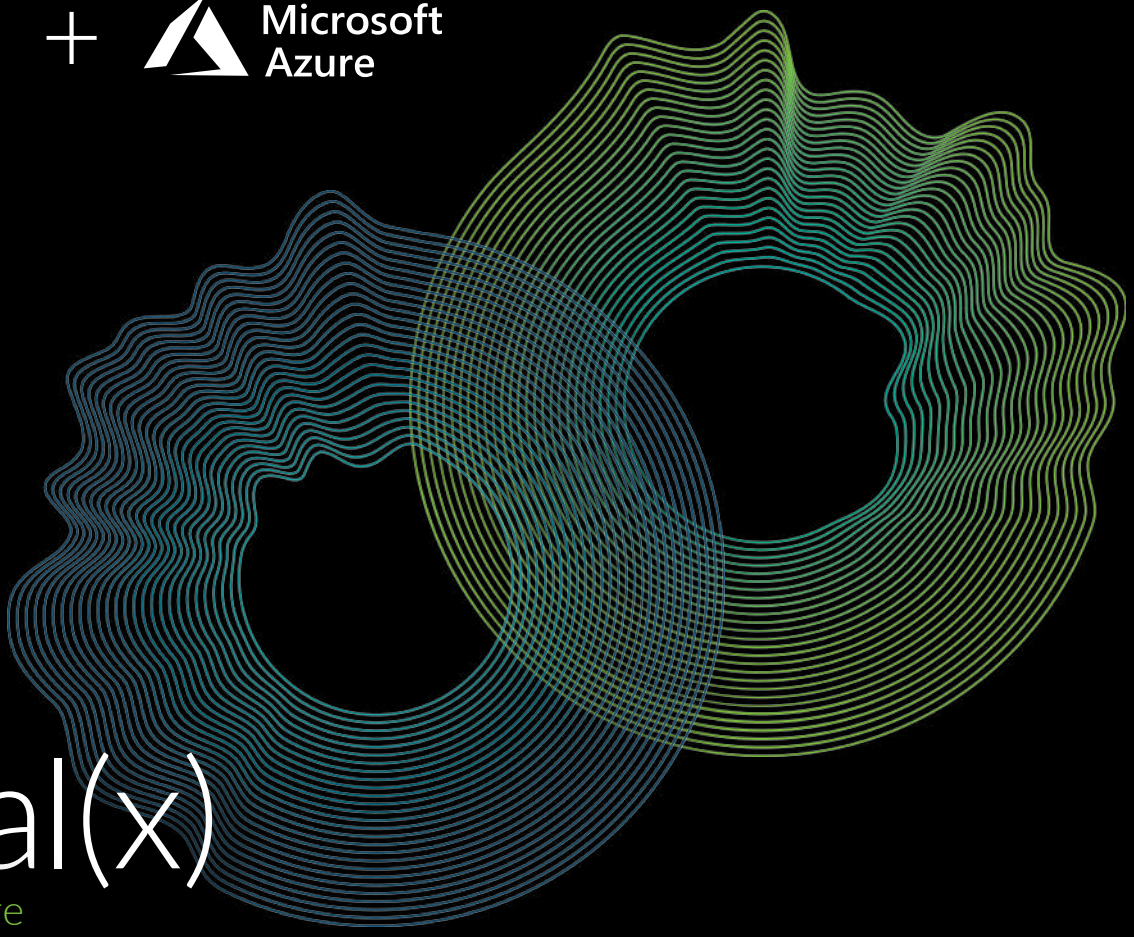
ExtraHop + Microsoft Azure



Reveal(x)

für Microsoft Azure

Schützen Sie Applikationen und Daten in Ihrer Umgebung mit Microsoft Azure durch eine cloud-native Lösung für Network Detection & Response (NDR).

SCHUTZ IHRER INVESTITION IN DIE AZURE CLOUD

Immer häufiger verschieben Unternehmen ihre geschäftskritischen Anwendungen in die Cloud, um sich die bessere Skalierbarkeit und Effizienz zunutze zu machen. Damit steigt aber der Druck auf das unternehmenseigene Security Operations Center (SOC), das nun auch in der Cloud-Umgebung für die nötige Sicherheit sorgen muss.

ExtraHop Reveal(x) für Azure bietet innerhalb des Netzwerkperimeters die nötige Transparenz und Funktionalität zur Erkennung, Untersuchung und Abwehr von Bedrohungen, damit Sie Ihre Applikationen und Daten in Ihrer gesamten hybriden Umgebung zuverlässig sichern können.

Erkennung von Cloud-Bedrohungen

ExtraHop Reveal(x) für Azure bekämpft die drei wichtigsten Arten von Bedrohungen in Cloud-Umgebungen: Fehlkonfigurationen, unbefugte Zugriffe und unsichere APIs. Reveal(x) kombiniert umfassende Inhaltsanalysen und Transaktionsdetails mit Ereignisdaten des Azure Security Center, um relevante Vorfälle zu identifizieren, einschließlich auffälligen Instanzen, deaktivierten Protokollsystemen und verdächtigen Dateiausführungen. ExtraHop Reveal(x) für Azure erkennt und klassifiziert sämtliche Datenaktivitäten in Ihrer Netzwerkumgebung.

Aussagekräftige Transaktionsdaten

ExtraHop konvertiert als einziger Anbieter sämtliche Kommunikationsdaten in ein vollständig indexiertes Protokoll mit Details zu allen Elementen aller Transaktionen. In diesem Umfang waren empirische Daten bisher nie zugänglich. Unsere sachlichen und kontextbezogenen Datensätze sind größer und aussagekräftiger als je zuvor und liefern Ihren Sicherheitsteams die Antworten auf alle wichtigen Fragen. Keine andere Datenquelle bietet annähernd so detaillierte und wertvolle Daten wie ExtraHop.

Gemeinsame Verantwortung

Keine andere Plattform liefert die nötige Transparenz, um eigene Pflichten im Rahmen gemeinsamer Verantwortungsmodelle effektiv wahrzunehmen und Sicherheitsressourcen (SOC-Analysten, Infrastruktur) basierend auf kritischen Daten und Risiken angemessen zu priorisieren. Cloud-Dienstleister nutzen Ansätze mit gemeinsamer Verantwortung, bei denen die Gewährleistung der Sicherheit weitestgehend dem Unternehmen überlassen wird. Reveal(x) für Azure erleichtert es SecOps-Teams, ihren Verpflichtungen zuverlässig nachzukommen.

FUNKTIONSWEISE

Reveal(x) macht sich Microsoft Azure Virtual Network Tap (vTAP) zunutze und kombiniert die Echtzeitanalyse des Netzwerk-Datenverkehrs mit Sicherheitsmeldungen des Azure Security Center, sodass Analysten alle nötigen Informationen für wirkungsvolle Reaktionen besitzen.

WICHTIGE FUNKTIONEN

Reveal(x) kombiniert die Analyse des Netzwerk-Datenverkehrs mit Sicherheitsmeldungen des Azure Security Center und bietet Analysten damit alle nötigen Informationen für wirkungsvolle Gegenmaßnahmen.

- **Out-of-Band-Entschlüsselung**
  Entschlüsseln und analysiere Sie sämtlichen Datenverkehr mit SSL/TLS 1.3 ohne Verzögerungen.
- **Transaktionsdecodierung**
  Reveal(x) decodiert über 70 Protokolle zugunsten einer schnelleren Erkennung, Analyse und Abwehr von Bedrohungen
- **Machine Learning in der Cloud**
  Über 5.000 extrahierte Kommunikationsmerkmale stehen für die Analyse von Verhaltensmustern bereit.

VOLLSTÄNDIGE TRANSPARENZ

Erfassen und verarbeiten Sie Ihre Netzwerkdaten in Echtzeit und auf Unternehmensmaßstab ohne Einbußen der Analysegenauigkeit: alle Transaktionen, alle Workloads, überall und jederzeit.

NAHTLOSE BEREITSTELLUNG

Durch die automatische Bereitstellung in neuen Cloud-Umgebungen via Azure vTAP beginnt Reveal(x) sofort mit der Überwachung und Identifizierung von Bedrohungen – schon nach einer Sekunde!

ÜBER EXTRAHOP NETWORKS

ExtraHop bietet cloud-native NDR-Tools für Hybridunternehmen. Durch vollständige Transparenz, Bedrohungserkennung in Echtzeit und automatisierte Untersuchungen mittels Machine Learning in der Cloud unterstützt ExtraHop Sicherheitsteams führender Unternehmen wie Credit Suisse, The Home Depot, Caesars Entertainment und Liberty Global. Lassen auch Sie unübersichtliche Warnmeldungen, Abläufe und Technologien hinter sich und profitieren Sie stattdessen von schnelleren Bedrohungsanalysen, einheitlichen Richtlinien in hybriden Umgebungen und einer Sicherheitsinfrastruktur, die perfekt auf die Cloud zugeschnitten ist. Überzeugen Sie sich selbst von der Leistungsfähigkeit von ExtraHop und sehen Sie sich unsere interaktive Online-Demoversion an: www.extrahop.com/demo.

© 2019 ExtraHop Networks, Inc. Alle Rechte vorbehalten. ExtraHop ist eine eingetragene Marke von ExtraHop Networks, Inc. in den Vereinigten Staaten und/oder anderen Ländern. Alle anderen Produktbezeichnungen sind Marken der jeweiligen Rechtsinhaber.

ExtraHop

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