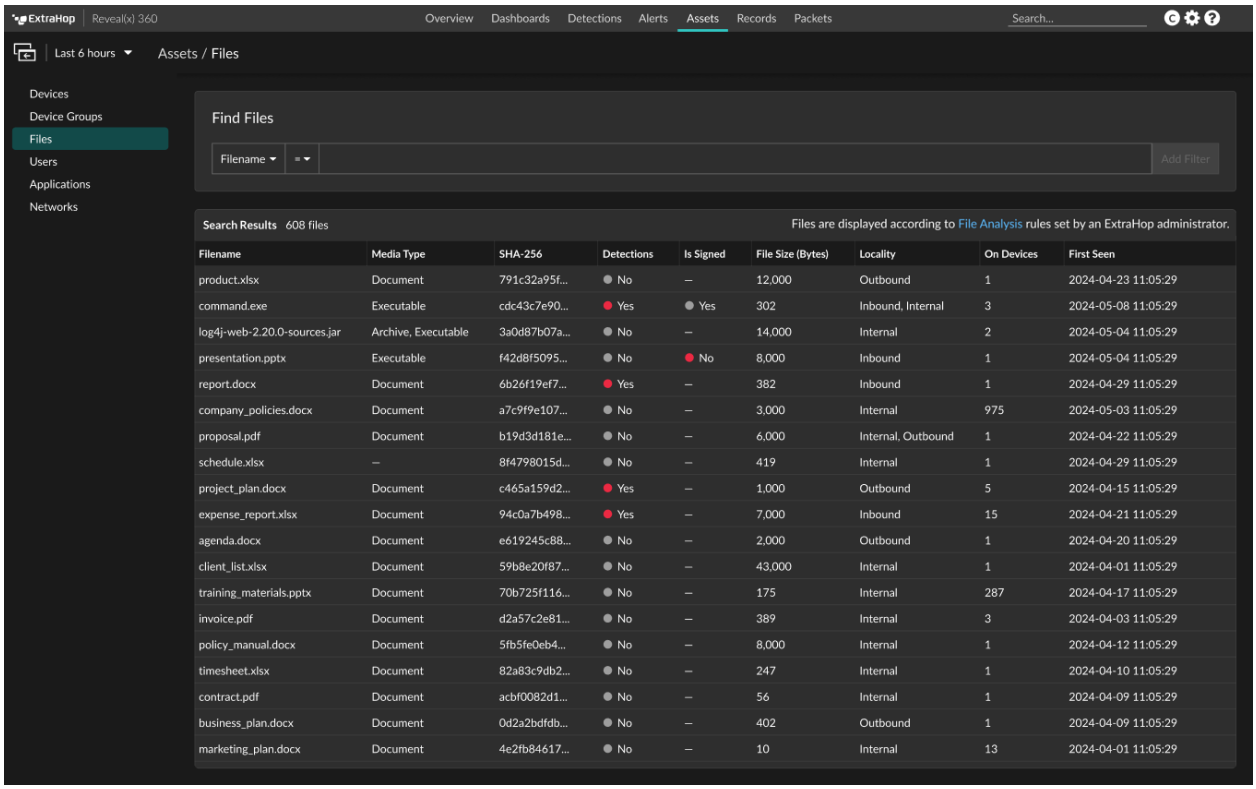
Dateien

Veröffentlicht: 2025-02-04

Metadaten aus Hash-Dateien sind ein wertvolles Tool zur Identifizierung von Malware und Risiken in Ihrem Netzwerk. Beispielsweise sind Dateien, die von mehreren Geräten heruntergeladen wurden, Dateien mit einer Erweiterung, die nicht dem Medientyp entspricht, unsignierte Dateien oder große ausgehende oder eingehende Dateiübertragungen Beobachtungen, die es wert sind, untersucht zu werden. Auf der Seite „Dateien“ wird eine Tabelle mit Hash-Dateien und zugehörigen Dateidetails angezeigt, die Sie filtern und durchsuchen können. Um die Seite „Dateien“ anzuzeigen, klicken Sie auf **Vermögenswerte** aus dem oberen Navigationsmenü und klicken Sie dann auf **Dateien** Diagramm.

Dateien werden mit dem SHA-256-Hashing-Algorithmus gehasht und in der Dateitabelle gemäß den Regeln angezeigt, die in der Einstellungen für die Dateianalyse. Sie können die Ergebnisse in der Tabelle Dateien verfeinern, indem Sie Suchfilterkriterien in der Dateien finden Abschnitt oder indem Sie in der Tabelle auf einen Popup-Operator klicken, um einen Filter hinzuzufügen.

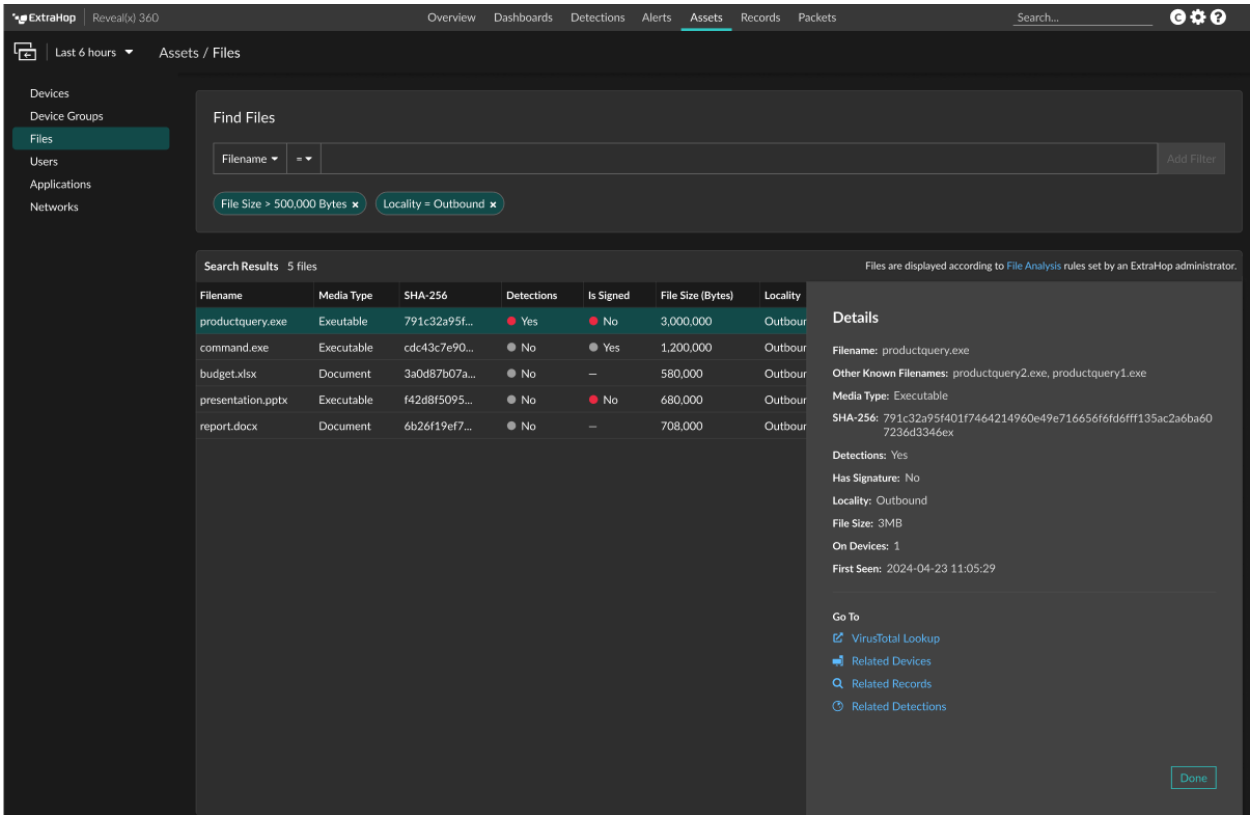


In der Tabelle Dateien werden die folgenden Details für jede Datei angezeigt.

Detail der Datei	Beschreibung
Dateiname	Der Name der Hash-Datei. Andere Dateinamen, die von demselben SHA-256-Hashing-Algorithmus zurückgegeben werden, werden im Detailbereich angezeigt.
Art des Mediums	Der Medientyp der Hash-Datei. Unterstützte Dateitypen sind Dokument, Archiv und Ausführbar. Das ExtraHop-System bestimmt den Datei-Medientyp, indem es Muster im Header und in den Anfangsbytes der Dateinutzlast analysiert.

Detail der Datei	Beschreibung
SHA-256	Der SHA-256-Datei-Hashing-Algorithmus wurde auf die Datei angewendet. Tipp: Du kannst findet Geräte, die bestimmten Hash-Dateien zugeordnet sind indem Sie den SHA-256-Filter zu einer Gerätesuche hinzufügen.
Erkennungen	Gibt an, ob die Hash-Datei an einer Erkennung beteiligt war, die einem Indikator in einer Bedrohungssammlung entsprach, z. B. einer Übertragung bösartige Datei. (Nur auf einer Konsole verfügbar, die an einen Sensor des Intrusion Detection System (IDS) angeschlossen ist, für Benutzer mit NDR-Modulzugriff)
Ist signiert	Gibt an, ob eine Signatur in der Hash-Datei beobachtet wurde, überprüft aber nicht, ob die Signatur gültig ist.
Größe der Datei	Die Größe der Hash-Datei in Byte.
Lokalität	Die Lokalität oder Flussrichtung der Hash-Datei. Unterstützte Orte sind Inbound, Outbound und Internal.
Auf Geräten	Die Anzahl der Geräte, auf denen die Hash-Datei beobachtet wurde.
Zuerst gesehen	Der Zeitstempel, zu dem die Hash-Datei zum ersten Mal beobachtet wurde.

Klicken Sie auf eine Datei in der Tabelle, um den Detailbereich zu öffnen und mehrere Links anzuzeigen, mit denen Sie den SHA-256-Datei-Hash untersuchen können.



- Klicken Sie **VirusTotal-Suche** um zur VirusTotal-Site zu navigieren und den Datei-Hash auf bösartige Inhalte zu überprüfen.
- Klicken Sie **Verwandte Geräte** um Geräte nach dem Datei-Hash zu filtern und Ergebnisse auf der Geräte Seite.
- Klicken Sie **Verwandte Datensätze** um Datensätze nach dem Datei-Hash zu filtern und Ergebnisse auf der Aufzeichnungen Seite.
- Klicken Sie **Verwandte Erkennungen** um Erkennungen nach dem Datei-Hash zu filtern und die Ergebnisse auf der Erkennungen Seite. (Nur auf einer Konsole verfügbar, die an einen IDS-Sensor (Intrusion Detection System) angeschlossen ist, für Benutzer mit Zugriff auf das NDR-Modul.)