Network Overview

Published: 2021-08-28

The Network Overview displays the active devices on your network, how they are communicating, and trends in important metrics. The Network Overview refreshes activity map and network health indicator data every minute.

Site Selector

Click the site selector at the top of the page to view data for one or more sites in your environment. View combined traffic across your networks or focus on a single site to help you quickly find device data. The site selector indicates when all or some sites are offline. Because data is not available from offline sites, the charts and device pages associated with offline sites might not show data or might only show limited data. The site selector is available from Command appliances and Reveal(x) 360 only.

Executive Report

Click **Generate Executive Report** to create a PDF file. The Executive Report provides a summary of the top detections and risks to your network from the last week. The Executive Report only includes information for the selected sites.

Active Devices

This count chart shows you the total number of devices that have been discovered by your ExtraHop system. Click the number to view a list of all discovered devices. The percentage shows you the rate of change for the selected time interval.

New Devices

This count chart shows you how many devices have been discovered within the past five days. Click the number to view a list of all of these devices.

Activity maps

An activity map cycles through the following protocols each minute when activity is detected:

- CIFS
- Database (DB)
- DNS
- FTP
- HTTP
- LDAP
- SSH
- SSL
- Telnet

Here are some ways you can interact with the activity map:

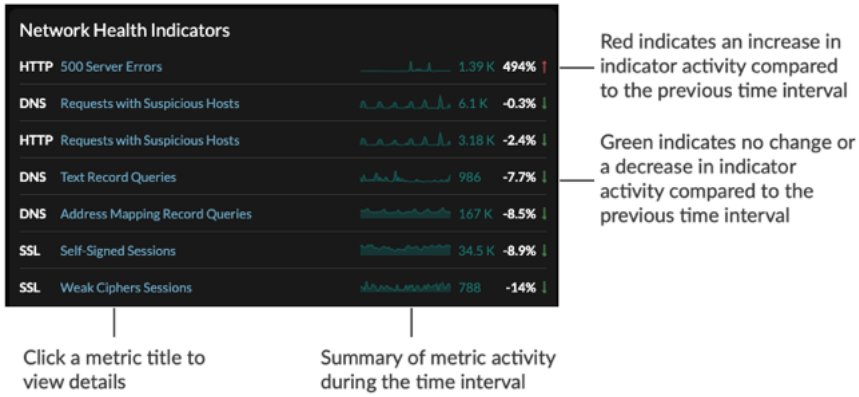
- Click the protocol name to open the activity map in a view that enables you to add steps and group filters. You can then save your modified activity map to revisit.
- Click the arrows around the protocol name to cycle through the available protocols. Protocols without activity in the specified time interval do not display.
- Click controls from the lower right corner of the activity map to pause and resume cycling, toggle between 2D and 3D visualization, and to zoom in and out of the map.
- Hover over a circle to see device labels and highlight device connections.
- Click a circle and then click the device name to view a protocol page for the device.

Learn more about navigating activity maps.

Network health indicators

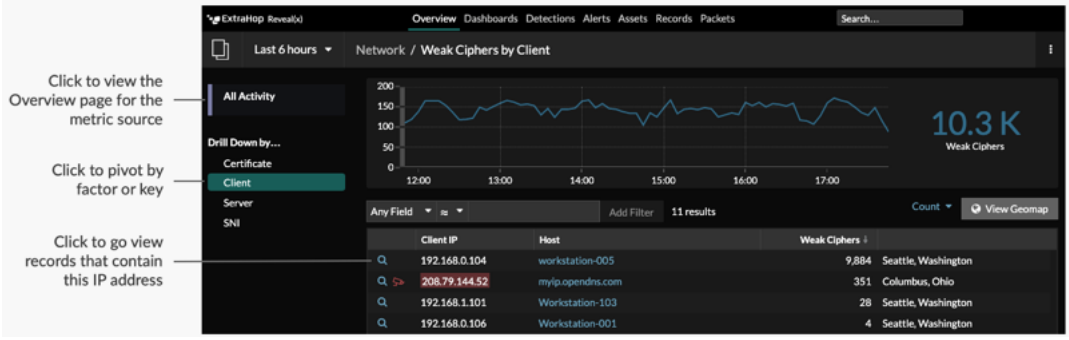
Network health indicators show you general trends related to network and security health. Network health indicators might signal weaknesses or issues in network performance or potentially suspicious activity.

Each network health indicator displays the percentage of change in network activity compared to the previous time interval. Metrics are listed in descending order, by percentage of greatest change to least. Network health indicators with no activity during the specified time interval are not displayed.



Depending on the type of network activity and the amount of change, you can launch an investigation by clicking the metric title to drill down to a detail page. You can then investigate which factors are contributing to the activity.

For example, click the title, such as Weak Ciphers Sessions. A detail page appears with all the clients, servers, certificates, and SNIs that were associated with weak cipher sessions, as shown in the following figure.



The following network health indicators can appear on the Network Overview page.

DNS - Address Mapping Record Queries

This network health indicator shows you the number of DNS requests received by DNS servers that included the A record type. An A record maps a domain name to the IP address (IPv4) of the domain host. Click the metric title to see which clients sent the most requests.

Why is this metric a security health indicator?

While DNS address mapping queries are normal, large or sudden increases can be an indicator of potential data exfiltration or a DNS tunnel. A DNS tunnel is a technique that encodes data into DNS queries for data exfiltration or command and control attacks. For example, sensitive data can be encoded into the hostname within the A record. You can view the A record by clicking the records icon next to a client that sent a high number of DNS requests.

DNS - FTP Responses

This network health indicator shows you the number of FTP responses sent by DNS servers. Click the metric title to see which servers sent the highest number of FTP responses.

Why is this metric a security health indicator?

The primary activity for DNS servers should be to resolve hostnames instead of sending files over FTP. Attackers can exploit weaknesses in DNS servers, which often go undetected. If there is an increasing number of FTP data transfer by DNS servers, investigate this suspicious activity.

DNS - Request Timeouts

This network health indicator shows you the number of timeouts that occurred after repeated unanswered DNS query requests were sent from clients. Click the metric title to see which clients were affected and which servers were not responding.

Why is this metric a security health indicator?

DNS can be a bottleneck in your network if hostname resolution cannot take place. A spike, or large increase in request timeouts, is disruptive to your network in general, and can also be an indicator of a distributed denial of service (DDoS).

DNS - Requests with Suspicious Hosts

This network health indicator shows you the number of DNS requests that included a suspicious hostname, according to threat intelligence applied to your Reveal(x) system. Click the metric title to see which hosts are considered suspicious. Click the red camera icon to see threat intelligence details about the hostname.

Why is this metric a security health indicator?

Threat intelligence provides known data about suspicious IP addresses, hostnames, and URIs. You should always investigate indicators of compromise that are identified by threat intelligence. You can view information about the entire DNS transaction by clicking the records icon next to a suspicious host query.

DNS - Text Record Queries

This network health indicator shows you the number of DNS requests received by DNS servers that included the TXT record type. A TXT record associates human-readable text with a host. Click the metric title to see which client sent the most DNS requests with the TXT record type.

Why is this metric a security health indicator?

DNS queries that include TXT records are typically uncommon, and large increases can be an indicator of a potential DNS tunnel. A DNS tunnel is a technique that encodes data into DNS queries for data exfiltration or command and control attacks. For example, malware or sensitive data can be encoded into the TXT record. You can view the TXT record by clicking the records icon next to a client that sent a high number of DNS requests.

HTTP - 404 Not Found Error

This network health indicator shows you the number of HTTP responses that included the 404 (Not Found) status code. Click the metric title to see which URIs were associated with the 404 status code.

Why is this metric a security health indicator?

While a certain number of 404 errors might be considered normal, a large increase in this client-side error could indicate a potential web directory scan. Attackers rely on information about the underlying web server and associated components that are returned in the HTTP 404 status code.

HTTP - 500 Server Errors

This network health indicator shows you the number of HTTP responses sent by servers that contained the 500 (Server Error) status code. Click the metric title to see which URIs were associated with the 500 status code.

Why is this metric a security health indicator?

A large or sudden increase in this server-side error could indicate a potential web directory scan. Web penetration tools deployed by attackers rely on information about the underlying web server and associated components that are returned in the HTTP 500 status code.

HTTP - Requests with Suspicious Hosts

This network health indicator shows you the number of HTTP requests that included a suspicious hostname, according to threat intelligence found in your Reveal(x) system. Click the metric title to see which hosts are considered suspicious. Click the red camera icon to see related threat intelligence details about the host.

Why is this metric a security health indicator?

Threat intelligence provides known data about suspicious IP addresses, hostnames, and URIs. You should always investigate indicators of compromise that are identified by threat intelligence. You can view information about the entire HTTP transaction by clicking the records icon next to a suspicious host.

HTTP - Requests with Suspicious URIs

This network health indicator shows you the number of HTTP requests that included a suspicious URI, according to threat intelligence found in your Reveal(x) system. Click the metric title to see which URIs are considered suspicious. Click the red camera icon to see related threat intelligence details about the URI.

Why is this metric a security health indicator?

Threat intelligence provides known data about suspicious IP addresses, hostnames, and URIs. You should always investigate indicators of compromise that are identified by threat intelligence. You can view information about the entire HTTP transaction by clicking the records icon next to a suspicious URI.

SSL - Expired Certificate Sessions

This network health indicator shows you the number of TLS/SSL sessions that were established with an expired certificate. Click the metric title to see which expired certificates had the most sessions.

Why is this metric a security health indicator?

Certificate authorities add expiration dates to certificates, which are required for establishing a secure TLS or SSL session. Sessions established with expired certificates could indicate that servers have certificate verification disabled, or that users ignored browser warnings when establishing the session. This type of activity increases the vulnerability of devices to man-in-the-middle attacks. Consider configuring your web servers to remove expired certificates.

SSL - Insecure SSLv3 Protocol Sessions

This network health indicator tells you the number of connections on your network that were established with SSL version 3.0. Click the metric title to see a list of servers and clients with SSLv3 sessions.

Why is this metric a security health indicator?

Known vulnerabilities, such as BEAST and POODLE, are associated with SSLv3. If you have a high number of SSLv3 sessions, consider configuring servers to support the latest version of TLS.

SSL - Insecure TLS 1.0 Protocol Sessions

This network health indicator tells you the number of connections on your network that were established with TLS version 1.0. Click the metric title to see a list of servers and clients with TLS 1.0 sessions.

Why is this metric a security health indicator?

Known vulnerabilities, such as BEAST and POODLE, are associated with TLS 1.0. If you have a high number of TLS 1.0 sessions, consider configuring servers to support the latest version of TLS.

SSL - Self-signed Sessions

This network health indicator shows you the number of TLS/SSL sessions that were established with self-signed certificates. Click the metric title to see which clients were associated with self-signed certificate sessions.

Why is this metric a security health indicator?

Self-signed certificates are not issued or verified by a certificate authority. The presence of self-signed certificates might indicate that software on your systems is not validating certificates, making your network vulnerable to man-in-the-middle attacks. A sudden or large increase in sessions with self-signed certificates could also indicate that an attacker is communicating with command and control servers.

SSL - Weak Cipher Sessions

This network health indicator shows you the number of the number of TLS/SSL sessions that were established with weak ciphers. Click the metric title to see which clients are associated with weak ciphers.

Why is this metric a security health indicator?

A cipher suite is a set of encryption algorithms that help secure a TLS/SSL connection. Algorithms within a cipher suite that are associated with known vulnerabilities are considered weak. You can view the cipher suite by clicking the records icon next to a client. Consider configuring your web servers to remove weak ciphers.

TCP - Suspicious TCP Connections

This network health indicator shows you the number of the number of outbound connections to suspicious IP addresses, according to threat intelligence found in your Reveal(x) system. Click the metric title to see which IP addresses are considered suspicious. Click the red camera icon to see related threat intelligence details about the IP address.

Why is this metric a security health indicator?

Threat intelligence provides known data about suspicious IP addresses, hostnames, and URIs. You should always investigate indicators of compromise that are identified by threat intelligence.

Learn more about your network with the Network dashboard.