

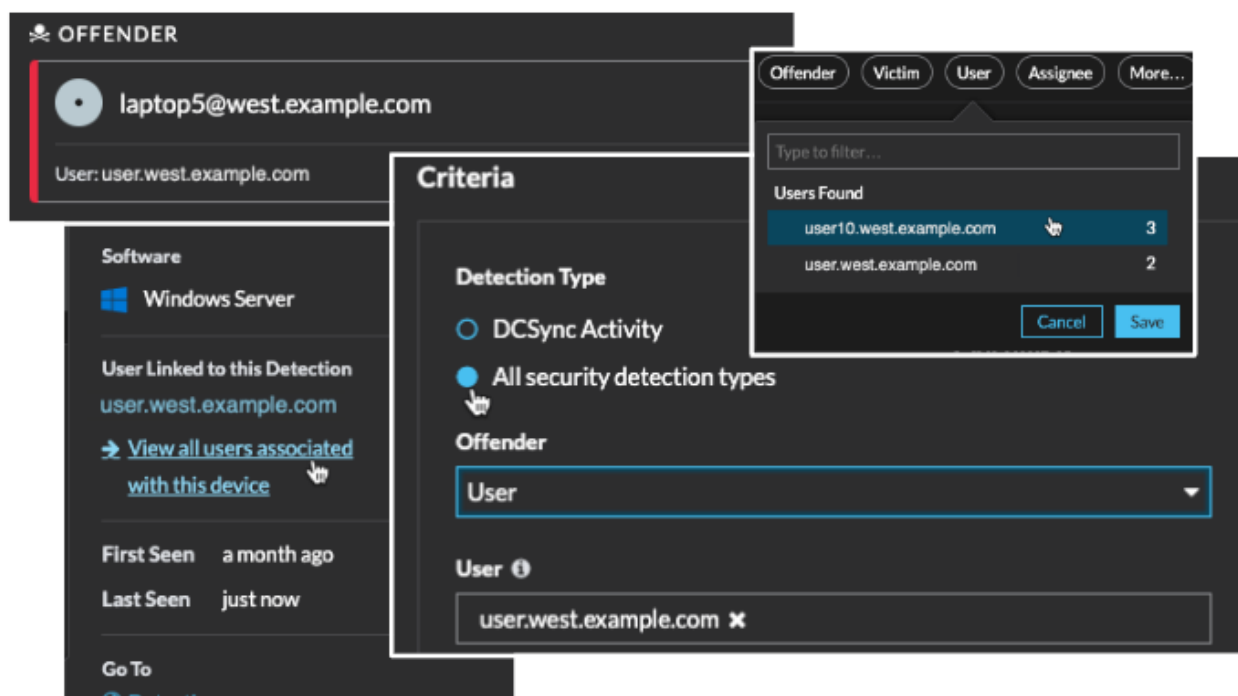
Was ist neu

Veröffentlicht: 2025-02-12

Während [Versionshinweise](#) geben Sie einen umfassenden Überblick über unsere Release-Updates. Hier finden Sie eine Vorschau auf unsere aufregendsten Funktionen in ExtraHop 9.9.

Benutzer bei Erkennungen

Benutzernamen sind jetzt in den Informationen zu den Erkennungsteilnehmern enthalten, sofern verfügbar. Du kannst [Erkennungen filtern](#) nach Benutzern, sehen Sie sich bestimmte Benutzer an, die mit Erkennungen verknüpft sind [Zusammenfassungen der Erkennung](#) und [Informationen zum Teilnehmer](#), und füge einen Teilnehmer-Benutzernamen als [Tuning-Regel](#) oder [Erkennungsbenachrichtigung](#) Kriterien.



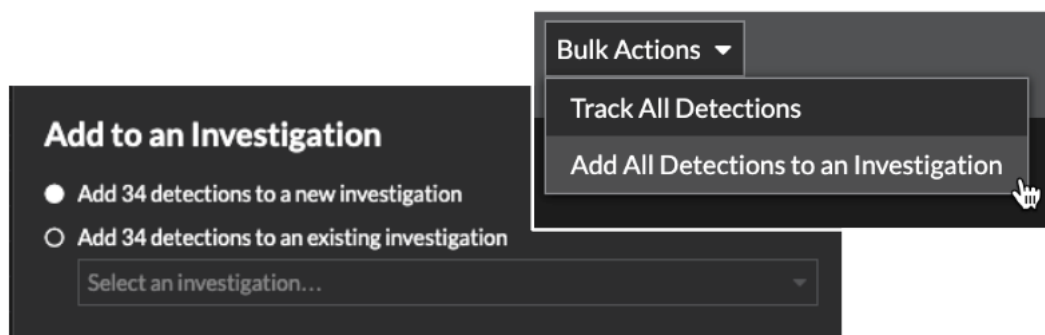
Erkennungsprotokoll

[Einzelheiten zur Erkennung](#) enthält jetzt ein mit Zeitstempel versehenes Protokoll der mit der Erkennung verbundenen Aktivitäten. Das Erkennungsprotokoll listet alle Updates auf, die mit der Erkennung verknüpft sind, und die [Tuning-Regeln](#) mit einer bestimmten Aktivität verbunden.

Log						
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	\$[ndi:ldap://192.168.210.94:13456]	80	—
2024-12-14 00:05	scanner5.example.com	workstation1	57951	\$[ndi:ldap://192.168.174.126:1345...	5985	—
2024-12-14 00:12	scanner5.example.com	workstation2	58439	\$[ndi:ldap://192.168.2.143:13456]	5985	—
2024-12-14 00:28	scanner5.example.com	accounting.west.example.com	48447	\$[ndi:ldap://192.168.116.196:1345...	5000	—
2024-12-14 00:28	scanner5.example.com	ap.west.example.com	41465	\$[ndi:ldap://192.168.169.3:13456]	80	—
2024-12-14 00:30	scanner5.example.com	international.west.example.com	41979	\$[ndi:ldap://192.168.47.179:13456]	8000	—
2024-12-14 00:33	scanner5.example.com	custservice.west.example.com	43007	\$[ndi:ldap://192.168.102.125:1345...	80	—
2024-12-14 01:15	scanner5.example.com	test-serv	45973	\$[ndi:ldap://192.168.130.179:1345...	80	19
2024-12-14 01:15	scanner5.example.com	test-serv	43531	\$[ndi:ldap://192.168.84.237:13456]	80	19
2024-12-14 01:35	scanner5.example.com	workstation3	53407	\$[ndi:ldap://192.168.127.79:13456]	80	—

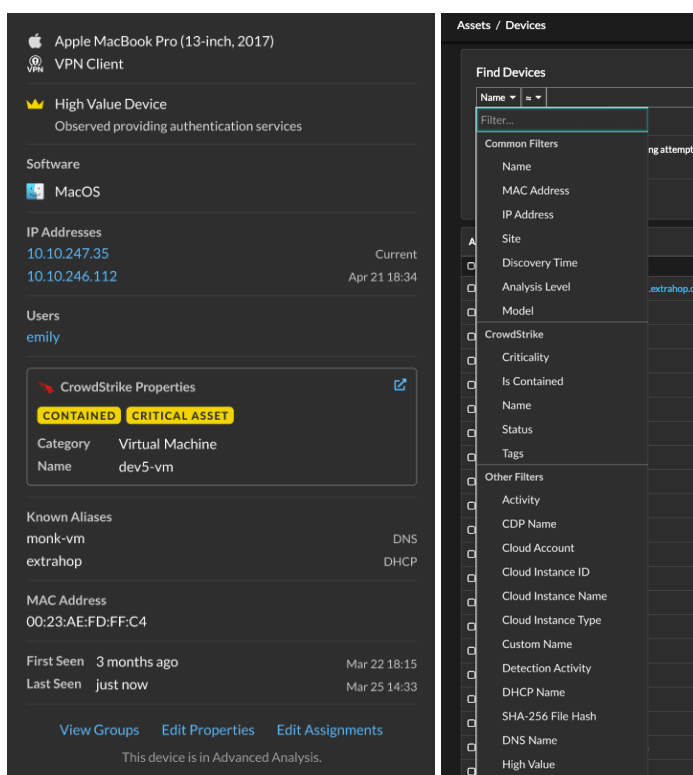
Massenaktionen

Sie können jetzt alle Erkennungen in einem hinzufügen [Zusammenfassung der Erkennung](#) zu einer Untersuchung. Im neuen Dropdownmenü „Massenaktionen“ können Sie [alle Funde verfolgen](#) in der Zusammenfassung oder füge alle Funde zu einem [Untersuchung](#).



Cloud-aktualisierte Geräteeigenschaften

(Nur RevealX 360) Unterstützung für die Anzeige von Cloud-Updates hinzugefügt [Eigenschaften Gerät](#) erhalten von [Integrationen](#) konfiguriert auf Ihrem ExtraHop-System, wie CrowdStrike. Sie können nach Cloud-Geräteeigenschaften filtern, um [finde ein Gerät](#) und zu [eine dynamische Gerätegruppe erstellen](#).



Für Administratoren

Datei-Hash-Suchlinks

Es wurde die Möglichkeit hinzugefügt, Links für externe Suchtools zu konfigurieren, um auf einfache Weise nach SHA-256-Datei-Hashes für zu suchen [RevealX 360](#) und [RevealX Enterprise](#). VirusTotal Lookup ist standardmäßig konfiguriert. Konfigurierte Links werden auf den Seiten „Geräte“, „Dateien“, „Aufzeichnungen“ und „Erkennungen“ angezeigt.

Lookup

IP ADDRESS FILE HASH

Display links to an external lookup tool for SHA-256 file hashes in the ExtraHop system by typing the URL of the tool. The URL must include the \$filehash variable, which is replaced with the SHA-256 hash of the file.

URL Template

Display Name

Display Options

☒ Show this link on all files

☐ Do not show this link

URL Template

Display Name

Display Options

☒ Show this link on all files

☐ Do not show this link

[Add Lookup Link](#)

Details

Filename: fd0b3f36-5596-4351-a52a-324d9881c330

Media Type: Executable

SHA-256: dd4ba3bf201df467ebc05868b8932d56a9d60c8bd81b8b7cf6d3d8da0c762b29

Detections: No

Is Signed: —

Locality: Inbound

File Size (Bytes): 178,830

On Devices: 4

First Seen: 2025-01-09 10:09:00

Go To

- [VirusTotal Lookup](#)
- [Kaspersky](#)
- [Related Devices](#)
- [Related Records](#)

Löschen inaktiver Geräte

Sie können angeben, wann und wie das System automatisch **löscht inaktive Geräte aus dem ExtraHop-System**. Sie können Geräte löschen, die für eine bestimmte Anzahl von Tagen inaktiv waren, und Sie können inaktive Geräte löschen, nachdem der Sensor eine bestimmte Anzahl von Geräten erkannt hat.

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 days.

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 days.

☒ Delete inactive devices after the sensor has discovered over devices.

Meldung auf dem Anmeldebildschirm

(Nur RevealX Enterprise) Sie können **füge dem Anmeldebildschirm eine benutzerdefinierte Nachricht hinzu** [↗](#) Ihres ExtraHop-Systems, um Grafiken und Logos anzuzeigen und Benutzern Informationen wie Passwortanforderungen, Richtlinienenerklärungen, Support-Links oder Wartungsankündigungen zu übermitteln. Die Meldung auf dem Anmeldebildschirm unterstützt Text und Grafiken 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

```
## 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.
```

Preview

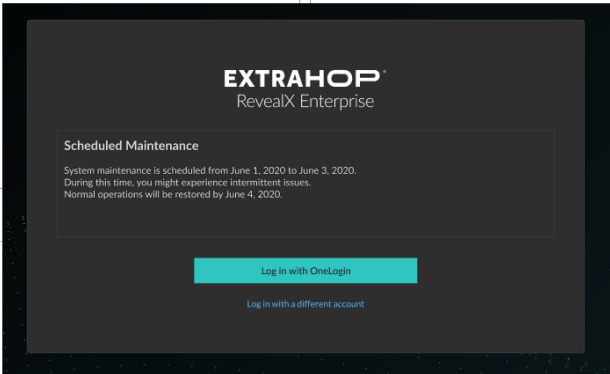
Scheduled Maintenance

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.

[Save Changes](#)



The screenshot shows the ExtraHop RevealX Enterprise login interface. At the top, the ExtraHop logo and 'RevealX Enterprise' are displayed. Below this, a 'Scheduled Maintenance' message is shown in a light gray box, matching the preview above. The message states: '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.' At the bottom of the login screen, there are two buttons: 'Log in with OneLogin' (highlighted in teal) and 'Log in with a different account'.

Für API-Entwickler

REST-API

Das wurde hinzugefügt `/users/{username}/lock` Endpunkt zum **Benutzerressource** [↗](#), wodurch Sie Benutzerkonten entsperren können. Auf diesen Endpunkt kann nur zugegriffen werden, wenn Sie das System so konfiguriert haben, dass Benutzerkonten nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche über die laufende Konfigurationsdatei automatisch gesperrt werden.