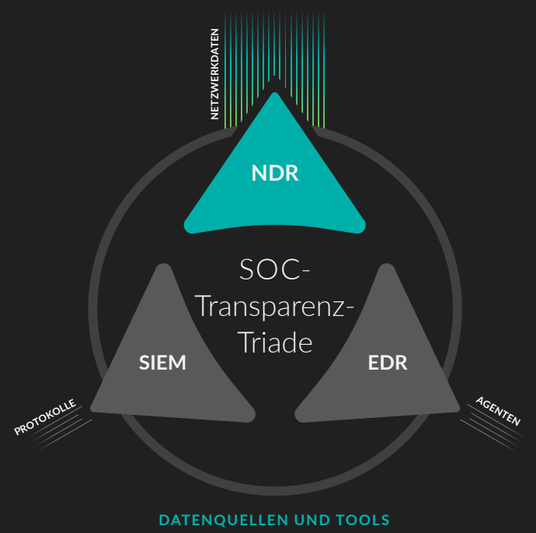
CLOUD-NATIVE NDR VERVOLLSTÄNDIGT SOC-TRANSPARENZ

Das fehlende Puzzleteil in den SOCs zahlreicher Unternehmen sind Netzwerkdaten. Network Detection and Response (NDR) liefert Erkenntnisse zu Netzwerkaktivitäten mit Kontextinformationen und kann selbst von cleveren Angreifern nicht deaktiviert oder umgangen werden, so wie dies bei protokoll- und agentenbasierten Tools der Fall ist. Deswegen ist das Netzwerk die beste Datenquelle für eine wahrlich cloud-native Herangehensweise an die Erkennung, Untersuchung und Abwehr von Bedrohungen in Hybridumgebungen.



VORTEILE FÜR KUNDEN

IDC

VOLLSTÄNDIGE TRANSPARENZ

95 %
schnellere Erkennung von Bedrohungen

BEDROHUNGSERKENNUNG IN ECHTZEIT

77 %
schnellere Klärung von Vorfällen

AUTOMATISIERTE UNTERSUCHUNGEN

59 %
geringerer Personalbedarf

DEMO STARTEN extrahop.com/demo

ÜBER EXTRAHOP NETWORKS

ExtraHop bietet cloud-native NDR-Tools für Hybridunternehmen. Unser innovativer Ansatz analysiert sämtliche Netzwerkinteraktionen und sorgt mittels Machine Learning für höchste Transparenz, Bedrohungserkennung in Echtzeit und automatische Prüfungen Ihrer Ressourcen in der Cloud. Wir sorgen für Einblicke statt Datenmüll in Form von unübersichtlichen Warnmeldungen, Abläufen und Technologien. Führende Unternehmen aus der ganzen Welt können dank ExtraHop Bedrohungen schneller erkennen, die Verfügbarkeit wichtiger Applikationen sicherstellen, ihre Cloud-Investitionen schützen und ihre Geschäftsabläufe erfolgreich beschleunigen.

ExtraHop
info@extrahop.com
www.extrahop.com

ExtraHop

Reveal(x) Cloud

In der Cloud kommt es auf Klarheit an. ExtraHop Reveal(x) Cloud ist eine cloud-native SaaS-Lösung für Network Detection and Response (NDR). Reveal(x) Cloud bietet SecOps-Teams höchst transparente Einblicke in ihre Cloud-Umgebungen, einschließlich Bedrohungserkennung in Echtzeit, zügiger Untersuchung von erkannten Risiken und automatisierter Reaktion.

VOLLSTÄNDIGE TRANSPARENZ

ExtraHop Reveal(x) Cloud sorgt für umfassende und kontinuierliche Transparenz von innen heraus und ermöglicht es SecOps-Teams, alle Daten, Transaktionen und Anwendungen genauestens zu überprüfen, um Cloud-Investitionen zu schützen. Ohne native Netzwerktransparenz in der Cloud müssen Unternehmen auf protokoll- oder agentengestützte Tools zurückgreifen, mit denen sich komplexe Bedrohungen nur schwierig zeitnah erkennen und untersuchen lassen.

BEDROHUNGSERKENNUNG IN ECHTZEIT

Als vollständig passive Lösung, die Datenpakete in Metadaten umwandelt, erlaubt es ExtraHop Reveal(x) Cloud, sämtliche Ressourcen zu durchsuchen. Durch die Kombination aus der automatisierten Erfassung und Klassifikation von Ressourcen mit der vollständigen Analyse aller Transaktionen und Machine Learning für die zuverlässige Bedrohungserkennung versetzt ExtraHop Reveal(x) Cloud Sicherheitsteams in die Lage, ihre Cloud-Ressourcen selbstständig zu überwachen und Risiken proaktiv abzuwehren.

AUTOMATISIERTE UNTERSUCHUNGEN

Reveal(x) Cloud führt Sie mit wenigen Klicks von einer Cloud-Sicherheitswarnung zum zugehörigen Datenpaket und erspart Ihnen langwierige Stunden des mühsamen Erfassens und Auswertens von Protokoll- und Agentendaten. Die native Integration mit AWS EC2, S3, Amazon CloudWatch, CloudTrail und Amazon VPC Flow Logs sowie Partnerschaften mit Orchestrierungs- und Ticketing-Plattformen wie ServiceNow und Phantom sorgen für drastisch schnellere Migrationen und Reaktionen.

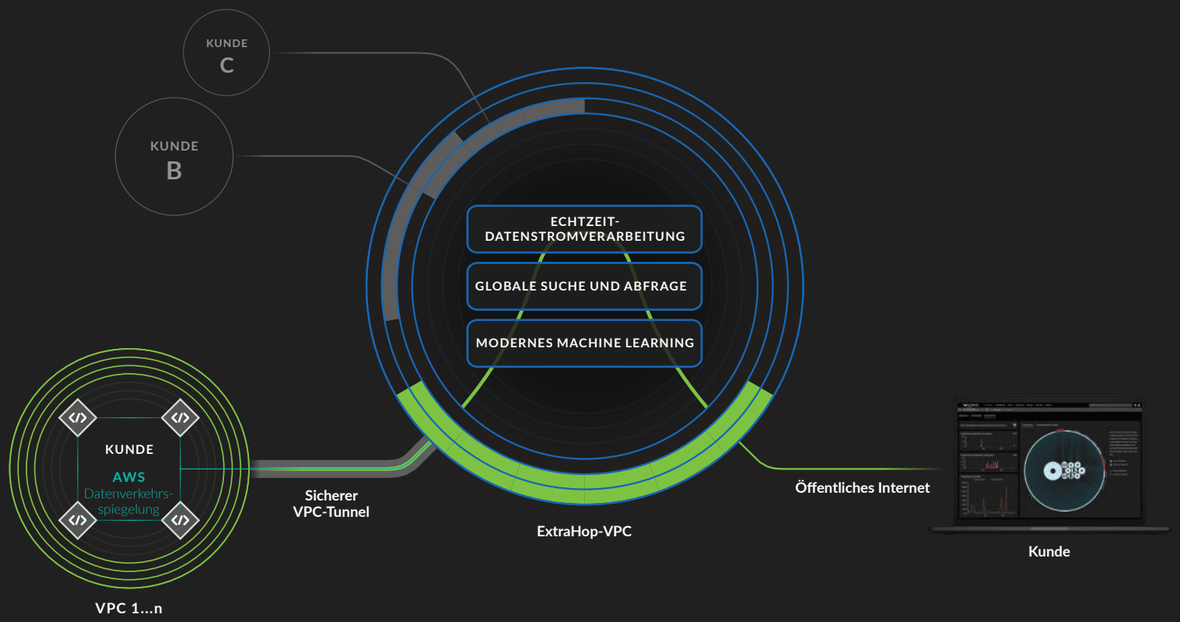
CLOUD-NATIVE SICHERHEIT FÜR HYBRIDUNTERNEHMEN

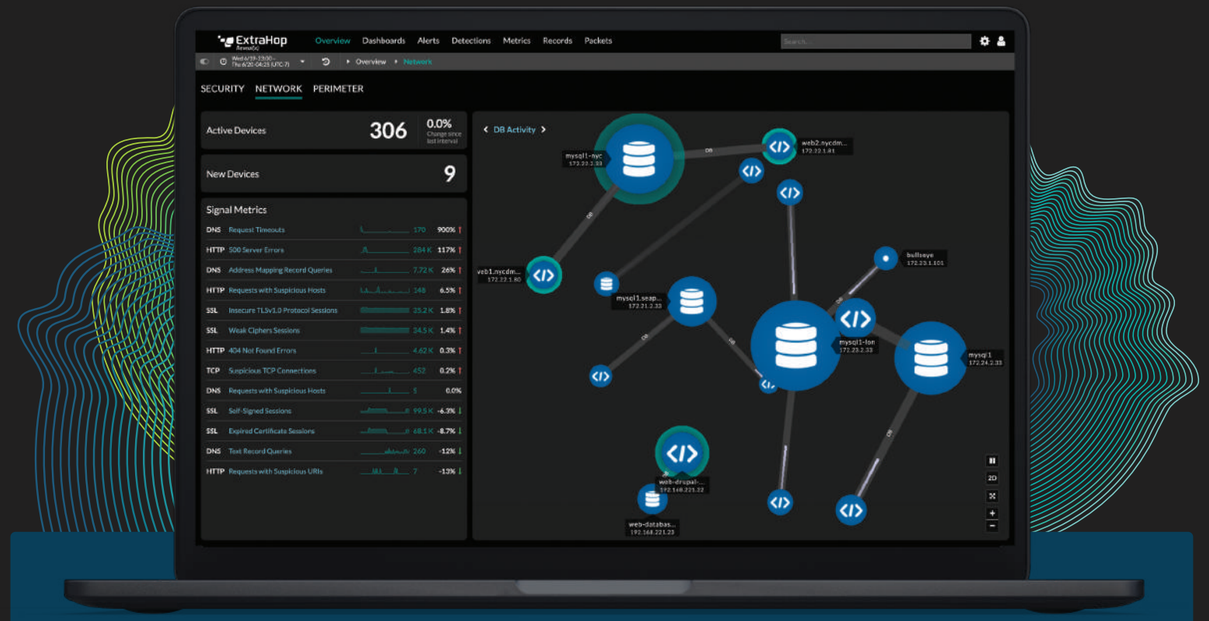
SaaS-basierte Erkennung und Abwehr von Bedrohungen

Die Cloud ist zweifelsohne ein mächtiges Tool für die IT- und Geschäftsabteilungen im Unternehmen. Sie bringt jedoch auch Hürden und Risiken mit sich. Vor allem Sicherheitsteams müssen nun eine noch größere Angriffsfläche sowie neue und unbekannte Risiken in den Griff bekommen. Trotz dieser Herausforderungen entscheiden sich viele Unternehmen aufgrund der Skalierbarkeit und Flexibilität für die Cloud. Einschränkungen von vorhandenen Sicherheitstools – die typischerweise auf Protokollen oder Agenten basieren – erschweren jedoch die zeitnahe Erkennung und Untersuchung komplexer Bedrohungen, da über die Virtual Private Clouds hinweg schlicht keine kontinuierliche Transparenz gegeben ist.

Dank ExtraHop Reveal(x) Cloud können Unternehmen nun ihre Hybridumgebung mit einem cloud-nativen Lösungsansatz sichern. Reveal(x) Cloud übernimmt die Erkennung, Analyse und Abwehr von Bedrohungen innerhalb des Netzwerkperimeters für sämtliche AWS-Workloads. So können SecOps-Teams auffällige Instanzen beobachten und Risiken eliminieren, die durch fehlerhafte Konfigurationen, unsichere APIs und unbefugte Zugriffe entstehen. ExtraHop Reveal(x) Cloud ist eine Saas-basierte Lösung, die unmittelbar und ohne Agenten bereitgestellt wird und sofort mit der Erfassung von Ressourcen, Bedrohungserkennung in Echtzeit und ML-basierten Abwehr beginnt.

Funktionsweise





FUNKTIONEN VON EXTRAHOP REVEAL(X) CLOUD

Kontrolle und Compliance
Durch Abgleich von bösartigen Aktivitäten mit der Wichtigkeit von Ressourcen werden zuverlässige Warnungen ausgegeben und Ihre Teams können sich auf die größten Bedrohungen konzentrieren.

Automatisierte Untersuchungen und Reaktionen
Bieten Sie nahtlose Sicheheitseinstellungen und behalten Sie den Überblick über Ihre Tools durch Integration in AWS CloudTrail, Amazon CloudWatch, VPC Flow Logs, Orchestrierungssysteme und mehr.

Decodierung von Protokollen auf der Applikationsebene
Analysieren und decodieren Sie Inhalte und Lasten von Cloud-Applikationen in jeder Skalierung.

In Cloud-Geschwindigkeit
Profitieren Sie von durchgängiger Transparenz für die Erkennung und Abwehr von Bedrohungen mit bis zu 25 Gbit/s je VPC.

Identity and Access Management
Analysieren Sie den Datenverkehr des Active Directory, um automatisch Anzeichen für Brute-Force-Angriffe und unbefugte Abfragen von Zugangsdaten hervorzuheben.

Skalierbare Entschlüsselung
Lassen Sie SSL/TLS passiv und in Echtzeit entschlüsseln, sodass Sie Ihre Compliance-Vorgaben erfüllen und verschlüsselte Bedrohungen vollständig offenlegen können.

ANWENDUNGSFÄLLE VON REVEAL(X) CLOUD

Sicherheitsteams können über eine einzige Plattform Workloads im Rechenzentrum und in der Cloud konsistent kontrollieren und ganzheitliche Bedrohungserkennungs- und Sicherheitsrichtlinien implementieren.

Erkennung von Angriffen

Darstellung von Abhängigkeiten

Bedrohungserkennung

Analyse von verschlüsseltem Datenverkehr

Compliance und Audit

Forensische Analysen

Bestand und Konfiguration

Schwachstellenanalyse

Bedrohungsabwehr

VORGESTELLTE INTEGRATIONEN

Amazon CloudTrail · Amazon CloudWatch · VPC Flow Logs · Radar · DEMISTO (A PALO ALTO NETWORKS COMPANY) · Phantom