Karten mit Aktivitäten

Veröffentlicht: 2023-10-24

Eine Aktivitätsdiagramm ist eine dynamische visuelle Darstellung der L4-L7-Protokollaktivität zwischen Geräten in Ihrem Netzwerk. Sie können sich ein 2D- oder 3D-Layout der Geräteverbindungen in Echtzeit ansehen , um mehr über den Verkehrsfluss und die Beziehungen zwischen Geräten zu erfahren.

Activity Maps können Ihnen bei den folgenden Anwendungsfällen helfen:

Schließen Sie eine Rechenzentrum- oder Cloud-Migration ab

Im Rahmen Ihrer Migrationsstrategie müssen Sie festlegen, welche Dienste wann ausgeschaltet werden können. Mithilfe einer Aktivitätsdiagramm können Sie erkennen, welche Geräte noch verbunden sind, sodass Sie unerwartete Serviceunterbrechungen während des Migrationsprozesses verhindern können. Weitere Informationen finden Sie in der Planen und überwachen Sie Ihre Migration mit Activity Maps Komplettlösung.

Identifizieren Sie die Hauptursache für eine langsame Anwendung

Anwendungen hängen häufig von mehreren Dienstebenen innerhalb eines Netzwerk ab. Mithilfe einer Activity Map können Sie die Lieferkette des Datenverkehrs zu Ihrem langsamen Anwendungsserver identifizieren. Klicken Sie auf ein Gerät, um verwandte Kennzahlen zu untersuchen, die mehr Aufschluss über die Ursache der Verlangsamung geben können.

Verfolgen Sie verdächtige Geräte oder unerwartete Verbindungen

Während eines Sicherheitsereignisses kann Ihnen eine Aktivitätsdiagramm dabei helfen, betroffene Geräte zu identifizieren, indem sie den mit einem verdächtigen Gerät verbundenen Ost-West-Verkehr in Echtzeit verfolgt. Im Rahmen einer täglichen Sicherheitsüberwachungsstrategie können Sie eine Aktivitätsdiagramm erstellen, um sicherzustellen, dass Geräte keine unerwarteten Verbindungen mit anderen Geräten herstellen.

Hier sind einige wichtige Überlegungen zu Activity Maps:

- Du kannst Aktivitätskarten erstellen für Geräte in den Bereichen Advanced, Standard, L2 Parent Analysis und Flow Analysis. Sie können keine Aktivitätsdiagramm für Geräte im Entdeckungsmodus erstellen. Weitere Informationen finden Sie unter Prioritäten der Analyse.
- Wenn Sie eine Aktivitätsdiagramm für ein Gerät oder eine Gerätegruppe erstellen, die während des ausgewählten Zeitintervalls keine Protokollaktivität aufweist, wird die Map ohne Daten angezeigt. Ändern Sie das Zeitintervall oder Ihre Herkunftsauswahl und versuchen Sie es erneut.
- Sie können eine Aktivitätsdiagramm aus einem erstellen Konsole um die Geräteverbindungen all Ihrer Sensoren zu sehen.
- Du kannst Speichern und Teilen einer Aktivitätsdiagramm, gewährt anderen Systembenutzern oder Gruppen Ansichts- oder Bearbeitungszugriff. Du kannst auch eine gespeicherte Aktivitätsdiagramm laden um Karteneigenschaften zu ändern.

Weitere Informationen zu Aktivitätskarten finden Sie in der Häufig gestellte Fragen zu Activity Maps.

Navigiere durch Aktivitätskarten

Nach eine Aktivitätskarte erstellen, können Sie mit der Untersuchung von Daten beginnen. In den folgenden Abschnitten finden Sie Informationen zur Interaktion mit einer Aktivitätsdiagramm und Informationen zu den Daten, die Sie sich gerade ansehen.

Grundriss

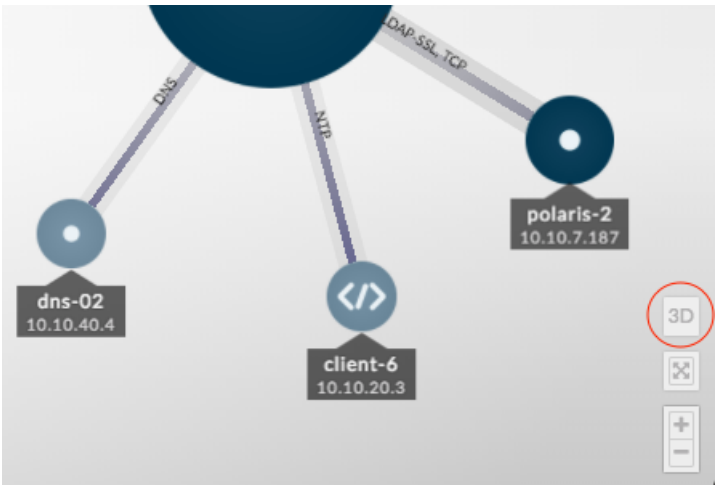
Geräte werden durch Kreise und Verbindungen durch Linien dargestellt.

Die Platzierung der Geräte ist für die Anzeige von Informationen optimiert. Das Layout kann sich ändern, wenn Daten zur Geräteaktivität in Echtzeit aktualisiert werden. Beispielsweise wird das Layout aktualisiert , wenn neue Verbindungen beobachtet werden oder Geräte inaktiv werden.

Hinweis: Wenn das Zeitintervall in der oberen linken Ecke der Seite auf Letzte 30 Minuten, Letzte 6 Stunden oder Letzter Tag eingestellt ist, werden die Aktivitätsdiagramm Map-Daten kontinuierlich jede Minute mit Echtzeitdaten aktualisiert. Legen Sie ein benutzerdefiniertes Zeitintervall mit einer bestimmten Start- und Endzeit fest, um Layoutaktualisierungen in Echtzeit zu stoppen.

2D- oder 3D-Layout

Standardmäßig werden Aktivitätskarten in einem 2D-Layout angezeigt, aber Sie können auf 3D klicken, um die Anzeige in ein rotierendes 3D-Modell zu ändern. Möglicherweise möchten Sie 3D-Karten auf einem großen Bildschirm in einem Netzwerk- oder Sicherheitszentrum präsentieren.

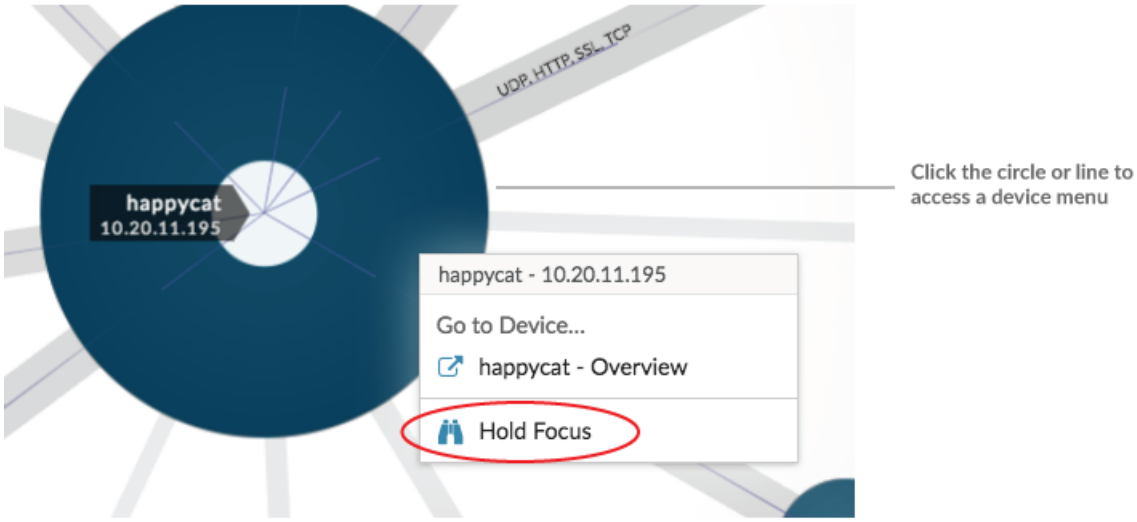


Neu positionieren, drehen und zoomen

Zoomen Sie mit den Steuerelementen in der unteren rechten Ecke der Seite in eine Karte hinein und heraus oder zoomen Sie mit dem Mausrad. Klicken und ziehen Sie mit der Maus, um eine 2D-Karte neu zu positionieren oder eine 3D-Karte zu drehen.

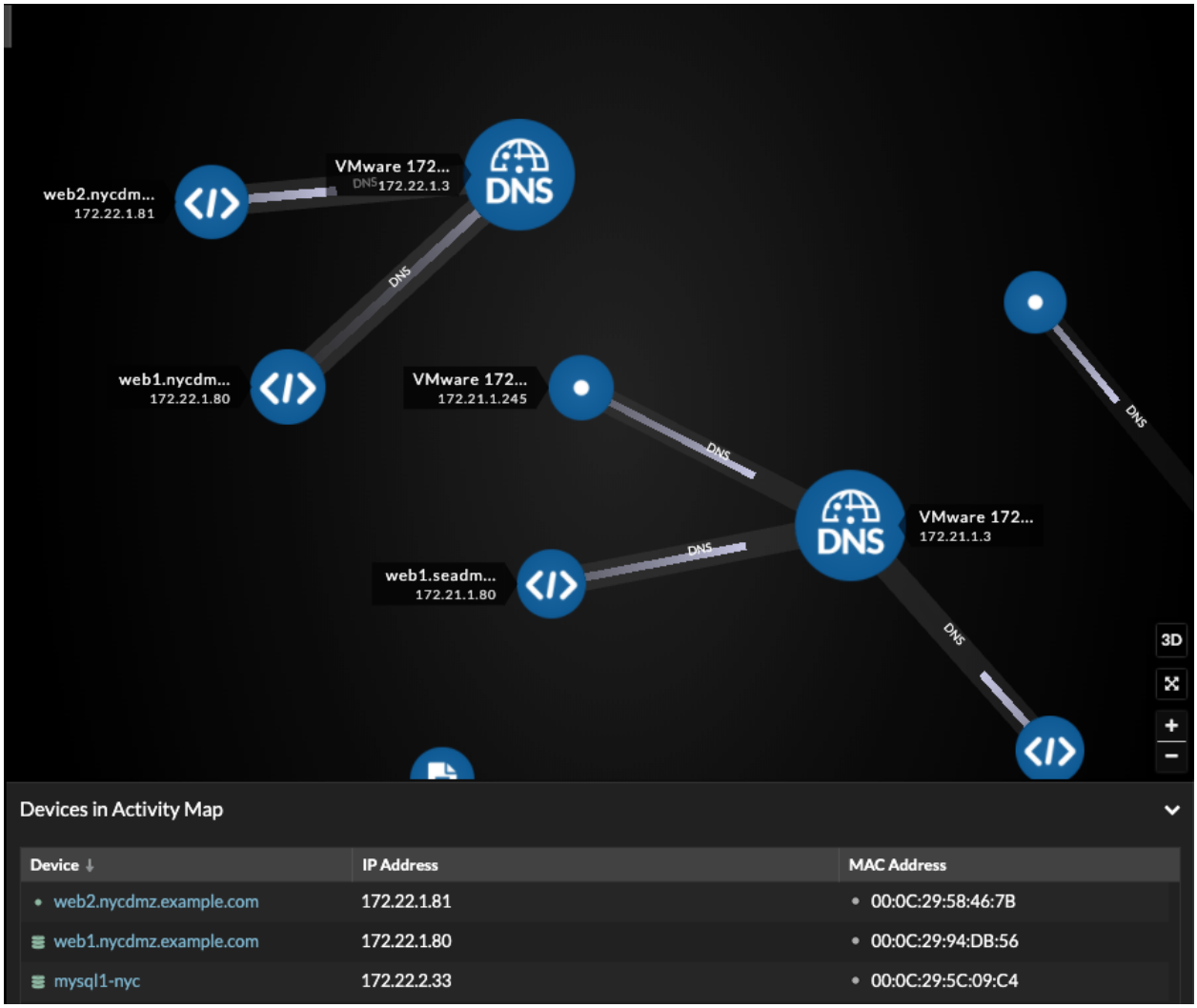
Fokus behalten

Klicken Sie auf ein beliebiges Gerät und wählen Sie **Fokus halten**. Sie können dann je nach Layout neu positionieren oder drehen und die Karte vergrößern oder verkleinern, während Sie sich auf das ausgewählte Gerät und seine unmittelbaren Gegenspieler konzentrieren.



Geräteliste anzeigen

klicken **Geräte in der Activity Map** unten auf der Seite, um eine Liste aller Geräte mit ihren Namen, IP-Adressen und MAC-Adressen anzuzeigen. Klicken Sie auf einen Gerätenamen, um zur Geräteseite zu navigieren.

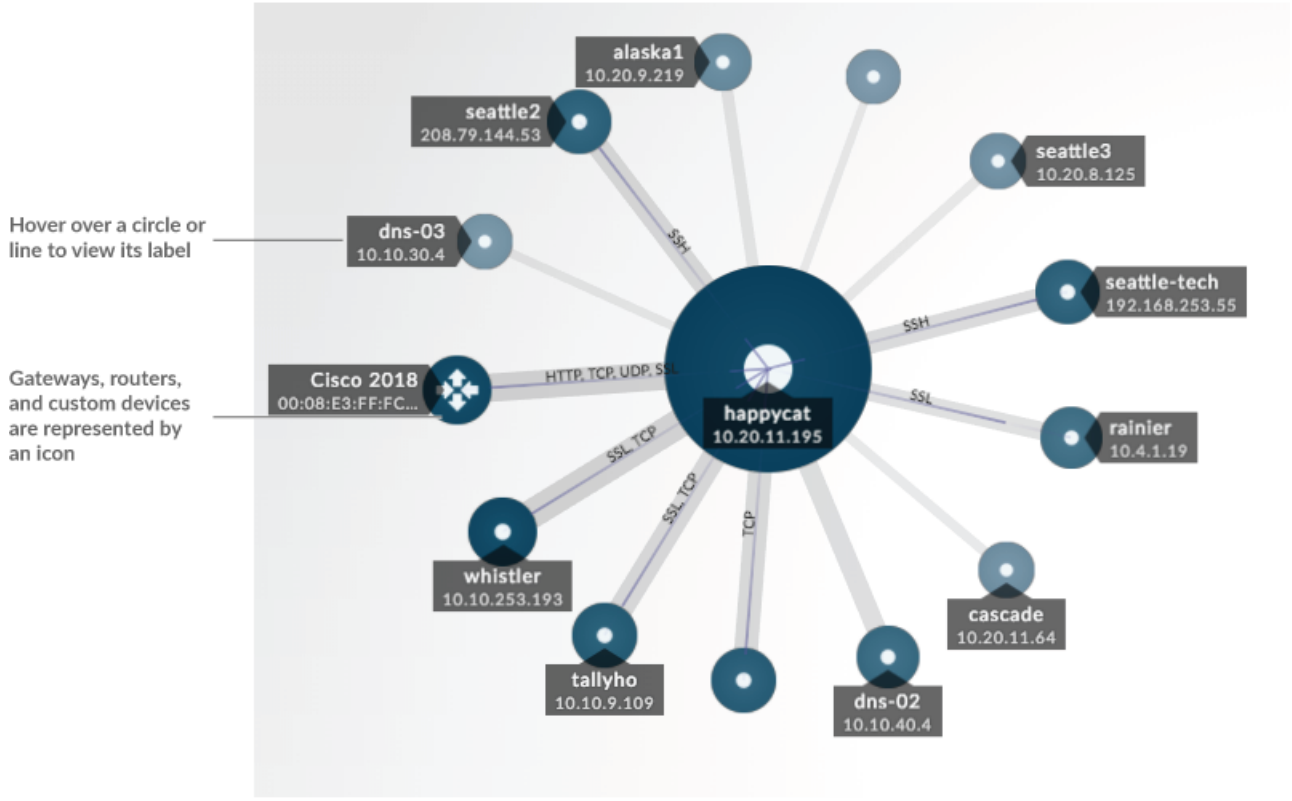


Beschriftungen und Icons

Kreisbeschriftungen enthalten Details wie den Hostnamen, die IP-Adresse oder die MAC-Adresse des Gerät.

Linienbeschriftungen enthalten Protokollnamen, die mit der Geräteverbindung und der Richtung des Datenverkehrs zwischen den Geräten verknüpft sind, was als animierte Impulse angezeigt wird. Spezifisch Geräterollen werden durch ein Symbol dargestellt.

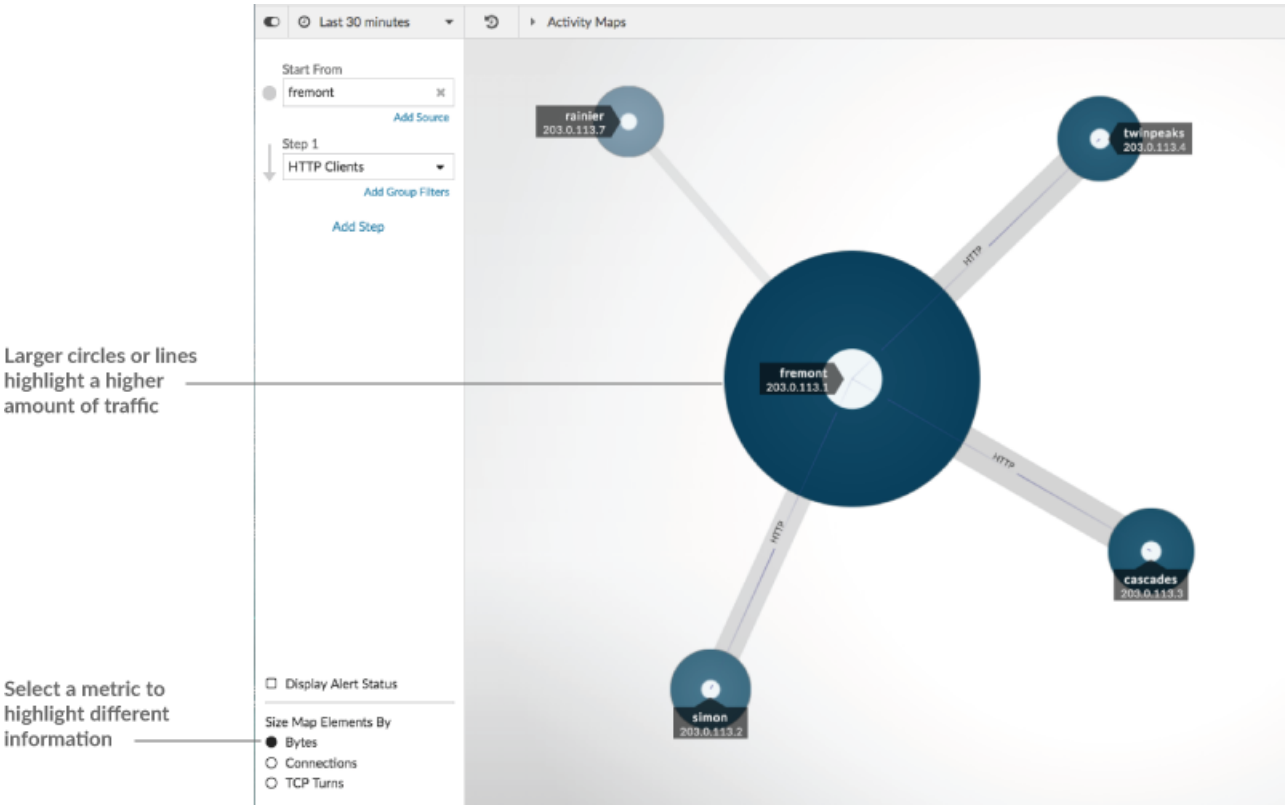
Um die Anzeige von Informationen zu optimieren, wird nicht jedes Etikett angezeigt. Bewegen Sie den Mauszeiger über einen Kreis oder eine Linie, um deren Bezeichnung anzuzeigen, wie in der folgenden Abbildung dargestellt.



Hinweis: Geräterollen werden einem Gerät automatisch zugewiesen, basierend auf der Art des Datenverkehrs, den das ExtraHop-System für dieses Gerät beobachtet. Weitere Informationen finden Sie unter Eine Geräterolle ändern.

Kreis- und Liniengröße

Die Größe der Objekte in der Karte entspricht einem Metrikwert, der dazu beiträgt, Bereiche mit erhöhter Aktivität hervorzuheben, z. B. die Anzahl der Byte oder das Verkehrsaufkommen, die mit einer Geräteverbindung verbunden sind.



Unten im linken Bereich können Sie eine andere Metrik für Kartenelemente auswählen:

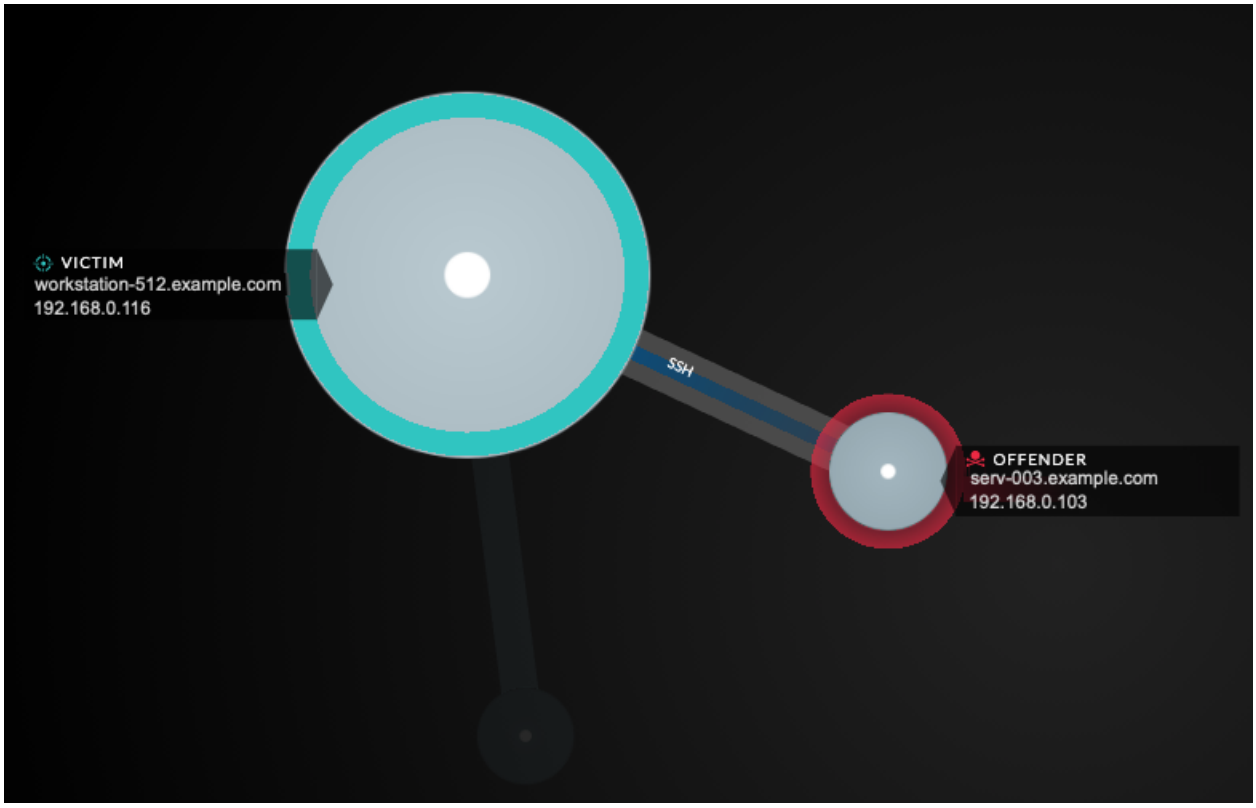
- **Byte:** Sehen Sie sich alle Geräte an, die während des Zeitintervalls Daten senden oder empfangen.
- **Verbindungen:** Es werden nur die Geräte angezeigt, die während des Zeitintervalls mindestens einmal eine neue Verbindung hergestellt haben.
- **TCP-Kurven:** Es werden nur die Geräte angezeigt, die während des Zeitintervalls mindestens einmal zwischen Senden und Empfangen von Daten gewechselt haben.

Farbe

Blau und Grau sind Standardfarben für Kreise und Linien. Diese Standardfarben sind für die Anzeige von Informationen in einer Karte optimiert. Sie können Ihrer Karte jedoch unterschiedliche Farben zuweisen, um den Schweregrad einer Alarm hervorzuheben oder anzuzeigen, wann eine Geräteverbindung hergestellt wurde.

Erkennungen

Erkennungen Die einem Gerät auf der Karte zugewiesenen Geräte erscheinen um den Kreis herum als animierte Impulse, sogenannte Erkennungsmarkierungen. Die Farbe des Pulses ist rot, wenn das Gerät der Täter ist, und blaugrün, wenn das Gerät Opfer der Erkennung ist. Der Teilnehmerstatus erscheint auch auf dem Geräteetikett.



Hinweis: Erkennungen durch maschinelles Lernen erfordern eine Verbindung zu ExtraHop Cloud Services.

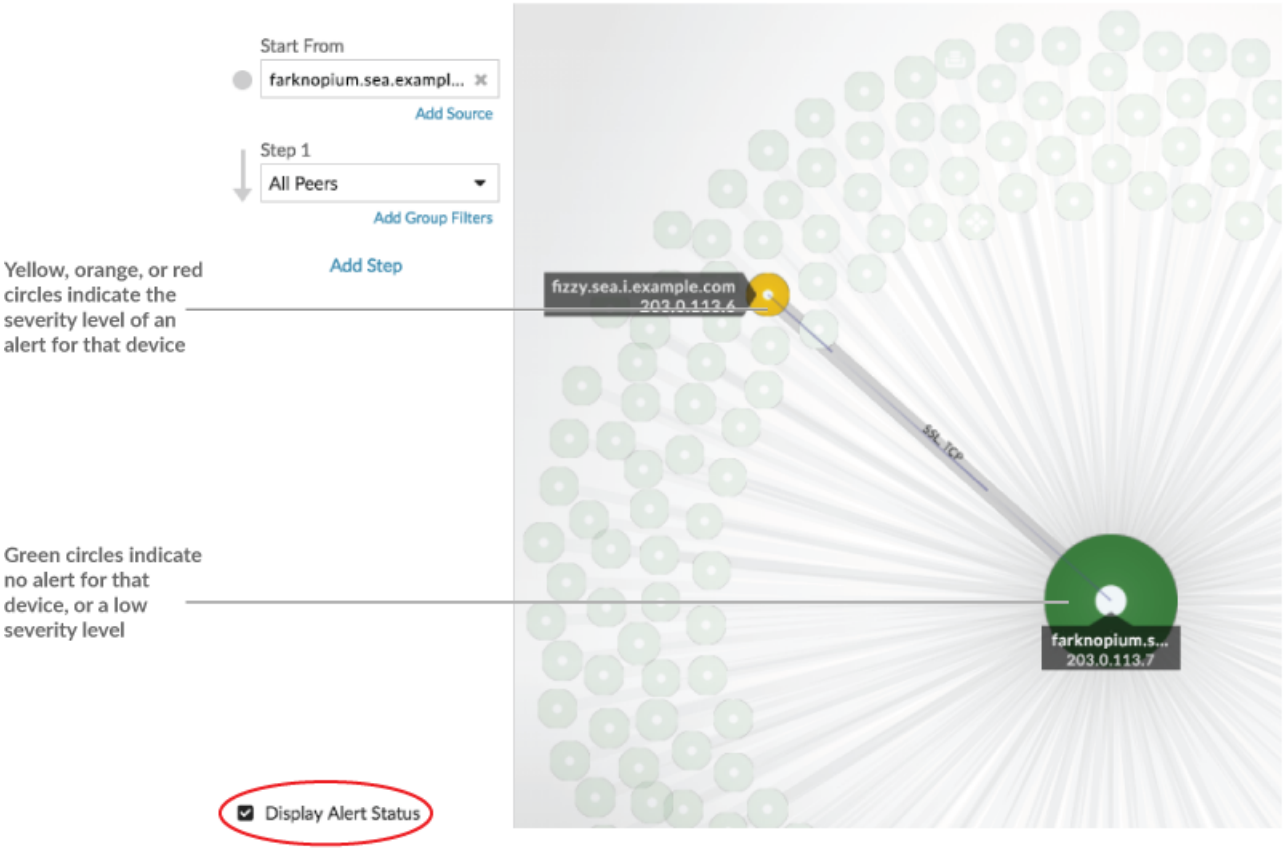
Klicken Sie auf einen Kreis mit einer Erkennungsmarkierung, um zugehörige Erkennungen anzuzeigen und zu ihnen zu navigieren, oder Seite „ Geräteübersicht“.

Wenn Erkennungsmarkierungen nicht wie erwartet auf Ihren Aktivitätskarten angezeigt werden, sind Erkennungsmarkierungen möglicherweise deaktiviert. Du kannst Erkennungsmarkierungen aktivieren oder deaktivieren von der **Nutzer** Speisekarte.

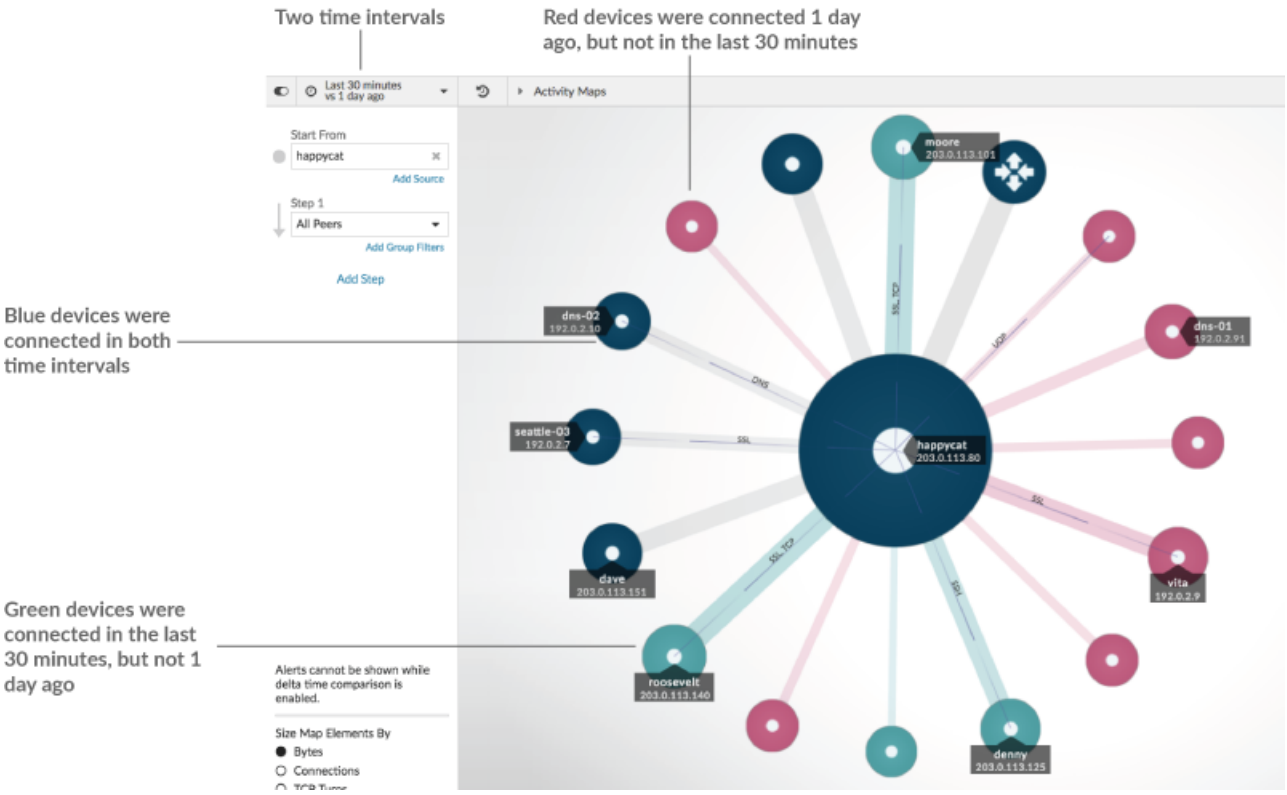
Alarmstatus (NPM-Modulzugriff erforderlich)

Um den Schweregrad einer Alarm für ein Gerät in Ihrer Karte anzuzeigen, wählen Sie **Warnstatus anzeigen** in der unteren linken Ecke oder auf der Seite, wie in der folgenden Abbildung dargestellt. Die Kreisfarbe entspricht dann dem schwerwiegendsten Status für alle Alarme, die einem Gerät während des Zeitintervalls zugewiesen wurden. Wenn einem Gerät keine Alarm zugewiesen ist oder die Warnstufe informativ ist, ist die Standardfarbe des Kreises grün.

Um die Alarm zu untersuchen, klicken Sie auf den Kreis und wählen Sie dann den Gerätenamen in der Gehe zu Gerät... Abschnitt. Scrollen Sie auf der Protokollseite des Geräts nach unten zu die Seite „Benachrichtigungen“ anzeigen.



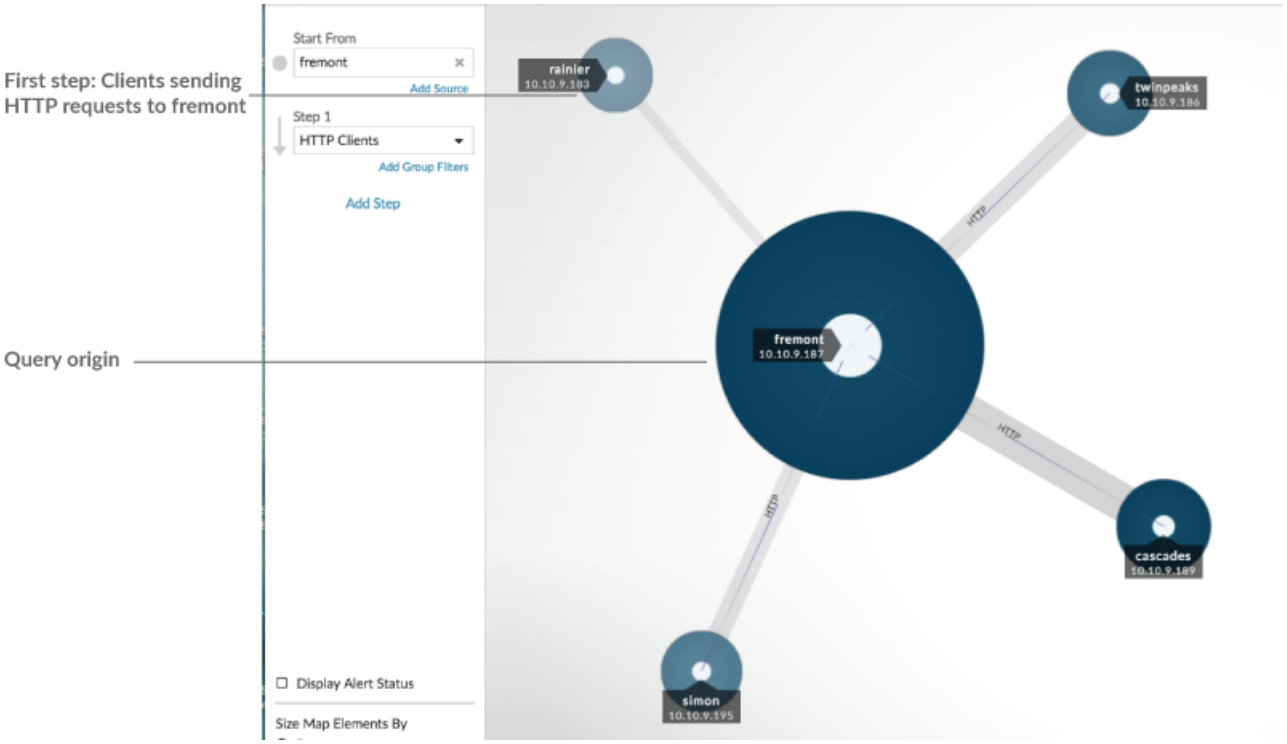
Vergleich von Zeitintervallen
Wenn du Vergleiche zwei Zeitintervalle, um Metrik Deltas zu finden, anhand verschiedener Farben in der Karte können Sie feststellen, wann Geräteverbindungen hergestellt wurden oder wann sich die Protokollaktivität für ein Gerät geändert hat. Zum Beispiel nach dem Erstellen eines Vergleichs zwischen **Gestern** und der **Letzte 30 Minuten**, neue Geräteverbindungen oder Aktivitäten, die nur im neueren Zeitintervall auftreten, werden grün angezeigt. Frühere Geräteverbindungen oder Aktivitäten, die nur im früheren Zeitintervall aufgetreten sind, sind rot. Geräteverbindungen, die sich zwischen den Zeitintervallen nicht geändert haben, sind blau. In der folgenden Abbildung werden neue Verbindungen, die in den letzten dreißig Minuten hergestellt wurden, durch grüne Kreise und Linien dargestellt.



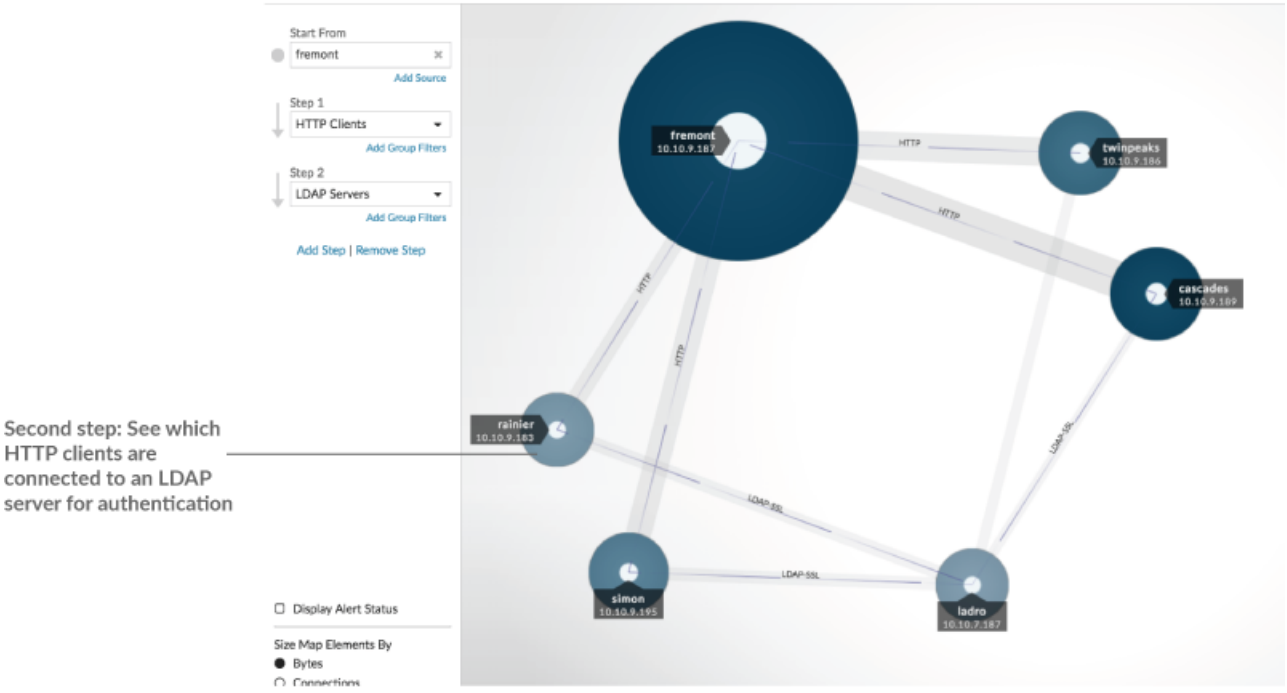
Hinweis: Wenn alle Geräte eine einzige Farbe haben, z. B. grün, bedeutet dies, dass die Abfrage im früheren Zeitintervall keine Ergebnisse erbracht hat. Beispielsweise hatte das Ursprungsgerät im früheren Zeitintervall keine Protokollaktivität.

Schritte und Filter zu einer Map hinzufügen

Ein Schritt ist eine Ebene von Verbindungen zwischen Geräten. Die Geräte in jedem Schritt haben eine Beziehung zu den Geräten im vorherigen Schritt. Diese Beziehungen werden durch ihre Protokollaktivität definiert.



Fügen Sie einer Aktivitätsdiagramm einen neuen Schritt hinzu, um Ihrer Karte eine weitere Informationsebene hinzuzufügen. Klicken Sie auf die Dropdownliste für einen bestimmten Schritt und wählen Sie dann eine Protokollaktivität aus.



Sie können Geräte auch in einem Schritt nach ihrer Gruppenmitgliedschaft filtern. Wenn Sie beispielsweise HTTP-Server auswählen, aber nur Ihre Testserver in der Map sehen möchten, können Sie HTTP-Server nach einer Gerätegruppe filtern, z. B. Meine Testserver.

Weitere Informationen zum Hinzufügen von Schritten und Filtern zu einer Map finden Sie unter Erstellen Sie eine Aktivitätsdiagramm.

Aktivitätskarten verwalten

Die folgenden Optionen zur Verwaltung deiner Aktivitätsdiagramm sind im Befehlsmenü in der oberen rechten Ecke verfügbar:

- Speichern und teilen Sie eine Aktivitätsdiagramm
- Eine gespeicherte Aktivitätsdiagramm laden und verwalten
- Aktivitätsdiagramm als PDF-, PNG- oder SVG-Datei exportieren

Bewährte Methoden für die Untersuchung von Aktivitätsdiagramm Map-Daten

Wenn Sie auf Ihrer Karte ein Gerät finden, das es wert ist, untersucht zu werden, haben Sie mehrere Möglichkeiten, weitere Informationen über dieses Gerät zu sammeln.

Suchen Sie nach kürzlich verbundenen Geräten

Klicken Sie auf das Zeitintervall in der oberen linken Ecke der Seite und klicken Sie auf **Vergleiche**. Sie können sehen, wie sich die Geräteverbindungen zwischen zwei verschiedenen Zeitintervallen geändert haben.

Weitere Informationen finden Sie unter Vergleich von Zeitintervallen.

Navigieren Sie zu den Protokollseiten, um verwandte Metrikaktivitäten zu finden

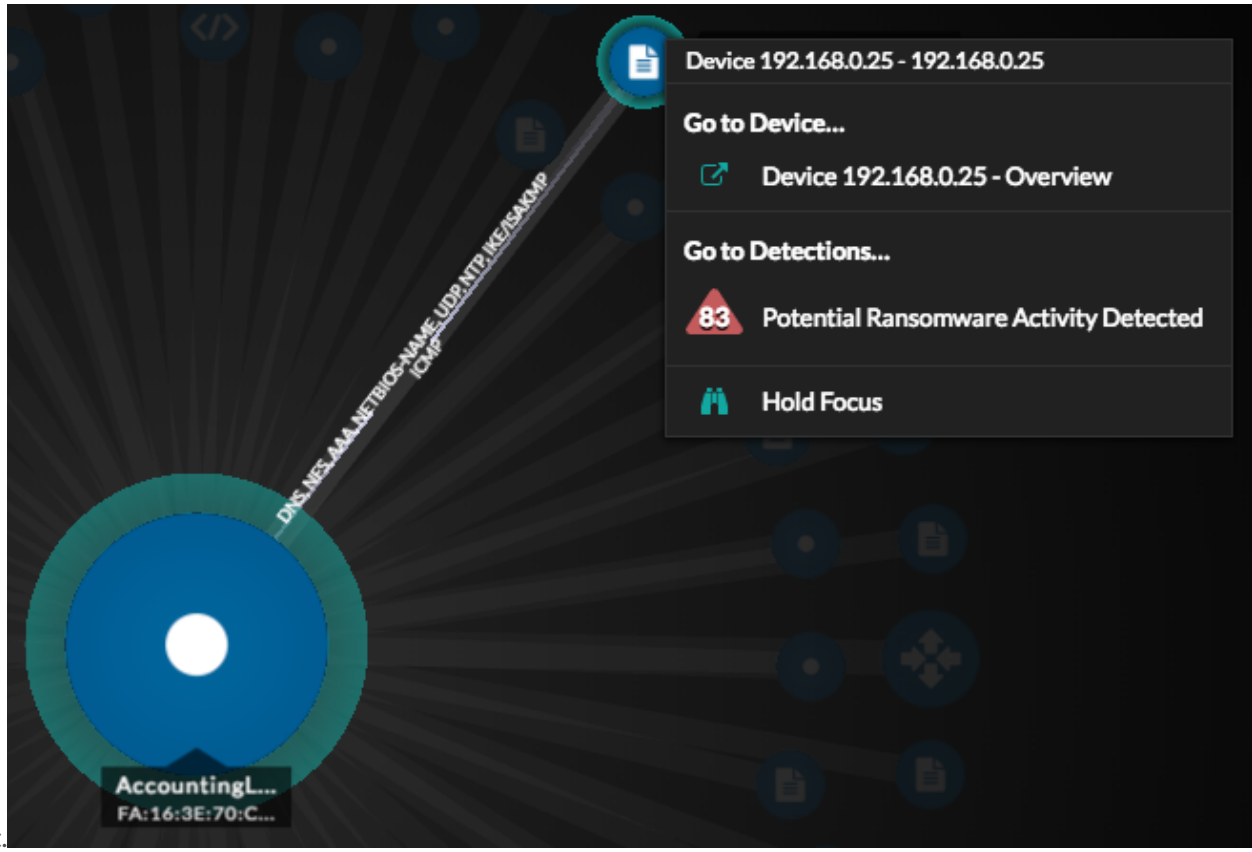
Klicken Sie auf einen Kreis oder eine Linie, um ein Dropdownmenü aufzurufen, wie in der folgenden Abbildung dargestellt.

Wählen Sie den Gerätenamen aus dem Menü aus, um die Seite Geräteübersicht aufzurufen. Klicken Sie im linken Bereich auf einen Protokollnamen, um die Protokollseite aufzurufen, die eine Zusammenfassung wichtiger Protokollmetriken enthält, die beobachtet wurden und mit dem Gerät verknüpft wurden. Auf einer Protokollseite finden Sie verwandte Metriken wie Fehler, Anfragen, Antworten und Serververarbeitungszeit. Sie können eine Metrik auch von einer Protokollseite aus aufschlüsseln, um Metrikdetails wie Server-IP-Adresse, Client-IP-Adresse, Statuscodes, Methoden und URIs anzuzeigen.

Navigieren Sie zu den auf dem Gerät identifizierten Erkennungen

Geräte auf einer Aktivitätsdiagramm, denen Erkennungen zugeordnet sind, werden als animierte Impulse rund um das kreisförmige Etikett angezeigt. Klicken Sie auf einen Kreis mit dieser

Erkennungsmarkierung, um ein Dropdownmenü aufzurufen, wie in der folgenden Abbildung dargestellt.



Wählen Sie einen Erkennungsnamen aus dem Menü aus, um zur Detailseite für diese Erkennung zu gelangen. Die Detailseite enthält Informationen über die Art der Erkennung und ihre Bedeutung sowie über den Zeitpunkt der Erkennung und die Dauer des Problems. Weitere Informationen finden Sie unter Seite mit Erkennungsdetails.

Suchen Sie nach Transaktionsdatensätzen, die mit einer Verbindung verknüpft sind (erfordert einen konfigurierten Recordstore)

Klicken Sie auf einen Kreis oder eine Linie, um das Drop-down-Menü aufzurufen. klicken **Aufzeichnungen**. Eine Datensatzabfrageseite wird geöffnet und zeigt alle Datensätze von jedem verbundenen Gerät an, einschließlich aller Datensatztypen, die den Geräteverbindungsprotokollen zugeordnet sind.