What's New

Published: 2025-01-22

While release notes ↗ provide a comprehensive view of our release updates, here is a preview of our most exciting features in ExtraHop 9.9.

Users in Detections

Usernames are now included in detection participant information when available. You can filter detections ↗ by user, see specific users that are linked to detections in detection summaries ↗ and participant information ↗, and add a participant username as a tuning rule ↗ or detection notification ↗ criteria.
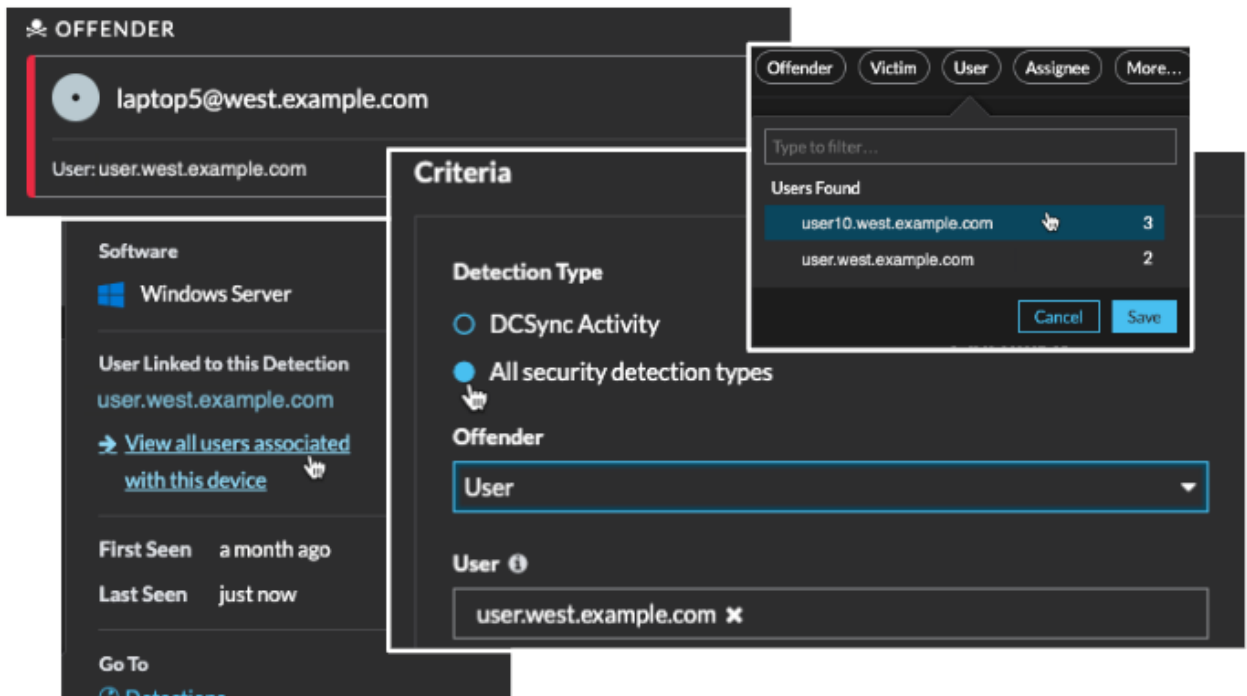

Detection Log

Detection details ↗ now contain a time-stamped log of activity associated with the detection. The detection log lists every update associated with the detection and the tuning rules ↗ associated with specific activity.

| Time	Offender / Client	Victim / Server	Client Port	JNDI String	Server Port	Tuning Rule
2024-12-13 23:55	scanner5.example.com	server.west.example.com	55083	${jndi:ldap://192.168.210.94:13456}	80	–
2024-12-14 00:05	scanner5.example.com	workstation1	57951	${jndi:ldap://192.168.174.126:1345...	5985	–
2024-12-14 00:12	scanner5.example.com	workstation2	58439	${jndi:ldap://192.168.2.143:13456}	5985	–
2024-12-14 00:28	scanner5.example.com	accounting.west.example.com	48447	${jndi:ldap://192.168.116.196:1345...	5000	–
2024-12-14 00:28	scanner5.example.com	ap.west.example.com	41465	${jndi:ldap://192.168.169.3:13456}	80	–
2024-12-14 00:30	scanner5.example.com	international.west.example.com	41979	${jndi:ldap://192.168.47.179:13456}	8000	–
2024-12-14 00:33	scanner5.example.com	custservice.west.example.com	43007	${jndi:ldap://192.168.102.125:1345...	80	–
2024-12-14 01:15	scanner5.example.com	test-serv	45973	${jndi:ldap://192.168.130.179:1345...	80	19
2024-12-14 01:15	scanner5.example.com	test-serv	43531	${jndi:ldap://192.168.84.237:13456}	80	19
2024-12-14 01:35	scanner5.example.com	workstation3	53407	${jndi:ldap://192.168.127.79:13456}	80	–

Bulk Actions

You can now add all the detections in a detection summary ☑ to an investigation. From the new Bulk Actions drop-down menu, you can track all detections ☑ in the summary or add all detections to an investigation ☑.
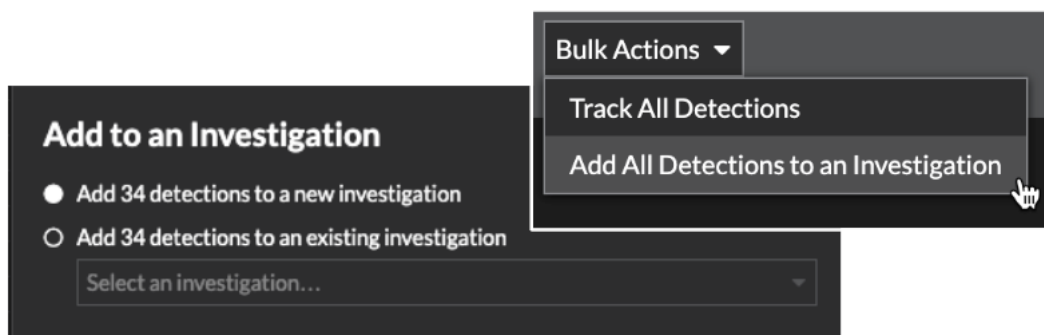
Cloud-updated Device Properties

(RevealX 360 only) Added support to display cloud-updated device properties ☑ obtained from integrations ☑ configured on your ExtraHop system, such as CrowdStrike. You can filter by cloud device properties to find a device ☑ and to create a dynamic device group ☑.
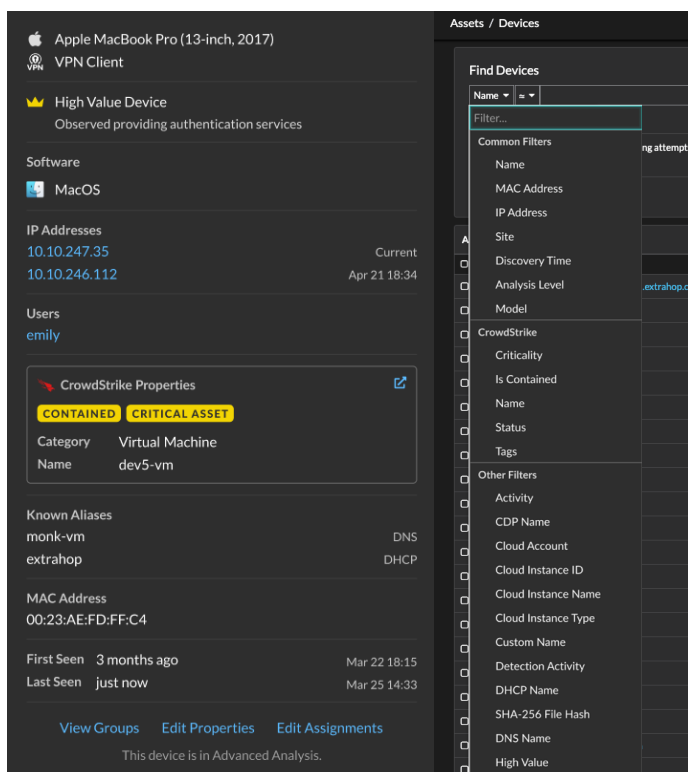
For Administrators

File Hash Lookup Links

Added the ability to configure external lookup tool links to easily look up SHA-256 file hashes for RevealX 360 ☑ and RevealX Enterprise ☑. VirusTotal Lookup is configured by default. Configured links are displayed on Devices, Files, Records, and Detections pages.

Inactive Device Deletion

You can specify when and how the system automatically deletes inactive devices from the ExtraHop system ☑. You can delete devices that have been inactive for a specified number of days and you can delete inactive devices after the sensor has discovered over a specified number of devices.

Inactive Sources

Search Results

Devices and applications appear in search results until they are inactive for over 90 days. The option below enables you to specify the number of days that sources are inactive and immediately remove them from search results.

Remove sources that have been inactive for [5] days.

[Remove Now]

ExtraHop System

Devices that become inactive remain in the ExtraHop system. The following options enable you to specify when and how the system deletes inactive devices. Devices deleted from the sensor are also deleted from the connected console.

☑ Delete devices that have been inactive for [90] days.

☑ Delete inactive devices after the sensor has discovered over [1,000,000] devices.

[Save]

Login Screen Message

(RevealX Enterprise only) You can add a custom message to the login screen ⧉ of your ExtraHop system to display graphics and logos and to convey information to users such as password requirements, policy statements, support links, or maintenance announcements. The login screen message supports text and graphics in Markdown syntax ⧉.

Login Screen Message

Specify a custom message to be displayed on the ExtraHop user login screen.

Login Message Settings

○ Do not display a login message
● Display a custom login message

Custom Login Message (supports Markdown format)

Editor	Preview
## Scheduled Maintenance System maintenance is scheduled from June 1, 2020 to June 3, 2020. During this time, you might experience intermittent issues. Normal operations will be restored by June 4, 2020.	**Scheduled Maintenance** System maintenance is scheduled from June 1, 2020 to June 3, 2020. During this time, you might experience intermittent issues. Normal operations will be restored by June 4, 2020.

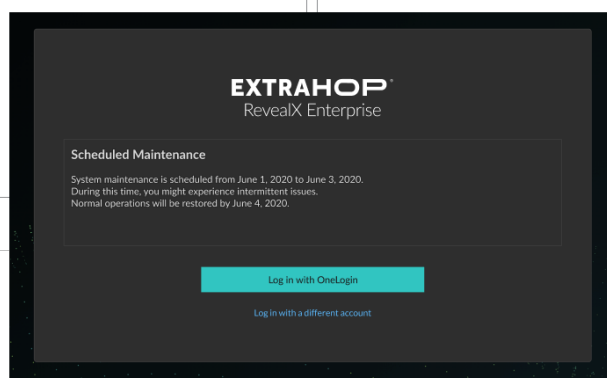[Save Changes]

EXTRAHOP®
RevealX Enterprise

Scheduled Maintenance

System maintenance is scheduled from June 1, 2020 to June 3, 2020.
During this time, you might experience intermittent issues.
Normal operations will be restored by June 4, 2020.

[Log in with OneLogin]

Log in with a different account

For API Developers

REST API

Added the `/users/{username}/lock` endpoint to the User resource ⧉, which enables you to unlock user accounts. This endpoint is accessible only if you have configured the system to automatically lock user accounts after a specified number of failed login attempts through the running configuration file.