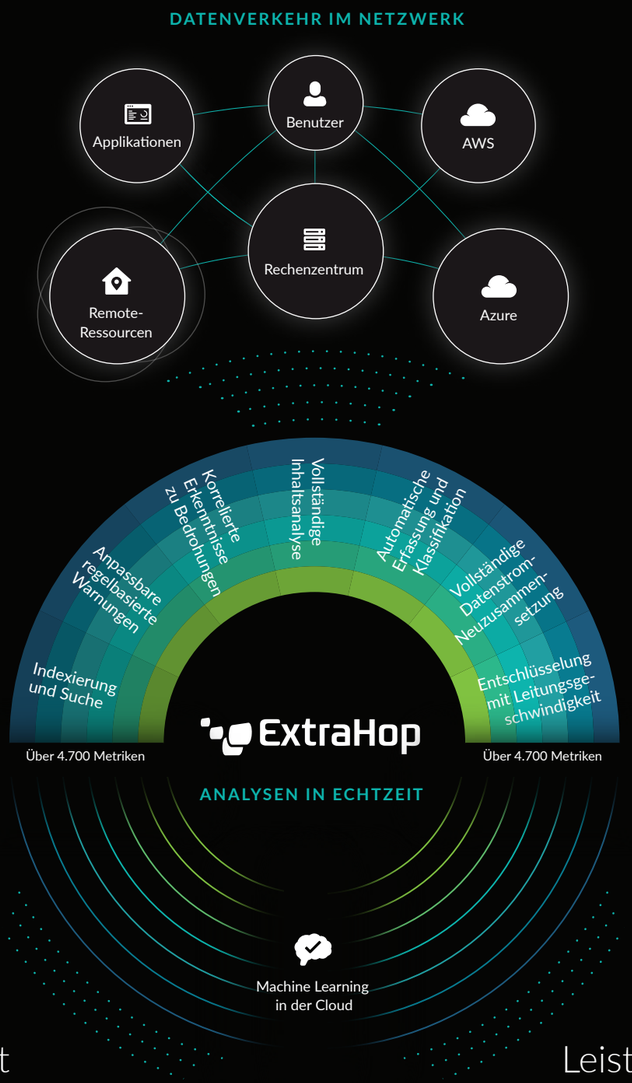


Sicherheit

Zuverlässige Bedrohungserkennung
Sicherheit und Compliance
Erfassung kritischer Ressourcen
1-Klick-Untersuchung von Bedrohungen
Automated Response via SOAR

GESCHÄFTSERGEBNISSE

Leistung

Anwendungsanalysen in Echtzeit
ML-gestützte Erkennung von Anomalien
Darstellung von Abhängigkeiten
Durchgängige Transparenz und Sicherheit
Automatisierte Untersuchungen

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
520 Pike Street, Suite 1600
Seattle, WA 98101, USA
+1 877 3339872 (Tel.)
+1 206 2746393 (Fax)
info@extrahop.com
www.extrahop.com

ExtraHop

ExtraHop Reveal(x)

Network Detection & Response für Hybridunternehmen

Reveal(x) bietet als einziges Tool zur Analyse des Netzwerk-Datenverkehrs die nötige Skalierbarkeit, Geschwindigkeit und Transparenz, mit der Sicherheitsteams in Unternehmen effizient auf Bedrohungen reagieren können und den Überblick über zunehmend komplexe hybride Netzwerkarchitekturen, Containerapplikationen und die Cloud behalten.

VOLLSTÄNDIGE TRANSPARENZ

Reveal(x) erfasst und klassifiziert automatisch jede Kommunikation zwischen Geräten im Netzwerk, und zwar mit Out-of-Band-Entschlüsselung in Echtzeit, sodass Sicherheitsteams versteckte Angreifer und wichtige Transaktionsdetails ohne Kompromisse bei der Compliance und beim Datenschutz einsehen können. Dank vollständiger Transparenz vom Rechenzentrum bis zur Cloud und zum Netzwerkrand haben Sie alle Ressourcen Ihres Unternehmens im Blick.

BEDROHUNGSERKENNUNG IN ECHTZEIT

Reveal(x) erkennt Bedrohungen in Echtzeit, indem über 4.700 Merkmale bei der Kommunikation durch Machine Learning in der Cloud und anpassbare regelbasierte Kontrollmechanismen geprüft werden. Reveal(x) identifiziert automatisch wichtige Ressourcen und vergleicht Peer-Gruppen, um Bedrohungen zuverlässiger zu erkennen, mit Risikobe-wertungen zu korrelieren und zusammen mit wichtigen Informationen darzustellen, damit Sie Ihre Gegenmaßnahmen priorisieren und zuversichtlich umsetzen können.

AUTOMATISIERTE UNTERSUCHUNGEN

Der Workflow von Reveal(x) führt Sie mit wenigen Klicks von einer Sicherheitswarnung bis zum zugehörigen Datenpaket und erspart Ihnen langwierige Stunden des mühsamen manuellen Erfassens und Auswertens von Daten. Stattdessen erhalten Sie sofort zuverlässige Antworten. Stabile Integrationen in Sicherheitstools wie Phantom, Splunk, Palo Alto und anderen helfen Ihnen, Datenmüll in Form von Warnungen zu vermeiden, nötige Untersuchungen zu automatisieren und die Daten Ihrer Kunden rechtzeitig zu schützen.

SCHLUSS MIT UNSICHERHEIT

Reveal(x) erkennt Bedrohungen in Echtzeit, zeigt Ihnen Details zu allen Phasen eines Angriffs und unterstützt Sie mit Anleitungen für weitere Schritte sowie mit Hinweisen auf Sicherheitsprogramme wie MITRE ATT&CK und die CIS Top 20. Mit diesen geballten Kontextinformationen erkennen Sie echte Bedrohungen bis zu 95 % schneller.

Command & Control	Reconnaissance	Sicherheitslücken	Laterale Aktivitäten	Aktivitäten mit Daten
Ausgehende Aktivitäten	Port-Scans	LLMNR Poisoning	Verdächtige RDP/SSH	Ransomware
Verdächtige IPs/URIs	Benutzeraufllistung	IP-Fragmentierung	Peer-Gruppen-Anomalien	Verschlüsselte Daten
Verdächtige Verbindungen	Anmeldeversuche	RDP Brute Force	Share- und Dateizugriff	Externe Datenübertragungen
Geolocation-Auffälligkeiten	Reverse DNS Lookups	Verdächtige CIFS	Transaktionsfehler	Entwendung von DB-Daten
Weitere erkannte Bedrohungen	Weitere erkannte Bedrohungen	Weitere erkannte Bedrohungen	Weitere erkannte Bedrohungen	Weitere erkannte Bedrohungen

PROAKTIVE SICHERHEIT – ANWENDUNGSFÄLLE

ERKENNUNG VON BEDROHUNGEN

Erkennung und Abwehr von Angriffen
Sie können Bedrohungen erkennen und Reaktionen verstärken oder automatisieren.

Hybride Sicherheit
Die Erkennung und Abwehr von Bedrohungen erfolgt für Cloud und Rechenzentrum einheitlich.

Erkennung von Insider-Bedrohungen
Sie können riskantes und verdächtiges Verhalten erkennen, einschränken und dokumentieren.

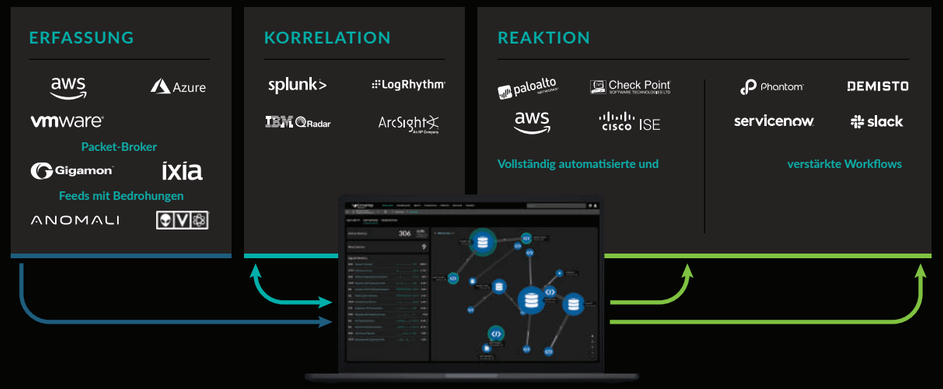
VERBESSERUNG DER SICHERHEIT

Produktivität von SOC + NOC
Durch Datenaustausch und integrierte Tools wird die Leistung Ihrer Teams optimiert.

Red Team/Audit-Ergebnisse
Potenzielle Sicherheitslücken und Schwachstellen werden erkannt und geprüft.

Sicherheitsvorkehrungen
Geräte werden erfasst, Verschlüsselungsmechanismen geprüft und riskante Ressourcen ausgemustert.

STÄRKUNG IHRER UNTERNEHMENSTOOLS



Die Integration in weitere Sicherheitstools für Unternehmen erleichtert die beschleunigte und automatisierte Reaktion auf erkannte Bedrohungen. So kann Ihr Team die nötige Zeit zur Klärung von Zwischenfällen um 59 % verkürzen.
Alle Integrationen finden Sie unter:
www.extrahop.com/platform/integrations

FUNKTIONEN VON EXTRAHOP REVEAL(X)

Automatisierte Bestandserfassung
Reveal(x) führt eine stets aktuelle Bestandsliste durch automatische Erfassung und Klassifikation aller kommunizierenden Ressourcen im Netzwerk.

PFS-Entschlüsselung
Reveal(x) entschlüsselt SSL/TLS 1.3 mit PFS passiv und in Echtzeit und warnt Sie rechtzeitig vor versteckten Bedrohungen in Ihrem eigenen Datenverkehr.

Automatisierte Untersuchungen
Reveal(x) ergänzt jede erkannte Bedrohung durch Kontext, Risikobewertungen, Hintergrundinformationen und empfohlene weitere Schritte für wirkungsvolle Gegenmaßnahmen.

Abgleich mit Peer-Gruppen
Durch automatische Einteilung von Geräten in präzise Peer-Gruppen erkennt Reveal(x) auffälliges Verhalten mit nur wenigen falsch positiven Meldungen.

Machine Learning in der Cloud
Dank Machine Learning in der Cloud und prädiktiver Modellierung mit über 4.700 Merkmalen kann Reveal(x) Bedrohungen Ihrer wichtigsten Ressourcen erkennen, priorisieren und kontextbezogen analysieren.

Überzeugende Orchestrierung Ihrer Reaktion
Reveal(x) übernimmt die Erkennung und Untersuchung von Bedrohungen, während die leistungsstarke Integration in Lösungen wie Phantom und Palo Alto verstärkte und automatisierte Gegenmaßnahmen ermöglicht.

EINBLICKE STATT DATENMÜLL FÜR UNSERE KUNDEN

IDC

95 % SCHNELLERE ERKENNUNG VON BEDROHUNGEN

77 % SCHNELLERE KLÄRUNG VON VORFÄLLEN

59 % GERINGERER PERSONALBEDARF

25 % MEHR SICHERHEITS-BEDROHUNGEN ERFOLGREICH ERKANNT