







Zscaler Risk360™

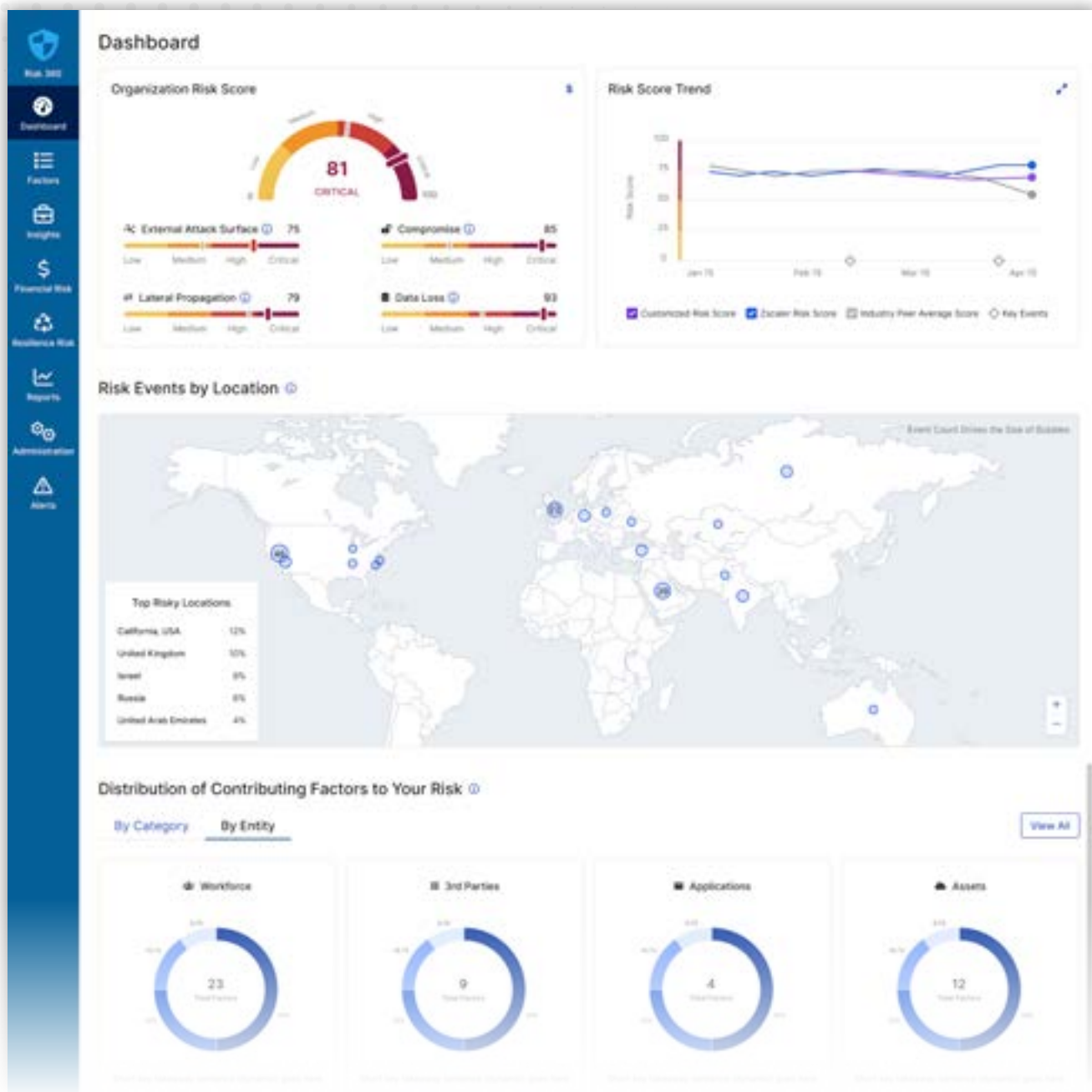
Un cadre complet de quantification et de visualisation des risques pour remédier au risque de cybersécurité

Zscaler Risk360 : cadre de quantification et de visualisation des risques

Risk360 est un puissant cadre de quantification et de visualisation des risques destiné à remédier aux risques de cybersécurité. Il intègre des données réelles provenant de sources externes, de votre environnement Zscaler et des recherches en sécurité de ThreatLabz pour générer un profil détaillé de votre posture de risque.

Risk360 exploite plus de 100 facteurs au sein de l'environnement de cybersécurité d'un client pour comprendre les estimations de pertes financières, les principaux facteurs de cyber-risque, les flux de travail d'investigation recommandés, les tendances et les comparaisons avec les autres entreprises, et fournit des diapositives exploitables au conseil d'administration du RSSI. Le modèle couvre les quatre étapes de l'attaque, à savoir l'attaque externe, la compromission, la propagation latérale et la perte de données, ainsi que toutes les entités de votre environnement, y compris les actifs, les applications, les utilisateurs et les tiers.

Surface d'attaque externe	Zscaler Risk360 examine un large éventail de variables accessibles au public, telles que les serveurs et les ASN exposés, afin de déterminer les actifs cloud sensibles. Ce rapport fournit une vue globale de tous les actifs connectés à Internet, ce qui donne une vue complète de la surface d'attaque externe potentiellement vulnérable et exposée.	
Risque de compromission	Zscaler Risk360 analyse un large éventail d'événements, de configurations de sécurité et d'attributs de flux de trafic pour calculer la probabilité d'une compromission. Cela permet à l'administrateur de comprendre le risque de compromission découlant de fichiers malveillants, de l'exposition du patient zéro et des utilisateurs manifestant des signes d'infection.	
Déplacement latéral	Zscaler Risk360 prend en compte les configurations et les mesures d'accès privé pour calculer le risque de propagation latérale. Cette vue permet d'évaluer les politiques de segmentation afin d'empêcher les cyberattaquants de pénétrer plus profondément dans le réseau.	
Perte de données	Les attributs des données sensibles sont recueillis pour déterminer si des données peuvent s'échapper de l'environnement d'un client. Il est impératif de comprendre et d'avoir une vue d'ensemble de la perte de données pour éviter les fuites et la compromission des données.	



Comment ça marche ?

1

Accès

Tous les clients de Zscaler peuvent immédiatement exploiter Zscaler Risk360.

2

Ingestion de données

Traite les données provenant de plusieurs sources de Zscaler ou non afin de fournir une vue d'ensemble des risques basée sur les données.

3

Atténuation des risques

Filtre, analyse en profondeur et identifie les facteurs de risque, et prend des mesures pour remédier aux problèmes les plus critiques responsables des cyber-risques.

4

Analyse financière

Estimations des pertes financières basées sur des données et des recherches pour votre secteur d'activité, mises en correspondance avec votre score de risque Zscaler.

La valeur de Zscaler Risk360

Quantification du risque

Zscaler Risk360 développe un score de risque pour chacune des quatre étapes d'une violation qui est affichée pour toutes les entités d'utilisation telles que le personnel, les tiers, les applications et les ressources. Le cadre de risque est étayé par des centaines de signaux basés sur plusieurs années de recherche en sécurité menées par les experts de Zscaler ThreatLabz. Étant donné que Zscaler Zero Trust Exchange est inline, la plateforme a la capacité unique d'identifier les facteurs de risque sans risque d'erreur. Outre les données de Zscaler Zero Trust Exchange, Zscaler Risk360 utilise également des données provenant de sources tierces telles que l'EDR pour fournir un score de risque éclairé. Tout cela est collectivement utile pour l'allocation du budget de cybersécurité, les investissements et les stratégies d'atténuation. Les équipes de sécurité peuvent exploiter les scores de Zscaler Risk360 pour justifier toutes les décisions d'investissement en sécurité.

Visualisation et reporting intuitifs

Zscaler Risk360 propose une visualisation et un reporting intuitifs pour analyser les notes de synthèse de haut niveau destinées aux dirigeants. Les dirigeants et les experts ont également la possibilité de filtrer et d'approfondir les principaux facteurs de risque de cybersécurité auxquels est exposée l'entreprise afin d'approfondir l'analyse et de prendre des décisions en matière de sécurité. Les clients peuvent étudier les estimations de l'exposition financière, y compris les recommandations de remédiation financière. Zscaler Risk360 permet d'exporter très facilement des diapositives de synthèse qui peuvent être présentées au conseil d'administration, expliquant le risque cybernétique, les principales conclusions sur le risque et l'estimation de l'exposition financière. Les équipes de sécurité peuvent se concentrer sur l'impact ajouté pour l'entreprise et automatiser le processus de reporting.

Avantages de Zscaler Risk360

- Acquisition d'une vue précise de l'exposition au risque à travers les quatre étapes de l'attaque
- Score de risque regroupé à travers plusieurs sources pour une compréhension totale du cyber-risque
- Compréhension des principaux facteurs de risque de cybersécurité auxquels est exposée l'entreprise et évaluation des facteurs contributifs
- Informations exploitables avec des flux de travail guidés pour enquêter sur les problèmes les plus critiques et y remédier
- Amélioration du reporting et de l'orientation au niveau des directeurs de département et du conseil d'administration pour la gestion des cyber-risques, la stratégie, la gouvernance et la conformité, et l'assurance contre les cyber-risques
- Reporting de la quantification des pertes financières, y compris les fourchettes de résultats de Monte Carlo
- Correspondances de sécurité avec les cadres de risques de sécurité : MITRE Attack et NISF CSF

Informations exploitables pour la remédiation

Le cadre de remédiation des risques priorisés de Zscaler Risk360 permet aux clients de mettre à jour ou de modifier les politiques. Il comprend également des flux de travail d'investigation guidés qui permettent d'approfondir l'analyse de problèmes spécifiques. Ils permettent, par exemple, d'identifier des utilisateurs spécifiques qui téléchargent des données sensibles. Les clients peuvent périodiquement contrôler le score de risque afin de mieux comprendre leur situation en matière de risque.

Cas d'utilisation

Quantification et visualisation du cyber-risque dans l'ensemble de l'entreprise

Zscaler Risk360 s'appuie sur des moteurs automatisés qui intègrent des données réelles provenant de sources internes (Zscaler Zero Trust Exchange) et externes (tiers). Le score de risque de l'entreprise est indiqué sur une échelle de 0 à 100 (100 étant critique), tout en se comparant aux homologues de l'industrie pour appréhender les points de référence et les tendances au fil du temps afin de constater l'amélioration de la posture de sécurité. De nombreuses entreprises adoptant le Zero Trust, Zscaler Risk360 aide également à visualiser le score de leur démarche de Zero Trust.

Remédiation à l'exposition basée sur les données

Grâce aux flux d'investigation guidés et aux recommandations exploitables, les clients peuvent prendre des mesures correctives rapides après avoir interprété leur score de risque. Cet outil permet de créer une liste de problèmes prioritaires qui peuvent être analysés avec le flux de travail d'investigation afin d'approfondir et analyser des problèmes spécifiques.

Impact financier de l'exposition aux cyber-risques

Les clients peuvent estimer l'impact financier des risques auxquels est exposée leur entreprise grâce à la quantification des pertes financières. Ce reporting sur l'exposition financière comprend une modélisation de Monte Carlo montrant une gamme de résultats financiers potentiels.

Rapports, cartographie des risques et conseils

Risk360 propose des rapports détaillés et prêts à l'emploi, tels que nos rapports du conseil des RSSI résumant les postures de cyber-risque pour les dirigeants et notre évaluation de la maturité en matière de cybersécurité optimisée par l'IA pour présenter le parcours Zero Trust d'une société et ses plus grands domaines de risque. Il présente également les correspondances de contrôle avec les cadres de risque de sécurité tels que MITRE Attack et NIST CSF et aide même à la production de rapports de conformité pour le règlement S-K article 106 de la SEC.

Adopter Zscaler Risk360

Chaque client de Zscaler dispose d'un accès rapide et facile au score de risque de son entreprise, ainsi qu'à des informations et des recommandations exploitables. Ce cadre de visualisation permet aux RSSI et aux DSI d'évaluer le cyber-risque et l'exposition financière tout en comparant leur score avec celui de leurs pairs et en suggérant des flux de travail permettant d'améliorer le score de risque. Les services qui ont accès à ce rapport peuvent détailler les données par type de risque, par entité (utilisateurs, tiers, applications, actifs) et par localisation. Le rapport permet de trier la liste des utilisateurs par risque et présente les applications (SaaS et privées combinées), les tiers et les actifs avec des scores de risque individuels et distincts.

Zscaler permet également de suivre le score de risque dans le temps afin de rendre compte des mesures prises en fonction des expositions et des recommandations suggérées.



Experience your world, secured.™

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale de ses clients pour qu'ils gagnent en agilité, efficacité, résilience et sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications, indépendamment de l'emplacement. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SSE constitue la plus vaste plateforme intégrée de sécurité cloud. Pour en savoir plus, rendez-vous sur zscaler.fr ou suivez-nous sur Twitter @zscaler.

©2023 Zscaler, Inc. Tous droits réservés. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, Zscaler Private Access™, ZIA™, ZPA™ et les autres marques commerciales répertoriées sur zscaler.fr/legal/trademarks sont soit 1) des marques déposées ou des marques de service, soit 2) des marques déposées ou des marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales sont la propriété de leurs détenteurs respectifs.