Finde ein Gerät

Veröffentlicht: 2025-02-04

Das ExtraHop-System erkennt automatisch Geräte wie Clients, Server, Router, Load Balancer und Gateways, die aktiv über das Kabel mit anderen Geräten kommunizieren. Sie können auf dem System nach einem bestimmten Gerät suchen und dann die Verkehrs- und Protokollmetriken auf einer Protokollseite anzeigen.

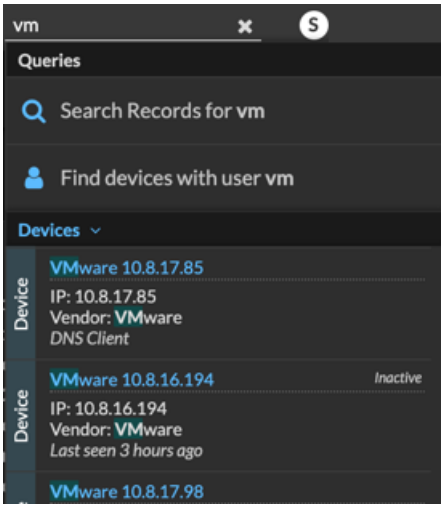
Es gibt mehrere Möglichkeiten, nach einem Gerät zu suchen:

- Finden Sie Geräte über eine globale Suche
- Geräte anhand von Details finden
- Finden Sie Geräte mit AI Search Assistant
- Finden Sie Geräte mit Suchvorschlägen
- Geräte anhand der Erkennungsaktivität finden
- Geräte anhand der Protokollaktivität finden
- Finden Sie Geräte, auf die ein bestimmter Benutzer zugegriffen hat
- Finden Sie Peer-Geräte

Finden Sie Geräte über eine globale Suche

Sie können über das globale Suchfeld oben auf der Seite nach Geräten suchen. Die globale Suche vergleicht einen Suchbegriff mit mehreren Geräteeigenschaften wie Hostname, IP-Adresse, bekanntem Alias, Anbieter, Tag, Beschreibung und Gerätegruppe. Wenn Sie beispielsweise nach dem Begriff suchen `vm`, in den Suchergebnissen werden möglicherweise Geräte angezeigt, die Folgendes enthalten `vm` im Gerätenamen, Gerätehersteller oder Geräte-Tag.

1. Geben Sie einen Suchbegriff in das globale Suchfeld oben auf der Seite ein.
2. Klicken Sie **Beliebiger Typ** und wählen Sie dann **Geräte**.
   Die Suchergebnisse werden in einer Liste unter dem Suchfeld angezeigt. Klicken Sie **Mehr Ergebnisse** um durch die Liste zu blättern.



Passende Geräte, die während des angegebenen Zeitintervalls keine Aktivität hatten, haben die Bezeichnung Inaktiv.

Hinweis: Geräte, die länger als 90 Tage inaktiv sind, werden von den globalen Suchergebnissen ausgeschlossen. Sie können jedoch sofort schließt alle Geräte aus, die seit weniger als 90 Tagen inaktiv waren über die Administrationseinstellungen.

3. Klicken Sie auf einen Gerätenamen, um das zu öffnen Seite „ Geräteübersicht“ und Geräteeigenschaften und Messwerte anzeigen.

Geräte anhand von Details finden

Sie können anhand von Informationen, die über das Kabel beobachtet wurden, wie IP-Adresse, MAC-Adresse, Hostname oder Protokollaktivität, nach Geräten suchen. Sie können auch anhand benutzerdefinierter Informationen wie Geräte-Tags nach Geräten suchen.

Mit dem Dreifeld-Suchfilter können Sie nach mehreren Kategorien gleichzeitig suchen. Sie können beispielsweise Filter für Gerätename, IP-Adresse und Rolle hinzufügen, um Ergebnisse für Geräte anzuzeigen, die alle angegebenen Kriterien erfüllen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
3. Optional: Falls angezeigt, klicken Sie auf **Standardsuche**.
4. Klicken Sie im Dreifeld-Filter auf **Name** und wählen Sie eine der folgenden Kategorien aus:

Option	Description
Name	Filtert Geräte nach dem erkannten Gerätenamen. Ein ermittelter Gerätename kann beispielsweise die IP-Adresse oder den Hostnamen enthalten.
MAC-Adresse	Filtert Geräte nach der MAC-Adresse des Gerät.
IP Adresse	Filtert Geräte nach IP-Adresse in den Blockformaten IPv4, IPv6 oder CIDR.
Standort	Filtert Geräte, die einer verbundenen Standort zugeordnet sind. Nur Konsole.
Zeit für Entdeckungsreisen	Filtert Geräte, die vom ExtraHop-System innerhalb des angegebenen Zeitintervalls automatisch erkannt werden. Weitere Informationen finden Sie unter Erstellen Sie eine Gerätegruppe basierend auf der Erkennungszeit.
Analyseebene	Filtert Geräte nach Analyseebene, die bestimmt, welche Daten und Metriken für ein Gerät erfasst werden. Sie können keine dynamische Gerätegruppe für Geräte erstellen, die nach Analyseebene gefiltert sind.
Modell	Filtert Geräte nach Marke, Familie oder Modellname. Die Marke steht für den Hersteller des Gerät. Eine Familie steht für eine Gruppierung, z. B. eine Produktlinie. Die folgenden Tipps können Ihnen helfen, das gewünschte Gerätemodell zu finden:

Option	Description
	• Sie können aus einer Liste von Marken auswählen, die in Ihrem ExtraHop-System gefunden wurden, und dann auf den Filter klicken, um die Ergebnisse zu verfeinern. • Sie können Hovertips neben Marken und Produktfamilien anzeigen, um zu sehen, wie viele Geräte und passende Modelle gefunden wurden. • Sie können eine Marke oder eine Familie auswählen, um alle Geräte in dieser Gruppe zu finden, unabhängig vom Modell.
Cloud-aktualisierte Eigenschaften	Filtert Geräte nach Cloud-aktualisierten Eigenschaften, die abgerufen wurden von Integrationen die auf Ihrem ExtraHop-System wie CrowdStrike konfiguriert sind. Der Filtername ist der Anbieter oder Partner, der mit der Integration verknüpft ist. Cloud-aktualisierte Eigenschaften variieren je nach Integration.
Aktivität	Filtert Geräte nach Protokollaktivität, die dem Gerät zugeordnet ist. Wenn Sie beispielsweise HTTP-Server auswählen, werden Geräte mit HTTP-Server-Metriken und jedes andere Gerät zurückgegeben, dessen Geräterolle auf HTTP-Server festgelegt ist. Filtert auch Geräte, die eine externe Verbindung akzeptiert oder initiiert haben, sodass Sie feststellen können, ob Geräte verdächtige Aktivitäten ausführen.
SHA-256-Datei-Hash	Filtert Geräte, auf denen Dateien beobachtet wurden, die mit dem SHA-256-Hashing-Algorithmus gehasht wurden. Sie können eine Tabelle mit Hash-Dateien auf der Seite „Dateien“.
Hoher Wert	Filtert Geräte, die als hoher Wert eingestuft werden, weil sie Authentifizierungsdienste bereitstellen, wichtige Dienste in Ihrem Netzwerk unterstützen oder die vom Benutzer als hochwertig eingestuft wurden.
Derzeit aktiv	Filtert Geräte nach Aktivitäten, die in den letzten 30 Minuten auf einem Gerät beobachtet wurden.
Netzwerk-Lokalitätstyp	Filtert Geräte nach allen internen oder externen Netzwerkstandorten.
Name der Netzwerklokalität	Filtert Geräte nach dem Namen der Netzwerklokalität.
Rolle	Filtert Geräte nach der zugewiesenen Geräterolle wie Gateway, Firewall, Load Balancer und DNS-Server.

Option	Description
Software	Filtert Geräte nach der auf dem Gerät erkannten Betriebssystemsoftware.
Art der Software	Filtert Geräte nach der Art der auf dem Gerät beobachteten Software, z. B. Angriffssimulator, Fernzugriff oder Datenbankserver.
Schlagwort	Filtert Geräte nach benutzerdefinierten Geräte-Tags.
Verkäufer	Filtert Geräte nach dem Namen des Geräteherstellers, der durch die OUI-Suche (Organizationally Unique Identifier) ermittelt wurde.
Cloud-Konto	Filtert Geräte nach dem Cloud-Dienstkonto, das dem Gerät zugeordnet ist. Verfügbar , wenn du Fügen Sie Cloud-Instanzeigenschaften über die REST-API hinzu.
Cloud-Instanz-ID	Filtert Geräte nach der Cloud-Instanz-ID, die dem Gerät zugeordnet ist. Verfügbar, wenn du Fügen Sie Cloud-Instanzeigenschaften über die REST-API hinzu.
Name der Cloud-Instanz	Filtert Geräte nach dem Cloud-Instanznamen, der dem Gerät zugewiesen ist. Verfügbar, wenn du Fügen Sie Cloud-Instanzeigenschaften über die REST-API hinzu.
Cloud-Instanztyp	Filtert Geräte nach dem Cloud-Instanztyp, der dem Gerät zugeordnet ist. Verfügbar, wenn du Fügen Sie Cloud-Instanzeigenschaften über die REST-API hinzu.
Cloud-Subnetz-ID	Filtert Geräte nach der Cloud-Subnetz-ID, die dem Gerät zugeordnet ist. Verfügbar, wenn du Fügen Sie Cloud-Instanzeigenschaften über die REST-API hinzu.
Virtuelle private Cloud	Filtert Geräte nach der VPC, die dem Gerät zugeordnet ist. Verfügbar, wenn du Fügen Sie Cloud-Instanzeigenschaften über die REST-API hinzu.
VLAN	Filtert Geräte nach dem Geräte-VLAN-Tag. VLAN-Informationen werden aus VLAN-Tags extrahiert, wenn der Datenverkehrsspiegelungsprozess sie auf dem Spiegelport beibehält. Nur verfügbar, wenn `devices_accross_vlans` Einstellung ist gesetzt auf `False` in der laufenden Konfigurationsdatei.

Option	Description
CDP-Name	Filtert Geräte nach dem CDP-Namen, der dem Gerät zugewiesen ist.
Benutzerdefinierter Name	Filtert Geräte nach dem benutzerdefinierten Namen, der dem Gerät zugewiesen wurde.
DHCP-Name	Filtert Geräte nach dem DHCP-Namen, der dem Gerät zugewiesen ist.
DNS-Name	Filtert Geräte nach einem beliebigen DNS-Namen, der dem Gerät zugewiesen ist.
NetBIOS-Name	Filtert Geräte nach dem NetBIOS-Namen, der dem Gerät zugewiesen ist.
Erkennungsaktivität	Filtert Geräte mit Erkennungsaktivität wo das Gerät ein Teilnehmer war. Aktiviert zusätzliche Kriterien wie Kategorie, Risikoscore und MITRE-Technik. **Hinweis** Sie können keine Gerätegruppe erstellen, die diese Kriterienoption enthält.

5. Wählen Sie einen der folgenden Operatoren aus. Die verfügbaren Operatoren hängen von der ausgewählten Kategorie ab:

Option	Description
=	Filtert Geräte, die exakt dem Suchfeld für die ausgewählte Kategorie entsprechen.
≈	Filtert Geräte, die nicht genau dem Suchfeld entsprechen.
≈	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie enthalten.
≈/	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie ausschließen.
beginnt mit	Filtert Geräte, die mit dem Wert des Suchfeldes für die ausgewählte Kategorie beginnen.
existiert	Filtert Geräte, die einen Wert für die ausgewählte Kategorie haben.
existiert nicht	Filtert Geräte, die keinen Wert für die ausgewählte Kategorie haben.
Spiel	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie enthalten.
und	Filtert Geräte, die den in zwei oder mehr Suchfeldern angegebenen Bedingungen entsprechen.
oder	Filtert Geräte, die mindestens eine in zwei oder mehr Suchfeldern angegebene Bedingung erfüllen.
nicht	Filtert Geräte, die die in einem Suchfeld angegebenen Bedingungen nicht erfüllen.

6. Geben Sie im Suchfeld die Zeichenfolge ein, die abgeglichen werden soll, oder wählen Sie einen Wert aus dem Dropdownmenü aus. Der Eingabetyp basiert auf der ausgewählten Kategorie.

   Wenn Sie beispielsweise Geräte anhand des Namens suchen möchten, geben Sie die Zeichenfolge, die abgeglichen werden soll, in das Suchfeld Feld. Wenn Sie Geräte anhand der Rolle suchen möchten, wählen Sie aus dem Dropdownmenü der Rollen aus.

   Hinweis: Abhängig von der ausgewählten Kategorie können Sie im Textfeld auf das Regex-Symbol klicken, um den Abgleich per regulärem Ausdruck zu aktivieren.

7. Klicken Sie **Filter hinzufügen**.
   Die Geräteliste wird nach den angegebenen Kriterien gefiltert.

Nächste Schritte

- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf der Seite „ Geräteübersicht“.
- Klicken Sie **Dynamische Gruppe erstellen** von der oberen rechten Ecke bis eine dynamische Gerätegruppe erstellen basierend auf den Filterkriterien.
- Klicken Sie auf das Befehlsmenü ⋮ und wählen Sie dann PDF oder CSV, um die Geräteliste in eine Datei zu exportieren.

Finden Sie Geräte mit AI Search Assistant

Mit dem AI Search Assistant können Sie nach Geräten suchen, deren Fragen in natürlicher, alltäglicher Sprache verfasst sind. So können Sie im Vergleich zur Erstellung einer Standard-Suchanfrage mit denselben Kriterien schnell komplexe Abfragen erstellen.

Wenn Sie beispielsweise „Welche Geräte haben HTTP-Verkehr mit TLS v1.0?“ eingeben , die folgende AI Search Assistant-Abfrage wird angezeigt:

```
(Detection Activity where  Device Role = As Participant and  Type =
 Deprecated SSL/TLS Versions )
```

Hier sind einige Dinge, die Sie bei der Suche nach Geräten mit AI Search Assistant beachten sollten:

- Eingabeaufforderungen sind demselben zugeordnet Filterkriterien für Gerät die Sie beim Erstellen einer Standardsuche angeben. Das ExtraHop-System ist möglicherweise nicht in der Lage, eine Abfrage zu verarbeiten, die Anfragen nach Geräteinformationen enthält, die außerhalb der Kriterien liegen.
- Die Eingabeaufforderungen können absolute und relative Zeitbereiche enthalten, z. B. „Welches meiner Geräte war diese Woche an blockierten Datenübertragungen beteiligt?“. Das aktuelle Jahr wird verwendet, wenn ein Jahr nicht im Datum enthalten ist.
- Die Eingabeaufforderungen sollten so klar und präzise wie möglich sein. Wir empfehlen Ihnen, einige Variationen zu schreiben, um Ihre Ergebnisse zu maximieren.
- Das ExtraHop-System kann Benutzeranweisungen zur Produktverbesserung speichern. Wir empfehlen, dass Sie in Ihren Eingabeaufforderungen keine urheberrechtlich geschützten oder vertraulichen Daten angeben.
- Sie können die Abfragefilterkriterien bearbeiten, um die Suchergebnisse zu verfeinern.

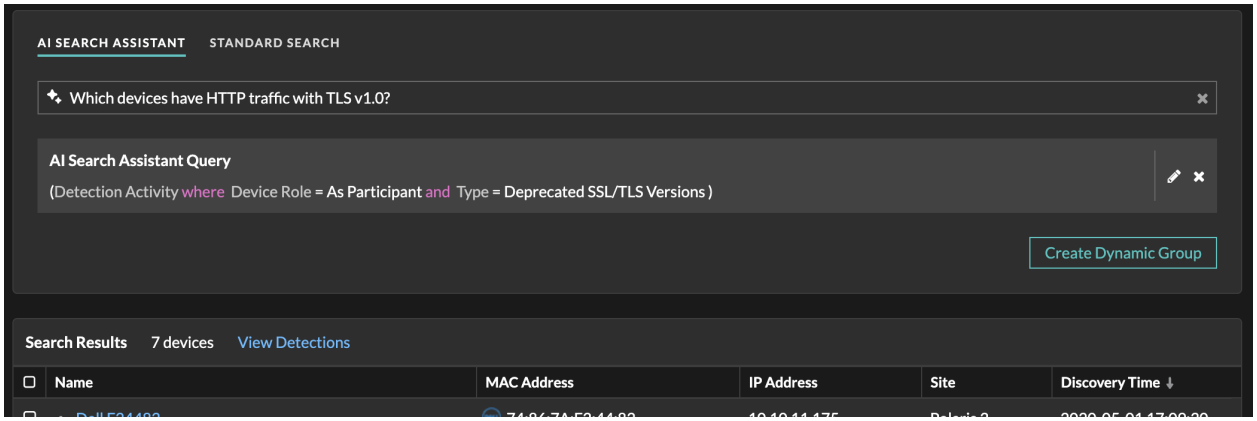
Bevor Sie beginnen

- Ihr ExtraHop-System muss verbunden mit ExtraHop Cloud Services.
- Der AI Search Assistant muss von Ihrem ExtraHop-Administrator aktiviert werden.

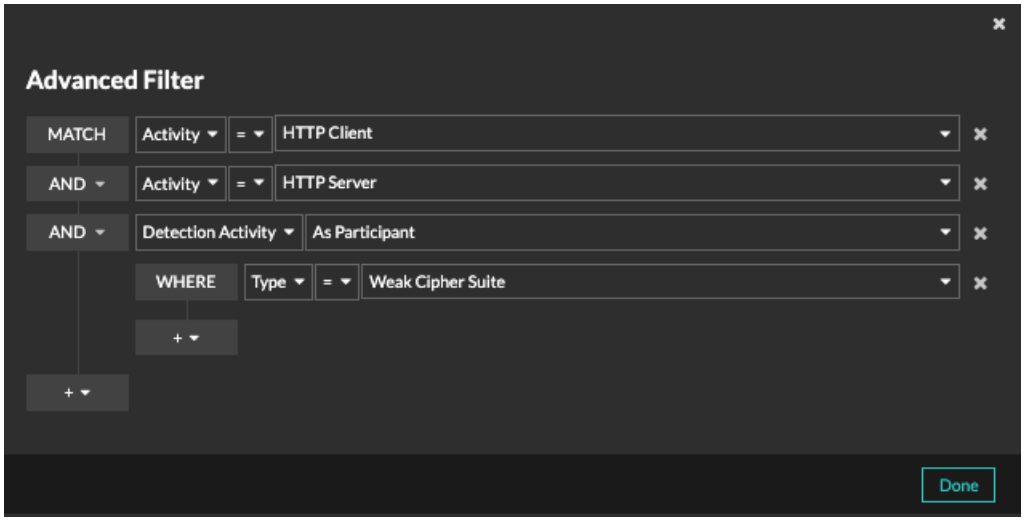
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte**.
3. Schreiben Sie eine Aufforderung in das Feld AI Search Assistant und drücken Sie die EINGABETASTE.

   Hinweis: Klicken Sie auf das Suchaufforderungsfeld, um eine aktuelle Abfrage oder eine vorgeschlagene Suche auszuwählen.

   Die Abfrageausgabe des AI Search Assistant und die Ergebnisliste werden angezeigt.



4. Optional: Klicken Sie im Abschnitt AI Search Assistant Query auf das Bearbeitungssymbol um das Fenster Erweiterter Filter zu öffnen und Ihre Abfragefilterkriterien zu verfeinern.



   a) Klicken Sie auf das Symbol „Filter hinzufügen“ + und wähle **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

      Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach HTTP-Clients und -Servern suchen, die an Erkennungen einer Schwache Verschlüsselung Suite beteiligt waren , können Sie eine Filtergruppe hinzufügen, um Erkennungen mit einer Risikoscore unter 30 auszuschließen.

   b) Klicken Sie **Erledigt**.

Nächste Schritte

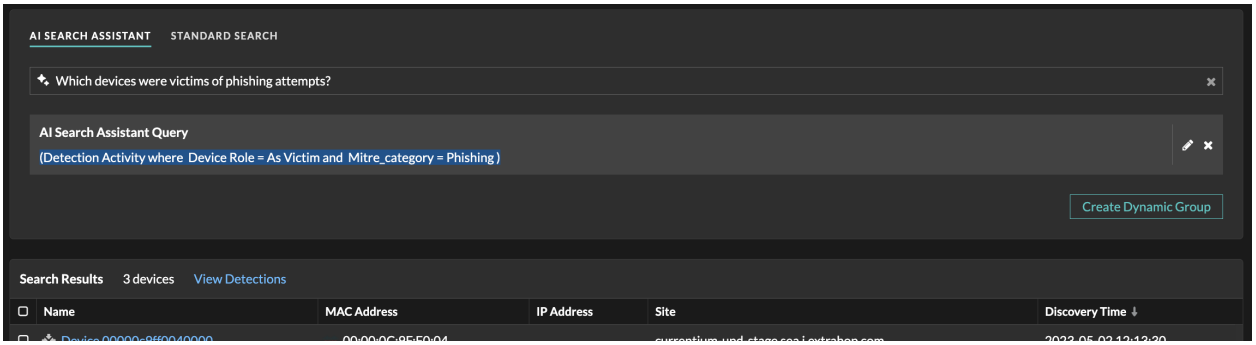
- Klicken Sie **Erkennungen anzeigen** um zur Seite „Entdeckungen“ zu navigieren; der Gerätefilter wird auf die Zusammenfassung der Erkennungen angewendet. Klicken Sie **Erweiterter Gerätefilter** um Filterkriterien anzuzeigen und zu bearbeiten.
- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf der Seite „ Geräteübersicht“ .
- Klicken Sie auf das Befehlsmenü ⋮ und wählen Sie dann PDF oder CSV, um die Geräteliste in eine Datei zu exportieren.

Finden Sie Geräte mit Suchvorschlägen

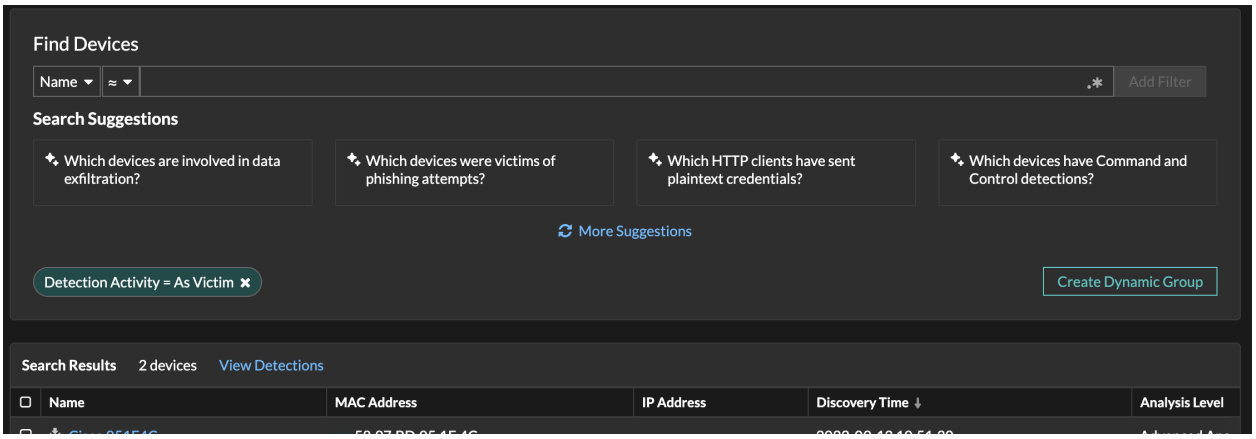
Das ExtraHop-System bietet mehrere Suchvorschläge mit vorgefertigten Filtern, mit denen Sie häufig verwendete Gerätesuchen effizienter durchführen können. Nachdem Sie eine vorgeschlagene Suche ausgewählt haben, können Sie die Filterkriterien bearbeiten, um Ihre Ergebnisse zu verfeinern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte**.
3. Klicken Sie auf eine vorgeschlagene Suchaufforderung.

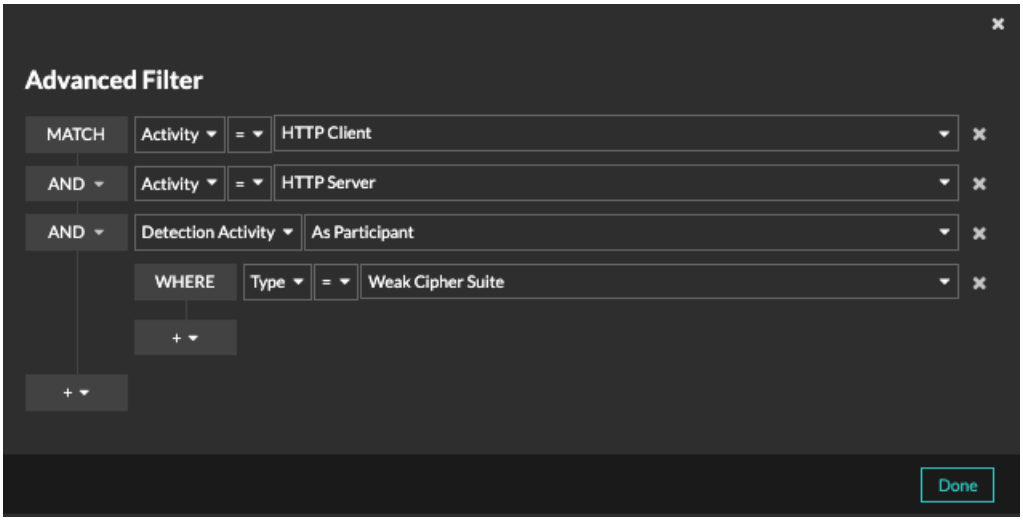
   Wenn AI Search Assistant aktiviert ist, werden Filterkriterien im Abfragefeld AI Search Assistant angezeigt.



   Andernfalls zeigt die Seite den Standardfilter an.



4. Optional: Klicken Sie im Abfragefeld des AI Search Assistant auf das Bearbeitungssymbol oder klicken Sie auf den Standardfilter , um das Fenster Erweiterter Filter zu öffnen und Ihre Abfrage zu verfeinern.



a) Klicken Sie auf das Symbol „Filter hinzufügen“ + und wähle **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

   Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach HTTP-Clients und -Servern suchen, die an Erkennungen einer Schwache Verschlüsselung Suite beteiligt waren , können Sie eine Filtergruppe hinzufügen, um Erkennungen auszuschließen, deren Risikoscore unter 30 liegt.

b) Klicken Sie **Erledigt**.

Nächste Schritte

- Klicken Sie **Erkennungen anzeigen** um zur Seite „Entdeckungen“ zu navigieren; der Gerätefilter wird auf die Zusammenfassung der Erkennungen angewendet. Klicken Sie **Erweiterter Gerätefilter** um Filterkriterien anzuzeigen und zu bearbeiten.
- Klicken Sie **Dynamische Gruppe erstellen** von der oberen rechten Ecke bis eine dynamische Gerätegruppe erstellen basierend auf den Filterkriterien.
- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf der Seite „ Geräteübersicht“.
- Klicken Sie auf das Befehlsmenü ⋮ und wählen Sie dann PDF oder CSV, um die Geräteliste in eine Datei zu exportieren.

Geräte anhand der Erkennungsaktivität finden

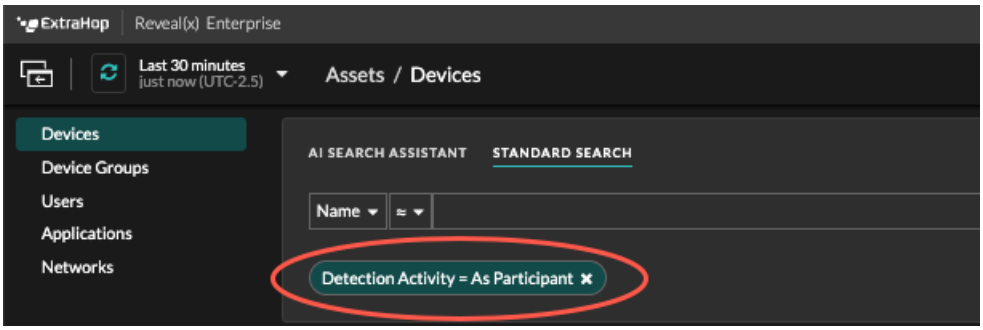
Sie können anhand der zugehörigen Erkennungen nach Geräten suchen, indem Sie Ihrem Suchfilter die Option Kriterien für Erkennungsaktivitäten hinzufügen und Ihre Suche dann mit Kriterien wie Erkennungskategorien, Risikobewertungen und MITRE-Techniken weiter verfeinern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
3. Optional: Klicken Sie **Standard-Suche** wenn die Registerkarte angezeigt wird.
4. Klicken Sie im Dreifeld-Filter auf **Name** und wähle **Erkennungsaktivität**.
5. Klicken Sie **Wählen Sie einen Artikel aus...** und wählen Sie eine der folgenden Optionen:

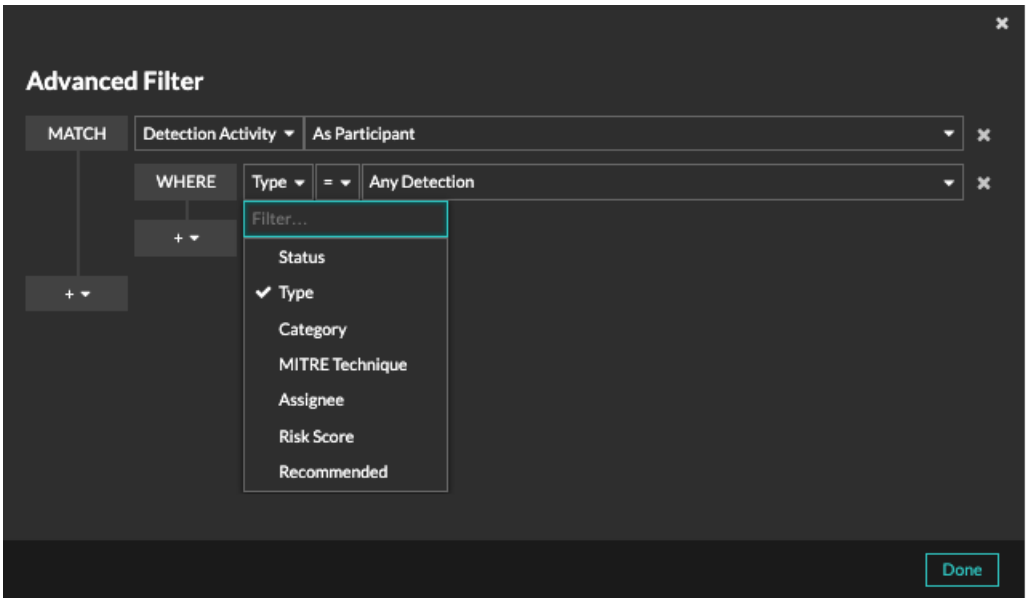
Option	Description
Als Teilnehmer	Filtert Geräte, die an einer Erkennung teilgenommen haben.

Option	Description
Als Täter	Filtert Geräte, die nur an einer Erkennung als Täter beteiligt waren.
Als Opfer	Filtert Geräte, die nur als Opfer an einer Erkennung teilgenommen haben.

6. Klicken Sie **Filter hinzufügen**.
7. Optional: Um zusätzliche Kriterien für die Erkennungsaktivität anzugeben, klicken Sie auf den Filter, den Sie gerade hinzugefügt haben.



Der erweiterte Filter wird geöffnet und zeigt die von Ihnen hinzugefügten MATCH-Kriterien an. Ein WHERE-Operator wird automatisch auf der sekundären Ebene des Filters für Erkennungsaktivitätskriterien hinzugefügt.



8. Klicken Sie **Typ** und wählen Sie eines der folgenden Kriterien für Erkennungsaktivitäten aus:

Option	Description
Status	Filtert Erkennungen nach Status, z. B. ob die Erkennung bestätigt oder geschlossen wurde
Typ	Filtert Erkennungen nach Typ, z. B. Datenexfiltration oder abgelaufene TLS-Serverzertifikate.

Option	Description
Kategorie	Filtert Erkennungen nach Kategorien, z. B. Angriff, Betrieb, Absicherung und Eindringen.
MITRE-Technik	Filtert Erkennungen nach der MITRE-Technik-ID. Das MITRE-Framework ist eine weithin anerkannte Wissensdatenbank für Angriffe.
Abtretungsempfänger	Filtert Erkennungen nach dem zugewiesenen Benutzer.
Risiko-Score	Filtert Erkennungen nach Risikoscore.
Empfehlenswert	Filtert Erkennungen, die für die Triage empfohlen werden, auch bekannt als Smart Triage. (nur NDR-Modul)

siehe Erkennungen filtern für weitere Informationen zu den Kriterien für Erkennungsaktivitäten.

9. Optional: Klicken Sie auf das Symbol „Filter hinzufügen“ und wähle **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

   Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach Geräten suchen, die in der Kategorie „Datenexfiltration“ als Straftäter gehandelt haben, können Sie eine Filtergruppe hinzufügen, um Erkennungen mit dem Status „ Geschlossen“ aus diesen Ergebnissen auszuschließen.
10. Klicken Sie **Speichern**.

Nächste Schritte

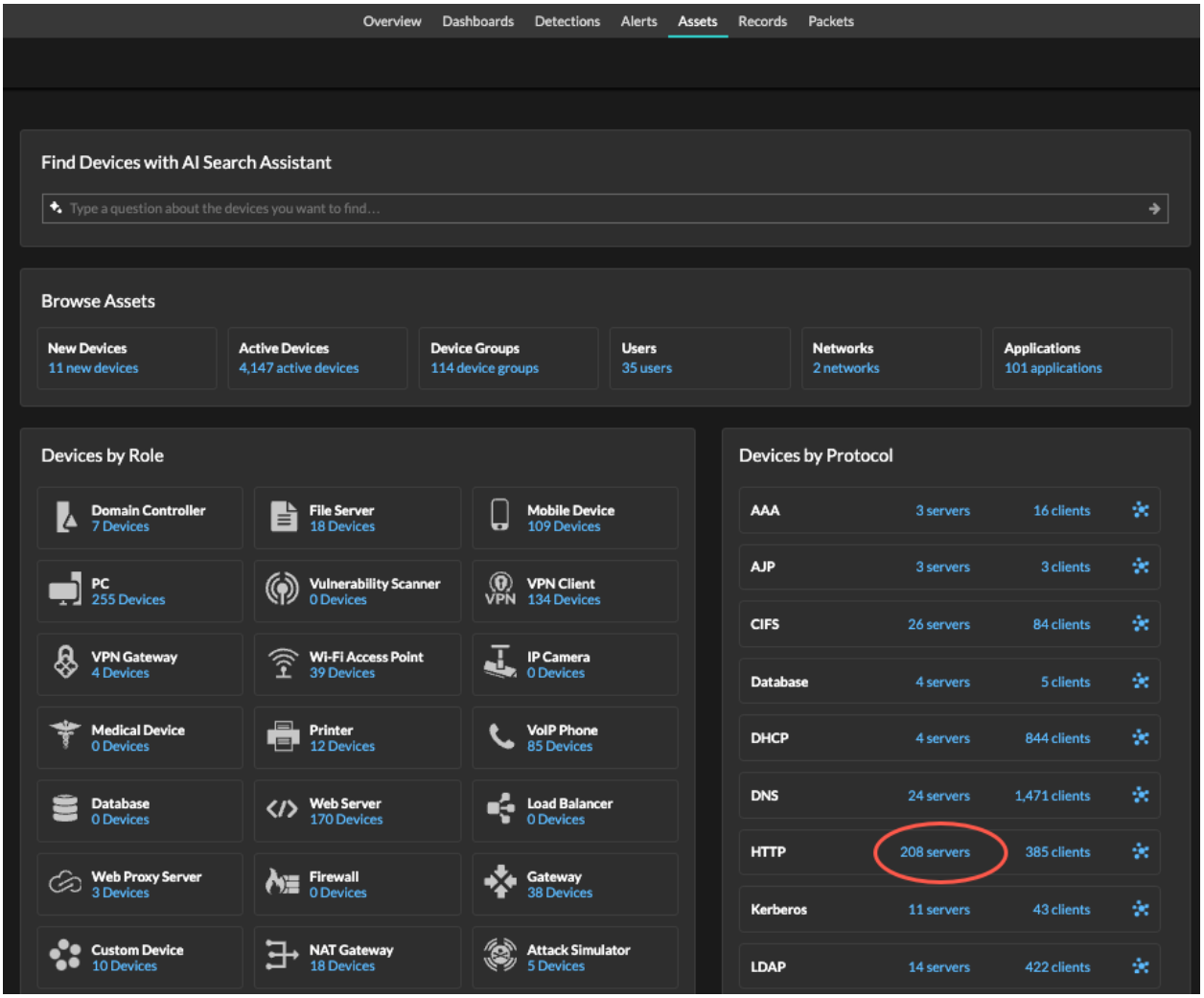
- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf der Seite „ Geräteübersicht“.
- Klicken Sie auf das Befehlsmenü ⋮ und wählen Sie dann PDF oder CSV, um die Geräteliste in eine Datei zu exportieren.

Geräte anhand der Protokollaktivität finden

Auf der Seite Geräte werden alle Protokolle angezeigt, die während des ausgewählten Zeitintervalls aktiv auf dem ExtraHop-System kommunizieren. Sie können schnell ein Gerät finden, das mit einem Protokoll verknüpft ist, oder ein stillgelegtes Gerät erkennen, das immer noch aktiv über ein Protokoll kommuniziert.

Im folgenden Beispiel zeigen wir Ihnen, wie Sie innerhalb der Gruppe der HTTP-Server nach einem Webserver suchen.

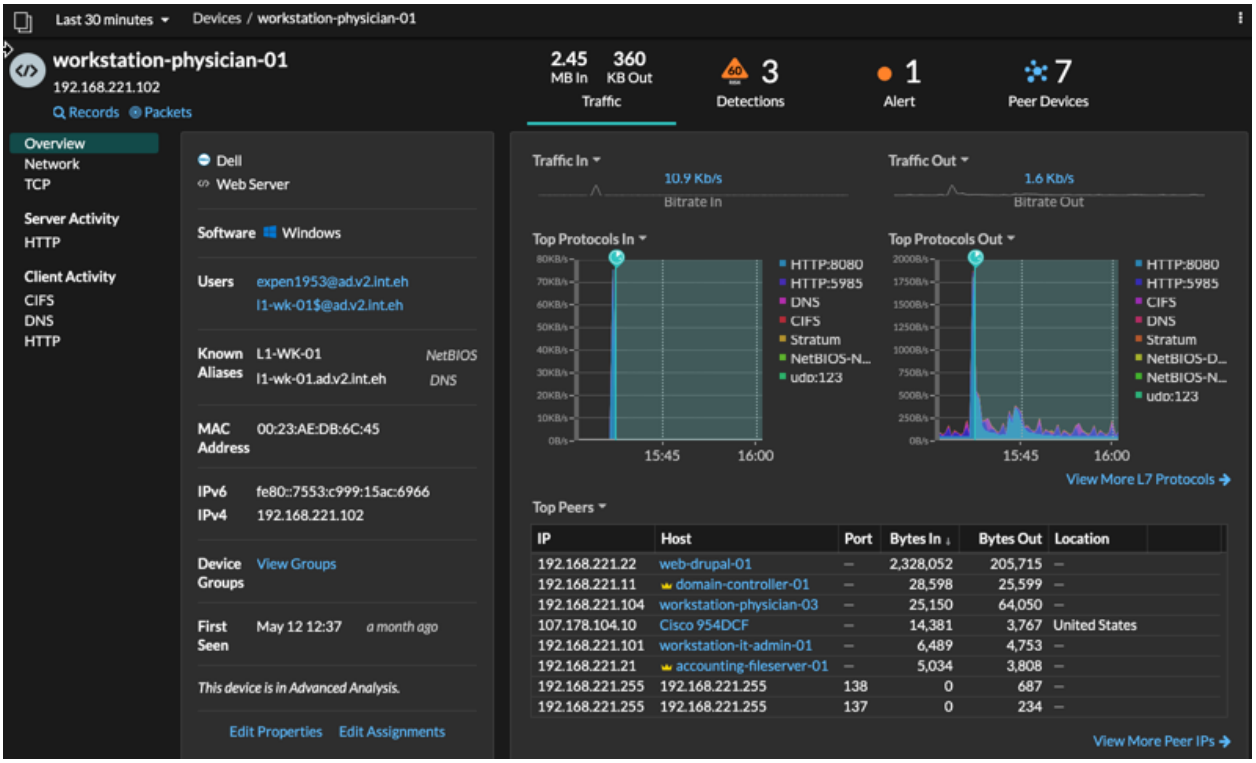
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte**.
3. Klicken Sie im Diagramm Geräte nach Protokollaktivität auf die Anzahl der HTTP-Server, wie in der folgenden Abbildung dargestellt.



Hinweis: Wenn Sie das gewünschte Protokoll nicht sehen, hat das ExtraHop-System diese Art von Protokollverkehr über die Leitung während des angegebenen Zeitintervalls möglicherweise nicht beobachtet, oder für das Protokoll ist möglicherweise eine Modullizenz erforderlich. Weitere Informationen finden Sie in der Ich sehe nicht den Protokollverkehr, den ich erwartet hatte? Abschnitt in den Häufig gestellten Fragen zur Lizenz.

Auf der Seite werden Verkehrs- und Protokollmetriken angezeigt, die der Gruppe von HTTP-Servern zugeordnet sind.

4. Klicken Sie oben auf der Seite auf **Mitglieder der Gruppe**.
   Auf der Seite wird eine Tabelle mit allen Geräten angezeigt, die während des ausgewählten Zeitintervalls HTTP-Antworten über die Leitung gesendet haben.
5. Klicken Sie in der Tabelle auf einen Gerätenamen.
   Auf der Seite werden Verkehrs- und Protokollmetriken angezeigt, die mit diesem Gerät verknüpft sind, ähnlich der folgenden Abbildung.



Finden Sie Geräte, auf die ein bestimmter Benutzer zugegriffen hat

Auf der Seite Benutzer können Sie aktive Benutzer und die Geräte sehen, mit denen sie sich während des angegebenen Zeitintervalls am ExtraHop-System angemeldet haben.

Hinweis: Du kannst auch Suche nach Benutzern aus dem globalen Suchfeld oben auf der Seite.

Dieses Verfahren zeigt Ihnen, wie Sie eine Suche von der Benutzerseite aus durchführen.

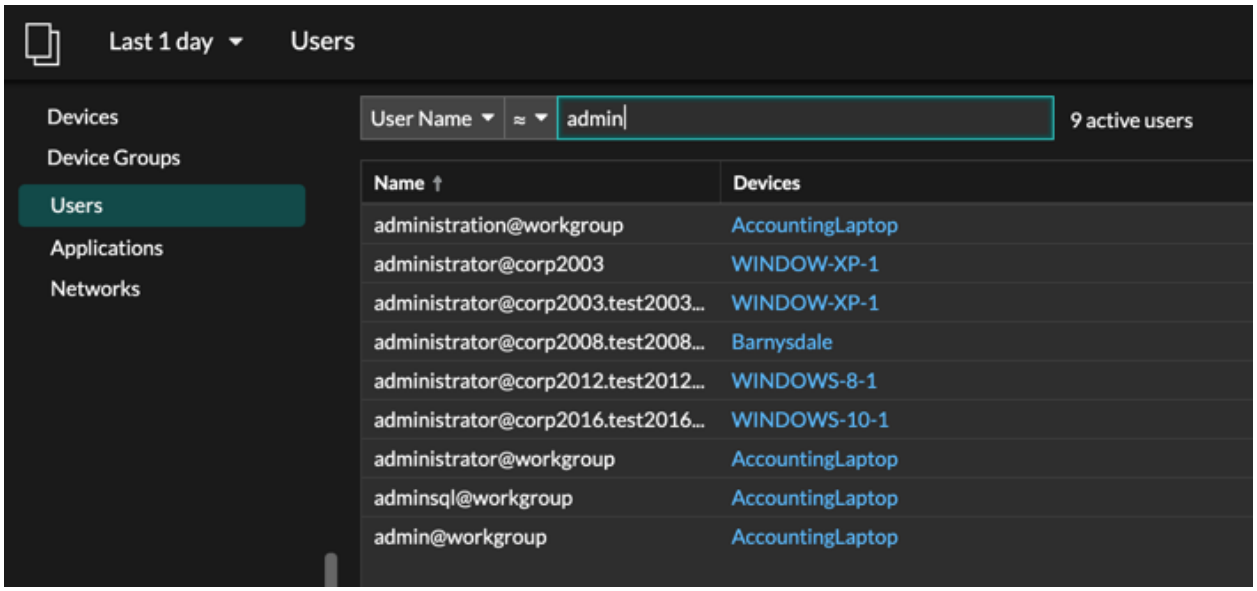
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Nutzer** Diagramm.
3. Wählen Sie in der Suchleiste eine der folgenden Kategorien aus dem Dropdownmenü aus:

Option	Description
Nutzername	Suchen Sie nach dem Benutzernamen, um zu erfahren, auf welche Geräte der Benutzer zugegriffen hat. Der Benutzername wird aus dem Authentifizierungsprotokoll wie LDAP oder Active Directory extrahiert.
Protokoll	Suchen Sie nach Protokollen, um zu erfahren, welche Benutzer auf Geräte zugegriffen haben, die über dieses Protokoll kommunizieren.
Gerätename	Suchen Sie nach dem Gerätenamen, um zu erfahren, welche Benutzer auf das Gerät zugegriffen haben.

4. Wählen Sie einen der folgenden Operatoren aus dem Drop-down-Menü aus:

Option	Description
=	Suchen Sie nach einem Namen oder Gerät, der genau mit dem Textfeld übereinstimmt.
≈	Suchen Sie nach Namen oder Geräten, die nicht genau mit dem Textfeld übereinstimmen.
≈ (Standard)	Suchen Sie nach einem Namen oder Gerät, das den Wert des Textfeldes enthält.
≈/	Suchen Sie nach einem Namen oder Gerät, das den Wert des Textfeldes ausschließt.

5. Geben Sie in das Textfeld den Namen des Benutzers oder Gerät Sie zuordnen oder ausschließen möchten.
Auf der Seite „Benutzer“ wird eine Ergebnisliste angezeigt, die der folgenden Abbildung ähnelt:



6. Klicken Sie auf den Namen eines Gerät, um das zu öffnen Seite „ Geräteübersicht“ und zeigen Sie alle Benutzer an, die während des angegebenen Zeitintervalls auf das Gerät zugegriffen haben.

Finden Sie Peer-Geräte

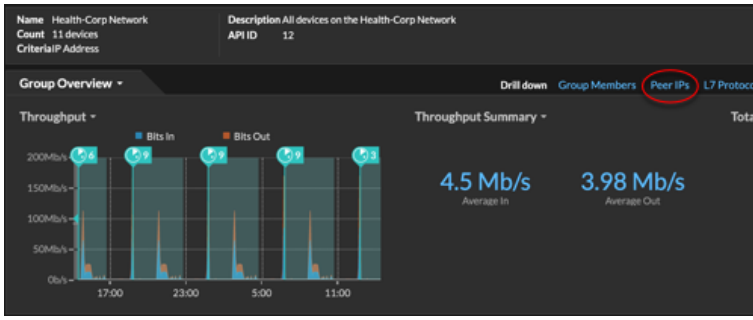
Wenn Sie wissen möchten, welche Geräte aktiv miteinander kommunizieren, können Sie auf einer Gerät- oder Gerätegruppen-Protokollseite einen Drilldown nach Peer-IPs durchführen.

Wenn du nach unten bohren Anhand der Peer-IP-Adresse können Sie eine Liste von Peer-Geräten untersuchen, Leistungs- oder Durchsatzmetriken anzeigen, die Peer-Geräten zugeordnet sind , und dann auf den Namen eines Peer-Geräts klicken, um weitere Protokollmetriken anzuzeigen.

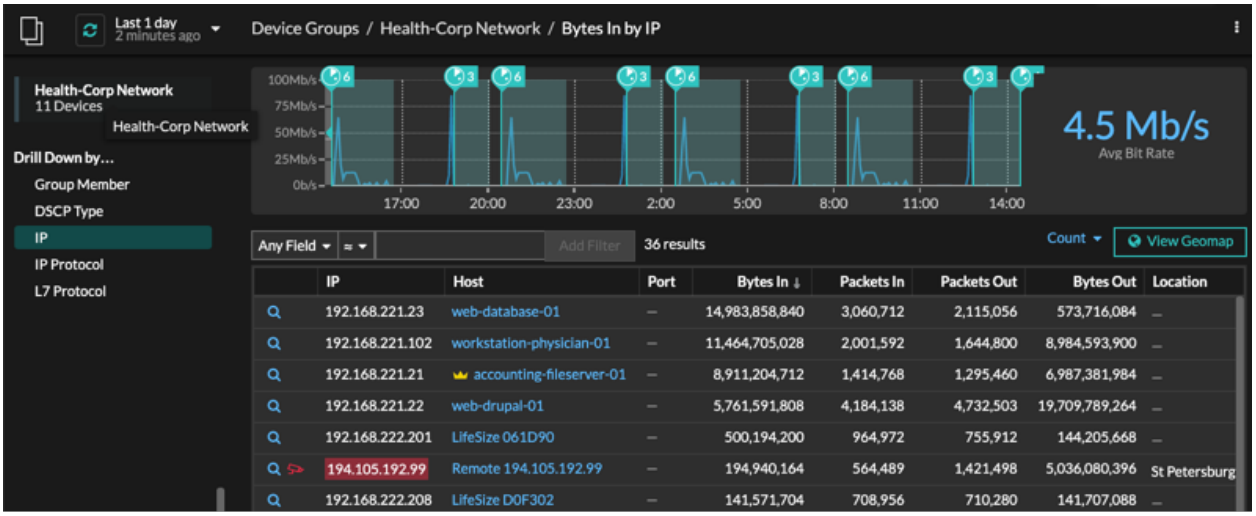
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und wählen Sie dann **Gerät** oder **Gerätegruppe** im linken Bereich.
3. Suche nach einem Gerät oder Gerätegruppe, und klicken Sie dann in der Ergebnisliste auf den Namen.
4. Klicken Sie auf der Übersichtsseite für das ausgewählte Gerät oder die Gerätegruppe auf einen der folgenden Links:

Option	Description
Für Geräte	klicken **Weitere Peer-IPs anzeigen**, befindet sich am unteren Rand des Top-Peer-Diagramms.

Für Gerätegruppen	klicken **Peer-IPs**, befindet sich im Abschnitt Details in der oberen rechten Ecke der Seite.



Eine Liste von Peer-Geräten wird angezeigt, die nach IP-Adresse aufgeschlüsselt sind. Sie können Netzwerk-Byte- und Paketinformationen für jedes Peer-Gerät untersuchen, wie in der folgenden Abbildung dargestellt.



View the peer device sending or receiving data from the source device. If available, click the hostname to learn about activity on that device.

View network throughput metrics for traffic associated with peer devices.