Finde ein Gerät

Veröffentlicht: 2023-11-13

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 Traffic- und Protokollmetriken auf einer Protokollseite anzeigen.

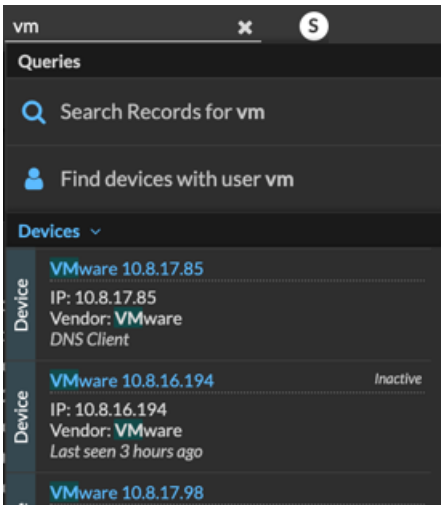
Es gibt mehrere Möglichkeiten, nach einem Gerät zu suchen:

- Finden Sie ein Gerät über eine globale Suche
- Suchen Sie anhand von Details nach einem Gerät
- Suchen Sie nach Geräten anhand der Protokollaktivität
- Suchen Sie nach Geräten, auf die ein bestimmter Benutzer zugegriffen hat
- Suche nach Peer-Geräten

Finden Sie ein Gerät 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, Hersteller, Tag, Beschreibung und Gerätegruppe. Wenn Sie beispielsweise nach dem Begriff suchen `vm`, in den Suchergebnissen werden möglicherweise Geräte angezeigt, die `vm` im Gerätenamen, Gerätehersteller oder Geräte-Tag.

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



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

   Hinweis: Geräte, die länger als 90 Tage inaktiv waren, werden von den globalen Suchergebnissen ausgeschlossen. Sie können jedoch sofort schließt alle Geräte aus, die weniger als 90 Tage inaktiv waren über die Administrationseinstellungen.
3. Klicken Sie auf einen Gerätenamen, um das zu öffnen Seite „ Geräteübersicht“ und sehen Sie sich Geräteeigenschaften und Messwerte an.

Suchen Sie anhand von Details nach einem Gerät

Sie können anhand von Informationen, die über das Kabel beobachtet wurden, nach Geräten suchen, z. B. IP-Adresse, MAC-Adresse, Hostname oder Protokollaktivität. 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 allen angegebenen Kriterien entsprechen.

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 **Geräte** im linken Bereich, und klicken Sie dann auf **Aktive Geräte** Diagramm.
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 entdeckter Gerätename kann beispielsweise die IP-Adresse oder den Hostnamen enthalten.
MAC-Adresse	Filtert Geräte nach der MAC-Adresse Gerät.
IP-Adresse	Filtert Geräte nach IP-Adresse in IPv4-, IPv6- oder CIDR-Blockformaten.
Standort	Filtert Geräte, die einer verbundenen Standort zugeordnet sind. Nur Konsole.
Entdeckungszeit	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, wodurch festgelegt wird, 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 und Modellnamen. Die folgenden Tipps können Ihnen helfen, das gewünschte Gerätemodell zu finden: • Wählen Sie den exakten Übereinstimmungsoperator (=) aus, um eine Dropdownliste vorhandener Modelle und Modellsätze anzuzeigen. • Wählen Sie den exakten Übereinstimmungsoperator (=) und wählen Sie dann **Maßgeschneiderte Modelle** um alle Geräte zu filtern, die einem

Option	Description
	benutzerdefinierten Modellsatz zugewiesen sind.
Aktivität	Filtert Geräte nach der Protokollaktivität, die dem Gerät zugeordnet ist. Wenn Sie beispielsweise HTTP-Server auswählen, werden Geräte mit HTTP-Server-Metriken zurückgegeben, und jedes andere Gerät, 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.
Cloud-Konto	Filtert Geräte nach dem Cloud-Dienstkonto, das dem Gerät zugeordnet ist.
Cloud-Instanz-ID	Filtert Geräte nach der Cloud-Instanz-ID, die dem Gerät zugeordnet ist.
Cloud-Instanztyp	Filtert Geräte nach dem Cloud-Instanztyp, der dem Gerät zugeordnet ist.
Hoher Wert	Filtert Geräte, die als hoher Wert eingestuft werden, weil sie Authentifizierungsdienste bereitstellen, wichtige Dienste in Ihrem Netzwerk unterstützen oder vom Benutzer als wertvoll angegeben 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 Netzwerkadresse.
Rolle	Filtert Geräte nach der zugewiesenen Geräterolle, z. B. Gateway, Firewall, Load Balancer und DNS-Server.
Software	Filtert Geräte nach der auf dem Gerät erkannten Betriebssystemsoftware.
Subnetz	Filtert Geräte nach dem Subnetz, das dem Gerät zugeordnet ist.
Schlagwort	Filtert Geräte nach benutzerdefinierten Gerätekennzeichnungen.
Verkäufer	Filtert Geräte nach dem Namen des Geräteanbieters, der durch die OUI-Suche (Organizationally Unique Identifier) bestimmt wird.
Virtuelle private Cloud	Filtert Geräte nach der VPC, die dem Gerät zugeordnet ist.
VLAN	Filtert Geräte nach dem Geräte-VLAN-Tag. VLAN-Informationen werden aus

Option	Description
	VLAN-Tags extrahiert, wenn sie bei der Datenverkehrsspiegelung auf dem Mirror-Port gespeichert werden. Nur verfügbar, wenn `devices_accross_vlans` Einstellung ist gesetzt auf `False` in der laufenden Konfigurationsdatei.
CDP-Name	Filtert Geräte nach dem CDP-Namen, der dem Gerät zugewiesen wurde.
Name der Cloud-Instanz	Filtert Geräte nach dem Cloud-Instanznamen, 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 wurde.
DNS-Name	Filtert Geräte nach jedem DNS-Namen, der dem Gerät zugewiesen wurde.
NetBIOS-Name	Filtert Geräte nach dem NetBIOS-Namen, der dem Gerät zugewiesen wurde.

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 der ausgewählten Kategorie entsprechen.
#	Filtert Geräte, die nicht exakt mit dem Suchfeld übereinstimmen.
≈	Filtert Geräte, die den Wert des Suchfeldes für die ausgewählte Kategorie enthalten.
≈/	Filtert Geräte, die den Wert des Suchfeldes 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 Suchfeldes für die ausgewählte Kategorie enthalten.

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

   Wenn Sie beispielsweise Geräte anhand des Namens suchen möchten, geben Sie die Zeichenfolge, nach der gesucht werden soll , in das Suchfeld Feld. Wenn Sie Geräte anhand von Rollen suchen möchten, wählen Sie aus der Dropdownliste der Rollen aus.

   Hinweis: Abhängig von der ausgewählten Kategorie können Sie im Textfeld auf das Regex-Symbol klicken, um den Abgleich anhand eines regulären Ausdrucks zu aktivieren.

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

Nächste Schritte

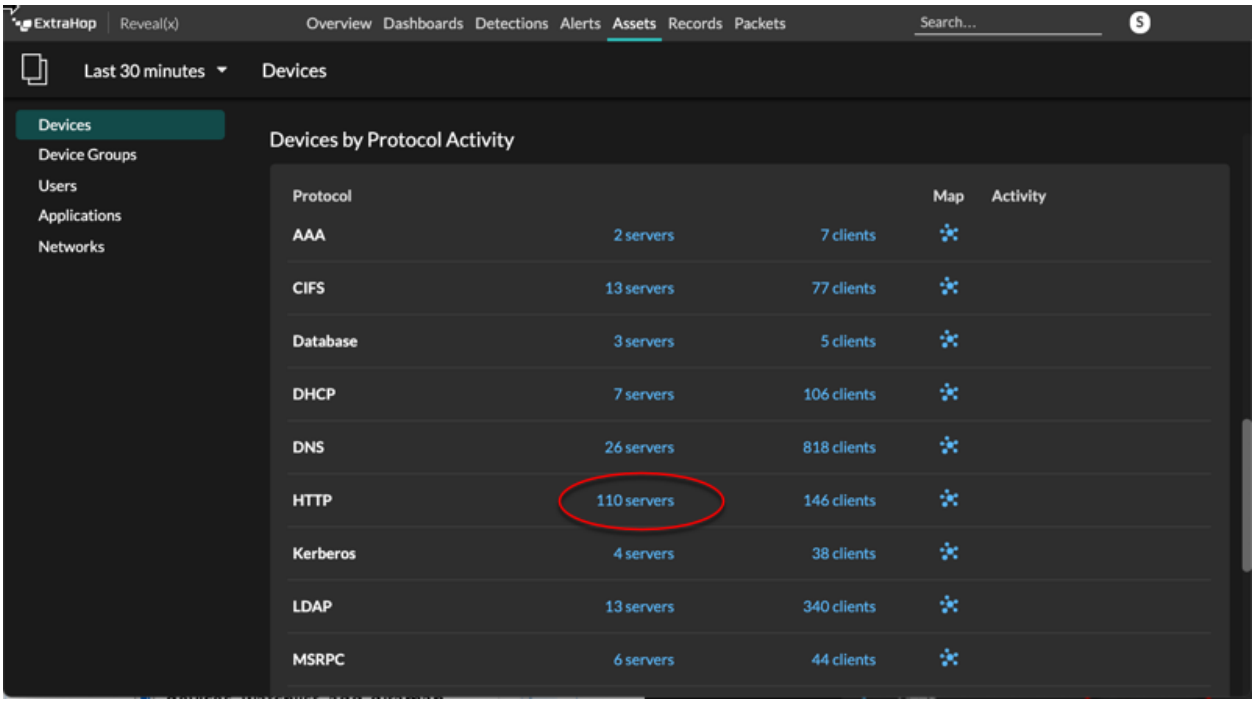
- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf dem Seite „ Geräteübersicht“ .
- klicken **Dynamische Gruppe erstellen** von der oberen rechten Ecke bis eine dynamische Gerätegruppe erstellen basierend auf den Filterkriterien.
- Klicken Sie auf das Befehlsmenü ⋮ und wählen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

Suchen Sie nach Geräten anhand der Protokollaktivität

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 finden, 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.

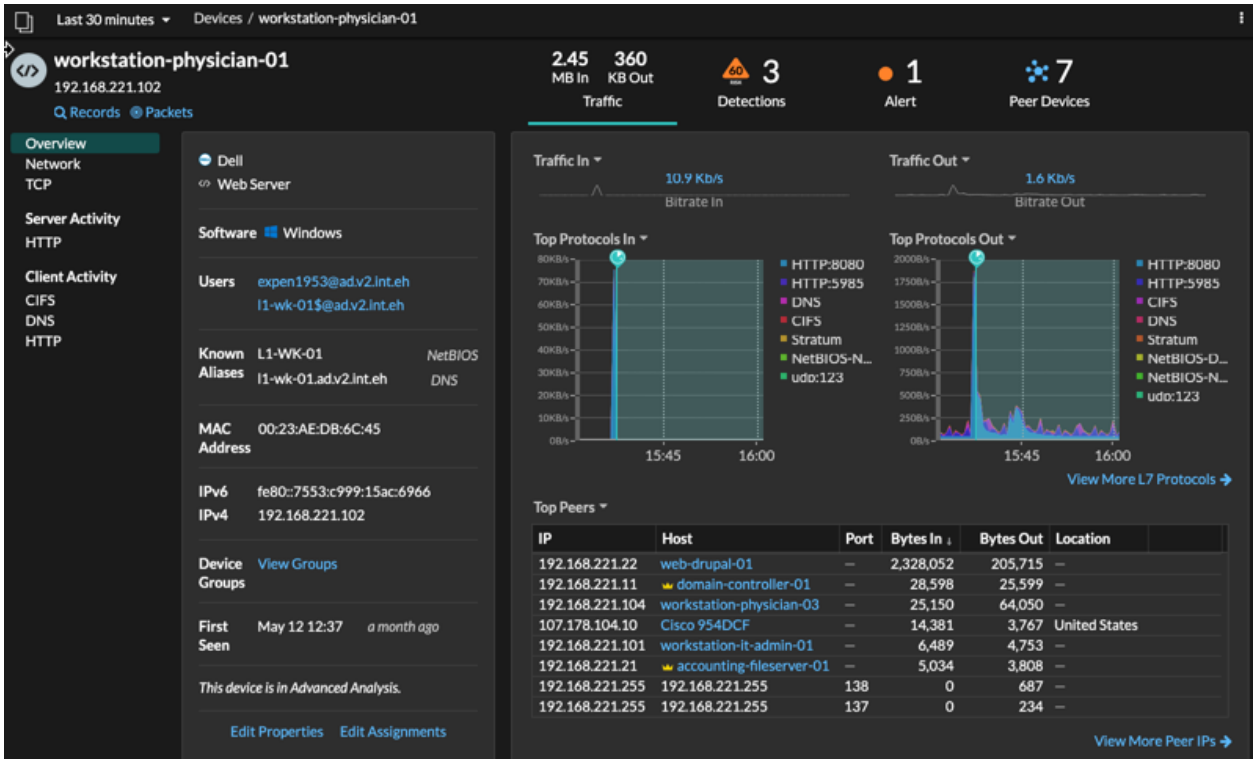


Hinweis: Wenn das gewünschte Protokoll nicht angezeigt wird, hat das ExtraHop-System diese Art von Protokollverkehr über die Leitung während des angegebenen Zeitintervalls

möglicherweise nicht beobachtet, oder das Protokoll erfordert möglicherweise eine Modullizenz. Weitere Informationen finden Sie in der Ich sehe den Protokollverkehr, den ich erwartet habe, nicht? Abschnitt in den häufig gestellten Fragen zur Lizenz.

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

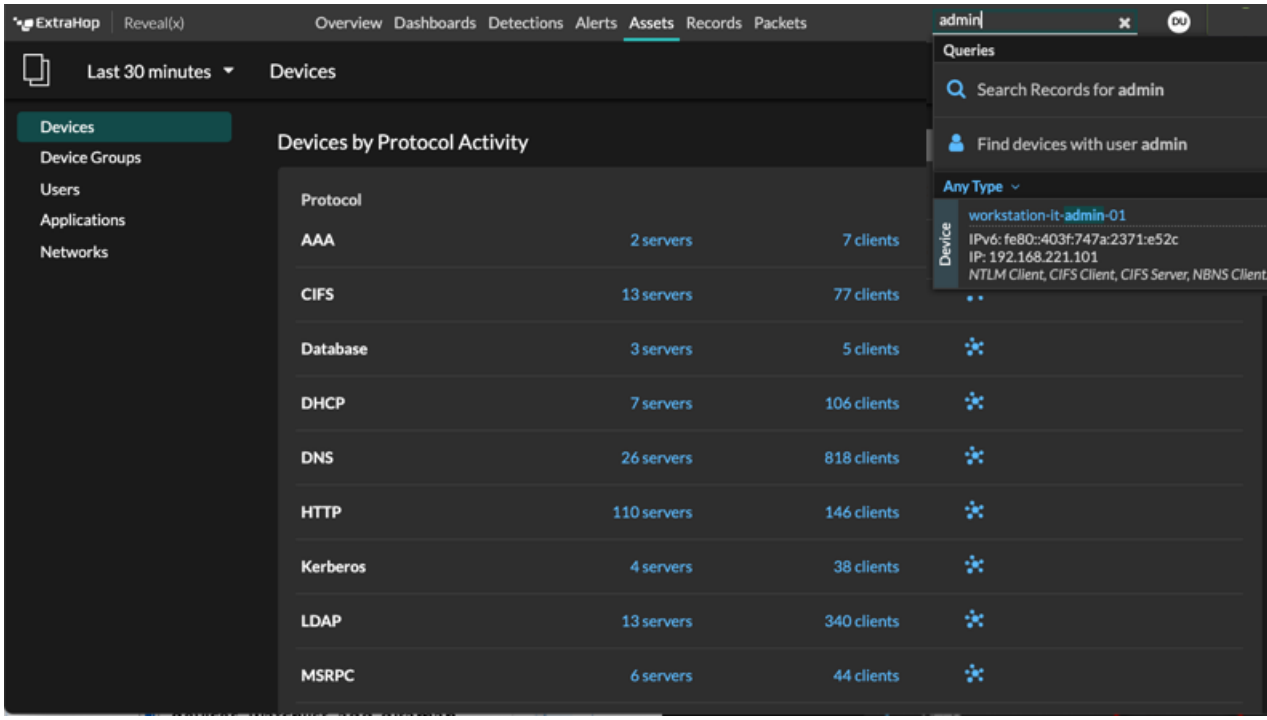
4. Klicken Sie oben auf der Seite auf **Mitglieder der Gruppe**.
   Auf der Seite wird eine Tabelle mit allen Geräten angezeigt, die während des ausgewählten Zeitintervalls HTTP-Antworten über das Kabel gesendet haben.
5. Klicken Sie in der Tabelle auf einen Gerätenamen.
   Auf der Seite werden Traffic-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



Suchen Sie nach Geräten, auf die ein bestimmter Benutzer zugegriffen hat

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

Hinweis: Sie können auch über das globale Suchfeld oben auf der Seite nach Benutzern suchen.



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**.
3. klicken **Nutzer** im linken Bereich.
4. Wählen Sie in der Suchleiste eine der folgenden Kategorien aus der Drop-down-Liste aus:

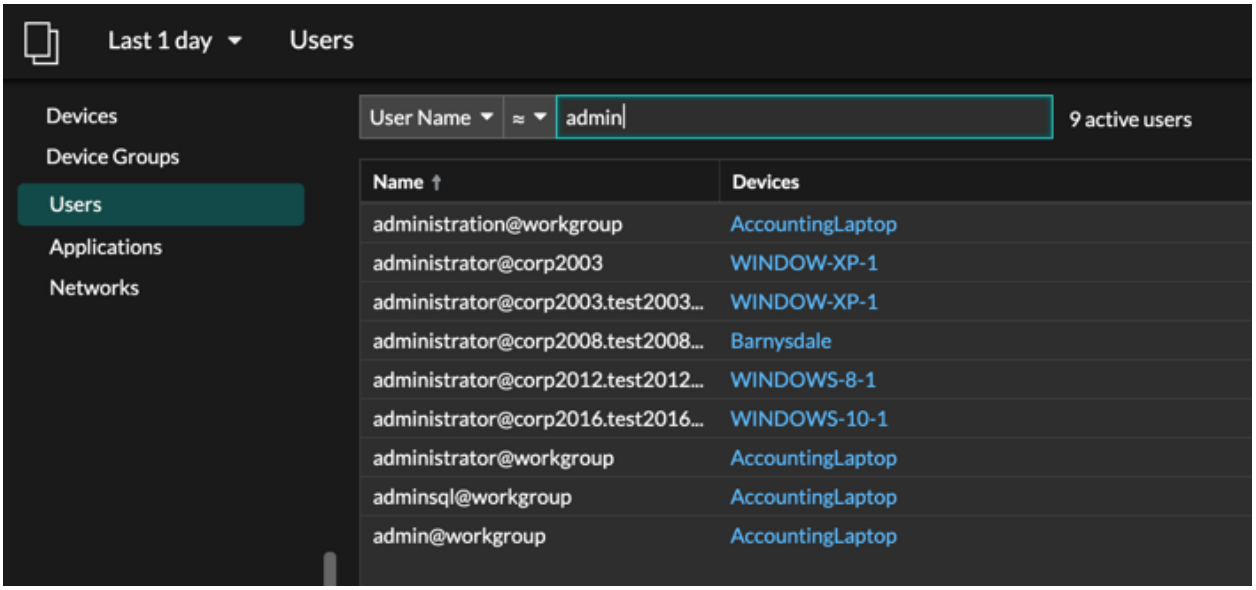
Option	Description
Nutzername	Suchen Sie nach dem Benutzernamen, um zu erfahren, auf welche Geräte der Benutzer zugegriffen hat. Der Benutzername wird aus dem Authentifizierungsprotokoll wie LDAP oder Active Directory extrahiert.
Protokoll	Suchen Sie nach Protokoll, um zu erfahren, welche Benutzer auf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

5. Wählen Sie einen der folgenden Operatoren aus der Dropdownliste aus:

Option	Description
=	Suchen Sie nach einem Namen oder Gerät, das exakt 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.

Option	Description
≈/	Suchen Sie nach einem Namen oder Gerät, das den Wert des Textfeldes ausschließt.

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



7. 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.

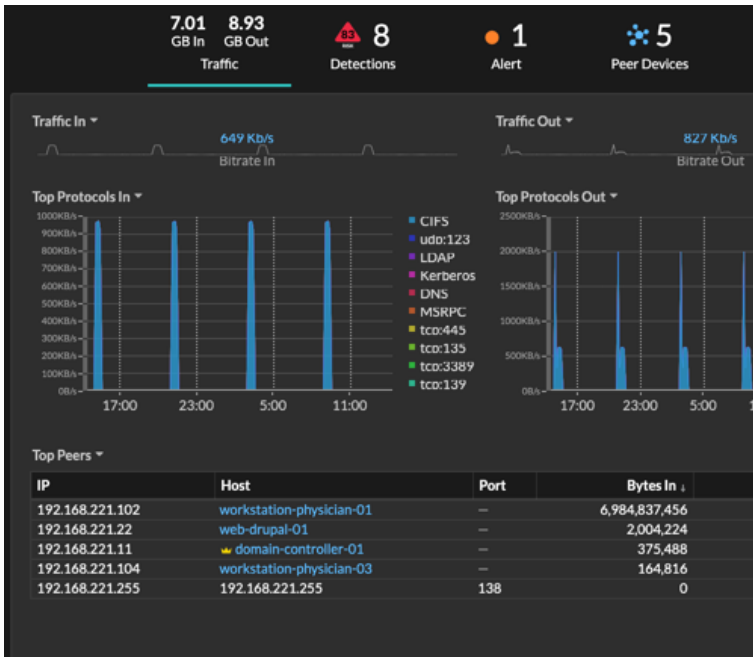
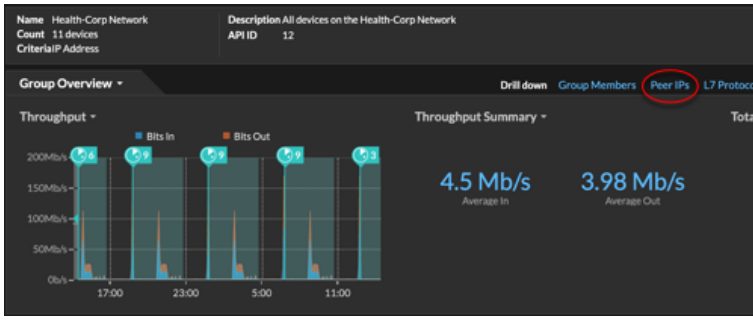
Suche nach Peer-Geräten

Wenn Sie wissen möchten, welche Geräte aktiv miteinander kommunizieren, können Sie von einer Protokollseite für Geräte oder Gerätegruppe aus nach Peer-IPs suchen.

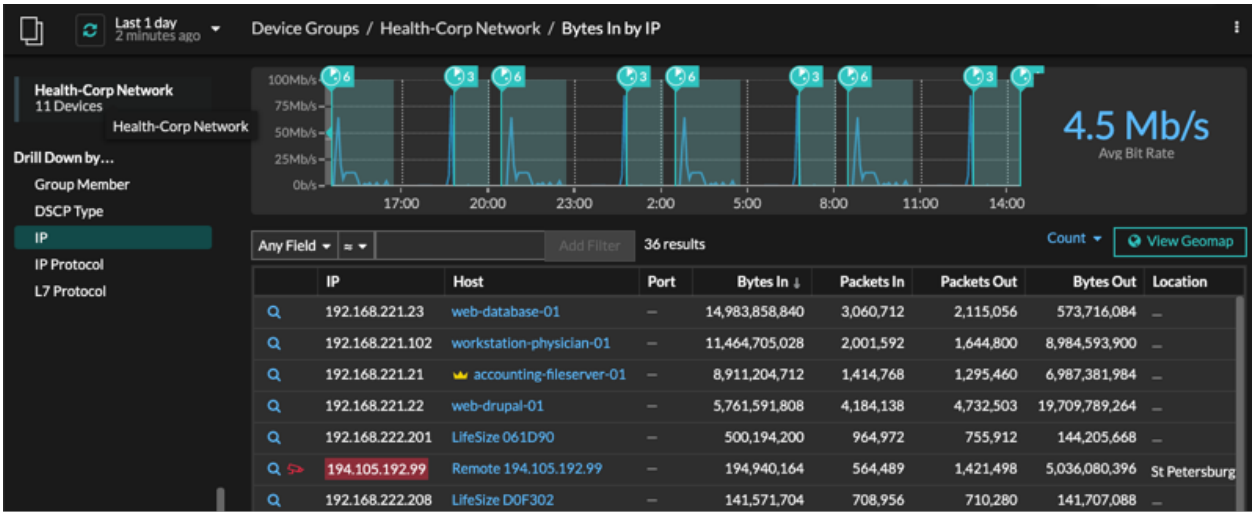
Wenn du bohren Nach Peer-IP-Adresse können Sie eine Liste von Peer-Geräten untersuchen, Leistungs- oder Durchsatzmetriken für Peer-Geräte anzeigen und dann auf einen Peer-Gerätenamen klicken, um zusätzliche Protokollmetriken anzuzeigen.

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. Suchen Sie 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-Charts.

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

Es wird eine Liste von Peer-Geräten angezeigt, die nach IP-Adresse aufgeschlüsselt sind. Sie können Netzwerkbytes- 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.