

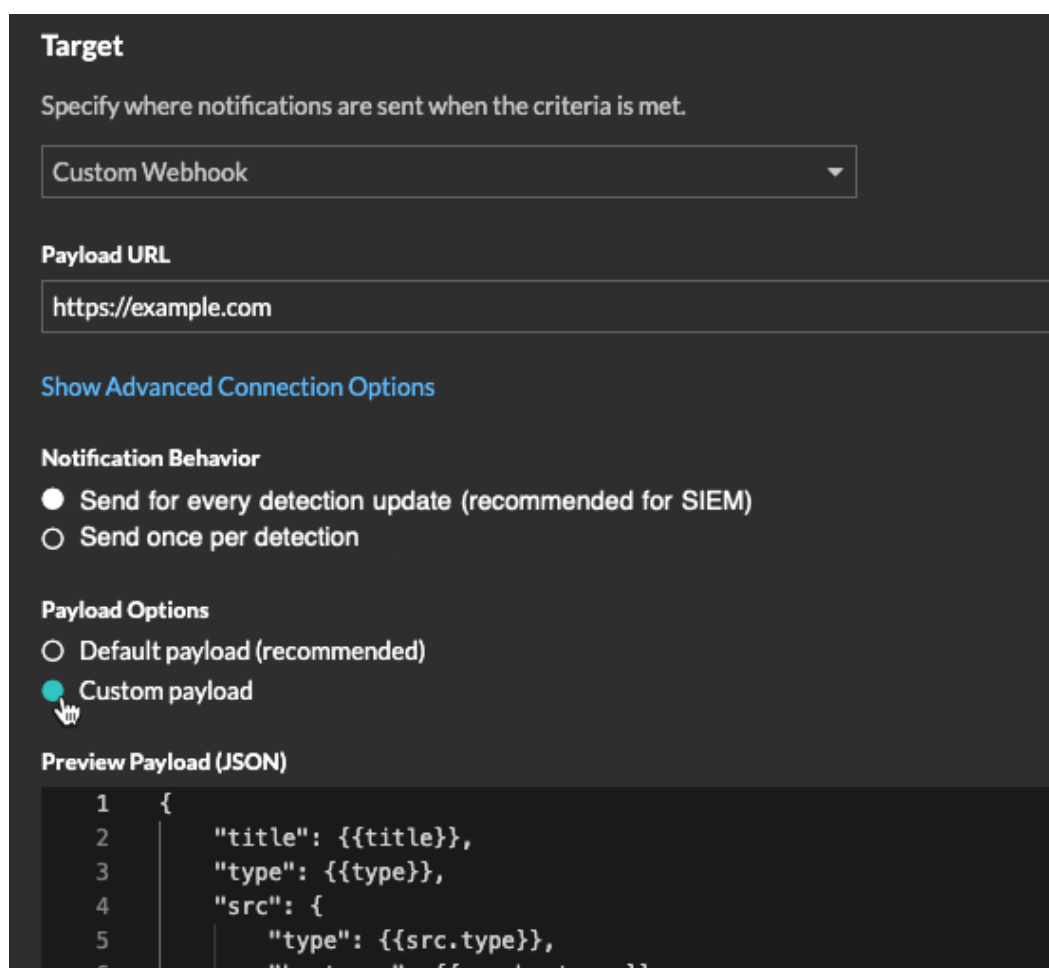
# What's New

Published: 2024-10-18

While [release notes](#) provide a comprehensive view of our release updates, here is a preview of our most exciting features in ExtraHop 9.8.

## Enhanced Detection Notifications

Detections and detection notifications have been optimized for exporting granular detection data. Users can now [configure notification rules](#) to send a default or custom webhook payload for every detection update, or only send one notification for each detection.



The screenshot shows a configuration panel for notification rules. It includes a 'Target' dropdown menu set to 'Custom Webhook', a 'Payload URL' text input field containing 'https://example.com', and a 'Show Advanced Connection Options' link. Under 'Notification Behavior', the 'Send for every detection update (recommended for SIEM)' radio button is selected. Under 'Payload Options', the 'Custom payload' radio button is selected. A 'Preview Payload (JSON)' section shows a code editor with the following JSON structure:

```
1  {
2    "title": {{title}},
3    "type": {{type}},
4    "src": {
5      "type": {{src.type}},
6      "hostname": {{src.hostname}}
```

## Security Operations Report

You can now select the contents to include in a [Security Operations Report](#) that you generate from an Overview page.

## Generate Security Operations Report

### Report Contents

- Attack Surface Visibility
- Threat Coverage
- Attack Detection
- Perimeter
- Security Hardening

### Time Interval

- Last  days
- Previous calendar week
- Previous calendar month

### Sites

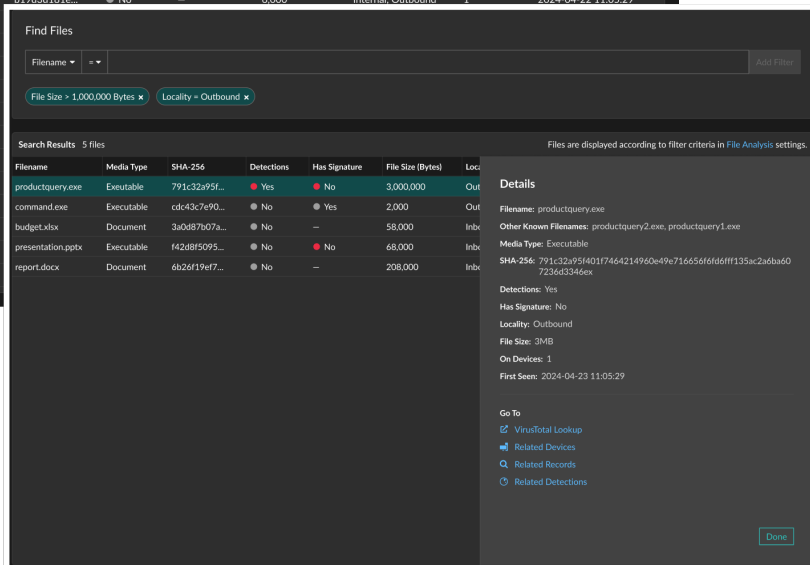
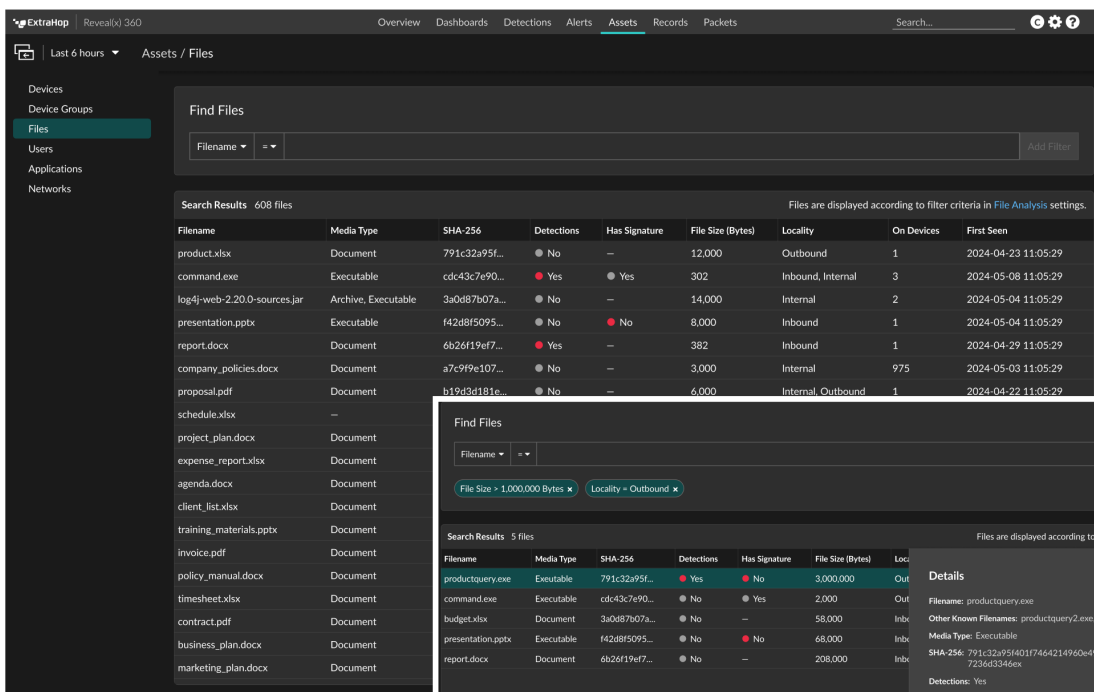
All Sites ▼

### Report Options

- Include explanation text

### New Files page

The [Files page](#) displays a table of files hashed according to filters that are configured and enabled from the File Analysis settings. File details enable you to further investigate the SHA-256 file hash in devices, records, detections, and VirusTotal Lookup, which is a third-party tool.



**New RevealX 360 Integrations**  
**Next Generation SIEM Integrations**

Added integrations for [CrowdStrike Falcon Next-Gen SIEM](#) and [Splunk Enterprise Security SIEM](#) that leverage [notification rules](#) to export ExtraHop detection data to the target SIEM.

EXTRAHOP | RevealX 360

Administration / Integrations

## Integrations

Click any tile to learn more about integrations developed by ExtraHop and by our technology partners.

Configure

Configure

**Integration Status**

Status: ● Integration Enabled  
 Proxy Sensor: ● prod-pdx-eda-6100v

[Send Test Event](#)
[Change Credentials](#)
[Delete Credentials](#)

**Notification Rules**

This integration is configured as the target for the following notification rules.

Name	Event Type	Status	Author	
All System Alerts	Security Detection	<span style="color: green;">●</span> Enabled	maebybluth	<a href="#">Edit</a>
NOC	Performance Detection	<span style="color: gray;">●</span> Disabled	tobias	<a href="#">Edit</a>

[Add Notification Rule](#)

### LevelBlue, Axonius, Cisco XDR Integrations

Added the following new integrations to help you investigate and respond to device and detection data:

- [LevelBlue](#) offers managed detection and response (MDR).
- [Axonius](#) is a cybersecurity asset management tool.
- [Cisco XDR](#) is a cloud-based extended detection and response solution.

EXTRAHOP | RevealX 360

Administration / Integrations

## Integrations

Click any tile to learn more about integrations developed by ExtraHop and by our technology partners.

Configure

Configure

Configure

### For Administrators

#### Packet Access Control

Administrators can now grant [privileges](#) that allow users to only download packet headers. RevealX 360 administrators can also set a [global policy](#) for packet slice size, and [enable sensor access control](#) to grant access to specific user groups.

**Edit Sensor Access Control**

You can enable packet download restrictions by specifying a SAML attribute value that limits packet access to assigned sensors.

**Options**

- Enable packet download restrictions
- Limited access  
On unassigned sensors, users with packet download privileges can download packet headers.
- No access  
On unassigned sensors, users have no packet access regardless of privileges.

**SAML Configuration**

Specify an attribute name  
SAML user group Manager

**Packet and Session Key Access**

- Packets and session keys ?
- Packets only ?
- Packet slices only ?
- Packet headers only ?
- No access

**Packet Slice Download Control**

Users with packet slices only privileges can download the first **64** bytes of a packet.

Save Changes

### File Extraction Password

A password is required to open .zip files extracted, or carved, from packets. Administrators can set the file extraction password from the Administration Settings on [RevealX Enterprise](#) or [RevealX 360](#) and share the password with approved users.

**File Extraction Password**

Specify the password required for users to unzip files extracted and downloaded from a packet query.

\*\*\*\*\*

Show Password Change Password

### Decryption for Multiple Domain Controllers

The ExtraHop system now [supports connecting multiple domain controllers](#) to a sensor to decrypt domain controller traffic. You can configure decryption on an individual sensor on RevealX Enterprise or through an integration on RevealX 360.

The image shows two screenshots from the ExtraHop interface. The left screenshot is the 'Domain Controller' configuration page, which includes a search bar, navigation links, and a status section indicating a successful sync on 2020/09/23 14:00. Below this are input fields for Host, Computer Name, Realm Name, Username, and Password, along with 'Test Connection', 'Remove Connection', and 'Save' buttons. A success message at the bottom states 'The connection to the target was successful.' The right screenshot shows the 'Microsoft Protocol Decryption' integration status page, featuring a status indicator (Up-to-date), host information (10.15.6.19), realm name (TESTLOCAL), sensor name (server.sea.leh.com), and a last successful sync timestamp (2024/07/30 16:30). It also includes a 'Connect to Another Domain Controller' section with an 'Add Credentials' button and a list of integration features such as enhanced detection coverage and visibility into encrypted traffic.

## For API Developers

### Trigger API

You can now store metrics and access properties for SOCKS and NMF traffic with new **SOCKS** and **NMF** classes.

### REST API

Added the `/appliances/sensortags` endpoint to the **RevealX 360 REST API**, which enables you to view and manage sensor tags.