Einführung in das ExtraHop-System

Veröffentlicht: 2025-02-04

In diesem Handbuch wird erklärt, wie das ExtraHop-System Ihre Daten sammelt und analysiert und wie die Kernsystemkomponenten und -funktionen Ihnen helfen, auf Erkennungen, Metriken, Transaktionen und Pakete über den Verkehr in Ihrem Netzwerk zuzugreifen.

Mithilfe von Workflows zur Überwachung der Netzwerkleistung können Sie überwachen, wie Dienste und Geräte miteinander interagieren und wie Transaktionen in Ihrem Netzwerk über die Datenverbindungsschicht (L2) zur Anwendungsebene (L7) Fluss. Mithilfe von Workflows zur Netzwerkerkennung und Reaktion können Sie Daten untersuchen, die aufgrund von Leistungseinbußen bis hin zu verdächtigen Verhaltensweisen erkannt wurden. Außerdem erhalten Sie einen Überblick darüber, welche Geräte an den MITRE ATT&CK-Taktiken, -Techniken und -Verfahren (TTPs) beteiligt waren, die mit fortgeschrittenen, mehrstufigen Angriffskampagnen in Verbindung stehen.

Video: Sehen Sie sich die entsprechende Schulung an: ExtraHop Systemübersicht

Plattform-Architektur

Das ExtraHop-System ist mit modularen Komponenten maßgeschneidert, die in Kombination Ihren individuellen Umweltanforderungen gerecht werden.

Module

ExtraHop-Module bieten eine Kombination aus Lösungen, Komponenten und Cloud-basierten Diensten, die für mehrere Anwendungsfälle einen Mehrwert bieten.

Module sind für Network Detection and Response (NDR) und Network Performance Monitoring (NPM) erhältlich, mit zusätzlichen Modulen für Intrusion Detection Systems (Intrusion Detection System) und Packet Forensics.

Administratoren können die rollenbasierte Zugriffskontrolle (RBAC) aktivieren, indem sie Benutzern Zugriff auf das NDR-Modul, das NPM-Modul oder beides gewähren.

Überwachung der Netzwerkleistung

Mit dem NPM-Modul können privilegierte Benutzer die folgenden Arten von Systemaufgaben ausführen.

- Wählen Sie ein Dashboard als Standard-Landingpage aus.
- Konfigurieren Sie Benachrichtigungen und Benachrichtigungen per E-Mail für diese Warnungen.
- Leistungserkennungen anzeigen.

Netzwerkerkennung und Reaktion

Mit dem NDR-Modul können privilegierte Benutzer die folgenden Arten von Systemaufgaben ausführen.

- Sehen Sie sich die Seite mit der Sicherheitsübersicht an.
- Sehen Sie sich Sicherheitserkennungen an.
- Untersuchungen anzeigen, erstellen und ändern.
- Bedrohungsinformationen anzeigen.

Benutzer, denen Zugriff auf beide Module gewährt wurde, dürfen alle diese Aufgaben ausführen. Sehen Sie die Leitfaden zur Migration um mehr über die Migration von Benutzern zum rollenbasierten Zugriff mit diesen Modulen zu erfahren.

Diese zusätzlichen Module sind auch für bestimmte Anwendungsfälle verfügbar:

Paket-Forensik

Das Packet Forensics Modul kann entweder mit dem NDR- oder NPM-Modul kombiniert werden, um eine vollständige PCAP, Speicherung und Abruf zu ermöglichen.

Systeme zur Erkennung von Eindringlingen

Das IDS-Modul muss mit dem NDR-Modul kombiniert werden und bietet Erkennungen auf der Grundlage von IDS-Signaturen nach Industriestandard. Die meisten ExtraHop-Paketsensoren sind für das IDS-Modul geeignet, sofern der Sensor für das NDR-Modul lizenziert ist.

Hinweis: Durchsatz kann beeinträchtigt werden, wenn mehr als ein Modul auf dem Sensor aktiviert ist.

Funktionen

Das ExtraHop-System bietet einen umfangreichen Funktionsumfang, mit dem Sie Erkennungen, Metriken, Aufzeichnungen und Pakete organisieren und analysieren können, die mit dem Verkehr in Ihrem Netzwerk verbunden sind.

Modul- und Systemzugriff werden bestimmt durch Benutzerrechte die von Ihrem ExtraHop-Administrator verwaltet werden.

Globale Funktionen

Die folgenden Funktionen sind in allen ExtraHop-Systemen verfügbar und erfordern keine speziellen Module.

- Überblick über das Netzwerk
- Perimeter im Überblick
- Benutzerdefinierte Dashboards
- Karten der Aktivitäten
- Active Directory Directory-Dashboard
- Generatives KI-Dashboard
- Geplante Dashboard-Berichte
- Erkennungsverfolgung
- Vermögenswerte
- Rekorde
- Pakete
- Integrationen (nur RevealX 360)
- API-Zugriff
- Prioritäten der Analyse
- Metrischer Katalog
- Bündel
- Trigger
- KI-Suchassistent (Vermögenswerte und Aufzeichnungen)

Funktionen des NDR-Moduls

Die folgenden Funktionen sind in ExtraHop-Systemen mit dem Network Detection and Response (NDR) -Modul verfügbar.

- Überblick über die Sicherheit
- KI-Suchassistent
- Berichte über Sicherheitsoperationen
- Integrierte Sicherheits-Dashboards
- Sicherheitserkennungen
- MITRE karte

- Ermittlungen
- Optimierungsregeln für Sicherheitserkennungen
- Benachrichtigungsregeln für Sicherheitserkennungen und Bedrohungsinformationen
- Bedrohungsinformationen
- Bedrohungsinformationen
- Datei-Analyse
- Dateiextraktion (Paketforensik erforderlich)

Funktionen des NPM-Moduls

Die folgenden Funktionen sind in ExtraHop-Systemen mit dem Network Performance Management (NPM) -Modul verfügbar.

- Integrierte Leistungs-Dashboards
- Leistungserkennungen
- Optimierungsregeln für Leistungserkennungen
- Benachrichtigungsregeln für Leistungserkennungen
- Warnmeldungen

Funktionen von Packet Forensics

Die folgenden Funktionen sind in ExtraHop-Systemen mit dem Modul Packet Forensics verfügbar.

- Paketerfassung
- Packetstore-Unterstützung
- Dateiextraktion (NDR erforderlich)

IDS-Funktionen

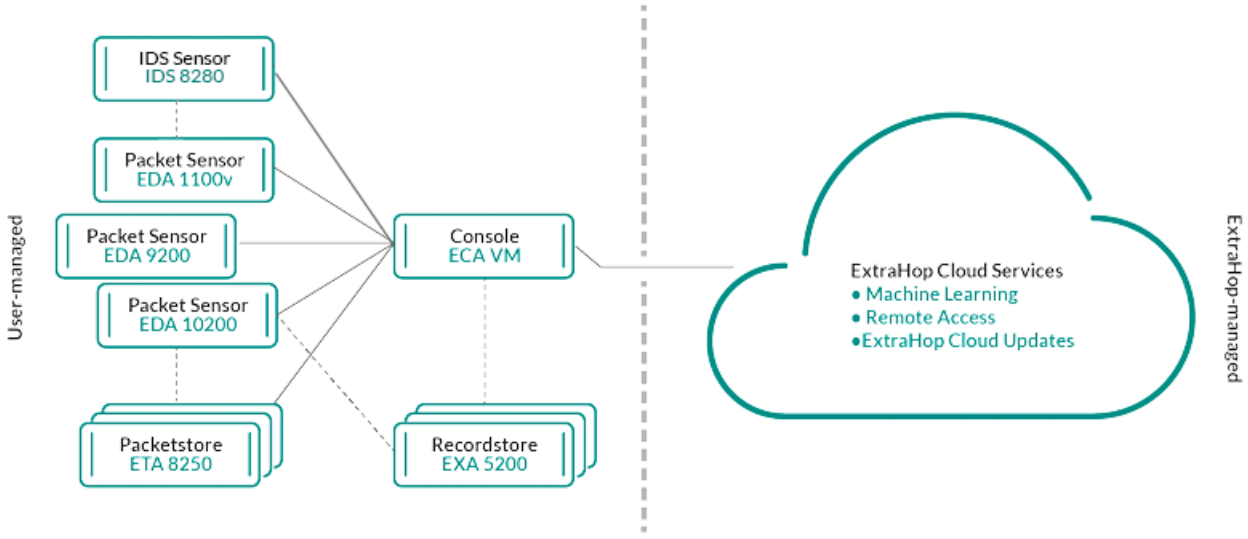
Die folgenden Funktionen sind in ExtraHop-Systemen mit dem Modul Intrusion Detection System (IDS) verfügbar.

- IDS-Erkennungen

Lösungen

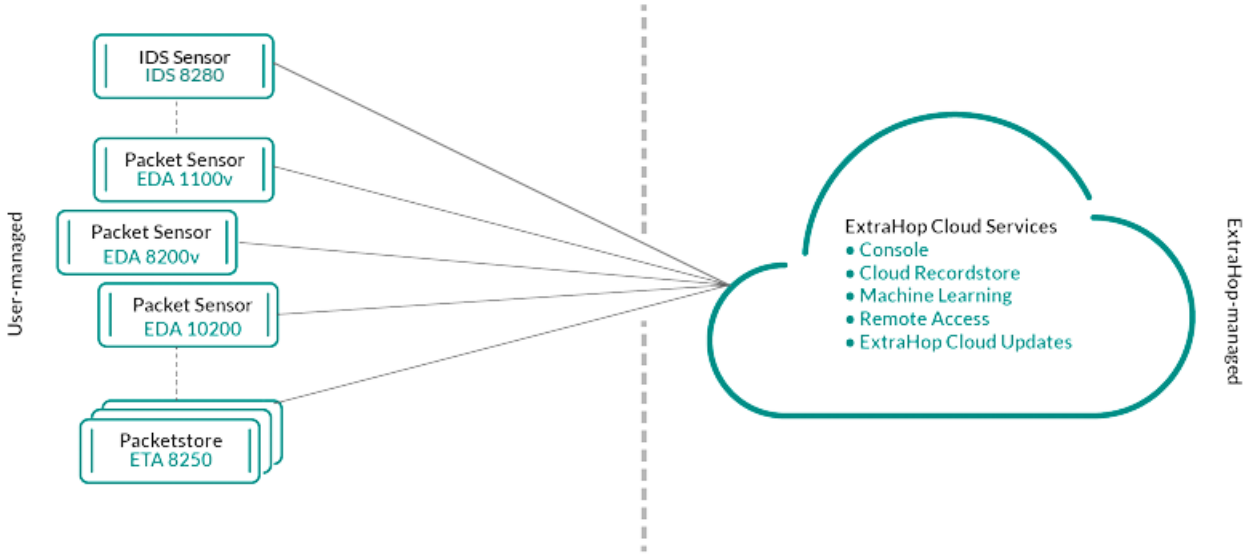
RevealX Enterprise

RevealX Enterprise ist eine selbstverwaltete Lösung, die Folgendes umfasst Sensoren, Konsolen, Paketspeicher, Plattenspeicher und Zugriff auf ExtraHop Cloud Services.



RevealX 360

RevealX 360 ist eine Software-as-a-Service (SaaS) -Lösung, die umfasst Sensoren und Paketspeicher und beinhaltet einen Cloud-basierten Recordstore mit Standard Investigation, einem Konsoleund Zugriff auf ExtraHop Cloud Services.



Komponenten

Jede Lösung bietet eine Reihe von Komponenten, die auf Ihre Umgebungsanforderungen zugeschnitten sind: Sensoren, Paketspeicher, Plattenspeicher und ein Konsole für zentralisiertes Management und einheitliche Datenansichten.

Paket-Sensoren

Paketsensoren erfassen, speichern und analysieren Metrik Daten über Ihr Netzwerk. Je nach Sensorgröße sind mehrere Ebenen der Datenanalyse, -erfassung und -speicherung verfügbar. Diese Sensoren sind sowohl in NPM- als auch in NDR-Modulen als physische, virtuelle und cloudbasierte Optionen in Größen erhältlich, die auf Ihre Analyseanforderungen zugeschnitten sind.

IDS-Sensoren

Die Sensoren des Intrusion Detection Systems (Intrusion Detection System) sind in Paketsensoren integriert, um Erkennungen auf der Grundlage der branchenüblichen IDS-Signatur zu generieren.

IDS-Sensoren werden als Zusatzmodul zum NDR-Modul eingesetzt. IDS-Sensoren sind eine physische Appliance mit einem zugehörigen Paketsensor und sind für RevealX 360- oder RevealX Enterprise-Umgebungen verfügbar.

Durchflusssensoren

Flusssensoren sind nur für RevealX 360 verfügbar und erfassen ausschließlich VPC-Flow-Logs, sodass Sie den von AWS-SaaS-Diensten verwalteten Datenverkehr sehen können.

Plattenläden

Recordstores lassen sich in Sensoren integrieren und Konsolen zu Transaktions- und Flow-Aufzeichnungen speichern das kann im gesamten ExtraHop-System abgefragt werden. Recordstores können als eigenständige physische oder virtuelle Optionen bereitgestellt und als Drittanbieter-Verbindungen zu Splunk oder BiqQuery von RevealX Enterprise unterstützt werden. RevealX 360 mit Standard Investigation bietet einen vollständig gehosteten, cloudbasierten Recordstore. Recordstores sind in Paketen mit NPM- und NDR-Modulen erhältlich.

Paketshops

Packetstores integrieren sich in Sensoren und Konsolen zur Verfügung stellen kontinuierliche PCAP und ausreichend Speicherplatz für eingehendere Untersuchungen und forensische Anforderungen. Packetstores können als eigenständige physische oder virtuelle Optionen bereitgestellt werden und sind als Zusatzmodul für Paketforensik sowohl für NPM- als auch für NDR-Module verfügbar.

Konsolen

Konsolen bieten eine browserbasierte Oberfläche, die eine Kommandozentrale für alle verbundenen Komponenten bietet. Konsolen können als eigenständige virtuelle oder cloudbasierte Optionen für RevealX Enterprise bereitgestellt werden und sind in RevealX 360 enthalten.

Die folgende Tabelle bietet einen Überblick über die für jede Lösung verfügbaren Optionen.

	RevealX Enterprise		**RevealX 360**	
	Körperlich	Virtuell/Cloud	Körperlich	Virtuell/Cloud
Paketsensor				
	SEIT 1200	EDA 1100 V AWS	SEIT 1200	EDA 1100 V AWS
	SEIT 6200	EDA 1100v Azurblau	SEIT 6200	EDA 1100v Azurblau
	AB 820	EDA 1100 V GCP	AB 820	EDA 1100 V GCP
	SEIT 8320	EDA 6320v GCP	SEIT 8320	EDA 6320v GCP
	SEIT 9200	EDA 8370v GCP	SEIT 9200	EDA 8370v GCP
	SEIT 9300	EDA 1100 V Linux KVM	SEIT 9300	EDA 1100 V Linux KVM
	VON 10200	EDA 1100 v VMware	VON 10200	EDA 1100 v VMware
	VON 10300	EDA 6100 v VMware	VON 10300	EDA 610 V AWS

	RevealX Enterprise		RevealX 360	
		EDA 610 V AWS		EDA 6100v Azurblau
		EDA 6100v Azurblau		EDA 6100 v VMware
		EDA 820 V AWS		EDA 820 V AWS
		RevealX Ultra AWS mit 1 Gbit/s und 10 Gbit/s		RevealX Ultra AWS mit 1 Gbit/s und 10 Gbit/s
		RevealX Ultra 1 Gbit/s und 10 Gbit/s GCP		RevealX Ultra 1 Gbit/s und 10 Gbit/s GCP
IDS-Sensor				
	Intrusion Detection System 8280	Intrusion Detection System 1280 v VMware	Intrusion Detection System 8280	Intrusion Detection System 1280 v VMware
	Intrusion Detection System 980	Intrusion Detection System 6280v VMWare	Intrusion Detection System 980	Intrusion Detection System 6280v VMWare
Durchflusssensor	N/A	N/A	N/A	
				EFC 1291v AWS (PVC)
				EFC 1292v (NetFlow)
Paketspeicher				
	BETA 6150	ETA 1150v AWS	BETA 6150	ETA 1150v AWS
	BETA 8250	ETA 1150v Azurblau	BETA 8250	ETA 1150v Azurblau
		ETA 1150 V GCP		ETA 1150 V GCP
		ETA 1150v VMware		ETA 1150v VMware
		ETA 6150v VMware		ETA 6150v VMware

	RevealX Enterprise		RevealX 360	
				In Ultra-Abonnements enthalten
Plattenladen	EXA 5200	EXA 5100 v AWS EXA 5100v Azurblau EXA 5100v Hyper-V EXA 5100v Linux KVM EXA 5100 v VMware	N/A	In Premium- und Ultra-Abonnements enthalten
Konsole	N/A	ECA-GESETZE ECA Azure ECA GCP ECA Hyper-V ECA Linux KVM ECA VMWare	N/A	In allen Abos enthalten

ExtraHop Cloud-Dienste

ExtraHop Cloud-Dienste aktualisiert die Sensoren automatisch mit neuen Erkennungen und kritischen Bedrohungsinformationen sowie mit Funktionserweiterungen und ermöglicht Ihren Account-Teams den Zugriff auf Fernsupport und professionelle Services.

Intelligente Sensoranalytik

Das ExtraHop-System bietet eine browserbasierte Oberfläche mit Tools, mit denen Sie Daten untersuchen und visualisieren, Ergebnisse sowohl in Top-down- als auch Bottom-up-Workflows untersuchen und anpassen können, wie Sie Ihre Netzwerkdaten sammeln, anzeigen und teilen. Fortgeschrittene Benutzer können sowohl administrative als auch Benutzeraufgaben über das automatisieren und skripten ExtraHop REST-API und passen Sie die Datenerfassung an über ExtraHop-Trigger-API, bei dem es sich um ein JavaScript-IDE-Tool handelt.

Das Herzstück des ExtraHop-Systems ist ein intelligentes Sensor das Metrikdaten über Ihr Netzwerk erfasst, speichert und analysiert — und je nach Bedarf verschiedene Ebenen der Datenanalyse, -erfassung und -speicherung bietet. Fühler sind mit Speicher ausgestattet, der ein Metrik-Lookback von 30 Tagen unterstützt. Beachten Sie, dass der tatsächliche Lookback je nach Verkehrsmustern, Transaktionsraten, der Anzahl der Endpunkte und der Anzahl der aktiven Protokolle variiert.

Konsolen dienen als Kommandozentrale mit Verbindungen zu mehreren Sensoren, Recordstores und Packetstores, die über Rechenzentren und Zweigstellen verteilt sind. Alle RevealX 360-Bereitstellungen enthalten eine Konsole; RevealX Enterprise kann virtuelle oder Cloud-Varianten bereitstellen.

Konsolen bieten einheitliche Datenansichten für alle Ihre Standorte und ermöglichen es Ihnen, bestimmte erweiterte Konfigurationen zu synchronisieren (z. B. löst aus und Warnungen) und Einstellungen (Tuning-Parameter, Analyse-Prioritäten, und Plattenläden).

In den folgenden Abschnitten werden die wichtigsten Funktionskomponenten des ExtraHop-Systems und deren Zusammenspiel beschrieben.

Sensortypen

Die Art von Sensor Die Art der Daten, die Sie bereitstellen, bestimmt die Art der Daten, die gesammelt, gespeichert und analysiert werden.

Daten verdrahten

Paketsensoren und Intrusion Detection System (IDS) -Sensoren beobachten unstrukturierte Pakete passiv über einen Port-Mirror oder greifen auf die Daten zu und speichern sie im lokalen Datenspeicher. Die Paketdaten werden einer Stream-Verarbeitung in Echtzeit unterzogen, bei der die Pakete in die folgenden Phasen in strukturierte wire data umgewandelt werden:

1. TCP-Zustandsmaschinen werden neu erstellt, um eine vollständige Reassemblierung durchzuführen.
2. Pakete werden gesammelt und in Flows gruppiert.
3. Die strukturierten Daten werden auf folgende Weise analysiert und verarbeitet:
   - Transaktionen werden identifiziert.
   - Geräte werden automatisch erkannt und anhand ihrer Aktivität klassifiziert.
   - Metriken werden generiert und mit Protokollen und Quellen verknüpft, und die Metrikdaten werden dann in Metrikzyklen aggregiert.
4. Wenn neue Metriken generiert und gespeichert werden und der Datenspeicher voll wird, werden die ältesten vorhandenen Metriken gemäß dem First-in-First-Out-Prinzip (FIFO) überschrieben.

Flow-Daten

Ein Fluss ist eine Reihe von Paketen, die Teil einer einzelnen Verbindung zwischen zwei Endpunkten sind. Fluss Sensoren sind für RevealX 360 verfügbar und bieten eine kontinuierliche Netzwerktransparenz auf der Grundlage von VPC-Flow-Protokollen, um AWS-Umgebungen abzusichern. VPC-Flow-Logs ermöglichen es Ihnen , Informationen über den IP-Verkehr zu und von Netzwerkschnittstellen in Ihrer VPC zu erfassen. Sie werden als Flow-Log-Datensätze aufgezeichnet, bei denen es sich um Protokollereignisse handelt, die aus Feldern bestehen, die den Datenverkehrsfluss beschreiben. Diese Protokolldaten ermöglichen es Ihnen, mithilfe fortschrittlicher maschineller Learning-Erkennungen nach Bedrohungen zu suchen.

Flow-Logs werden aufgenommen, dedupliziert und dann in Flows gruppiert. Die Flows werden dann mit Daten (wie MAC-Adressen) angereichert, die von AWS EC2-APIs abgefragt werden.

Die Flüsse werden dann auf folgende Weise analysiert und verarbeitet:

- Geräte werden automatisch anhand ihrer an bestimmten Ports beobachteten Aktivität erkannt und klassifiziert.
- Grundlegende L2-L4-Metriken werden generiert und in Metrikzyklen aggregiert.
- ExFlow-Datensatztypen werden generiert und veröffentlicht.

Metriken, Datensätze und Pakete

ExtraHop-Sensoren erfassen und speichern mehrere Tiefen der Netzwerkinteraktion als Metriken. Metriken sind aggregierte Beobachtungen über Endpunktinteraktionen im Laufe der Zeit. Packetstores sammeln und speichern die zwischen zwei Endpunkten übertragenen Rohdaten als Pakete. Plattenläden Sammeln und Speichern von Datensätzen, bei denen es sich um strukturierte Informationen über Transaktions-, Nachrichten- und Netzwerkflüsse handelt.

Sie können all diese Interaktionen von einzelnen Sensoren aus anzeigen und abfragen oder von einem Konsole das ist mit einem komplexen Einsatz von Sensoren, Paketspeichern und Plattenläden verbunden.

Wenn ein Client beispielsweise eine HTTP-Anfrage an einen Server sendet, enthält jeder Datentyp Folgendes:

- Das Paket enthält die Rohdaten, die bei der Interaktion gesendet und empfangen wurden.
- Der zugehörige Datensatz enthält die mit einem Zeitstempel versehenen Metadaten über die Interaktion: den Zeitpunkt der Anfrage, die IP-Adresse des Client und Server, die angeforderte URI, etwaige Fehlermeldungen.
- Die zugehörige Metrik (HTTP-Anfragen) enthält eine Zusammenfassung dieser Interaktion mit anderen beobachteten Interaktionen während des angegebenen Zeitraums, z. B. wie viele Anfragen aufgetreten sind, wie viele dieser Anfragen erfolgreich waren, wie viele Clients Anfragen gesendet haben und wie viele Server die Anfragen erhalten haben.

Sowohl Metriken als auch Datensätze können angepasst werden, um spezifische Metadaten auf JavaScript-Basis zu extrahieren und zu speichern löst aus. Während das ExtraHop-System über 4.600 integrierte Metriken, vielleicht möchten Sie eine erstellen benutzerdefinierte Metrik, die 404-Fehler sammelt und aggregiert nur von kritischen Webservern. Und vielleicht möchten Sie Ihren Plattenspeicher nur maximieren, indem Sie Erfassung von Transaktionen, die über einen verdächtigen Port stattgefunden haben.

Erkennung von Geräten

Nachdem ein Gerät erkannt wurde, beginnt das ExtraHop-System mit der Erfassung von Metriken, die auf der für dieses Gerät konfigurierten Analyseebene basieren. Du kannst Finde ein Gerät nach ihrer MAC-Adresse, IP-Adresse oder ihrem Namen (z. B. ein aus dem DNS-Verkehr beobachteter Hostname, NetBIOS-Name, Cisco Discovery Protocol (CDP) -Name, DHCP-Name oder ein benutzerdefinierter Name, den Sie dem Gerät zugewiesen haben).

Das ExtraHop-System kann Geräte anhand ihrer MAC-Adresse (L2 Discovery) oder anhand ihrer IP-Adressen (L3 Discovery) erkennen und verfolgen. L2 Discovery bietet den Vorteil, dass Messwerte für ein Gerät auch dann verfolgt werden können, wenn die IP-Adresse durch eine DHCP-Anfrage geändert oder neu zugewiesen wird. Standardmäßig ist das ExtraHop-System für L2 Discovery konfiguriert.

IPv4- und IPv6-Adressen von Geräten werden anhand von ARP-Nachrichten (Address Resolution Protocol), NDP-Antworten (Neighbor Discovery Protocol), lokalen Broadcasts oder lokalem Subnetz-Multicast-Verkehr ermittelt. Die MAC-Adresse und die IP-Adresse für Geräte werden in den Suchergebnissen im gesamten System zusammen mit den Geräteinformationen angezeigt.

L2-Entdeckung

In L2 Discovery erstellt das ExtraHop-System einen Geräteeintrag für jede lokale MAC-Adresse, die über das Kabel erkannt wurde. IP-Adressen werden der MAC-Adresse zugeordnet, aber Metriken werden zusammen mit der MAC-Adresse des Gerät gespeichert, auch wenn sich die IP-Adresse ändert.

IP-Adressen, die außerhalb von lokal überwachten Broadcast-Domänen beobachtet werden, werden auf einem der eingehenden Router in Ihrem Netzwerk aggregiert. Wenn ein Gerät eine DHCP-Anfrage über einen Router sendet, der als DHCP-Relay-Agent fungiert, erkennt das ExtraHop-System die IP-Adresse und ordnet sie der MAC-Adresse des Gerät zu. Wenn sich die IP-Adresse für das Gerät mit einer nachfolgenden Anfrage über den DHCP-Relay-Agenten ändert, aktualisiert das ExtraHop-System seine Zuordnung und verfolgt die Gerätemetriken weiterhin anhand der MAC-Adresse.

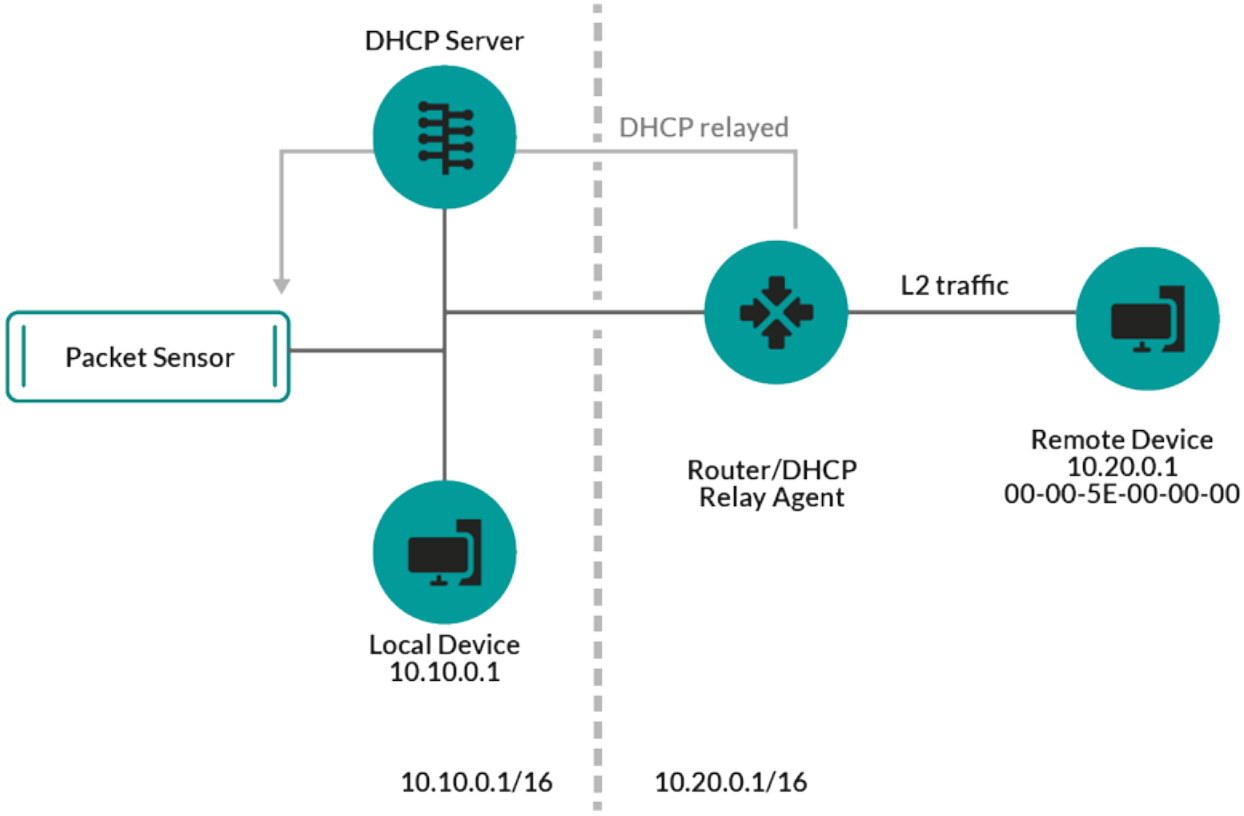


Abbildung 1: Sowohl die MAC-Adresse als auch die IP-Adresse werden für das entferntes Gerät erkannt.

Wenn kein DHCP-Relay-Agent konfiguriert ist, können Remote-Geräte anhand ihrer IP-Adressen erkannt werden über L3-Erkennung per Fernzugriff.

L3-Entdeckung

In L3 Discovery erstellt und verknüpft das ExtraHop-System zwei Einträge für jedes lokal erkannte Gerät: einen übergeordneten L2-Eintrag mit einer MAC-Adresse und einen untergeordneten L3-Eintrag mit IP-Adressen und der MAC-Adresse.

Hier sind einige wichtige Überlegungen zur L3-Entdeckung:

- Wenn auf einem Router Proxy-ARP aktiviert ist, erstellt das ExtraHop-System für jede IP-Adresse, für die der Router ARP-Anfragen beantwortet, ein L3-Gerät.
- Wenn Sie in Ihrem Netzwerk ein Proxy-ARP konfiguriert haben, erkennt das ExtraHop-System möglicherweise automatisch Remote-Geräte.
- L2-Metriken, die keinem bestimmten untergeordneten L3-Gerät zugeordnet werden können (z. B. L2-Broadcast-Verkehr), werden dem L2-Elterngerät zugeordnet.

L3-Erkennung per Fernzugriff

Wenn das ExtraHop-System eine IP-Adresse erkennt, der kein ARP- oder NDP-Verkehr zugeordnet ist, wird dieses Gerät als entferntes Gerät betrachtet. Remote-Geräte werden nicht automatisch erkannt, aber Sie können einen Remote-IP-Adressbereich hinzufügen und Geräte erkennen, die sich außerhalb des lokalen Netzwerk befinden. Für jede IP-Adresse, die innerhalb des Remote-IP-Adressbereichs beobachtet wird, wird ein Geräteeintrag erstellt. (Remote-Geräte haben keine übergeordneten L2-Einträge.)

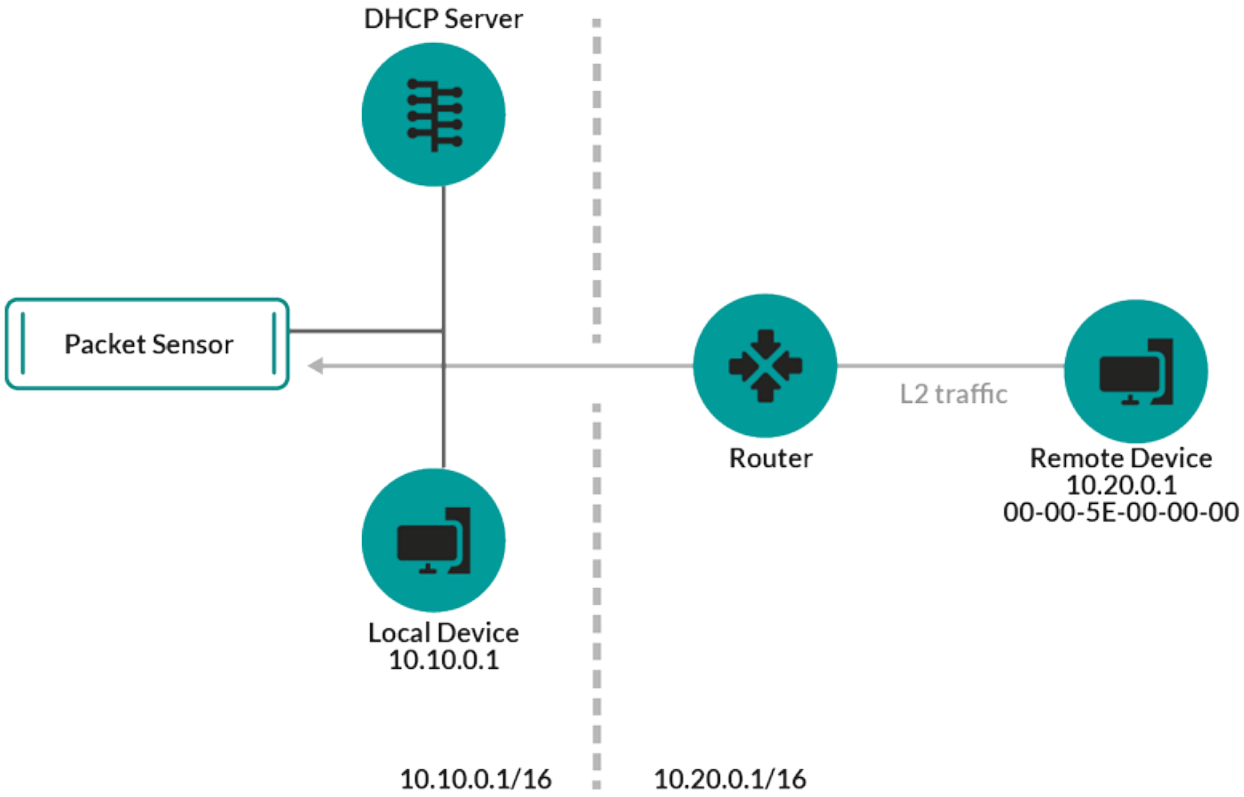


Abbildung 2: Für das entferntes Gerät wird nur die IP-Adresse erkannt.

Im Folgenden finden Sie einige Empfehlungen zur Konfiguration von Remote L3 Discovery:

- Ihre Client-Geräte befinden sich in einem Netzwerksegment, das nicht direkt angezapft wird.
- Ihr Unternehmen verfügt über eine Außenstelle ohne ein ExtraHop-System vor Ort, aber die Benutzer an diesem Standort greifen auf zentrale Rechenzentrumsressourcen zu, die direkt von einem ExtraHop-System überwacht werden. Die IP-Adressen am Remote-Standort können als Geräte erkannt werden.
- Ein Cloud-Dienst oder ein anderer externer Dienst hostet Ihre Remote-Anwendungen und hat einen bekannten IP-Adressbereich. Die Remote-Server innerhalb dieses IP-Adressbereichs können individuell verfolgt werden.

VPN-Entdeckung
VPN-Entdeckung ermöglicht es dem ExtraHop-System, die privaten RFC-1918-IP-Adressen, die VPN-Clients zugewiesen wurden, mit ihren öffentlichen, externen IP-Adressen zu korrelieren. Dieser erweiterte Einblick in den Nord-Süd-Verkehr reduziert Hindernisse bei der Untersuchung von Sicherheitsvorfällen und Leistungsproblemen , an denen externe VPN-Clients beteiligt sind. (Für diese Funktion ist ein VPN-Gateway erforderlich, das vom Benutzer manuell zugewiesen wird.)

Software-Fingerabdruck

Im ExtraHop-System bieten Betriebssystem (OS) und Software-Fingerprinting einen erheblichen Sicherheitswert, da sie eine genaue Geräteidentifikation und -klassifizierung ermöglichen. Diese granulare Sichtbarkeit ermöglicht es Sicherheitsteams, Bedrohungen effektiver zu erkennen und darauf zu reagieren und die Bedrohungssuche und die Reaktion auf Vorfälle zu verbessern.

Software-Fingerprinting funktioniert, indem passiv beobachtete Netzwerkfelder mit einer kuratierten Sammlung von Fingerabdrücken abgeglichen werden, die in unserer Datenbank gespeichert sind, um einen performanten Abgleich zu ermöglichen. Diese Fingerabdrücke werden in der Cloud aktualisiert und über ExtraHop Cloud Services an die Paketsensoren übertragen.

Im Gegensatz zu anderen Produkten, die aktiv nach diesen Informationen suchen, beobachtet das ExtraHop-System opportunistisch Fingerabdrücke, die auf natürliche Weise im Netzwerk vorkommen. Das ExtraHop-System verfügt derzeit über 45 Netzwerkfelder (über verschiedene Protokolle hinweg), die passiv beobachtet werden, um das Betriebssystem und die Software Gerät zu identifizieren. Diese Felder reichen von HTTP-Server-Headern über X.509-Zertifikatssubjekte bis hin zu DHCP-Anbietern und vielem mehr.

Software-Frame-Deduplizierung

Das ExtraHop-System entfernt standardmäßig doppelte L2- und L3-Frames und -Pakete, wenn Metriken aus Ihrer Netzwerkaktivität erfasst und aggregiert werden.

Das Systemzustand Die Seite enthält Diagramme, in denen doppelte L2- und L3-Pakete angezeigt werden, die vom ExtraHop-System entfernt wurden. Die Deduplizierung funktioniert standardmäßig über 10-Gbit/s-Ports.

L2-Deduplizierung

Bei der L2-Deduplizierung werden identische Ethernet-Frames entfernt, bei denen Ethernet-Header und Payload übereinstimmen müssen. Das ExtraHop-System sucht nach Duplikaten und entfernt global nur das unmittelbar vorhergehende Paket, wenn das Duplikat innerhalb von 1 Millisekunde nach dem Originalpaket eintrifft. Eine L2-Duplizierung liegt normalerweise nur vor, wenn genau dasselbe Paket im Datenfeed zu sehen ist, was in der Regel auf ein Problem mit der Portspiegelung zurückzuführen ist.

L3-Deduplizierung

Die L3-Deduplizierung entfernt TCP- oder UDP-Pakete mit identischen IP-Adress-ID-Feldern im gleichen Fluss, wobei nur das IP-Paket übereinstimmen muss. Der Inhalt aller Header, die dem überprüften IP-Header vorausgehen, kann unterschiedlich sein. Die L3-Deduplizierung wird derzeit nur für IPv4 unterstützt, nicht für IPv6. Das ExtraHop-System sucht nach Duplikaten und entfernt nur das unmittelbar vorhergehende Paket im Fluss, wenn das Duplikat innerhalb von 1 Millisekunde nach dem ursprünglichen Paket ankommt und wenn das Paket in dieselbe Richtung reist. Damit ein Paket dedupliziert werden kann, dürfen zwischen den beiden doppelten Paketen keine anderen Pakete empfangen werden. Darüber hinaus müssen Pakete dieselbe Länge und dasselbe IP-Adress-ID-Feld haben, und TCP-Pakete müssen auch dieselbe TCP-Prüfsumme haben.

Standardmäßig sind Datenflüsse über VLANs aktiviert, und da die L3-Deduplizierung pro Datenfluss erfolgt, entfernt die L3-Deduplizierung dasselbe Paket, das verschiedene VLANs durchläuft. Die L3-Deduplizierung ist oft das Ergebnis der Spiegelung desselben Datenverkehrs über mehrere Schnittstellen desselben Routers, und dieser Verkehr kann als irrelevante TCP-Neuübertragungen im ExtraHop-System auftauchen.

Erkennung von Bedrohungen

Das ExtraHop-System bietet sowohl maschinelles Lernen als auch regelbasiertes Erkennungen die aktive oder potenzielle Bedrohungen, Netzwerkschwächen, die anfällig für Exploits sind, und suboptimale Konfigurationen, die die Netzwerkleistung beeinträchtigen können, identifizieren.

Zusätzlich Diagramme, Visualisierungen, und Karten zur Geräteaktivität ermöglichen Sie die proaktive Bedrohungssuche.

Optimierung der Erkennung

Reduzieren Sie Geräusche und lassen Sie nur kritische Erkennungen erkennen indem Sie Details über Ihr Netzwerk hinzufügen, anhand derer bekannte Parameter wie vertrauenswürdige Domänen und Schwachstellenscanner identifiziert werden können.

Darüber hinaus können Sie Optimierungsregeln erstellen, die bestimmte Erkennungen oder Teilnehmer verbergen und unerwünschte Geräusche weiter reduzieren.

Netzwerk-Lokalität
Standardmäßig wird jedes Gerät mit einer RFC1918-IP-Adresse (in einem 10/8-, 172.16/12- oder 192.168/16 CIDR-Block enthalten) auf dem System als internes Gerät klassifiziert.

Da einige Netzwerkumgebungen jedoch IP-Adressen enthalten, die nicht RFC1918 entsprechen, als Teil ihres internen Netzwerk, können Sie die interne oder externe Klassifizierung für IP-Adressen ändern von der Seite Network Locations.

Bedrohungsinformationen
Das ExtraHop-System umfasst kuratierte Bedrohungsinformationen Feeds von ExtraHop und Crowdstrike Falcon, die über die Cloud aktualisiert werden, sobald neue Bedrohungen entdeckt werden. Du kannst auch Bedrohungssammlungen hinzufügen von einem Drittanbieter.

Bedrohungsinformationen
Bedrohungsinformationen stellen Informationen über unmittelbare Bedrohungen bereit , die auf Netzwerke abzielen. Aktuelle Erkennungen, gezielte Datensatz- und Paketabfragen sowie betroffene Geräte werden als Ausgangspunkt für Ihre Untersuchung angezeigt. Der Zugriff erfolgt über Überblick über die Sicherheit Seite.

Integrationen
RevealX 360 bietet mehrere Drittanbieter-Integrationen, die das Erkennung- und Reaktionsmanagement verbessern und einen besseren Überblick über den Netzwerkverkehr bieten können.

Kortex XSOAR

Exportieren Sie ExtraHop-Erkennungen, führen Sie Antwort-Playbooks aus und fragen Sie Gerätedetails in Cortex XSOAR ab.

Crowdstrike

Sehen Sie sich Details zu CrowdStrike-Geräten an und fügen Sie diese Geräte aus dem ExtraHop-System hinzu.

Microsoft 365

Importieren Sie Microsoft 365-Erkennungen und -Ereignisse, überwachen Sie Microsoft 365-Metriken in integrierten Dashboards und lassen Sie sich Details zu Risikoereignissen in Datensätzen anzeigen.

Microsoft-Protokollentschlüsselung

Entschlüsseln Sie den Datenverkehr über Microsoft-Protokolle wie LDAP, RPC, SMB und WSMan, um die Erkennung von Sicherheitsangriffen in Ihrer Microsoft Windows-Umgebung zu verbessern.

Q-Radar

Exportieren und betrachten Sie ExtraHop-Erkennungen in Ihrem QRadar SIEM.

Splunk SIEM für Unternehmenssicherheit

Exportieren und zeigen Sie ExtraHop-Erkennungen in Ihrem Splunk SIEM an.

Splunk SOAR

Exportieren und zeigen Sie ExtraHop-Erkennungen, -Metriken und -Pakete in Ihrer Splunk SOAR-Lösung an.