

Zscaler Risk360™

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



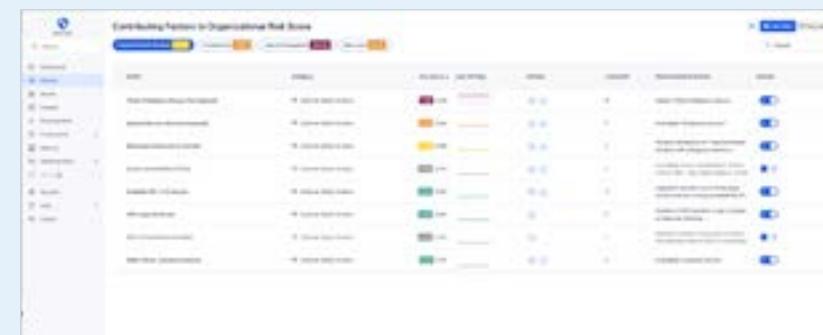
Zscaler Risk360 : cadre de quantification et de visualisation des risques

Risk360 est un puissant cadre de quantification et de visualisation des risques conçu pour remédier aux risques de cybersécurité. Il intègre des données réelles provenant 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 l'aider à 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 et les utilisateurs.

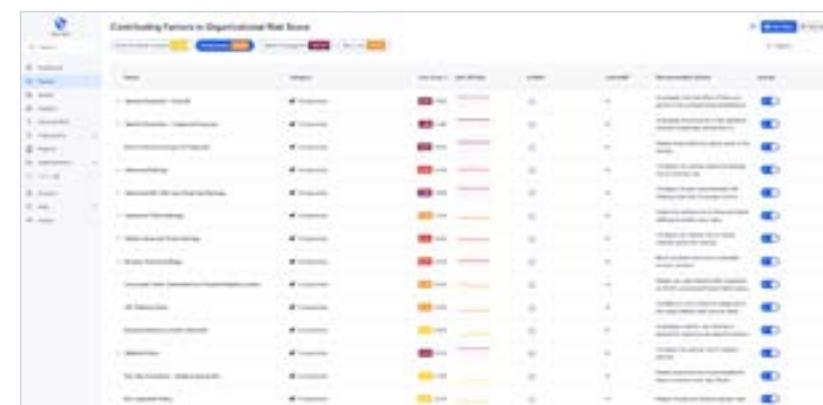
SURFACE D'ATTAQUE EXTERNE

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 qui manifestent 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 cyber-criminels de pénétrer plus profondément dans le réseau.



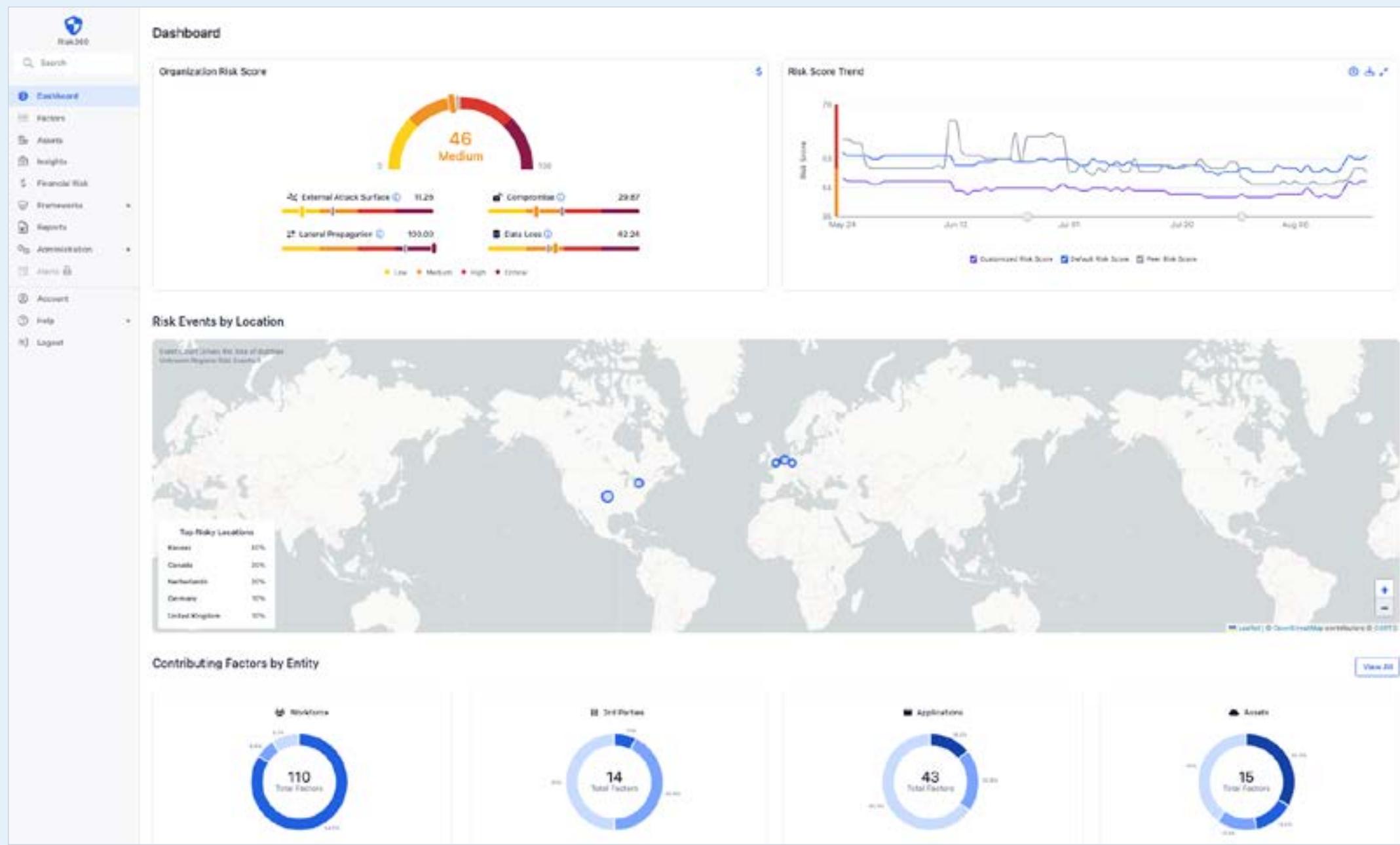
PERTE DE DONNÉES

Les attributs des données sensibles sont recueillis pour déterminer si des données peuvent filtrer 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.





Découvrez le profil de risque de votre entreprise, les tendances et les principaux facteurs contributifs grâce à des informations exploitables.



Mode opératoire

1 ACCÈS

De nombreux clients Zscaler peuvent exploiter Zscaler Risk360 sans attendre.

2 INGESTION DE DONNÉES

Traitez les données provenant de plusieurs sources de Zscaler pour fournir une vue d'ensemble générale des risques basée sur les données.

3 ATTÉNUER LES RISQUES

Filtrez, analysez et identifiez les facteurs de risque et prenez des mesures pour remédier aux problèmes les plus critiques à l'origine des cyber-risques.

4 ANALYSE FINANCIÈRE

Estimations des pertes financières de votre entreprise basées sur des données et des recherches, corrélées à votre score Zscaler.



La valeur de Zscaler Risk360

Quantification du risque

Zscaler Risk360 développe un score de risque pour chacune des quatre étapes de violation. Celui-ci est affiché pour tous les types d'utilisation tels que le personnel, les tiers, les applications et les actifs. 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. La plateforme Zscaler Zero Trust Exchange étant inline, elle dispose de la capacité unique d'identifier les facteurs de risque avec assurance. Collectivement, ces capacités sont très utiles pour l'allocation du budget, l'investissement et les stratégies d'atténuation en matière de cybersécurité. Les équipes de sécurité peuvent exploiter les scores de Zscaler Risk360 pour justifier toutes leurs décisions d'investissement dans la sécurité.

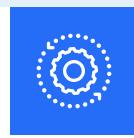
Visualisation et création de rapports intuitifs

Zscaler Risk360 offre une visualisation et des rapports intuitifs qui présentent aux dirigeants une synthèse claire et de haut niveau. Les dirigeants et les praticiens peuvent également filtrer et explorer en profondeur les principaux facteurs de cyber-risques de l'entreprise afin d'affiner leurs analyses et de prendre des décisions de sécurité éclairées. Zscaler Risk360 facilite l'exportation de diapositives de synthèse destinées aux dirigeants, intégrables aux présentations de conseil d'administration, qui présentent de manière claire les cyber-risques, les principaux facteurs de risque identifiés et l'exposition financière estimée. Les équipes de sécurité peuvent se concentrer sur la création de valeur pour l'entreprise et automatiser le processus de reporting.

Informations décisionnelles pour guider la remédiation

Le cadre de correction des risques prioritaires dans Zscaler Risk360 permet aux clients d'agir de mettre les politiques à jour ou les modifier. Il comprend également des flux de travail d'enquête guidés qui permettent d'approfondir l'analyse de problèmes spécifiques. Il s'agit par exemple d'identifier des utilisateurs spécifiques qui téléchargent des données sensibles. Les clients peuvent périodiquement contrôler leur score de risque pour mieux comprendre leur situation.

Avantages de Zscaler Risk360

 Acquisition d'une vue précise de l'exposition au risque à travers les quatre étapes de l'attaque	 Regrouper le score de risque 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, la conformité et l'assurance contre les cyber-risques	

Cas d'utilisation

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

Zscaler Risk360 s'appuie sur des moteurs automatisés qui ingèrent des données provenant de sources internes (Zscaler Zero Trust Exchange). Le score de risque de l'entreprise est renseigné sur une échelle de 0 à 100 (100 étant critique). Il est également comparé à des pairs du secteur afin de comprendre les points de référence et les tendances au fil du temps, et suivre l'amélioration de la posture de sécurité. Zscaler aide également plusieurs entreprises qui s'engagent sur la voie du Zero Trust à visualiser leur score de progression.

Remédiation à l'exposition basée sur les données

Grâce aux flux d'investigation guidés et aux recommandations exploitables fournies, les clients peuvent agir rapidement pour remédier aux problèmes après avoir compris leur score de risque. Cet outil permet de créer une liste de problèmes prioritaires qui peuvent être analysés avec le processus d'investigation afin d'approfondir et examiner des problèmes spécifiques.

Impact financier de l'exposition aux cyber-risques

Les clients peuvent procéder à une quantification des pertes financières afin d'estimer l'impact financier des risques auxquels est exposée leur entreprise.

Rapports, cartographie des risques et conseils

Risk360 propose des rapports détaillés prêts à l'emploi, tels que nos rapports de comité de direction pour les RSSI, qui synthétisent les postures de cyber-risque à l'intention des dirigeants. Ainsi que notre évaluation de la maturité de la cybersécurité optimisée par l'IA afin d'illustrer le parcours Zero Trust d'une entreprise et mettre en lumière les principaux risques auxquels elle est exposée.

Adopter Zscaler Risk360

De nombreux clients de Zscaler disposent d'un accès rapide et simple 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 à celui de leurs pairs et en suggérant des leviers d'amélioration du score de risque. Les services qui ont accès à ce rapport peuvent analyser les données sous différents angles : par type de risque, par entité (utilisateurs, tiers, applications, actifs) et par emplacement. Le rapport permet de trier la liste des utilisateurs par risque et présente les applications (SaaS et privées combinées) et les actifs avec des scores de risque individuels et distincts.

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

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.

© 2025 Zscaler, Inc. Tous droits réservés. Zscaler™ et les autres marques commerciales répertoriées sur zscaler.com/fr/legal/trademarks sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.



Zero Trust
Everywhere