CLOUDFLARE

Leitfaden

Risikoverwaltung an einem einzigen Ort

Komplexität und Risiko reduzieren – ein Leitfaden für CISO

Inhalt

Mehr als Risikoverwaltung: Unified Risk Posture

Als CISO trägt man die Verantwortung für Cybersicherheit und Risikoverwaltung. Doch die Technik und die digitalen Assets, die für das Unternehmen Risiken schaffen, befinden sich nicht immer im eigenen Einflussbereich. Das gilt zum Beispiel für:

- Die mit dem Internet verbundenen, von Angestellten und Dritten verwendeten Anwendungen, Geräte, Clouds und Netzwerke
- Die von Mitarbeitenden und Kunden generierten, gespeicherten und übermittelten Daten
- Der Quellcode und die API, die von Entwicklern erstellt und benutzt werden

Mit der Zeit werden viele Einzellösungen angeschafft, weil die Unternehmen versuchen, den Schutz für ihre zunehmend weiter verstreuten IT-Umgebungen auszudehnen. Diese Tools arbeiten jedoch allzu häufig isoliert und bieten nur begrenzte Interoperabilität. Das kann es für Sicherheitsabteilungen schwierig machen, den Überblick über die von ihnen generierten Daten und die Risiken zu behalten. Diese Fragmentierung verursacht zu großen manuellen Aufwand und eine zielführende Priorisierung der Risiken nimmt zu viel Zeit und zu viel Expertise in Anspruch.

Eine solche Komplexität birgt Gefahren. Beispielsweise haben in einer Umfrage der Enterprise Strategy Group von TechTarget **drei Viertel (76 Prozent) der Unternehmen angegeben, dass sie über eines dem Internet ausgesetzten, unbemerkten, nicht oder schlecht verwalteten Assets einen Cyberangriff erlebt haben.**

Um das Cybersicherheitsniveau für die gesamte dezentrale Umgebung zu erhöhen, sind Veränderungen erforderlich. Im Kontext sich ausweitender Angriffsflächen sollten Unternehmen eine einheitlichere, stärker integrierte Herangehensweise an die Risikoverwaltung prüfen. Damit lässt sich Folgendes erreichen:

- **Effizientere Beseitigung** von Risiken mit geringerem Aufwand
- **Optimierung** dessen, was mit bestehenden Tools und Risikohinweisen getan werden kann
- Schnellere **Anpassung** an eine sich wandelnde Bedrohungslage
- **Automatisierung** einer größeren Zahl von Sicherheitsabläufen

„Risikoverwaltung an einem einzigen Ort: Komplexität und Risiko reduzieren – ein Leitfaden für CISO“ erläutert die Vorteile, Anwendungsbereiche und ein dreistufiges Framework (siehe unten) für die Risikoverwaltung. Mehr erfahren Sie im folgenden Text.

Dreistufiges Framework

Bewertung des Risikos für sämtliche IT-Umgebungen

… durch den Austausch von Risikoindikatoren zwischen verschiedenen Tools für einen umfassenderen Überblick

… zur Durchsetzung von Risikokontrollen und zum Schutz des Unternehmens.

Wie funktioniert Risikoverwaltung an einem einzigen Ort?

Viele Einzelteile – ein gemeinsames Ziel

Auf Führungsebene müssen für bei der Risikoverwaltung im Wesentlichen drei Aufgaben erfüllt werden:

1. Bewertung der Risiken für sämtliche IT-Umgebungen mithilfe dynamischer firmeneigener Scoring-Modelle
2. Austausch von Risikohinweisen – also Daten zwischen Tools – zur Gewinnung eines umfassenderen Überblicks über die bestehenden Risiken
3. Automatisierte und einheitliche Durchsetzung von Kontrollen auf Grundlage der gewonnenen Erkenntnisse

Die Bündelung der Risikoverwaltung vereinfacht diesen Prozess, indem diese Schritte in so wenigen Sicherheitssystemen wie möglich durchgeführt werden: idealerweise auf einer einzigen Plattform. Die Kombination aus einem dynamischen, firmeneigenen Risiko-Score, Integrationen zum Austausch von Informationen zwischen Sicherheitstools und automatisierten Sicherheitsmaßnahmen gibt Unternehmen eines solidest Rüstzeug, um Risiken zu beurteilen, zu priorisieren und zu neutralisieren.

Dieser Ansatz ist umso wirkungsvoller, je mehr man den Überblick und die Kontrolle über die eigene Angriffsfläche verbessern kann – unter anderem zum Schutz von Mitarbeitenden, Anwendungen, Daten und Netzwerken.

Durch die Bündelung dieser Aufgaben der Risikoverwaltung auf einer einzigen Plattform kann außerdem die Abhängigkeit von Einzellösungen verringert werden. Darüber hinaus lässt sich mit den Risikohinweisen aus dem vorhandenen IT-Ökosystem mehr anfangen und Schutzmaßnahmen können überall angewandt werden.

Das Bündeln der Risikoverwaltung erleichtert die Anpassung an Veränderungen interner und externer Risikovektoren. Dazu gehören:

Nutzerbezogene Risiken

- Phishing
- Ransomware
- Fernzugriff
- Mobilgeräte / BYOD
- Drittanbieter / Lieferkette
- … und vieles mehr.

Datenbezogene Risiken

- Datenverlust / Datenoffenlegung
- Datendiebstahl / Datenleck
- Datenschutzverstöße
- Compliance-Verstöße
- Datenmanipulation
- … und vieles mehr.

Anwendungsbezogene Risiken

- Denial Of Service
- Zero-Day-Schwachstellen
- SQL-Injection
- Cross-Site Scripting
- KONTOÜBERNAHMEN
- Schatten-IT (inklusive API)
- … und vieles mehr.

Vorteile der Risikoverwaltung an einem einzigen Ort

Wenn Bewertung, Austausch und Durchsetzung von einem einzigen Ort aus gesteuert werden können, wird die Risikoverwaltung für die gesamte Angriffsfläche unkomplizierter und weniger aufwendig.

Vorteile	Ausgewählte Kennzahlen
Reduzierung des Arbeitsaufwand für SecOps durch einen geringeren manuellen Anteil bei Richtlinienerstellung und größere Flexibilität bei der Vorfallreaktion	• Steigerung der Zahl automatisierter Arbeitsabläufe • Reduzierung der Zahl von Klicks bei der Richtlinienerstellung • Verkürzung der mittleren Zeit bis zur Erkennung von Bedrohungen • Verkürzung der mittleren Zeit bis zur Reaktion auf Bedrohungen
Verringerung des Cyberrisikos durch automatische und dynamische Durchsetzung von Maßnahmen zur Risikoneutralisierung für die Angriffsfläche	• Reduzierung der Zahl schwerwiegender Vorfälle • Steigerung der Zahl automatisch blockierter Bedrohungen

Sicherheitstechnologien und ihre Rolle bei der Bündelung der Risikoverwaltung

Security Service Edge (SSE)-Plattformen ermöglichen es Unternehmen, den Zugriff abzusichern, sich vor Bedrohungen abzuschirmen und Daten sowohl in webbasierten, als auch in per SaaS bereitgestellten und in Form privater Anwendungen gestalteter Umgebungen zu schützen. Dank dieser großen Bandbreite bieten SSE-Plattformen einen einzigartigen Überblick über Nutzeraktivitäten für sämtliche IT-Umgebungen. So werden Modelle angereichert, anhand derer sich riskantes oder verdächtiges Verhalten in Echtzeit aufspüren lässt. Zudem hilft die cloudbasierte SSE-Herangehensweise an Netzwerksicherheit dabei, die Erstellung und Durchsetzung von Richtlinien für das gesamte Unternehmen an einem zentralen Punkt zusammenzuführen.

Während bei SSE der Schwerpunkt auf dem Schutz der internen IT-Infrastruktur eines Unternehmens liegt, geht es bei der Webanwendungs- und API-Sicherheit **(Web Application and API Security – WAAP)** um den Schutz der öffentlich zugänglichen Angriffsfläche. Es muss also ein breites Spektrum an Risiken, darunter die Ausnutzung von Schwachstellen, Bots, unbefugter Zugriff, Betrug, Missbrauch und Denial-of-Service, eingehegt werden.

Das Zusammenführen von SSE- und WAAP-Funktionen auf einer einzigen Plattform kann Unternehmen dabei helfen, die Risikoverwaltung auf die Schlüsselbereiche Mitarbeitende, Anwendungen und Daten auszuweiten.

Andere bewährte Technologien ergänzen die SSE- und WAAP-Sicherheitsplattformen:

- **Security Information and Event Management (SIEM)- und Extended Detection and Response (XDR)**-Plattformen fassen Protokolle und Risikoinformationen für sämtliche Umgebungen zwecks Überwachung, Analyse und Berichterstattung zusammen. Viele Unternehmen greifen auf solche Tools zurück, um Sicherheitsvorfälle zu untersuchen, darauf zu reagieren und die Compliance zu gewährleisten.
- Unternehmen setzen auch häufig Anbieter von **Endpunktsicherheit** zum Schutz von Geräten sowie auf Tools für das **Identitäts- und Zugriffsmanagement** zur Authentifizierung von Nutzern ein. Als zusätzliche Sicherheitsebenen liefern diese Tools umfangreiche Informationen über Geräte- und Nutzeraktivitäten, die dann von mehreren Sicherheitsplattformen gemeinsam verwendet werden können.

Jede der genannten Technologien weist für sich genommen gewisse Einschränkungen hinsichtlich der Übersicht und Kontrolle über die Angriffsfläche auf. Doch **die Nutzung der Funktionen und der Informationen des gesamten Sicherheits-Ökosystems bildet die Grundlage für eine effektivere Risikoverwaltung.**

1. Schritt: Bewertung des Risikos

Erstellung von Risiko-Scores für alle Nutzer mit SSE vereinfachen

Modelle zur Analyse des Nutzer- und Entitätsverhaltens (User and Entity Behavior Analytics – UEBA) spielen eine wichtige Rolle bei der Anpassung von Unternehmen an sich verändernde Risiken. UEBA-Modelle stützen sich häufig auf maschinelles Lernen. Sie erkennen ungewöhnliche oder gefährliche Aktivitäten von Nutzern, Geräten und anderen Entitäten und alarmieren dann Sicherheitsteams, damit Gegenmaßnahmen ergriffen werden können. Das erspart umfangreiche manuelle Analysen und trägt dazu bei, mit den Bedrohungen Schritt zu halten.

In der Praxis ist der Einsatz von UEBA-Modellen aber unter Umständen immer noch ineffizient. Beispielsweise werden diese Modelle häufig für SIEM- und XDR-Tools verwendet. Um Ungenauigkeiten zu vermeiden, müssen bei diesen Werkzeugen dann aber Feinabstimmungen und Anpassungen vorgenommen werden, die selbst gut ausgestattete SOC ab einem gewissen Umfang nicht mehr leisten können.

Alternativ kann die Erstellung von Risiko-Scores direkt in eine SSE-Plattform eingebettet werden. Das hilft bei der einheitlichen Protokollierung und der Durchsetzung von Regeln für webbasierte, per SaaS bereitgestellte und private Anwendungen. Dadurch wird der komplizierte Einsatz von UEBA-Modellen ausschließlich innerhalb von SIEM/XDR-Plattformen vermieden. SSE-Plattformen können den Kreislauf zwischen der Erkennung risikobehafteten Verhaltens und der Durchsetzung von Richtlinien (z. B. Blockieren von Datenverkehr) in Netzwerksicherheitsumgebungen schnell schließen.

Beispiele für Einsatz von nutzerbezogenen Risiko-Scores

Bei der Erstellung von Risiko-Scores für Nutzer – eine Komponente von UEBA – werden die Nutzeraktivitäten auf verdächtige und risikobehafteten Aktionen hin überprüft. Bei gefährlicheren Aktionen werden höhere Scores vergeben. An diesen lässt sich die Wahrscheinlichkeit einer Kompromittierung, einer Insider-Bedrohung oder anderer Risiken ablesen. Die Erstellung nutzerbezogener Risiko-Scores ist ein gängiges Feature von SSE-Plattformen, die direkten Einblick in sämtliche Netzwerkaktivitäten haben.

Nutzern kann in Echtzeit beispielsweise aus den folgenden Gründen ein hoher Risiko-Score zugewiesen werden:

- **Unmöglicher Ortswechsel:** Ein Nutzer meldet sich innerhalb eines unangemessen kurzen Zeitraums von zwei verschiedenen Standorten aus an (z. B.: ein Mitarbeiter meldet sich von New York City aus an und dann ein paar Minuten später von Sydney aus)
- **Wiederholte Data Loss Prevention (DLP)-Verstöße:** Sensible oder vertrauliche Informationen werden in einer Weise verschoben oder weitergegeben, die gegen Unternehmensrichtlinien oder -vorschriften verstößt (z. B. wenn eine Entwicklerin versucht, geschützten Quellcode in einen KI-Chatbot eines Drittanbieters hochzuladen)
- **Wiederholte Verwendung von risikobehafteten Geräten:** Geräte werden als unsicher eingestuft oder verstoßen gegen Unternehmensrichtlinien (z. B. wenn ihnen die neuesten Betriebssystem-Updates fehlen oder sie ungepatchte Sicherheitslücken aufweisen)

Zusammenführung der Risikobewertung für sämtliche Nutzer und Anwendungen

SSE-Plattformen bilden eine immer beliebtere moderne Grundlage für die Erkennung von Risiken auf Nutzerebene mit UEBA-Modellen. Aufgrund des heutigen Fokus auf IT-Konsolidierung suchen Unternehmen jedoch nach Möglichkeiten, die Risikobewertung weiter auszudehnen, um Bedrohungen für öffentlich zugängliche Anwendungen, Websites und API mit abzudecken.

Durch die Zusammenführung von SSE- und WAAP-Sicherheitsfunktionen auf einer Plattform erhalten Unternehmen Übersicht, Kontrolle und gemeinsame Informationen über Nutzer und Anwendungen, die einen erheblichen Anteil der Angriffsfläche eines typischen Unternehmens ausmachen.

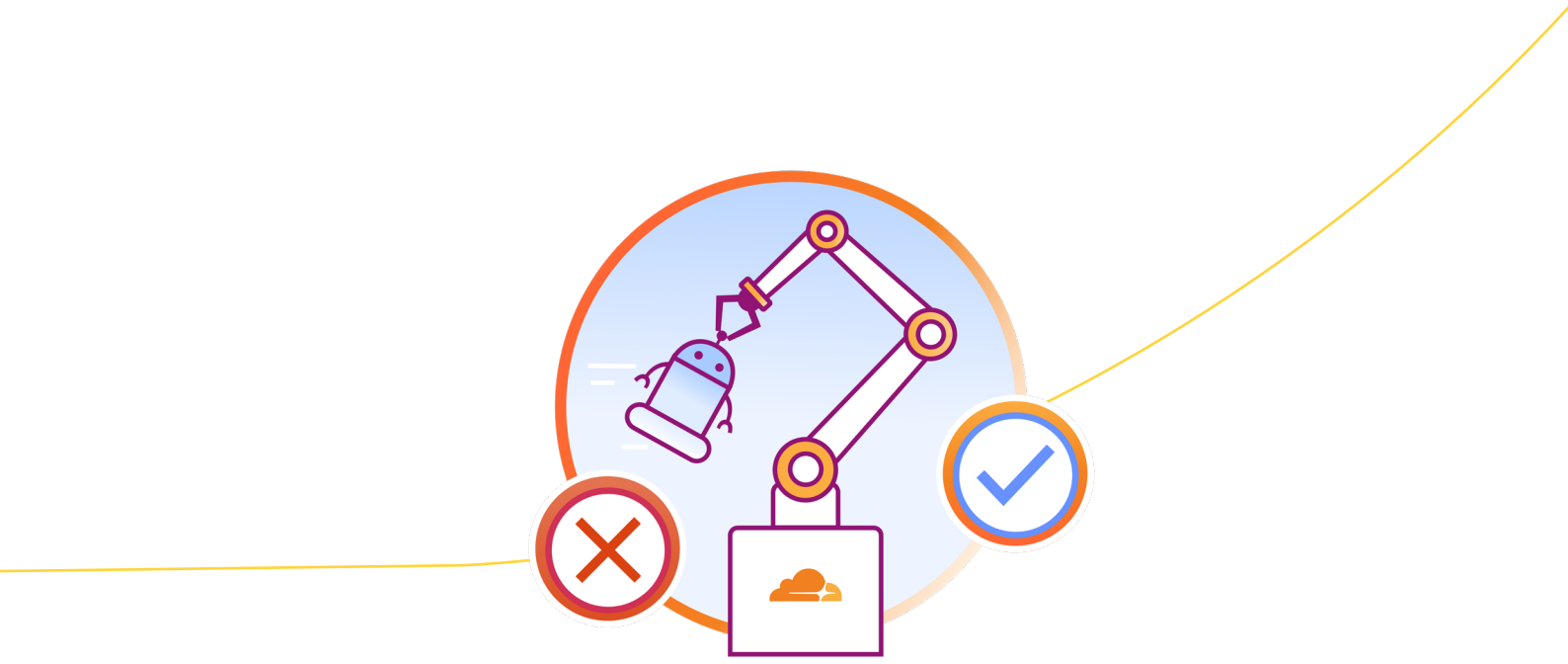
Beispielmodelle für Risiken bei Anwendungen

Zum Schutz von Anwendungen erkennt und neutralisiert die Cloudflare-Plattform beispielsweise bösartige Payloads und Bots mithilfe von Risikomodellen wie den folgenden, die durch maschinelles Lernen (ML) unterstützt werden:

- Unser **WAF Attack Score**, der eine Bewertung darüber bietet, ob eine Anfrage eine Zero-Day-Schwachstelle oder eines der weit verbreiteten Risiken aus den OWASP Top 10 enthält, etwa SQL-Injection, Cross-Site-Scripting oder einen Payload zur Remote Code Execution
- Unser **Bot-Score**, der die Wahrscheinlichkeit anzeigt, laut der eine Anfrage von einem Bot stammt
- Unser **Klassifizierer für schädliche Skripte**, der die Gefahren von Browser-Skripten für Ihre Website-Besucher prüft

Andere ML-Modelle helfen Sicherheitsteams beim Aufspüren neuer API-Endpunkte und -Schemata, ohne dass der Kunde dafür im Vorfeld irgendwelche Angaben machen muss.

Ein Überblick über die Anwendungsinfrastruktur hilft dabei, Risiken proaktiv in Dashboards anzeigen zu lassen. Dabei kann es sich unter anderem um ungeschützte RDP-Server, nicht überprüfte DNS-Einträge oder Domains ohne TLD-Verschlüsselung handeln.



2. Schritt: Austausch von Risikohinweisen

Mit vorhandenen Tools mehr erreichen, und zwar mit weniger Aufwand

Stellen Sie sich vor, dass Ihr Sicherheitsteam einen auf den Auftragnehmer „Tom Fischer“ abzielenden Phishing-Versuch erkannt (und gestoppt) hat. Wenn festgestellt wird, dass ein Nutzer von einer Phishing-Kampagne betroffen ist, kann das ausreichen, um diesen als risikobehaftet einzustufen. Das entspricht dem gerade beschriebenen ersten Schritt. Eine Erhöhung der Risiko-Scores dieses Nutzers kann dazu führen, dass sein Zugriff auf Systeme eingeschränkt wird.

Aber handelte es sich um einen Einzelfall? Oder nehmen dieselben Angreifer Tom oder andere Mitarbeitende weiterhin auf andere Weise ins Visier? Wurde womöglich sein Gerät bereits kompromittiert?

CISO brauchen das Gesamtbild – nicht nur eine Reihe von Protokollen – um die Cybersicherheit ihres Unternehmens kontinuierlich aufrechtzuerhalten und zu stärken.

Um effektiv und effizient auf Bedrohungen reagieren zu können, benötigen CISO einen automatisierten Zwei-Wege-Austausch von Risikohinweisen mit ihrem übergeordneten Ökosystem von Tools, einschließlich:

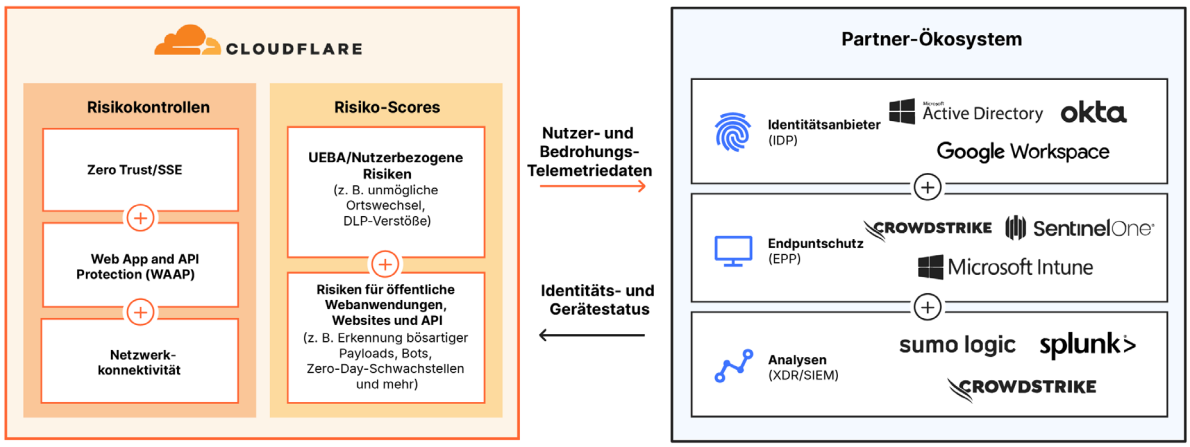
- **Identitätsanbieter (IdP)** speichern und verwalten die digitalen Identitäten Ihrer Nutzer
- **Endpunktschutz (EPP)**-Dienstleister sichern die Geräte ab, die mit Ihrem Netzwerk verbunden sind
- **Security Information and Event Management (SIEM)**-Plattformen sammmeln, analysieren und verwalten Ihre Protokoll- und Vorfallsdaten, um nach Anzeichen für Sicherheitsvorfälle zu suchen
- **Extended Detection and Response (XDR)**-Plattformen optimieren die Aufnahme von Sicherheitsdatenanalysen und helfen Ihnen bei der Durchsetzung weitere Präventions- und Abhilfemaßnahmen

Bei dem Vorfall, in den „Tom“ verwickelt ist, entlastet eine an einem einzigen Ort gebündelte Risikoverwaltung Ihre SecOps-Teams, indem automatisch Informationen mit Ihren vorhandenen Sicherheitstools ausgetauscht werden:

1. Telemetriedaten von Cloudflare, einschließlich Protokolle über blockierte Aktivitäten und sogar Risiko-Scores individueller Nutzer, werden in Ihrem gesamten Sicherheits-Ökosystem ausgetauscht – auch mit SIEM- und XDR-Tools, die parallel dazu mit tiefergehenden automatischen Scans fortfahren können.
2. Diese Sicherheitstools melden dynamische Risikoinformationen an Cloudflare zurück. Zum Beispiel können IdP- und EPP-Partner ihre nutzer- und gerätebezogenen Risiko-Scores an Cloudflare übermitteln, damit sie in Statusprüfungen zur Zugriffsbeschränkung einfließen können.

Einmalige Integrationen von Cloudflare mit diesen EPP-, IdP-, XDR- und SIEM-Tools verschaffen CISO einen besseren Überblick und automatisieren die Sicherheitsorchestrierung für mehrere Domains. Auf diese Weise können Ihre SecOps-Teams **mit den vorhandenen Tools mehr erreichen.**

Firmeneigene Risikobewertung von Cloudflare und Austausch von Risikohinweisen mit erstklassigen Partnern



3. Schritt: Durchsetzung

Risikokontrolle für die wachsende Angriffsfläche automatisieren

Mit den ersten beiden Schritten können CISO einen dynamischen und ganzheitlichen Überblick über die Risiken in ihren Umgebungen gewinnen.

Der letzte Schritt ist jedoch der wichtigste: die Durchsetzung von Kontrollen und Schutzmaßnahmen auf Grundlage der in Schritt 1 und 2 gewonnenen Erkenntnisse. Eine Plattform, auf der alle drei Schritte zusammengeführt werden, hilft bei der einheitlichen Anwendung von Richtlinien auf alle Standorte und alle Umgebungen. Damit passen sich die Sicherheitsvorkehrungen an Ihre Bedürfnisse an.

Die folgenden drei Anwendungsfälle veranschaulichen, wie die Durchsetzung dafür sorgt, dass eine einheitliche, an einem Ort gebündelte Risikoverwaltung mit Cloudflare in der Praxis Vorteile bringt.

Anwendungsfall Nr. 1: Einführung von Zero Trust mit Überprüfung des Gerätestatus

Cloudflare arbeitet mit Ihren EPP- und SIEM-Tools zusammen, um Zero Trust-Kontrollen durchzusetzen, die sich auf die Ihre gesamte Belegschaft betreffenden Risiken einstellen.

Nehmen wir zum Beispiel ein Szenario, in dem ein Nutzer über verschiedene Kanäle, einschließlich Web und E-Mail, angegriffen wird. Cloudflare ergreift dann folgende Maßnahmen:

- **Bereitstellung der ersten Verteidigungslinie** durch Verhindern des Surfens auf riskanten Websites und das Blockieren von Phishing-E-Mails
- **Erfassung des von Ihrem EPP-Tool übermittelten Gerätestatus**, das das Gerät des Nutzers gescannt und eine Infizierung festgestellt hat
- **Einschränkung des Zugriffs des Nutzers** für Anwendungen auf Grundlage des von Ihrem EPP-Tool gemeldeten Gerätestatus
- **Weitergabe von Protokolldaten** an Ihre SIEM/XDR-Plattform zur eingehenderen Analyse, die zu weiteren Abhilfemaßnahmen wie der Quarantäne des Geräts führen kann

Anwendungsfall Nr. 2: Schutz von Anwendungen, API und Websites – selbst vor Zero-Day-Schwachstellen

Für Sicherheitsteams ist es schwierig, mit den ständigen Angriffen mittels Zero-Day-Schwachstellen, Bots, bösartiger clientseitiger Dritt-Skripte, Injection und anderer Sicherheitslücken Schritt zu halten.

Cloudflare hilft bei der Verteidigung von Anwendungen, API und Websites durch:

- **Automatisches Blockieren** von bösartigen Payloads, Bots und sogar Zero-Day-Schwachstellen mithilfe von ML-gestützten Risikomodellen, die Angriffsvarianten und gefährlichen oder anomalen Datenverkehr identifizieren.
- **Überblick an zentraler Stelle** mit Dashboards und Analysen zur Überprüfung potenzieller Fehlkonfigurationen, Risiken von Datenlecks und Schwachstellen, die Ihre Infrastruktur betreffen.

Mit Cloudflare können dieselben Sicherheitsvorkehrungen, die Unternehmen vor öffentlich zugänglichen Anwendungen anwenden können (wie WAF, DDoS-Abwehr und Bot-Management), auch zum Schutz interner Infrastrukturen wie selbst gehosteter Jira- und Confluence-Server eingesetzt werden.

Anwendungsfall Nr. 3: Schutz sensibler Daten

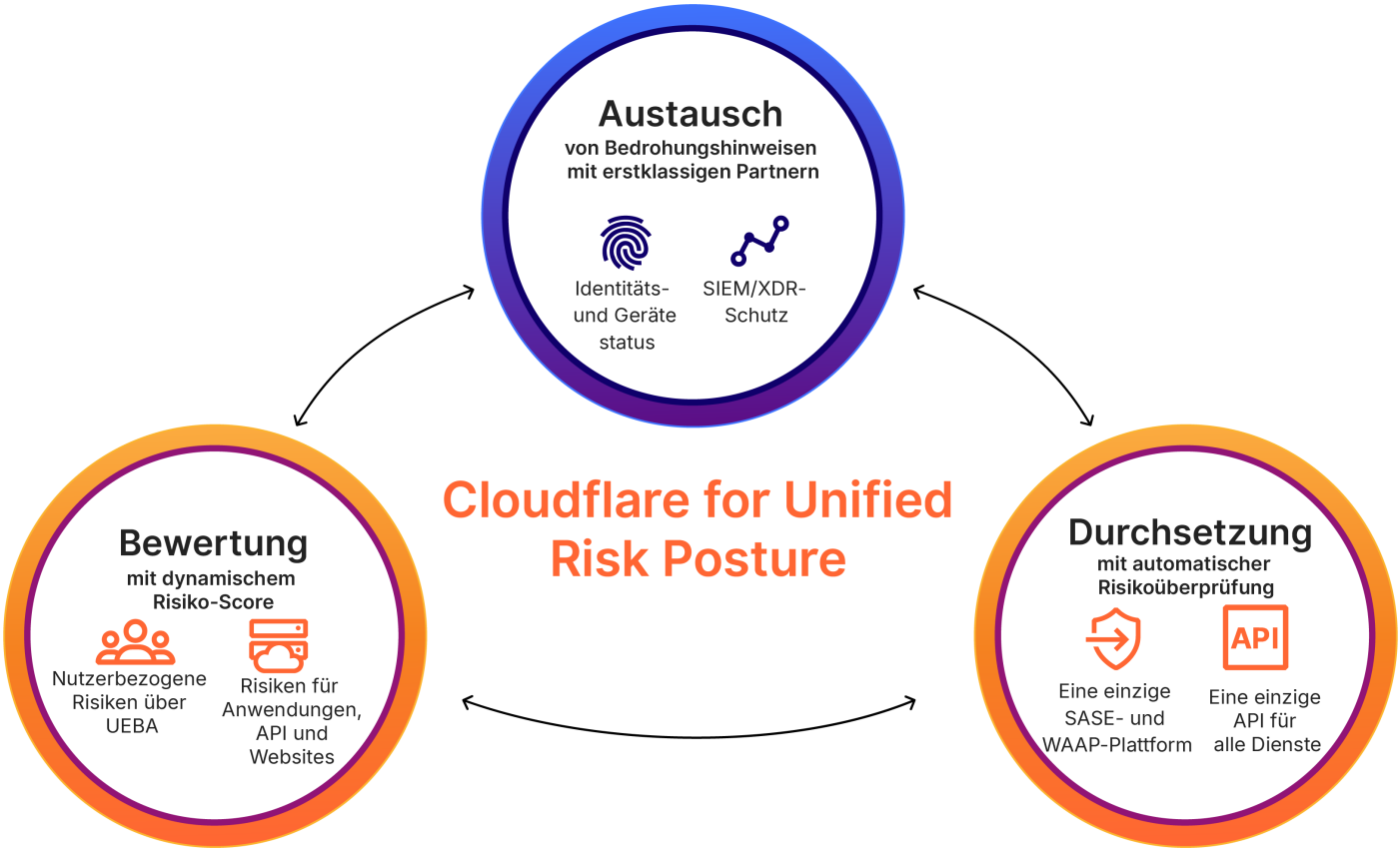
Angesichts der schieren Menge an Big Data, IoT-Geräten und der zunehmenden Beliebtheit von KI und LLM ist es schwieriger denn je, den Überblick zu behalten und die Sicherheitskontrollen über die gemeinsame Nutzung von Daten in Cloud-Umgebungen zu gewährleisten.

Nutzer, die mit hohem Risiko behaftet sind und mit sensiblen Daten zu tun haben, lassen sich mithilfe von Cloudflare leicht identifizieren, sodass ihr Zugriff entsprechend eingeschränkt werden kann.

Wenn beispielsweise ein Entwickler versucht, geschützten Quellcode in ein öffentliches GitHub-Repository hochzuladen, ergreift Cloudflare folgende Maßnahmen:

- **Durchsetzung von Datenkontrollen**, um diesen Upload zu blockieren und zu verhindern, dass der Quellcode den Firmenbereich verlässt
- **Heraufsetzung des Risiko-Scores des Nutzers** (über UEBA) auf Grundlage dieser verdächtigen Aktivität, damit das Sicherheitspersonal weitere Untersuchungen durchführen kann
- **Beschränkung des Zugriffs** bis zum Abschluss der Untersuchung, entweder durch Isolieren oder durch vollständiges Sperren des Zugriffs auf Firmenanwendungen

Was für Cloudflare for Unified Risk Posture spricht



Einfachheit | Eine Plattform zur Risikoverwaltung an einem einzigen Ort

Cloudflare reduziert den betrieblichen Aufwand durch die Konsolidierung der Sicherheit und die Vereinfachung der Risikoverwaltung für alle Mitarbeitenden, Anwendungen und Netzwerke.

Cloudflare hilft Ihnen durch die Zusammenführung von SSE- und WAAP-Risiko-Scores und -Kontrollen auf einer einzigen Plattform und in einem einzigen globalen Netzwerk, auf mehrere, sich überschneidende Tools zu verzichten, die ansonsten Redundanz, blinde Flecken und versteckte Kosten verursachen.

- Verringerung des Zeit- und Arbeitsaufwands für die Erstellung und Durchsetzung von Richtlinien
- Erweiterung des Schutzes in Ihrem eigenen Tempo mit grenzenloser Interoperabilität zwischen Diensten
- Orchestrierung aller Dienste mit unserer API, die eine Anpassung und Automatisierung ermöglicht
- Minimierung und Schutz der Angriffsfläche mit bewährten Zero Trust-Prinzipien

„Cloudflare hilft uns, Gefahren erfolgreicher und mit weniger Anstrengung abzuwehren. Außerdem lässt sich ein Zero Trust-Konzept im gesamten Unternehmen damit leichter umsetzen.“

indeed

Was für Cloudflare for Unified Risk Posture spricht

Flexibilität | Einmalige Integrationen mit erstklassigen Partnern

Cloudflare arbeitet mit den Tools, die Sie bereits für den Austausch von Risikodaten verwenden. Im Gegensatz zu anderen Anbietern müssen Sie Integrationen bei uns nur einmal einrichten. Anschließend können diese Funktionen dann auf der gesamten Plattform von Cloudflare genutzt werden, sodass Sie sich nicht auf die Einrichtung konzentrieren müssen, sondern sich dem Risikomanagement widmen können.

Anbieter von Endpunktschutz (EPP): Wenn sich ein Nutzer bei einer von Cloudflare geschützten Anwendung anmeldet, können wir überprüfen, ob das Gerät von einem EPP geschützt wird. Dieser wiederum kann prüfen, ob das Gerät mit Malware infiziert wurde oder andere aktive Sicherheitsbedrohungen bestehen. In einigen Fällen bezieht Cloudflare Risiko-Scores von EPP-Partnern, um eingehender zu prüfen, ob ein Gerät als zu risikobehaftet für den Zugriff auf interne Anwendungen oder Netzwerkfunktionen eingestuft wird. Durch diesen sofortigen Informationsaustausch werden Bedrohungen automatisch neutralisiert.

Identitätsanbieter (IdP): In der Zwischenzeit überprüfen Identitätsanbieter, ob die auf das Netzwerk zugreifenden Mitarbeitenden auch wirklich die sind, für die sie sich ausgeben. Cloudflare arbeitet mit führenden IdP zusammen, um betrügerische Zugriffsversuche zu vereiteln, was unter anderem unmögliche Ortswechsel umfasst.

SIEM/XDR-Anbieter: Unsere Zusammenarbeit erstreckt sich auch auf SIEM- und XDR-Partner, die umfassende Daten von Cloudflare in ein zentralisiertes Dashboard einspeisen. Dies ermöglicht es Analysten, Sicherheitsbedrohungen schnell zu erkennen und darauf zu reagieren. Einige XDR, darunter auch solche, die durch KI/ML unterstützt werden, versorgen Analysten mit aussagekräftigen Warnungen und ermöglichen entschlossenes Handeln zur Neutralisierung von Bedrohungen, bevor diese eskalieren.

Skalierbarkeit | Ein globales Netzwerk zur Durchsetzung und für Bedrohungsdaten

Jeder unserer Sicherheitsdienste ist für Kunden bei jedem unserer mehr als 320 Netzwerkstandorte einsetzbar (Stand: 1. Quartal 2024). Die Single-Pass-Überprüfung und Richtliniendurchsetzung funktionieren immer schnell, einheitlich und zuverlässig.

Darüber hinaus werden unsere KI/ML-gestützten Modelle zur Identifizierung von Risiken durch einzigartige Daten aus unserem globalen Netzwerk unterstützt, darunter:

- Erkenntnisse aus unserer Funktion als Reverse-Proxy, der von fast 20 % des Webs genutzt wird
- ca. 3 Bio. DNS-Anfragen pro Tag
- Durchsuchung von mehr als 8 Mrd. Webseiten alle zwei Wochen
- durchschnittlich 209 Mrd. blockierte Cyberbedrohungen am Tag

> **„Eine einzige Cloudflare-Lösung zu haben, die uns dabei hilft, die Komplexität unserer globalen Aktivitäten zu bewältigen, hat uns die Arbeit wesentlich erleichtert. Cloudflare hat uns bei jedem Schritt unterstützt.“**
>
> Delivery Hero

Mehr erfahren

Cloudflare for Unified Risk Posture ist eine neue Reihe von Funktionen zur Risikoverwaltung im Bereich Cybersicherheit, die Unternehmen bei der automatischen und dynamischen Durchsetzung von Maßnahmen zur Neutralisierung von Risiken in Verbindung mit ihrer wachsenden Angriffsfläche unterstützen.

Erfahren Sie mehr über den einheitlichen Cloudflare-Ansatz

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV:BDES-5826.2024MAY15