Zero Trust + IA

La sécurité optimale
et intelligente de
votre entreprise

LIVRE BLANC

Le Zero Trust et l'IA sont nécessaires. Pourquoi ?

Les méthodes de travail actuelles ont profondément évolué. Autrefois, les collaborateurs venaient au bureau tous les jours. Ils accédaient aux applications et ressources informatiques hébergées dans les data centers sur site de leur entreprise. En d'autres termes, les utilisateurs, les applications et les données étant tous regroupés au bureau, et les entreprises opéraient essentiellement dans un contexte sur site (on-premises). Cependant, deux tendances qui se renforcent mutuellement ont modifié à jamais ce statu quo.

Tout d'abord, l'essor du cloud et des applications SaaS (Software-as-a-Service) comme Salesforce et Microsoft 365 a affranchi les entreprises du développement et de la gestion de leurs ressources informatiques sur site. Elles ont commencé à faire appel à des applications et outils fournis en tant que service à partir des clouds de leurs fournisseurs. Cette flexibilité a été un moteur de dynamisme pour les entreprises, mais aussi un levier de maîtrise des coûts.

Deuxièmement, l'adoption des applications cloud a été un catalyseur de cette tendance qu'est le télétravail. Les ressources informatiques étant hors site, les utilisateurs n'avaient plus besoin de se rendre au bureau pour y accéder. Naturellement, la pandémie mondiale de 2020 a accéléré l'adoption du télétravail (et des applications cloud), les entreprises tentant de préserver leur productivité tout en se conformant aux obligations de confinement. Une fois de plus, la flexibilité accrue a favorisé le dynamisme et la maîtrise des coûts.

Ces transformations, bien que parfaitement utiles, ont engendré d'importants défis liés aux cyber-risques et à la pression concurrentielle :

- Les cyber-risques ont augmenté parce que les modèles traditionnels de sécurité cloisonnées n'ont pas été conçus pour le cloud ni le télétravail, et n'ont pas pu s'adapter à la sophistication croissante des menaces modernes.
- Les pressions concurrentielles se sont accrues parce que l'amélioration de la productivité et le dynamisme sont devenus la norme, mettant les organisations au défi d'être aussi performantes que possible tout en répondant le plus rapidement possible aux attentes croissantes des clients.

Pour réussir aujourd'hui, les entreprises doivent relever ce double défi de productivité et de dynamisme. À ce titre, l'émergence de l'intelligence artificielle et de l'apprentissage automatique (IA/AA) constitue un autre phénomène majeur. En très peu de temps, l'IA s'est généralisé sur le lieu de travail moderne, tant au niveau des solutions métiers que des outils de cybersécurité. Il est tentant de réduire l'IA à un simple buzzword marketing. Pourtant, cet IA est la clé pour répondre aux deux défis susmentionnés, notamment lorsque l'IA est associée au Zero Trust. C'est la raison pour laquelle d'innombrables entreprises dans le monde se tournent vers Zscaler.

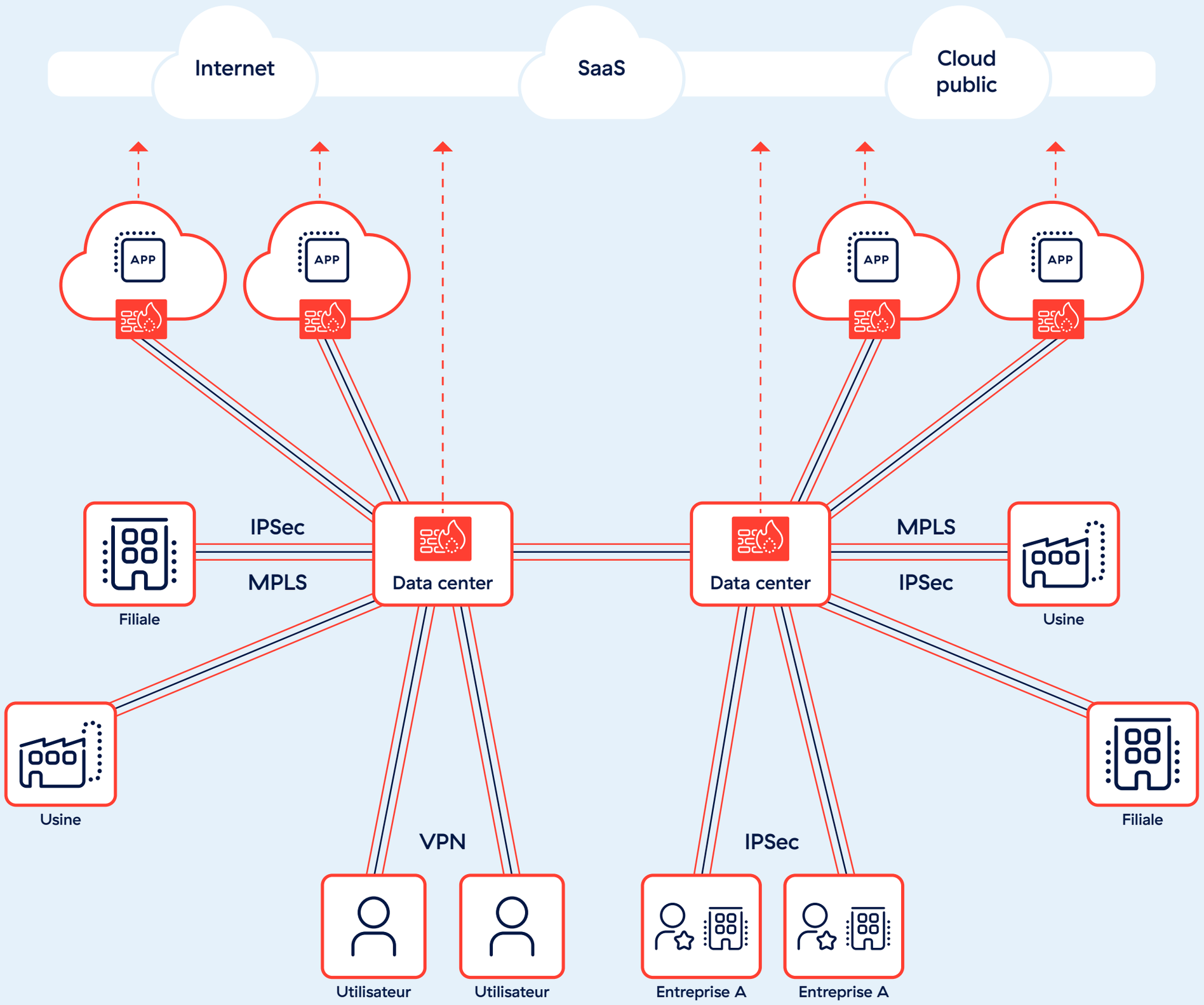
Zero Trust + IA avec Zscaler

La plateforme cloud native Zscaler Zero Trust Exchange offre une architecture Zero Trust qui mise sur l'IA/AA (Intelligence Artificielle/Apprentissage Auromatique) pour renforcer ses capacités. Ce mix pertinent entre architecture Zero Trust et IA répond aux deux problématiques susmentionnées, à savoir la recrudescence des risques et cette pression d'en faire toujours plus avec moins. Pour en comprendre les raisons, examinons chacun de ces deux éléments.

ARCHITECTURE ZERO TRUST

Le Zero Trust n'est pas un nouvel outil autonome de sécurité. Il s'agit plutôt d'une approche fondamentalement différente, distincte des architectures de sécurité standards basées sur le périmètre, et exempte des défauts méthodologiques du passé. C'est pourquoi il est important de capitaliser que le modèle Zero Trust comme socle pour déployer l'IA dans le domaine de la sécurité. Dans le cas contraire, faire appel à l'IA pour améliorer une architecture de sécurité périmétrique reviendrait à polir un miroir brisé : son éclat peut s'améliorer, mais il reste intrinsèquement défectueux.

Architecture orientée pare-feu et VPN



Un réseau de confiance interconnecte les utilisateurs, les sites et les applications. La protection contre les menaces et des données impliquent de sécuriser le réseau.

C'est rigide, complexe, présente un risque pour la sécurité et constitue un obstacle à la transformation.

Illustration 1 : Architecture basée sur le périmètre

Les architectures périmétriques, reposant sur des outils tels que les pare-feu et les VPN, se contentent d'établir un périmètre sécurisé autour du réseau en étoile d'une entreprise. C'est la raison pour laquelle on les appelle souvent des modèles de sécurité cloisonnée. Les architectures basées sur le périmètre ont été conçues pour les environnements sur site uniquement, bien avant l'essor des applications cloud et du télétravail. Ces architectures posent un certain nombre de problématiques aux entreprises qui essaient de les utiliser aujourd'hui :

- Ils élargissent la surface d'attaque en étendant le réseau à davantage d'utilisateurs, d'appareils, de clouds et d'emplacements, et en utilisant des pare-feu et des VPN, qui dont les adresses IP sont publiques.
- Ils favorisent la compromission parce que leurs appareils sous-jacents (matériels et virtuels) manquent de l'évolutivité nécessaire pour inspecter le trafic chiffré à l'échelle, **où se cachent 86 % des menaces**.
- Ils ne parviennent pas à arrêter le déplacement latéral des menaces car ils placent les utilisateurs et les entités sur le réseau, où ils peuvent accéder aux diverses ressources connectées.
- Ils ne peuvent pas éliminer la perte de données en raison de leur incapacité à évoluer et à inspecter le trafic chiffré, et à sécuriser les voies de fuite modernes telles que le partage dans les applications SaaS.
- Ils augmentent la complexité et les coûts liés à une myriade de produits de sécurité ponctuels et de réseaux tentaculaires, dont l'achat, la configuration et la maintenance sont coûteux.
- Ils nuisent à la productivité des utilisateurs parce qu'ils requièrent le backhauling du trafic vers un data center centralisé, ce qui ajoute une latence qui perturbe les expériences numériques.

L'année 2024 a été marquée par une série de vulnérabilités des pare-feu et VPN chez **Ivanti**, **Cisco** et **Palo Alto Networks**, soulignant la nécessité de retirer ces outils et d'adopter une architecture Zero Trust.

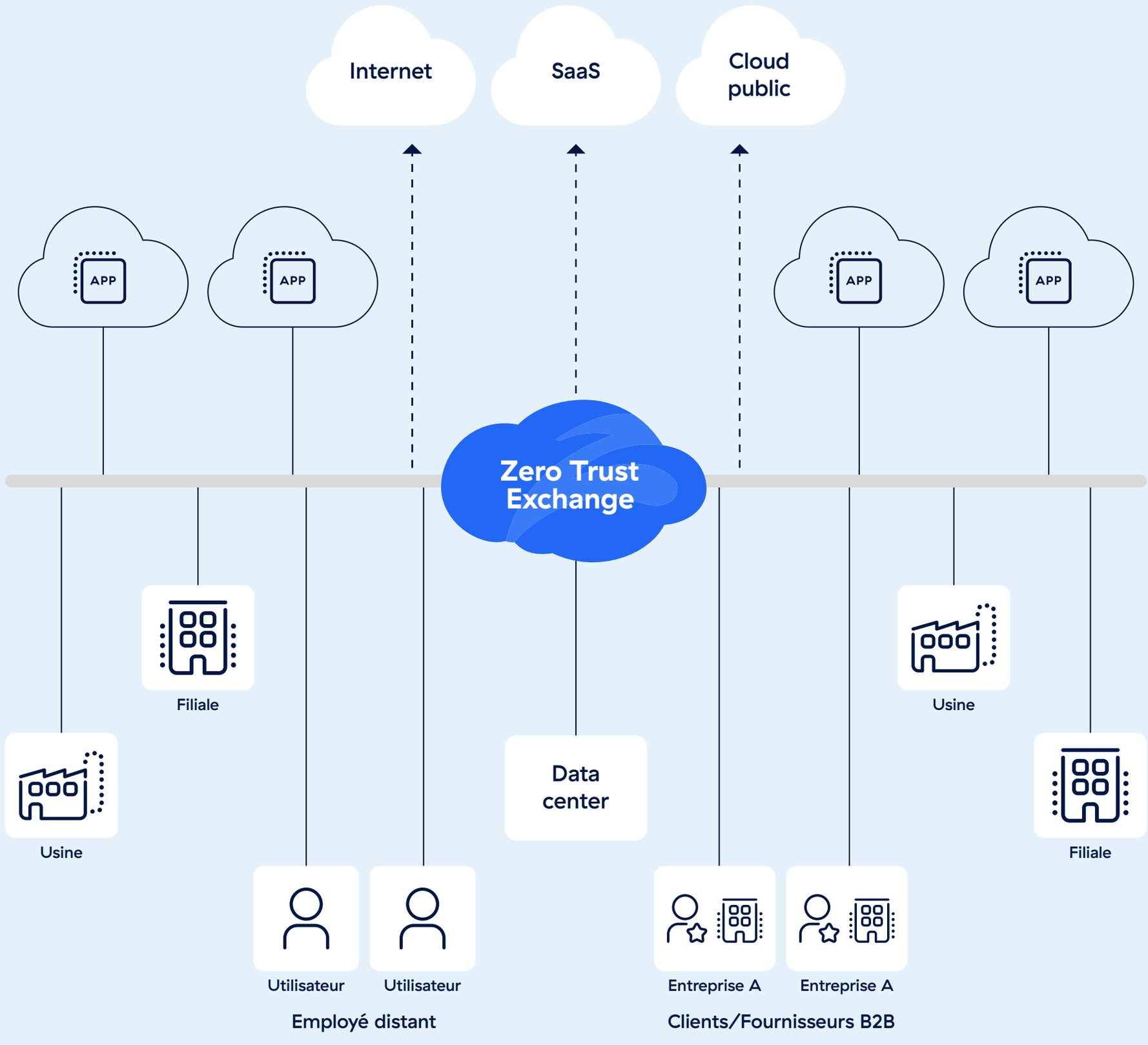


Illustration 2 : Architecture Zero Trust avec Zscaler

Comme nous l'avons mentionné, le Zero Trust est fondamentalement différent des architectures basées sur le périmètre. Loin d'être une simple ligne de défense protégeant le réseau coporate, le Zero Trust agit comme un commutateur intelligent qui fournit une connectivité sécurisée any-to-any, en mode one-to-one : les utilisateurs se connectent directement aux applications plutôt qu'au réseau dans son ensemble. Les éléments de contexte sont pris en compte pour déterminer qui peut accéder à quoi. En d'autres termes, Zscaler dissocie la sécurité et la connectivité de l'accès au réseau et applique le principe d'un accès sur la base du moindre privilège. Cette connectivité Zero Trust et de multiples autres fonctionnalités sont fournies sous forme de service, au niveau de l'edge, par Zero

Trust Exchange, le cloud de sécurité mondial hautes performances de Zscaler. Le backhauling du trafic n'est désormais plus nécessaire.

Avec Zscaler, l'architecture Zero Trust :

- Minimise la surface d'attaque en arrêtant l'expansion sans fin du réseau, en éliminant le besoin de pare-feu, de VPN et de leurs adresses IP publiques, et en dissimulant les applications derrière Zscaler
- Stoppe les compromis grâce à un nuage de sécurité haute performance qui évolue en fonction des besoins pour inspecter n'importe quel volume de trafic chiffré et appliquer des politiques en temps réel.
- Empêche le déplacement latéral des menaces en connectant les utilisateurs directement aux applications auxquelles ils sont autorisés à accéder plutôt qu'au réseau avec ses nombreuses ressources connectées
- Bloque la perte de données, qu'elle soit malveillante ou accidentelle, sur tous les vecteurs de fuite de données, dont le trafic chiffré, les applications cloud et les terminaux.
- Réduit les coûts et la complexité en simplifiant la mise en réseau avec une connectivité directe à l'application et en éliminant les produits de sécurité ponctuels grâce à une plateforme complète
- Renforce la productivité en améliorant l'expérience utilisateur grâce à la connectivité directe avec les applications et à l'acheminement du trafic par le chemin le plus court jusqu'à sa destination.

Avec tous ces atouts, le Zero Trust propose l'architecture idéale pour déployer des fonctionnalités IA et AA.

LEADERSHIP EN MATIÈRE D'IA

Zscaler assure des avantages majeurs dans le domaine de l'IA/AA. En effet, l'efficacité de l'IA dépend en grande partie de la qualité des données d'entraînement. Des données non pertinentes en entrée donnent lieu à des résultats médiocres.

Plus vaste plateforme de sécurité au monde, le Zero Trust Exchange de Zscaler offre une connectivité sécurisée en tant que service à des milliers d'entreprises représentant plus de 40 millions d'utilisateurs dans le monde, sans compter d'innombrables workloads, dispositifs IoT/OT, collaborateurs tiers, et bien plus encore. Cette envergure permet à Zscaler de traiter plus de 500 milliards de transactions chaque jour (plus de 45 fois le nombre de recherches quotidiennes sur Google), ainsi que 500 000 milliards de signaux de télémétrie quotidiens. Zscaler examine minutieusement les éléments de contexte afin de piloter en toute sécurité l'accès aux ressources informatiques. L'éventail des données traitées est large et porte sur les identités, les dispositifs, les contenus, les destinations et le réseau, et ce, pour chaque tentative d'accès. De plus, Zscaler capitalise sur les données provenant de ThreatLabz, notre équipe interne de recherche sur les menaces qui étudie en permanence les tactiques, techniques et technologies utilisées par les cybercriminels. Zscaler capitalise ainsi sur des années de recherches et d'études sur les cybermenaces, leur mode opératoire et leur sophistication croissante.

Zscaler Data Fabric for Security bénéficie de plus de 150 intégrations prédéfinies avec une diversité de solutions de sécurité et métiers. Les sources de données de sécurité sont notamment des scanners de vulnérabilité tels que Tenable, Qualys et Wiz, des solutions de détection et de réponse aux menaces sur les terminaux (EDR) telles que CrowdStrike, des outils de gestion des identités tels que ceux d'Okta, de Ping Identity et de Microsoft, et plus de 60 flux d'informations sur les menaces. Les sources de données métiers incluent SAP pour les données de coûts et de licences, Workday pour les informations sur la structure organisationnelle, ServiceNow pour la base de données de gestion des configuration, etc. Zscaler ingère les données à partir de ces sources, les associe à ses ensembles de données propriétaires, les duplique et les enrichit. Il n'est pas nécessaire de regrouper manuellement les données provenant de plusieurs sources en un seul emplacement : Zscaler gère automatiquement le processus.

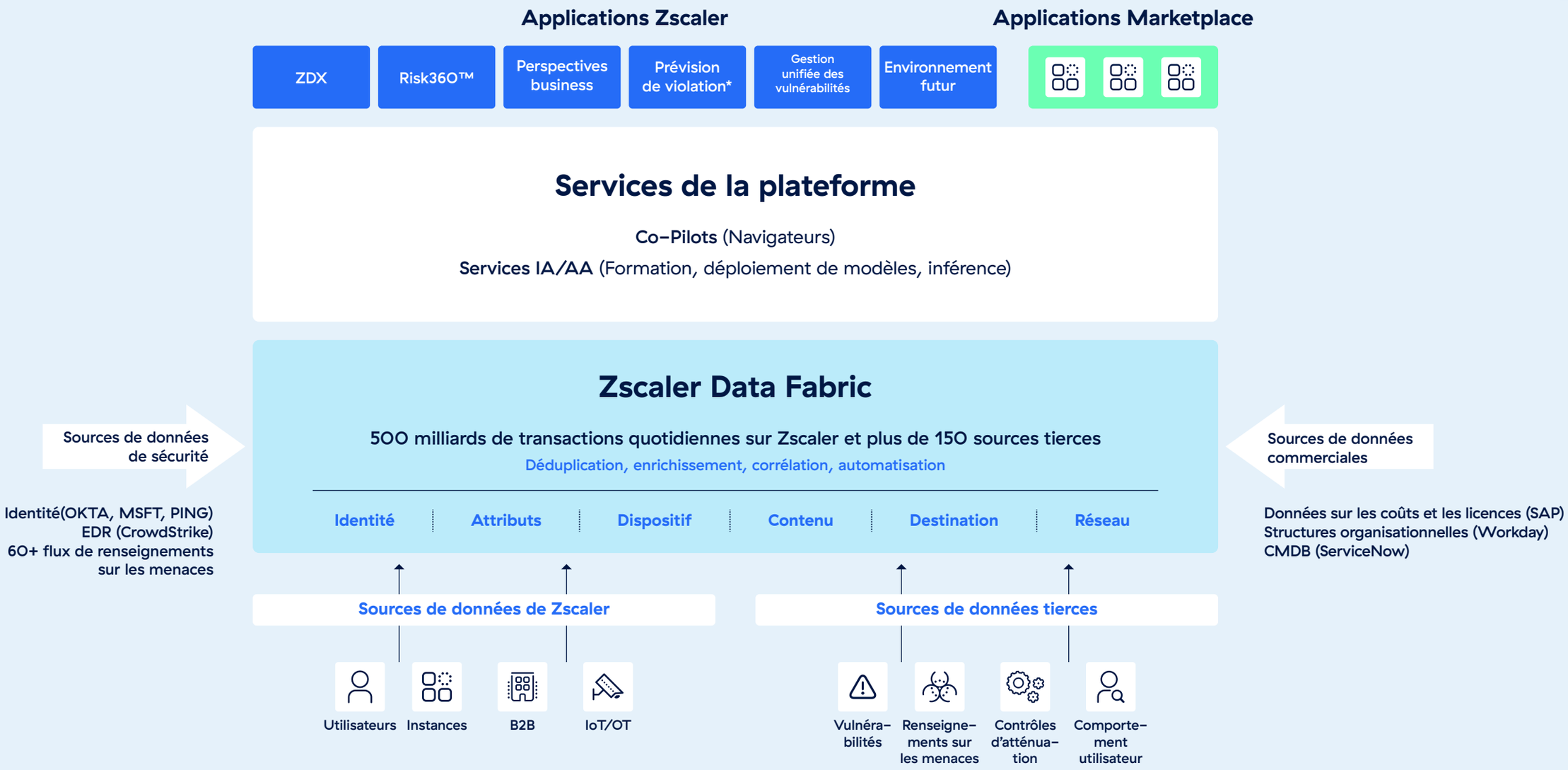


Illustration 3 : Leadership et avantages de Zscaler en matière d'IA

Grâce à ce vaste référentiel de données pertinentes, qui permettent d'entraîner de grands modèles de langage (LLM) conçus sur mesure, Zscaler accélère les prises de décision sur la base des données. Les solutions optimisées par IA de Zero Trust Exchange offrent des options sophistiquées en matière de traitement analytique, d'automatisation et de productivité. Nous détaillerons dans la suite de ce livre blanc les différentes façons dont la plateforme Zscaler exploite l'IA/AA pour relever les défis modernes, afin de vous aider à sécuriser et à optimiser votre entreprise.

Sécuriser votre entreprise avec Zscaler

L'architecture Zero Trust pallie les carences des architectures périmétriques et offre, à ce titre, une sécurité plus robuste et une maîtrise des cyber-risques. Cependant, la force d'une architecture Zero Trust associée à des fonctionnalités de sécurité de pointe optimisées par IA étaye les les défenses des entreprises contre les cybercriminels et les menaces avancées. Zscaler propose à la fois une architecture Zero Trust et des fonctionnalités pilotées par IA pour réduire les risques mais aussi améliorer la productivité des utilisateurs et des administrateurs.

Sandbox cloud, optimisée par IA

Face à la sophistication croissante des cybermenaces, les entreprises doivent pouvoir compter sur des capacités temps-réel de détection et de maîtrise des risques. Dans le cas contraire,

elles peuvent facilement être compromises par des cybercriminels astucieux utilisant des techniques furtives qui évoluent constamment. La technologie de Sandbox est conçue pour exécuter des fichiers potentiellement malveillants au sein d'un environnement sûr, à distance des utilisateurs, afin de déterminer si l'accès à ces fichiers est sans danger.

Malheureusement, les méthodes traditionnelles d'analyse en sandbox impliquent souvent d'arbitrer entre sécurité et productivité. Si les critères de la sandbox sont trop laxistes, des fichiers malveillants peuvent se frayer un chemin vers les dispositifs des utilisateurs et s'immiscer au sein des entreprises. Si les critères du sandbox sont trop stricts, il est davantage probable que des fichiers inoffensifs soient mis en quarantaine, que l'accès des utilisateurs à ces fichiers soit impossible pendant plusieurs minutes et que la productivité en pâtisse.

Zero Trust Exchange tire parti de l'IA en proposant une sandbox qui associe sécurité et productivité.

L'intégration de l'AA dans Zscaler Sandbox garantit une détection plus fiable, dans la mesure où le modèle AA a été entraîné et affiné sur la base d'années d'analyses et d'interactions avec plus de 550 millions d'échantillons de fichiers.

Lorsque les administrateurs activent le paramètre « AI Instant Verdict » via un simple clic, les fichiers réputés malveillants dont le score IA/AA de menace est compris entre 91 et 100 sont automatiquement neutralisés, sans que l'utilisateur ait à patienter pendant que le fichier est exécuté ailleurs.
La protection devient immédiate contre les menaces zero-day utilisant des fichiers, sans impact sur la productivité des utilisateurs. De plus, la neutralisation instantanée des fichiers réputés malveillants minimise le nombre d'incidents zero-day potentiels à analyser, réduisant ainsi la charge de travail des équipes SOC, ce qui leur permet de se consacrer à d'autres projets de sécurité plus stratégiques.
En d'autres termes, les entreprises peuvent se protéger des menaces tout en préservant le temps de travail des équipes SOC et des utilisateurs finaux.

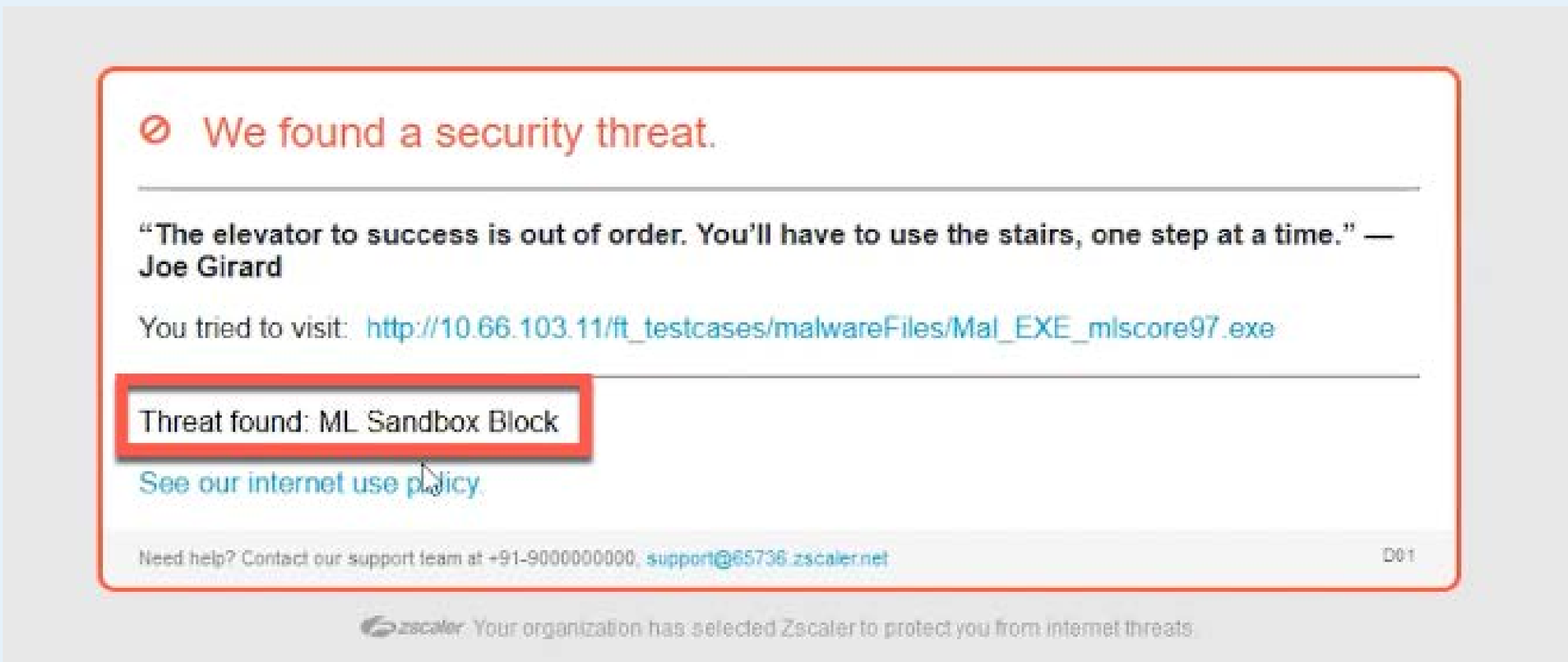


Illustration 4 : Notification utilisateur d'AI Instant Verdict

Smart Browser Isolation

Les cybercriminels utilisent des sites Web malveillants pour télécharger des contenus malveillants sur les navigateurs et les dispositifs des utilisateurs, créant ainsi une tête de pont pour lancer leurs attaques contre les entreprises des utilisateurs. Les outils de filtrage d'URL capables de bloquer l'accès à divers sites Web permettent de traiter cette problématique. En règle générale, ils filtrent les sites web malveillants connus ainsi que les domaines nouvellement enregistrés dont la fiabilité n'a pas encore été démontrée. Cette approche présente hélas certaines faiblesses majeures. En premier lieu, des sites Web fiables et éprouvés peuvent toujours diffuser, sans le savoir, du contenu malveillant, via des publicités ou des iframes zéro pixel positionnées par des cybercriminels par exemple. En outre, neutraliser tous les domaines nouvellement enregistrés perturbe la productivité des utilisateurs en les empêchant d'accéder à des outils Web nouveaux, mais légitimes, ainsi qu'à des sites Web existants et fiables dont les domaines ont simplement été mis à jour. Dans les deux cas, les nombreuses demandes de support qui en résulte pèsent sur la productivité du service informatique.

Zscaler Smart Browser Isolation répond parfaitement à ces défis de sécurité et de productivité. La solution est qualifiée de « smart » (intelligente), avec ses modèles IA et AA qui lui permettent de reconnaître automatiquement les contenus Web potentiellement malveillants. Les entreprises gardent ainsi une longueur d'avance sur les menaces émergentes associées à des domaines nouvellement enregistrés, ainsi que sur les menaces dissimulées dans des domaines de confiance.

Avec Smart Browser Isolation, lorsqu'un utilisateur visite un site web considéré comme suspect par l'IA, la session de l'utilisateur est « cloisonnée ».
Ceci signifie que la session Web est migrée vers Zero Trust Exchange et que seuls des pixels/images de la session sont renvoyés par le cloud Zscaler vers le dispositif de l'utilisateur final. Les flux d'images de la session cloisonnée apparaissent de manière normale chez l'utilisateur, mais celui-ci n'interagit pas directement avec le site web, ce qui empêche tout contenu malveillant de cibler son terminal. Les tentatives de téléchargement de menaces ne peuvent donc pas atteindre le dispositif, tandis que les fuites de données potentielles peuvent être contrôlées, en empêchant tout chargement de fichiers et le copier/coller de texte. Les risques sont ainsi maîtrisés, sans blocages excessifs qui empêcheraient l'accès aux outils Web légitimes indispensables aux utilisateurs. Cette approche implique un nombre moins important de demandes de support et contribue à la productivité tant des utilisateurs que des équipes informatiques.

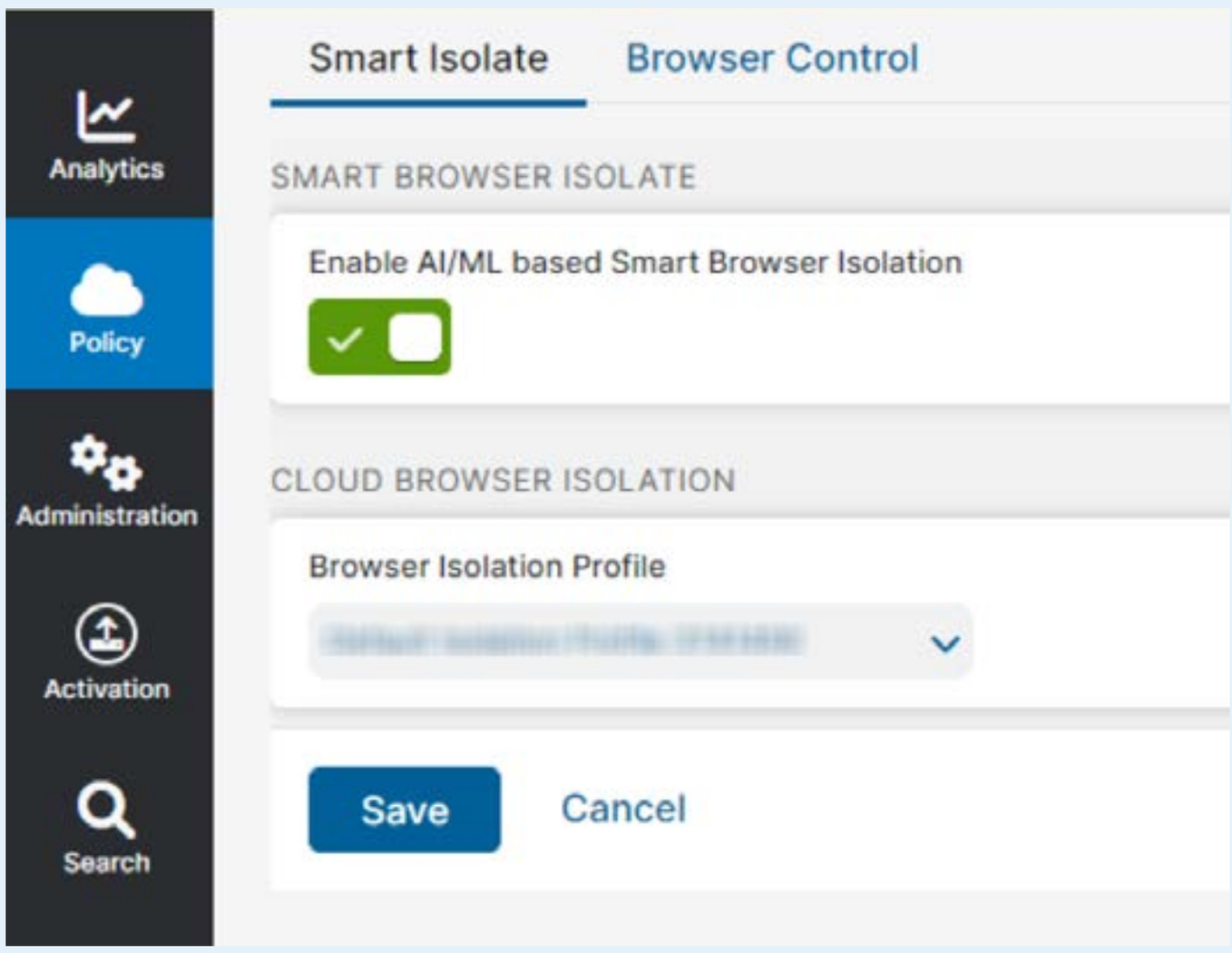


Illustration 5 : Activation en un clic de Smart Browser Isolation

Segmentation des applications optimisée par l'IA

Les entreprises qui s'appuient sur des architectures de sécurité centrées sur le réseau et conçues avec des outils traditionnels tels que des pare-feux peinent à prévenir le déplacement latéral de menaces. Comme nous l'avons déjà mentionné, le déplacement latéral fait référence à la manière dont des assaillants présents sur le réseau peuvent se mouvoir entre les ressources connectées et accéder à leurs données sensibles. Faute d'une segmentation efficace pour empêcher cela, le rayon d'action d'une attaque peut être considérable, permettant des fuites de données à grande échelle ainsi que des préjudices financiers et de réputation considérables.

Malheureusement, les entreprises ont généralement du mal à déployer et à maintenir des pratiques de segmentation réseau solides. Les méthodes traditionnelles reposent sur une configuration manuelle, qui est sujette aux erreurs humaines et peut entraîner des erreurs de configuration qui exposent des ressources critiques. De plus, la nature dynamique des réseaux modernes, avec l'adoption croissante des services cloud et du télétravail, ne permet pas de suivre les changements constants dans la topologie des réseaux et les demandes d'accès des utilisateurs. Cette complexité augmente les coûts de gestion et entrave encore davantage la capacité à déployer des stratégies de segmentation efficaces.

Comme expliqué précédemment, l'architecture Zero Trust avec Zscaler consiste à fournir un accès direct aux applications, sans transiter via le réseau. Cette segmentation Zero Trust prévient les déplacements latéraux pour les utilisateurs, les instances, les sites distants et les dispositifs. Pour réduire davantage le rayon d'impact potentiel d'une intrusion, Zscaler propose une segmentation des applications optimisée par l'IA. En tirant partir de l'intelligence artificielle, Zscaler crée automatiquement des segments applicatifs pertinents pour les clients.

Cette segmentation optimisée par IA surveille et analyse en permanence le comportement des utilisateurs et l'utilisation des applications. Elle s'appuie sur des algorithmes d'AA pour identifier les modèles et les anomalies, afin de déterminer les collaborateurs qui ont besoin d'accéder à quelles applications. Par exemple, si seul un petit sous-ensemble de collaborateurs accède à une application financière, Zscaler créera automatiquement un segment qui restreint l'accès applicatif à ce groupe d'utilisateurs. Cette approche ciblée réduit considérablement les possibilités de déplacement latéral d'une application à une autre.

Cette segmentation par IA constitue une approche fondamentalement nouvelle. Elle identifie avec précision et limite l'accès aux applications sensibles de manière proactive et automatique. En simplifiant le processus de segmentation, elle élimine les complexités, les erreurs et les risques associés aux méthodes traditionnelles. Il en résulte une charge moindre en matière de gestion et de configuration manuelle, d'où un gain de temps et de ressources pour les équipes informatiques, leur permettant de concentrer leurs efforts sur d'autres tâches de sécurité essentielles.

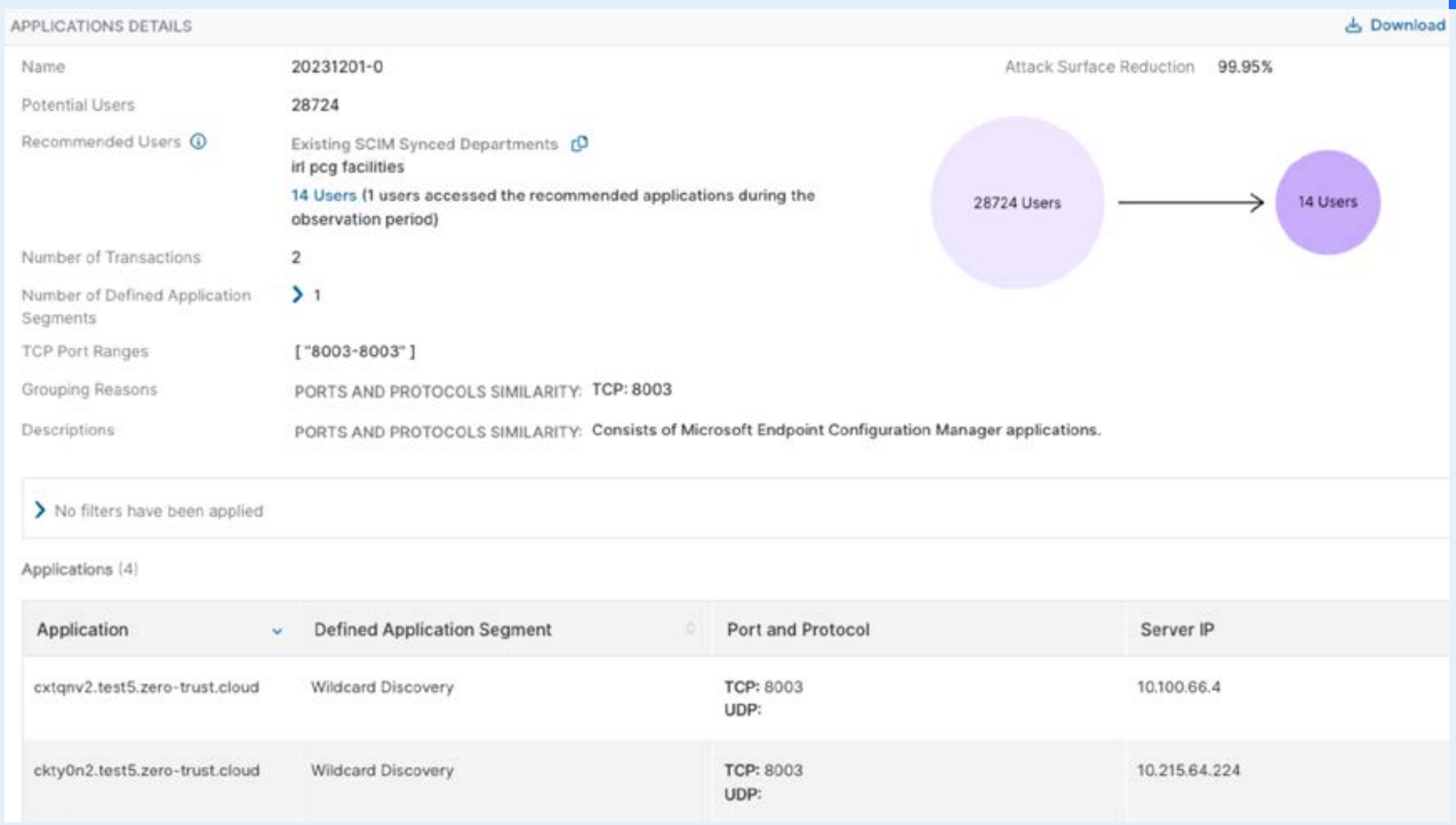


Illustration 6 : Recommandation d'une segmentation des applications optimisée par IA

Découverte automatique des données par IA

Le contexte digital actuel représente un défi de taille pour la sécurité des données. Les données sont disséminées en dehors du data center traditionnel, stockées et accessibles en permanence sur le Web, les applications cloud et les dispositifs des utilisateurs distants. Par conséquent, les entreprises sont aux prises avec une nouvelle réalité : il est difficile d'identifier les informations sensibles et leur destination. Les RSSI et les équipes chargées de la protection des données ont donc de plus en plus de mal à garantir la sécurité des données.

Faire appel à des produits autonomes (des solutions distinctes de prévention des pertes de données pour le réseau, le cloud, le web et les terminaux) pour sécuriser les données disséminées s'avère peu efficace. Ces outils fonctionnent généralement de manière cloisonnée, induisant des lacunes en termes de visibilité et des temps de réponse médiocres. Au-delà, ils exigent une duplication manuelle des politiques d'une solution à l'autre, un processus long et sujet à des erreurs. En fin de compte, cette approche fragmentaire attise le risque de perte de données et renchérie les coûts et la complexité.

Avec Zscaler AI Auto Data Discovery, les entreprises accélèrent leur capacité à identifier, classer et contrôler automatiquement les données, à mesure qu'elles sont créées et quelle que soit leur destination. L'IA de Zscaler a été minutieusement entraînée à identifier les fichiers et les données sensibles dans n'importe quel contexte, que ce soit au repos dans des environnements SaaS, IaaS ou PaaS, en cours d'utilisation sur le terminal d'un utilisateur, ou en transit vers le web via un trafic chiffré. Les administrateurs ne sont plus tenus de dupliquer les règles pour chacun des outils disparates, ni même de configurer des dictionnaires ou des politiques de classification des données dans

Zscaler, pour identifier les données sensibles. La solution est complète dans sa portée et auto-matisée dans son exécution, ce qui minimise les carences de visibilité dont souffrent d'autres outils et réduit les erreurs inhérentes à la création manuelle de règles. Les entreprises accélèrent et affinent ainsi la découverte et la protection des données, en veillant à ce que les informations sensibles soient sécurisées sur l'ensemble des vecteurs potentiels de fuite de données.

Outre une protection renforcée, AI Auto Data Discovery simplifie la supervision de la sécurité des données. Comme nous l'avons mentionné plus haut, les multiples tableaux de bord qu'offrent les produits cloisonnés sont consolidés. La duplication manuelle des politiques et la configuration de dictionnaires de DLP ne sont plus nécessaires. L'automatisation, qui est pilotée par IA, n'exige aucune expertise particulière. Elle permet aux entreprises de déployer et administrer plus rapidement les programmes de protection des données. Il en résulte une nette amélioration de la sécurité et, d'autre part, de la productivité des administrateurs.

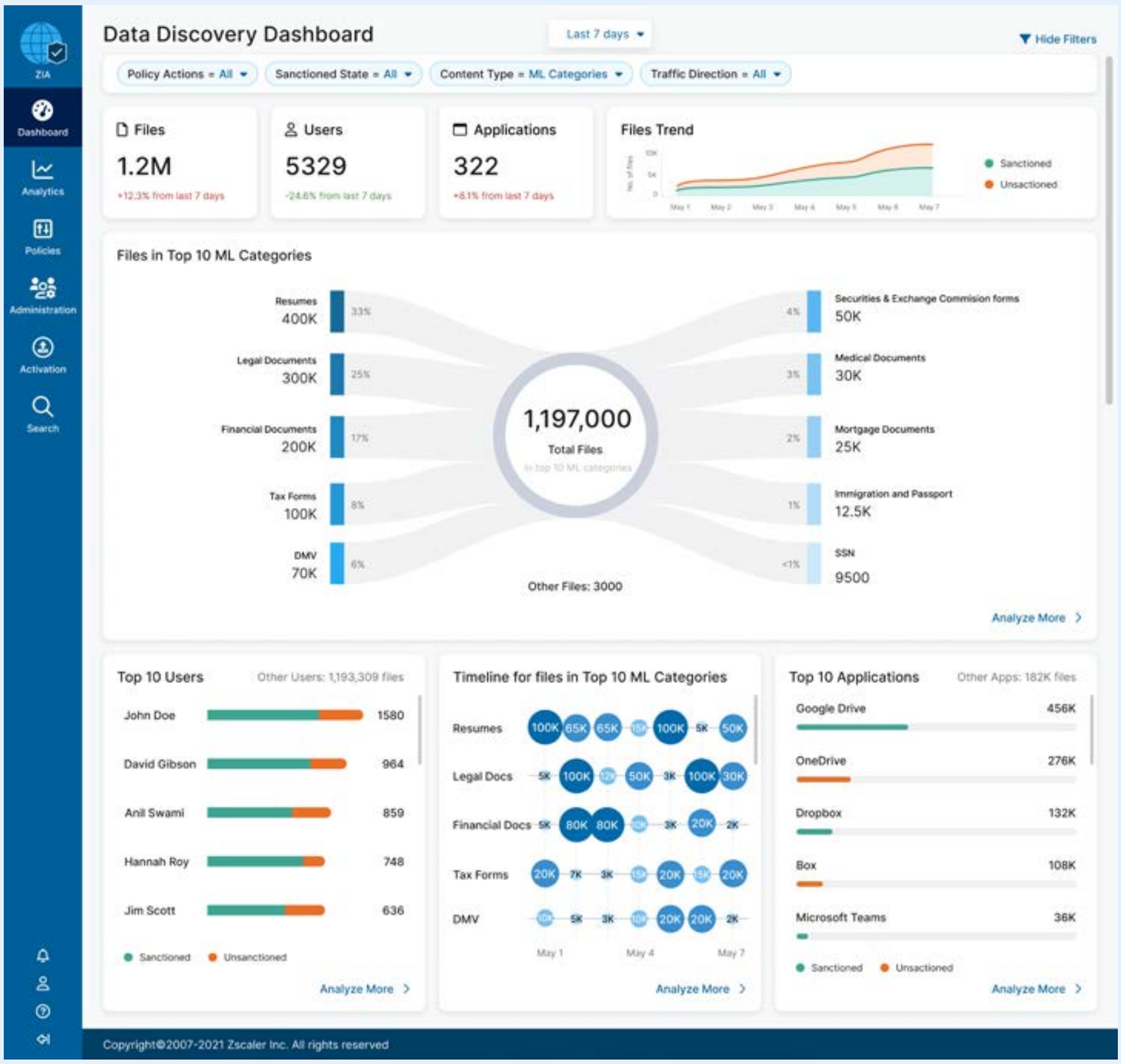


Illustration 7 : Tableau de bord de AI Auto Data Discovery

Optimiser votre entreprise avec Zscaler

La plateforme Zscaler, disponible dans le cloud, fournit la sécurité et la connectivité en tant que service, ce qui signifie que tout le trafic des clients transite par Zero Trust Exchange. Opérant en mode inline et bénéficiant d'intégrations avec plus de 150 solutions de sécurité et métier, Zscaler génère des perspectives pertinentes tout en favorisant un traitement analytique et une prise de décision entièrement automatisés, en temps réel et pilotées par IA, sans agrégation et collecte complexes de données. En d'autres termes, l'adoption du Zero Trust et de l'IA avec Zscaler, si elle améliore la sécurité, optimise également l'opérationnel des entreprises.

Zscaler Digital Experience (ZDX)

Nombre d'utilisateurs dans le monde ont adopté les applications cloud et sont passés au travail hybride, pour gagner en flexibilité par rapport aux environnements traditionnels sur site. Cependant, la transformation digitale induit une constellation complexe de liens réseau et de routage couvrant l'ensemble du globe, les FAI, les réseaux Wi-Fi résidentiels, les appareils personnels des employés, les applications SaaS etc., dont une grande partie se situe à l'extérieur du périmètre réseau de l'entreprise. En conséquence, cette évolution engendre deux problématiques majeures pour les entreprises.

En premier lieu, chaque nouveau cloud, réseau, dispositif ou site alimente la complexité et constitue un nouveau point de défaillance potentiel. Les expériences digitales (et la productivité des utilisateurs) sont par conséquent davantage susceptibles d'être perturbées. Deuxièmement, les environnements distincts et non consolidés aboutissent à une visibilité parcellaire sur les expériences digitales. Les outils de monitoring des dispositifs, des réseaux et des applications, utilisés par différentes équipes n'offrent qu'une visibilité fragmentée de la chaîne de fourniture applicative. Il en résulte des zones d'ombre entre l'appareil de l'utilisateur et l'application, et la nécessité de mobiliser des équipes distinctes pour exporter et corréler manuellement les données de chaque outil. De ce fait, les équipes de support doivent s'investir lourdement pour résoudre les problématiques, ce qui leur fait perdre un temps précieux, tout comme à l'utilisateur final.

Zscaler Digital Experience (ZDX), une composante de Zero Trust Exchange, a été conçu en réponse à ces problématiques. En s'appuyant sur l'architecture proxy inline de Zscaler, ZDX dispose des moyens pour décloisonner la surveillance des dispositifs, des réseaux et des applications, et pour fournir une visibilité complète de bout en bout sur les expériences des utilisateurs.

La solution capitalise sur cette visibilité pour mener des analyses de causes profondes optimisées par IA, qui traitent automatiquement les problèmes d'expérience utilisateur, identifie leurs origines et accélère leur résolution, en un simple clic. Cette même IA est exploitée par un tableau de bord des incidents qui assure une corrélation automatisée de données pour détecter les problématiques furtives affectant plusieurs utilisateurs, peu importe leur origine (applications, Wi-Fi, FAI, terminaux ou autre). Plus récemment, ZDX a proposé un mode de libre-service pour les utilisateurs. Un moteur IA exécuté dans l'agent **Zscaler Client Connector** informe les utilisateurs des dysfonctionnements de la connexion Wi-Fi ou d'une utilisation élevée des ressources CPU, puis leur suggère des solutions, sans faire appel au support technique. Enfin, toutes ces fonctionnalités sont utilisables en langage naturel via ZDX Copilot, de sorte que les administrateurs peuvent poser des questions à un assistant d'IA générative qui les aide à automatiser les tâches, leur apporte une visibilité sur l'expérience digitale et effectue des analyses détaillées.

Ce robuste panel fonctionnel simplifie les opérations de dépannage pour les équipes informatiques et garantit que les utilisateurs bénéficient d'expériences digitales aussi productives possibles.

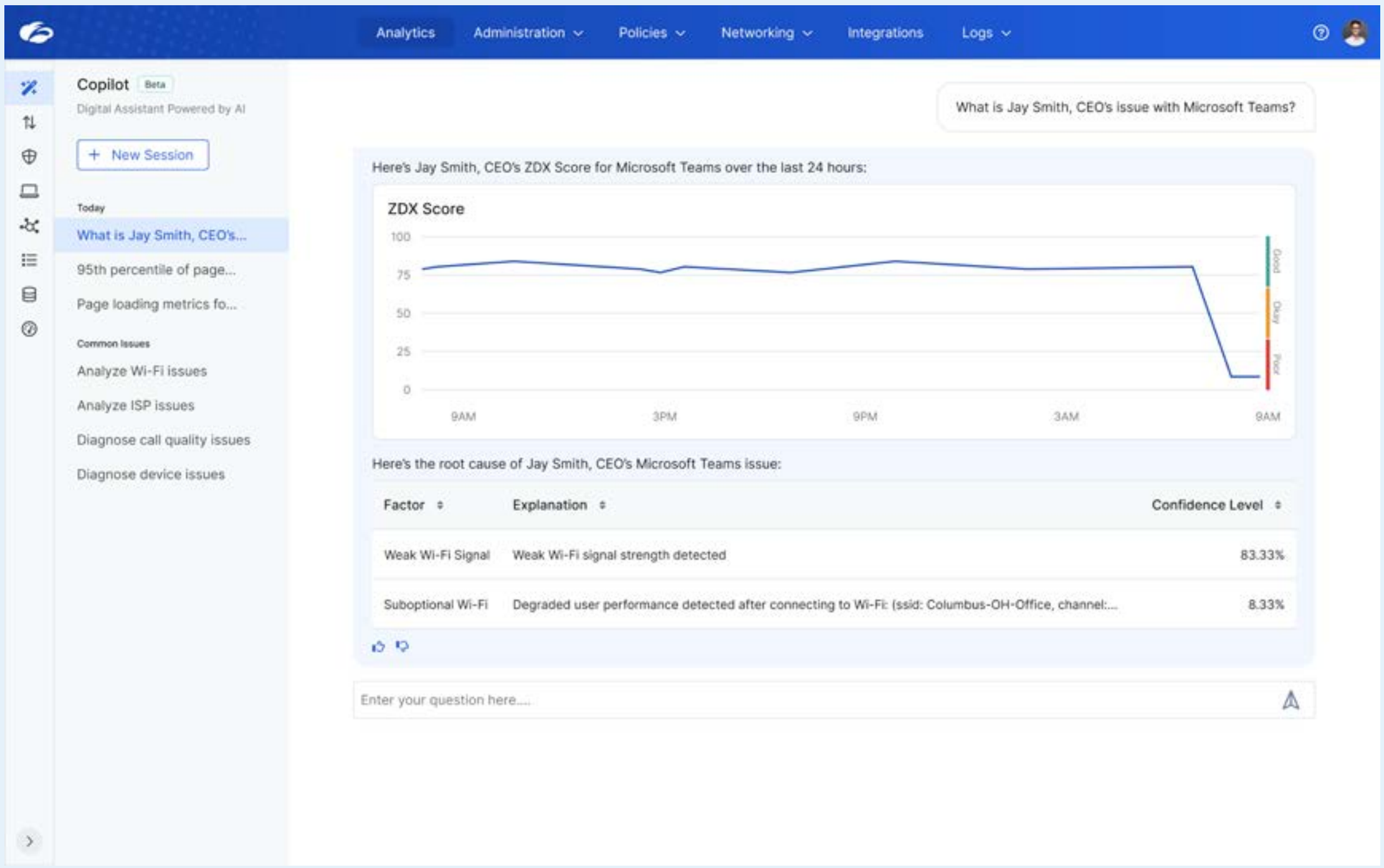


Illustration 8 : Réponse de ZDX Copilot à une invite

Perspectives business

Les applications SaaS améliorent la productivité et la flexibilité des entreprises. Mais la facilité de leur déploiement crée également des défis de gestion et d'optimisation de leur utilisation. Le fait de disposer de licences distinctes pour des applications SaaS redondantes telles que Box, Dropbox et Google Drive creuse les dépenses SaaS ainsi que les charges d'exploitation. D'autre part, les licences et les modules SaaS relèvent du gaspillage de ressources.

Le télétravail et le travail hybride constituent également des atouts pour la flexibilité et la productivité des employés. Toutefois, la modification du lieu de travail implique un changement des schémas traditionnels d'utilisation des bureaux.

Par conséquent, les entreprises peinent à déterminer la meilleure façon de gérer leur utilisation des espaces de bureau, ce qui entraîne inévitablement un gaspillage de ressources et d'argent.

Les entreprises doivent disposer d'une visibilité sur l'utilisation de leur SaaS et de leurs bureaux afin d'optimiser leurs opérations et éliminer les coûts inutiles. Mais les méthodes classiques permettant d'obtenir cette visibilité sont souvent manuelles, fastidieuses et peu précises. Les données cloisonnées et les outils distincts compliquent la tâche des équipes chargées de l'informatique, des achats et des services généraux, qui doivent prendre des décisions éclairées pour réaliser des économies.

Zscaler Business Insights offre aux entreprises une visibilité précise et complète sur leurs applications SaaS et leurs espaces de travail. Pour ce faire, la solution s'appuie sur la puissance de Zero Trust Exchange, le cloud de sécurité inline de Zscaler, qui traite l'ensemble du trafic des clients et peut identifier qui travaille, où et quand, ainsi que les ressources qui sont utilisées. Des intégrations prédéfinies avec des solutions d'entreprise telles que SAP et Workday enrichissent les données Zscaler d'informations relatives aux coûts, aux licences et à la structure organisationnelle. L'IA exploite l'ensemble de données et permet aux responsables fonctionnels de prendre des décisions basées sur des données factuelles pour une allocation des ressources et une optimisation des dépenses plus efficaces.

Pour optimiser le SaaS, Business Insights fournit une visibilité complète sur l'utilisation des applications. La solution identifie les applications redondantes et fournit des informations relatives à l'utilisation des applications SaaS, aux offres retenues et au nombre de postes achetés, ainsi qu'aux utilisateurs actifs. En ce qui concerne la planification de l'espace de travail et l'optimisation de l'utilisation des bureaux, Business Insights fournit des tendances et informations pertinentes, telles que les jours et les heures de présence sur site des collaborateurs ainsi que les départements métiers qui utilisent les bureaux.

Business Insights permet aux entreprises de prendre des décisions éclairées pour une adoption plus efficace du SaaS et du travail hybride.

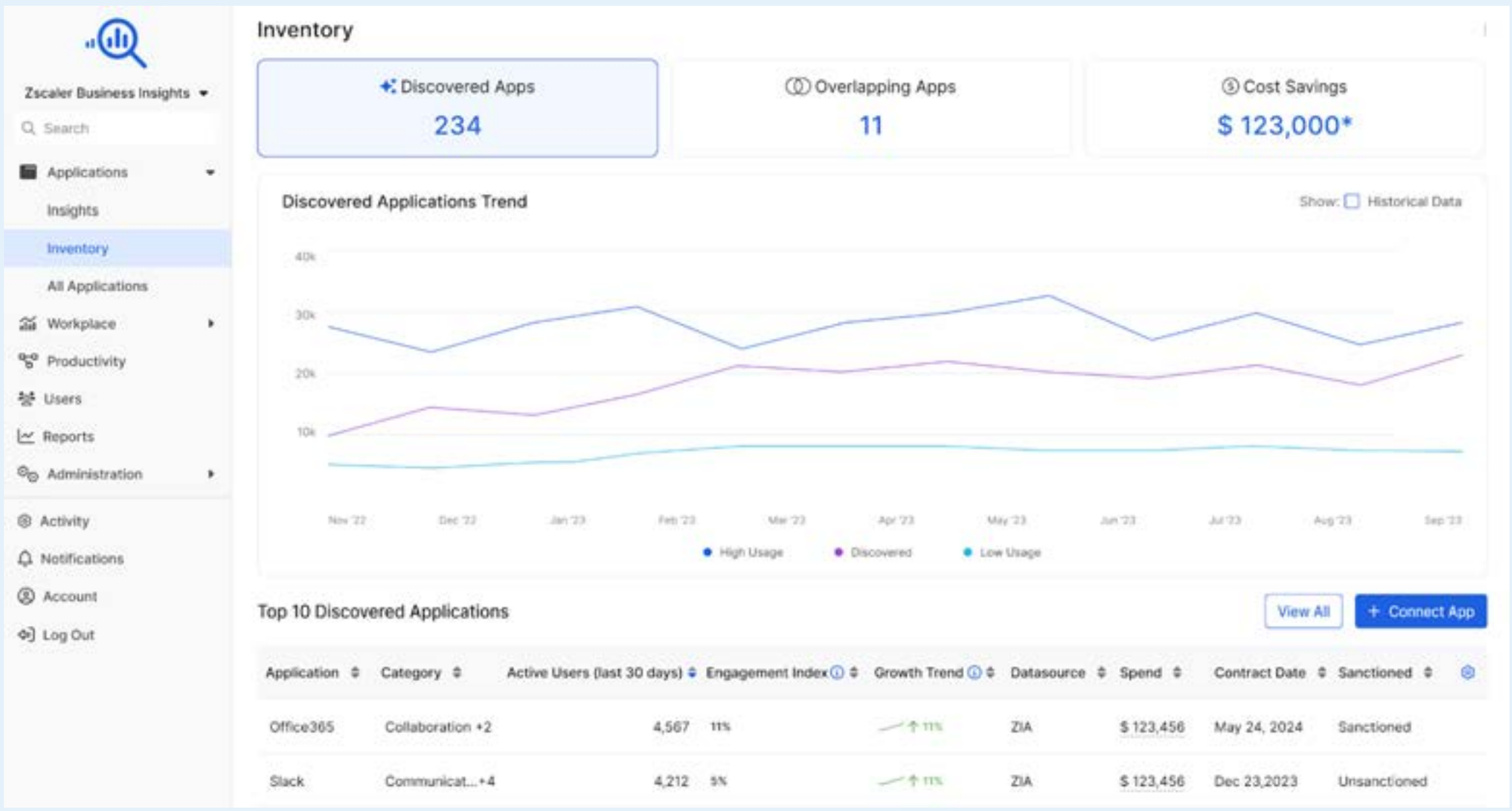


Illustration 9 : Tableau de bord Business Insights

Risk360

Dans le contexte digital actuel, en constante évolution, les entreprises doivent composer avec toujours plus de complexité et un nombre croissant de vulnérabilités. Pire, les cybercriminels affinent constamment leurs méthodes, adoptent les dernières techniques malveillantes et rendent leurs attaques plus sophistiquées. Les outils de sécurité traditionnels et les processus manuels ne parviennent pas à fournir une vue d'ensemble de ces risques. En effet, le cloisonnement des tableaux de bord de sécurité et la fragmentation des données empêchent les responsables de la sécurité d'évaluer les risques de manière globale et d'y remédier de manière efficace.

La mise en conformité avec les réglementations de sécurité constitue une difficulté supplémentaire. Les entreprises doivent démontrer leur conformité aux réglementations sectorielles en apportant la preuve qu'elles ont adopté des pratiques de gestion des risques appropriées. Cependant, en l'absence d'un cadre unifié et intégré de gestion des risques, les entreprises peinent à faire le lien entre leurs fonctionnalités de sécurité et les exigences réglementaires, si bien qu'il leur est difficile de rendre compte de la posture de risques et de prouver la mise en conformité.

Pour comprendre les risques et démontrer leur conformité, les administrateurs de la sécurité sont appelés à regrouper des informations provenant de diverses sources disjointes et à élaborer des rapports. Mais ce processus manuel et fastidieux leur fait perdre un temps précieux et accroît les frais de gestion.

Pour remédier à cette situation, Zscaler propose Risk360, un framework complet et décisionnel qui permet de quantifier avec précision les cyber-risques. Risk360 exploite automatiquement les données en temps réel provenant de l'environnement Zscaler d'une entreprise, des sources externes de données et des informations fournies par l'équipe de recherche sur les menaces de Zscaler ThreatLabz. Il n'est pas nécessaire d'agréger manuellement les données ou de compiler des rapports.

Risk360 fournit une visibilité globale sur la posture de sécurité d'une entreprise et quantifie le risque associé à l'exposition de sa surface d'attaque, au potentiel de compromission, à la possibilité de déplacement latéral et à la probabilité de perte de données. La solution tire parti de l'IA pour évaluer la maturité en matière de cybersécurité, ce qui évite de faire appel à des services de conseil coûteux et renseigne les entreprises sur l'état d'avancement de leur migration vers le Zero Trust. La solution fournit des tableaux de bords sur les risques, des informations granulaires sur les facteurs de risque, des détails sur une éventuelle exposition aux risques financiers, des rapports sur mesure pour les cadres dirigeants, ainsi que des recommandations que les entreprises peuvent immédiatement mettre en pratique afin de maîtriser les risques. Elle contribue également à la mise en conformité de la sécurité grâce à des mappings prédéfinis avec des frameworks tels que MITRE ATT&CK et NIST CSF, ainsi qu'un accompagnement au reporting selon les exigences de la **réglementation SEC S-K Item 106**.

Avec Risk360, les entreprises peuvent systématiquement évaluer et minimiser les risques, assurer leur conformité réglementaire, mais aussi alléger leurs tâches d'administration et leurs coûts de gestion. En d'autres termes, cette solution est un nouvel exemple de la capacité de Zero Trust à sécuriser et optimiser les entreprises grâce à la puissance du Zero Trust et de l'IA.

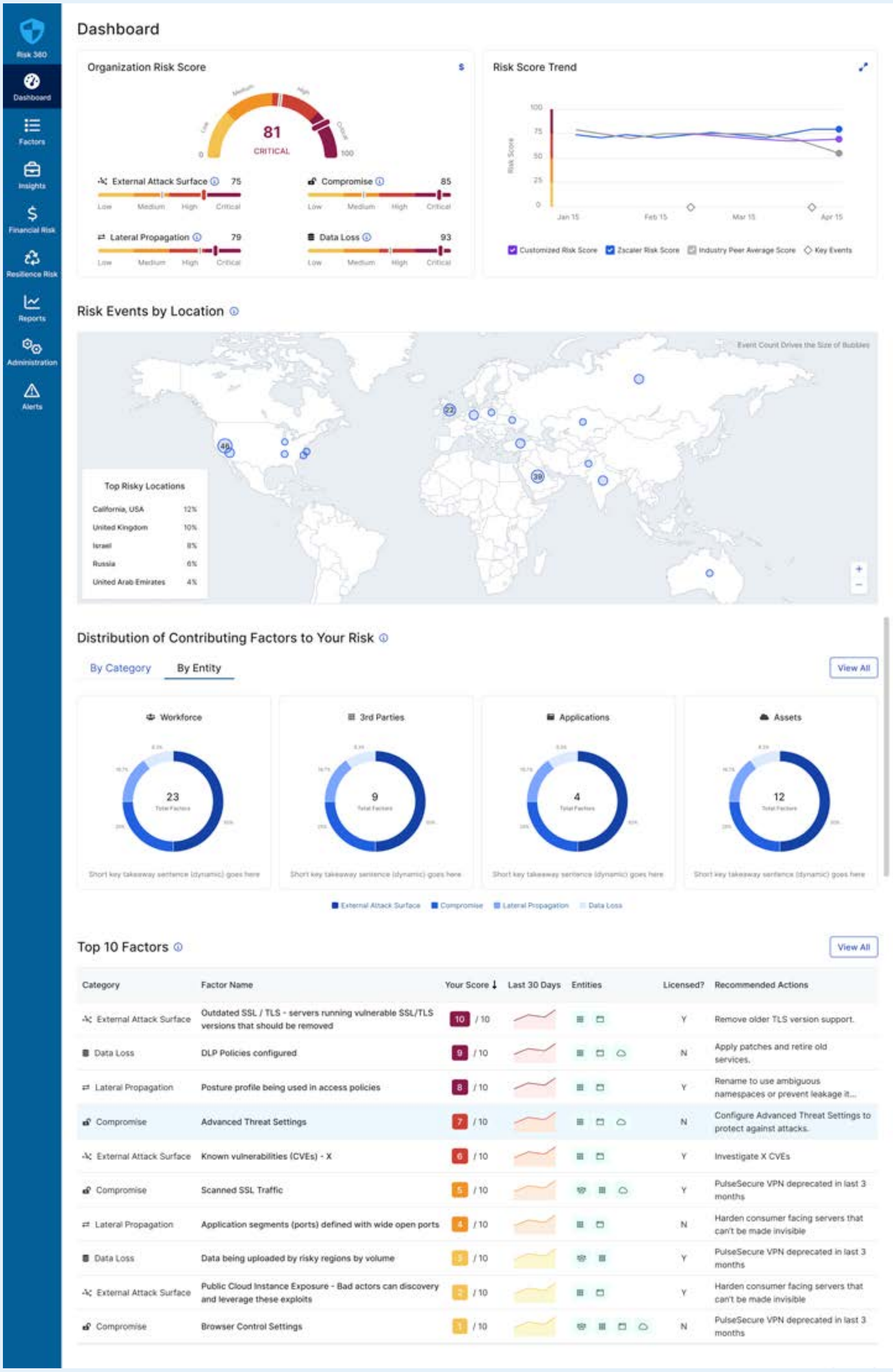


Illustration 10 : Tableau de bord de Risk360

Synthèse

Les risques cyber et la pression concurrentielle constituent plus que jamais de vrais défis. Pour assurer leur pérennité, les entreprises doivent déjouer les cybermenaces et les pertes de données, mais également veiller à opérer aussi efficacement que possible. Heureusement, le Zero Trust associé à l'IA constitue un duo puissant pour tenir ces deux objectifs.

En tant que pionnier et acteur innovant des architectures Zero Trust, Zscaler permet à de nombreux clients dans le monde de réduire leurs risques. Sa plateforme Zero Trust Exchange, évolutive et ouverte grâce à de multiples intégrations, concrétise des avantages stratégiques en matière de données et d'IA/AA. En d'autres termes, Zscaler vous permet de sécuriser et d'optimiser votre entreprise comme jamais auparavant.

Pour en savoir plus sur le Zero Trust et découvrir pourquoi Zscaler est idéalement placé pour tenir les promesses de cette architecture moderne, inscrivez-vous à l'un des prochains volets de notre webinaire mensuel, **« Zero Trust 101 : Commencer votre parcours ici »**. Il s'agit de la première partie d'une série de trois volets conçus pour vous accompagner tout au long de votre parcours vers le Zero Trust.

Ou, si vous souhaitez voir les capacités d'IA évoquées dans ce livre blanc (et plus encore), vous pouvez **demander une démonstration personnalisée**.

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte de données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 160 data centers dans le monde, Zero Trust Exchange™, basé sur SSE, constitue la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **www.zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

+1 408 533 0288 **Zscaler, Inc. (siège monde) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/fr**

zscaler™

Zero Trust Everywhere