RAPID7

LÖSUNGSÜBERSICHT

VISUALISIEREN SIE IHRE ANGRIFFSFLÄCHE INTERN WIE EXTERN

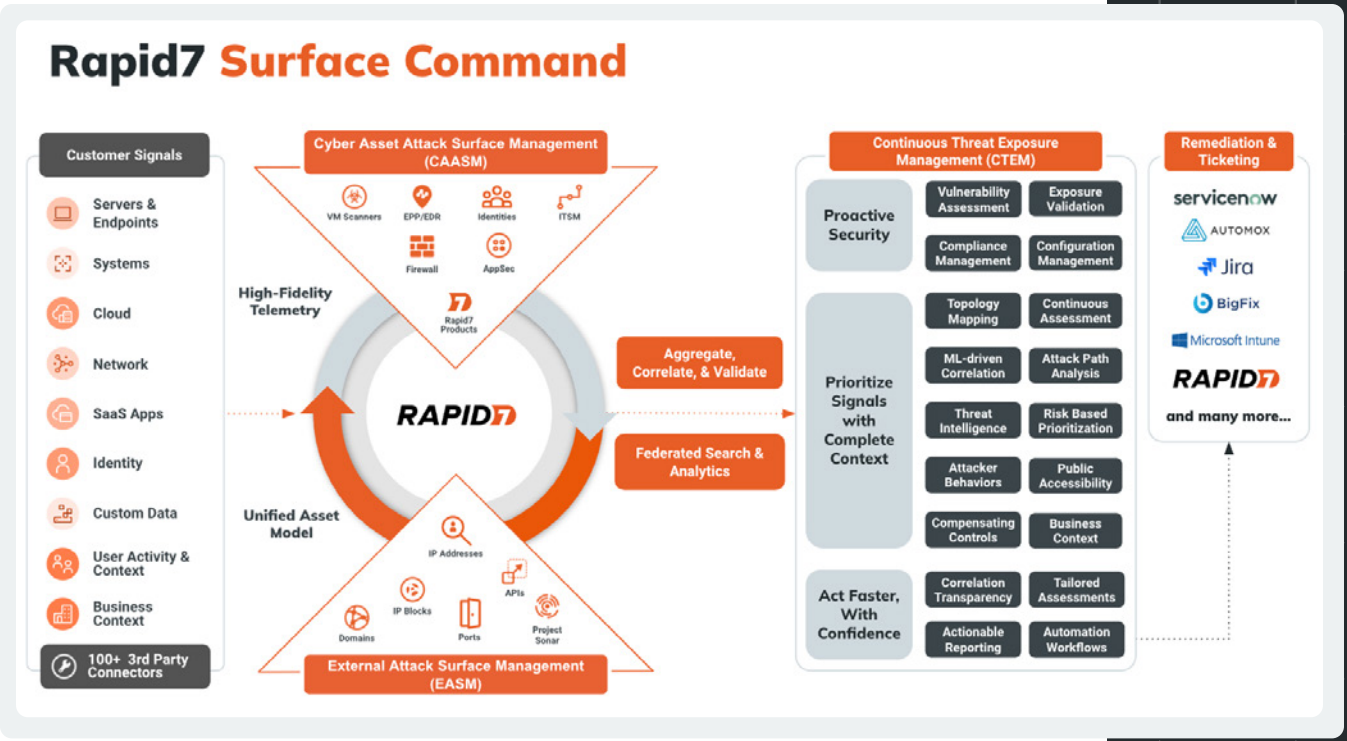
MIT RAPID7 SURFACE COMMAND

Surface Command kombiniert kontinuierliches externes Scannen mit dem internen Kontext von Assets vom Endpunkt bis zur Cloud

Unternehmen geben immer mehr Geld für Tools aus, um ihre Umgebungen zu verwalten und zu sichern, haben jedoch immer weniger Einblick in diese Tools. Dadurch entsteht eine weitläufige Angriffsfläche, die über interne, externe und hybride Umgebungen verteilt ist. Das ist ein klarer Vorteil für den Angreifer. Heute führen die wenigen Teams, die diese Situation tatsächlich im Griff haben, manuelle und umständliche Dateneingaben durch, um ihre Asset- und Sicherheitsdaten mithilfe von Tabellen zu korrelieren und Systeme zu identifizieren, bei denen Cybersecurity-Kontrollmechanismen fehlen, die noch nicht gepatcht wurden oder deren Compliance unzureichend ist. Cyberkriminelle können diesen Wildwuchs an Daten 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 Surface Command bricht Datensilos auf, indem es für umfassende Transparenz in hybriden Umgebungen sorgt und so eine dynamische 360-Grad-Ansicht Ihrer gesamten Angriffsfläche an einem Ort bietet. Mit externen Scans wird die Angriffsfläche aus der Perspektive eines Angreifers analysiert, wobei Schwachstellen erkannt und validiert werden und gleichzeitig Bereiche hervorgehoben werden können, bei denen die Wahrscheinlichkeit eines Angriffs besonders hoch ist. Surface Command kombiniert diese externen Scans mit einer detaillierten Bestandsaufnahme Ihrer internen Assets, unabhängig davon, mit welchem Sicherheits- oder IT-Tool sie gescannt werden. So erhalten Sie vollständige Transparenz über Ihre Angriffsfläche, und zwar ohne das Risiko von blinden Flecken, ungeschützten Assets und unkontrolliertem Zugriff. Dank dem Verständnis, wie Assets konfiguriert sind, können Sie Fehlkonfigurationen, Schatten-IT und Probleme mit der Compliance schnell erkennen und beheben. Dieser integrierte Ansatz bietet Ihnen einen ganzheitlichen Überblick über Ihre digitale Landschaft, sodass Sie Risiken proaktiv eindämmen, Bedrohungen vorbeugen und Angriffe schnell abwehren können.

> **Nur 17 % der Unternehmen können einen Großteil (mindestens 95 %) ihrer Assets eindeutig identifizieren und inventarisieren.“**
>
> **2024 Gartner® Innovation Insight:** Attack Surface Management report



Erstellen und unterhalten Sie eine zentrale Datenquelle für Ihre gesamte digitale Umgebung

Vereinheitlichen und korrelieren Sie Ihre Assets und Identitäten über all Ihre internen Tools hinweg. 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.

Förderung der Verantwortlichkeit in allen Teams

Klären Sie, wer für Assets verantwortlich ist, und sorgen Sie für mehr Verantwortlichkeit bei Verstößen gegen die Compliance. Dadurch erhalten Cybersecurity- und GRC-Teams Klarheit darüber, an welche Stakeholder sie sich bei erforderlichen Gegenmaßnahmen wenden müssen.

Bieten Sie Incident Respondern den vollständigen Kontext

Sicherheitsanalysten können laufende Bedrohungen wirksamer priorisieren, wenn sie den Kontext von Assets, Schwachstellen und Sicherheitskontrollen an einem Ort abrufen können. So können sie anhand von Informationen bekannter Assets und Taktiken, Techniken und Verfahren fundierte Entscheidungen treffen und unternehmensweites Threat Hunting ermöglichen.

Gleichen Sie die Ergebnisse mit regelmäßigen externen Scans ab, um die tatsächliche Angriffsfläche Ihres Unternehmens nachzuvollziehen.

Decken Sie Schatten-IT und die unkontrollierte Nutzung von IT-Ressourcen auf

Identifizieren Sie unbekannte Benutzer und Assets, die mit Ihrem Netzwerk verbunden sind, mit dem notwendigen Kontext, um das relative Risiko und die erforderlichen Abhilfemaßnahmen einschätzen zu können.

Optimieren Sie CMDB-Tools und unterstützen Sie das Asset-Lifecycle-Management

Erfassen Sie die Technologieakzeptanz in Ihrem Unternehmen und nutzen Sie leistungsstarke native Abfragefunktionen, um tiefgreifende Einblicke zu erhalten, z. B. welche Assets noch aktiv sind und wann sie zuletzt aktualisiert oder geändert wurden.

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