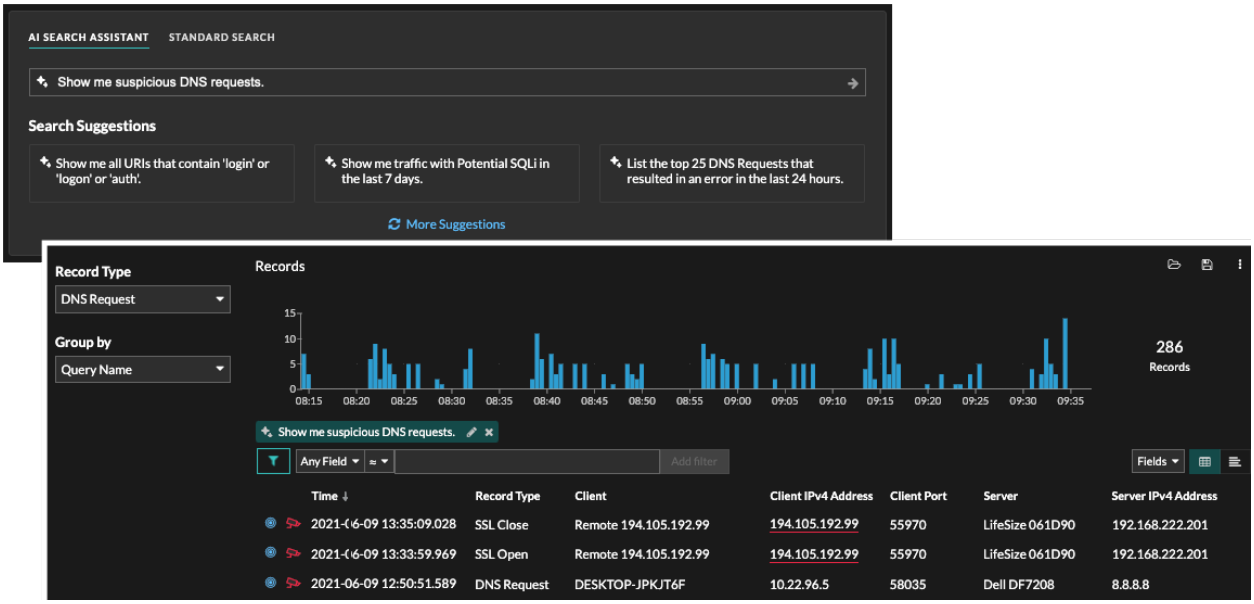
What's New

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.

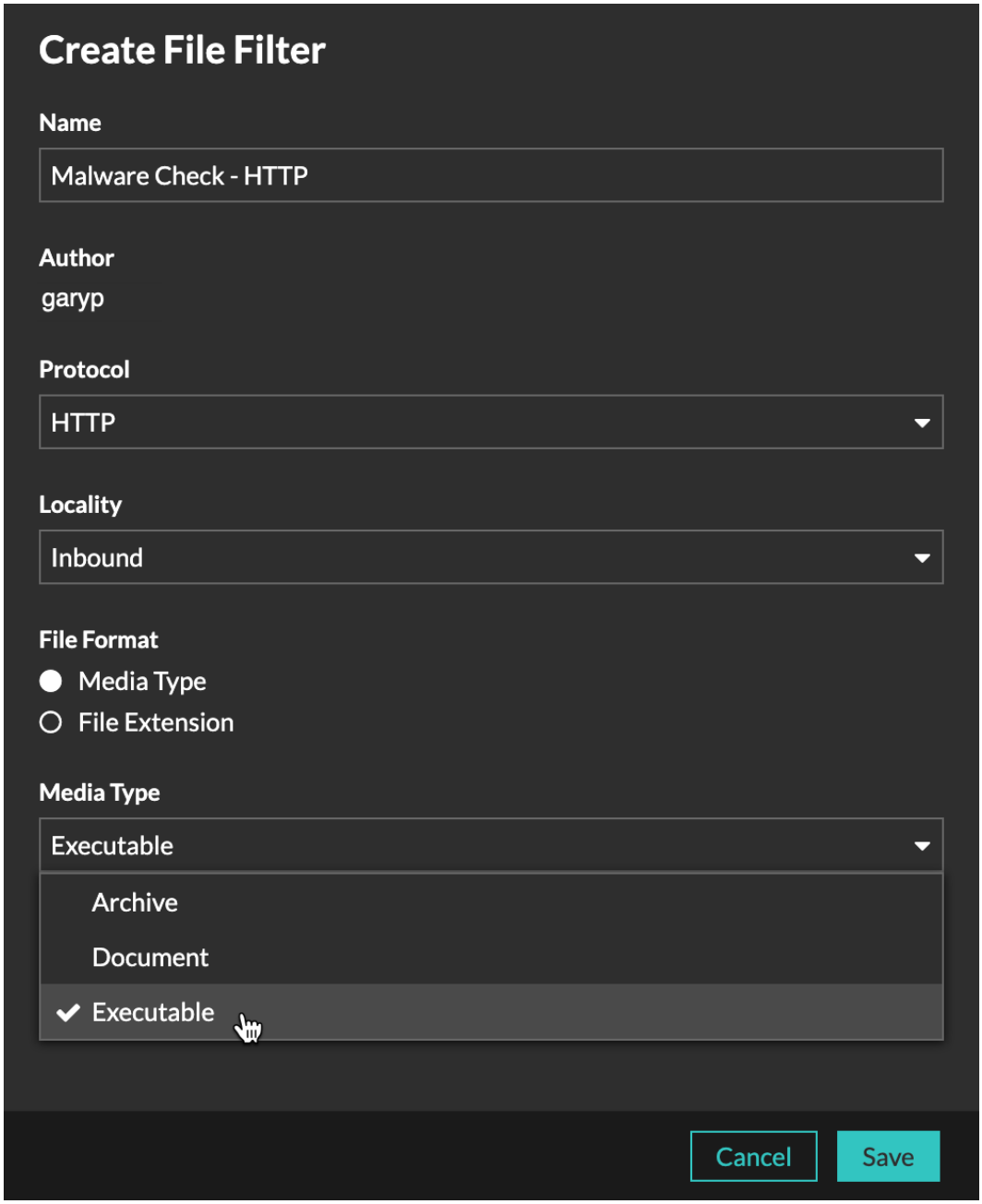
AI Search Assistant

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.



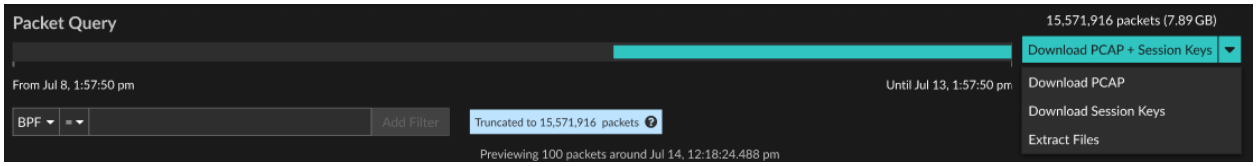
File Analysis

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.)

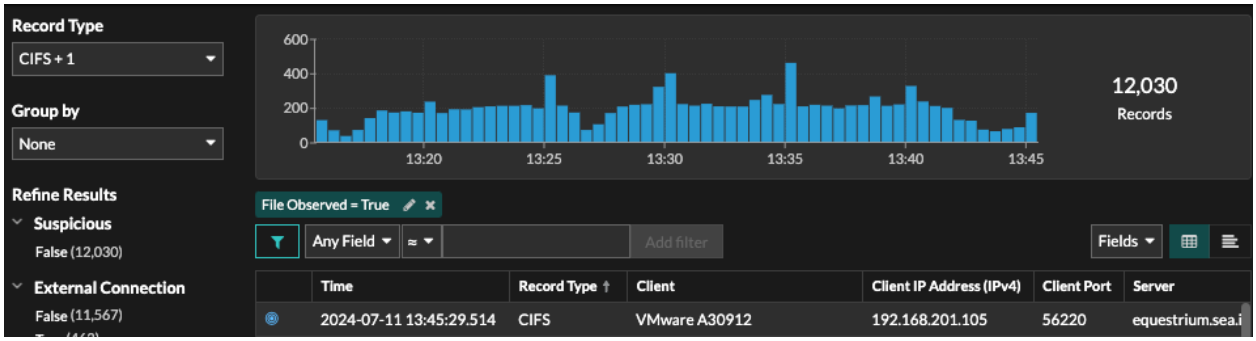


File Extraction

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.

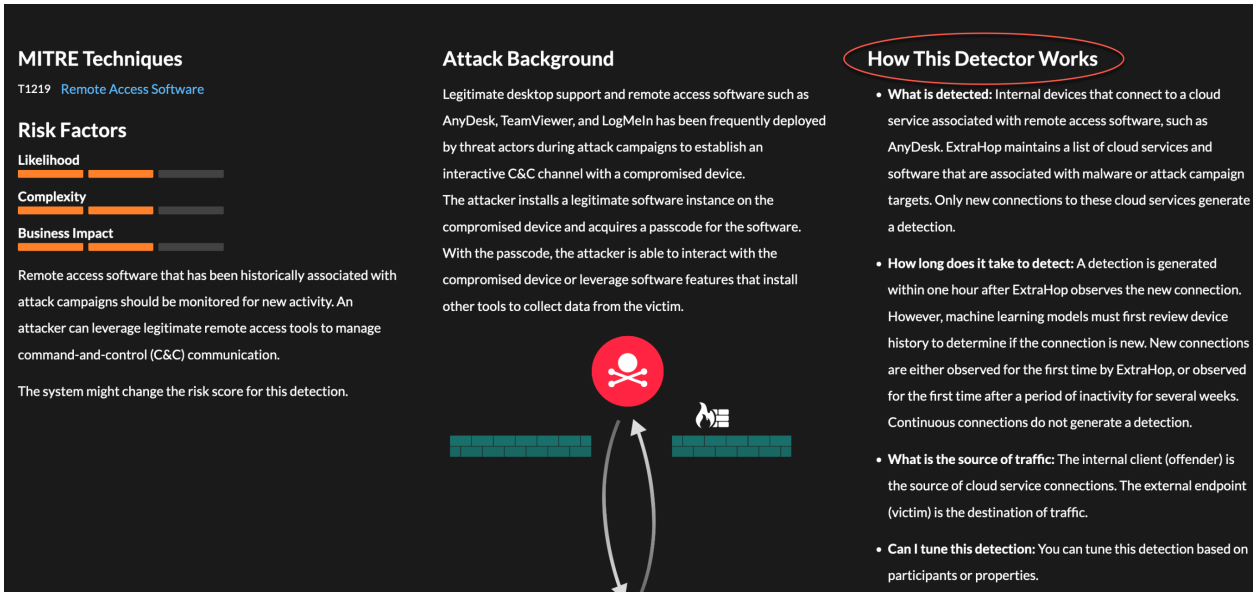


From the Records page, you can search for HTTP or CIFs record types and filter by "File Observed". Click the packets icon next to the record associated with files you want to extract.



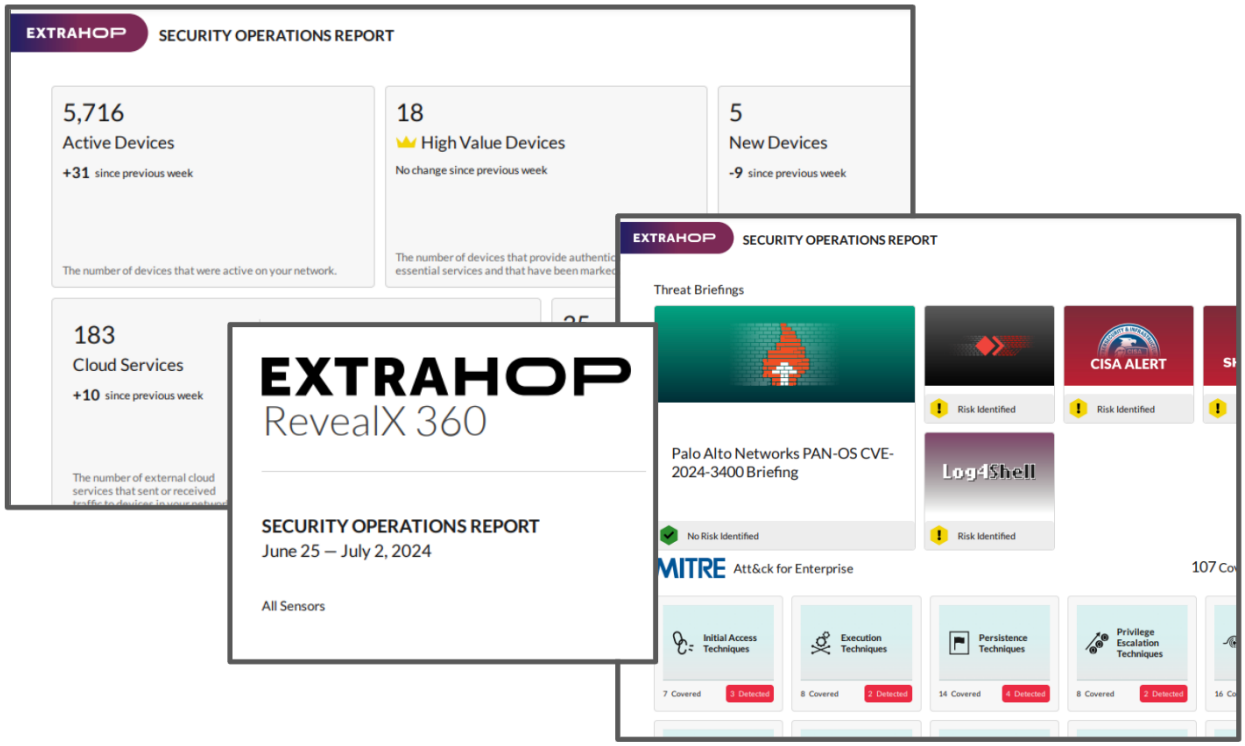
How This Detector Works

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.



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.



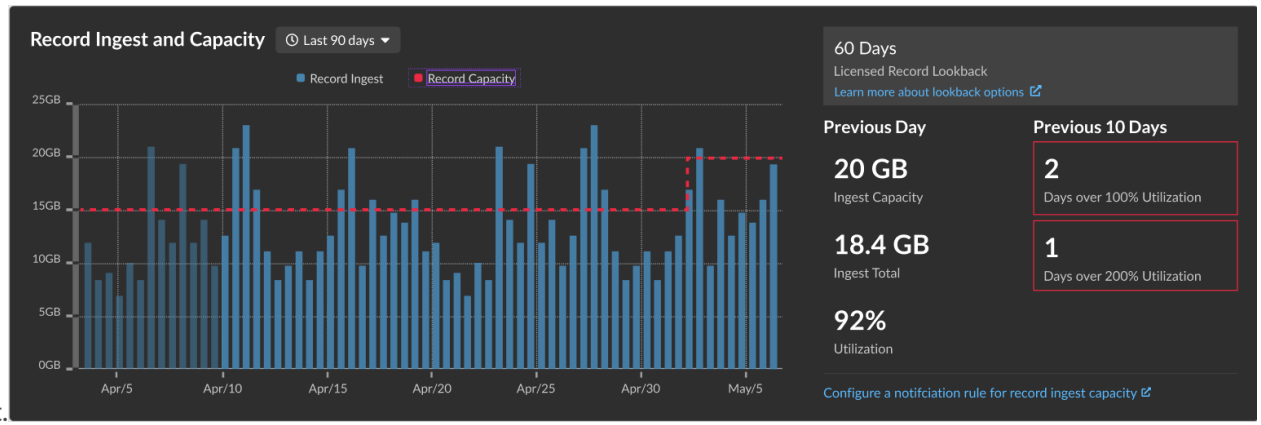
For Administrators

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 chart.



For API Developers

Trigger API

You can now store metrics and access properties for NTP and TFTP traffic with the new `NTP`The `Network Time Protocol (NTP) class enables you to store metrics and access properties on NTP_MESSAGE events.` and `TFTP`The `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`.