Geräte

Veröffentlicht: 2023-11-13

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

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 Messwerte für ein Gerät auch dann verfolgt werden können, wenn die IP-Adresse über eine DHCP-Anfrage geändert oder neu zugewiesen wird. Wenn L3 Discovery aktiviert ist, ist es wichtig zu wissen, dass Geräte möglicherweise nicht eins zu eins mit den physischen Geräten in Ihrer Umgebung korrelieren. 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 von Analyseebene für dieses Gerät konfiguriert. Die Analyseebene bestimmt, welche Arten von Metriken generiert werden und welche Funktionen für die Organisation von Metrikdaten verfügbar sind.

Navigationsgeräte

klicken **Vermögenswerte** aus dem oberen Menü und dann klicken **Geräte** um die folgenden Diagramme anzuzeigen, die Aufschluss über die aktiven Geräte geben, die während des ausgewählten Zeitintervalls in Ihrem Netzwerk erkannt wurden:

Aktive Geräte

Zeigt die Gesamtzahl der Geräte an, die vom ExtraHop-System erkannt wurden. Klicken Sie auf die Nummer, 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 dem Seite „ Geräteübersicht“.

Neue Geräte

Zeigt die Anzahl der Geräte an, die im letzten Monat entdeckt wurden, sowie die prozentuale Änderungsrate. Klicken Sie auf die Nummer, um eine Liste all dieser Geräte anzuzeigen.

Geräte nach Rolle

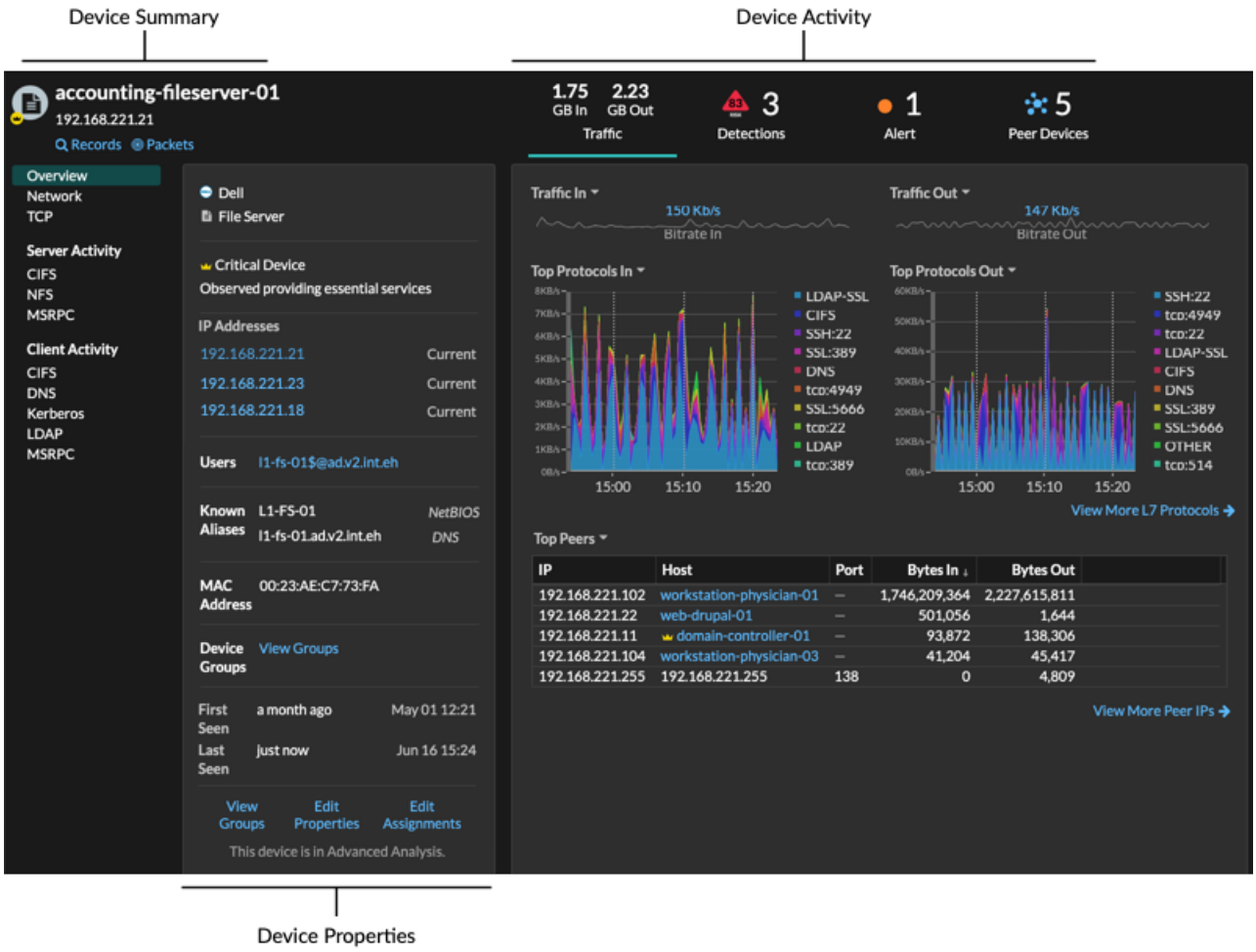
Zeigt jede Geräterolle und die Anzahl der Geräte an, die jeder Rolle zugewiesen sind, die während des angegebenen Zeitintervalls aktiv ist. Klicken Sie auf eine Geräterolle, um eine integrierte Seite mit der Übersicht über Gerätegruppen aufzurufen, die Metrikdaten, Peer-IPs und Protokollaktivitäten für 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 Gerätegruppenübersichtsseite mit spezifischen Metrikdiagrammen zu dieser Protokollaktivität aufzurufen. Klicken Sie auf eine Aktivitätsdiagramm, um alle Gerät-zu-Gerät-Verbindungen zu sehen. 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 ermittelt 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-Adresse oder MAC-Adresse und die dem Gerät zugewiesene Rolle. Wenn der Blick von einem Konsole, der Name der mit dem Gerät verknüpften Standort wird ebenfalls angezeigt.

- klicken **Aufzeichnungen** 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.

Hochwertiges Gerät

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

IP-Adressen

Eine Liste von IP-Adressen, die zu einem beliebigen Zeitpunkt während des ausgewählten Zeitintervalls auf dem Gerät beobachtet wurden. Wenn L2-Entdeckung aktiviert ist, zeigt die Liste möglicherweise sowohl IPv4- als auch IPv6-Adressen an, die gleichzeitig auf dem Gerät beobachtet werden, oder die Liste zeigt möglicherweise mehrere IP-Adressen an , 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 kann 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, mit denen die IP-Adresse verknüpft wurde, anzuzeigen.

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)
- Subnetz
- Name der Cloud-Instanz (wird in der Eigenschaft Known Alias angezeigt)
- Beschreibung der Cloud-Instanz (Instanz-Metadaten werden automatisch für Geräte in Flow Analysis angezeigt)

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

Nutzer

Eine Liste der authentifizierten Benutzer, die am Gerät angemeldet sind. Klicken Sie auf einen Nutzernamen um auf die Seite Benutzer 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.

Hardware und Software

Die Hardware oder der Hersteller, die Marke und das Modell des Geräts sowie alle Betriebssysteme, die auf dem Gerät ausgeführt werden.

Das ExtraHop-System beobachtet den Netzwerkverkehr auf Geräten, um automatisch Hersteller, Marke und Modell zu ermitteln, oder Sie können manuell eine neue Marke und ein neues Modell zuweisen.

Hinweis: (CrowdStrike-Integration nur auf Reveal (x) 360) Klicken Sie auf Links von CrowdStrike-Geräten, um Gerätedetails in CrowdStrike Falcon anzuzeigen, und die Eindämmung von CrowdStrike-Geräten einleiten die an einer Sicherheitserkennung Erkennung.

Schlagworte

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

Zuerst und zuletzt gesehen

Die Zeitstempel von der ersten Entdeckung des Geräts und der letzten Aktivität auf dem Gerät. NEU erscheint, wenn das Gerät innerhalb der letzten fünf Tage entdeckt wurde

Analyse

Die Ebene der Analyse die dieses Gerät empfängt.

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

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

Aktivität auf dem Gerät

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 bohren zu Metriken in Verkehrskarten.

  Hinweis: Verkehrsdiagramme sind nicht verfügbar, wenn die Geräteanalyseebene auf Entdeckungsmodus ist. Um Verkehrskarten für das Gerät zu aktivieren, erhöhen Sie das Gerät auf Fortgeschrittene Analyse oder Standardanalyse.
- klicken **Erkennungen** , um eine Liste der Entdeckungen anzuzeigen, und klicken Sie dann auf einen Erkennungsnamen, um Erkennungsdetails anzeigen.
- klicken **Ähnliche Geräte** um eine Liste von Geräten mit ähnlichem Netzwerkverkehrsverhalten anzuzeigen, das bei einer Analyse des maschinellen Lernens beobachtet wurde. Mit ähnlichen Geräten können Sie bei der Bedrohungssuche Einblick in das normale Geräteverhalten gewinnen. Diese Registerkarte wird nur angezeigt, wenn dem Gerät ähnliche Geräte zugeordnet sind.
- (NPM-Modulzugriff erforderlich.) klicken **Alerts** , um eine Liste von Benachrichtigungen anzuzeigen, und klicken Sie dann auf einen Warnungsnamen, um Warnungsdetails anzeigen. Diese Registerkarte wird nur angezeigt, wenn dem Gerät Warnmeldungen zugeordnet sind.
- klicken **Peer-Geräte** zu Sehen Sie sich eine Aktivitätsdiagramm an, eine visuelle Darstellung der L4-L7-Protokollaktivität zwischen Geräten in Ihrem Netzwerk. Zu Ändern Sie die Aktivitätsdiagramm mit zusätzlichen Filtern und Schritten, klicken Sie **Activity Map öffnen**.

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

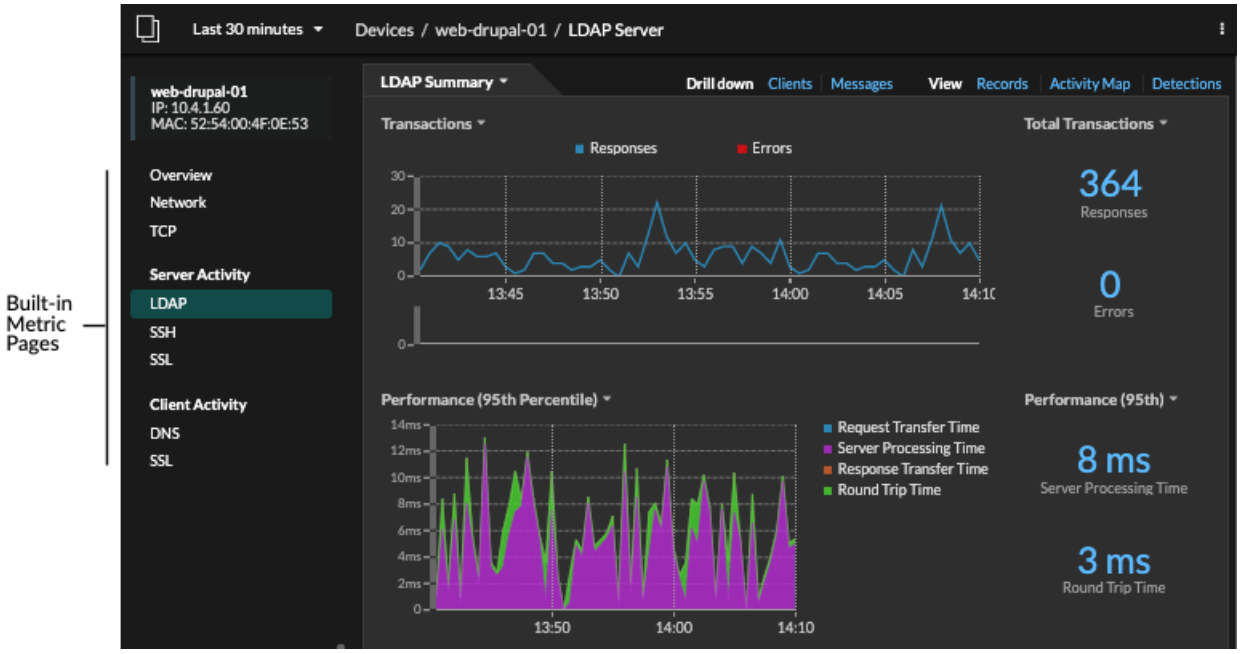
  - `tab=traffic`
  - `tab=detections`
  - `tab=alerts`
  - `tab=peers`

  Die folgende URL zeigt beispielsweise immer Erkennungsaktivitäten 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 IP-Adress-Link, um Details zu einer IP-Adresse anzuzeigen.

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

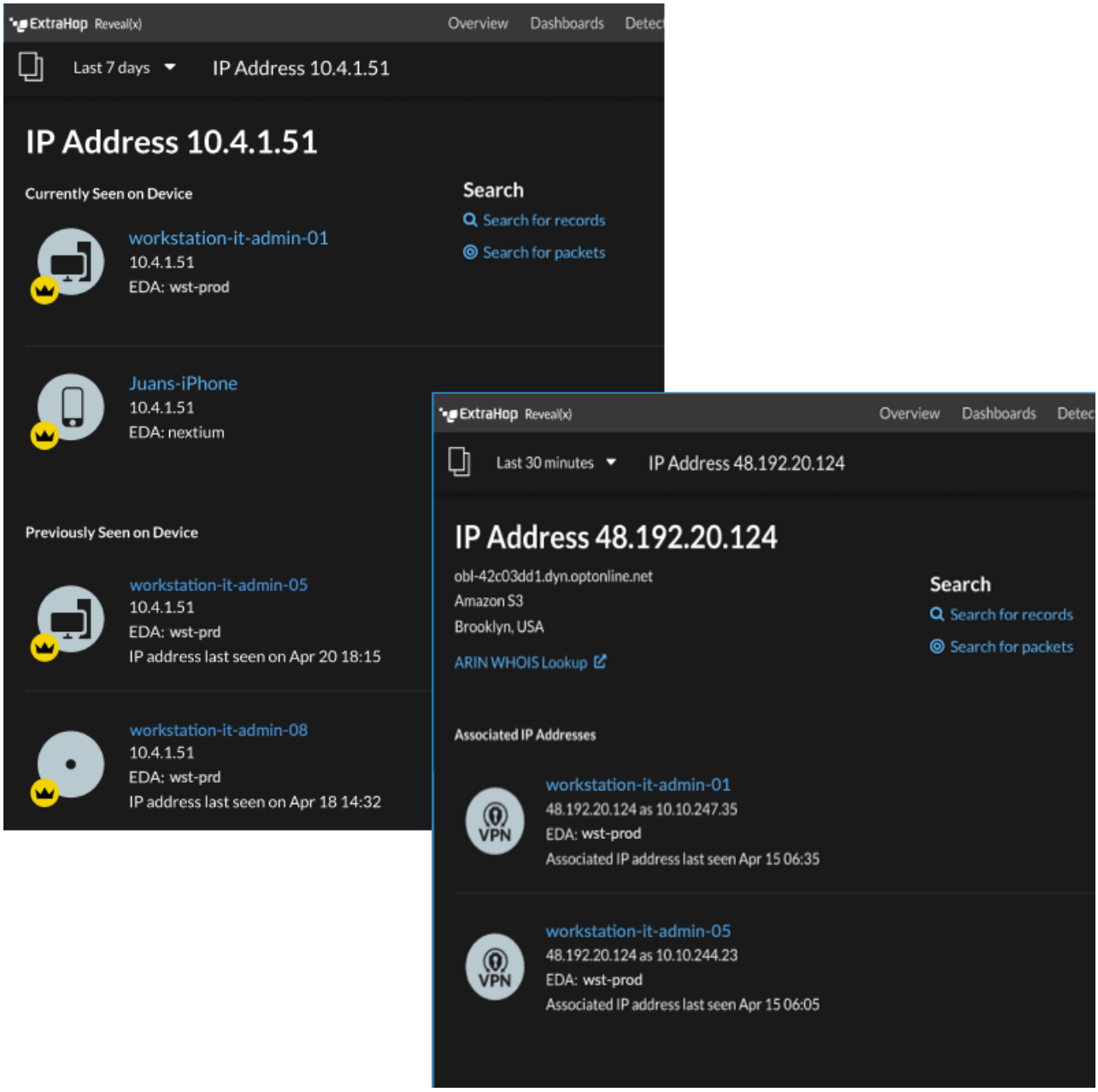
- Jedes Gerät, auf dem die IP-Adresse derzeit beobachtet wird, unabhängig vom ausgewählten Zeitintervall.
- Jedes Gerät, bei dem die IP-Adresse zuvor innerhalb des ausgewählten Zeitintervalls beobachtet wurde, einschließlich des Zeitstempel, ab dem die IP-Adresse zuletzt auf dem Gerät gesehen wurde.

Wenn L2-Entdeckung aktiviert ist, können sowohl IPv4- als auch IPv6-Adressen gleichzeitig auf dem Gerät beobachtet werden, oder es können dem Gerät im Laufe der Zeit unterschiedliche IP-Adressen von 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 kann 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 gesehen 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 die Seite mit der Geräteübersicht anzeigen.
- klicken **Suche nach Datensätzen** um eine zu starten Datensatzabfrage das wird nach der IP gefiltert .
- klicken **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 zusammenfassen. 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. Mit Gerätegruppen können Sie weiterhin Metriken für jedes einzelne Gerät oder Gruppenmitglied anzeigen. Die Messwerte für ein benutzerdefiniertes Gerät werden wie für ein einzelnes Gerät gesammelt und angezeigt. Sie können keine einzelnen Gerätemetriken anzeigen.

Sowohl Gerätegruppen als auch benutzerdefinierte Geräte können Metriken auf der Grundlage Ihrer angegebenen Kriterien dynamisch aggregieren. Wir empfehlen, zuverlässige Kriterien wie die IP-Adresse des Gerät, die MAC-Adresse, das VLAN, das Tag oder den 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	• Gerätenamen und Aliase • IP-Adresse, MAC-Adresse, Subnetz • Quell- und Zielport • Entdeckungszeit • Kritikalität des Geräts • Rolle des Geräts • Protokollaktivität • Externe Verbindungen • Anbieter, Modell, Software • Eigenschaften der Cloud-Instanz • VLAN • Geräte-Tags	• IP-Adresse • Bidirektionaler, eingehender oder ausgehender Datenverkehr • Peer-IP-Adresse • Quellport • Zielhafen • VLAN
Leistungskosten	Vergleichsweise niedrig. Da Gerätegruppen nur Metriken kombinieren, die bereits berechnet wurden, hat dies einen relativ geringen Effekt auf die Erfassung von Metrik. Bei einer hohen Anzahl von Gerätegruppen mit einer großen Anzahl von Geräten und komplexen Kriterien wird die Verarbeitung jedoch mehr Zeit in Anspruch nehmen.	Vergleichsweise hoch. Da die Metriken für benutzerdefinierte Geräte auf der Grundlage benutzerdefinierter Kriterien aggregiert werden, erfordert eine große Anzahl von benutzerdefinierten Geräten oder benutzerdefinierten Geräten mit extrem weit gefassten Kriterien mehr Verarbeitung. Benutzerdefinierte Geräte erhöhen auch die Anzahl der Systemobjekte, denen Metriken zugewiesen werden.
Metriken einzelner Gerät anzeigen	Ja	Nein
Bearbeitungssteuerung für Benutzer mit eingeschränktem Schreibzugriff	Ja Nutzer mit eingeschränkte Schreibrechte kann Gerätegruppen erstellen und bearbeiten. Diese globale	Nein

	Gerätegruppen	Maßgeschneiderte Geräte
	Berechtigungsrichtlinie muss in den Administrationseinstellungen aktiviert werden.	
Bewährte Verfahren	Erstellen Sie für lokale Geräte, auf denen Sie die Metriken in einem einzigen Diagramm anzeigen und vergleichen möchten. Gerätegruppen können als Metrik Quelle festgelegt werden.	Erstellen Sie es für Geräte, die sich außerhalb Ihres lokalen Netzwerk befinden, oder für Datenverkehrsarten, die Sie als eine einzige Quelle organisieren möchten. Beispielsweise möchten Sie möglicherweise alle physischen Schnittstellen auf einem Server als ein einziges benutzerdefiniertes Gerät definieren, um die Messwerte 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 über eine Gruppe von Geräten verfügen, für die Sie Messwerte zu einem einzigen Gerät zusammenfassen möchten. Bei diesen Geräten kann es sich sogar um unterschiedliche physische Schnittstellen handeln, die sich auf demselben Gerät befinden. Wenn Sie die Messwerte für diese Schnittstellen zusammenfassen, können Sie leichter nachvollziehen, wie stark Ihre physischen Ressourcen insgesamt belastet sind, und nicht anhand der einzelnen 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 entfernten Standort oder Cloud-Dienst aus zu sammeln. Du kannst Erfassen Sie Metriken von Remote-Standorten für benutzerdefinierte Geräte um zu erfahren, wie Dienste an entfernten Standorten genutzt werden, und um 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 Messwerte zu einem einzigen Gerät zusammengefasst, das L2-L7-Metriken erfasst. Ein einzelnes benutzerdefiniertes Gerät zählt als ein Gerät auf Ihre lizenzierte Kapazität für Erweiterte Analyse oder Standardanalyse, was es Ihnen ermöglicht ein benutzerdefiniertes Gerät zur Beobachtungsliste hinzufügen. Alle Auslöser oder Warnungen werden dem benutzerdefinierten Gerät ebenfalls als einzelnes Gerät zugewiesen.

Benutzerdefinierte Geräte aggregieren zwar Metriken auf der Grundlage ihrer definierten Kriterien, aber die Metrikberechnungen werden nicht genauso behandelt wie für erkannte Geräte. Angenommen, Sie haben einem benutzerdefinierten Gerät einen Auslöser zugewiesen, das Datensätze in einen Recordstore überträgt. 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 der Leitung entspricht.

Benutzerdefinierte Geräte können sich auf die Gesamtleistung des Systems auswirken. 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 von benutzerdefinierten Geräten die Leistung Ihres Systems 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 für mehrere Geräte verfolgen können, die normalerweise nach gemeinsamen Attributen wie Protokollaktivitäten gruppiert sind.

Du kannst eine statische Gerätegruppe erstellen das erfordert, dass Sie manuell ein Gerät 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. Sie können zum Beispiel Erstellen Sie eine dynamische Gerätegruppe basierend auf der Geräteerkennungszeit das fügt Geräte hinzu , die während eines bestimmten Zeitintervalls entdeckt wurden.

Standardmäßig enthält die Gerätegruppenseite die folgenden dynamischen Gerätegruppen, die Sie überschreiben oder löschen können:

Neue Geräte (letzte 24 Stunden)

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

Neue Geräte (letzte 7 Tage)

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

Das ExtraHop-System umfasst auch integrierte dynamische Gerätegruppen nach Rolle und Protokoll. Sie können integrierte Gerätegruppen als Metrikquelle für Objekte wie Diagramme, Benachrichtigungen, 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 CIFS-Clients, um die Seite Gerätegruppenübersicht aufzurufen. 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.

Die Erfassung von Metriken mit Gerätegruppen hat keine Auswirkungen auf die Leistung. Wir empfehlen Ihnen jedoch, priorisieren Sie diese Gruppen durch ihre Bedeutung, sicherzustellen, dass die richtigen Geräte den höchsten Analysegrad erhalten.

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

Durch das Erstellen einer Gerätegruppe können Sie all diese Geräte als eine einzige Metrik Quelle verwalten, anstatt sie als einzelne Quellen zu Ihren Diagrammen hinzuzufügen. Beachten Sie jedoch, dass alle zugewiesenen Auslöser oder Benachrichtigungen jedem Gruppenmitglied (oder 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

Je nach Art des Datenverkehrs, der dem Gerät oder dem Gerätemodell zugeordnet 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 beobachtete Traffic- und Verhaltensänderungen beobachtet werden. Wenn beispielsweise ein PC in einen Server umfunktioniert wurde, können Sie die Rolle sofort ändern, oder die Änderung wird im Laufe der Zeit beobachtet 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. Die benutzerdefinierte Rolle kann einem Gerät nicht manuell zugewiesen werden.
	Angriffssimulator	Ein Gerät, auf dem Software zur Breach- und Angriffssimulation (BAS) ausgeführt wird, um Angriffe in einem Netzwerk zu simulieren.
	Datenbank	Ein Gerät, das hauptsächlich eine Datenbankinstanz hostet.

Ikone	Rolle	Beschreibung
	DHCP-Server	Ein Gerät, das hauptsächlich DHCP-Serveraktivitäten verarbeitet.
	DNS-Server	Ein Gerät, das hauptsächlich DNS-Serveraktivitäten verarbeitet.
	Domänencontroller	Ein Gerät, das als Domänencontroller für Kerberos-, CIFS- und MSRPC-Serveraktivitäten fungiert.
	Dateiserver	Ein Gerät, das auf Lese- und Schreibanforderungen für Dateien über NFS - und CIFS/SMB-Protokolle reagiert.
	Brandmauer	Ein Gerät, das den eingehenden und ausgehenden Netzwerkverkehr überwacht und den Datenverkehr gemäß den Sicherheitsregeln blockiert. Das ExtraHop-System weist Geräten diese Rolle nicht automatisch zu.
	Tor	Ein Gerät, das als Router oder Gateway fungiert. Das ExtraHop-System sucht bei der Identifizierung von Gateways nach Geräten, denen eine große Anzahl an eindeutigen IP-Adressen zugeordnet ist (ab einem bestimmten Schwellenwert). Gateway-Gerätenamen enthalten den Routernamen wie Cisco B1B500. Im Gegensatz zu anderen L2-Elterngeräte, du kannst ein Gateway-Gerät zur Beobachtungsliste hinzufügen für erweiterte Analysen.

Ikone	Rolle	Beschreibung
	IP-Kamera	Ein Gerät, das Bild- und Videodaten über das Netzwerk sendet. Das ExtraHop-System weist diese Rolle basierend auf dem Gerätemodell zu.
	Load Balancer	Ein Gerät, das als Reverse-Proxy für die Verteilung des Datenverkehrs auf mehrere Server fungiert.
	Medizinisches Gerät	Ein Gerät, das für Gesundheitsbedürfnisse und medizinische Umgebungen entwickelt wurde. Das ExtraHop-System weist diese Rolle möglicherweise zu, wenn es sich bei einem Gerät um eine bekannte medizinische Marke und ein bekanntes medizinisches Modell handelt oder wenn das Gerät DICOM-Verkehr verarbeitet.
	Mobilgerät	Ein Gerät, auf dem ein mobiles Betriebssystem installiert ist, z. B. iOS oder Android.
	NAT-Schnittstelle	Ein Gerät, das als Network Address Translation (NAT) -Gateway fungiert. Das ExtraHop-System weist diese Rolle möglicherweise zu, 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 Geräteeigenschaften für Software, Hardwaremarke und -modell sowie authentifizierte Benutzer nicht mehr für das Gerät angezeigt.

Ikone	Rolle	Beschreibung
	PC	Ein Gerät wie ein Laptop, ein Desktop, eine Windows-VM oder ein macOS-Gerät, das DNS-, HTTP- und SSL-Clientdatenverkehr 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 über mDNS beobachteten Datenverkehrs (Multicast-DNS) 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, weist das ExtraHop-System 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 von externen VPN-Peers zu, wenn die automatische Klassifizierung für diese Rolle in der laufenden Konfigurationsdatei aktiviert ist.
	Schwachstellen-Scanner	Ein Gerät, auf dem Programme zum Schwachstellenscanner ausgeführt werden.

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