Zscaler Risk360™

Ein umfassendes Framework zur Behebung von Cybersicherheitsrisiken durch Quantifizierung und Visualisierung

LÖSUNGSPROFIL

Zscaler Risk360: Framework zur Quantifizierung und Visualisierung von Risiken

Risk360 ist ein leistungsstarkes Framework zur Behebung von Cybersicherheitsrisiken durch zuverlässige Quantifizierung und Visualisierung. Es erfasst echte Daten aus Ihrer Zscaler-Umgebung und Sicherheits-forschung von ThreatLabz, um ein detailliertes Profil Ihres Risikostatus zu erstellen.

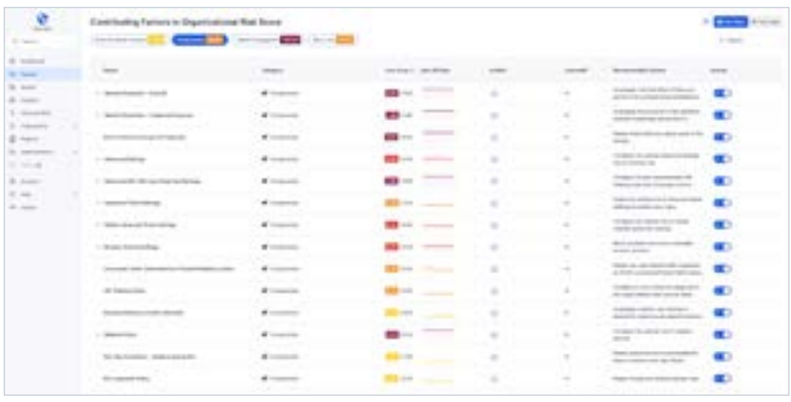
Risk360 berücksichtigt über 100 Einzelfaktoren innerhalb der Cybersicherheitsumgebung des betreffenden Unternehmens und liefert Schätzwerte zur Quantifizierung potenzieller finanzieller Verluste, Erkenntnisse zu den wichtigsten Risikofaktoren, Empfehlungen für Untersuchungsverfahren, Trend- und Branchenvergleiche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

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 breite Palette von Ereignissen, Sicherheitskonfigurationen und Traffic-Attributen, um die Wahrscheinlichkeit eines Kompromisses zu berechnen. Auf diese Weise kann der Administrator das Angriffsrisiko erkennen, das von schädlichen Dateien, Patient-Zero-Risiken und Usern mit Infektionsverdacht ausgeht.



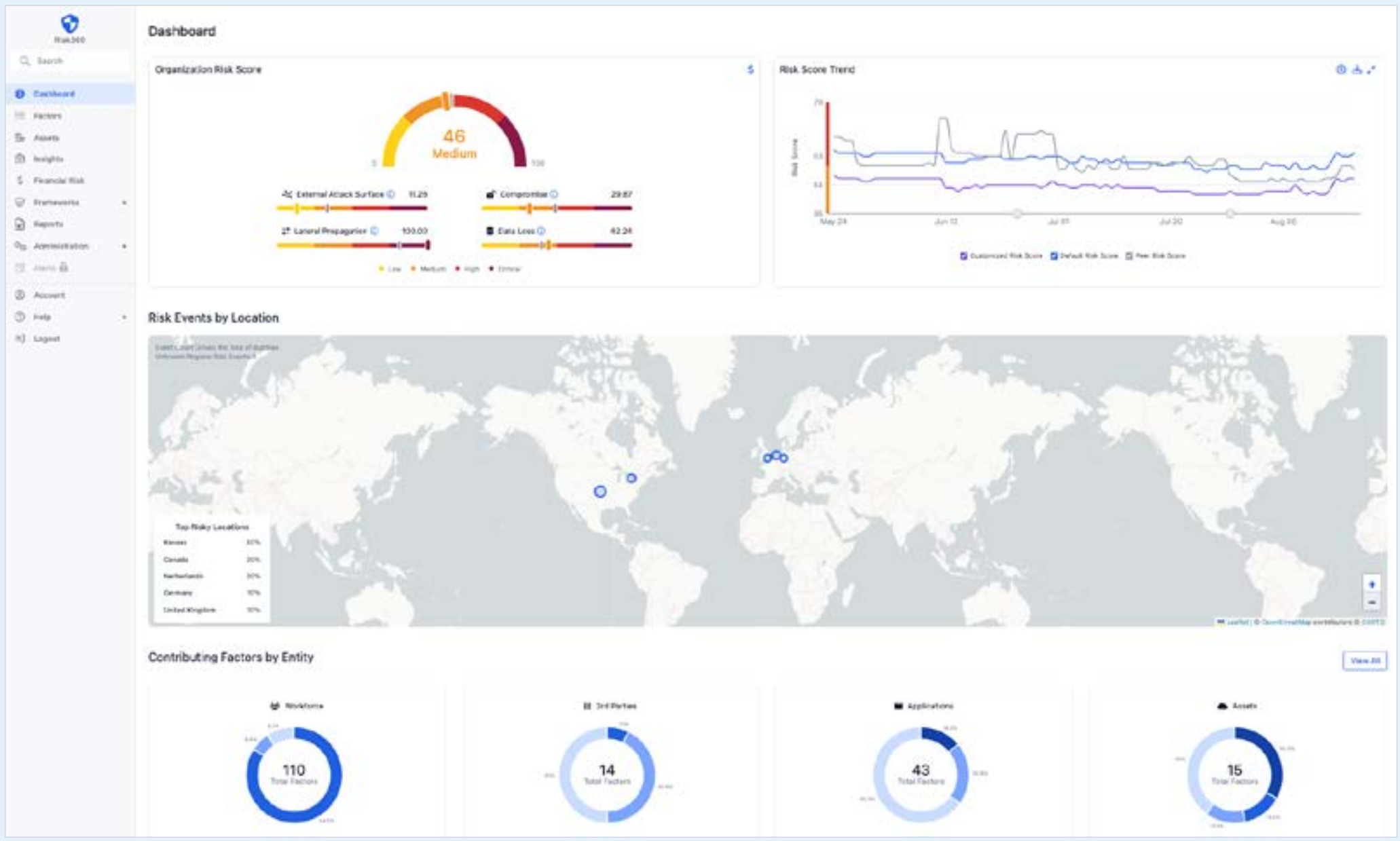
LATERALE BEWEGUNG

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 Daten-pannen und -kompromittierungen zu vermeiden.

Entdecken Sie das Risikoprofil, die Trends und die wichtigsten Faktoren Ihres Unternehmens mit umsetzbaren Erkenntnissen



Wie funktioniert das?

1 ZUGANG

Viele Zscaler–Kunden können Zscaler Risk36O sofort nutzen.

2 DATENAUFNAHME

Verarbeiten Sie Daten aus mehreren Zscaler–Quellen, um einen umfassenden, datengesteuerten Überblick über das Risiko zu erhalten.

3 RISIKEN MINIMIEREN

Filtern, analysieren und erkennen Sie Risikofaktoren. Ergreifen Sie Maßnahmen, um die kritischsten Probleme zu beheben, die das Cyberrisiko verursachen.

4 FINANZANALYSE

Datenbasierte und forschungsgestützte Schätzungen der finanziellen Verluste Ihres Unternehmens, die Ihrem Zscaler–Score zugeordnet sind.

Der Mehrwert von Zscaler Risk360

Quantifizierung des Risikos

Zscaler Risk360 ermittelt für jede der vier Stufen eines Sicherheitsverstoßes einen Risiko-Score, der für alle Nutzungseinheiten wie Mitarbeiter, Drittanbieter, Anwendungen und Assets visualisiert wird. Das Risiko-Framework wird durch Hunderte von Signalen gestützt, die auf mehrjähriger Sicherheitsforschung der Experten von Zscaler ThreatLabz basieren. Da die Zscaler Zero Trust Exchange inline geschlatet ist, verfügt die Plattform über die einzigartige Fähigkeit, Risikofaktoren zuverlässig zu erkennen. All dies ist insgesamt hilfreich für die Budgetzuweisung, Investitionen und Minderungsstrategien im Bereich Cybersicherheit. Sicherheitsverantwortliche können die Bewertungen von Zscaler Risk360 nutzen, um für alle Entscheidungen zu Sicherheitsinvestitionen einen Business Case zu erstellen.

Intuitive Visualisierung und Berichterstattung

Zscaler Risk360 bietet intuitive Visualisierung und Berichterstattung zur Erstellung von Zusammenfassungen für Führungskräfte. Führungs- und Fachkräfte haben außerdem die Möglichkeit, die wichtigsten Faktoren für das Cybersicherheitsrisiko des Unternehmens herauszufiltern und genauer zu untersuchen, um weitere Analysen durchzuführen und Sicherheitsentscheidungen zu treffen. Mit Zscaler Risk360 können Sie ganz einfach Folien mit einer Zusammenfassung exportieren, die in Vorstandspräsentationen verwendet werden können und Cyberrisiken, wichtige Risikoergebnisse und die geschätzte finanzielle Belastung erläutern. Sicherheitsverantwortliche können sich darauf konzentrieren, den Geschäftsnutzen zu steigern und den Berichtsprozess zu automatisieren.

Umsetzbare Erkenntnisse zur Behebung

Mit dem priorisierten Framework zur Risikobehebung innerhalb von Zscaler Risk360 können Kunden bei Bedarf Maßnahmen zur Aktualisierung oder Änderung von Richtlinien umsetzen. Es beinhaltet außerdem geführte Untersuchungsabläufe, die eine tiefere Analyse spezifischer Probleme ermöglichen. Beispiel: Erkennung bestimmter User, die vertrauliche Daten hochladen. Kunden können den Risiko-Score regelmäßig überwachen, um ihren Risikostatus besser zu verstehen.

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 Ihrem Unternehmen 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

Anwendungsfälle

Quantifizierung und Visualisierung von Cyberrisiken im gesamten Unternehmen

Zscaler Risk360 nutzt automatische Engines, die echte Daten aus internen Quellen (Zscaler Zero Trust Exchange) aufnehmen. Der Risiko-Score des Unternehmens wird auf einer Skala von 0 bis 100 angegeben (wobei 100 kritisch ist). Gleichzeitig wird ein Vergleich mit Mitbewerbern durchgeführt, um Benchmarks und Trends im Zeitverlauf zu verstehen und so eine Verbesserung der Sicherheitslage zu erkennen. Zscaler Risk360 unterstützt Unternehmen auch durch die Visualisierung des Risiko-Scores im Zuge der Umstellung auf Zero Trust.

Datengestützte Risikobehebung

Mit den geführten Untersuchungsabläufen und Erkenntnissen für umsetzbare Empfehlungen können Kunden nach der Analyse des Risiko-Scores Maßnahmen zur schnellen Behebung ergreifen. Mit diesem Tool können Sie eine priorisierte Liste von Problemen erstellen, die mit dem Untersuchungsablauf analysiert werden können, um bestimmte Probleme genauer zu analysieren.

Finanzielle Auswirkungen der Cyber-Risiken

Kunden können die finanziellen Auswirkungen des Risikos ihres Unternehmens mithilfe der Quantifizierung finanzieller Verluste abschätzen.

Berichterstattung, Risikovisualisierung und Anleitung

Risk360 liefert detaillierte, sofort einsatzbereite Berichte wie unsere CISO-Vorstandsberichte, die den Cyber-Risikostatus für Führungskräfte zusammenfassen. Sowie unsere KI-gestützte Bewertung der Cybersicherheitsreife, um den Fortschritt bei der Zero-Trust-Transformation eines Unternehmens und die größten Risikobereiche aufzuzeigen.

Einführung von Zscaler Risk360

Viele Zscaler-Kunden können schnell und einfach den Risiko-Score ihres Unternehmens sowie umsetzbare Erkenntnisse und Empfehlungen einsehen. Dieses Visualisierungsframework ermöglicht es CISOs und CIOs, Cyberrisiken und finanzielle Gefährdungen zu bewerten, den Score mit dem von Mitbewerbern zu vergleichen und Arbeitsabläufe zur Verbesserung des Risiko-Scores vorzuschlagen. Fachkräfte, die Zugriff auf diesen Bericht haben, können die Daten nach Risikotyp, Entität (User, Anwendungen, Assets) und Standort aufschlüsseln. Der Bericht ermöglicht das Sortieren der Userliste nach Risiko und zeigt Anwendungen (sowohl in SaaS- als auch privaten und kombinierten Umgebungen) und Assets mit individuellen, diskreten Risikobewertungen.

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

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **www.zscaler.com/de**. Gerne können Sie uns auch auf X folgen **@zscaler**.

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

Zero Trust Everywhere