

What's New

Published: 2024-10-29

While [release notes](#) provide a comprehensive view of our release updates, here is a preview of our most exciting features in ExtraHop 9.7.

AI Search Assistant

[AI Search Assistant](#) now enables you to initiate searches from the Records page by typing a question or request about your stored records. That question, or prompt, is mapped to filter criteria and returns search results. RevealX 360 and RevealX Enterprise administrators must opt-in to this feature, which is disabled by default.

The screenshot displays the AI Search Assistant interface. At the top, there are two tabs: "AI SEARCH ASSISTANT" and "STANDARD SEARCH". Below the tabs is a search input field containing the prompt "Show me suspicious DNS requests." Below the input field, there are three search suggestions:

- Show me all URLs that contain 'login' or 'logon' or 'auth'.
- Show me traffic with Potential SQLi in the last 7 days.
- List the top 25 DNS Requests that resulted in an error in the last 24 hours.

Below the suggestions is a "More Suggestions" link. The main interface shows a "Records" view with a bar chart and a table of results. The bar chart shows the frequency of records over time, with a peak around 08:40. The table below the chart shows the following records:

Time	Record Type	Client	Client IPv4 Address	Client Port	Server	Server IPv4 Address
2021-16-09 13:35:09.028	SSL Close	Remote 194.105.192.99	194.105.192.99	55970	LifeSize 061D90	192.168.222.201
2021-16-09 13:33:59.969	SSL Open	Remote 194.105.192.99	194.105.192.99	55970	LifeSize 061D90	192.168.222.201
2021-06-09 12:50:51.589	DNS Request	DESKTOP-JPKJT6F	10.22.96.5	58035	Dell DF7208	8.8.8.8

File Analysis

You can now [create custom file filters](#) that determine which files are hashed on the system with the SHA-256 hashing algorithm. File hashes that match a threat collection generate a detection, and file hash data can be queried in records. (Requires Collective Threat Analysis and an IDS license.)

Create File Filter

Name

Author

garyp

Protocol

Locality

File Format

Media Type
 File Extension

Media Type

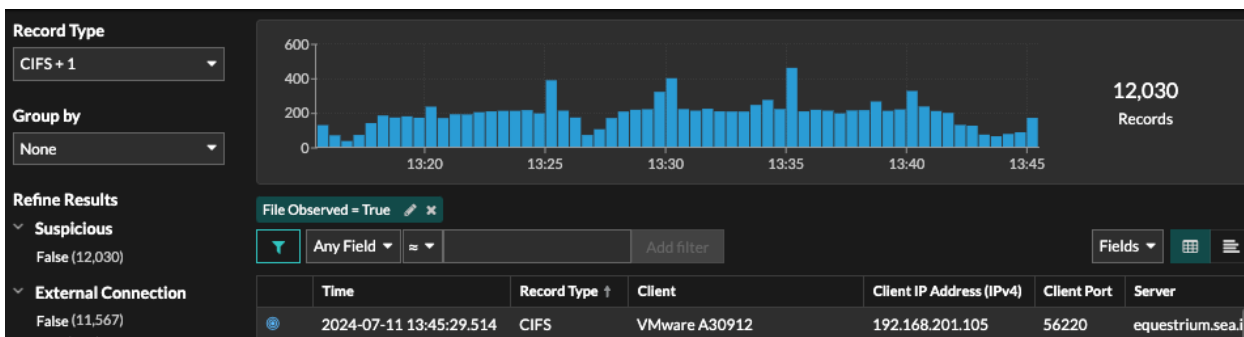
- Archive
- Document
- Executable

File Extraction

You can **extract files from packets** that contain data from HTTP or CIFS traffic. Extracted files are downloaded from the browser to your local machine in a .zip file. File extraction (also known as file carving) is only available to users with access to the NDR and Packet Forensics modules.

The screenshot shows the 'Packet Query' interface. At the top right, it displays '15,571,916 packets (7.89 GB)'. Below this, there are three buttons: 'Download PCAP + Session Keys', 'Download PCAP', and 'Download Session Keys'. At the bottom right, there is an 'Extract Files' button. The interface also shows a time range from 'From Jul 8, 1:57:50 pm' to 'Until Jul 13, 1:57:50 pm'. A 'BPF' dropdown menu is visible on the left, and a 'Truncated to 15,571,916 packets' message is shown in the center.

From the Records page, you can search for HTTP or CIFS record types and filter by "File Observed". Click the packets icon next to the record associated with files you want to extract.



How This Detector Works

For some detection types, a How This Detector Works section is available in [detection details](#) that provides answers to frequently asked questions about why a detection appears in your ExtraHop system.

MITRE Techniques

T1219 Remote Access Software

Risk Factors

Likelihood

Complexity

Business Impact

Remote access software that has been historically associated with attack campaigns should be monitored for new activity. An attacker can leverage legitimate remote access tools to manage command-and-control (C&C) communication.

The system might change the risk score for this detection.

Attack Background

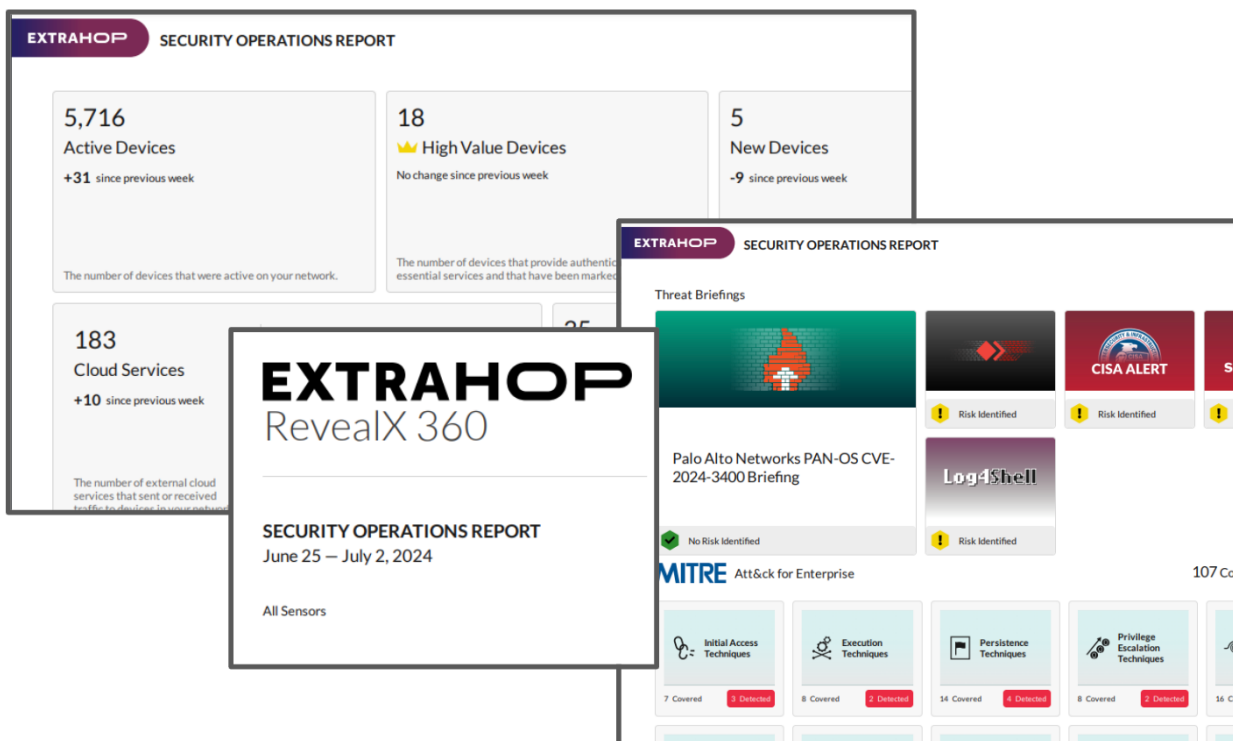
Legitimate desktop support and remote access software such as AnyDesk, TeamViewer, and LogMeIn has been frequently deployed by threat actors during attack campaigns to establish an interactive C&C channel with a compromised device. The attacker installs a legitimate software instance on the compromised device and acquires a passcode for the software. With the passcode, the attacker is able to interact with the compromised device or leverage software features that install other tools to collect data from the victim.

How This Detector Works

- What is detected:** Internal devices that connect to a cloud service associated with remote access software, such as AnyDesk. ExtraHop maintains a list of cloud services and software that are associated with malware or attack campaign targets. Only new connections to these cloud services generate a detection.
- How long does it take to detect:** A detection is generated within one hour after ExtraHop observes the new connection. However, machine learning models must first review device history to determine if the connection is new. New connections are either observed for the first time by ExtraHop, or observed for the first time after a period of inactivity for several weeks. Continuous connections do not generate a detection.
- What is the source of traffic:** The internal client (offender) is the source of cloud service connections. The external endpoint (victim) is the destination of traffic.
- Can I tune this detection:** You can tune this detection based on participants or properties.

Security Operations Report

The Security Operations Report (formerly called the Executive Report) contains an enhanced summary of important system indicators related to your attack surface and threat coverage.



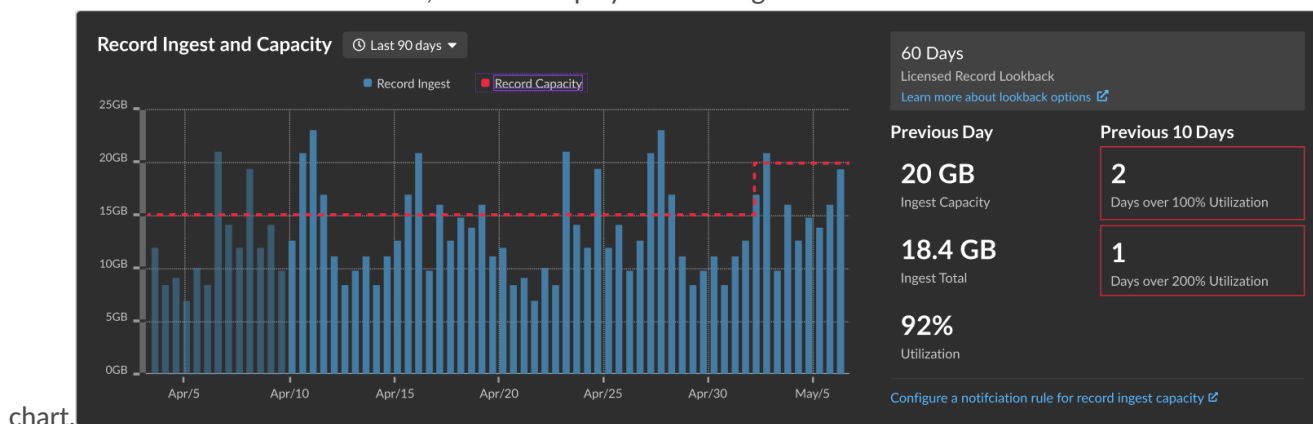
For Administrators

New Maximum Sensor Limit

The ExtraHop system can now support consoles that manage up to 250 sensors.

Record Lookback Options

From the [Record Ingest and Capacity chart](#), ExtraHop administrators for RevealX 360 can select an interval of 30, 90, or 180 days depending on the amount of licensed record lookback, which is displayed to the right of the bar



For API Developers

Trigger API

You can now store metrics and access properties for NTP and TFTP traffic with the new NTPThe Network Time Protocol (NTP) class enables you to store metrics and access properties on NTP_MESSAGE events. and TFTPThe TFTP (Trivial File Transfer Protocol) class enables you to store metrics and access properties on TFTP_REQUEST and TFTP_RESPONSE events. classes.

REST API

You can now **extract files (also known as file carving)** from packets through the `/packets/search` endpoint [↗](#) by specifying the `output` parameter as `extract`.