Asset Exposure Management: Präzise und umsetzbare CAASM-Erkenntnisse

Alle Ressourcen auf einen Blick. Lückenlose Abdeckung. Weniger Risiko.

Herausforderung für Unternehmen

Sicherheitsteams verbringen unzählige Stunden damit, Informationen aus mehreren unterschiedlichen Systemen zusammenzuführen, um eine genaue Bestandsaufnahme der Ressourcen zu erstellen. Trotz dieser Bemühungen bleiben die Listen der Ressourcen unvollständig und ungenau, was die Risikobewertung erheblich beeinträchtigt. Darüber hinaus ist es mit den aktuellen Tools äußerst schwierig, die Daten zu aktualisieren, wenn Teams fehlende oder falsche Informationen feststellen. Die meisten Teams haben Schwierigkeiten, kritische Sicherheitsfragen zu beantworten, wie z. B.:

- Wie viele IT-Assets besitzen wir wirklich?
- Wie genau ist unsere CMDB?
- Wem sollte ein Ticket zur Problembehebung für ein bestimmtes Asset zugewiesen werden?
- Welches Schutzniveau gilt für jede unserer wichtigsten Ressourcen?
- Zu welchem User, welcher Region, welcher Abteilung usw. gehören die einzelnen Ressourcen?
- Für welche Assets fehlt Schutzsoftware wie EDR?

Erhalten Sie mit unserem neuen Ansatz für CAASM eine präzise Übersicht über alle Ihre Ressourcen

Zscaler Asset Exposure Management bietet das umfangreichste, genaueste und detaillierteste Ressourceninventar der Branche. Durch die Nutzung der Datenkorrelation, die durch das patentierte Data Fabric for Security möglich ist, können Sie mit dem einzigartigen CAASM-Ansatz von Zscaler Lücken in der Abdeckung identifizieren, die CMDB-Hygiene automatisieren, Workflows zur Risikominderung erstellen und das Risiko für Ressourcen reduzieren. Die Lösung dient als zentrale Informationsquelle für Sicherheit, IT und andere Unternehmensbereiche, um die Ergebnisse in den Bereichen Sicherheit und Compliance zu verbessern, und als Grundlage für CTEM-Lösungen (Continuous Threat Exposure Management).

- **Ein zuverlässiges Inventar Ihrer Ressourcen erstellen:** Ermöglichen Sie die Auflösung von Ressourcen über Dutzende von Quellsystemen hinweg, um ein ganzheitliches und genaues Inventar zu erstellen.
- **Deckungslücken bei Ressourcen aufdecken und schließen:** Korrelieren Sie sämtliche Informationen zu den Ressourcen, um Fehlkonfigurationen und fehlende Kontrollen zu ermitteln.
- **Unternehmensrisiken minimieren:** Erfahren Sie, wie Sie Richtlinien zur Risikominimierung aktivieren, Workflows zuweisen und verfolgen und Ihre CMDB automatisch aktualisieren.
- **Ein effektives CTEM-Programm durchführen:** Ergänzen Sie Ihr lückenloses Exposure-Management-Programm mit umfassenden und vollständigen Ressourceninformationen.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Wie funktioniert das?

Für ein effektives Asset Exposure Management müssen unzählige bisher isolierte Datenquellen ermittelt und korreliert werden. Zscaler hat Pionierarbeit bei der Nutzung einer Data Fabric geleistet, das die Skalierbarkeit und Effektivität von Cyber Attack Surface and Asset Management (CAASM) grundlegend verändert.

Die Zscaler Data Fabric for Security aggregiert und korreliert nahtlos Informationen über Ressourcen aus über 150 Sicherheitstools und Geschäftssystemen und ermöglicht es Unternehmen so, ihre Angriffsfläche besser nachzuvollziehen und zu verwalten. Durch die Harmonisierung, Deduplizierung, Korrelation und Anreicherung von Millionen von Datenpunkten bietet die Data Fabric eine umfassende Übersicht über Ressourcen, Kontrollen, Lücken und Fehlkonfigurationen. Feedbackschleifen innerhalb des breiteren Zscaler-Ökosystems tragen zusätzlich dazu bei, diese Risiken für Ressourcen automatisch zu minimieren.

Weitere Informationen unter: zscaler.com/de/caasm

Durch folgende Maßnahmen lässt sich die Angriffsfläche verringern:

- **Aufbau eines einheitlichen, deduplizierten Ressourceninventars:** Erhalten Sie umfassende Transparenz über sämtliche Assets, einschließlich Endgeräte, Cloud-Ressourcen, Netzwerkgeräte und mehr. Erhalten Sie eine vollständige Darstellung der Angriffsfläche Ihrer Assets durch die kontinuierliche quellenübergreifende Deduplizierung, Korrelation und Auflösung von Assetinformationen.
- **Identifizierung und Erfassung von Compliance-Problemen und Fehlkonfigurationen:** Identifizieren Sie problemlos potenzielle Compliance-Probleme und Fehlkonfigurationen (z. B. Ressourcen ohne EDR, veraltete Agent-Versionen) und erstellen Sie daraus konkrete Aufgaben, um Ihren Sicherheitsstatus zu verbessern.
- **Gesteigertes Vertrauensniveau in Ihre CMDB:** Verbessern Sie die Genauigkeit und Vollständigkeit der CMDB. Identifizieren Sie Ressourcen, die nicht in Ihrer CMDB registriert sind oder bei denen Eigentümer, Informationen zum Speicherort oder andere Angaben fehlen. Erstellen Sie Workflows für Ihre zuständigen Teams, um die Vollständigkeit und Genauigkeit der Ressourcendetails zu gewährleisten.
- **Durchführung effizienter Maßnahmen zur Minimierung von Risken:** Aktivieren Sie Richtlinienanpassungen und andere Kontrollen, um das Risiko zu verringern, initiieren Sie Workflows, um Richtlinienverletzungen Eigentümern zuzuweisen, verfolgen Sie den Fortschritt der Schadensbegrenzung und aktualisieren Sie Ihre CMDB automatisch, damit sie immer korrekt und vollständig ist.
- **Verbesserung der teamübergreifenden Zusammenarbeit durch aussagekräftige Berichte und Dashboards:** Generieren Sie Dashboards und Berichte für den CMDB-Integritätsstatus und die Compliance-Kontrollen und nutzen Sie dabei eine Bibliothek vorgefertigter und userdefinierter Metriken.

zscaler™ | Experience your world, secured.™

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter 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 Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.com/de** oder folgen Sie uns auf Twitter unter **@zscaler**.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ und weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Marken bzw. Dienstleistungsmarken oder (ii) Marken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

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