augmentation des risques
- Les solutions de sécurité traditionnelles n'intégraient pas les fonctionnalités essentielles du cloud pour permettre une résolution proactive des problèmes des utilisateurs

Parcours par étapes

1. **Fourniture d'un accès direct à Internet,** exploitant les fonctionnalités d'inspection et de journalisation du trafic afin d'éviter les violations de politiques
2. **Remplacement des appliances VPN par un accès Zero Trust, basé sur le moindre privilège** aux applications et ressources privées
3. **Exploitation des fonctionnalités Zscaler optimisées par l'IA et intégration étroite avec Microsoft** afin d'identifier et de résoudre plus rapidement les problèmes des utilisateurs

Résultats

- **Améliore l'expérience de télétravail de plus de 2 500 utilisateurset** élimine les problèmes liés au VPN : les demandes d'assistance chutent de 100 %
- **Accélère les délais des fusions et acquisitions et garantit une intégration plus sécurisée** des sociétés acquises grâce à une architecture de sécurité Zero Trust
- **Réduit le temps nécessaire à l'identification et à la résolution des problèmes** à quelques minutes seulement grâce à des fonctionnalités de reporting et de surveillance robustes

L'un mes critères de sélection des outils d'infrastructure et de sécurité est qu'ils doivent vous aider à être plus performant sur le plan opérationnel et renforcer votre sécurité. Zscaler répond à ces deux critères.

Richard Casselberry
Vice-président, Sécurité informatique, Architecture & Conformité,
ATN International

Voir le témoignage client

Cox Automotive déploie Zero Trust par phases avec Zscaler Zero Trust Exchange

Zscaler rationalise l'architecture de sécurité, sécurise la connectivité des utilisateurs sur les cinq continents et protège les données de millions d'acheteurs de voitures en ligne

COX AUTOMOTIVE EN BREF

Le plus grand fournisseur mondial de services et de technologies automobiles

Vente au détail et en gros

Atlanta, Géorgie, États-Unis

2,3 milliards d'interactions en ligne par an

30K+
membres de l'équipe Protégés

40K
clients concessionnaires automobiles pris en charge

Une
plateforme unique réduit la complexité

Défis

- Recherchait une plateforme compatible avec le cloud qui pourrait servir de base à une architecture de sécurité Zero Trust globale
- Les appliances de pare-feu traditionnelles peinaient à inspecter le trafic Internet à grande échelle pour un groupe d'utilisateurs dispersés dans le monde entier
- Les VPN traditionnels ne prenaient pas en charge les politiques de contrôle d'accès basées sur l'identité, ce qui exposait davantage les applications et les données privées

Parcours par étapes

1. **Déploiement d'une plateforme Zero Trust cloud native et multi-entité** spécialement conçue pour s'intégrer à d'autres solutions cloud
2. **Fourniture d'une connectivité sécurisée et directe à Internet et aux applications SaaS**, exploitant les capacités d'inspection du trafic inline
3. **Remplacement des VPN par un accès Zero Trust** pour établir des politiques de sécurité microsegmentées et basées sur le moindre privilège pour les applications privées

Résultats

- **Sécurise une équipe répartie sur cinq continents,** offrant la flexibilité du télétravail et améliorant l'expérience utilisateur
- **Protège les applications et ressources privées critiques**, dont les données de millions de clients, de manière plus économe
- **Supprime les solutions de sécurité traditionnelles, notamment les pare-feu et les VPN,** afin de rationaliser les processus informatiques et l'intégration des fusions et acquisitions

Une fois les agents installés sur les appareils de chacun, il sera facile d'intégrer d'autres fonctionnalités de Zscaler dans notre architecture. Il suffira simplement d'appuyer sur l'interrupteur « on ».

Jon Mahes
Gestionnaire principal, Cybersécurité, Cox Automotive

Voir le témoignage client

Le gouvernement du District de Columbia regroupe sa sécurité sur Zscaler Zero Trust Exchange

Zscaler remplace les appliances VPN traditionnelles pour rationaliser l'architecture de sécurité, renforcer la sensibilisation aux risques en temps réel et protéger 15 000 utilisateurs

GOUVERNEMENT DE D.C. EN BREF

Supervise et gère tous les services essentiels pour les résidents du District de Columbia

- Fédéral et gouvernement
- Washington, D.C., États-Unis
- Plus de 15 000 employés

15 000
employés du gouvernement sécurisés

~3Mrd
transactions traitées par mois

+ de 200 000
menaces de sécurité bloquées par mois

Défis

- Une infrastructure de sécurité obsolète ne pouvait soutenir le télétravail et nuisait à l'efficacité opérationnelle
- Les appliances VPN traditionnels étendent le réseau d'entreprise aux appareils des utilisateurs finaux, exposant ainsi les données sensibles à un risque de violation
- Les anciens produits de sécurité ponctuels limitaient la visibilité sur les menaces, ce qui rendait l'évaluation et l'atténuation des risques plus difficiles

Parcours par étapes

1. **Fourniture d'une connectivité sécurisée et directe à Internet et aux applications SaaS**, assurant la flexibilité du télétravail
2. **Remplacement des VPN traditionnels par un accès Zero Trust microsegmenté** afin d'appliquer des politiques de sécurité cohérentes aux ressources privées
3. **Exploitation des données et des informations optimisées par l'IA pour renforcer la sensibilisation aux risques** et atténuer les menaces potentielles en temps réel, à grande échelle

Résultats

- **L'architecture Zero Trust renforce la sécurité** traite environ 3 milliards de transactions et bloque plus de 200 000 menaces par mois
- **Améliore l'expérience des 15 000 utilisateurs distants**et s'intègre parfaitement aux solutions d'identité existantes
- **Permet une approche plus globale de la gestion des risques**, grâce à une meilleure connaissance des facteurs de risque et de la posture de sécurité

Le partenariat avec Zscaler s'est révélé inestimable pour nous. Nous avons déployé la plateforme à une vitesse record, intégré les utilisateurs plus efficacement et amélioré l'expérience utilisateur.

Suneel Cherukuri
RSSI, gouvernement de D.C.

Voir le témoignage client

DMI met en œuvre le BYOD à grande échelle, améliorant la protection des données et réalisant des économies substantielles

Zscaler fournit une connectivité Zero Trust à l'ensemble du personnel et permet aux employés de travailler en toute sécurité sur l'appareil de leur choix

DMI EN BREF

DMI est un fournisseur mondial de services numériques de premier plan qui travaille à l'intersection des secteurs public et privé

High-Tech

McLean, Virginie, États-Unis

Plus de 2 100 employés répartis dans 80 pays

Plus de 700K USD
d'économies annuelles

Moins de 2
semaines pour déployer

3 %
résolution des SLA plus rapide après le déploiement

Défis

- L'installation de nouveau matériel dans un environnement traditionnel entraînait des temps d'arrêt, provoquait des interruptions et nécessitait des mises à jour régulières
- Le fait d'obliger les utilisateurs à travailler à partir des appareils de DMI a réduit la productivité des employés et a eu un impact négatif sur l'empreinte carbone globale de l'entreprise

Parcours par étapes

1. **Accès Internet sécurisé et véritable connectivité Zero Trust** pour les employés, les sous-traitants et les tiers sans configuration manuelle et fastidieuse des appareils
2. **Déploiement de l'initiative BYOD (utilisation d'appareils personnels) soutenue par l'isolation du navigateur,** permettant aux employés de travailler sur l'appareil de leur choix

Résultats

- **Déploie Zero Trust en 2 semaines** sans impact sur les utilisateurs ni temps d'arrêt
- **Économise 700 000 USD par an,** améliore les expériences d'intégration et de départ et réduit le temps de configuration de nouveaux bureaux et appareils

Grâce au projet BYOD, nous avons pu réaliser des économies en n'ayant pas à acheter d'ordinateurs portables pour les personnes qui n'en avaient pas besoin. Cela a permis à DMI de réaliser une économie annuelle de plus de 700 000 USD, ce qui est énorme !

Mauricio Mendoza
Vice-président, Informatique et Sécurité mondiales, DMI

Voir le témoignage client

Eaton sécurise ses opérations mondiales grâce à une segmentation optimisée par l'IA

Zscaler aide un fabricant mondial à opérer sa transition vers le cloud grâce à une protection avancée contre les menaces, une réduction des risques de violation et une plus grande visibilité par le biais d'intégrations de partenaires

APERÇU D'EATON

Fabricant mondial d'équipements électriques pour l'aéronautique et d'autres industries

- Production industrielle
- Cleveland, Ohio, États-Unis
- Plus de 90 000 employés et utilisateurs répartis dans 170 pays

4 M

menaces bloquées en un mois

90K

employés dans le monde se connectent à Internet et aux applications privées via Zero Trust

De nombreux

partenaires d'alliance stratégique s'intègrent de manière homogène

Défis

- Les VPN et pare-feu traditionnels entravaient la croissance et n'étaient pas en mesure de prendre en charge plus de 30 000 employés d'usine pendant la pandémie et après
- L'architecture de sécurité traditionnelle basée sur le périmètre était incompatible avec la stratégie cloud-firstde la société et ses besoins de segmentation
- Le manque de visibilité limitait la détection des menaces et ralentissait le temps de correction

Parcours par étapes

1. **Remplacement des outils de sécurité** et d'accès par une connectivité Zero Trust à Internet et aux applications privées
2. **Adoption des innovations de l'IA** afin de découvrir et combattre les menaces basées sur l'IA et fournir une segmentation pour les sites de fabrication
3. **Amélioration de la connaissance des attaques** grâce à une détection et une réponse préventives et prédictives des violations

Résultats

- **Fournit une expérience utilisateur plus sécurisée, fiable et réglementée** pour les employés et les tiers
- **Exploite la puissance de l'IA pour la détection des menaces,** la prévention de la perte de données, la correction, la visibilité sur l'utilisation de ChatGPT et la segmentation des applications
- **Renforce le contrôle de l'accès** grâce à la segmentation Zero Trust et à l'intégration avec les outils EDR, CDR et NDR

Zscaler est facile à utiliser et ses fonctionnalités sont intégrées dans un unique agent de terminal. Nous avons pu déployer rapidement Zscaler dans notre environnement mondial et étendre ses capacités avec un minimum de ressources de notre côté.

Jason Koler
RSSI, Eaton Corporation

Voir le témoignage client

Guaranteed Rate bloque des millions de menaces et accélère l'intégration des fusions et acquisitions de plusieurs mois à quelques jours

Zscaler remplace le matériel de sécurité, et offre une résilience supérieure, une sécurité permanente et réduit la surface d'attaque

GUARANTEED RATE

Deuxième plus grand leader du crédit immobilier aux États-Unis, avec plus de 500 filiales dans 50 États

Services financiers et d'assurances

Chicago, Illinois, États-Unis

6 000+ employés

97 %
du trafic chiffré inspecté

2,5 M
Menaces bloquées en 3 mois

2-3x
Accès plus rapide aux Applications

Défis

- L'utilisation d'un VPN pour se connecter à des centaines d'applications privées sur site et dans AWS a ouvert la surface d'attaque
- Le backhauling du trafic de plus de 500 sites distants vers le data center nuisait aux performances et à la productivité
- L'ancien pare-feu ne pouvait pas détecter les menaces de type« zero-day » pénétrant dans le réseau depuis Internet et se déplaçant latéralement

Parcours par étapes

1. **Sécurisation de l'accès à Internet et aux SaaS depuis le cloud**— plus de backhauling depuis plus de 500 filiales
2. **Remplacement du VPN**, procurant aux utilisateurs un accès rapide et fiable à plus de 500 applications privées dans le data center et le cloud
3. **Optimisation de l'expérience utilisateur** en identifiant et en résolvant les problèmes de performances de manière plus rapide et plus efficace

Résultats

- **Minimise la surface d'attaque** en donnant aux utilisateurs un accès direct, basé sur le moindre privilège, tout en optimisant la détection et la réponse
- **Réduit le risque de compromission** grâce à la surveillance du trafic TLS/SSL inline et à une protection contre les menaces avancées optimisée par l'IA
- **Empêche les déplacements latéraux** grâce à une technologie de tromperie qui éloigne les hackers des ressources sensibles et contient les menaces en temps réel

Avec Risk360, nous pouvons gagner en visibilité sur les angles morts du cyber-risque. Cette visibilité nous permet de mieux cibler nos efforts afin de traiter et de réduire les cyber-risques les plus pressants.

Darin Hurd
RSSI chez GUARANTEED RATE

Voir le témoignage client

MGM Resorts International mise sur une architecture Zero Trust cloud native

Zscaler offre un délai de rentabilisation inégalé grâce à la segmentation Zero Trust, à la protection contre la perte de données et à des renseignements détaillés et exploitables dans toute l'entreprise

MGM RESORTS INTERNATIONAL

Leader dans le domaine des jeux, du divertissement et de l'hôtellerie avec 31 complexes touristiques dans le monde

Divertissement et hôtellerie

Las Vegas, Nevada, États-Unis

70 000 employés dans le monde

Jour 1
valeur immédiate depuis la plateforme

275K+
Menaces bloquées chaque mois

50 %
utilisation plus efficace des appareils pour le personnel

Défis

- La sécurité cloisonnée augmentait le risque de déplacement latéral en donnant aux utilisateurs un large accès au réseau
- Les passerelles VPN traditionnelles créaient des congestions de trafic, au détriment de l'expérience utilisateur
- Les outils de sécurité traditionnels offraient une visibilité limitée sur l'activité de navigation de l'ensemble des utilisateurs

Parcours par étapes

1. **Remplacement des VPN et déploiement d'une segmentation Zero Trust** sur l'ensemble du personnel
2. **Déploiement rapide** d'une suite de solutions d'accès privé, d'expérience numérique et de protection des données
3. **Adoption d'une technologie de tromperie** pour se protéger des tentatives de compromission des hackers actifs

Résultats

- **Améliore l'expérience des employés** grâce à des performances et une connectivité plus rapides dans tout l'environnement
- **Garde une longueur d'avance sur les menaces émergentes** grâce à une DLP complète, un accès privé et une segmentation Zero Trust
- **Renforce la posture de sécurité de l'entreprise** tout en contribuant à accélérer les activités grâce à une approche cloud-first

Nous avons déployé la segmentation Zero Trust pour l'ensemble de nos collaborateurs en un temps record, et la maintenance quotidienne de la solution de protection contre la perte de données avec des informations sur nos applications. De notre point de vue, les avantages ont été rapides et faciles à obtenir.

Stephen Harrison
RSSI, MGM Resorts International

Voir le témoignage client

Mercury Financial améliore sa sécurité et son efficacité avec Zscaler Zero Trust Exchange

Zscaler offre des intégrations homogènes et des fonctionnalités d'IA pour sécuriser le télétravail depuis n'importe quel emplacement et protéger les données financières sensibles contre les menaces

MERCURY FINANCIAL

Une société de services financiers non bancaires qui aide ses clients à obtenir et gérer leur crédit

Services financiers et d'assurances

Austin, Texas, États-Unis

Plus de 500 employés

100 %

expérience transparente pour les travailleurs distants

76 %

de réduction des demandes d'assistance informatiques

Zéro

temps d'arrêt dû à des malwares

Défis

- Les solutions de sécurité traditionnelles ne permettaient pas l'inspection complète du trafic inline, ce qui entravait la détection et la prévention des menaces
- Les anciens VPN étaient incompatibles avec les besoins cloud-first d'un personnel distribué, ce qui nuisait à l'expérience utilisateur
- Le manque de données relatives à l'activité des utilisateurs et à la posture des appareils compliquait le diagnostic et la résolution des problèmes pour le personnel distant

Parcours par étapes

1. **Sécurisation de la connectivité directe à Internet**, à l'aide de fonctionnalités de confinement des menaces optimisées par l'IA pour empêcher la compromission des données
2. **Remplacement des VPN par un accès Zero Trust microsegmenté** pour les applications privées afin de garantir le contrôle et la sécurité des connexions distantes
3. **Exploitation d'intégrations clés et d'informations utilisateur plus solides** pour alléger les frais administratifs sans augmenter les risques

Résultats

- **Réduit la surface d'attaque :** aucun temps d'arrêt causé par un malware ou un ransomware depuis le déploiement de Zscaler
- **Limite les déplacements latéraux et réduit le rayon d'explosion** si une menace s'infiltre dans la pile de sécurité, ce qui garantit une correction plus rapide
- **Les intégrations avec AWS, Crowdstrike et Okta rationalisent l'infrastructure de sécurité** et renforcent la conformité réglementaire

Nous considérons Zscaler comme un leader dans ce domaine car il est complet et couvre toutes les facettes du Zero Trust. Pour obtenir ailleurs les mêmes fonctionnalités que celles de Zscaler, nous devrions déployer plusieurs solutions de différents fournisseurs.

Arjun Thusu
Directeur de l'information
Mercury Financial

Voir le témoignage client

Molson Coors profite d'une expérience utilisateur exceptionnelle grâce à Zscaler Zero Trust Exchange

Zscaler élimine le besoin d'appliances VPN, sécurise la connectivité pour un personnel international et fournit des informations qui permettent de résoudre les problèmes plus rapidement

MOLSON COORS

Troisième brasseur mondial et innovateur d'envergure mondiale dans l'industrie des boissons

Alimentation, boissons et tabac

Chicago, Illinois, États-Unis

Plus de 17 000 employés, Plus de 42 brasseries

17K
d'utilisateurs sécurisés avec le Zero Trust

96 %
résolution plus rapide des problèmes des utilisateurs

Des millions
de menaces bloquées quotidiennement

Défis

- Les appliances de pare-feu ne pouvaient pas s'adapter à la demande d'accès distant à Internet et peinaient à inspecter le trafic inline
- Le manque de visibilité sur l'activité des utilisateurs et la posture des appareils permettait difficilement d'identifier et de résoudre les problèmes de performance
- Une architecture de sécurité traditionnelle reposant sur des appliances VPN avait créé un environnement réseau plat et une surface d'attaque plus large

Parcours par étapes

1. **Fourniture d'un accès direct à Internet avec des fonctions avancées de détection des menaces** pour assurer la sécurité des utilisateurs distants et tiers
2. **Exploitation de la visibilité de bout en bout sur les utilisateurs et les appareils** pour simplifier la gestion de la sécurité et résoudre plus rapidement les problèmes des utilisateurs
3. **Remplacement des VPN traditionnels par un accès Zero Trust pour les applications privées** afin de protéger les ressources et d'améliorer l'expérience utilisateur

Résultats

- **Assure une excellente expérience utilisateur aux employés** qui travaillent dans 42 brasseries à travers le monde, ainsi qu'aux partenaires tiers
- **Améliore le temps moyen de résolution des problèmes des utilisateurs** en identifiant les causes profondes et en automatisant l'atténuation en quelques minutes, et non en plusieurs heures
- **Bloque les menaces avancées** et élimine les déplacements latéraux pour sécuriser les applications privées et les données d'entreprise sensibles

Le nombre de menaces bloquées uniquement par Zscaler se chiffre toujours en centaines de milliers ou en millions selon les jours. C'est simple, facile à utiliser. Vous pouvez vous y entraîner immédiatement. Il n'y a aucune limite.

Jérémy Bauer
Directeur principal de la sécurité de l'information (RSSI), Molson Coors Beverage Company

Voir le témoignage client

Le Département de l'éducation de la ville de New York migre du VPN vers le Zero Trust

Zscaler aide à sécuriser l'accès à Internet et aux applications privées pour plus d'un million d'utilisateurs et plus de deux millions d'appareils

DÉPARTEMENT DE L'ÉDUCATION DE LA VILLE DE NEW YORK EN BREF

Le Département de l'éducation de la ville de New York (NYC DOE) est le plus grand système scolaire des États-Unis et l'un des plus importants au monde. Il accueille plus d'un million d'étudiants de la maternelle à la terminale, avec un personnel de plus de 150 000 enseignants et administrateurs répartis dans les cinq arrondissements de New York.

Enseignement

Ville de New York, New York, États-Unis

Plus d'un million d'utilisateurs et plus de deux millions d'appareils

2M+
d'appareils d'étudiants et d'employés sécurisés

15 %
diminution des attaques

40 %
plus de menaces Bloqué

Défis

- L'infrastructure existante ne pouvait pas évoluer pour offrir une expérience sécurisée et cohérente à plus d'un million d'utilisateurs
- L'approche traditionnelle de VPN et de pare-feu était inefficace pour bloquer les cybermenaces avancées
- La mauvaise visibilité sur les terminaux compliquait grandement la maintenance et la surveillance des appareils d'apprentissage à distance du département

Parcours par étapes

1. **Sécurisation de l'accès à Internet et aux SaaS** avec une architecture de proxy Zero Trust qui inspecte l'intégralité du trafic TLS/SSL à grande échelle
2. **Remplacement du VPN par un accès réseau Zero Trust (ZTNA)** pour une connectivité utilisateur rapide et homogène
3. **Amélioration de la visibilité** sur les réseaux et les appareils grâce à une surveillance de bout en bout de l'expérience numérique

Résultats

- **Étend un accès rapide, fiable et sécurisé** aux applications d'apprentissage pour les étudiants et les employés partout, sur n'importe quel appareil
- **Filtre le trafic en fonction du contenu**, au-delà du simple blocage d'URL, pour assurer la conformité CIPA sur les appareils d'apprentissage
- **Améliore les performances du réseau** en détectant et en résolvant les problèmes de réseau et de DNS dans l'environnement

Je pense que Zscaler peut être un partenaire de choix pour nous aider à comprendre l'utilisation que nous faisons de l'IA et à accélérer la réponse aux incidents et trouver l'aiguille qui se cache dans la botte de foin.

Demond Waters
RSSI, Département de l'éducation de la ville de New York

Voir le témoignage client

Southwest Gas exploite Zscaler Zero Trust Exchange pour optimiser une expérience utilisateur sécurisée

Zscaler élimine la dépendance aux solutions de sécurité traditionnelles pour offrir une connectivité plus rapide et plus fiable à 2 300 employés hybrides et 50 bureaux extérieurs

SOUTHWEST GAS EN BREF

Société énergétique qui fournit du gaz naturel en Arizona, au Nevada et en Californie

Énergie, pétrole, gaz et mines

Las Vegas, Nevada, États-Unis

2 millions de clients

4–6
semaines pour déployer zero trust

95 %
des cas d'utilisation satisfaits

Une
plateforme à fournisseur unique pour plus de simplicité

Défis

- Une infrastructure de sécurité traditionnelle ne pouvait pas évoluer pour soutenir la transformation du cloud ou le passage au travail hybride
- Il était difficile de fournir une connectivité Internet rapide et fiable aux bureaux extérieurs et aux employés distants dans les zones rurales
- Les VPN en place ne permettaient pas d'appliquer des politiques d'accès basées sur l'identité, ce qui exposait davantage les applications et les données privées aux menaces

Parcours par étapes

1. **Déploiement d'une plateforme Zero Trust multi-entité**, rationalisant la pile de sécurité et optimisant les environnements de télétravail
2. **Fourniture d'un accès direct à Internet et aux applications SaaS** avec une protection cohérente contre les menaces, quel que soit l'emplacement
3. **Remplacement des VPN par un accès Zero Trust pour les applications privées** afin de réduire la surface d'attaque et d'endiguer la perte de données

Résultats

- **Sécurise la flexibilité du télétravail pour 2 300 employés hybrides** et protège les utilisateurs et les données dans 50 bureaux extérieurs
- **Permet des politiques de contrôle d'accès microsegmentées et basées sur le moindre privilège** pour les applications privées, préservant ainsi la sécurité des données critiques
- **Accélère l'adoption du Zero Trust**, élimine la complexité de la gestion de la sécurité et réduit les demandes d'assistance technique

Après avoir réalisé une preuve de valeur (PoV), nous avons sélectionné Zscaler pour son architecture moderne, qui nous a permis de mettre notre pile de sécurité dans le cloud et d'optimiser un personnel distant.

David Petroski
Architecte principal en infrastructure, Southwest Gas

Voir le témoignage client

United Airlines détecte et bloque les menaces en constante évolution avec Zscaler Zero Trust Exchange

Zscaler élimine 40 % de menaces en plus que les anciennes solutions pour sécuriser 80 000 utilisateurs dans le monde et proposer des voyages plus sûrs à 143 millions de passagers

UNITED AIRLINES EN BREF

Société américaine d'aviation et troisième plus grande compagnie aérienne au monde, opérant dans 48 pays

Services de transport

Chicago, Illinois, États-Unis

Plus de 80 000 employés sur plus de 350 sites

6
mois pour la transformation Zero Trust

1PB
du trafic TLS inspecté

$3M+
économies de coûts par rapport aux solutions traditionnelles

Défis

- Une architecture traditionnelle basée sur le périmètre et dépendante des data centers ne pouvait pas soutenir une transformation numérique accélérée
- Les pare-feu et VPN traditionnels manquaient de l'agilité requise pour s'adapter à l'accroissement du télétravail, ce qui mettait les utilisateurs et les données en danger
- Les produits de sécurité précédents ne disposaient pas de capacités avancées de détection des menaces, exposant ainsi une surface d'attaque plus large

Parcours par étapes

1. **Fourniture d'une connectivité directe et sécurisée à Internet et aux applications SaaS** pour garantir une protection cohérente des utilisateurs où qu'ils soient
2. **Remplacement des VPN par des politiques d'accès Zero Trust basées sur le moindre privilège** pour protéger les applications et les données privées contre les compromissions
3. **Intégration du cloud et fonctions de surveillance de l'expérience** pour augmenter la visibilité en temps réel sur les menaces

Résultats

- **Permet à 80 000 employés de travailler en toute sécurité depuis n'importe quel endroit** et sécurise l'accès à distance à plus de 2 000 applications privées critiques
- **Réduit la complexité et le coût de l'architecture :** plus besoin de pare-feu dans les aéroports et six produits de sécurité ont été supprimés
- **Unifie l'écosystème de sécurité et applique dynamiquement les politiques** pour bloquer 40 % de menaces supplémentaires et améliorer la posture de sécurité

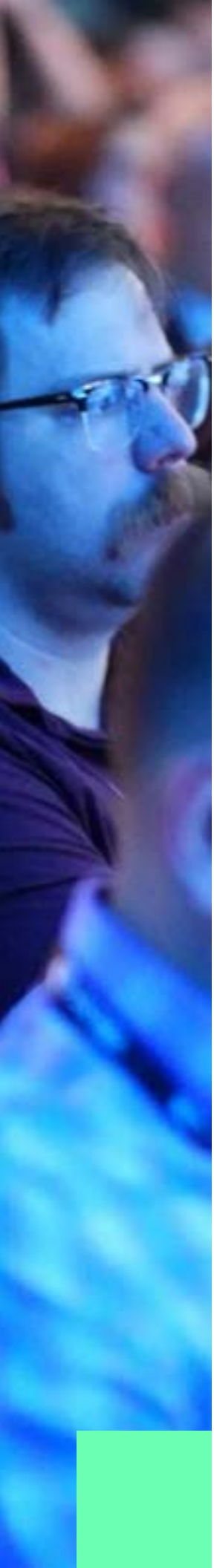
Zscaler nous procure la tranquillité d'esprit sachant que le trafic sera sécurisé, quel que soit le réseau sous-jacent, pour nos employés, nos clients et nos partenaires.

Deneen DeFiore
Vice-président et responsable de la sécurité des systèmes d'information, United Airlines

Voir le témoignage client

Europe, Moyen-Orient et Afrique

Consultez les témoignages de clients par région



Raiffeisen Bank International

Raiffeisen Bank International transforme la sécurité avec Zscaler Zero Trust Exchange

Zscaler remplace les appliances traditionnelles pour fournir une protection complète contre les menaces, permettre la flexibilité du travail à distance et réduire les coûts liés à la sécurité

RAIFFEISEN BANK EN BREF

L'une des principales banques d'affaires et d'investissement d'Autriche

Services financiers et d'assurances

Vienne, Autriche

Des millions de clients sur 12 marchés

44K
employés protégés par Zero Trust

18,6M
clients bénéficient de services bancaires sécurisés

Une
plateforme qui offre un Zero Trust intégral

Défis

- Une infrastructure de sécurité traditionnelle n'était pas compatible avec une approche cloud-first, ce qui mettait en danger les utilisateurs et les workloads
- Les appliances de sécurité traditionnelles ne soutenaient pas la flexibilité du télétravail, ce qui entraînait des temps de latence et une baisse des performances
- Les VPN ne permettaient pas un accès basé sur l'identité pour les applications privées, ce qui créait des politiques incohérentes et élargissait la surface d'attaque

Parcours par étapes

1. **Déploiement d'une plateforme Zero Trust complète**, exploitant les services edges privés et publics pour sécuriser les utilisateurs où qu'ils se trouvent
2. **Sécurisation de la connectivité directe à Internet sans backhauling** pour garantir des expériences utilisateur cohérentes à un personnel hybride
3. **Remplacement des appliances VPN par un accès Zero Trust pour les applications privées** et affinement des politiques d'accès basées sur l'identité

Résultats

- **Sécurise la connectivité sortante et entrante pour un personnel hybride**, offrant une protection cohérente à chaque emplacement
- **Réduit la latence et améliore les performances des applications SaaS et privées** pour améliorer l'expérience des utilisateurs au bureau et distants
- **Rationalise l'architecture de sécurité et offre une protection complète contre les menaces** tout en réduisant les dépenses de sécurité

Le partenariat avec Zscaler nous a permis d'améliorer la sécurité, de réduire les coûts et d'offrir une meilleure expérience utilisateur en appliquant nos principes Zero Trust.

Peter Gerdenitsch
RSSI Groupe, Raiffeisen Bank International

Voir le témoignage client

Le conseil municipal de Magdebourg sécurise sa transformation numérique avec Zscaler Zero Trust Exchange

La capitale d'État allemand remplace ses appliances VPN et renforce l'autonomie de son personnel hybride tout en jetant les bases d'une évolution numérique continue avec Zscaler

LA CAPITALE D'ÉTAT MAGDEBOURG EN BREF

Fournit des services administratifs aux résidents de la capitale du Land de Saxe-Anhalt

Fédéral et gouvernement

Magdebourg, Allemagne

2 500 employés

2,5K
employés hybrides sécurisés

230K
habitants de la ville pris en charge

Une
solution à fournisseur unique pour simplifier la sécurité

Défis

- Une architecture de sécurité traditionnelle basée sur le matériel n'était pas suffisamment agile pour soutenir les objectifs de transformation numérique
- Les solutions de proxy et de pare-feu traditionnelles ne pouvaient pas évoluer pour sécuriser la connectivité Internet d'un personnel de plus en plus hybride
- Les VPN ne permettaient pas un contrôle granulaire de l'accès, ce qui exposait davantage les applications privées et limitait les capacités de télétravail

Parcours par étapes

1. **Déploiement d'une plateforme Zero Trust cloud native** pour moderniser l'architecture de sécurité et permettre la poursuite de la transformation numérique
2. **Introduction d'une connectivité Internet directe et sécurisée**, exploitant la fonctionnalité d'inspection du trafic intégrée pour gérer les menaces
3. **Sécurisation de l'accès aux applications privées avec des contrôles Zero Trust basés sur l'identité**, garantissant une protection cohérente des données critiques

Résultats

- **Améliore l'expérience utilisateur pour un personnel hybride** et sécurise le télétravail pour jusqu'à 1 500 utilisateurs par mois
- **Réduit les coûts de sécurité et la complexité de gestion** grâce à une architecture qui supprime les produits de sécurité ponctuels traditionnels
- **Accélère les efforts futurs de transformation numérique** grâce à une architecture de sécurité Zero Trust complète et évolutive

Nous voulions être un modèle pour d'autres municipalités et les encourager à évaluer et à déployer de bonnes solutions pour l'entreprise, comme nous l'avons fait avec une solution de sécurité basée sur le cloud.

Dr Tim Hoppe
Bureau des statistiques, des élections et de la numérisation, Ville de Magdebourg

Voir le témoignage client

Cisalfa Sport renforce sa posture de sécurité en accélérant le déploiement de Zscaler en moins de trois mois

La plateforme Zero Trust réduit la surface d'attaque et garantit une expérience utilisateur homogène pour les employés et les utilisateurs tiers

CISALFA SPORT EN BREF

Le premier détaillant omnicanal de sport en Italie

- Vente au détail et en gros
- Curno (BG), Italie
- Plus de 3 600 employés

2,5
mois pour le déploiement de Zscaler à l'échelle de société

130+
partenaires et sous-traitants tiers accèdent en toute sécurité aux applications privées et à l'infrastructure sur site

70 %
utilisateurs intégrés dans les 2 semaines du déploiement

Défis

- Un VPN permettait à tous les employés et aux tiers d'accéder sans restriction à l'ensemble du réseau de l'entreprise, ce qui augmentait le risque et le rayon d'action des attaques potentielles.
- Deux solutions VPN traditionnelles comportaient des politiques et des configurations conflictuelles, ce qui entraînait un manque de cohérence au niveau de la sécurité et des problèmes de gestion de la sécurité
- L'accès aux applications par le biais du VPN ralentissait les performances et entraînait un nombre élevé de tickets d'assistance de la part des utilisateurs internes et externes

Parcours par étapes

1. **Réduction de la surface d'attaque** en remplaçant les VPN vulnérables par un accès direct de l'utilisateur à l'application privée
2. **Empêcher le déplacement latéral des menaces** grâce à l'application de politiques d'accès sur la base du moindre privilège pour tous les utilisateurs
3. **Amélioration de l'expérience utilisateur** grâce à l'amélioration des performances et de la fiabilité des applications : plus de perturbations ni de connexions VPN multiples pour accéder aux ressources

Résultats

- **Renforce la posture de sécurité globale** en fournissant à tous les utilisateurs un accès direct de l'utilisateur à l'application et une application cohérente des politiques
- **Permet un accès homogène, transparent et sans client** aux applications et données privées pour les partenaires et les sous-traitants
- **Réduit les tickets d'assistance liés à la latence** grâce à une connectivité ultra-rapide fournie via le point de présence le plus proche

Zscaler Zero Trust Exchange [...] couvre tous les aspects : un accès plus rapide et mieux sécurisé aux applications sans avoir besoin de VPN, une réduction des risques sur l'ensemble de l'environnement et une voie explicite vers l'expansion du Zero Trust.

Fabio Freti
Responsable des opérations et de l'infrastructure informatique, Cisalfa Sport

Voir le témoignage client

Hydro renforce sa posture de sécurité et ses efforts de durabilité avec Zscaler Zero Trust Exchange

Zscaler réduit la surface d'attaque et l'empreinte carbone du fournisseur d'énergie renouvelable qui souhaite renoncer à son matériel existant au profit d'une solution 100 % cloud-first

HYDRO EN BREF

Une des plus grandes sociétés d'énergie renouvelable au monde, présente dans 40 pays

Production industrielle

Oslo, Norvège

31 000 employés

33K
employés sécurisés avec le Zero Trust

Un
approche fournisseur pour réduire les coûts et la complexité

100 %
Opérations cloud Objectif

Défis

- L'infrastructure de sécurité et le matériel existants consommaient beaucoup d'énergie et n'étaient pas conformes aux objectifs de développement durable de l'entreprise
- Un réseau MPLS à faible bande passante ne pouvait pas évoluer pour prendre en charge l'augmentation du trafic de données vers le cloud, ce qui entraînait une baisse des performances
- Les VPN traditionnels avec des politiques d'accès tout ou rien mettaient le réseau en danger, ce qui a entraîné une coûteuse attaque de ransomware

Parcours par étapes

1. **Fourniture d'une connectivité sécurisée et directe à Internet**, éliminant le backhauling du trafic et améliorant la fiabilité de l'accès
2. **Remplacement des VPN traditionnels par un accès Zero Trust basé sur des politiques** pour les applications privées afin de protéger les données contre les cyberattaques
3. **Déploiement d'une solution de surveillance de l'expérience spécialement conçue pour le trafic cloud** afin de permettre une résolution plus rapide des problèmes des utilisateurs

Résultats

- **Élimine la dépendance aux produits ponctuels traditionnels** et réduit l'empreinte carbone grâce à une plateforme de sécurité cloud native et multi-entité
- **Améliore les performances des applications SaaS**, optimisant ainsi l'expérience utilisateur de 33 000 employés répartis sur 140 sites
- **Réduit les coûts et la complexité de gestion tout en améliorant la posture de sécurité** à l'aide d'une solution Zero Trust à fournisseur unique

Avec Zscaler Private Access, les utilisateurs n'ont plus besoin de se connecter au réseau pour accéder à nos applications privées. À présent, tandis que nous continuons à faire évoluer notre environnement de travail moderne, nous souhaitons supprimer graduellement le VPN.

Armin Auth
Responsable des programmes stratégiques I&T

Voir le témoignage client

Capitec accélère sa transformation numérique et protège ses données financières avec Zscaler

La plus grande banque d'Afrique du Sud déploie une sécurité Zero Trust en trois mois, protégeant 17 000 utilisateurs et bloquant 745 000 menaces sur la plateforme Zero Trust Exchange

CAPITEC EN BREF

La plus grande banque d'Afrique du Sud, au service de 21 millions de personnes et classée n°1 pour la satisfaction du client

Services financiers et d'assurances

Le Cap, Afrique du Sud

15 450 employés répartis dans 860 agences

3
secondes pour migrer des applications privées vers AWS

125M
violations de politiques évitées en un an

3
mois pour déployer un Zero Trust complet zero trust

Défis

- L'architecture de sécurité basée sur le périmètre ne pouvait pas protéger de manière efficace les données financières sensibles contre les compromissions et les fuites
- Les appliances de sécurité traditionnelles telles que les pare-feu et les VPN étaient complexes à gérer et la productivité des utilisateurs en pâtissait
- La visibilité limitée sur l'expérience utilisateur empêchait une approche proactive de l'identification et de la résolution des incidents

Parcours par étapes

1. **Sécurisation de la connectivité directe à Internet et aux applications SaaS**, exploitant l'inspection du trafic pour éviter toute compromission des données
2. **Remplacement des appliances VPN traditionnelles par un accès Zero Trust** pour les applications privées et les données financières sensibles
3. **Utilisation des capacités avancées d'expérience numérique et d'informations exploitables** pour résoudre les problèmes d'expérience utilisateur récurrents

Résultats

- **Sécurise l'accès de 17 000 utilisateurs à Internet et aux applications cloud**, empêchant 125 millions de violations de politique par an
- **Protège une application bancaire privée à laquelle accèdent plus de 11 millions de clients** grâce à un accès Zero Trust basé sur des politiques
- **Accélère la transformation numérique :** quelques secondes suffisent pour migrer les applications vers AWS sans temps d'arrêt ni défaillances de la sécurité

Nous avons intégré la plateforme Zero Trust Exchange à notre environnement et nos agents logiciels de sécurité Zero Trust ont été déployés auprès de tous nos utilisateurs en trois mois.

Andrew Baker
Directeur technique, Capitec

Voir le témoignage client

noatum

Noatum déploie une suite de technologies Zscaler pour prendre en charge divers cas d'utilisation

Notamment l'accès sécurisé à Internet, aux SaaS et aux applications privées, l'amélioration de la détection des cybermenaces et l'optimisation de l'expérience utilisateur

NOATUM EN BREF

Noatum est un groupe multinational leader des services de transport et de logistique

- Services de transport
- Barcelone, Espagne
- Plus de 4 300 employés

Jour 1
Valeur immédiate de la plateforme

Zéro
dépendance aux VPN et aux pare-feu

360
degrés de quantification des risques

Défis

- Les VPN traditionnels exposaient trop l'entreprise aux cyberattaques lorsque les utilisateurs accédaient à Internet
- Les mesures de sécurité traditionnelles telles que les pare-feu empêchaient l'entreprise d'inspecter le trafic chiffré
- Les architectures basées sur le périmètre ont considérablement allongé le processus d'intégration des fusions et acquisitions

Parcours par étapes

1. **Remplacement des VPN** par une plateforme cloud pour permettre un accès sécurisé à Internet et aux applications privées
2. **Création d'un hub unique de surveillance d'expérience basé sur le cloud** avec ZDX
3. **Évalue les risques commerciaux** de manière globale avec Zscaler Risk360

Résultats

- **Permet le télétravail** en toute confiance grâce à un accès utilisateur sécurisé et homogène
- **Minimise les incidents utilisateurs** et améliore l'analyse des causes profondes, apportant connaissance et agilité
- **Améliore l'évaluation des risques** ainsi que la défense contre les menaces en dissimulant les systèmes et les applications sur Internet

Le problème était le VPN traditionnel, notre exposition aux services Internet et le risque de subir des attaques en permanence, c'est ce qui nous a vraiment poussés à chercher une solution comme Zscaler.

Josep Pou
RSSI, Noatum

Voir le témoignage client

Sanitas offre une connectivité sécurisée et homogène avec Zscaler Internet Access

Déploiement de protections pour Internet, SaaS et applications privées pour plus de 12 OOO utilisateurs, où qu'ils travaillent

SANITAS EN BREF

Sanitas Grande compagnie d'assurance médicale à forte croissance

Soins de santé et industrie pharmaceutique

Madrid, Espagne

Plus de 11 7OO employés en Espagne, en Europe et AMÉRIQUE LATINE

2,5
mois pour déployer à tous les utilisateurs

12–15k
d'utilisateurs protégés par notre plateforme

Zéro
besoin de se connecter à un data center

Défis

- Des unités commerciales distinctes signifiaient des moyens de sécurité distincts en l'absence d'un modèle basé sur le cloud
- Les VPN créaient un processus fastidieux d'authentification des utilisateurs assorti d'une sécurité médiocre
- Les bureaux des partenaires ne pouvaient pas se connecter aux data centers ni accéder aux applications

Parcours par étapes

1. Déploiement d'une solution Zero Trust homogène et basée sur le cloud pour sécuriser l'ensemble de l'entreprise à grande échelle
2. Remplacement des VPN par un modèle Zero Trust pour améliorer la connectivité pour tous les utilisateurs, quel que soit leur emplacement
3. Fourniture d'un accès sécurisé et homogène aux applications à tous les utilisateurs, y compris les partenaires

Résultats

- Sécurise 12 000 à 15 000 utilisateurs en deux mois et demi avec Zscaler Internet Access
- Permet le télétravail, favorisant ainsi la flexibilité et l'agilité de l'entreprise, avec une expérience similaire à celle du bureau
- Fournit un accès sécurisé aux workloads et aux applications

Les employés peuvent désormais travailler de chez eux, comme s'ils étaient au bureau, de manière transparente, flexible et extrêmement agile, et sans les contraintes que nous subissions auparavant avec d'autres solutions.

Antonio Cerezo
Responsable de la cybersécurité, Europe & Amérique latine

Voir le témoignage client

Colt Technology Services améliore la sécurité et l'expérience numérique avec Zero Trust Exchange

En s'associant à Zscaler pour déployer une architecture Zero Trust en trois mois, la société peut aider d'autres entreprises à réaliser la transformation de leur sécurité

COLT TECHNOLOGY SERVICES EN BREF

Fournit des services de réseau, vocaux et de data center à plus de 25 OOO entreprises dans le monde

Télécommunications

Londres, Royaume-Uni

Plus de 5 OOO employés dans 60 bureaux à travers le monde

5K
employés hybrides protégés

83 %
déploiement plus rapide que les solutions traditionnelles

100M
violations de la politique évitées chaque trimestre

Défis

- L'accélération de la migration vers le cloud pour prendre en charge un environnement de travail hybride avait augmenté la surface d'attaque et le risque de compromission
- Une solution proxy vieillissante ne pouvait pas gérer l'inspection inline du trafic chiffré, ce qui créait des angles morts propices aux malwares
- Les appliances VPN traditionnelles ne permettaient pas de déployer des politiques d'accès privé dynamique aux applications, ce qui compliquait le maintien du télétravail

Parcours par étapes

1. **Déploiement d'une architecture de sécurité Zero Trust cloud native** pour prendre en charge les opérations commerciales cloud-first et le travail hybride
2. **Fourniture d'un accès direct et sécurisé à Interne**, inspection de l'ensemble du trafic chiffré pour bloquer les menaces et la perte de données
3. **Remplacement des appliances VPN traditionnelles par un accès Zero Trust pour les applications privées**, facilitant et sécurisant le télétravail

Résultats

- **Offre une expérience numérique exceptionnelle à plus de 5 000 employés hybrides** tout en sécurisant le trafic sortant et entrant
- **Inspecte le trafic Internet à grande échelle**, traitant 6,7 milliards de transactions et bloquant 476 000 menaces de sécurité par trimestre
- **Prend en charge les politiques d'accès aux applications privées micro-segmentées et basées sur des politiques,** ce qui n'est pas possible avec les VPN traditionnels

Zscaler nous aide à améliorer à la fois l'expérience utilisateur et la sécurité. La plateforme Zscaler cloud native protège nos employés, quel que soit leur lieu de travail et les appareils qu'ils utilisent.

Ash Surti
Directeur des technologies numériques et de l'information, Colt Technology Services

Voir le témoignage client

Primetals Technologies crée un espace de travail hybride sécurisé avec Zscaler Zero Trust Exchange

Le leader mondial de la production de métaux abandonne les data centers et regroupe une pile de sécurité traditionnelle pour accélérer la transformation numérique avec Zscaler

PRIMETALS TECHNOLOGIES EN BREF

Leader mondial des solutions pour usines métallurgiques, spécialisé dans la production d'acier

High-Tech

Londres, Royaume-Uni

Plus de 7 500 collaborateurs

7,5K
utilisateurs sécurisés avec le Zero Trust

Jusqu'à 35 %
de réduction des coûts d'infrastructure

4,53/5
note de satisfaction des employés

Défis

- Une pile de sécurité traditionnelle construite autour de data centers ne pouvait pas évoluer pour prendre en charge une transformation numérique cloud-first
- Les appliances de sécurité traditionnelles, y compris les pare-feu et les VPN, n'étaient pas suffisamment agiles pour prendre en charge une nouvelle conception de réseau SD-WAN
- Les appliances VPN obsolètes ne sécurisaient pas de manière efficace la connectivité à distance pour un personnel hybride dispersé dans le monde entier

Parcours par étapes

1. **Déploiement d'une connectivité directe à Internet compatible avec le SD-WAN** pour rationaliser l'infrastructure et améliorer les performances
2. **Remplacement des VPN par un accès Zero Trust pour les applications privées** afin de permettre aux utilisateurs du monde entier de travailler en toute sécurité où qu'ils se trouvent{
3. **Exploitation des fonctionnalités avancées de surveillance de l'expérience utilisateur** pour garantir le fonctionnement optimal des outils de collaboration du personnel

Résultats

- **Simplifie la pile de sécurité**, réduit la dépendance aux data centers et diminue les dépenses liées aux coûts globaux d'infrastructure
- **Sécurise une connectivité sortante et entrante homogène** pour un groupe d'utilisateurs hybride, dont 25 % travaillent entièrement à distance
- **Réduit le volume des tickets d'assistance et résout plus rapidement les problèmes**, améliorant ainsi l'expérience de l'utilisateur final et allégeant les frais administratifs

Dans le cadre de notre transition vers le cloud, nous devions moderniser notre pile de sécurité... Zero Trust Exchange de Zscaler a joué un rôle essentiel pour tenir cet objectif.

Ralph Deleja-Hotko
Responsable des solutions back-end et cloud, Primetals Technologies

Voir le témoignage client

Unilever améliore la sécurité globale et permet un accès « juste suffisant » aux applications avec Zero Trust

Zscaler permet à Unilever de se passer des VPN, de fournir aux utilisateurs une connectivité directe et sécurisée aux applications et à Internet, et de rationaliser ses opérations dans 190 pays.

UNILEVER EN BREF

Société mondiale de biens de consommation dont les produits sont utilisés quotidiennement par 3,4 milliards de personnes

Production industrielle

Londres, Royaume-Uni

Ventes dans 190 pays

3Mrd+

Détail des transactions sécurisées chaque semaine

99,9 %

de disponibilité lors du traitement de 220 To de données en deux mois

1 500+

applications gérées avec un accès Zero Trust « juste suffisant »

Défis

- La flexibilité des VPN traditionnels était limitée et ils ne pouvaient pas évoluer avec la stratégie cloud mondiale d'Unilever
- Le modèle de sécurité traditionnel augmentait les risques en raison d'un contrôle d'accès et d'une visibilité insuffisants
- La demande croissante d'accès à distance avait mis à rude épreuve l'infrastructure VPN, impactant l'expérience utilisateur

Parcours par étapes

1. **Activation de l'accès sécurisé à Internet et SaaS pour les utilisateurs** avec une inspection complète du trafic TLS/SSL et une protection contre les menaces avancées
2. **Remplacement du VPN** par un accès Zero Trust aux applications privées
3. **Amélioration de l'expérience utilisateur** en fournissant une surveillance de l'expérience numérique pour identifier et résoudre rapidement les problèmes de performances

Résultats

- **Réduit les risques** grâce à un accès direct et sécurisé aux applications et sans les limitations et vulnérabilités du VPN
- **Améliore l'efficacité opérationnelle** en traitant le trafic de données à grande échelle avec une disponibilité de 99,99 %
- **Soutient la stratégie mondiale de cloud** en fournissant un accès à distance sécurisé dans 190 pays, préservant ainsi la flexibilité du personnel d'Unilever

L'approche Zero Trust de Zscaler a transformé la sécurité chez Unilever. L'élimination des engorgements inhérents aux VPN permet à notre personnel mondial d'accéder en toute sécurité aux applications, améliorant ainsi les performances, la flexibilité et la résilience.

Richard Mardling
Directeur de l'accès et de la connectivité, Unilever

Voir le témoignage client

APJ

Consultez les témoignages de clients par région

John Holland réduit les coûts de mise en réseau de 50 % grâce à Zscaler Zero Trust Exchange

Zscaler facilite la transition vers le SD-WAN et permet de supprimer des centaines de pare-feu, améliorant ainsi l'efficacité opérationnelle et la posture de sécurité

JOHN HOLLAND EN BREF

Entreprise intégrée d'infrastructures, de construction, de transport ferroviaire et multimodal

Construction

Melbourne, Victoria, Australie

Plus de 5 000 employés, répartis sur plus de 120 sites

1 semaine
pour déployer zero trust

6K
personnel et sous-traitants protégés

122K
menaces bloquées en trois mois

Défis

- Une architecture de sécurité périmétrique traditionnelle ne pouvait pas évoluer pour prendre en charge des opérations commerciales de plus en plus axées sur le cloud
- Un réseau MPLS obsolète reposait sur un important backhauling du trafic, ce qui ralentissait les services informatiques et augmentait les coûts
- Les appliances de pare-feu traditionnels n'étaient pas assez agiles pour inspecter le trafic chiffré inline, ce qui augmentait la vulnérabilité aux menaces

Parcours par étapes

1. **Déploiement d'une plateforme de sécurité Zero Trust complète et cloud native** pour créer un environnement informatique plus agile et évolutif
2. **Réduction de la dépendance aux appliances de pare-feu et des coûts de mise en réseau** grâce à un accès direct et sécurisé à Internet et aux applications SaaS
3. **Exploitation des fonctionnalités avancées de détection des menaces pour rationaliser l'écosystème de sécurité** et éliminer le risque de compromission des données

Résultats

- **Migre 100 % des utilisateurs vers Zero Trust en une semaine** et permet un provisionnement plus rapide de l'accès réseau sur plus de 120 sites de projet
- **Supprime des centaines d'appliances de pare-feu traditionnelles avec une connectivité Zero Trust**, réduisant de 50 % les coûts de mise en réseau
- **Sécurise la connectivité des utilisateurs**, traitant 400 To de trafic et prévenant 98 millions de violations de politique par trimestre

Zscaler fournit le reste de notre sécurité qui a simplifié nos processus, et par cette simplification, il a considérablement renforcé notre sécurité.

Kier Morrison
Directeur général, Opérations technologiques informatiques, John Holland

Voir le témoignage client

Probe CX abandonne progressivement ses VPN pour sécuriser 7 600 employés et applications critiques sur Zscaler Zero Trust Exchange

Zscaler rationalise la pile de sécurité, simplifie la gestion des politiques et réduit les dépenses technologiques tout en maintenant un haut niveau de sécurité

PROBE CX EN BREF

Un des plus grands prestataires de services d'externalisation de l'expérience client et des processus métier

Services

Melbourne, Victoria, Australie

19 000 collaborateurs, opérations dans 32 sites de livraison

100 %
des VPN sont supprimés

8,1 Mrd
de transactions traitées en un trimestre

3,1M
Menaces bloquées en trois mois

Défis

- Une architecture de sécurité traditionnelle ne pouvait pas s'adapter au développement rapide des effectifs ou à l'évolution d'une approche cloud-first
- Les VPN traditionnels ne permettaient pas d'appliquer des politiques de contrôle d'accès micro-segmentées, ce qui exposait davantage les applications privées
- La visibilité limitée sur l'expérience utilisateur et les performances des applications compliquait et ralentissait la résolution des incidents

Parcours par étapes

1. **Sécurisation de la connectivité directe à Internet et aux applications SaaS**, inspectant le trafic en ligne, sans devoir effectuer un backhauling
2. **Remplacement des VPN par un accès Zero Trust aux applications privées** afin de mieux protéger la propriété intellectuelle et les données critiques
3. **Exploitation des capacités avancées de l'expérience utilisateur** pour résoudre les problèmes plus rapidement et homogénéiser l'expérience de télétravail

Résultats

- **Offre une flexibilité de télétravail soutenue par les principes de Zero Trust** à 7 600 utilisateurs dans cinq pays
- **Traite environ 285 To de trafic par trimestre**, en appliquant des politiques de sécurité cohérentes et en minimisant la surface d'attaque
- **Simplifie la gestion de la sécurité avec une plateforme multi-entité** qui offre une sécurité Zero Trust à un moindre coût total de possession

La mise en œuvre de cette technologie nous a permis de supprimer 100 % de ces VPN de notre environnement, ce qui représente un avantage majeur.

Rohan Khanna
Directeur de la technologie, Probe CX

Voir le témoignage client

Persistent

Persistent renforce sa sécurité tout en économisant 2 millions de dollars en coûts d'investissement/d'exploitation d'une année sur l'autre

Zero Trust protège les données sensibles des clients et les données IP, favorise l'innovation, réduit la complexité et soutient les objectifs environnementaux, sociaux et de gouvernance (ESG)

PERSISTENT EN BREF

Un partenaire mondial d'ingénierie numérique et de modernisation d'entreprise qui aide les sociétés à faire progresser leurs innovations

High–Tech

Pune, Inde

23 000 employés dans 21 pays

85 %

d'amélioration de la posture de sécurité en éliminant les VPN

80+

attaques de haute priorité interceptées en 90 jours grâce à la tromperie

4X

accès plus rapide aux applications privées qu'avec un VPN

Défis

- Fournir aux télétravailleurs de 21 pays une connectivité rapide et une expérience utilisateur plus productive
- Protéger la propriété intellectuelle et les données sensibles des clients dans l'environnement cloud
- Simplifier une infrastructure complexe
- Réduire les coûts matériels et opérationnels dans l'ensemble de l'environnement
- Trouver un partenaire Zero Trust à long terme avec une solution évolutive qui favorise une expansion rapide
- Minimiser l'impact environnemental en réduisant l'empreinte carbone

Parcours par étapes

1. **Amélioration de la posture de sécurité** grâce à des connexions directes et sécurisées à Internet, aux applications SaaS et privées
2. **Réduction de la latence, diminution des coûts et amélioration de l'expérience utilisateur** en éliminant les VPN et les pare-feu peu fiables et non sécurisés
3. **Protection de la propriété intellectuelle et des données client grâce à** une technologie avancée de prévention de la perte de données (DLP) et de tromperie

Résultats

- **Améliore et accélère de 4 fois l'accès à distance** pour 23 000 collaborateurs répartis dans le monde
- **Élimine la complexité** et améliore l'efficacité et l'efficience de la sécurité
- **Accélère la détection et la réponse** grâce à l'intégration avec CrowdStrike, Microsoft Entra ID et Securonix
- **Élargit le portefeuille** d'offres de la société avec une pratique de sécurité axée sur Zscaler pour ses propres clients

Zscaler DLP procure à l'équipe de sécurité une vue granulaire de l'utilisation des applications d'IA génératives fantômes, y compris les invites de saisie, et applique le blocage DLP en temps réel et l'isolement des applications

Debashis Singh
Directeur de l'information, Persistent

Voir le témoignage client

社会医療法人財団善仙会
恵寿総合病院
Keiju Medical Center

Le Centre médical Keiju transforme les soins numériques aux patients grâce à Zscaler Zero Trust Exchange

Zscaler fournit une solution pour un accès mobile sécurisé aux données EMR, permet aux médecins de collaborer de n'importe où et améliore l'expérience des patients

CENTRE MEDICAL KEIJU EN BREF

Le seul hôpital de soutien médical de la région de Noto, reconnu comme un leader du numérique

Soins de santé et industrie pharmaceutique

Ville de Nanao, préfecture d'Ishikawa, Japon

Plus de 800 collaborateurs pour plus de 400 lits

800
staff médical protégé

100s
appareils mobiles connectés en toute sécurité

1
plateforme pour une sécurité Zero Trust

Défis

- Une architecture de sécurité basée sur le périmètre ne pouvait pas s'adapter à l'accroissement de la demande de soins numériques et de télémédecine
- Les pare-feu traditionnels ne pouvaient pas sécuriser la connectivité Internet à distance, ce qui limitait le recrutement de médecins à une petite zone locale
- Les VPN traditionnels exposaient davantage les applications et ressources privées, notamment les données sensibles des patients, à des risques de compromission

Parcours par étapes

1. **Déploiement d'une architecture de sécurité Zero Trust cloud native** pour soutenir d'autres moyens de fournir des soins numériques aux patients
2. **Introduction d'une connectivité sécurisée et directe à Internet**, permettant au personnel médical de travailler de manière flexible et sûre depuis n'importe quel emplacement
3. **Suppression des appliances VPN et adoption de l'accès Zero Trust** aux applications privées afin de protéger l'accès à distance aux données EMR

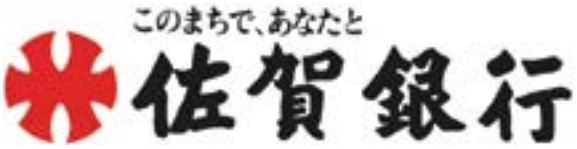
Résultats

- **Permet au personnel médical de travailler de n'importe où** et élargit les possibilités de recrutement de médecins de qualité
- **Protège les dossiers sensibles des patients contre les menaces** lorsqu'ils sont consultés à distance : plus de 500 appareils mobiles se connectent en toute sécurité aux données EMR
- **Élimine le besoin d'appliances de sécurité traditionnels** et améliore l'efficacité opérationnelle, pour de meilleurs soins aux patients

La transformation numérique est essentielle pour permettre au personnel de travailler efficacement avec des ressources limitées. De nombreux médecins vivent plus loin [...] nous avions donc besoin d'un environnement d'accès à distance sécurisé et facile à utiliser.

M. Masahiro Kamino
Président du Conseil d'Administration, Centre médical Keiju

Voir le témoignage client



The Bank of Saga soutient la transformation numérique sur Zscaler Zero Trust Exchange

Zscaler rationalise l'infrastructure, réduit la dépendance aux solutions traditionnelles, et renforce la posture de sécurité à mesure que les opérations bancaires migrent vers le cloud

THE BANK OF SAGA EN BREF

Fournisseur de services financiers axé sur la communauté, qui s'efforce d'améliorer la commodité pour le client

Services financiers et d'assurances

Ville de Saga, préfecture de Saga, Japon

Plus de 1 200 employés

~33 %
des coûts de communication en moins

1,8K
d'utilisateurs sécurisés avec le Zero Trust

Un
authentification unique dope la productivité

Défis

- Une architecture de sécurité traditionnelle basée sur le périmètre ne permettrait pas à la banque de poursuivre ses efforts de migration vers le cloud
- Les appliances de sécurité traditionnelles n'étaient pas suffisamment flexibles pour s'adapter à l'augmentation de la demande d'une connectivité Internet directe et fiable
- La maintenance des VPN était coûteuse et ceux-ci élargissaient la surface d'attaque, exposant les applications et données privées aux menaces

Parcours par étapes

1. **Déploiement d'une plateforme Zero Trust complète et cloud native** pour appliquer des politiques de sécurité cohérentes à l'échelle de la société
2. **Introduction d'une connectivité directe à Internet** et exploitation de l'inspection du trafic inline pour sécuriser l'accès aux applications SaaS publiques
3. **Remplacement des VPN par un accès Zero Trust aux applications privées**, en exploitant des options de configuration granulaires pour protéger les données critiques

Résultats

- **Sécurise la connectivité sortante et entrante des employés**, en appliquant des politiques d'accès cohérentes quel que soit l'emplacement
- **Protège les applications bancaires privées et les données critiques contre toute compromission**, sécurisant et améliorant l'expérience client
- **Rationalise la pile de sécurité et remplace les appliances traditionnelles**, simplifiant ainsi la gestion des politiques et réduisant les coûts

Un passage vers le cloud est indispensable à la transformation numérique. … [Cependant,] la limite de sécurité conventionnelle ne permet pas de tirer pleinement parti de la commodité du SaaS et des services web. La sécurité Zero Trust était essentielle.

M. Hiroaki Hayashida
Directeur adjoint, Groupe de planification et de développement des systèmes, Département des systèmes, Siège social de la gestion des affaires, The Bank of Saga

Voir le témoignage client

Cebu Pacific Air sécurise son personnel hybride avec Zscaler Zero Trust Exchange

Zscaler améliore l'expérience de télétravail de 3 900 employés et protège les opérations commerciales critiques dans sept pôles stratégiques en Asie

CEBU PACIFIC AIR EN BREF

Compagnie aérienne leader aux Philippines, opérant des vols vers plus de 60 destinations

Services de transport

Manille, Philippines

3 900 employés répartis dans sept pôles stratégiques

234M

de violations de la politique évitées chaque trimestre

90 %

d'augmentation de la satisfaction des utilisateurs

2

semaines pour déployer l'accès Zero Trust aux applications distantes

Défis

- Une infrastructure de sécurité traditionnelle ralentissait les efforts de transformation numérique et augmentait le risque de compromission et de menaces
- Les appliances de sécurité traditionnelles ne pouvaient pas protéger de manière adéquate les ressources privées essentielles aux opérations commerciales
- Les appliances VPN étaient confrontées à des problèmes de performance et de connectivité, rendant le télétravail plus difficile et moins sécurisé

Parcours par étapes

1. **Abandon d'une architecture de sécurité traditionnelle obsolète**, au profit du déploiement d'une plateforme cloud native Zero Trust complète
2. **Fourniture d'un accès Internet direct et sécurisé avec des fonctionnalités de protection contre les menaces avancées** pour mieux prendre en charge un personnel hybride
3. **Remplacement des appliances VPN traditionnelles par un accès Zero Trust** pour appliquer des contrôles d'accès granulaires aux applications privées

Résultats

- **Sécurise la connectivité du télétravail pour 3 900 utilisateurs avec une alternative au VPN sécurisée**, améliorant ainsi de 90 % la satisfaction des utilisateurs
- **Rationalise la pile de sécurité tout en offrant une protection solide**— traite 733 millions de transactions par an
- **Empêche 234 millions de violations de politique et bloque 45 000 menaces de sécurité en un seul trimestre**, améliorant ainsi la posture de sécurité

Notre environnement de travail est dynamique et avec Zscaler, les employés peuvent continuer à travailler de manière productive et conservent leur capacité à se connecter aux ressources dont ils ont besoin sans compromettre la sécurité.

Laureen Cansana
CIO, Cebu Pacific Air

Voir le témoignage client

maxeon

Maxeon Solar Technologies réalise sa transformation numérique avec Zscaler à la suite d'une cession

Le leader de l'énergie solaire élimine les data centers pour améliorer la sécurité et les expériences de télétravail de 5 000 utilisateurs dans le monde sur la plateforme Zero Trust Exchange

MAXEON EN BREF

Fabricant mondial de panneaux solaires avec une présence commerciale dans plus de 100 pays

Énergie, pétrole, gaz et mines

Singapour

5 000 employés, répartis sur 40 sites

134 %
de trafic traité en plus chaque trimestre

31M
de violations de politiques évitées en un trimestre

2,9 millions
de menaces bloquées en trois mois

Défis

- La sécurité du périmètre traditionnelle, bâtie autour des data centers, ne prendrait pas en charge une infrastructure évolutive cloud-first
- Les pare-feu existants ne pouvaient pas s'adapter à l'accroissement des besoins d'accès à distance, ce qui nuisait aux performances et augmentait les risques
- La gestion des solutions DLP antérieures était compliquée, ce qui exposait la propriété intellectuelle et les actifs critiques à des risques

Parcours par étapes

1. **Sécurisation de la connectivité directe à Internet avec inspection du trafic inline** pour protéger les utilisateurs partout où ils ont besoin d'un accès en ligne
2. **Déploiement d'une solution de surveillance de l'expérience spécialement conçue pour le Zero Trust** afin de rationaliser les processus d'intégration et d'octroi de licences
3. **Introduction d'une solution DLP intégrée** pour protéger les informations critiques, garantir la conformité et prévenir les violations de données

Résultats

- **Accélère la transformation numérique :** tous les data centers sont mis hors service et 70 % des workloads ont migré vers le cloud
- **Offre la flexibilité sécurisée du télétravail** à un groupe d'utilisateurs dispersés géographiquement dans 16 pays
- **Protège les données IP stratégiques, dont plus de 1 400 brevets**, améliorant ainsi la posture de sécurité et garantissant la continuité d'activité

Après avoir évalué plusieurs fournisseurs de renom, Zscaler s'est clairement imposé grâce à sa position dominante dans le Magic Quadrant de Gartner et à ses capacités éprouvées.

Stephen Gani
RSSI, Maxeon Solar Technologies

Voir le témoignage client