RAPID7

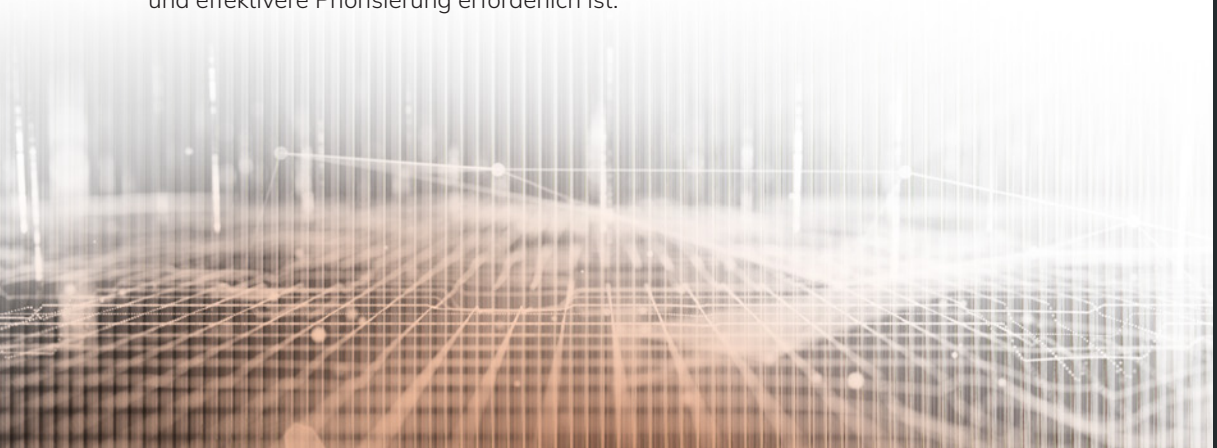
LÖSUNGSÜBERSICHT

ERMITTELN UND PRIORISIEREN SIE BEDROHUNGEN VOM ENDPUNKT BIS ZUR CLOUD MIT RAPID7 EXPOSURE COMMAND

Schützen Sie Ihre gesamte Angriffsfläche vor Bedrohungen mithilfe kontextbezogener Informationen aus allen Tools in Ihrem Stack

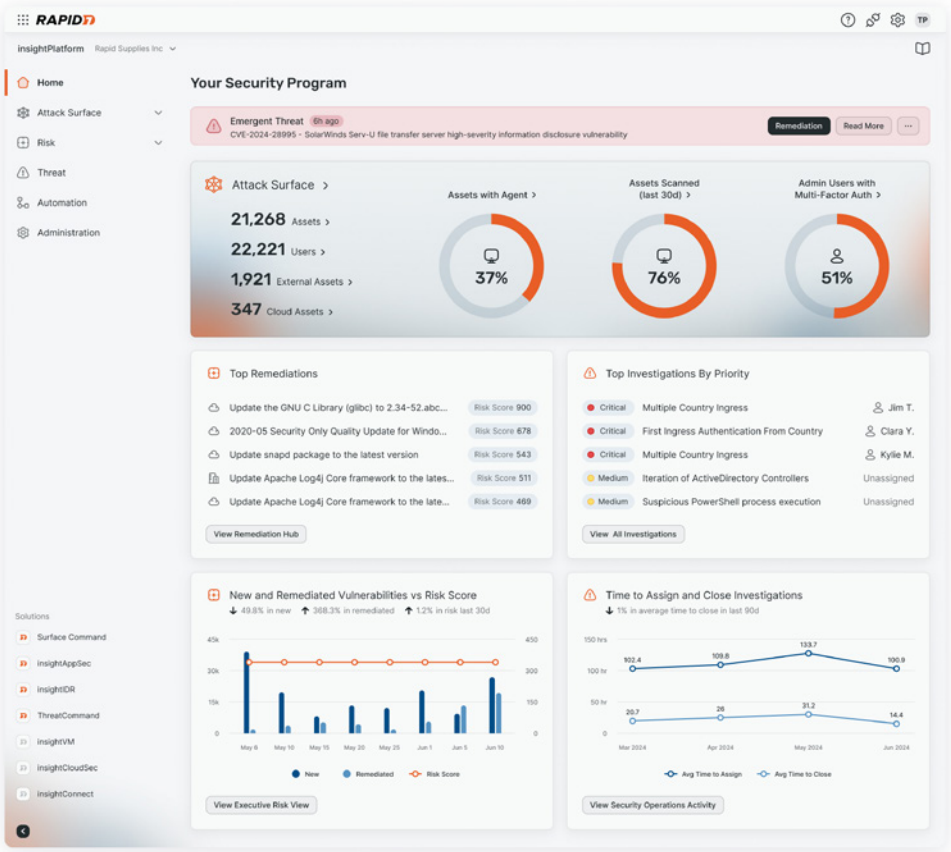
Unternehmen geben immer mehr Geld für Tools aus, um ihre Unternehmen zu verwalten und zu sichern, haben jedoch immer weniger Einblick in ihre Umgebung. Dadurch entsteht eine weitläufige Angriffsfläche, die über interne, externe und hybride Umgebungen verteilt ist. Das ist ein klarer Vorteil für den Angreifer. Cyberkriminelle können diesen Wildwuchs an Daten und Datensilos ausnutzen, indem sie sich in den Datenbergen verstecken und auf Ihre Unfähigkeit setzen, Ihre Angriffsfläche zu korrelieren und zu visualisieren und die für Ihre Sicherheit entscheidenden Einblicke zu identifizieren.

Rapid7 Exposure Command bietet nicht nur vollständige Transparenz über die Angriffsfläche, sondern auch einen hochpräzisen Risikokontext und Einblicke in die Sicherheitslage Ihres Unternehmens. Dabei werden die Ergebnisse sowohl unserer nativen Funktionen zur Erkennung von Schwachstellen als auch von bereits vorhandenen Schwachstellen- und Anreicherungsquellen von Drittanbietern zusammengeführt. Durch dieses Situationsbewusstsein können sich die Teams gezielt auf die Gefährdungen und Schwachstellen konzentrieren, die Angreifer im Visier haben – mit dem bedrohungsbezogenen Risikokontext, der für eine effizientere und effektivere Priorisierung erforderlich ist.



> **Nur 17 % der Unternehmen können einen Großteil (mindestens 95 %) ihrer Assets eindeutig identifizieren und inventarisieren.“**

2024 Gartner® Innovation Insight: Attack Surface Management Report



Erstellen Sie eine zentrale Datenquelle für Ihre gesamte digitale Umgebung

Vereinheitlichen und korrelieren Sie Ihre Assets und Identitäten in Ihrem gesamten Sicherheitsökosystem. Gleichen Sie die Ergebnisse mit regelmäßigen externen Scans ab, um die tatsächliche Angriffsfläche Ihres Unternehmens nachzuvollziehen und eine zentrale Datenquelle für alle Teams einzurichten.

Ermitteln Sie Assets, denen angemessene Sicherheitskontrollmechanismen fehlen

Ermitteln Sie kontinuierlich Lücken in der Cybersecurity-Abdeckung, um festzustellen, wo Assets keine Kontrollmechanismen wie Sicherheitsagenten für Endpunkte und Schwachstellen-Scans aufweisen, und welche Identitäten über Administratorzugriff verfügen oder keine MFA nutzen.

Priorisieren Sie die Behebung von Schwachstellen in Ihrer gesamten Angriffsfläche

Reichern Sie die kontinuierliche Überwachung der Angriffsoberfläche mit umfassendem Umgebungskontext und automatisiertem Risiko-Scoring an, um die riskantesten toxischen Kombinationen zu identifizieren und zu beseitigen.

Bis 2026 werden Unternehmen, die ihre Cybersecurity-Investitionen basierend auf einem Programm für kontinuierliches Exposure Management priorisieren, mit dreimal geringerer Wahrschein-lichkeit von einem Verstoß betroffen sein.“

Die wichtigsten strategischen Technologietrends für 2024: Continuous Threat Exposure Management, Gartner

Identifizieren Sie Pfade für die Ausbreitung im Netzwerk in Cloud-Umgebungen

Mit der Attack Path-Analyse können Teams die Beziehungen zwischen vernetzten Cloud-Ressourcen visualisieren und das Risiko für eine Ausbreitung von Angreifern in Ihrer Umgebung aufdecken, sollten diese Zugriff auf Ihre Umgebung erlangt haben.

Sorgen Sie für Verantwortlichkeit und Compliance in hybriden Umgebungen

Erlangen Sie ein Verständnis für den Cybersecurity-Status und die Eigentumsverhältnisse von Assets und sorgen Sie für die Einhaltung interner Richtlinien, branchenüblicher Best Practices und regulatorischer Frameworks in Ihrer gesamten hybriden Umgebung.

Reduzieren Sie proaktiv Risiken in Cloud-nativen Apps vom Code bis zur Cloud

Wehren Sie Cloud-Risiken schon vor der Produktion ab – mit IaC und kontinuierlichem Web-App-Scanning, das den Entwicklern in ihrem Arbeitsumfeld umsetzbares Feedback liefert.

Überwachen Sie den Zugriff und die Berechtigungen in all Ihren Clouds

Behalten Sie stets den Überblick über alle Konten und deren effektiven Zugriff im gesamten Unternehmen, wobei Rollen mit übermäßiger Berechtigung und potenzielle Rechteausweitungen gekennzeichnet werden und LPA-Richtlinien (Least Privilege Access) automatisch und in großem Umfang durchgesetzt werden.

Über Rapid7

Rapid7 schafft eine sicherere digitale Zukunft für alle, indem es Unternehmen dabei hilft, ihre Sicherheitsprogramme vor dem Hintergrund des sich beschleunigenden digitalen Wandels zu stärken. Unser Portfolio erstklassiger Lösungen versetzt Sicherheitsexperten in die Lage, Risiken zu managen und Bedrohungen über die gesamte Bedrohungslandschaft hinweg zu beseitigen – von Apps über die Cloud bis hin zur traditionellen Infrastruktur und dem Dark Web. Wir fördern Open-Source-Communities und innovative Forschung und nutzen diese Einblicke zur Optimierung unserer Produkte und zur Aufklärung der globalen Sicherheits-Community über die neuesten Angriffsmethoden. Weltweit vertrauen mehr als 11.000 Kunden auf unsere branchenführenden Lösungen und Services, mit denen sie Angreifern und der Konkurrenz immer einen Schritt voraus und für die Zukunft gerüstet sind.

RAPID7

PRODUKTE

Cloud Security
XDR & SIEM
Threat Intelligence
Schwachstellen-Risikomanagement
Anwendungssicherheit
Orchestrierung und Automatisierung
Managed Services

KONTAKTIEREN SIE UNS

rapid7.com/contact