Geräte

Veröffentlicht: 2025-02-04

Das ExtraHop-System erkennt und klassifiziert automatisch Geräte, auch Endpunkte genannt, die aktiv über Ihr Netzwerk kommunizieren, wie Clients, Server, Router, Load Balancer und Gateways. Jedes Gerät erhält die höchste verfügbare Analyseniveau, basierend auf Ihrer Systemkonfiguration.

Das ExtraHop-System kann Geräte entdecken und verfolgen nach ihrer MAC-Adresse (L2 Discovery) oder nach ihren IP-Adressen (L3 Discovery). Die Aktivierung von L2 Discovery bietet den Vorteil, dass Metriken für ein Gerät auch dann verfolgt werden, wenn die IP-Adresse durch eine DHCP-Anfrage geändert oder neu zugewiesen wird. Wenn L3 Discovery aktiviert ist, ist es wichtig zu wissen, dass Geräte möglicherweise keine Eins-zu-Eins-Beziehung zu den physischen Geräten in Ihrer Umgebung haben. Wenn beispielsweise ein einzelnes physisches Gerät über mehrere aktive Netzwerkschnittstellen verfügt, wird dieses Gerät vom ExtraHop-System als mehrere Geräte identifiziert.

Nachdem ein Gerät erkannt wurde, beginnt das ExtraHop-System mit der Erfassung von Metriken auf der Grundlage der Analyseebene für dieses Gerät konfiguriert. Die Analyseebene bestimmt, welche Arten von Metriken generiert werden und welche Funktionen für die Organisation von Metrikdaten verfügbar sind.

Navigierende Geräte

klicken **Vermögenswerte** aus dem oberen Menü, um Suchoptionen und Diagramme anzuzeigen, die einen Einblick in die aktiven Geräte geben, die während des ausgewählten Zeitintervalls in Ihrem Netzwerk entdeckt wurden:

AI Search Assistant (erfordert Zugriff auf das NDR-Modul)

Ermöglicht es Ihnen suche nach Geräten mit Fragen geschrieben in natürlicher, alltäglicher Sprache. KI-Suchassistent muss vom ExtraHop-Administrator aktiviert werden.

Standard-Suchfeld

Stellt einen Filter bereit, zu dem Kriterien hinzugefügt werden können suche nach bestimmten Geräten. Klicken Sie auf den Filter, um die Suchkriterien zu ändern.

Vorschläge für die Suche

Bietet Suchvorschläge, die die erstellten Suchfilter nutzen.

Aktive Geräte

Zeigt die Gesamtzahl der Geräte an, die vom ExtraHop-System während des ausgewählten Zeitintervalls erkannt wurden. Klicken Sie auf die Zahl, um eine Liste aller erkannten Geräte anzuzeigen. In der Liste der aktiven Geräte können Sie suche nach bestimmten Geräten oder klicken Sie auf einen Gerätenamen, um Gerätedetails auf der Seite „ Geräteübersicht“.

Neue Geräte

Zeigt die Anzahl der Geräte an, die in den letzten fünf Tagen entdeckt wurden. Klicken Sie auf die Nummer, um eine Liste all dieser Geräte anzuzeigen.

Geräte nach Rolle

Zeigt jede Geräterolle und die Anzahl der Geräte an, die jeder Rolle zugewiesen sind, die während des angegebenen Zeitintervalls aktiv ist. Klicken Sie auf eine Geräterolle, um eine integrierte Übersichtsseite für Gerätegruppen anzuzeigen, die Metrikdaten, Peer-IPs und Protokollaktivitäten für diese Gerätegruppe enthält. Sie können auch zusätzliche Filterkriterien hinzufügen und die Gruppe als neue dynamische Gerätegruppe speichern.

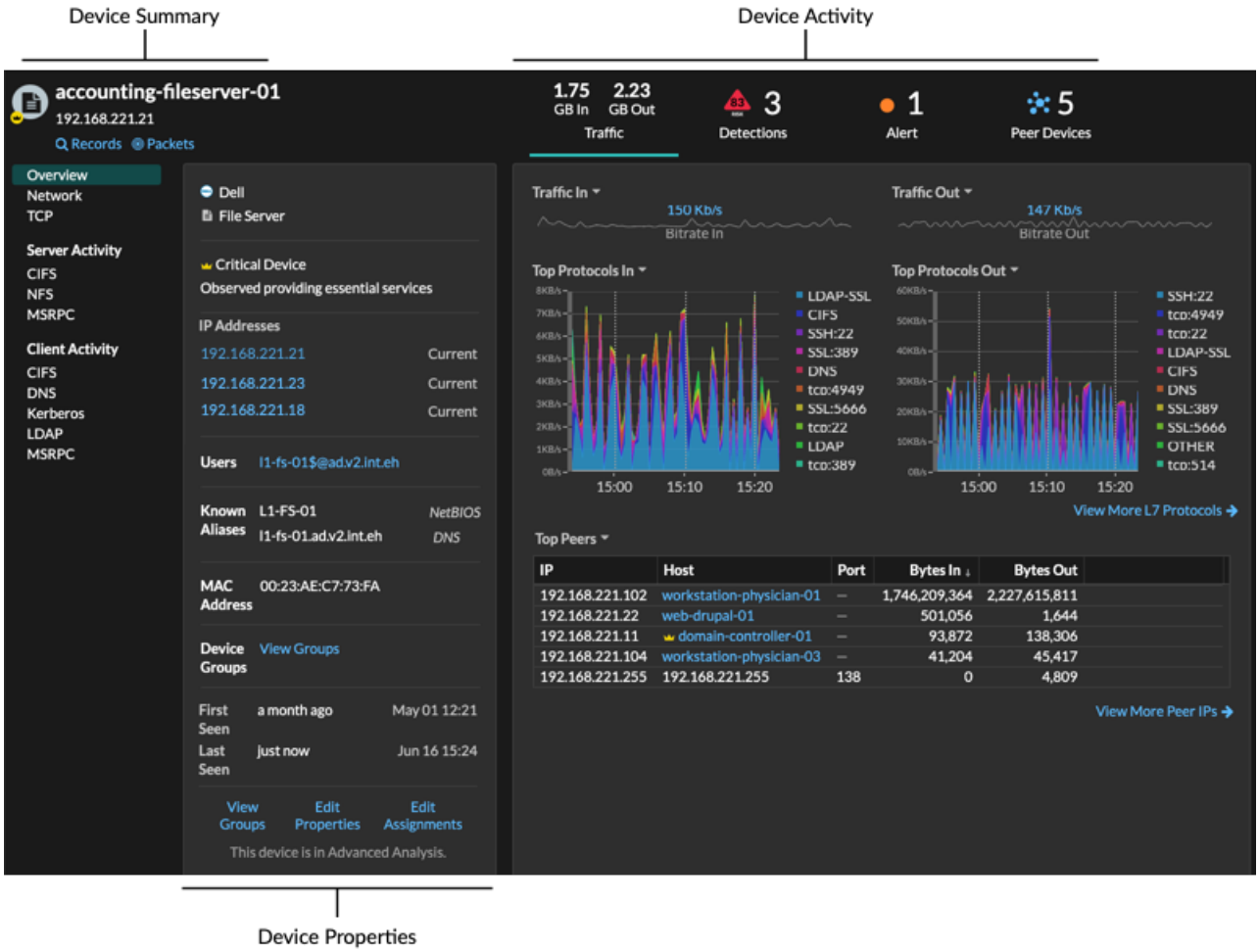
Geräte nach Protokollaktivität

Zeigt eine Liste der Protokollaktivitäten an, die in Ihrem Netzwerk gefunden wurden. Klicken Sie auf einen Protokollnamen oder eine Geräteanzahl, um eine integrierte Übersichtsseite mit bestimmten Metrikdiagrammen zu dieser Protokollaktivität anzuzeigen. Klicken Sie auf eine Aktivitätsdiagramm,

um alle Gerät-zu-Gerät-Verbindungen anzuzeigen. Sie können auch zusätzliche Filterkriterien hinzufügen und die Gruppe als neue dynamische Gerätegruppe speichern.

Seite „Geräteübersicht“

Wenn Sie auf einen Gerätenamen klicken, können Sie alle Informationen, die das ExtraHop-System über das Gerät gefunden hat, auf der Seite Geräteübersicht einsehen. Die Seite „Geräteübersicht“ ist in drei Abschnitte unterteilt: eine Zusammenfassung auf oberster Ebene, einen Eigenschaftenbereich und einen Aktivitätsbereich.



Zusammenfassung des Geräts

Die Geräteübersicht enthält Informationen wie den Gerätenamen, die aktuelle IP - oder MAC-Adresse und die dem Gerät zugewiesene Rolle. Wenn Sie von einem aus betrachten Konsole, der Name der mit dem Gerät verknüpften Standort wird ebenfalls angezeigt.

- klicken **Rekorde** um eine zu starten Datensatzabfrage das wird von diesem Gerät gefiltert.
- klicken **Pakete** um eine zu starten Paketabfrage das wird von diesem Gerät gefiltert.

Eigenschaften des Geräts

Der Abschnitt mit den Geräteeigenschaften enthält die folgenden bekannten Attribute und Zuweisungen für das Gerät.

Marke und Modell

Die Marke (oder der Hersteller) des Gerät und das Gerätemodell, falls verfügbar.

Das ExtraHop-System beobachtet den Netzwerkverkehr auf Geräten, um automatisch Marke und Modell zu ermitteln, oder Sie können Manuelles Zuweisen einer neuen Marke und eines neuen Modells.

Rolle des Geräts

Das ExtraHop-System weist automatisch eine Geräterolle, z. B. ein Gateway, ein Server, eine Datenbank oder ein Load Balancer, basierend auf der Art des Datenverkehrs, der mit dem Gerät oder dem Gerätemodell verknüpft ist. Sie können manuell eine Geräterolle ändern.

Hochwertiges Gerät

Eine hoher Wert Ikone erscheint, wenn das ExtraHop-System beobachtet hat, dass das Gerät die Authentifizierung oder wichtige Dienste bereitstellt; Sie können auch geben Sie manuell ein Gerät als hoher Wert. Die Risikowerte für Erkennungen auf hoher Wert Geräten werden erhöht.

Software

Das primäre Betriebssystem oder die Software, die auf dem Gerät ausgeführt wird.

Hinweis: CrowdStrike-Integration (nur auf RevealX 360) Sie können auf Links von Geräten klicken, auf denen die CrowdStrike-Software ausgeführt wird, um Gerätedetails in CrowdStrike Falcon anzuzeigen und die Eindämmung von CrowdStrike-Geräten einleiten das sind Teilnehmer an einer Sicherheitserkennung.

IP-Adressen

Eine Liste der IP-Adressen, die zu einem beliebigen Zeitpunkt während des ausgewählten Zeitintervalls auf dem Gerät beobachtet wurden. Wenn L2 Discovery aktiviert ist, werden in der Liste möglicherweise sowohl IPv4- als auch IPv6-Adressen angezeigt, die gleichzeitig auf dem Gerät beobachtet werden, oder in der Liste werden möglicherweise mehrere IP-Adressen angezeigt, die über DHCP-Anfragen zu unterschiedlichen Zeiten zugewiesen wurden. Ein Zeitstempel gibt an, wann die IP-Adresse zuletzt auf dem Gerät beobachtet wurde. Klicken Sie auf eine IP-Adresse um andere Geräte anzuzeigen, auf denen die IP-Adresse gesehen wurde.

Zugeordnete IP-Adressen

Eine Liste von IP-Adressen, normalerweise außerhalb des Netzwerk, die dem Gerät zu einem beliebigen Zeitpunkt während des ausgewählten Zeitintervalls zugeordnet sind. Beispielsweise könnte ein VPN-Client in Ihrem Netzwerk mit einer externen IP-Adresse im öffentlichen Internet verknüpft sein. Ein Zeitstempel gibt an, wann die IP-Adresse zuletzt mit dem Gerät verknüpft wurde. Klicken Sie auf eine zugehörige IP-Adresse um Details wie den geografischen Standort und andere Geräte anzuzeigen, mit denen die IP-Adresse verknüpft wurde.

Cloud-aktualisierte Eigenschaften (nur RevealX 360)

Eine Liste der über die Cloud aktualisierten Geräteeigenschaften, abgerufen von Integrationen die auf Ihrem ExtraHop-System wie CrowdStrike konfiguriert sind. Cloud-aktualisierte Eigenschaften variieren je nach Integration.

Cloud-aktualisierte Geräteeigenschaften werden auch angezeigt, wenn Sie den Mauszeiger über einen Gerätenamen bewegen, um Eigenschaftsdetails im gesamten ExtraHop-System anzuzeigen. Sie können nach Cloud-aktualisierten Eigenschaften filtern, um finde ein Gerät und zu eine dynamische Gerätegruppe erstellen.

Eigenschaften der Cloud-Instanz

Die folgenden Cloud-Instanzeigenschaften werden für das Gerät angezeigt, wenn Sie die Eigenschaften über die REST-API konfigurieren:

- Cloud-Konto
- Cloud-Instanztyp
- Virtuelle private Cloud (VPC)
- Cloud-Subnetz-ID
- Cloud-Instanzname (erscheint in der Eigenschaft Bekannter Alias)
- Beschreibung der Cloud-Instanz (Instanz-Metadaten werden automatisch für Geräte in Flow Analysis angezeigt)

siehe Fügen Sie Cloud-Instanz-Eigenschaften über den ExtraHop API Explorer hinzu für weitere Informationen.

Nutzer

Eine Liste der authentifizierten Benutzer, die am Gerät angemeldet sind. Klicken Sie auf einen Benutzernamen um zur Benutzerseite zu gehen und zu sehen, auf welchen anderen Geräten der Benutzer angemeldet ist.

Bekannte Aliase

Eine Liste von Alternativen Gerätenamen und das Quellprogramm oder Protokoll.

Hinweis Es werden mehrere DNS-Namen unterstützt.

Schlagworte

Das dem Gerät zugewiesene Tags. Klicken Sie auf einen Tag-Namen, um die anderen Geräte anzuzeigen, denen das Tag zugewiesen ist.

Zuerst und zuletzt gesehen

Die Zeitstempel von dem Zeitpunkt, an dem das Gerät zum ersten Mal entdeckt wurde und wann die Aktivität zuletzt auf dem Gerät beobachtet wurde. NEU erscheint, wenn das Gerät innerhalb der letzten fünf Tage entdeckt wurde

Analyse

Das Ebene der Analyse die dieses Gerät empfängt.

Hier sind einige Möglichkeiten, wie Sie Geräteeigenschaften anzeigen und ändern können:

- klicken **Gruppen ansehen** um das zu sehen Gerätegruppe Mitgliedschaft für das Gerät.
- klicken **Eigenschaften bearbeiten** um Geräteeigenschaften anzuzeigen oder zu ändern , wie Geräterolle, Gerätegruppenmitgliedschaften, oder Geräte-Tags.
- klicken **Zuweisungen bearbeiten** um welche einzusehen oder zu ändern Warnungen und löst aus sind dem Gerät zugewiesen.

Aktivität des Geräts

Der Abschnitt Geräteaktivität enthält Informationen darüber, wie das Gerät mit anderen Geräten kommuniziert und welche Erkennungen und Warnungen mit dem Gerät verknüpft sind.

- klicken **Verkehr** um Diagramme für Protokoll- und Peer-Daten anzuzeigen, und dann nach unten bohren zu Metriken in Verkehrskarten.

  Hinweis Verkehrsdiagramme sind nicht verfügbar, wenn sich die Geräteanalyseebene im Entdeckungsmodus befindet. Um Verkehrskarten für das Gerät zu aktivieren, erhöhen Sie das Gerät auf Fortgeschrittene Analyse oder Standardanalyse.
- klicken **Erkennungen** um eine Liste der Funde anzuzeigen, und klicken Sie dann auf einen Erkennungsnamen, um Erkennungsdetails anzeigen.
- klicken **Ähnliche Geräte** um eine Liste von Geräten mit ähnlichem Netzwerkverkehrsverhalten anzuzeigen, das durch maschinelle Lernanalysen beobachtet wurde. Ähnliche Geräte können Ihnen helfen, bei der Suche nach Bedrohungen einen Einblick in das normale Geräteverhalten zu erhalten. Diese Registerkarte wird nur angezeigt, wenn dem Gerät ähnliche Geräte zugeordnet sind.
- (Zugriff auf das NPM-Modul erforderlich.) klicken **Warnmeldungen** um eine Liste von Warnungen anzuzeigen, und klicken Sie dann auf einen Warnungsnamen, um Warnungsdetails anzeigen. Diese Registerkarte wird nur angezeigt, wenn dem Gerät Warnungen zugeordnet sind.
- klicken **Peer-Geräte** zu eine Aktivitätsdiagramm, das ist eine visuelle Darstellung der L4-L7-Protokollaktivität zwischen Geräten in Ihrem Netzwerk. Zu modifizieren Sie die Aktivitätsdiagramm mit zusätzlichen Filtern und Schritten klicken Sie auf **Aktivitätenkarte öffnen**.

Hinweis Sie können die Seite „Geräteübersicht“ mit einem Lesezeichen für eine bestimmte Aktivitätsansicht versehen, indem Sie die `tab` URL-Parameter für einen der folgenden Werte:

- `tab=traffic`

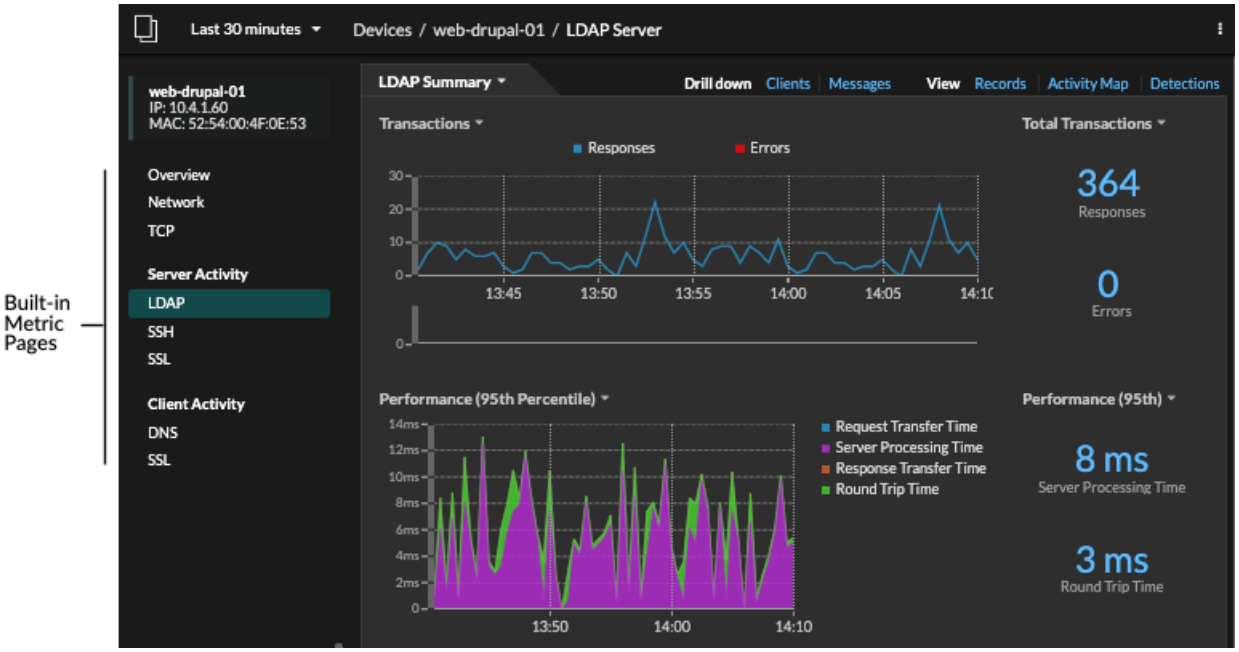
- `tab=detections`
- `tab=alerts`
- `tab=peers`

Beispielsweise zeigt die folgende URL immer die Erkennungsaktivität für das angegebene Gerät an:

```
https://example-eda/extrahop/#/metrics/devices//0026b94c03810000/
overview/&tab=detections
```

Geräte-Metriken

Metriken sind Echtzeitmessungen Ihres Netzwerkverkehrs, die das ExtraHop-System aus Netzwerk- oder Flussdaten berechnet. Aus dem Geräteverkehr gesammelte Messwerte können in integrierten Diagrammen und Grafiken auf einer Geräteseite angezeigt werden.



Klicken Sie im linken Bereich auf eine integrierte Metrikseite, um die oberste Ebene anzuzeigen Gerätemetriken oder Client und Server Metriken nach Protokoll. Klicken Sie auf ein Diagramm, um Detailseiten mit Metriken aufrufen, die Metrikwerte für einen bestimmten Schlüssel (z. B. eine Client- oder Server-IP-Adresse) anzeigen.

Zusätzlich zu den integrierten Netzwerk- und TCP-Seiten zeigen Geräte integrierte Metrikseiten für zugehörige Cloud-Dienste an, sofern Daten verfügbar sind. Sehen Sie die Referenz zu Protokollmetriken für weitere Informationen darüber, welche Daten auf den integrierten Geräteseiten verfügbar sind.

Das ExtraHop-System bietet Tausende von integrierten Metriken. Hier sind einige Möglichkeiten, wie Sie weitere Einblicke in Ihre Geräte gewinnen können

- Erstellen Sie ein Diagramm um bestimmte Kennzahlen zu visualisieren und das Diagramm in einem Dashboard zu speichern.
- Erstellen Sie eine Aktivitätsdiagramm um die Beziehungen zwischen Peer-Geräten über bestimmte Protokolle hinweg anzuzeigen.
- Schreiben Sie einen Auslöser erstellen benutzerdefinierte Metriken oder erstelle eine Anwendung Container zum Sammeln von Metriken für bestimmte Geräte.

Angaben zur IP-Adresse

Geben Sie eine IP-Adresse in das globale Suchfeld ein oder klicken Sie auf einer Seite mit der Geräteübersicht auf einen Link zur IP-Adresse, um Details zu einer IP-Adresse anzuzeigen.

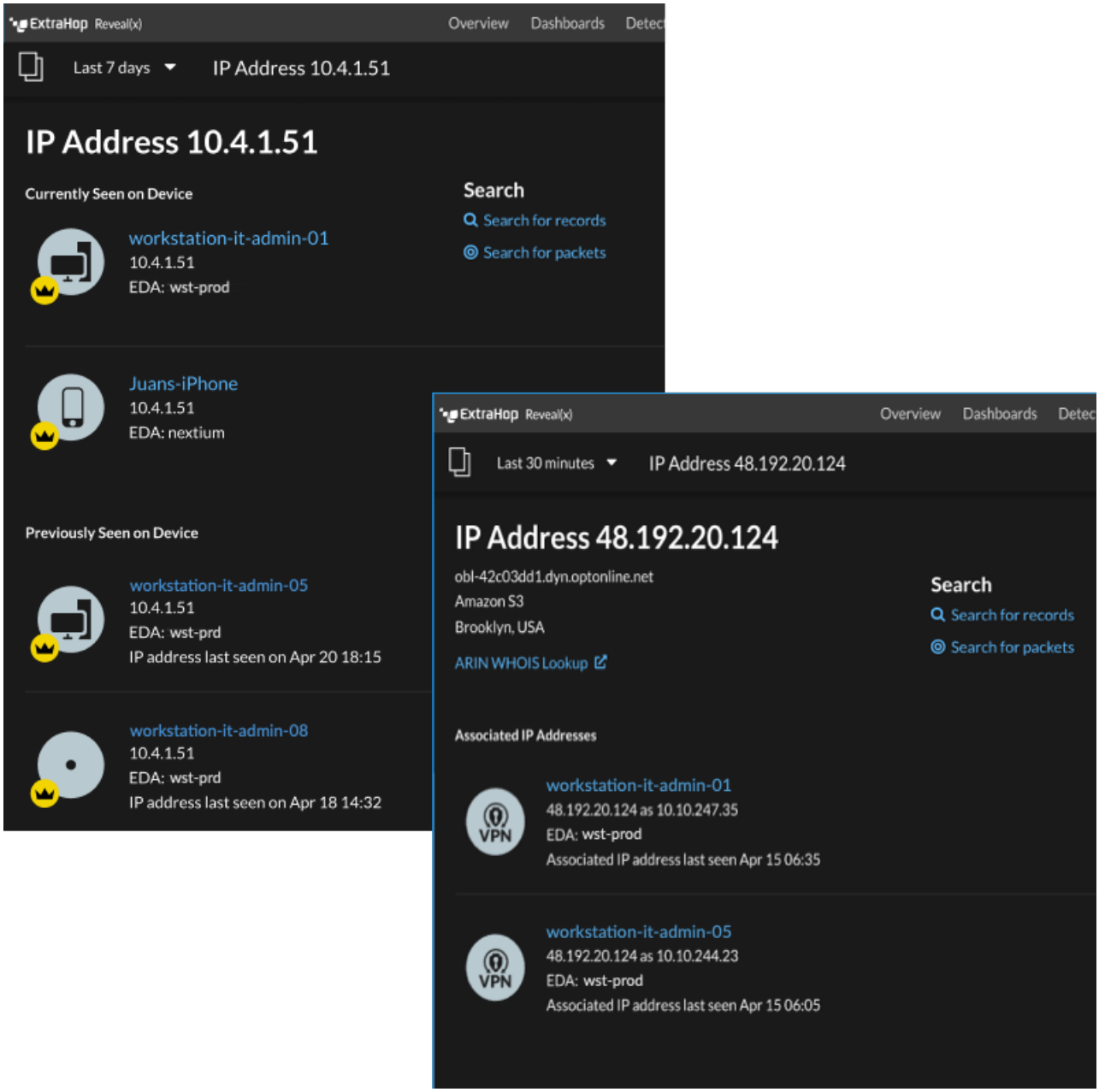
Die folgenden Informationen werden für eine IP-Adresse angezeigt, die auf einem Gerät angezeigt wird:

- Jedes Gerät, auf dem die IP-Adresse derzeit beobachtet wird, unabhängig vom ausgewählten Zeitintervall.
- Jedes Gerät, bei dem die IP-Adresse zuvor innerhalb des ausgewählten Zeitintervalls beobachtet wurde, einschließlich des Zeitstempel, ab dem die IP-Adresse zuletzt auf dem Gerät angezeigt wurde.

Wenn L2 Discovery aktiviert ist, können sowohl IPv4- als auch IPv6-Adressen gleichzeitig auf dem Gerät beobachtet werden, oder dem Gerät können im Laufe der Zeit unterschiedliche IP-Adressen per DHCP zugewiesen werden.

Die folgenden Informationen werden für eine IP-Adresse angezeigt, die einem Gerät zugeordnet ist:

- Die Geolokalisierung der IP-Adresse und Links zur ARIN Whois-Website.
- Jedes Gerät, bei dem die zugehörige IP-Adresse zu einem beliebigen Zeitpunkt während des ausgewählten Zeitintervalls außerhalb des Netzwerk gesehen wurde. Beispielsweise könnte ein VPN-Client in Ihrem Netzwerk mit einer externen IP-Adresse im öffentlichen Internet verknüpft sein.
- Alle Cloud-Dienste, die mit der IP-Adresse verknüpft sind.
- Die IP-Adresse des Gerät, wie sie vom ExtraHop-System in Ihrem Netzwerk gesehen wird.
- Der Zeitstempel, zu dem die zugehörige IP-Adresse zuletzt auf dem Gerät angezeigt wurde.



Hier sind einige Möglichkeiten, wie Sie zusätzliche IP-Adresse und Geräteinformationen anzeigen können:

- Zeigen Sie mit der Maus auf einen Gerätenamen, um die Geräteeigenschaften anzuzeigen.
- Klicken Sie auf einen Gerätenamen, um Sehen Sie sich die Seite mit der Geräteübersicht an.
- Klicken Sie **Suche nach Aufzeichnungen** um eine zu starten Abfrage Datensatz das wird durch die IP gefiltert .
- Klicken Sie **Suche nach Paketen** um eine zu starten Paketabfrage das wird von diesem Gerät gefiltert.

Geräte gruppieren

Sowohl mit benutzerdefinierten Geräten als auch mit Gerätegruppen können Sie Ihre Gerätekennzahlen aggregieren. Benutzerdefinierte Geräte sind vom Benutzer erstellte Geräte, die Metriken auf der Grundlage bestimmter Kriterien sammeln, während Gerätegruppen Metriken für alle angegebenen Geräte in einer Gruppe sammeln. Bei Gerätegruppen können Sie weiterhin Messwerte für jedes einzelne Gerät oder

Gruppenmitglied anzeigen. Die Messwerte für ein benutzerdefiniertes Gerät werden wie für ein einzelnes Gerät erfasst und angezeigt — Sie können keine individuellen Gerätemetriken anzeigen.

Sowohl Gerätegruppen als auch benutzerdefinierte Geräte können Metriken basierend auf Ihren angegebenen Kriterien dynamisch aggregieren. Wir empfehlen, zuverlässige Kriterien wie Geräte-IP-Adresse, MAC-Adresse, VLAN, Tag oder Typ auszuwählen. Sie können Geräte zwar anhand ihres Namens auswählen, aber wenn der DNS-Name nicht automatisch erkannt wird, wird das Gerät nicht hinzugefügt.

	Gerätegruppen	**Maßgeschneiderte Geräte**
Kriterien	Beinhaltet: • Gerätenamen und Aliase • IP-Adresse, MAC-Adresse, Subnetz • Quell- und Zielport • Entdeckungszeit • Kritikalität des Geräts • Rolle „Gerät“ • Protokollaktivität • Externe Verbindungen • Anbieter, Modell, Software • Eigenschaften der Cloud-Instanz • VLAN • Geräte-Tags	• IP-Adresse • Bidirektionaler, eingehender oder ausgehender Datenverkehr • Peer-IP-Adresse • Quellport • Zielport • VLAN
Kosten der Leistung	Vergleichsweise niedrig. Da Gerätegruppen nur Metriken kombinieren, die bereits berechnet wurden, hat dies einen relativ geringen Effekt auf die Erfassung von Metrik. Die Verarbeitung einer hohen Anzahl von Gerätegruppen mit einer großen Anzahl von Geräten und komplexen Kriterien nimmt jedoch mehr Zeit in Anspruch.	Vergleichsweise hoch. Da die Metriken für benutzerdefinierte Geräte auf der Grundlage benutzerdefinierter Kriterien aggregiert werden, erfordert eine große Anzahl benutzerdefinierter Geräte oder benutzerdefinierter Geräte mit extrem breiten Kriterien mehr Verarbeitung. Benutzerdefinierte Geräte erhöhen auch die Anzahl der Systemobjekte, für die Metriken übertragen werden.
Einzelne Gerätekennzahlen anzeigen	Ja	Nein
Bearbeitungssteuerung für Benutzer mit eingeschränktem Schreibzugriff	Ja Nutzer mit eingeschränkte Schreibrechte kann Gerätegruppen erstellen und bearbeiten. Diese globale Rechterichtlinie muss in den Administrationseinstellungen aktiviert werden.	Nein
Bewährte Verfahren	Erstellen Sie für lokale Geräte, bei denen Sie die Metriken in einem einzigen Diagramm anzeigen und vergleichen möchten.	Erstellen Sie für Geräte, die sich außerhalb Ihres lokalen Netzwerk befinden, oder für Arten von Datenverkehr, den Sie als eine

	Gerätegruppen	Maßgeschneiderte Geräte
	Gerätegruppen können als Metrikquelle festgelegt werden.	einzige Quelle organisieren möchten. Beispielsweise möchten Sie möglicherweise alle physischen Schnittstellen auf einem Server als ein einziges benutzerdefiniertes Gerät definieren, um die Messobjekte für diesen Server als Ganzes besser anzeigen zu können.

Maßgeschneiderte Geräte

Mit benutzerdefinierten Geräten können Sie Messwerte für Geräte erfassen, die sich außerhalb Ihres lokalen Netzwerk befinden oder wenn Sie eine Gruppe von Geräten haben, für die Sie Metriken als einzelnes Gerät aggregieren möchten. Bei diesen Geräten kann es sich sogar um unterschiedliche physische Schnittstellen handeln, die sich auf demselben Gerät befinden. Wenn Sie die Metriken für diese Schnittstellen aggregieren, können Sie leichter nachvollziehen, wie stark Ihre physischen Ressourcen insgesamt belastet sind, und nicht nach Schnittstellen.

Du könntest ein benutzerdefiniertes Gerät erstellen um einzelne Geräte außerhalb Ihrer lokalen Broadcast-Domain zu verfolgen oder Metriken über mehrere bekannte IP-Adressen oder CIDR-Blöcke von einem Remote-Standort oder Cloud-Dienst zu sammeln. Du kannst Erfassung von Remote-Site-Metriken für benutzerdefinierte Geräte um zu erfahren, wie Dienste an entfernten Standorten genutzt werden, und um einen Einblick in den Verkehr zwischen entfernten Standorten und einem Rechenzentrum zu erhalten. Sehen Sie die Referenz zu Protokollmetriken für eine vollständige Liste der Metriken und Beschreibungen von Remote-Standorten.

Nachdem Sie ein benutzerdefiniertes Gerät erstellt haben, werden alle mit den IP-Adressen und Ports verknüpften Metriken in einem einzigen Gerät zusammengefasst, das L2-L7-Metriken erfasst. Ein einzelnes benutzerdefiniertes Gerät zählt als ein Gerät für Ihre lizenzierte Kapazität für Erweiterte Analyse oder Standardanalyse, was es Ihnen ermöglicht füge ein benutzerdefiniertes Gerät zur Beobachtungsliste. Alle Auslöser oder Warnungen werden dem benutzerdefinierten Gerät ebenfalls als einzelnes Gerät zugewiesen.

Benutzerdefinierte Geräte aggregieren zwar Metriken auf der Grundlage ihrer definierten Kriterien, die Metrikberechnungen werden jedoch nicht so behandelt wie bei erkannten Geräten. Beispielsweise könnten Sie einem benutzerdefinierten Gerät, das Datensätze an einen Recordstore überträgt, einen Auslöser zugewiesen haben. Das benutzerdefinierte Gerät wird jedoch in keinem Transaktionsdatensatz als Client oder Server angezeigt. Das ExtraHop-System füllt diese Attribute mit dem Gerät, das der Konversation auf den Wire-Daten entspricht.

Benutzerdefinierte Geräte können die Gesamtsystemleistung beeinträchtigen, daher sollten Sie die folgenden Konfigurationen vermeiden:

- Vermeiden Sie es, mehrere benutzerdefinierte Geräte für dieselben IP-Adressen oder Ports zu erstellen. Benutzerdefinierte Geräte , die mit sich überschneidenden Kriterien konfiguriert sind, können die Systemleistung beeinträchtigen.
- Vermeiden Sie es, ein benutzerdefiniertes Gerät für eine Vielzahl von IP-Adressen oder Ports zu erstellen, da dies die Systemleistung beeinträchtigen könnte.

Wenn eine große Anzahl benutzerdefinierter Geräte die Systemleistung beeinträchtigt, können Sie ein benutzerdefiniertes Gerät löschen oder deaktivieren. Die eindeutige Discovery-ID für das benutzerdefinierte Gerät verbleibt immer im System. siehe Erstellen Sie ein benutzerdefiniertes Gerät zur Überwachung des Datenverkehrs in entfernten Büros um sich mit kundenspezifischen Geräten vertraut zu machen.

Gerätegruppen

Eine Gerätegruppe ist eine benutzerdefinierte Sammlung, mit der Sie Messwerte auf mehreren Geräten verfolgen können, die in der Regel nach gemeinsamen Attributen wie Protokollaktivitäten gruppiert sind.

Du kannst eine statische Gerätegruppe erstellen das erfordert, dass Sie ein Gerät manuell zur Gruppe hinzufügen oder daraus entfernen. Oder du kannst eine dynamische Gerätegruppe erstellen das beinhaltet Kriterien, die bestimmen, welche Geräte automatisch in die Gruppe aufgenommen werden. Zum Beispiel können Sie Erstellen Sie eine dynamische Gerätegruppe auf der Grundlage der Geräteerkennungszeit das fügt Geräte hinzu , die während eines bestimmten Zeitintervalls erkannt wurden.

Standardmäßig enthält die Seite „Gerätegruppe“ die folgenden dynamischen Gerätegruppen, die Sie überschreiben oder löschen können:

Neue Geräte (letzte 24 Stunden)

Beinhaltet Assets und Endpunkte, die das ExtraHop-System in den letzten 24 Stunden zum ersten Mal gesehen hat.

Neue Geräte (letzte 7 Tage)

Beinhaltet Assets und Endpunkte, die das ExtraHop-System in den letzten 7 Tagen zum ersten Mal gesehen hat.

Das ExtraHop-System umfasst auch integrierte dynamische Gerätegruppen nach Rolle und Protokoll. Sie können integrierte Gerätegruppen als Metrikquelle für Objekte wie Diagramme, Warnungen, Auslöser und Aktivitätskarten zuweisen. Sie können eine integrierte Gerätegruppe nicht überschreiben oder löschen, aber Sie können Filterkriterien hinzufügen und sie als neue Gerätegruppe speichern.

Klicken Sie auf der Seite Geräte auf eine Geräteanzahl für eine Rolle oder ein Protokoll, z. B. Domänencontroller oder SMB-Clients, um die Seite mit der Gerätegruppenübersicht anzuzeigen. Wenn Sie oben auf der Seite auf den Filter klicken, können Sie zusätzliche Kriterien hinzufügen und die Seitendaten bei Bedarf aktualisieren, anstatt eine Gerätegruppe erstellen zu müssen.

Das Erfassen von Messwerten mit Gerätegruppen hat keine Auswirkungen auf die Leistung. Wir empfehlen Ihnen jedoch, priorisieren Sie diese Gruppen weil sie wichtig sind, um sicherzustellen, dass die richtigen Geräte ein Höchstmaß an Analyse erhalten.

Gerätegruppen sind eine gute Wahl, wenn Sie Geräte haben, die Sie gemeinsam als Quelle verwenden möchten. Sie könnten beispielsweise Metriken für alle Ihre Produktionswebserver mit hoher Priorität in einem Dashboard sammeln und anzeigen.

Indem Sie eine Gerätegruppe erstellen, können Sie all diese Geräte als eine einzige Metrikquelle verwalten, anstatt sie als einzelne Quellen zu Ihren Diagrammen hinzuzufügen. Beachten Sie jedoch, dass alle zugewiesenen Auslöser oder Warnungen jedem Gruppenmitglied (oder jedem einzelnen Gerät) zugewiesen werden.

Gerätenamen und Rollen

Nachdem ein Gerät erkannt wurde, verfolgt das ExtraHop-System den gesamten mit dem Gerät verbundenen Datenverkehr, um den Gerätenamen und die Rolle zu ermitteln.

Gerätenamen

Das ExtraHop-System erkennt Gerätenamen durch passive Überwachung von Benennungsprotokollen wie DNS, DHCP, NETBIOS und Cisco Discovery Protocol (CDP).

Wenn ein Name nicht über ein Benennungsprotokoll ermittelt wird, wird der Standardname aus Geräteattributen wie MAC-Adressen und IP-Adressen abgeleitet. Für einige Geräte, die auf Fluss entdeckt wurden Sensoren, weist das ExtraHop-System Namen basierend auf der Rolle des Gerät zu, z. B. Internet Gateway oder Amazon DNS Server. Du kannst auch einen benutzerdefinierten Namen erstellen oder einen Cloud-Instanznamen festlegen für ein Gerät.

Ein Gerät kann anhand mehrerer Namen identifiziert werden, die auf der Seite Geräteübersicht als Bekannte Aliase angezeigt werden. Wenn ein Gerät mehrere Namen hat, Die Reihenfolge der Anzeigepriorität ist in den Administrationseinstellungen festgelegt. Sie können nach einem beliebigen Namen suchen, um finde ein Gerät.

Hinweis Benutzerdefinierte Namen werden nicht zwischen verbundenen ExtraHop-Systemen synchronisiert. Beispielsweise ist ein für einen Sensor erstellter benutzerdefinierter Name nicht über eine verbundene Konsole verfügbar.

Wenn ein Gerätename keinen Hostnamen enthält, hat das ExtraHop-System noch keinen mit diesem Gerät verbundenen Verkehr mit dem Namensprotokoll beobachtet. Das ExtraHop-System führt keine DNS-Suchen nach Gerätenamen durch.

Geräterollen

Basierend auf der Art des Datenverkehrs, der mit dem Gerät oder dem Gerätemodell verknüpft ist, weist das ExtraHop-System dem Gerät automatisch eine Rolle zu, z. B. ein Gateway, einen Server, eine Datenbank oder einen Load Balancer. Die Rolle Andere wird Geräten zugewiesen, die nicht identifiziert werden können.

Einem Gerät kann jeweils nur eine Rolle zugewiesen werden. Sie können manuell eine Geräterolle ändern, oder das ExtraHop-System weist möglicherweise eine andere Rolle zu, wenn sich der beobachtete Verkehr und das Verhalten ändern. Wenn beispielsweise ein PC zu einem Server umfunktioniert wurde, können Sie die Rolle sofort ändern, oder die Änderung kann im Laufe der Zeit beobachtet werden und die Rolle wird vom System aktualisiert.

Das ExtraHop-System identifiziert die folgenden Rollen:

Ikone	Rolle	Beschreibung
	Benutzerdefiniertes Gerät	Ein vom Benutzer erstelltes Gerät, das Metriken auf der Grundlage bestimmter Kriterien erfasst. Das ExtraHop-System weist diese Rolle automatisch zu, wenn Sie ein benutzerdefiniertes Gerät erstellen. Sie können einem Gerät die benutzerdefinierte Rolle nicht manuell zuweisen.
	Angriffssimulator	Ein Gerät, auf dem eine Software zur Breach- und Angriffssimulation (BAS) ausgeführt wird, um Angriffe in einem Netzwerk zu simulieren.
	Datenbank	Ein Gerät, das hauptsächlich eine Datenbankinstanz hostet.
	DHCP-Server	Ein Gerät, das hauptsächlich DHCP-Serveraktivitäten verarbeitet.

Ikone	Rolle	Beschreibung
	DNS-Server	Ein Gerät, das hauptsächlich DNS-Serveraktivitäten verarbeitet.
	Domänencontroller	Ein Gerät, das als Domänencontroller für Kerberos-, SMB- und MSRPC-Serveraktivitäten fungiert.
	Dateiserver	Ein Gerät, das auf Lese- und Schreibanforderungen für Dateien über NFS - und SMB-Protokolle reagiert.
	Brandmauer	Ein Gerät, das den eingehenden und ausgehenden Netzwerkverkehr überwacht und den Verkehr gemäß den Sicherheitsregeln blockiert. Das ExtraHop-System weist diese Rolle Geräten nicht automatisch zu.
	Tor	Ein Gerät, das als Router oder Gateway fungiert. Das ExtraHop-System sucht bei der Identifizierung von Gateways nach Geräten, die einer großen Anzahl eindeutiger IP-Adressen zugeordnet sind (über einem bestimmten Schwellenwert). Zu den Gateway-Gerätenamen gehört der Routername wie Cisco B1B500. Im Gegensatz zu anderen L2-Elterngeräte, du kannst ein Gateway-Gerät zur Beobachtungsliste hinzufügen für erweiterte Analysen.
	IP-Kamera	Ein Gerät, das Bild- und Videodaten über das Netzwerk sendet. Das ExtraHop-System weist diese Rolle basierend auf dem Gerätemodell zu.

Ikone	Rolle	Beschreibung
	Load Balancer	Ein Gerät, das als Reverse-Proxy für die Verteilung des Datenverkehrs auf mehrere Server fungiert.
	Medizinisches Gerät	Ein Gerät, das für medizinische Bedürfnisse und medizinische Umgebungen entwickelt wurde. Das ExtraHop-System kann diese Rolle zuweisen, wenn es sich bei einem Gerät um eine bekannte medizinische Marke und ein bekanntes medizinisches Modell handelt oder wenn das Gerät DICOM-Verkehr verarbeitet.
	Mobiles Gerät	Ein Gerät, auf dem ein mobiles Betriebssystem wie iOS oder Android installiert ist.
	NAT-Gateway	Ein Gerät, das als Network Address Translation (NAT) - Gateway fungiert. Das ExtraHop-System kann diese Rolle zuweisen, wenn ein Gerät mit vier oder mehr Betriebssystem-Fingerabdruckfamilien oder mit vier oder mehr Hardware- oder Herstellermarken und -modellen verknüpft ist. Nachdem einem Gerät diese Rolle zugewiesen wurde, werden die Geräteeigenschaften für Software, Hardwaremarke und -modell sowie authentifizierte Benutzer für das Gerät nicht mehr angezeigt.
	PC	Ein Gerät wie ein Laptop, ein Desktop, eine Windows-VM oder ein macOS-Gerät, das den DNS-, HTTP- und TLS-Client-Verkehr verarbeitet.
	Drucker	Ein Gerät, mit dem Benutzer Text und Grafiken von anderen angeschlossenen Geräten drucken können. Das ExtraHop-System weist diese Rolle auf der Grundlage des Gerätemodells oder des

Ikone	Rolle	Beschreibung
		über mDNS (Multicast-DNS) beobachteten Datenverkehrs zu.
	VoIP-Telefon	Ein Gerät, das Voice over IP (VoIP) -Telefonanrufe verwaltet.
	VPN-Client	Ein internes Gerät, das mit einer Remote-IP-Adresse kommuniziert. Wenn VPN-Client-Erkennung ist aktiviert, das ExtraHop-System weist diese Rolle automatisch internen Geräten zu, die über ein VPN-Gateway mit Remote-IP-Adressen kommunizieren. Sie können einem Gerät die VPN-Client-Rolle nicht manuell zuweisen.
	VPN-Gateway	Ein Gerät, das zwei oder mehr VPN-Geräte oder Netzwerke miteinander verbindet , um Remoteverbindungen zu überbrücken. Das ExtraHop-System weist diese Rolle Geräten mit einer großen Anzahl externer VPN-Peers zu, wenn die automatische Klassifizierung für diese Rolle in der laufenden Konfigurationsdatei aktiviert ist.
	Schwachstellen-Scanner	Ein Gerät, auf dem Schwachstellen-Scanner-Programme ausgeführt werden.
	Web-Proxyserver	Ein Gerät, das HTTP-Anfragen zwischen einem Gerät und einem anderen Server verarbeitet.
	Webserver	Ein Gerät, das hauptsächlich Webressourcen hostet und auf HTTP-Anfragen reagiert.

Ikone	Rolle	Beschreibung
	Wi-Fi-Zugangspunkt	Ein Gerät, das ein drahtloses lokales Netzwerk erstellt und ein drahtloses Netzwerksignal an einen bestimmten Bereich projiziert. Das ExtraHop-System weist diese Rolle basierend auf dem Gerätemodell zu.