May 2023

NETSKOPE ADVANCED UEBA CASE STUDIES

INTRODUCTION

This report contains real-world customer-validated case studies of insider threats, compromised devices, and compromised accounts detected by Netskope Advanced UEBA. Advanced UEBA automatically learns normal user behavior and scores users according to their risk, based on more than 50 machine learning models combined with advanced heuristics tuned specifically to identify insider threats, compromised devices, and compromised accounts. Advanced UEBA monitors all activities on the Netskope Intelligent Security Service Edge (SSE) platform, including Next Gen SWG, API CASB, Netskope Private Access, and Cloud Firewall. Advanced UEBA complements other security controls, including data loss prevention (DLP) policies and threat protection policies, to identify hidden threats that, while rare, can have significant impact if left undetected.

netskope
+
Threat Labs

User Confidence Index

Advanced UEBA detects three different types of hidden threats:

- Insider Threats
- Compromised Devices
- Compromised Credentials

Each user is assigned a User Confidence Index (UCI) score that tracks the risk a user poses to the organization based upon the alerts they have generated. The individual alerts are specific and actionable, based on a combination of machine learning and heuristics. Each alert results in a penalty to the user's UCI score, which will fall into the following three ranges:

Good:	651 - 1000
Moderate:	351 - 650
Poor:	0 - 350

Users with a **moderate** UCI score are likely, and users with poor severity UCI scores users are *highly* likely, to have suffered a compromise or represent an insider threat. Each case study will indicate the Netskope products contributing to the detection of the threat and highlight the specific alerts involved and the impact they had on the UCI score.

About this Report

Netskope provides threat and data protection to millions of users worldwide. Information presented in this report is based on anonymized usage data collected by the Netskope Security Cloud platform relating to a subset of Netskope customers with prior authorization. This report contains information about detections raised by Netskope's Advanced UEBA product. Information in this report is based on the period starting January 1, 2023 through April 30, 2023.

Case Study 1: Insider Threat - Data Exfiltration

Threat Summary

A user uploaded a large quantity of sensitive corporate data to their personal Google Drive.

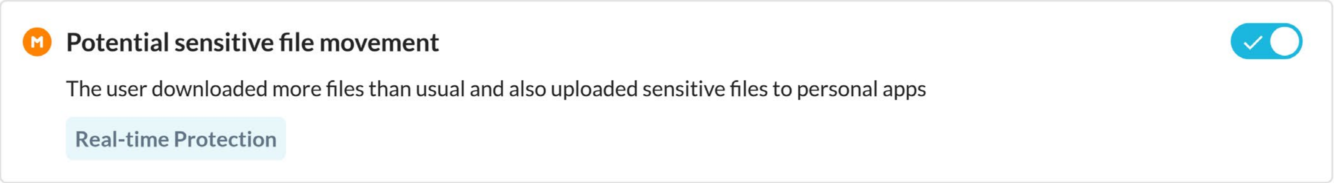
Required Features

Cloud Inline/NG SWG + DLP + Advanced UEBA

Summary

From a managed device, a user downloaded more than 2,180 files from a corporate managed OneDrive instance and then uploaded more than 465 files to their personal Google Drive. There were 37 files uploaded that matched DLP policies designed to detect sensitive information. The download and upload activities triggered alerts related to risky data movement. The activity reduced the user's UCI from 998 (good) to 562 (moderate).

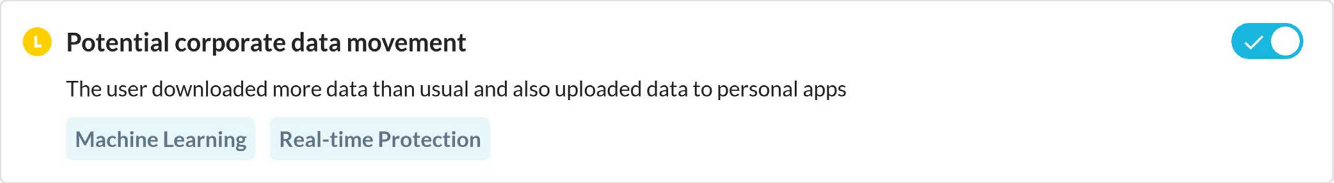
Detections Involved



M **Potential sensitive file movement** ✓

The user downloaded more files than usual and also uploaded sensitive files to personal apps

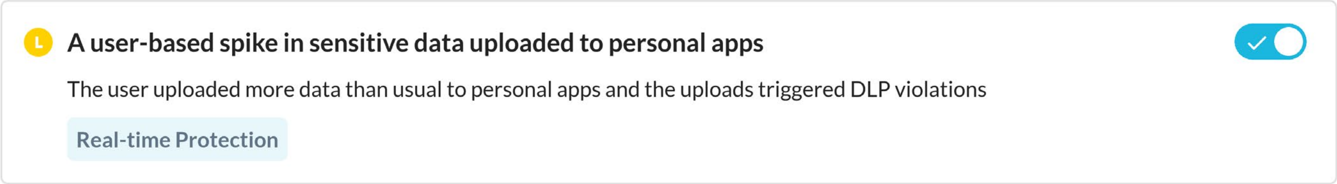
Real-time Protection



L **Potential corporate data movement** ✓

The user downloaded more data than usual and also uploaded data to personal apps

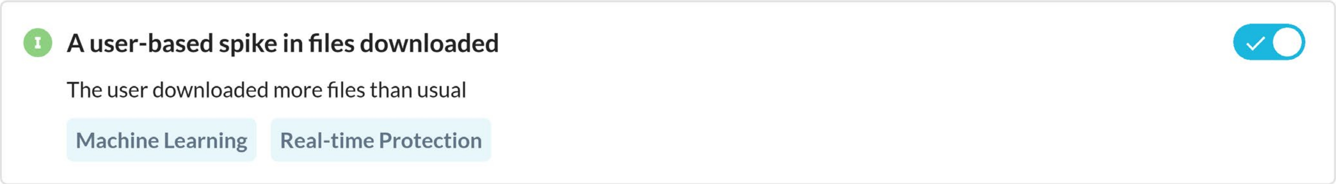
Machine Learning | Real-time Protection



L **A user-based spike in sensitive data uploaded to personal apps** ✓

The user uploaded more data than usual to personal apps and the uploads triggered DLP violations

Real-time Protection



I **A user-based spike in files downloaded** ✓

The user downloaded more files than usual

Machine Learning | Real-time Protection

Case Study 2: Insider Threat - Data Exfiltration

Threat Summary

A user uploaded a large quantity of sensitive corporate data to their personal Google Drive before they left the organization.

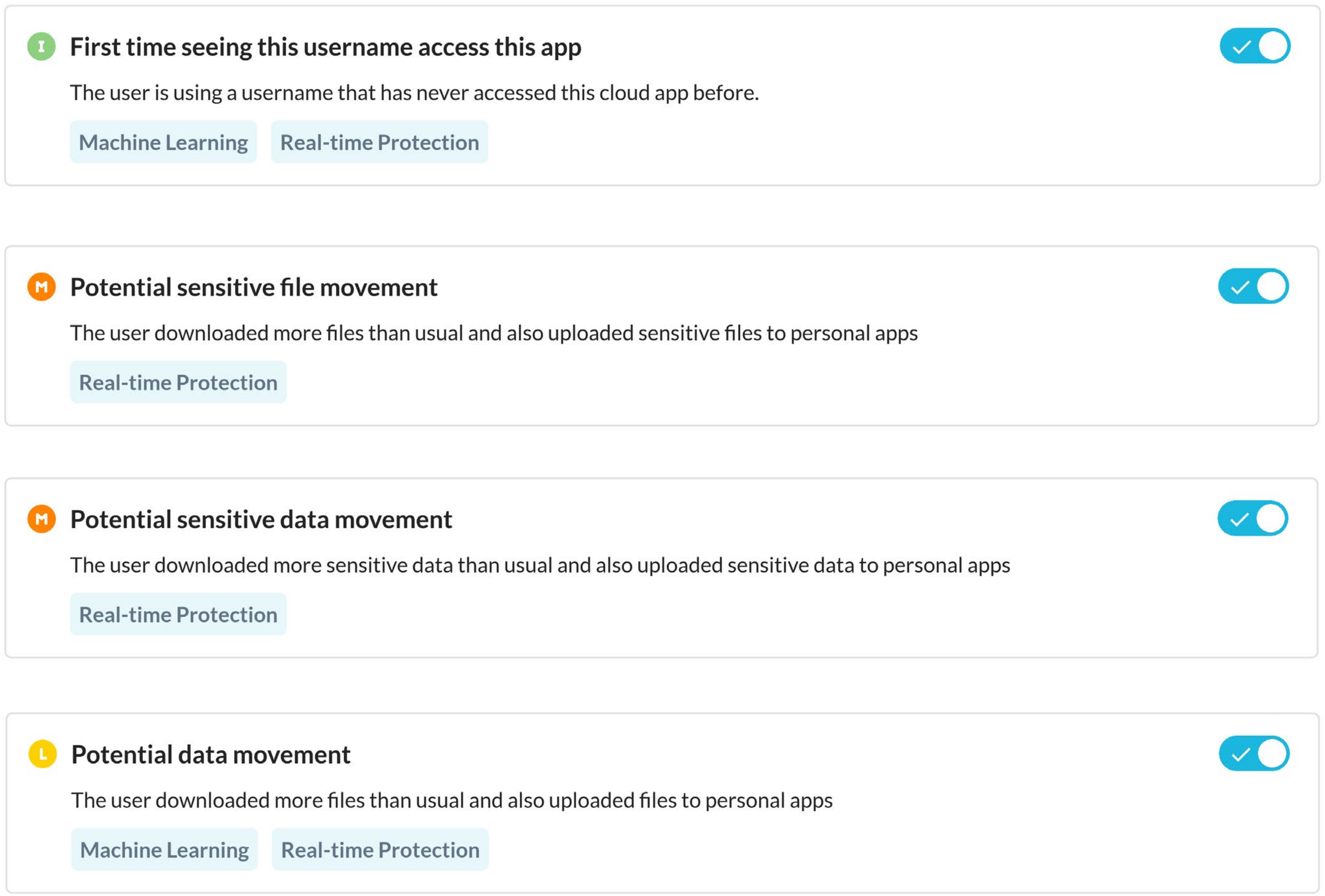
Required Features

Cloud Inline/NG SWG + DLP + Advanced UEBA

Summary

A user uploaded approximately 2,400 files to their personal Google Drive from a managed device. More than 1,500 of the uploaded files triggered DLP policies designed to identify sensitive information. This was also the first time the user authenticated to their personal Google Drive from the managed device. The authentication and subsequent upload activity triggered multiple types of alerts around data movement. The data exfiltration activity started approximately 12 days prior to the user leaving the organization. The alerts reduced the user's UCI from 998 (good) to 147 (poor).

Detections Involved



I **First time seeing this username access this app** ✓

The user is using a username that has never accessed this cloud app before.

Machine Learning | Real-time Protection

M **Potential sensitive file movement** ✓

The user downloaded more files than usual and also uploaded sensitive files to personal apps

Real-time Protection

M **Potential sensitive data movement** ✓

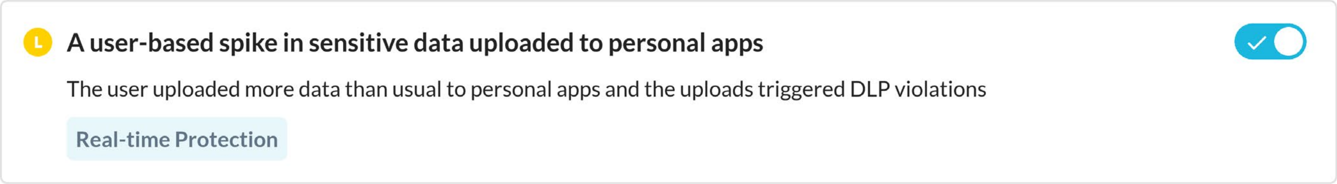
The user downloaded more sensitive data than usual and also uploaded sensitive data to personal apps

Real-time Protection

L **Potential data movement** ✓

The user downloaded more files than usual and also uploaded files to personal apps

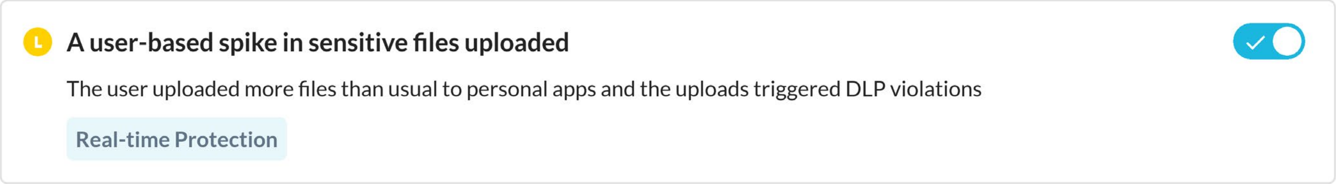
Machine Learning | Real-time Protection



L **A user-based spike in sensitive data uploaded to personal apps** ✓

The user uploaded more data than usual to personal apps and the uploads triggered DLP violations

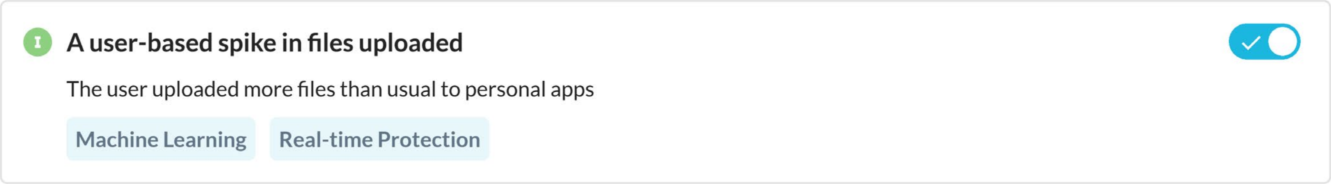
Real-time Protection



L **A user-based spike in sensitive files uploaded** ✓

The user uploaded more files than usual to personal apps and the uploads triggered DLP violations

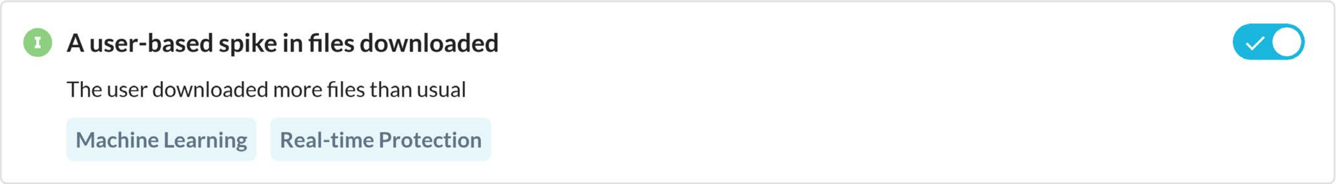
Real-time Protection



I **A user-based spike in files uploaded** ✓

The user uploaded more files than usual to personal apps

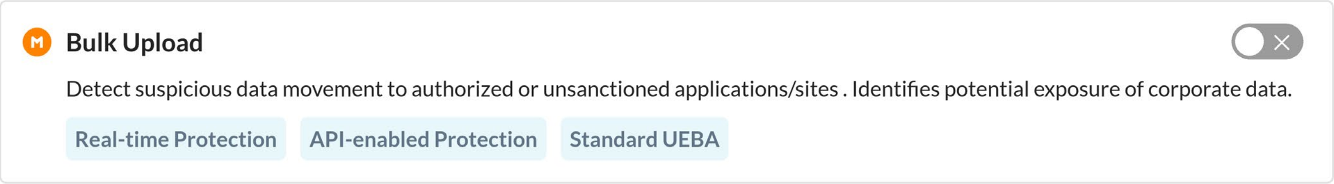
Machine Learning | Real-time Protection



I **A user-based spike in files downloaded** ✓

The user downloaded more files than usual

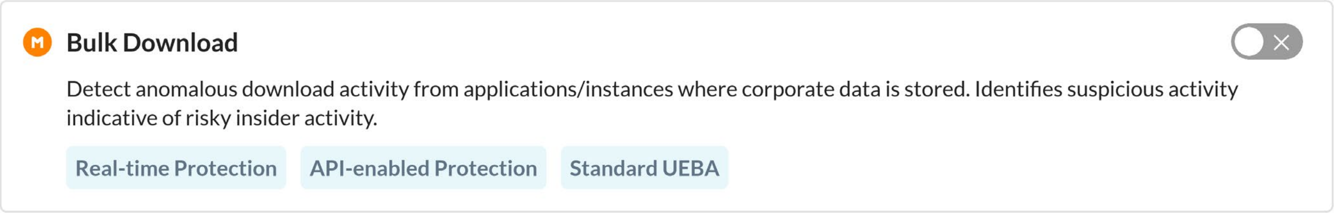
Machine Learning | Real-time Protection



M **Bulk Upload** ✕

Detect suspicious data movement to authorized or unsanctioned applications/sites . Identifies potential exposure of corporate data.

Real-time Protection | API-enabled Protection | Standard UEBA



M **Bulk Download** ✕

Detect anomalous download activity from applications/instances where corporate data is stored. Identifies suspicious activity indicative of risky insider activity.

Real-time Protection | API-enabled Protection | Standard UEBA

Case Study 3: Compromised Device - Ransomware

Threat Summary

An unmanaged device was infected with BlackMirror Ransomware.

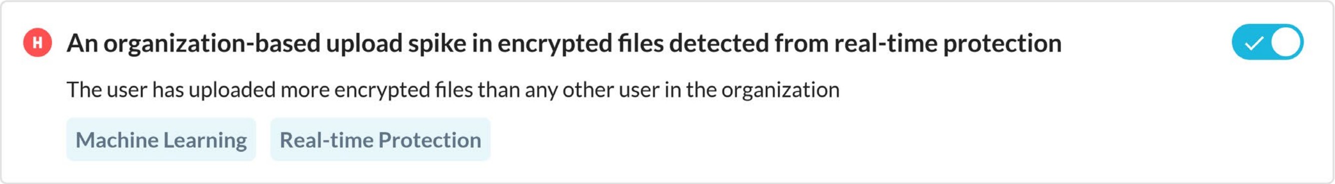
Required Features

CASB API + DLP + Advanced UEBA

Summary

A user uploaded files encrypted by the Crysis Arena ransomware to their company's managed Google Drive instance from an unmanaged device and shared the files with other users within the organization. The files had the extension[black.mirror@qq.com].arena, which is used by the Crysis Arena ransomware. The files also triggered alerts for uploads of a large number of encrypted files, identified by Netskope's ML-powered encrypted file detection. The alerts reduced the user's UCI from 998 (good) to 648 (moderate).

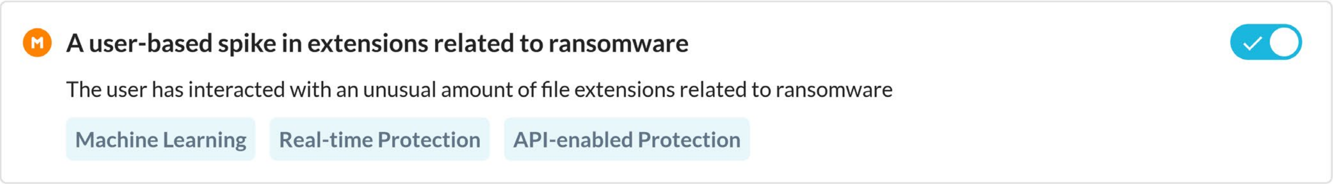
Detections Involved



H **An organization-based upload spike in encrypted files detected from real-time protection** ✓

The user has uploaded more encrypted files than any other user in the organization

Machine Learning | Real-time Protection



M **A user-based spike in extensions related to ransomware** ✓

The user has interacted with an unusual amount of file extensions related to ransomware

Machine Learning | Real-time Protection | API-enabled Protection

Case Study 4: Compromised Device - Ransomware

Threat Summary

An unmanaged device was infected with RansomExx ransomware.

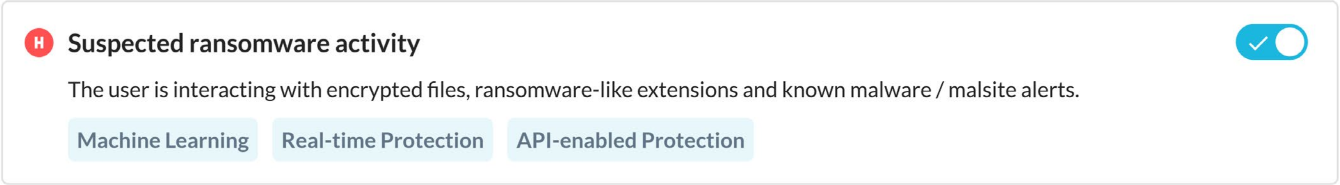
Required Features

CASB API + DLP + Advanced UEBA

Summary

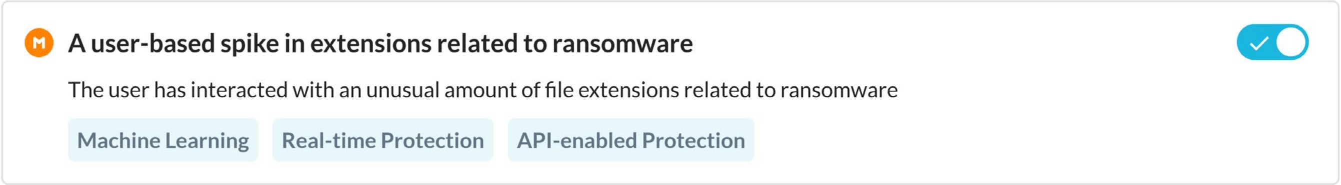
A user uploaded more than 1,880 unique files from an unmanaged device to their company's managed Microsoft O365 OneDrive instance. The files contained a .exx extension appended to the original file names. The extension is used by the RansomExx ransomware. The activity triggered a number of alerts related to spikes of files uploaded, encrypted files uploaded (identified by Netskope's ML-powered encrypted file detection), and suspected ransomware activity. The alerts reduced the user's UCI from 967 (good) to 197 (poor).

Detections Involved



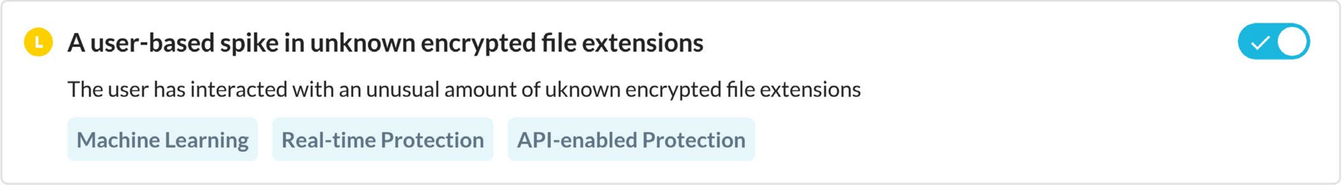
H **Suspected ransomware activity** ✓

The user is interacting with encrypted files, ransomware-like extensions and known malware / malsite alerts.



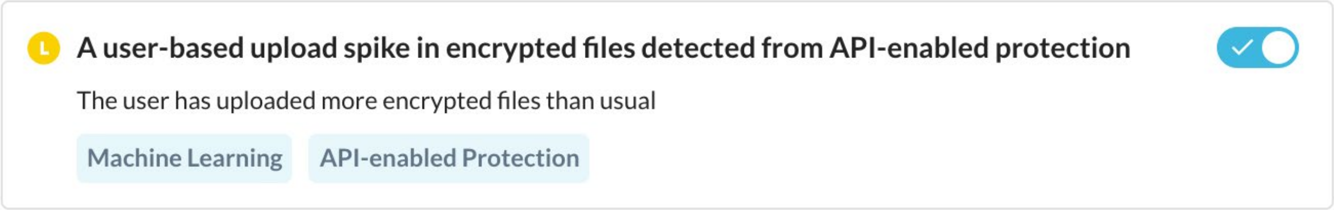
M **A user-based spike in extensions related to ransomware** ✓

The user has interacted with an unusual amount of file extensions related to ransomware



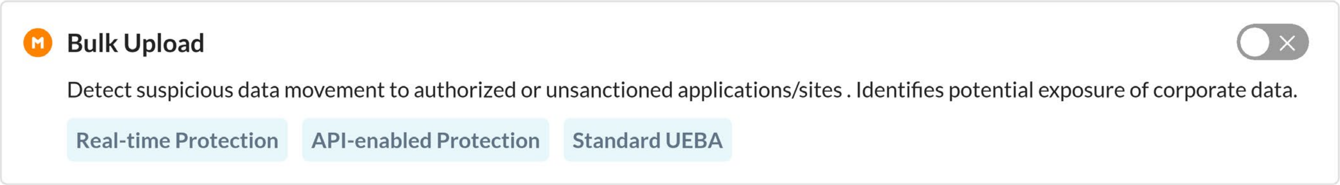
L **A user-based spike in unknown encrypted file extensions** ✓

The user has interacted with an unusual amount of uknown encrypted file extensions



L **A user-based upload spike in encrypted files detected from API-enabled protection** ✓

The user has uploaded more encrypted files than usual



M **Bulk Upload** ✕

Detect suspicious data movement to authorized or unsanctioned applications/sites . Identifies potential exposure of corporate data.

Case Study 5: Compromised Account

Threat Summary

A user’s Office365 credential was being used from an unrecognized location.

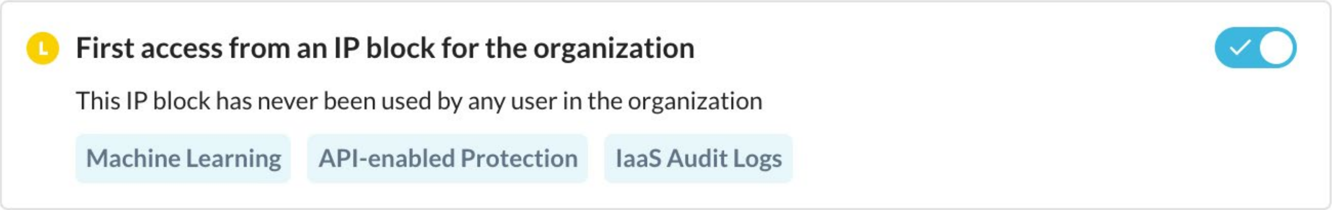
Required Features

CASB API + Advanced UEBA

Summary

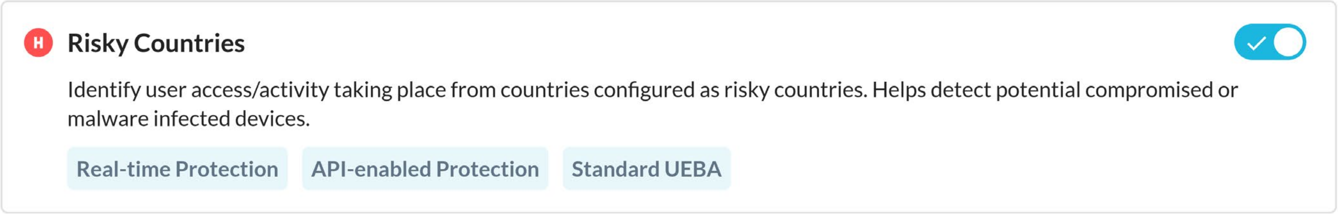
A user successfully authenticated from multiple IP addresses in an IP address block that had never before been used by any other user in the organization. The authentications were to the company’s managed Microsoft Office 365 OneDrive instance, and set off the "First access from an IP block for the organization" five times. It also triggered the “Risky Countries” alert for access originating from countries in a customer-configured watchlist. The alerts reduced the user’s UCI from 998 (good) to 472 (moderate).

Detections Involved



First access from an IP block for the organization

This IP block has never been used by any user in the organization



Risky Countries

Identify user access/activity taking place from countries configured as risky countries. Helps detect potential compromised or malware infected devices.

Case Study 6: Compromised Account

Threat Summary

A user’s Office365 credential was being used from an unrecognized location.

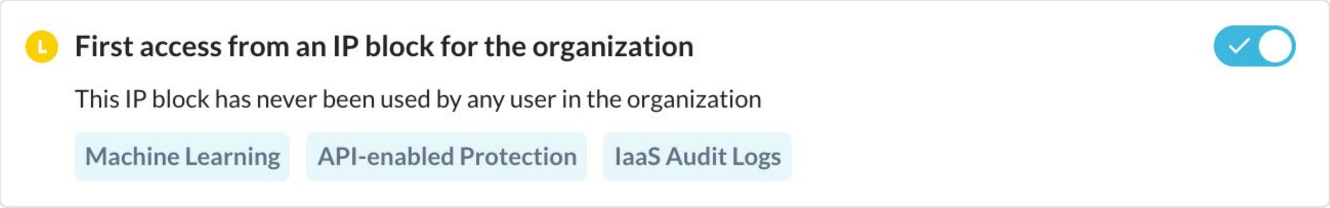
Required Features

CASB API + Advanced UEBA

Summary

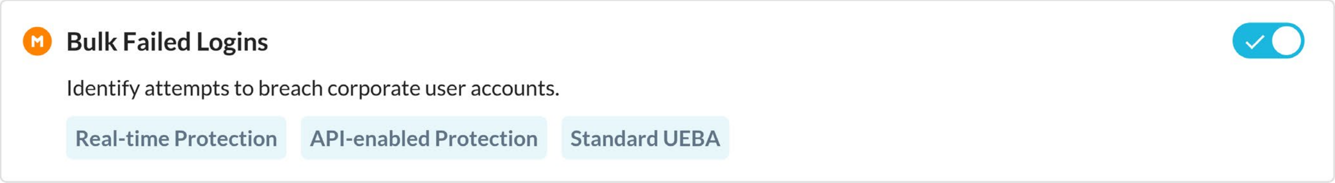
A user had 279 failed login attempts, which triggered 28 “Bulk Failed Logins” alerts. The user successfully authenticated from IP addresses in an IP address block that had never before been used by any other user in the organization. The authentications were to the company’s managed Microsoft Office 365 OneDrive and Sharepoint instances, and set off the "First access from an IP block for the organization" 13 times. The user also triggered the "Risky Countries" alert. The alerts reduced the user’s UCI from 998 (good) to 233 (poor).

Detections Involved



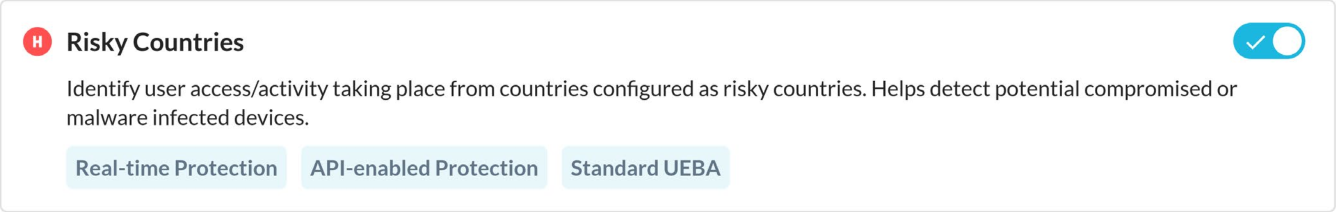
First access from an IP block for the organization

This IP block has never been used by any user in the organization



Bulk Failed Logins

Identify attempts to breach corporate user accounts.



Risky Countries

Identify user access/activity taking place from countries configured as risky countries. Helps detect potential compromised or malware infected devices.

MITIGATING INSIDER RISK

Risky insider behaviors determined by UEBA AI-driven machine learning models trigger user specific alerts and automatic UCI score reductions. Insider risk mitigation strategies can be implemented in addition to threat prevention and data loss prevention policies.

1. Netskope Cloud Exchange includes a Cloud Risk Exchange (CRE) module that is designed to ingest user, device and application risk scores, creating a dashboard view of contributors to a company's overall risk score and trend. This tool, freely available to all Netskope customers, can be used to normalize risk scores across multiple vendors, and trigger risk-reducing actions through business rules that are tuned to a weighted score.
2. Real-time policies with UCI enable automated policy-based actions when a user's UCI drops below a configured threshold. These policies can be used to drive mitigation actions such as step-up authentication, and limiting user access to sensitive data.
3. Netskope Advanced Analytics provides an insider threat dashboard in the Netskope Library for monitoring a user's risky activities. The dashboard can be further customized for tenant specific requirements.

Increasingly, insider threat cases and high-profile data leaks illustrate the need for strong insider threat programs within organizations. The number of infamous and damaging attacks illustrates that the threat posed by trusted insiders is significant. This threat will continue to grow as increased information-sharing results in greater access to and distribution of sensitive information.

Customers are advised to leverage the AI/ML driven detections in Advanced UEBA on top of other controls, including Advanced DLP and Advanced Threat, to uncover these hidden threats and develop an insider threat response program to effectively deter, react, and protect their organizations.