Lösungsprofil

Zscaler Risk360™

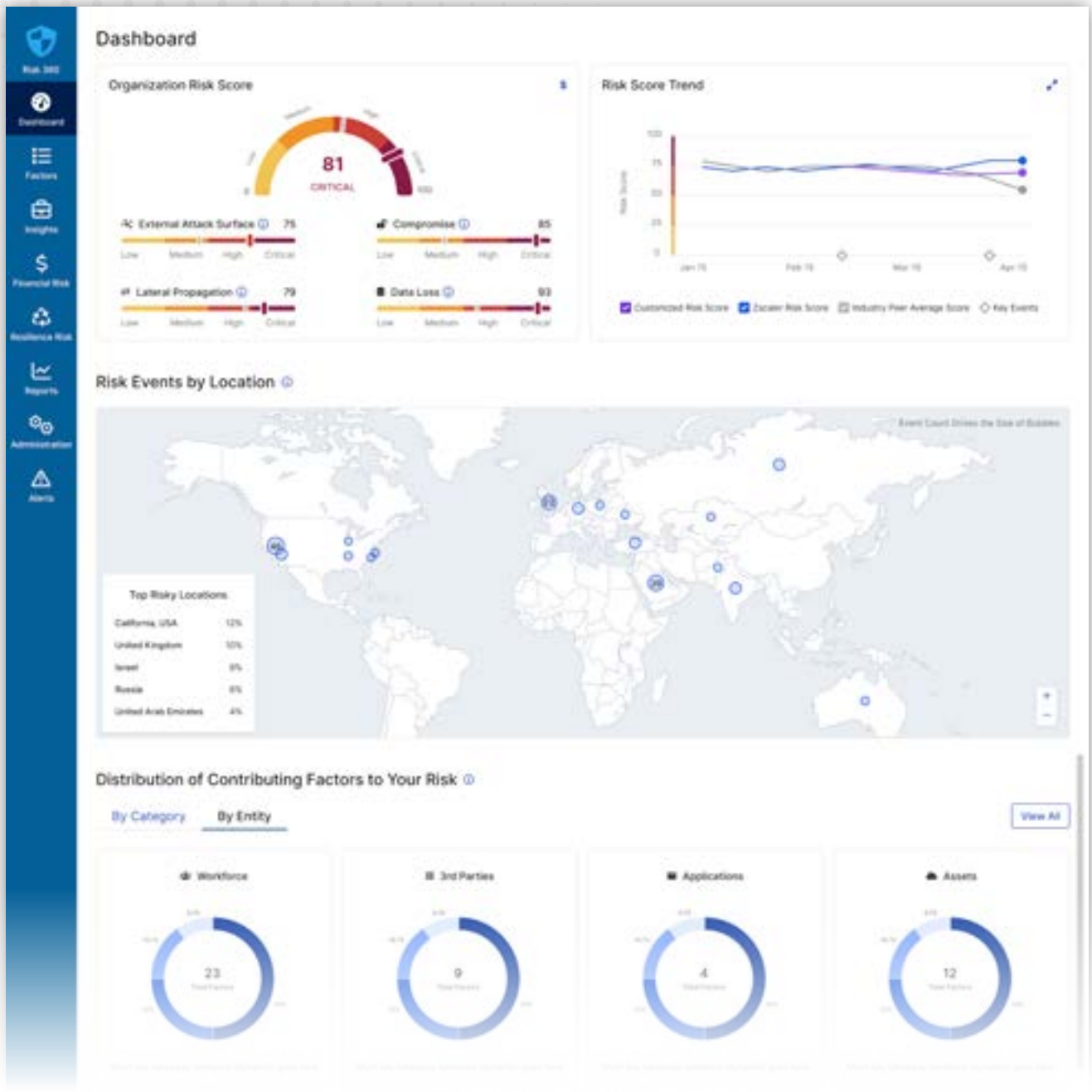
Ein umfassendes Framework zur Behebung von Cybersicherheitsrisiken durch Quantifizierung und Visualisierung

Zscaler Risk360: Framework zur Quantifizierung und Visualisierung von Risiken

Risk360 ist ein leistungsstarkes Framework zur Behebung von Cybersicherheitsrisiken durch Quantifizierung und Visualisierung. Das Risk360-Modell erstellt ein detailliertes Profil Ihres aktuellen Risikostatus anhand von Echtzeitdaten aus externen Quellen und Ihrer Zscaler-Umgebung sowie Forschungsergebnissen von ThreatLabz.

Zscaler Risk360 berücksichtigt über 100 Einzelfaktoren innerhalb der Cybersicherheitsumgebung der betreffenden Organisation und liefert Schätzwerte zur Quantifizierung potenzieller finanzieller Verluste, Erkenntnisse zu den wichtigsten Risikofaktoren, Empfehlungen für Untersuchungsverfahren, Trend- und Branchenvergleiche sowie verwertbare CISO-Folien für Vorstandspräsentationen. Das Modell erstellt Risikobewertungen zu allen vier Phasen eines Cyberangriffs — von der externen Angriffsfläche über die Kompromittierung des Netzwerks und einer lateralen Ausbreitung bis hin zur Datenexfiltration — sowie für alle Elemente Ihrer IT-Umgebung wie Ressourcen, Anwendungen und interne sowie externe User.

Externe Angriffsfläche	Zscaler Risk360 untersucht eine Vielzahl öffentlich zugänglicher Variablen wie z. B. exponierte Server und ASNs, um sensible Cloud-Ressourcen zu identifizieren. Dieser Report bietet einen ganzheitlichen Überblick über alle für das Internet zugänglichen Ressourcen und damit eine vollständige Übersicht über die externe Angriffsfläche, die potenziell angreifbar und gefährdet ist.	
Kompromittierungsrisiko	Zscaler Risk360 analysiert eine Reihe von Ereignissen, Sicherheitskonfigurationen und Traffic-Flow-Attributen, um die Wahrscheinlichkeit einer Kompromittierung zu berechnen. So können Administratoren das Risiko eines Angriffs durch schädliche Dateien, Patient-Zero-Bedrohungen und kompromittierte User erkennen.	
Laterale Bewegung	Das Tool berücksichtigt zudem Konfigurationen und Metriken für private Zugriffe, um das Risiko einer lateralen Ausbreitung zu berechnen. So können Sie Ihre Segmentierungsrichtlinien überprüfen, um Cyberkriminelle daran zu hindern, weiter in das Netzwerk vordringen.	
Datenverluste	Die Attribute sensibler Daten werden erfasst, um festzustellen, ob Daten aus der Umgebung eines Kunden nach außen gelangen könnten. Ein umfassender Überblick über Datenverluste ist unerlässlich, um Datenpannen und -kompromittierungen zu vermeiden.	



Wie funktioniert das?

1 Zugriff
Alle Zscaler–Kunden können Zscaler Risk360 sofort nutzen.

2 Datenerfassung
Verarbeitet Daten aus verschiedenen Zscaler– und sonstigen Quellen, um einen umfassenden datengestützten Überblick über Risiken zu erstellen.

3 Risikominderung
Filtern, analysieren und identifizieren Sie Risikofaktoren und ergreifen Sie Maßnahmen, um die kritischsten Probleme zu beheben, die zu Cyberrisiken führen.

4 Finanzanalyse
Datengestützte und fundierte Schätzungen zu finanziellen Verlusten für Ihre Branche, die Ihrem Zscaler Risk Score zugeordnet werden.

Der Mehrwert von Zscaler Risk360

Risikoquantifizierung
Zscaler Risk360 erstellt eine Risikobewertung für Mitarbeiter, Dritte, Anwendungen und Ressourcen zu allen vier Angriffsphasen. Das Risiko-Framework basiert dabei auf Hunderten von Signalen und der langjährigen Erfahrung von Zscaler ThreatLabz. Da die Zscaler Zero Trust Exchange direkt zwischengeschaltet ist, werden Risikofaktoren zuverlässig erkannt. Zusätzlich zu den Daten der Zscaler Zero Trust Exchange nutzt Zscaler Risk360 zur Erstellung fundierter Risikobewertungen auch Daten aus externen Quellen wie Endpunkterkennung und -reaktion. Das unterstützt die Budgetplanung im Bereich Cybersicherheit sowie Investitions- und Risikostrategien. Die von Zscaler Risk360 generierten Ergebnisse können anschließend für Investitionsentscheidungen genutzt werden.

Intuitive Visualisierung und Reporting
Durch seine intuitiven Funktionen für Visualisierung und Reporting bietet Zscaler Risk360 Führungskräften einen umfassenden Überblick über alle relevanten Informationen. Des Weiteren besteht die Möglichkeit, die wichtigsten Risikofaktoren zu filtern und genauer zu beleuchten, um weitere Analysen durchzuführen und sicherheitsrelevante Entscheidungen zu treffen. Kunden können zudem Schätzungen des finanziellen Risikos einschließlich Empfehlungen für entsprechende Abhilfemaßnahmen einsehen. Mit Zscaler Risk360 lassen sich detaillierte Folien für Vorstandspräsentationen exportieren, um das Cyberrisiko, die wichtigsten Erkenntnisse und das geschätzte finanzielle Risiko darzustellen. Sicherheitsteams können somit den Reportingprozess automatisieren und sich darauf konzentrieren, einen Mehrwert für die Organisation zu schaffen.

Vorteile von Zscaler Risk360

- Detaillierter Einblick in die Risikoexposition in allen vier Phasen eines Angriffs
- Konsolidierter Risk Score aus mehreren Quellen für ein umfassendes Verständnis des Cyberrisikos
- Überblick über die wichtigsten Risikotreiber in Ihrer Organisation und Bewertung zugehöriger Faktoren
- Verwertbare Erkenntnisse durch Workflows mit Schritt-für-Schritt-Anweisungen zur Untersuchung und Behebung der kritischsten Probleme
- Optimiertes Reporting und Hilfestellungen für CXO und Vorstand in den Bereichen Management von Cyberrisiken, Strategien, Governance, Compliance sowie Cyberrisikoversicherung
- Bezifferung finanzieller Schäden und Monte-Carlo-Simulationen
- Berücksichtigung von Risiko-Frameworks wie MITRE Attack und NISF CSF

Verwertbare Erkenntnisse zur Risikobehebung
Mithilfe des prioritätsbasierten Frameworks zur Risikobehebung in Zscaler Risk360 können Kunden Maßnahmen zur Aktualisierung oder Änderung von Richtlinien ergreifen. Enthalten sind außerdem Untersuchungsworkflows mit Schritt-für-Schritt-Anweisungen, um detaillierte Analysen zu erstellen und bestimmte Probleme genauer zu untersuchen — beispielsweise können User identifiziert werden, die sensible Daten hochladen. Kunden können ihren Risk Score regelmäßig kontrollieren und haben so jederzeit einen Überblick über ihren Risikostatus.

Anwendungsfälle

Quantifizierung und Visualisierung von Cyberrisiken im gesamten Unternehmen
Zscaler Risk360 nutzt automatisierte Engines, die reale Daten aus internen Quellen, also der Zscaler Zero Trust Exchange, und externen Quellen von Drittanbietern verarbeiten. Der Risk Score des Unternehmens wird auf einer Skala von 0 bis 100 angegeben, wobei 100 für ein kritisches Risiko steht. Auch Vergleiche mit anderen Unternehmen der Branche sind möglich, um Benchmarks und Trends im Zeitverlauf zu ermitteln und die Entwicklung des Sicherheitsstatus zu verfolgen. Da viele Organisationen ihre Sicherheitsmodelle auf Zero Trust umstellen, können sie sich in Zscaler Risk360 auch Daten zum Stand dieser Umstellung anzeigen lassen.

Datengestützte Behebung von Sicherheitsrisiken
Mithilfe der Untersuchungsworkflows, ihrer Schritt-für-Schritt-Anweisungen und der auf verwertbaren Erkenntnissen basierenden Empfehlungen können Kunden Maßnahmen zur schnellen Problembehebung ergreifen. Das Tool hilft bei der Erstellung einer nach Prioritäten geordneten Liste von Problembereichen, die sich mit dem Untersuchungsworkflow analysieren lassen, um detaillierte Informationen zu den jeweiligen Risiken zu erhalten.

Finanzielle Folgen von Cyberrisiken
Anhand der Berechnungen lässt sich die finanzielle Tragweite des jeweiligen Risikos genau abschätzen. Dabei kommen auch Monte-Carlo-Simulationen zum Einsatz, die mögliche finanzielle Ergebnisse aufzeigen.

Berichterstattung, Risikoabbildung und Hilfestellung
Risk360 generiert detaillierte Reports wie CISO-Vorstandsberichte, die die Cyber-Risikolage für Führungskräfte zusammenfassen, und KI-gestützte Evaluierungen der Cybersicherheit, die den aktuellen Entwicklungsstand und die größten Risikobereiche aufzeigen. Zudem werden Risiko-Frameworks wie MITRE Attack und NIST CSF sowie SEC-Vorgaben zur Compliance-Berichterstattung (SEC Regulation S-K Item 106) berücksichtigt.

Einführung von Zscaler Risk360

Jeder Zscaler-Kunde hat schnellen und einfachen Zugriff auf den Risk Score seiner Organisation sowie auf verwertbare Erkenntnisse und Empfehlungen. Mit diesem Framework können CISOs und CIOs das Cyberrisiko ebenso wie das finanzielle Risiko beurteilen, ihren Score mit dem ähnlicher Organisationen vergleichen und Workflows zur Verbesserung des Risk Scores vorschlagen. Mitarbeiter mit Zugriff auf diesen Report haben die Möglichkeit, die Daten nach Risikotyp, Entität (interne und externe User, Anwendungen sowie Ressourcen) und Standort aufzuschlüsseln und zu sortieren. Zudem lässt sich die Userliste nach Risiko ordnen und zeigt Anwendungen (sowohl SaaS als auch privat) sowie Drittanbieter und Ressourcen mit individuellen Risikobewertungen an.

Darüber hinaus bietet Zscaler die Möglichkeit, den Risk Score im Zeitverlauf nachzuvollziehen, um zu ermitteln, wie wirksam die ergriffenen Maßnahmen bislang sind.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de