Erstellen Sie ein benutzerdefiniertes Gerät zur Überwachung des Datenverkehrs in entfernten Büros

Veröffentlicht: 2024-08-07

Nach der Installation des ExtraHop-Systems in Ihrem Rechenzentrum gewinnen Sie schnell Erkenntnisse über Ihr Netzwerk. Da das ExtraHop-System automatisch Geräte erkennt, die in Ihrem Netzwerk kommunizieren, können Sie damit beginnen, Datenverkehrsengpässe zu erkennen oder Probleme bei langsamen Diensten zu beheben. Aber wie gewinnen Sie Erkenntnisse über wichtigen Verkehr an abgelegenen Standorten außerhalb Ihres Rechenzentrum?

Von ein benutzerdefiniertes Gerät erstellen, können Sie leicht lernen, wie abgelegene Standorte Dienste und Anwendungen nutzen. Benutzerdefinierte Geräte erfassen Metriken aus dem Netzwerkverkehr auf der Grundlage von Kriterien, die Sie angeben, z. B. ein IP-Adress-Subnetz, eine Reihe von Ports oder ein virtuelles LAN (VLAN). Mit einem benutzerdefinierten Gerät können Sie die folgenden Verkehrsarten überwachen:

- Verkehr an entfernten Standorten, z. B. in Zweigstellen, Geschäften und Kliniken.
- Verkehr mit Geschäftspartnern von Drittanbietern, z. B. Kreditkartenabwickler und Zeitnehmer.
- „Das Internet“, wo Sie Traffic von einer Reihe bekannter öffentlicher IP-Adressen wie 8.0.0.0/7 sammeln können.

Sie können einem Dashboard-Diagramm ein benutzerdefiniertes Gerät als Metrikquelle hinzufügen, um den Verkehr auf dem Gerät einfach zu überwachen. Ein benutzerdefiniertes Gerät kann auch als Metrik Quelle für Auslöser und Warnungen ausgewählt werden.

Ein benutzerdefiniertes Gerät zählt nur als ein einziges Gerät auf Ihr lizenziertes Gerätelimit, was hilfreich ist, um die Geräteanzahl niedrig zu halten. Es ist jedoch wichtig zu beachten, dass benutzerdefinierte Geräte die Systemleistung beeinträchtigen, wenn sie nicht richtig konfiguriert sind.

In dieser exemplarischen Vorgehensweise erfahren Sie, wie Sie ein benutzerdefiniertes Gerät erstellen und den Datenverkehr an entfernten Standorten überwachen, indem Sie die folgenden Schritte ausführen:

- Erstellen Sie ein benutzerdefiniertes Gerät für ein Subnetz von Zweigstellengeräten.
- Erstellen Sie ein Dashboard zur Überwachung der Bandbreite und Latenz des Datenverkehrs in Zweigstellen.

Voraussetzungen

Sie müssen über ein Benutzerkonto mit vollen System- oder vollen Schreibrechten verfügen.

Im Folgenden finden Sie einige Richtlinien zur Konfiguration benutzerdefinierter Geräte:

- Vermeiden Sie es, mehrere benutzerdefinierte Geräte für dieselben IP-Adressen oder Ports zu erstellen. Überlappende benutzerdefinierte Geräte können die Systemleistung beeinträchtigen.
- Wenn Sie ein benutzerdefiniertes Gerät von einem aus konfigurieren Konsole, Sie müssen einen Sensor angeben. Das benutzerdefinierte Gerät ist nur für den angegebenen Sensor verfügbar.

Benutzerdefiniertes Gerät erstellen

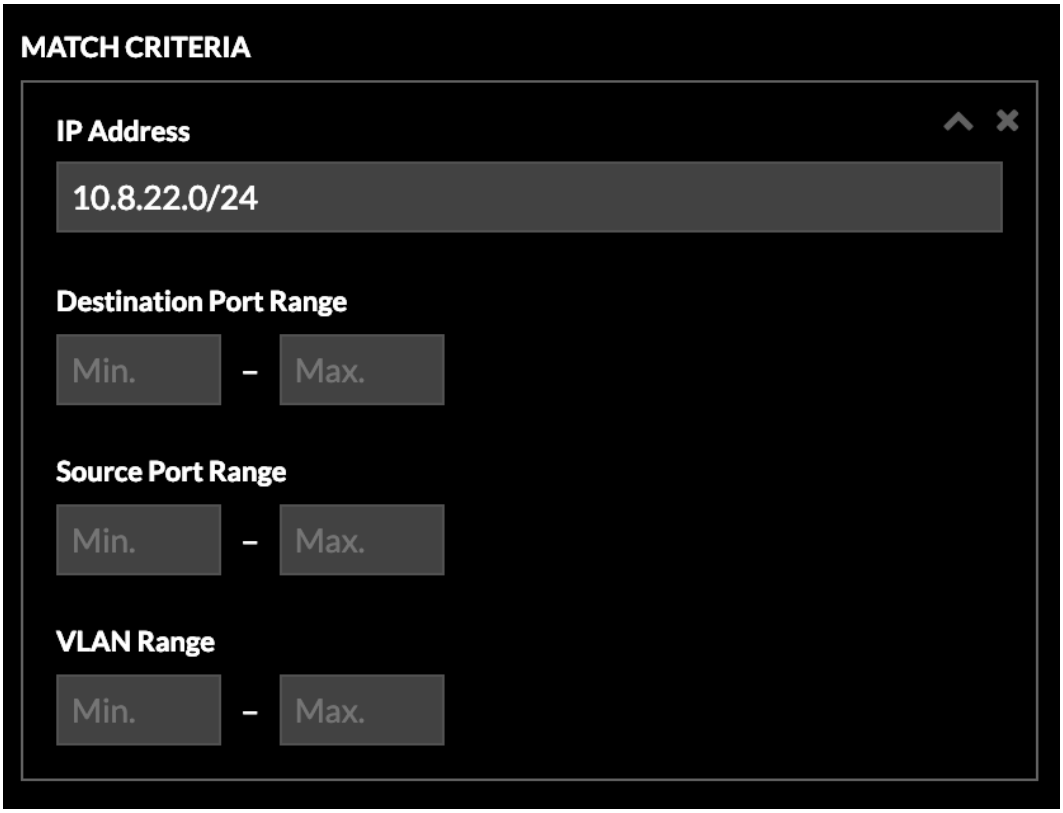
Fangen wir an, ein maßgeschneidertes Gerät für unsere Niederlassung in Seattle zu entwickeln.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

2. Klicken Sie auf das Symbol Systemeinstellungen in der oberen rechten Ecke der Seite, und klicken Sie dann auf **Maßgeschneiderte Geräte**.
3. Klicken Sie oben auf der Seite auf **Erstellen**.
4. In der **Name** Feld, geben Sie einen Namen für Ihr Gerät ein. Benennen Sie Ihr Gerät beispielsweise mit der Region der Zweigstelle. In diesem Beispiel geben Sie dem Gerät einen Namen `Seattle`.
5. In der **Discovery-ID** Feld, geben Sie eine eindeutige Kennung für das Gerät ein, z. B. eine Geschäfts- oder Büronummer. In diesem Beispiel geben Sie `Store_09045` für die Discovery-ID.

Hinweis: Wenn dieses Feld leer gelassen wird, wird die Discovery-ID aus dem benutzerdefinierten Gerätenamen generiert. Die Discovery-ID darf keine Leerzeichen enthalten und kann nach dem Speichern des benutzerdefinierten Gerät nicht geändert werden.

6. In der **Beschreibung** Feld, geben Sie Informationen ein, anhand derer dieses Remote-Netzwerk bei zukünftigen Suchen identifiziert werden kann. Geben Sie beispielsweise die Adresse der Zweigstelle ein, damit Sie nach diesem benutzerdefinierten Gerät anhand von Stadt oder Postleitzahl suchen können.
7. (Nur Konsole) Aus dem **Fühler** Wählen Sie in der Dropdownliste den Sensor aus, den Sie dem benutzerdefinierten Gerät zuordnen möchten.
8. klicken **Kriterien hinzufügen** um die IP-Adressen der Geräte anzugeben, für die Sie Messwerte sammeln werden.
9. In der **IP Adresse** Feld, geben Sie eine CIDR-Notation für das Subnetz der Niederlassung in Seattle ein. Für dieses Beispiel geben Sie `10,8,22,0/24`. Sie können die Port- und VLAN-Felder leer lassen.



10. klicken **Speichern**.

Ihr benutzerdefiniertes Gerät ist erstellt! Es dauert einige Minuten, bis das benutzerdefinierte Gerät Geräte im Remote-Netzwerk Netzwerk. Wenn das ExtraHop-System Traffic beobachtet, der die Übereinstimmungskriterien erfüllt (z. B. das 10.8.22.0/24-Subnetz), werden Metriken für dieses benutzerdefinierte Gerät verfügbar.

Als Nächstes erstellen wir ein Dashboard, um benutzerdefinierte Gerätemetriken einfach zu überwachen.

Erstellen Sie ein Dashboard

Sie können ein Dashboard erstellen, um bestimmte Diagramme und Daten für das von Ihnen erstellte benutzerdefinierte Gerät anzuzeigen.

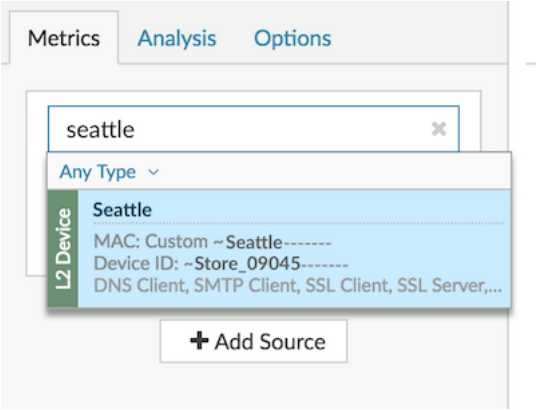
1. Klicken Sie oben auf der Seite auf **Dashboards**.
2. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke und wähle **Neues Dashboard** um ein leeres Dashboard zu erstellen.
3. Geben Sie einen Namen für Ihr Dashboard in der **Titel** Feld. Geben Sie für diese exemplarische Vorgehensweise ein `Verkehr in den Filialen in Seattle`.
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. Textfeld-Widgets können benutzerdefinierten erklärenden Text zu einem Dashboard oder Diagramm enthalten. Für diese exemplarische Vorgehensweise werden Sie jedoch keinen Text hinzufügen. 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 klicken **Löschen**.
   b) klicken **Widget löschen**.

Als Nächstes fügen Sie dem leeren Diagramm Durchsatzmetriken über das Verkehrsvolumen hinzu.

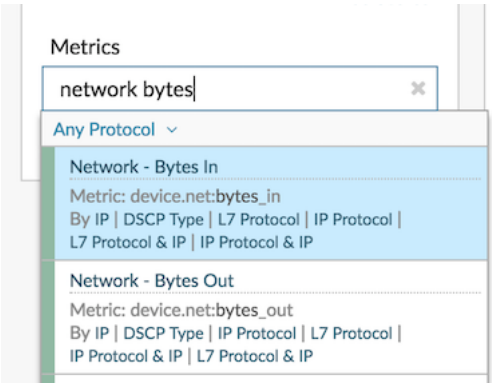
Netzwerkdurchsatz zu Ihrem Dashboard hinzufügen

Lassen Sie uns die Anzahl der Netzwerkbytes überwachen, die in das Remote-Netzwerk ein- und ausgehen.

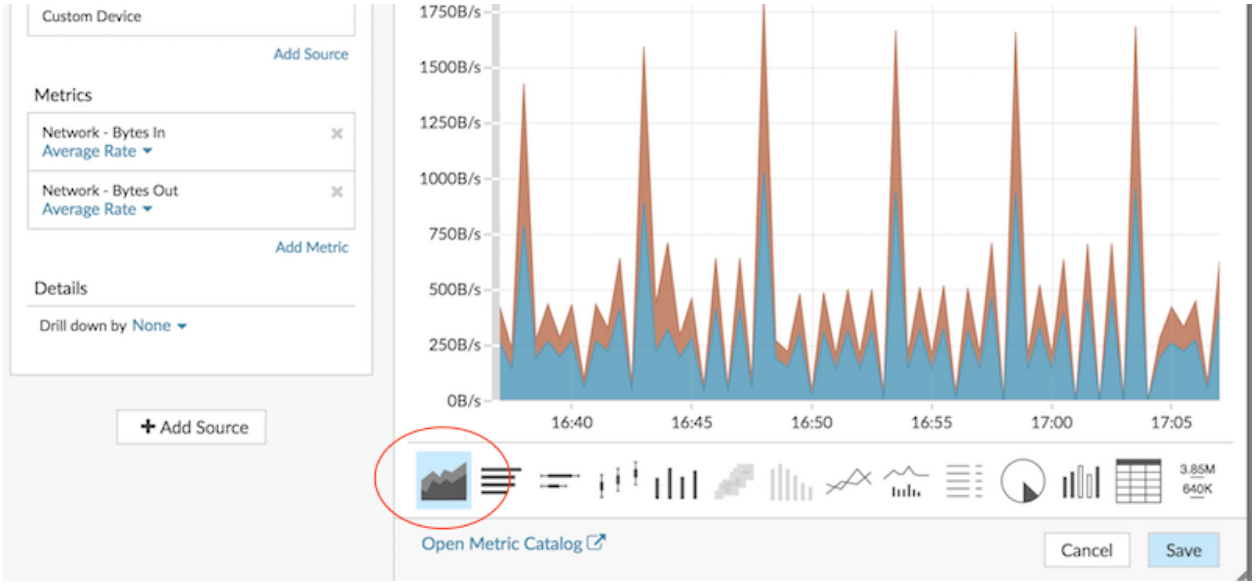
1. Klicken Sie in Ihrem neu erstellten Dashboard auf das leere Diagramm-Widget, um den Metric Explorer zu öffnen.
2. klicken **Quelle hinzufügen**.
3. In der Quellen Feld, Typ `Seattle`, und wählen Sie dann das benutzerdefinierte Gerät aus den Ergebnissen aus, wie im folgenden Beispiel gezeigt.



4. In der Metriken Feld, Typ `Netzwerk-Bytes`, und wählen Sie dann **Netzwerk — Eingehende Byte** aus den Ergebnissen, wie im folgenden Beispiel gezeigt.



5. klicken **Metrik hinzufügen**, typ `Netzwerk-Bytes`, und wählen Sie dann **Netzwerk — Ausgehende Bytes** aus den Ergebnissen.
6. Klicken Sie auf **Gebiet** Diagramm.



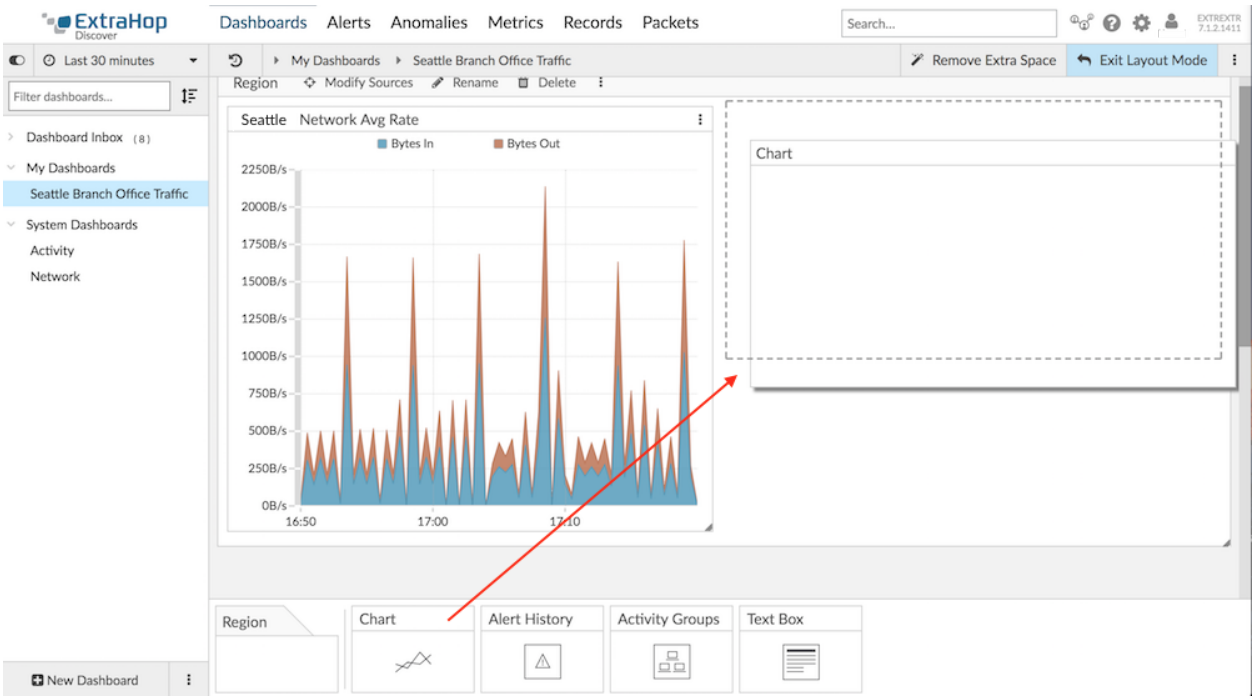
7. klicken **Speichern**.

Als Nächstes fügen Sie die Metrik Round Trip Time hinzu, um die Netzwerklatenz zu überwachen.

Fügen Sie Ihrem Diagramm die Netzwerklatenz hinzu

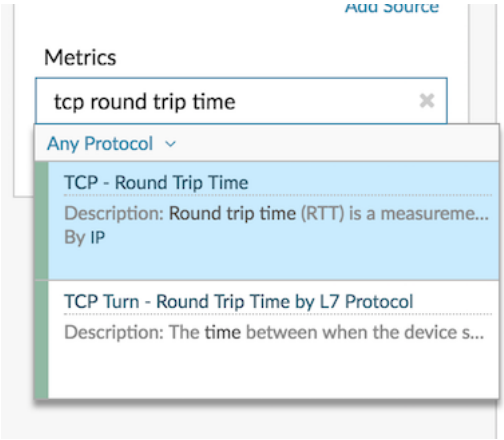
Lassen Sie uns nun überwachen, ob sich die Netzwerklatenz auf das Remote-Netzwerk auswirkt.

1. Klicken Sie unten auf der Seite „Dashboards“ auf ein Diagramm-Widget und ziehen Sie es in den leeren Bereich neben dem ersten Diagramm, wie im folgenden Beispiel gezeigt.

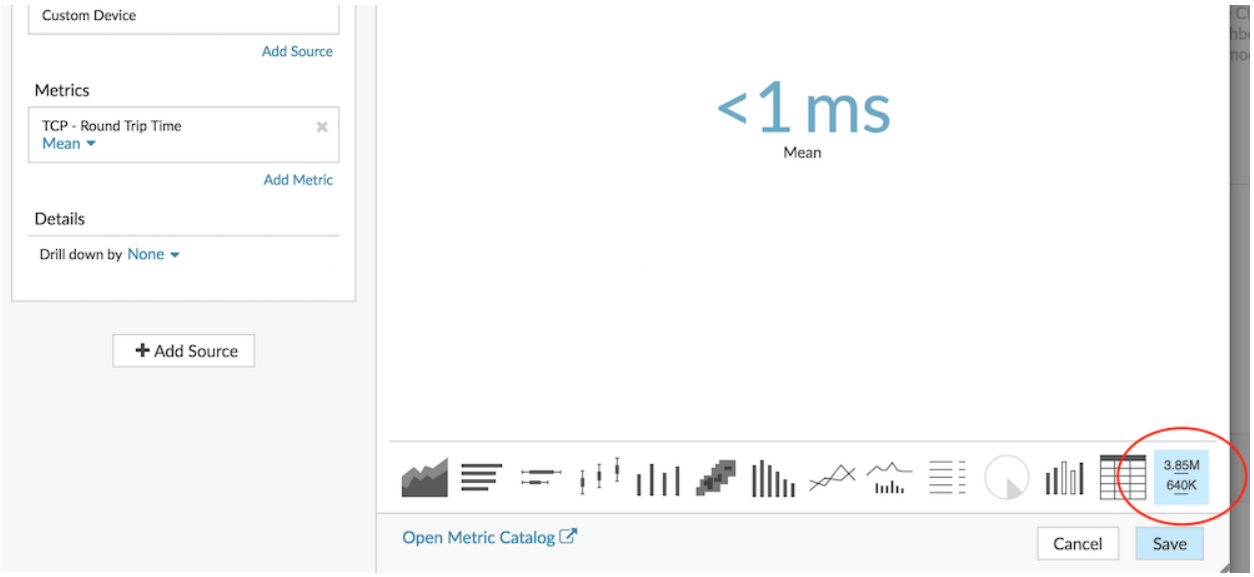


2. Klicken Sie auf das leere Diagramm.
3. klicken **Quelle hinzufügen**, typ `Seattle`, und wählen Sie dann **Seattle** aus den Ergebnissen.

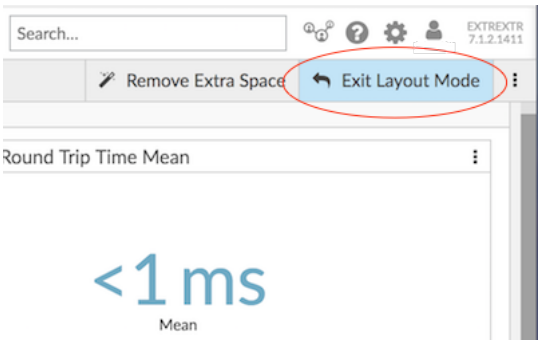
4. In der Metriken Feld, Typ `TCP-Hin- und Rückflugzeit`, und wählen Sie dann **TCP - Hin- und Rückflugzeit** aus den Ergebnissen, wie im folgenden Beispiel gezeigt.



5. Klicken Sie auf **Wert** Diagramm.



6. klicken **Speichern**.
7. Klicken Sie in der oberen rechten Ecke der Seite auf **Layoutmodus verlassen**.



Ihr Dashboard ist fertig! Sie können jetzt die Netzwerkleistung im Auge behalten, indem Sie die folgenden Aufgaben ausführen:

- Ein Dashboard teilen
- Hinzufügen einer Dynamische Basislinie zu einem Diagramm

Probleme beheben

Sie haben jetzt einige Diagramme, auf die Sie zurückgreifen können, wenn eine langsame Netzwerkleistung gemeldet wird. Die folgende Tabelle enthält Vorschläge zur Interpretation von Diagrammdaten und zur anschließenden Behebung von Problemen.

Mögliches Problem	Folgemaßnahmen
Ein plötzlicher Anstieg des Verkehrs	Untersuchen Sie die Daten der Dashboard-Diagramme, um zu verstehen, was zum Traffic beiträgt. Sie können auch Protokollseitendaten untersuchen. Klicken Sie auf den Diagrammtitel und dann auf den benutzerdefinierten Gerätenamen in der Gehe zu... Abschnitt. Eine Protokollseite für das benutzerdefinierte Gerät wird angezeigt. Erstellen Sie eine Aktivitätsdiagramm um Geräteverbindungen und das Verkehrsaufkommen zwischen Verbindungen zu sehen. Du kannst auch zwei Zeitintervalle vergleichen aus verschiedenen Geschäftszeiten, um den Unterschied in den Metrik Werten zu sehen.
Langsame Anwendung	Stellen Sie fest, ob die langsame Anwendung mit einem clientseitigen Problem in der Zweigstelle oder mit Servern im lokalen Rechenzentrum zusammenhängt. Klicken Sie auf den Diagrammtitel und dann auf den Namen des benutzerdefinierten Geräts in der Gehe zu... Abschnitt. Eine Protokollseite für das benutzerdefinierte Gerät wird angezeigt. Klicken Sie im Bereich Client-Aktivität im linken Bereich auf **HTTP**, **Datenbank**, **DNS**, oder **ICA** (Citrix), um clientseitige Fehlermetriken zu untersuchen. Klicken Sie im Abschnitt Serveraktivität auf Protokolle und untersuchen Sie Messwerte wie Fehler und Serververarbeitungszeit. Diese Messwerte zeigen Ihnen, dass Server möglicherweise zu dem Problem beitragen.
Zunahme des Verkehrsaufkommens im Laufe der Zeit	Hinzufügen einer Dynamische Basislinie zu einem Diagramm um Trends bei Verkehrsdaten im Zeitverlauf zu verfolgen. Beachten Sie, dass das ExtraHop-System beginnt, eine Dynamische Basislinie zu erstellen, nachdem sie dem Diagramm hinzugefügt wurde. Sie können keine Basisdaten mit historischen Daten anzeigen.

Mögliches Problem	Folgemaßnahmen
Zunahme von Netzwerküberlastungen oder anderen Datenübertragungsproblemen	Untersuchen Sie TCP-Metriken, um zu sehen, wie sich das Netzwerk auf die Anwendungsleistung auswirkt. Klicken Sie auf den Diagrammtitel und dann auf das benutzerdefinierte Gerät in der Gehe zu... Abschnitt des Drop-down-Menüs. Eine Protokollseite für das benutzerdefinierte Gerät wird angezeigt. Suchen Sie nach großen Werten für die folgenden Metriken: • Timeouts für die erneute Übertragung (RTOs In/Out) bei Netzwerküberlastung • Round Trip Time (RTT) für Netzwerklatenz • Empfangen Sie Window Throttling und Zero Windows bei Datenübertragungsproblemen