

Assets

Published: 2020-04-01

All of the metric activity collected from the wire data on your network is logically grouped into sections on the Assets page, where you can navigate to find the data you need.

Devices

Devices, also known as assets and endpoints, are objects on your network with a MAC address or IP address that have been automatically discovered and classified by the ExtraHop system. Assign any device to a chart, alert, or trigger as a metric source. [Learn more about Devices](#).

Device Groups

[Device groups](#) are user-defined sets of devices that can be collectively assigned as a metric source to a chart, alert, or trigger. You can [create a dynamic device group](#) that adds devices that matches your specified criteria or you can [create a static device group](#) and manually add or remove devices.

You can also assign the following built-in device groups as a metric source:

New Devices (Last 24 Hours)

This device group includes assets and endpoints that were first seen by the ExtraHop system over the last 24 hours until now.

New Device (Last 7 Days)

This device group includes assets and endpoints that were first seen by the ExtraHop system over the last 7 days until now.

Vulnerability Scanners

This device group includes devices that are designated or acting as vulnerability scanners. For example, a device that sends an HTTP request associated with known scanner activity is automatically added to this device group.

VMware

This device group includes assets and endpoints that were automatically associated with the VMware vendor role.

Domain Controllers

This device group includes devices that are designated or acting as domain controllers. The ExtraHop system considers a device a domain controller if it has processed all of the following types of activity in the last 30 minutes:

- Kerberos server
- CIFS server
- MSRPC server

Mobile Devices

This device group includes devices that are designated or acting as mobile devices. The ExtraHop system considers a device a mobile device if it has iOS or Android software installed.

Web Proxy Servers

This device group includes devices that are designated or acting as web proxy servers. The ExtraHop system considers a device a web proxy server if it has processed an HTTP/1.x request between a device and another server in the last 30 minutes.

DHCP Server

This device group includes devices that are designated or acting as DHCP servers. The ExtraHop system considers a device a DHCP server if it has dynamically assigned network parameters to client devices in the last 30 minutes.

Protocols

The Protocols page displays a list of the protocol activity found on your network. Click any protocol to see a built-in page with specific metric charts about that protocol activity.

You can also monitor protocol traffic through the following options:

- Add the protocol as an activity group to a chart.
- [Create an activity map](#) for a protocol to see all device-to-device connections. Learn about traffic flow between devices in [Activity maps](#).

Learn more about protocol metrics in the [Protocol Metrics Reference](#), which contains descriptions for all of the metrics that appear in the ExtraHop system.

Users

The Users page displays a list of all active users found on your network and the devices the user logged in to. The user name is extracted from the authentication protocol, such as LDAP or Active Directory. [Search for devices accessed by a specific user](#).



Note: These users are not associated with user accounts for the ExtraHop system.

Applications

Applications are user-defined containers that represent distributed systems on your network. Create an application to view all of the metric activity associated with your website traffic—web transactions, DNS requests and responses, and database transactions. See the [Applications FAQ](#).

Basic applications that filter built-in metrics by protocol activity can be [created through the Web UI](#). Complex applications that collect custom metrics or metrics from non-L7 traffic must be [created through a trigger](#), which requires JavaScript code. Learn more about [building Triggers](#).

Networks

Networks are the wire network or flow network data feeds to the ExtraHop system. Click an entry to see the VLANs associated with a wire data capture, or click an entry to see the interfaces associated with a flow network.