Überwachen Sie neue Geräte in Ihrem Netzwerk

Veröffentlicht: 2024-07-02

Jedes neue Gerät, das sich mit Ihrem Netzwerk verbindet, birgt ein potenzielles Risiko. Daher ist es wichtig, neu entdeckte Geräte schnell zu identifizieren und deren Aktivität zu überwachen. Das ExtraHop-System erstellt automatisch eine Gerätegruppe für Geräte, die am letzten Tag und in der letzten Woche entdeckt wurden. Diese Gerätegruppe erfasst jedoch standardmäßig begrenzte Messwerte und ist in Ihrem System-Dashboard nicht sichtbar.

In dieser exemplarischen Vorgehensweise priorisieren wir zunächst die Gruppe der neu entdeckten Geräte, um umfassende Messwerte zu sammeln. Anschließend erstellen wir ein Dashboard zur Überwachung der Geräteaktivität und schließlich erstellen wir einen täglichen Bericht, um interessante Änderungen zu verfolgen.

Nach Abschluss dieser exemplarischen Vorgehensweise können Sie die folgenden Fragen beantworten:

- Wie viele neue Geräte sind in der letzten Woche in meinem Netzwerk erschienen?
- Wie viel eingehender und ausgehender Datenverkehr ist mit neuen Geräten verbunden?
- Was sind die täglichen Änderungen bei der Aktivität neuer Gerät?
- Wie erfahre ich mehr, wenn ich interessante Geräteaktivitäten finde?

Voraussetzungen

- Machen Sie sich mit den Konzepten in dieser Komplettlösung vertraut, indem Sie die Häufig gestellte Fragen zur Geräteerkennung, Priorisieren Sie Gruppen für Erweiterte Analyse, der FAQ zu Metriken und der Referenz zu Protokollmetriken Themen.
- Sie müssen Zugang zu einem haben Konsole mit System- und Zugriffsadministrationsrechten, um einen Bericht zu planen.

Priorisieren Sie neue Geräte für die erweiterte Analyse

Zunächst priorisieren wir die neu entdeckte Gerätegruppe, um umfassende Metriken zu sammeln Erweiterte Analyse. Indem Sie Ihrer Gruppe für Erweiterte Analyse Priorität einräumen, stellen Sie sicher, dass das ExtraHop-System L2-L7-Metriken für neue Geräte erfasst.

Wenn dein Konsole ist nicht Verwaltung von Analyseprioritäten Für Ihre Sensoren können Sie diese Anleitung stattdessen von einem Sensor aus ausführen und den letzten Abschnitt weglassen. (Geplante Berichte können nur aus einem erstellt werden Konsole.)

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann auf **Analyse-Prioritäten**.
3. In der Für Erweiterte Analyse Abschnitt, klicken **eine Gruppe hinzufügen** um eine erste Gruppe hinzuzufügen oder **Gruppe hinzufügen** um weitere Gruppen hinzuzufügen.
4. Typ `new devices` in der **GRUPPE** Dropdownliste, und wählen Sie dann **Neue Geräte (letzte 7 Tage)**.
5. Klicken Sie oben auf der Seite auf **Speichern**.

Lassen Sie uns nun ein Dashboard erstellen, um die Aktivitäten neuer Gerät zu überwachen.

Erstellen Sie ein Dashboard

Indem Sie ein Dashboard für Ihre Gruppe erstellen, können Sie die Geräteaktivitäten auf einen Blick visualisieren.

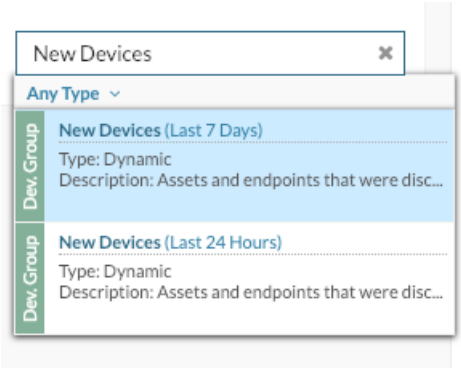
1. Klicken Sie oben auf der Seite auf **Dashboards**.
2. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke und wähle **Neues Dashboard** um ein leeres Dashboard zu erstellen.
3. Geben Sie einen Namen für Ihr Dashboard in der **Titel** Feld. Geben Sie für diese exemplarische Vorgehensweise ein `Neue Geräte`.
4. klicken **Erstellen**.
   Wenn Sie ein neues Dashboard erstellen, wird ein Arbeitsbereich in einem bearbeitbaren Layoutmodus geöffnet. Dieser Arbeitsbereich enthält eine einzelne Region und zwei leere Widgets: ein Diagramm und ein Textfeld.
5. Löschen Sie das Textfeld, indem Sie die folgenden Schritte ausführen:
   a) Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke des Textfeld-Widgets und wählen Sie **Löschen**.
   b) klicken **Widget löschen**.
   Textfeld-Widgets können benutzerdefinierten erklärenden Text zu einem Dashboard oder Diagramm enthalten. Für diese exemplarische Vorgehensweise werden wir jedoch keinen Text hinzufügen.

Als Nächstes fügen wir unserem Dashboard Diagramme hinzu, die zeigen, welche neuen Geräte in der letzten Woche entdeckt wurden und was sie im Netzwerk getan haben.

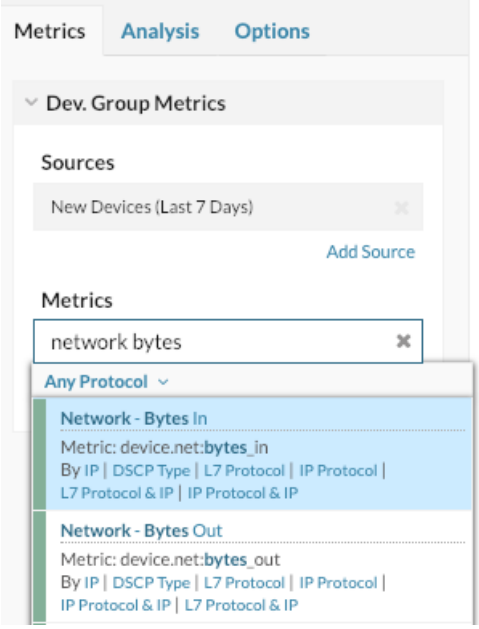
Fügen Sie ein Diagramm hinzu, das den Verkehrsdurchsatz für neue Geräte zeigt

In diesem Schritt erstellen wir eine Tabelle, in der alle Geräte aufgeführt sind, die in den letzten sieben Tagen entdeckt wurden. Die Menge des eingehenden und ausgehenden Datenverkehrs, die in der letzten Woche beobachtet wurde, wird neben jedem Gerät angezeigt. In diesem Dashboard können Sie erfahren, wie viel Traffic jedes neue Gerät generiert.

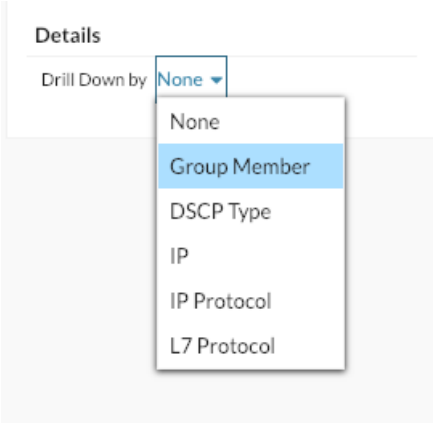
1. Klicken Sie in Ihrem neu erstellten Dashboard auf das leere Diagramm-Widget, um den Metric Explorer zu öffnen.
2. klicken **Quelle hinzufügen**.
3. Geben Sie im Feld Quellen Folgendes ein `New Devices` um die Ergebnisse zu filtern, und wählen Sie dann **Neue Geräte (letzte 7 Tage)** für einen angeschlossenen Sensor.



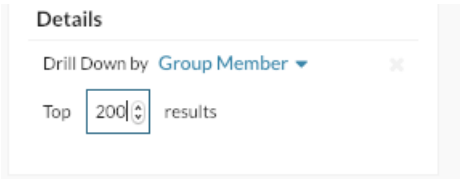
4. Geben Sie im Feld Metriken Folgendes ein `network bytes` um Ergebnisse aus allen verfügbaren Metriken zu filtern, und klicken Sie dann auf **Eingehende Netzwerk-Bytes** .



5. klicken **Metrik hinzufügen**, typ `network bytes`, und wählen Sie dann **Ausgehende Netzwerk-Bytes**.
6. Klicken Sie unten im Fenster auf **Tabelle**.
7. In der Einzelheiten Abschnitt, klicken **Keine**, und klicken Sie dann auf **Mitglied der Gruppe**.

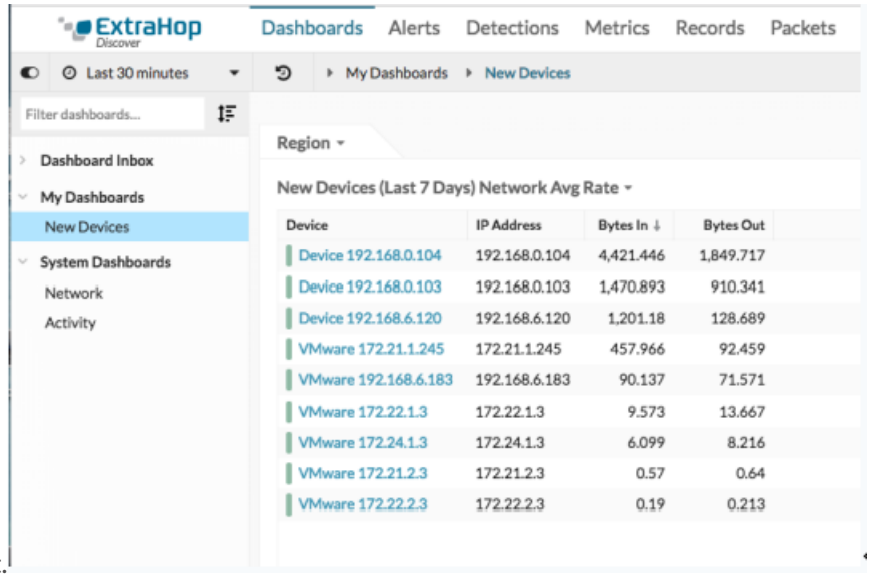


8. Optional: Klicken Sie auf **Optionen** Registerkarte. In der Einheiten Abschnitt, klicken **Bytes nach Bits umrechnen**. Der Durchsatz wird jetzt in Bits pro Sekunde angezeigt.
9. Optional: Klicken Sie unter der Metrik auf **Durchschnittliche Rate** und dann klicken **Zählen**.
   Die Gesamtmenge des Durchsatzes wird jetzt anstelle der durchschnittlichen Durchsatzmenge pro Sekunde angezeigt.
10. Klicken Sie im Feld Top-Ergebnisse auf **5**, typ `200`, und drücken Sie dann `Eingeben`.



11. klicken **Speichern**.
12. klicken **Layoutmodus verlassen**.

In der Tabelle werden nun alle in der letzten Woche neu entdeckten Geräte und deren Durchsatz angezeigt, wie in der folgenden Abbildung dargestellt.



Lassen Sie uns nun einen täglichen Bericht zur Überwachung neuer Geräte einrichten.

Planen Sie einen täglichen Bericht

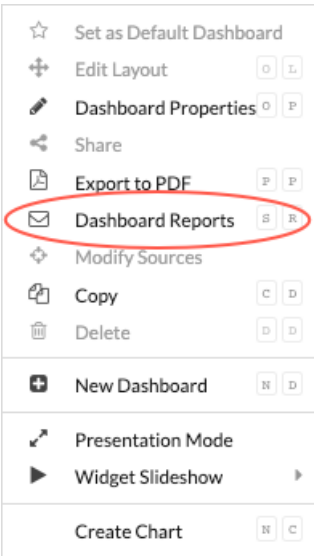
Nachdem Sie Ihr Dashboard für neue Geräte erstellt haben, können Sie einen täglichen Bericht über die Aktivitäten neuer Gerät am letzten Tag erstellen. Dieser Bericht ist eine PDF-Datei des Dashboard, die per E-Mail an jeden Empfänger gesendet werden kann. Geplante Berichte können nur aus einem erstellt werden Konsole.

In den folgenden Schritten zeigen wir Ihnen, wie Sie einen täglichen Bericht planen, der um 7:00 Uhr veröffentlicht wird.

1. Aus dem Konsole, klicken **Armaturenbretter** oben auf der Seite, und klicken Sie dann auf **Neue Geräte** Dashboard im linken Bereich.

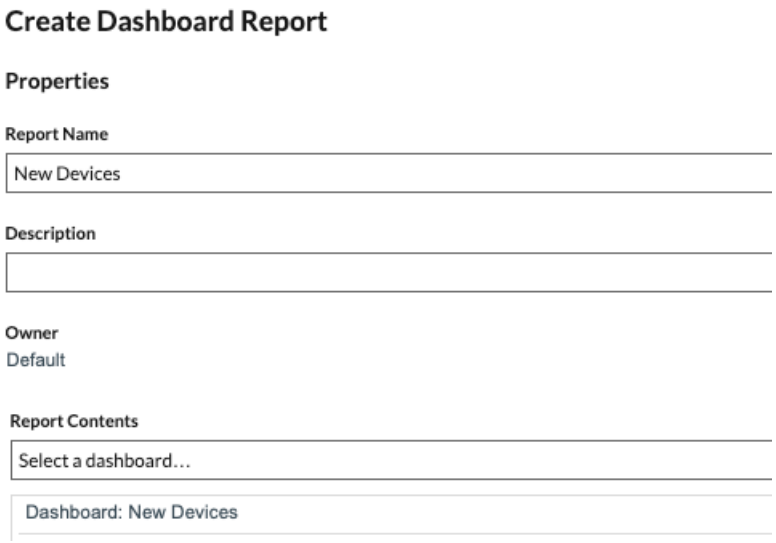
   Hinweis: Jeder Bericht kann nur mit einem Dashboard verknüpft werden. Sie können einen Bericht für jedes Dashboard erstellen, das Ihnen gehört oder das mit Ihnen geteilt wurde.

2. Klicken Sie in der oberen rechten Ecke der Dashboard-Seite auf das Befehlsmenü ⋮, und klicken Sie dann auf **Dashboard-Berichte**.



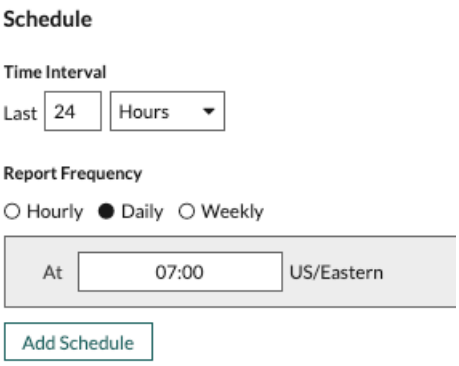
3. Eine Seite mit geplanten Berichten wird angezeigt, auf der alle Berichte angezeigt werden, die auf dem Konsole.

   Wenn keine Berichte erstellt wurden, ist diese Seite leer.
4. Klicken Sie in der oberen rechten Ecke auf **Erstellen**.
5. In der **Name des Berichts** Feld, der Name des Dashboard wird angezeigt, wie in der folgenden Abbildung dargestellt.



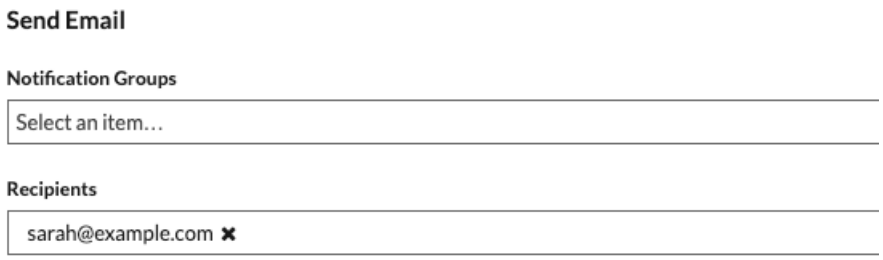
6. Scrollen Sie nach unten zum Zeitintervall Abschnitt. Belassen Sie die Standardeinstellung von **Letzte 11 Tage**. Der Bericht wird neuen Geräteverkehr enthalten, der im Laufe des Vortages aufgetreten ist.

   Hinweis: Weitere Informationen zur Konfiguration der einzelnen Feld finden Sie unter Einen geplanten Bericht erstellen.
7. In der Häufigkeit melden Abschnitt, klicken Sie in den **Bei** Dropdownliste und klicken Sie auf 07:00, um täglich um 7:00 Uhr eine E-Mail zu senden.



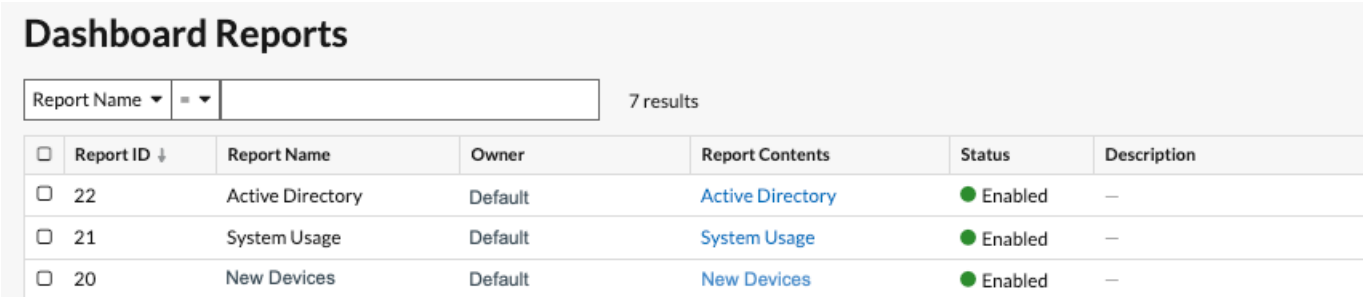
Hinweis: Die für Ihre Konsole eingestellte Systemzeit bestimmt die Zeitzone, die bei der Konfiguration Ihres Berichts angezeigt wird. Weitere Informationen zur Konfiguration der Zeitzone für Ihre Konsole über die ExtraHop-Administrationseinstellungen finden Sie unter Konfigurieren Sie die Systemzeit.

8. Geben Sie Ihre E-Mail-Adresse in das Feld Empfänger ein.



Hinweis: Das ExtraHop-System speichert keine E-Mail-Adressen für ExtraHop-Benutzerkonten. Wenn Ihr ExtraHop RevealX Enterprise-System jedoch konfiguriert mit einer E-Mail-Gruppe, Sie können eine Benachrichtigungsgruppe auswählen, die per E-Mail gesendet werden soll. RevealX 360 unterstützt keine E-Mail-Benachrichtigungsgruppen.

9. Optional: Klicken Sie **Jetzt senden** um eine Test-E-Mail an den Empfänger zu senden.
10. Klicken Sie **Erledigt**. Ihr geplanter Bericht wird jetzt auf der Seite Dashboard-Berichte angezeigt, wie in der folgenden Abbildung dargestellt.



11. Klicken Sie in der unteren rechten Ecke der Seite auf **Erledigt** erneut , um zu Ihrem Dashboard zurückzukehren.

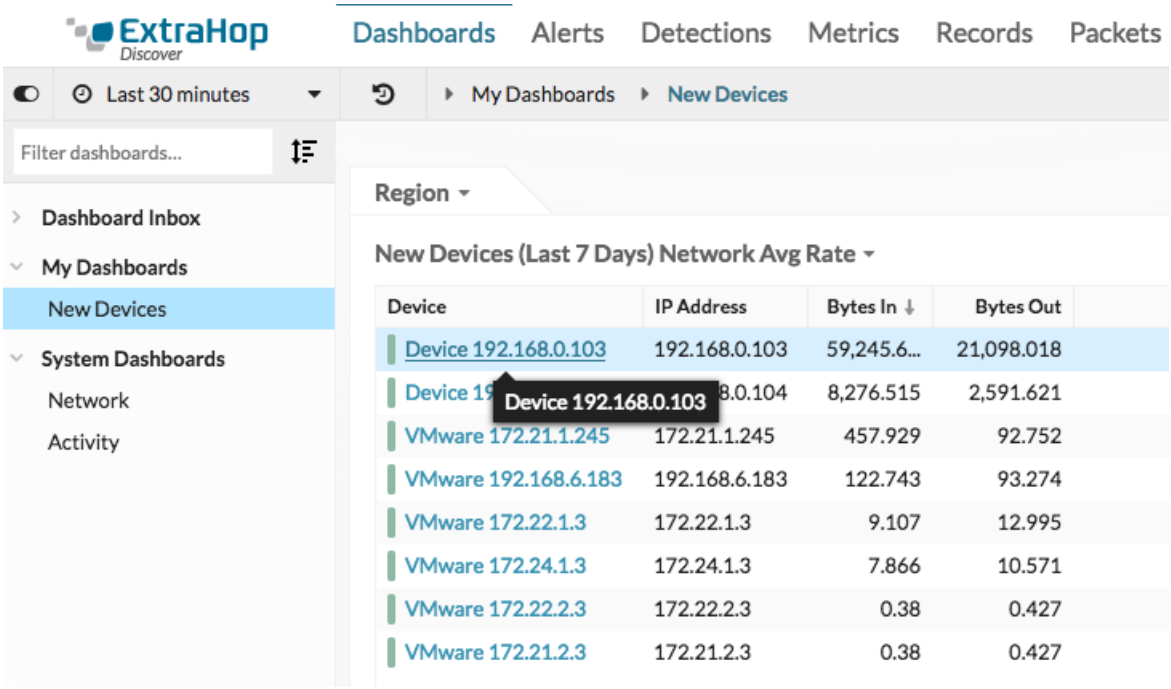
Wenn Sie die per E-Mail gesendete PDF-Datei erhalten, klicken Sie auf **Bericht auf ExtraHop ansehen** um auf das Dashboard zuzugreifen, das den Bericht generiert hat. Für ExtraHop-Benutzer öffnet der Link die Konsole und das Dashboard ist auf das im Bericht angegebene Zeitintervall eingestellt.

Im nächsten Abschnitt werden wir uns einige Möglichkeiten ansehen, wie Sie Geräte untersuchen können, die ungewöhnliche Aktivitäten aufweisen.

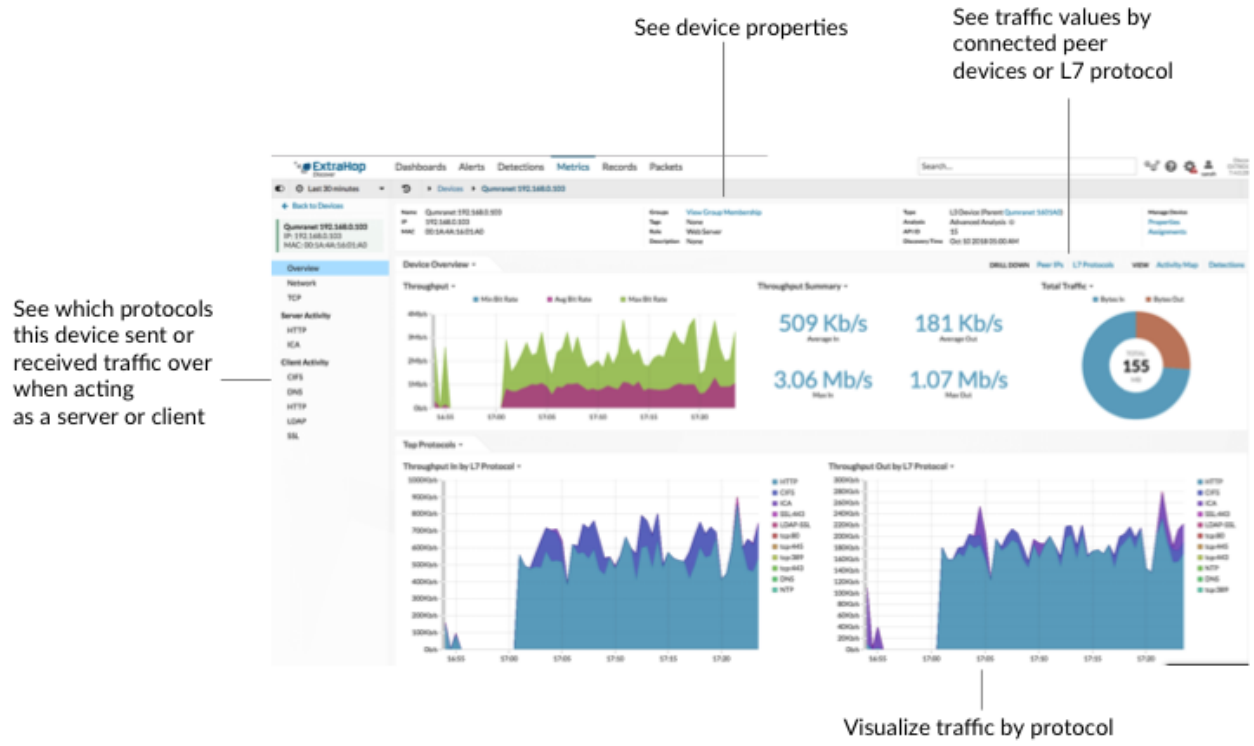
Nächste Schritte: Untersuchen Sie ein neues Gerät

Wenn Sie feststellen, dass ein neues Gerät eine große Menge an Datenverkehr über Ihr Netzwerk sendet, können Sie eine Protokollseite aufrufen, um zu erfahren, was das Gerät tut.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Klicken Sie auf **Neue Geräte** Dashboard im linken Bereich, und klicken Sie dann auf den Gerätenamen, wie in der folgenden Abbildung dargestellt.



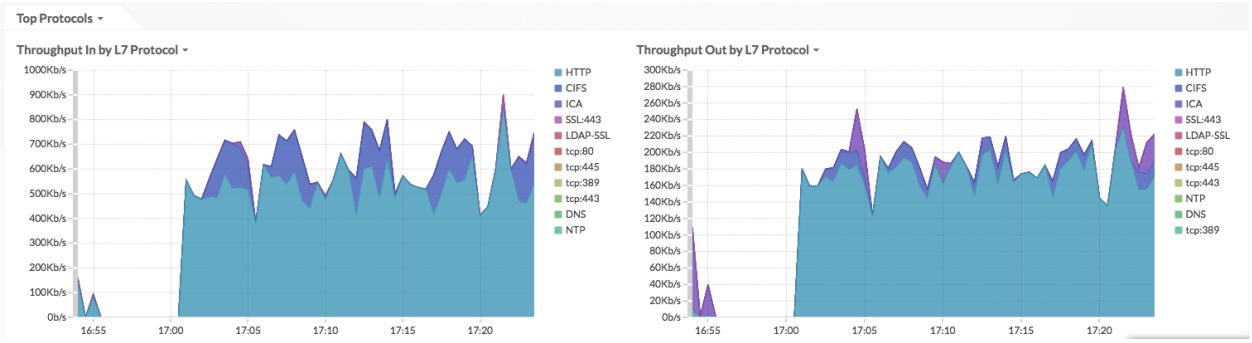
Eine Protokollseite wird angezeigt, die zugehörige Metrikdaten für dieses Gerät enthält.



Auf der Protokollseite können Sie die folgenden Fragen beantworten.

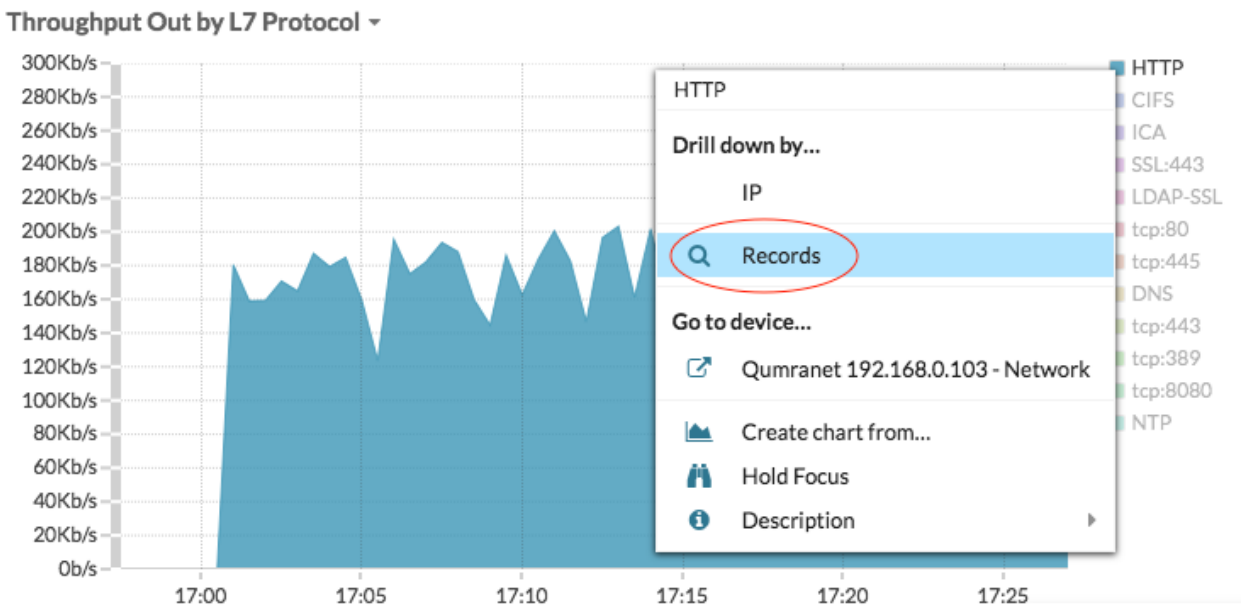
Was ist die primäre Art der Aktivität für dieses Gerät?

Sehen Sie sich die Diagramme für den eingehenden Durchsatz nach dem L7-Protokoll und den ausgehenden Durchsatz nach dem L7-Protokoll an. Das Verkehrsvolumen ist nach Protokollen auf Anwendungsebene (L7) aufgeschlüsselt. Im folgenden Beispiel können wir sehen, dass HTTP-Transaktionen die primäre Art von Verkehr für dieses Gerät sind.

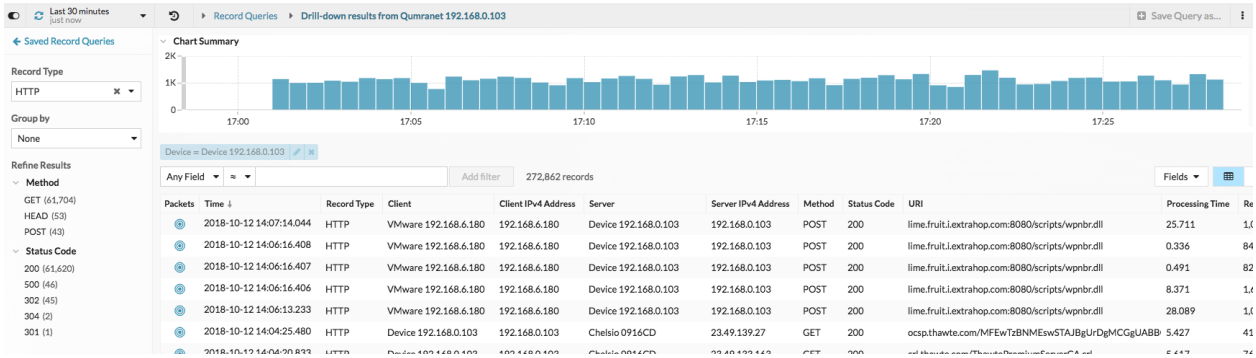


Welche Transaktionen sind mit dem hohen Verkehrsaufkommen verbunden?

Wenn Sie über einen verbundenen Recordstore verfügen, klicken Sie im Diagramm auf eine Protokollbezeichnung, und klicken Sie dann auf **Rekorde**.



Du kannst sehen Transaktionsebene Einzelheiten.

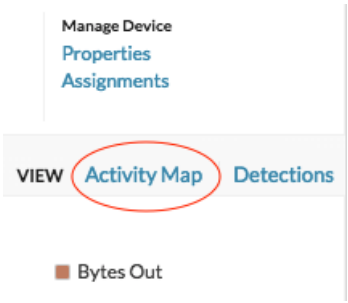


Welche Peer-Geräte sind mit diesem neuen Gerät verbunden?

Es gibt zwei Möglichkeiten, um zu sehen, welche Netzwerkgeräte mit Ihrem Gerät verbunden sind.

- In der BOHREN Abschnitt, klicken **Peer-IPs** um eine Liste der Verkehrswerte von verbundenen Peer-Geräten zu sehen.

- In der ANSICHT Abschnitt, klicken **Karte der Aktivitäten** um Verbindungen mit Peer-Geräten anhand von Protokollaktivitäten zu visualisieren.


Manage Device
Properties
Assignments
VIEW
Activity Map
Detections
Bytes Out