Cloud Security Solutions Blog

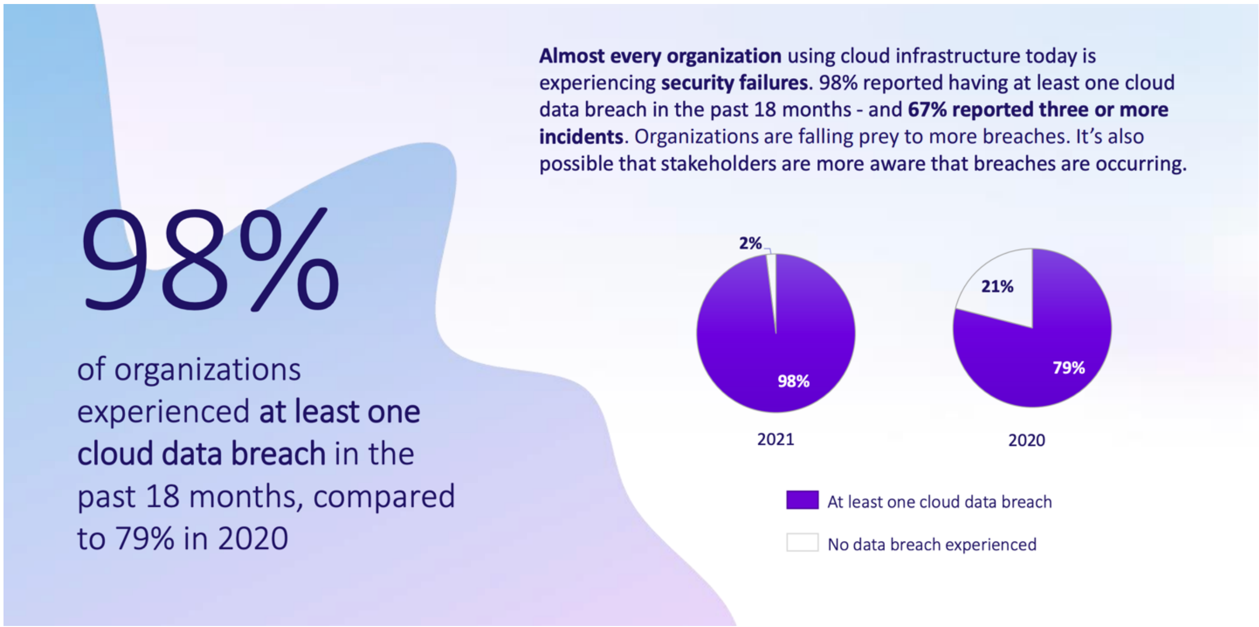
Mitigate Common Cloud Threats with MVISION Cloud

New company.
Enterprise focused.
Bright future.

February 3, 2022

Team, In this blog I would like to highlight the most common cloud threats that can bring risk to your organization. These were identified by the McAfee team in Q2 2021 and subsequently covered in the recent McAfee Enterprise Advanced Threat Research Report published in October 2021. Most important, I will share how the MVISION Unified Cloud Edge platform can help your organization mitigate these threats.

According to a **2021 IDC Survey Report on the state of Cloud Security**, 98% of organizations reported having at least one cloud data breach in the past 18 months and 67% reported three or more incidents.

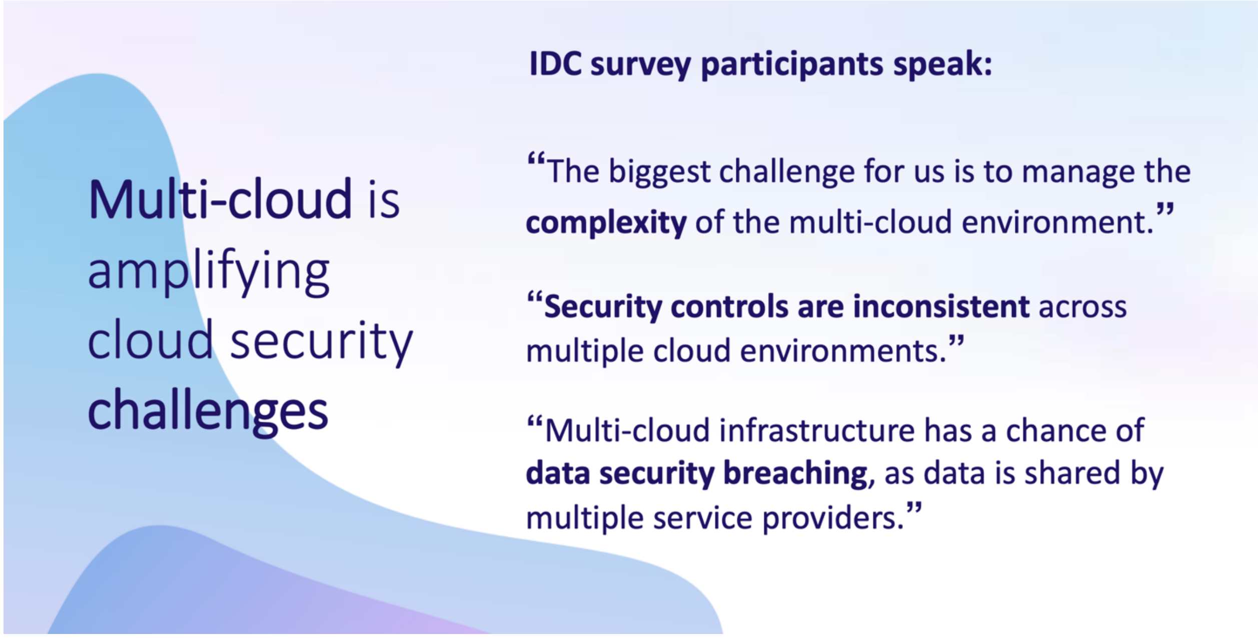


Almost every organization using cloud infrastructure today is experiencing **security failures**. 98% reported having at least one cloud data breach in the past 18 months - and **67% reported three or more incidents**. Organizations are falling prey to more breaches. It's also possible that stakeholders are more aware that breaches are occurring.

98%

of organizations experienced **at least one cloud data breach** in the past 18 months, compared to 79% in 2020

2%
98%
2021
21%
79%
2020
🟪 At least one cloud data breach
□ No data breach experienced



Multi-cloud is amplifying cloud security challenges

IDC survey participants speak:

"The biggest challenge for us is to manage the **complexity** of the multi-cloud environment."

"**Security controls are inconsistent** across multiple cloud environments."

"Multi-cloud infrastructure has a chance of **data security breaching**, as data is shared by multiple service providers."

So how are these attackers getting in?

In our latest Advanced Threat Research **report** published in October 2021, McAfee Enterprise's Advanced Threat team identified the most common cloud threat vectors.

Most common cloud threats published in our research in October 2021 include:

1. Excessive Usage from Anomalous Location.
2. Insider Data Exfiltration.
3. Privilege Access Misuse.
4. High Risk Data Exfiltration.
5. Privilege Access Exfiltration.
6. Land Expand Exfiltration.
7. Suspicious Superhuman.
8. Data Exfiltration by Privileged User.

How to Mitigate Suspicious Access with MVISION Unified Cloud Edge (SSE)

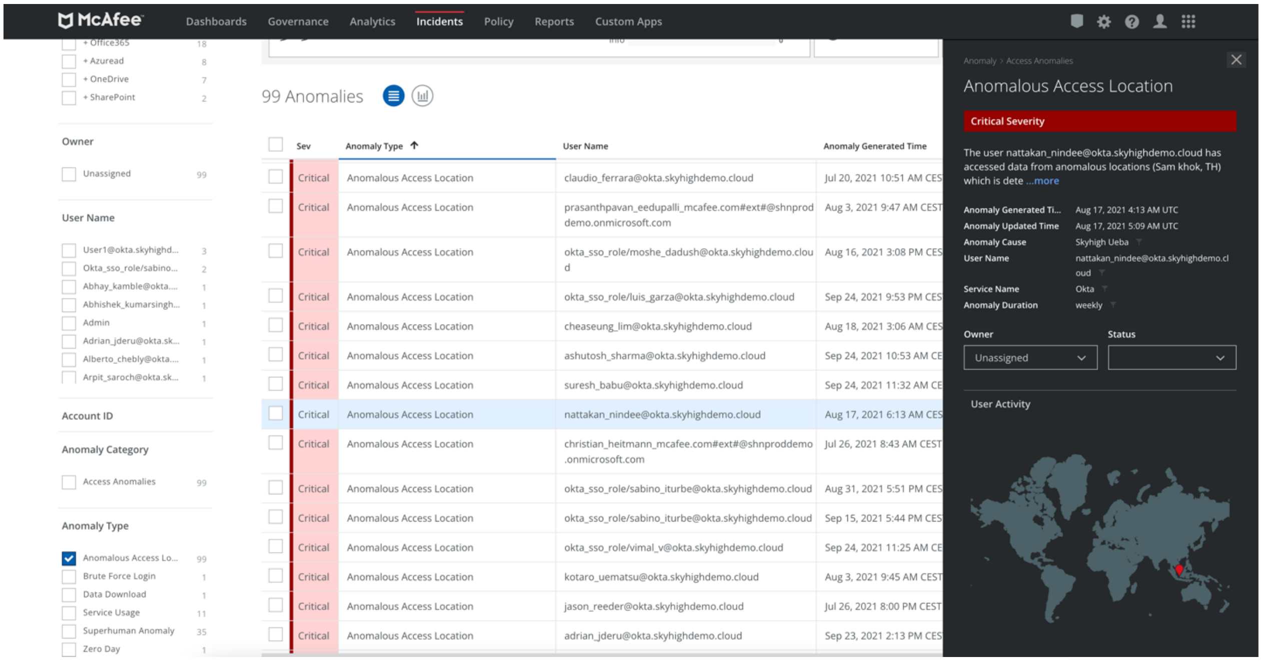
Suspicious access anomalies generally deserve rapid attention by your security team. This activity can involve any number of different behaviors that reflect anomalous access patterns, file changes, database activities and other abnormal activity that indicates a possible attack. The two most common suspicious access anomalies from our research are:

Excessive Usage from Anomalous Location:

This usage pattern begins with login from a location that has not been previously detected and is anomalous to the user’s organization. The threat actor then initiates data access, which may include high volumes suggestive of data exfiltration and/or other privileged access activity.

How MVISION Unified Cloud Edge helps

MVISION Unified Cloud Edge's User and Entity Behavior Analytics (UEBA) evaluate user activities beyond an initial login. This includes user movements, access to organizational assets and the context with which that access occurs. For example, when a user registers activity from an IP address, geographic location, or an organization that is suspicious, on a block list, or is associated directly with a competitor this behaviour will trigger anomaly detection. The use of anomalous access locations are generally good indicators of potentially compromised accounts or insider threats.



□ + Office365	18
□ + Azuread	8
□ + OneDrive	7
□ + SharePoint	2

Owner

□ Unassigned	99

User Name

□ User1@okta.skyhighd...	3
□ Okta_sso_role/sabino...	2
□ Abhay_kamble@okta....	1
□ Abhishek_kumarsingh...	1
□ Admin	1
□ Adrian_jderu@okta.sk...	1
□ Alberto_chebly@okta....	1
□ Arpit_saroch@okta.sk...	1

Account ID

Anomaly Category

□ Access Anomalies	99

Anomaly Type

☑ Anomalous Access Lo...	99
□ Brute Force Login	1
□ Data Download	1
□ Service Usage	11
□ Superhuman Anomaly	35
□ Zero Day	1

99 Anomalies

□	Sev	Anomaly Type ↑	User Name	Anomaly Generated Time
□	Critical	Anomalous Access Location	claudio_ferrara@okta.skyhighdemo.cloud	Jul 20, 2021 10:51 AM CES
□	Critical	Anomalous Access Location	prasanthpavan_eedupalli_mcafee.com#ext#@shnproddemo.onmicrosoft.com	Aug 3, 2021 9:47 AM CEST
□	Critical	Anomalous Access Location	okta_sso_role/moshe_dadush@okta.skyhighdemo.cloud	Aug 16, 2021 3:08 PM CES
□	Critical	Anomalous Access Location	okta_sso_role/luis_garza@okta.skyhighdemo.cloud	Sep 24, 2021 9:53 PM CES
□	Critical	Anomalous Access Location	cheaseung_lim@okta.skyhighdemo.cloud	Aug 18, 2021 3:06 AM CES
□	Critical	Anomalous Access Location	ashutosh_sharma@okta.skyhighdemo.cloud	Sep 24, 2021 10:53 AM CE
□	Critical	Anomalous Access Location	suresh_babu@okta.skyhighdemo.cloud	Sep 24, 2021 11:32 AM CE
□	Critical	Anomalous Access Location	nattakan_nindee@okta.skyhighdemo.cloud	Aug 17, 2021 6:13 AM CES
□	Critical	Anomalous Access Location	christian_heitmann_mcafee.com#ext#@shnproddemo.onmicrosoft.com	Jul 26, 2021 8:43 AM CEST
□	Critical	Anomalous Access Location	okta_sso_role/sabino_iturbe@okta.skyhighdemo.cloud	Aug 31, 2021 5:51 PM CES
□	Critical	Anomalous Access Location	okta_sso_role/sabino_iturbe@okta.skyhighdemo.cloud	Sep 15, 2021 5:44 PM CES
□	Critical	Anomalous Access Location	okta_sso_role/vimal_v@okta.skyhighdemo.cloud	Sep 24, 2021 11:25 AM CE
□	Critical	Anomalous Access Location	kotaro_uematsu@okta.skyhighdemo.cloud	Aug 3, 2021 9:45 AM CEST
□	Critical	Anomalous Access Location	jason_reeder@okta.skyhighdemo.cloud	Jul 26, 2021 8:00 PM CEST
□	Critical	Anomalous Access Location	adrian_jderu@okta.skyhighdemo.cloud	Sep 23, 2021 2:13 PM CES

Anomaly > Access Anomalies

Anomalous Access Location

Critical Severity

The user nattakan_nindee@okta.skyhighdemo.cloud has accessed data from anomalous locations (Sam khok, TH) which is dete ...more

Anomaly Generated Ti...	Aug 17, 2021 4:13 AM UTC
Anomaly Updated Time	Aug 17, 2021 5:09 AM UTC
Anomaly Cause	Skyhigh Ueba
User Name	nattakan_nindee@okta.skyhighdemo.cloud
Service Name	Okta
Anomaly Duration	weekly

Owner: Unassigned

Status:

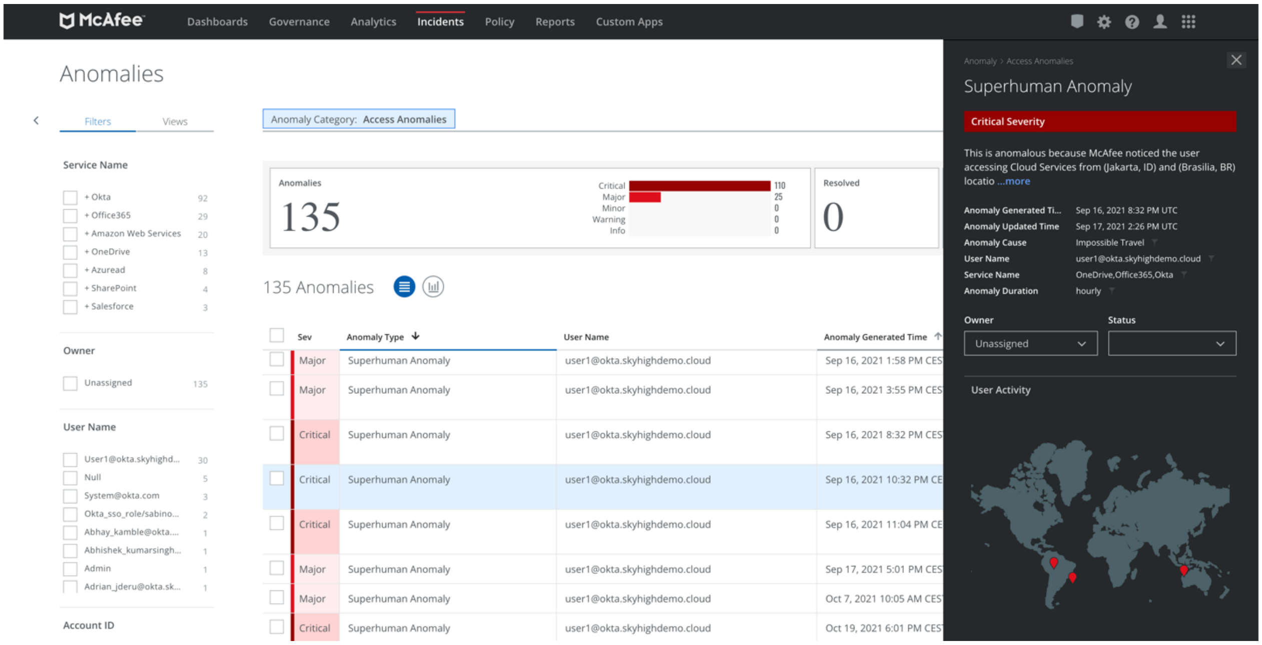
User Activity

Suspicious Superhuman:

In the second type of suspicious access our research noted, a login is attempted from more than one geographically distant location, and then another login is attempted form another geographic location which is impossible to travel to in the window of time since the first login attempt. As an example of suspicious superhuman behavior might login into Microsoft 365 from an IP address in Singapore, and then log into Slack from an IP address in California five minute later.

How MVISION Unified Cloud Edge helps

MVISION Unified Cloud Edge's UEBA detects Superhuman Anomalies in these scenarios. Login from a geographically distant locations is followed by another in a time period which is much too short given the required travel time. This Superhuman Anomaly detection is triggered even if two different supported cloud services are accessed from geographically distant locations for the same user.



Anomalies

Anomaly Category: Access Anomalies

Service Name

□ + Okta	92
□ + Office365	29
□ + Amazon Web Services	20
□ + OneDrive	13
□ + Azuread	8
□ + SharePoint	4
□ + Salesforce	3

Owner

□ Unassigned	135

User Name

□ User1@okta.skyhighd...	30
□ Null	5
□ System@okta.com	3
□ Okta_sso_role/sabino...	2
□ Abhay_kamble@okta....	1
□ Abhishek_kumarsingh...	1
□ Admin	1
□ Adrian_jderu@okta.sk...	1

Account ID

Anomalies 135

Critical	110
Major	25
Minor	0
Warning	0
Info	0

Resolved 0

□	Sev	Anomaly Type	User Name	Anomaly Generated Time
□	Major	Superhuman Anomaly	user1@okta.skyhighdemo.cloud	Sep 16, 2021 1:58 PM CES
□	Major	Superhuman Anomaly	user1@okta.skyhighdemo.cloud	Sep 16, 2021 3:55 PM CES
□	Critical	Superhuman Anomaly	user1@okta.skyhighdemo.cloud	Sep 16, 2021 8:32 PM CES
□	Critical	Superhuman Anomaly	user1@okta.skyhighdemo.cloud	Sep 16, 2021 10:32 PM CE
□	Critical	Superhuman Anomaly	user1@okta.skyhighdemo.cloud	Sep 16, 2021 11:04 PM CE
□	Major	Superhuman Anomaly	user1@okta.skyhighdemo.cloud	Sep 17, 2021 5:01 PM CES
□	Major	Superhuman Anomaly	user1@okta.skyhighdemo.cloud	Oct 7, 2021 10:05 AM CES
□	Critical	Superhuman Anomaly	user1@okta.skyhighdemo.cloud	Oct 19, 2021 6:01 PM CES

Anomaly > Access Anomalies

Superhuman Anomaly

Critical Severity

This is anomalous because McAfee noticed the user accessing Cloud Services from (Jakarta, ID) and (Brasilia, BR) locatio ...more

Anomaly Generated Ti...	Sep 16, 2021 8:32 PM UTC
Anomaly Updated Time	Sep 17, 2021 2:26 PM UTC
Anomaly Cause	Impossible Travel
User Name	user1@okta.skyhighdemo.cloud
Service Name	OneDrive,Office365,Okta
Anomaly Duration	hourly

Owner: Unassigned

Status:

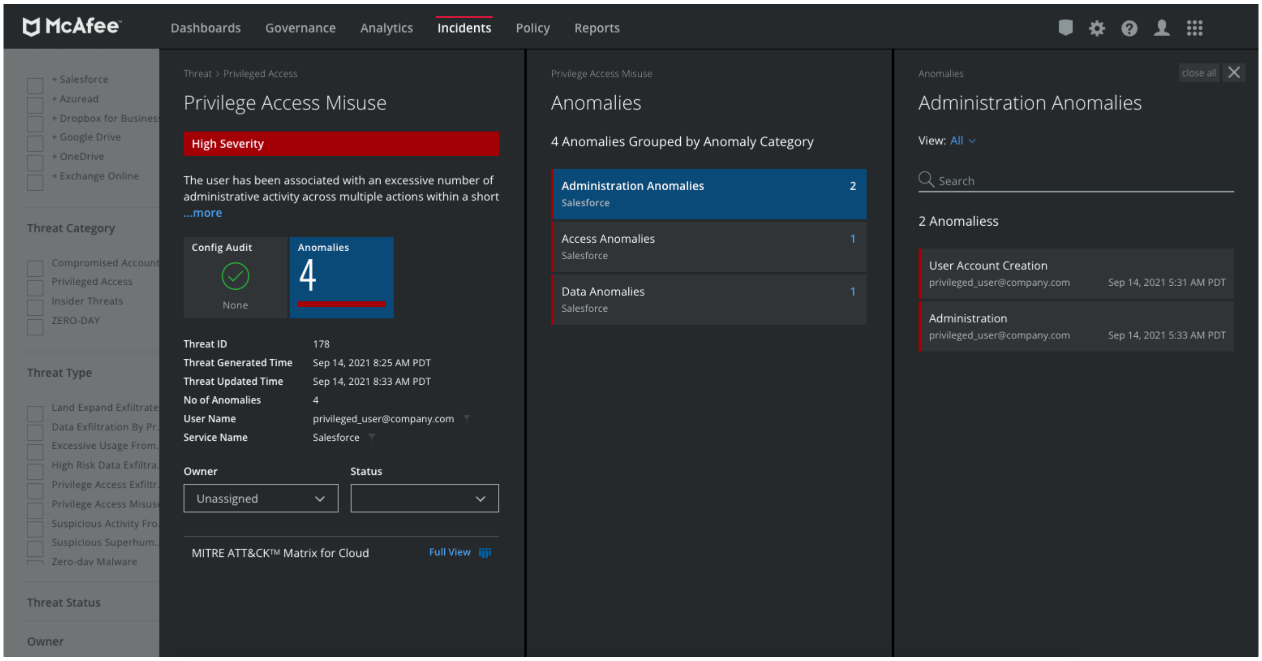
How to Mitigate Privilege Abuse with MVISION Unified Cloud Edge (SSE)

Privilege Access Misuse and Data Exfiltration by Privileged User

Privileged account misuse is one of the most dangerous threats because it is relatively easy for threat actors to execute and takes considerable time to detect. The simplest and most common situation is when a malicious insider uses legitimate permissions for malicious activities. For example, malicious users who can add, delete, or modify existing users have unparalleled access to an organization's Sanctioned IT cloud services. This provides these malicious users the greatest opportunity to compromise valuable or sensitive data.

How MVISION Unified Cloud Edge helps

MVISION Unified Cloud Edge identifies Privileged Access anomalies when an administrative user engages in activity that exceeds established thresholds for normal behaviour in a Sanctioned cloud service. This may indicate a malicious user is creating new accounts to conceal unauthorized access. Malicious users may also take advantage of activity such as an unusually large hiring spike or an unfortunate period of layoffs to manipulate account credentials. These administrative anomalies are linked to specific threats involving privileged access misuse. These anomalies are most easily identified based on activity thresholds and are then mapped to specific service actions.



Threat > Privileged Access

Privilege Access Misuse

High Severity

The user has been associated with an excessive number of administrative activity across multiple actions within a short ...more

Config Audit ✓ None

Anomalies 4

Threat ID	178
Threat Generated Time	Sep 14, 2021 8:25 AM PDT
Threat Updated Time	Sep 14, 2021 8:33 AM PDT
No of Anomalies	4
User Name	privileged_user@company.com
Service Name	Salesforce

Owner: Unassigned

Status:

MITRE ATT&CK™ Matrix for Cloud

Privilege Access Misuse

Anomalies

4 Anomalies Grouped by Anomaly Category

Administration Anomalies Salesforce	2
Access Anomalies Salesforce	1
Data Anomalies Salesforce	1

Anomalies

Administration Anomalies

View: All

2 Anomaliess

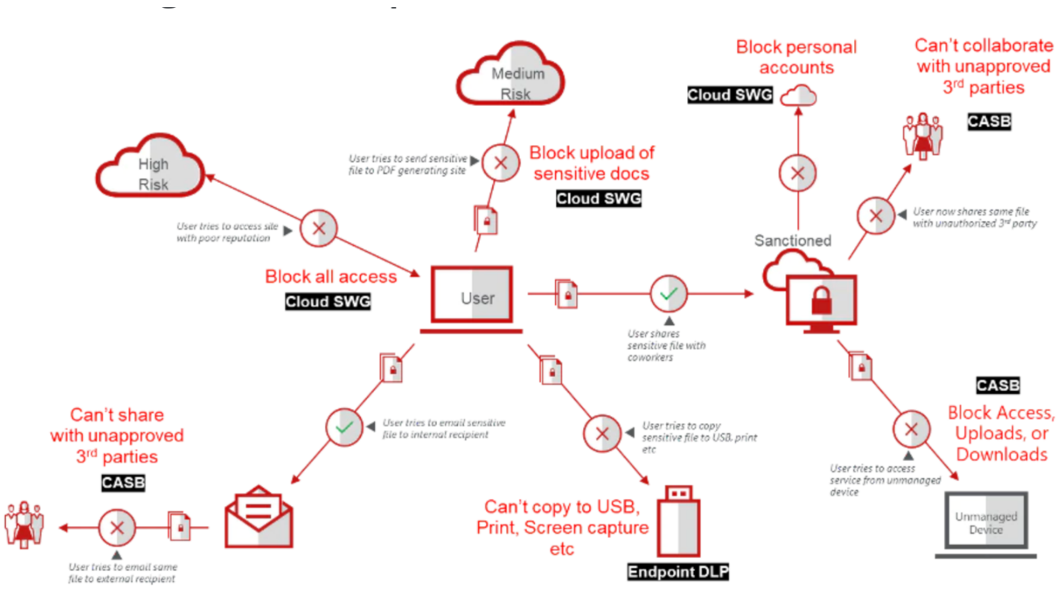
User Account Creation privileged_user@company.com	Sep 14, 2021 5:31 AM PDT
Administration privileged_user@company.com	Sep 14, 2021 5:33 AM PDT

How to Mitigate Data Exfiltration with MVISION Unified Cloud Edge

Data exfiltration occurs either through outsider or insider threats. It could be carried out by external cybercriminals, or employees that try to gain access to an organization's assets and data with malicious intent. Legacy approaches to data loss prevention (DLP), such as building walls around the critical data, fail in today's always-connected world.

Let’s have a look how MVISION UCE unified data protection across endpoints, networks, and the cloud. MVISION UCE provides organizations with consistent DLP Policy, data classification and incident management across the network. MVISION UCE also protects both sanctioned and unsanctioned (Shadow IT) cloud applications, web traffic, and endpoints, thereby covering multiple key exfiltration vectors.

Unified Multi-Vector Data Protection

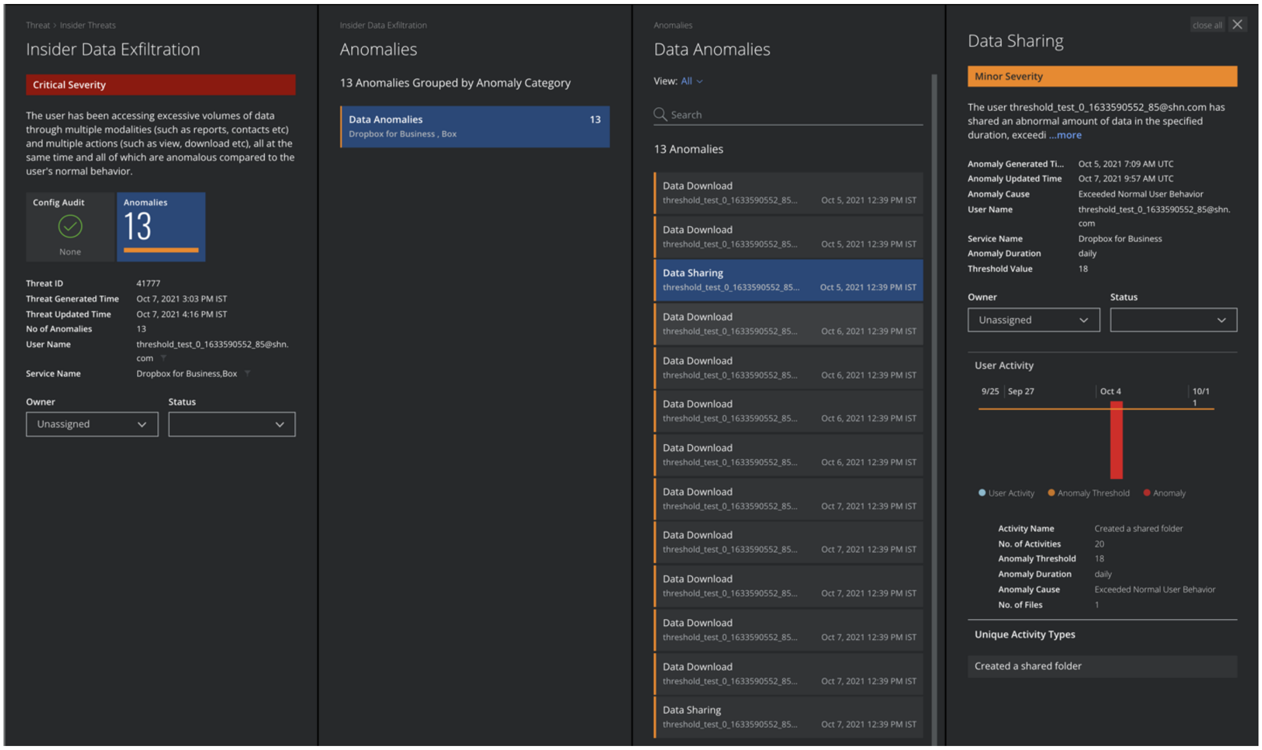

Medium Risk
High Risk
Block personal accounts
Cloud SWG
Can’t collaborate with unapproved 3rd parties
CASB
User tries to send sensitive file to PDF generating site
Block upload of sensitive docs
Cloud SWG
User tries to access site with poor reputation
Sanctioned
User now shares same file with unauthorized 3rd party
Block all access
Cloud SWG
User
User shares sensitive file with coworkers
CASB
Block Access, Uploads, or Downloads
Can’t share with unapproved 3rd parties
CASB
User tries to email sensitive file to internal recipient
User tries to copy sensitive file to USB, print etc
User tries to access service from unmanaged device
Can’t copy to USB, Print, Screen capture etc
Endpoint DLP
Unmanaged Device
User tries to email same file to external recipient

Insider Data Exfiltration:

An insider data threat is a threat to an organization that comes from malicious personnel within the organization. Malicious insiders may be employees, contractors, or third-party suppliers. Malicious insiders generally have inside information concerning the organization's security practices, data, and computer systems which they can use to compromise the organization’s assets and networks. The threat’s brought by an insider data threat generally involve the theft of commercially valuable information or the theft of confidential intellectual property.

How MVISION Unified Cloud Edge helps

MVISION Unified Cloud Edge detect anomalous behavior across multiple dimensions with respect to data movement. This behavior data may include the amount of data which is uploaded, downloaded, or shared, the volume of user actions, access counts, and frequency of these actions within cloud services. Insider Threats anomalies may also indicate users are accessing an unusual number of files for a special project.



Threat > Insider Threats

Insider Data Exfiltration

Critical Severity

The user has been accessing excessive volumes of data through multiple modalities (such as reports, contacts etc) and multiple actions (such as view, download etc), all at the same time and all of which are anomalous compared to the user's normal behavior.

Config Audit ✓ None

Anomalies 13

Threat ID	41777
Threat Generated Time	Oct 7, 2021 3:03 PM IST
Threat Updated Time	Oct 7, 2021 4:16 PM IST
No of Anomalies	13
User Name	threshold_test_0_1633590552_85@shn.com
Service Name	Dropbox for Business,Box

Owner: Unassigned

Status:

Insider Data Exfiltration

Anomalies

13 Anomalies Grouped by Anomaly Category

Data Anomalies 13
Dropbox for Business , Box

Anomalies

Data Anomalies

View: All

Search

13 Anomalies

Data Download	threshold_test_0_1633590552_85...	Oct 5, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 5, 2021 12:39 PM IST
Data Sharing	threshold_test_0_1633590552_85...	Oct 5, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 6, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 6, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 6, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 6, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 7, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 7, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 7, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 7, 2021 12:39 PM IST
Data Download	threshold_test_0_1633590552_85...	Oct 7, 2021 12:39 PM IST
Data Sharing	threshold_test_0_1633590552_85...	Oct 7, 2021 12:39 PM IST

Data Sharing

Minor Severity

The user threshold_test_0_1633590552_85@shn.com has shared an abnormal amount of data in the specified duration, exceedi ...more

Anomaly Generated Ti...	Oct 5, 2021 7:09 AM UTC
Anomaly Updated Time	Oct 7, 2021 9:57 AM UTC
Anomaly Cause	Exceeded Normal User Behavior
User Name	threshold_test_0_1633590552_85@shn.com
Service Name	Dropbox for Business
Anomaly Duration	daily
Threshold Value	18

Owner: Unassigned

Status:

User Activity

Activity Name	Created a shared folder
No. of Activities	20
Anomaly Threshold	18
Anomaly Duration	daily
Anomaly Cause	Exceeded Normal User Behavior
No. of Files	1

Unique Activity Types

Created a shared folder

High Risk Data Exfiltration:

Data is classified as High Risk if protection of the data is required by law or regulation, or, if the loss of confidentiality, integrity, or availability of the data could have a significant adverse impact on the safety, finances, or reputation of the organization. Organizations are experiencing high risk data loss across a wide range of content, formats, and methods, from documents to databases, stolen electronically or physically, and orchestrated by malicious insiders or external threat actors.

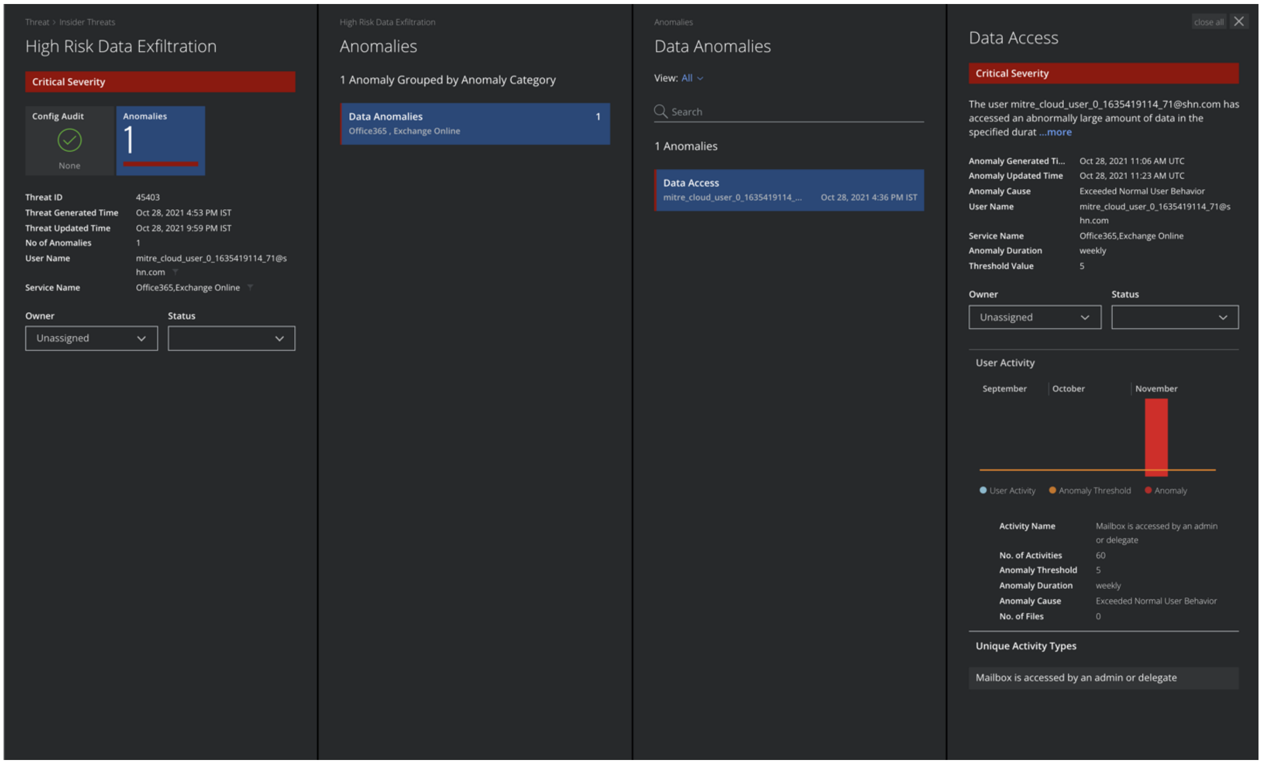
Example of High Risk data may include:

- Health Information, including Protected Health Information (PHI).
- Health Insurance policy ID numbers.
- Social Security Numbers.

- Credit card numbers.
- Financial account numbers.
- Export controlled information.
- Driver's license numbers.
- Passport and visa numbers.

How MVISION Unified Cloud Edge helps

MVISION Unified Cloud Edge can detect anomalies related to malicious insiders and users who may have found access to data for which they are not authorized. MVISION Unified Cloud Edge can also identify users who have access to high-risk data that may be at risk of loss.



Threat > Insider Threats

High Risk Data Exfiltration

Critical Severity

Config Audit: None

Anomalies: 1

Threat ID	45403
Threat Generated Time	Oct 28, 2021 4:53 PM IST
Threat Updated Time	Oct 28, 2021 9:59 PM IST
No of Anomalies	1
User Name	mitre_cloud_user_0_1635419114_71@shn.com
Service Name	Office365,Exchange Online

Owner: Unassigned
Status:

High Risk Data Exfiltration

Anomalies

1 Anomaly Grouped by Anomaly Category

Data Anomalies 1
Office365 , Exchange Online

Anomalies

Data Anomalies

View: All

Search

1 Anomalies

Data Access
mitre_cloud_user_0_1635419114_... Oct 28, 2021 4:36 PM IST

close all

Data Access

Critical Severity

The user mitre_cloud_user_0_1635419114_71@shn.com has accessed an abnormally large amount of data in the specified durat ...more

Anomaly Generated Ti...	Oct 28, 2021 11:06 AM UTC
Anomaly Updated Time	Oct 28, 2021 11:23 AM UTC
Anomaly Cause	Exceeded Normal User Behavior
User Name	mitre_cloud_user_0_1635419114_71@shn.com
Service Name	Office365,Exchange Online
Anomaly Duration	weekly
Threshold Value	5

Owner: Unassigned
Status:

User Activity

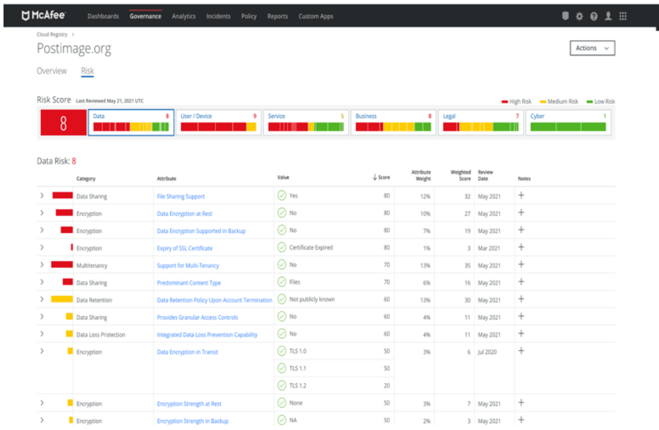
Activity Name	Mailbox is accessed by an admin or delegate
No. of Activities	60
Anomaly Threshold	5
Anomaly Duration	weekly
Anomaly Cause	Exceeded Normal User Behavior
No. of Files	0

Unique Activity Types

Mailbox is accessed by an admin or delegate

Exfiltration to High-Risk Cloud Services:

MVISION UCE detects the usage of risky unsanctioned cloud services and enforces policies, such blocking cloud services with a high risk, which can help prevent exfiltration of data.



Postimage.org

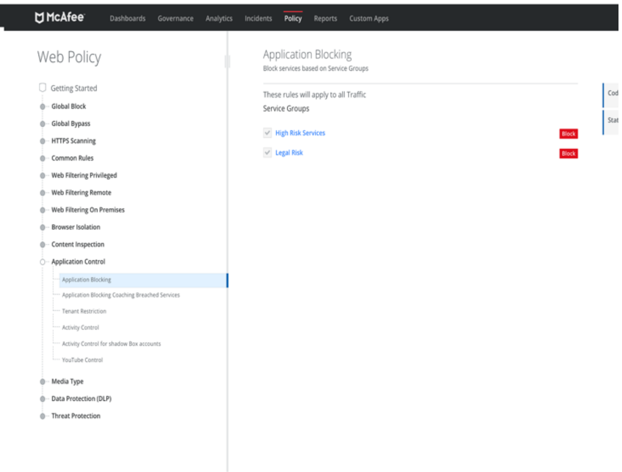
Risk Score Last Reviewed May 21, 2021 UTC

🟥 High Risk 🟨 Medium Risk 🟩 Low Risk

8	Data	User / Device	Service	Business	Legal	Cyber
	8	9	5	8	7	1

Data Risk: 8

Category	Attribute	Value	↓ Score	Attribute Weight	Weighted Score	Review Date	Notes
Data Sharing	File Sharing Support	✓ Yes	80	12%	32	May 2021	+
Encryption	Data Encryption at Rest	✓ No	80	10%	27	May 2021	+
Encryption	Data Encryption Supported in Backup	✓ No	80	7%	19	May 2021	+
Encryption	Expiry of SSL Certificate	✓ Certificate Expired	80	1%	3	Mar 2021	+
Multitenancy	Support for Multi-Tenancy	✓ No	70	13%	35	May 2021	+
Data Sharing	Predominant Content Type	✓ Files	70	6%	16	May 2021	+
Data Retention	Data Retention Policy Upon Account Termination	✓ Not publicly known	60	13%	30	May 2021	+
Data Sharing	Provides Granular Access Controls	✓ No	60	4%	11	May 2021	+
Data Loss Protection	Integrated Data Loss Prevention Capability	✓ No	60	4%	11	May 2021	+
Encryption	Data Encryption in Transit	✓ TLS 1.0	50	3%	6	Jul 2020	+
		✓ TLS 1.1	50				
		✓ TLS 1.2	20				
Encryption	Encryption Strength at Rest	✓ None	50	3%	7	May 2021	+
Encryption	Encryption Strength in Backup	✓ NA	50	2%	3	May 2021	+



Application Blocking

Block services based on Service Groups

These rules will apply to all Traffic

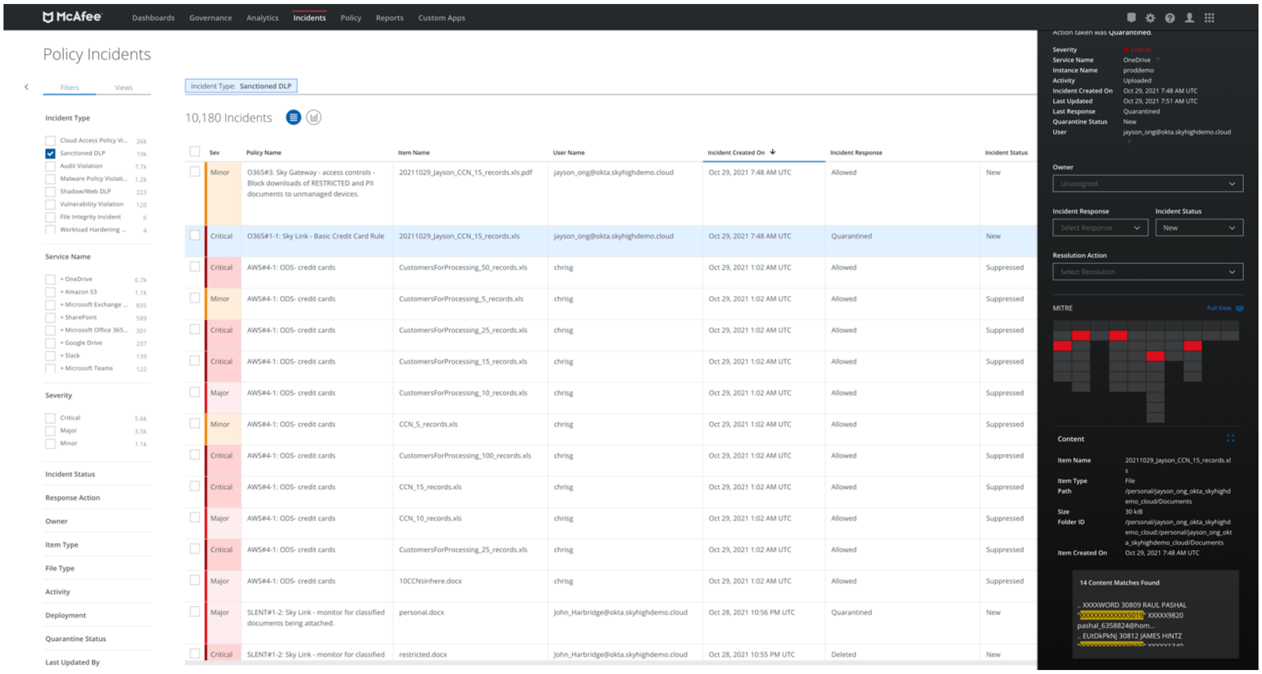
Service Groups

☑ High Risk Services — Block

☑ Legal Risk — Block

Exfiltration from sanctioned cloud services:

MVISION UCE apply collaboration controls to block unauthorized third party sharing and use inline controls like Tenant Restrictions to ensure employees always login with their corporate accounts and not with their personal accounts.



Policy Incidents

Incident Type

□	Cloud Access Policy Vi...	26k
☑	Sanctioned DLP	10k
□	Audit Violation	7.7k
□	Malware Policy Violati...	1.2k
□	Shadow/Web DLP	223
□	Vulnerability Violation	120
□	File Integrity Incident	6
□	Workload Hardening ...	4

Service Name

□	+ OneDrive	6.7k
□	+ Amazon S3	1.1k
□	+ Microsoft Exchange ...	835
□	+ SharePoint	589
□	+ Microsoft Office 365...	301
□	+ Google Drive	207
□	+ Slack	139
□	+ Microsoft Teams	122

Severity

□	Critical	5.6k
□	Major	3.5k
□	Minor	1.1k

Incident Status

Response Action

Owner

Item Type

File Type

Activity

Deployment

Quarantine Status

Last Updated By

Incident Type: Sanctioned DLP

10,180 Incidents

□	Sev	Policy Name	Item Name	User Name	Incident Created On	Incident Response	Incident Status
□	Minor	O365#3. Sky Gateway - access controls - Block downloads of RESTRICTED and PII documents to unmanaged devices.	20211029_Jayson_CCN_15_records.xls.pdf	jayson_ong@okta.skyhighdemo.cloud	Oct 29, 2021 7:48 AM UTC	Allowed	New
□	Critical	O365#1-1: Sky Link - Basic Credit Card Rule	20211029_Jayson_CCN_15_records.xls	jayson_ong@okta.skyhighdemo.cloud	Oct 29, 2021 7:48 AM UTC	Quarantined	New
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_50_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Minor	AWS#4-1: ODS- credit cards	CustomersForProcessing_5_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_25_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_15_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Major	AWS#4-1: ODS- credit cards	CustomersForProcessing_10_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Minor	AWS#4-1: ODS- credit cards	CCN_5_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_100_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CCN_15_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Major	AWS#4-1: ODS- credit cards	CCN_10_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_25_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Major	AWS#4-1: ODS- credit cards	10CCNsinhere.docx	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Major	SLENT#1-2: Sky Link - monitor for classified documents being attached.	personal.docx	John_Harbridge@okta.skyhighdemo.cloud	Oct 28, 2021 10:56 PM UTC	Quarantined	New
□	Critical	SLENT#1-2: Sky Link - monitor for classified	restricted.docx	John_Harbridge@okta.skyhighdemo.cloud	Oct 28, 2021 10:55 PM UTC	Deleted	New

Action taken was Quarantined.

Severity	● Critical
Service Name	OneDrive
Instance Name	proddemo
Activity	Uploaded
Incident Created On	Oct 29, 2021 7:48 AM UTC
Last Updated	Oct 29, 2021 7:51 AM UTC
Last Response	Quarantined
Quarantine Status	New
User	jayson_ong@okta.skyhighdemo.cloud

Owner: Unassigned

Incident Response: Select Response

Incident Status: New

Resolution Action: Select Resolution

MITRE

Content

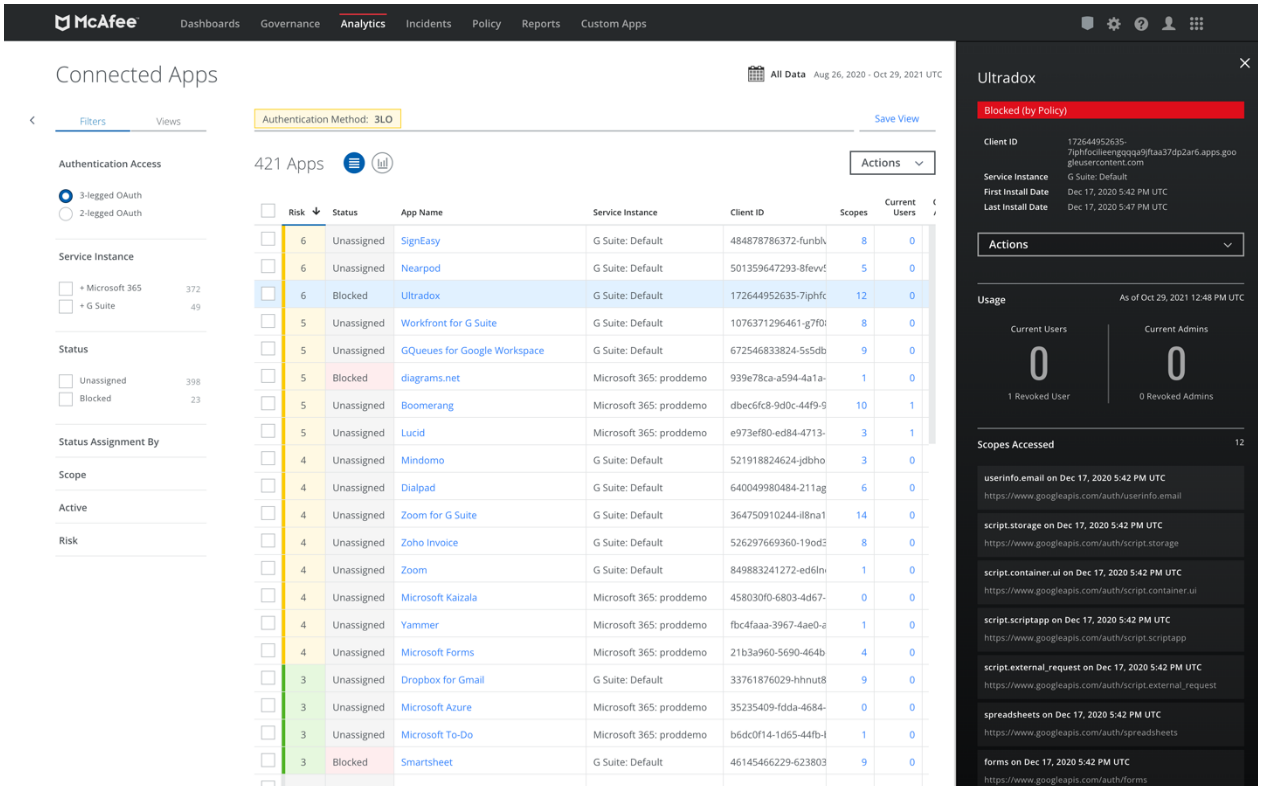
Item Name	20211029_Jayson_CCN_15_records.xls
Item Type	File
Path	/personal/jayson_ong_okta_skyhighdemo_cloud/Documents
Size	30 kiB
Folder ID	/personal/jayson_ong_okta_skyhighdemo_cloud:/personal/jayson_ong_okta_skyhighdemo_cloud/Documents
Item Created On	Oct 29, 2021 7:48 AM UTC

14 Content Matches Found

.. XXXXWORD 30809 RAUL PASHAL "XXXXXXXXXXXX5019" XXXXX9820 pashal_6358824@hom...
.. EUtDkPkNj 30812 JAMES HINTZ

Exfiltration via Connected Apps:

MVISION UCE incident manager discovers risky unsanctioned third-party applications associated with Microsoft 365, Google Drive and other cloud applications and connected to the corporate environment via OAuth. MVISION UCE provides a workflow to manually remediate, audit, allow or block Connected Apps access to users' data, notify users via email of an app's status, and revoke access as needed.



Connected Apps

All Data Aug 26, 2020 - Oct 29, 2021 UTC

Authentication Method: 3LO

Authentication Access

● 3-legged OAuth
○ 2-legged OAuth

Service Instance

□	+ Microsoft 365	372
□	+ G Suite	49

Status

□	Unassigned	398
□	Blocked	23

Status Assignment By

Scope

Active

Risk

421 Apps

□	Risk ↓	Status	App Name	Service Instance	Client ID	Scopes	Current Users
□	6	Unassigned	SignEasy	G Suite: Default	484878786372-funbl	8	0
□	6	Unassigned	Nearpod	G Suite: Default	501359647293-8fevv	5	0
□	6	Blocked	Ultradox	G Suite: Default	172644952635-7iphf	12	0
□	5	Unassigned	Workfront for G Suite	G Suite: Default	1076371296461-g7f0	8	0
□	5	Unassigned	GQueues for Google Workspace	G Suite: Default	672546833824-5s5db	9	0
□	5	Blocked	diagrams.net	Microsoft 365: proddemo	939e78ca-a594-4a1a-	1	0
□	5	Unassigned	Boomerang	Microsoft 365: proddemo	dbec6fc8-9d0c-44f9-	10	1
□	5	Unassigned	Lucid	Microsoft 365: proddemo	e973ef80-ed84-4713-	3	1
□	4	Unassigned	Mindomo	G Suite: Default	521918824624-jdbho	3	0
□	4	Unassigned	Dialpad	G Suite: Default	640049980484-211ag	6	0
□	4	Unassigned	Zoom for G Suite	G Suite: Default	364750910244-il8na1	14	0
□	4	Unassigned	Zoho Invoice	G Suite: Default	526297669360-19od	8	0
□	4	Unassigned	Zoom	G Suite: Default	849883241272-ed6ln	1	0
□	4	Unassigned	Microsoft Kaizala	Microsoft 365: proddemo	458030f0-6803-4d67-	0	0
□	4	Unassigned	Yammer	Microsoft 365: proddemo	fbc4faaa-3967-4ae0-	1	0
□	4	Unassigned	Microsoft Forms	Microsoft 365: proddemo	21b3a960-5690-464b	4	0
□	3	Unassigned	Dropbox for Gmail	G Suite: Default	33761876029-hhnut8	9	0
□	3	Unassigned	Microsoft Azure	Microsoft 365: proddemo	35235409-fdda-4684-	0	0
□	3	Unassigned	Microsoft To-Do	Microsoft 365: proddemo	b6dc0f14-1d65-44fb-	1	0
□	3	Blocked	Smartsheet	G Suite: Default	46145466229-623803	9	0

Ultradox

Blocked (by Policy)

Client ID	172644952635-7iphfocilieengqqqa9jftaa37dp2ar6.apps.googleusercontent.com
Service Instance	G Suite: Default
First Install Date	Dec 17, 2020 5:42 PM UTC
Last Install Date	Dec 17, 2020 5:47 PM UTC

Usage

As of Oct 29, 2021 12:48 PM UTC

Current Users	Current Admins
0	0
1 Revoked User	0 Revoked Admins

Scopes Accessed 12

userinfo.email on Dec 17, 2020 5:42 PM UTC
https://www.googleapis.com/auth/userinfo.email

script.storage on Dec 17, 2020 5:42 PM UTC
https://www.googleapis.com/auth/script.storage

script.container.ui on Dec 17, 2020 5:42 PM UTC
https://www.googleapis.com/auth/script.container.ui

script.scriptapp on Dec 17, 2020 5:42 PM UTC
https://www.googleapis.com/auth/script.scriptapp

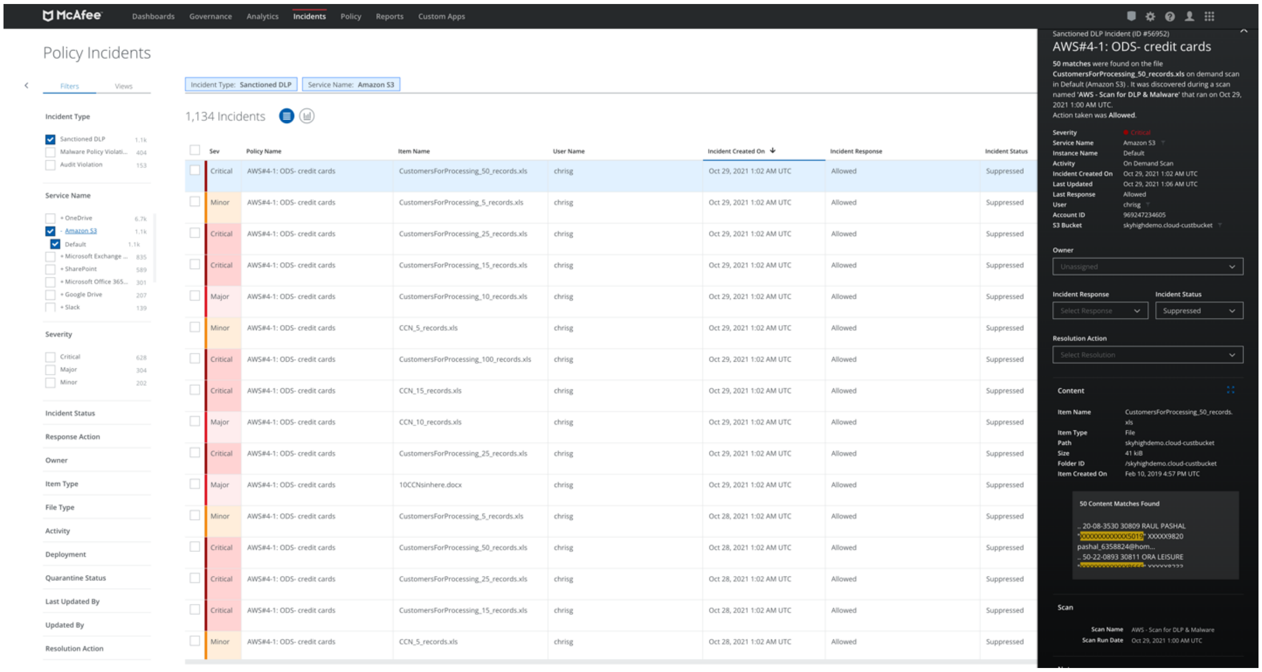
script.external_request on Dec 17, 2020 5:42 PM UTC
https://www.googleapis.com/auth/script.external_request

spreadsheets on Dec 17, 2020 5:42 PM UTC
https://www.googleapis.com/auth/spreadsheets

forms on Dec 17, 2020 5:42 PM UTC
https://www.googleapis.com/auth/forms

Public Cloud Storage Data Exfiltration:

MVISION UCE offers organizations visibility into critical or sensitive data stored in Amazon Simple Storage Service (S3), Microsoft Azure blob storage, and Google cloud storage buckets. MVISION UCE helps to assure proper protection of data used in all these cloud environments. MVISION UCE's content engine automatically classifies sensitive information, and then enforces controls to remove or quarantine sensitive data and prevent data exfiltration.



Policy Incidents

Incident Type

- ☑ Sanctioned DLP 1.1k
- □ Malware Policy Violati... 404
- □ Audit Violation 153

Service Name

- □ + OneDrive 6.7k
- ☑ - Amazon S3 1.1k
  - ☑ Default 1.1k
- □ + Microsoft Exchange ... 835
- □ + SharePoint 589
- □ + Microsoft Office 365... 301
- □ + Google Drive 207
- □ + Slack 139

Severity

- □ Critical 628
- □ Major 304
- □ Minor 202

Incident Status

Response Action

Owner

Item Type

File Type

Activity

Deployment

Quarantine Status

Last Updated By

Updated By

Resolution Action

Incident Type: Sanctioned DLP | Service Name: Amazon S3

1,134 Incidents

□	Sev	Policy Name	Item Name	User Name	Incident Created On	Incident Response	Incident Status
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_50_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Minor	AWS#4-1: ODS- credit cards	CustomersForProcessing_5_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_25_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_15_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Major	AWS#4-1: ODS- credit cards	CustomersForProcessing_10_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Minor	AWS#4-1: ODS- credit cards	CCN_5_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_100_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CCN_15_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Major	AWS#4-1: ODS- credit cards	CCN_10_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_25_records.xls	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Major	AWS#4-1: ODS- credit cards	10CCNsinhere.docx	chrisg	Oct 29, 2021 1:02 AM UTC	Allowed	Suppressed
□	Minor	AWS#4-1: ODS- credit cards	CustomersForProcessing_5_records.xls	chrisg	Oct 28, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_50_records.xls	chrisg	Oct 28, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_25_records.xls	chrisg	Oct 28, 2021 1:02 AM UTC	Allowed	Suppressed
□	Critical	AWS#4-1: ODS- credit cards	CustomersForProcessing_15_records.xls	chrisg	Oct 28, 2021 1:02 AM UTC	Allowed	Suppressed
□	Minor	AWS#4-1: ODS- credit cards	CCN_5_records.xls	chrisg	Oct 28, 2021 1:02 AM UTC	Allowed	Suppressed

Sanctioned DLP Incident (ID #56952)

AWS#4-1: ODS- credit cards

50 matches were found on the file **CustomersForProcessing_50_records.xls** on demand scan in Default (Amazon S3) . It was discovered during a scan named **'AWS - Scan for DLP & Malware'** that ran on Oct 29, 2021 1:00 AM UTC.
Action taken was **Allowed.**

Severity	● Critical
Service Name	Amazon S3
Instance Name	Default
Activity	On Demand Scan
Incident Created On	Oct 29, 2021 1:02 AM UTC
Last Updated	Oct 29, 2021 1:06 AM UTC
Last Response	Allowed
User	chrisg
Account ID	969247234605
S3 Bucket	skyhighdemo.cloud-custbucket

Owner: Unassigned

Incident Response: Select Response

Incident Status: Suppressed

Resolution Action: Select Resolution

Content

Item Name	CustomersForProcessing_50_records.xls
Item Type	File
Path	skyhighdemo.cloud-custbucket
Size	41 kiB
Folder ID	/skyhighdemo.cloud-custbucket
Item Created On	Feb 10, 2019 4:57 PM UTC

50 Content Matches Found

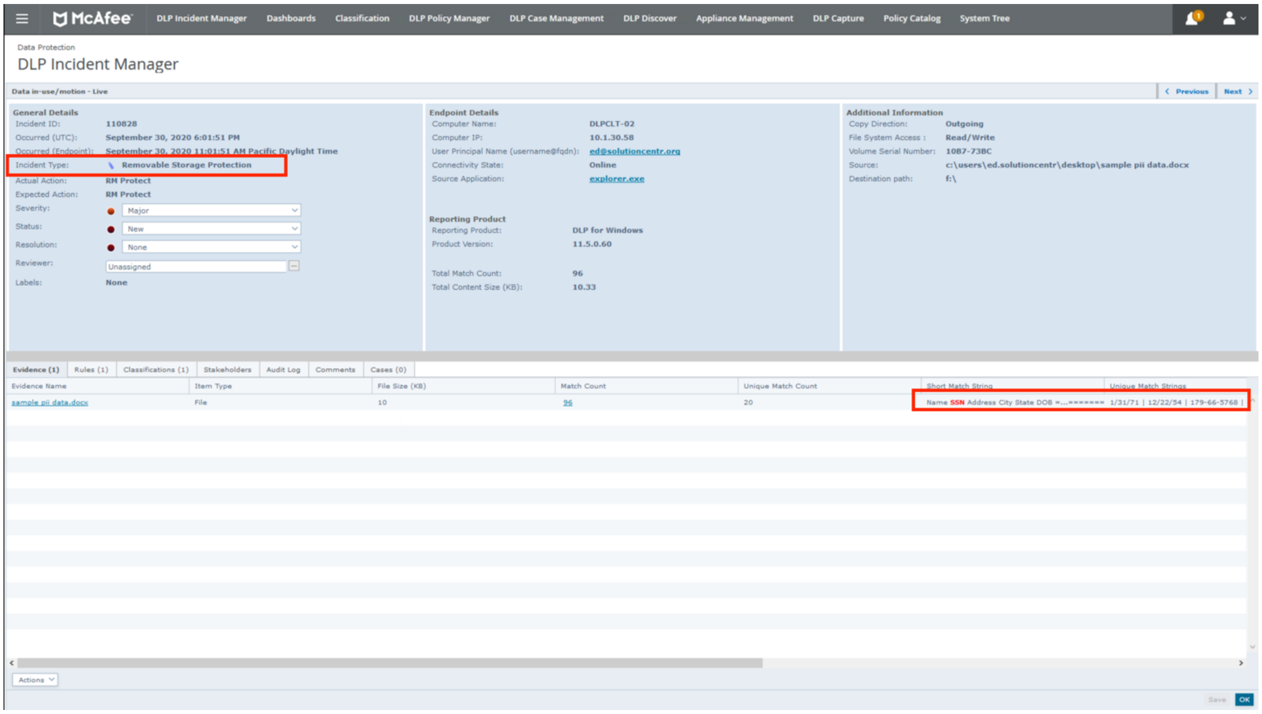
.. 20-08-3530 30809 RAUL PASHAL "XXXXXXXXXXXX5019" XXXXX9820 pashal_6358824@hom...
.. 50-22-0893 30811 ORA LEISURE

Scan

Scan Name	AWS - Scan for DLP & Malware
Scan Run Date	Oct 29, 2021 1:00 AM UTC

Exfiltration from endpoint devices:

McAfee DLP Endpoint provides protection for possible leaking channels, including removable storage devices, email, web, printing, clipboard, screen capture, file sharing, and more. McAfee DLP Endpoint is integrated with MVISION Unified Cloud Edge DLP so it's easy to extend on premise DLP policies to MVISION Unified Cloud Edge for data loss detection.



Data Protection

DLP Incident Manager

Data in-use/motion - Live

General Details

Incident ID: 110828
Occurred (UTC): September 30, 2020 6:01:51 PM
Occurred (Endpoint): September 30, 2020 11:01:51 AM Pacific Daylight Time
Incident Type: Removable Storage Protection
Actual Action: RM Protect
Expected Action: RM Protect
Severity: Major
Status: New
Resolution: None
Reviewer: Unassigned
Labels: None

Endpoint Details

Computer Name: DLPCLT-02
Computer IP: 10.1.30.58
User Principal Name (username@fqdn): ed@solutioncentr.org
Connectivity State: Online
Source Application: explorer.exe

Reporting Product

Reporting Product: DLP for Windows
Product Version: 11.5.0.60

Total Match Count: 96
Total Content Size (KB): 10.33

Additional Information

Copy Direction: Outgoing
File System Access : Read/Write
Volume Serial Number: 10B7-73BC
Source: c:\users\ed.solutioncentr\desktop\sample pii data.docx
Destination path: f:\

Evidence (1) | Rules (1) | Classifications (1) | Stakeholders | Audit Log | Comments | Cases (0)

Evidence Name	Item Type	File Size (KB)	Match Count	Unique Match Count	Short Match String	Unique Match Strings
sample pii data.docx	File	10	96	20	Name SSN Address City State DOB =...=======	1/31/71 | 12/22/54 | 179-66-5768 |

How to mitigate Cloud Native attacks?

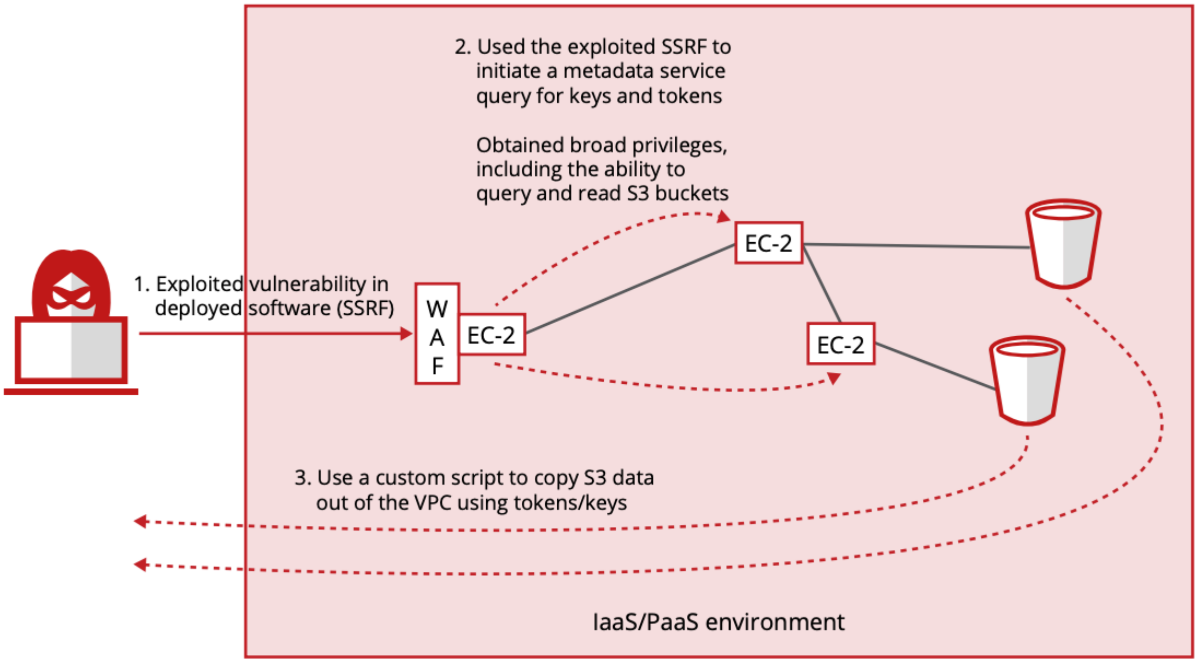
Land Expand Exfiltration

Infrastructure-as-a-Service (IaaS) is at a great risk for Cloud-Native Breaches, with 99% of misconfiguration incidents in public cloud environments going undetected, according to a **McAfee report**. Cloud-native breaches occur when an adversarial actor gains access to a cloud customer's resources, locates valuable data, and then exfiltrates that data. The steps in this attack chain might be as follows:

1. Land by gaining a foothold into the IaaS/PaaS environment.
   Leverage compromised/weak credentials to gain access as a legitimate user. Exploit a vulnerability, such as server-side request forgery (SSRF), in deployed software. Capitalize on misconfigurations of ingress/egress security groups.

2. Expand by finding ways to move beyond the landing node. Leverage privileges associated with a compromised node to access remote nodes. Probe for and exploit weakly protected applications or databases. Capitalize on weak network controls.

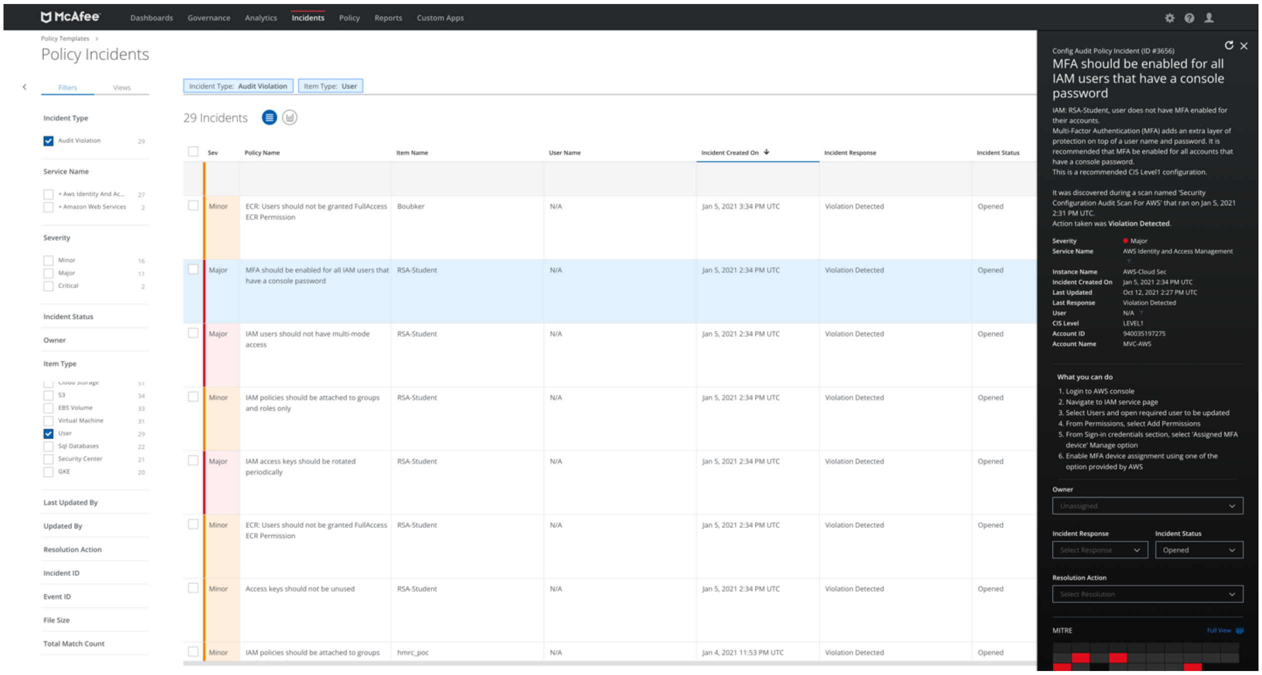
3. Exfiltrate data while staying under the radar. Copy data from the storage account to anonymous nodes on the internet. Create a storage gateway to gain access to the data from a remote location. Copy data from the storage accounts to a remote location outside the virtual private cloud (VPC).


2. Used the exploited SSRF to initiate a metadata service query for keys and tokens
Obtained broad privileges, including the ability to query and read S3 buckets
1. Exploited vulnerability in deployed software (SSRF)
W A F
EC-2
EC-2
EC-2
3. Use a custom script to copy S3 data out of the VPC using tokens/keys
IaaS/PaaS environment

How MVISION Unified Cloud Edge helps

MVISION CNAPP can help detect the landing phase whereby the attacker seeks to identify vulnerabilities and leverage weak user credentials. In real-time MVISION CNAPP detects and prioritizes misconfigurations across the entire cloud environment. MVISION CNAPP also leverages Center for Internet Security (CIS) benchmarks and many security best practices to help guard the customer environment against a data breach.

Many of these CIS benchmarks cover identity and access management (IAM). These may include, as an example, but not be limited to restricting the use of root credentials, the use groups for IAM policies, applying conditions to IAM policies, least privilege in IAM, the use of MFA for better security, strong passwords, and the use unique access keys. IAM access keys should be rotated periodically.



Policy Incidents

Incident Type: Audit Violation | Item Type: User

Incident Type
☑ Audit Violation 29

Service Name
□ + Aws Identity And Ac... 27
□ + Amazon Web Services 2

Severity
□ Minor 16
□ Major 11
□ Critical 2

Incident Status

Owner

Item Type
□ Cloud Storage 51
□ S3 34
□ EBS Volume 33
□ Virtual Machine 31
☑ User 29
□ Sql Databases 22
□ Security Center 21
□ GKE 20

Last Updated By

Updated By

Resolution Action

Incident ID

Event ID

File Size

Total Match Count

29 Incidents

Sev	Policy Name	Item Name	User Name	Incident Created On	Incident Response	Incident Status
Minor	ECR: Users should not be granted FullAccess ECR Permission	Boubker	N/A	Jan 5, 2021 3:34 PM UTC	Violation Detected	Opened
Major	MFA should be enabled for all IAM users that have a console password	RSA-Student	N/A	Jan 5, 2021 2:34 PM UTC	Violation Detected	Opened
Major	IAM users should not have multi-mode access	RSA-Student	N/A	Jan 5, 2021 2:34 PM UTC	Violation Detected	Opened
Minor	IAM policies should be attached to groups and roles only	RSA-Student	N/A	Jan 5, 2021 2:34 PM UTC	Violation Detected	Opened
Major	IAM access keys should be rotated periodically	RSA-Student	N/A	Jan 5, 2021 2:34 PM UTC	Violation Detected	Opened
Minor	ECR: Users should not be granted FullAccess ECR Permission	RSA-Student	N/A	Jan 5, 2021 2:34 PM UTC	Violation Detected	Opened
Minor	Access keys should not be unused	RSA-Student	N/A	Jan 5, 2021 2:34 PM UTC	Violation Detected	Opened
Minor	IAM policies should be attached to groups	hmrc_poc	N/A	Jan 4, 2021 11:53 PM UTC	Violation Detected	Opened

Config Audit Policy Incident (ID #3656)

MFA should be enabled for all IAM users that have a console password

IAM: RSA-Student, user does not have MFA enabled for their accounts.
Multi-Factor Authentication (MFA) adds an extra layer of protection on top of a user name and password. It is recommended that MFA be enabled for all accounts that have a console password.
This is a recommended CIS Level1 configuration.

It was discovered during a scan named 'Security Configuration Audit Scan For AWS' that ran on Jan 5, 2021 2:31 PM UTC.
Action taken was **Violation Detected**.

Severity	● Major
Service Name	AWS Identity and Access Management
Instance Name	AWS-Cloud Sec
Incident Created On	Jan 5, 2021 2:34 PM UTC
Last Updated	Oct 12, 2021 2:27 PM UTC
Last Response	Violation Detected
User	N/A
CIS Level	LEVEL1
Account ID	940035197275
Account Name	MVC-AWS

What you can do

1. Login to AWS console
2. Navigate to IAM service page
3. Select Users and open required user to be updated
4. From Permissions, select Add Permissions
5. From Sign-in credentials section, select 'Assigned MFA device' Manage option
6. Enable MFA device assignment using one of the option provided by AWS

Owner: Unassigned

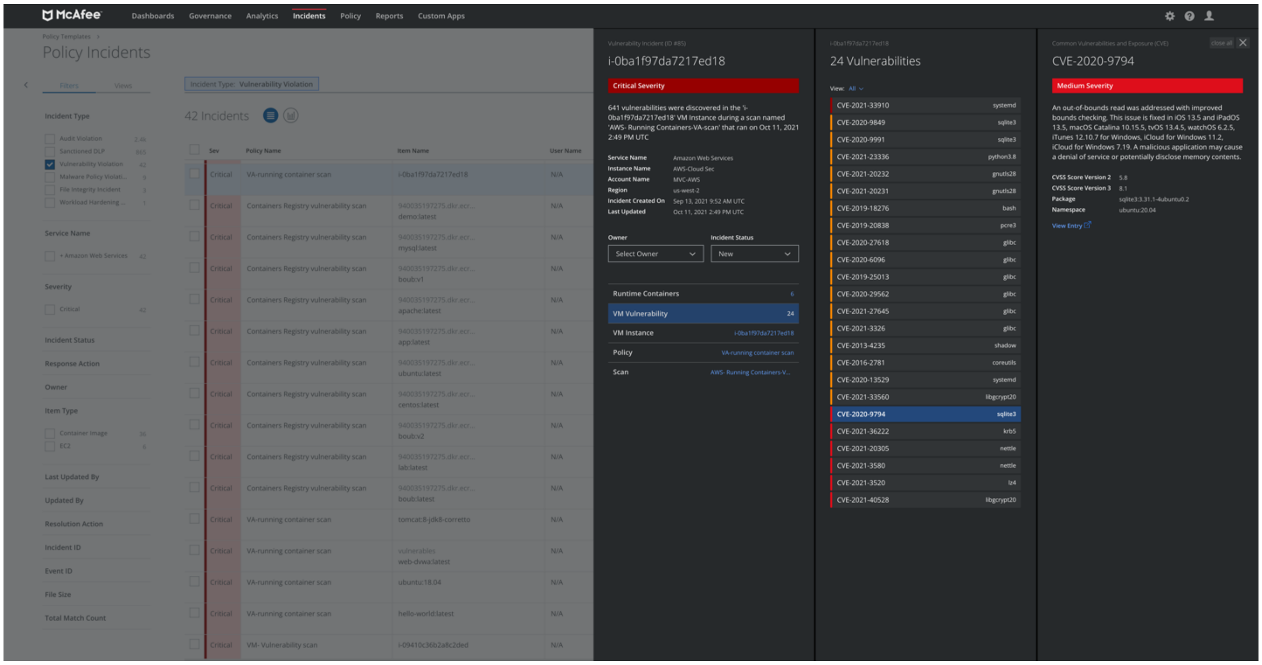
Incident Response: Select Response

Incident Status: Opened

Resolution Action: Select Resolution

MVISION CNAPP ensure that applications are protected from attacks and exploits throughout the full build-ship-run lifecycle by:

- Vulnerability scanning during the application build process in CI/CD.
- Vulnerability scanning in the container registry, the runtime container, and the underline operating system where the container is running.
- Preventing rogue container process to run by applying process allow listing.



Policy Incidents

Incident Type: Vulnerability Violation

42 Incidents

Incident Type

- □ Audit Violation 2.4k
- □ Sanctioned DLP 865
- ☑ Vulnerability Violation 42
- □ Malware Policy Violati... 9
- □ File Integrity Incident 3
- □ Workload Hardening ... 1

Service Name

- □ + Amazon Web Services 42

Severity

- □ Critical 42

Incident Status

Response Action

Owner

Item Type

- □ Container Image 36
- □ EC2 6

Last Updated By

Updated By

Resolution Action

Incident ID

Event ID

File Size

Total Match Count

□	Sev	Policy Name	Item Name	User Name
□	Critical	VA-running container scan	i-0ba1f97da7217ed18	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... demo:latest	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... mysql:latest	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... boub:v1	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... apache:latest	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... app:latest	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... ubuntu:latest	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... centos:latest	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... boub:v2	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... lab:latest	N/A
□	Critical	Containers Registry vulnerability scan	940035197275.dkr.ecr... boub:latest	N/A
□	Critical	VA-running container scan	tomcat:8-jdk8-corretto	N/A
□	Critical	VA-running container scan	vulnerables web-dvwa:latest	N/A
□	Critical	VA-running container scan	ubuntu:18.04	N/A
□	Critical	VA-running container scan	hello-world:latest	N/A
□	Critical	VM- Vulnerability scan	i-09410c36b2a8c2ded	N/A

Vulnerability Incident (ID #85)

i-0ba1f97da7217ed18

Critical Severity

641 vulnerabilities were discovered in the 'i-0ba1f97da7217ed18' VM Instance during a scan named 'AWS- Running Containers-VA-scan' that ran on Oct 11, 2021 2:49 PM UTC

Service Name	Amazon Web Services
Instance Name	AWS-Cloud Sec
Account Name	MVC-AWS
Region	us-west-2
Incident Created On	Sep 13, 2021 9:52 AM UTC
Last Updated	Oct 11, 2021 2:49 PM UTC

Owner: Select Owner
Incident Status: New

Runtime Containers	6
VM Vulnerability	24
VM Instance	i-0ba1f97da7217ed18
Policy	VA-running container scan
Scan	AWS- Running Containers-V...

i-0ba1f97da7217ed18

24 Vulnerabilities

View: All

CVE-2021-33910	systemd
CVE-2020-9849	sqlite3
CVE-2020-9991	sqlite3
CVE-2021-23336	python3.8
CVE-2021-20232	gnutls28
CVE-2021-20231	gnutls28
CVE-2019-18276	bash
CVE-2019-20838	pcre3
CVE-2020-27618	glibc
CVE-2020-6096	glibc
CVE-2019-25013	glibc
CVE-2020-29562	glibc
CVE-2021-27645	glibc
CVE-2021-3326	glibc
CVE-2013-4235	shadow
CVE-2016-2781	coreutils
CVE-2020-13529	systemd
CVE-2021-33560	libgcrypt20
CVE-2020-9794	sqlite3
CVE-2021-36222	krb5
CVE-2021-20305	nettle
CVE-2021-3580	nettle
CVE-2021-3520	lz4
CVE-2021-40528	libgcrypt20

Common Vulnerabilities and Exposure (CVE)

CVE-2020-9794

Medium Severity

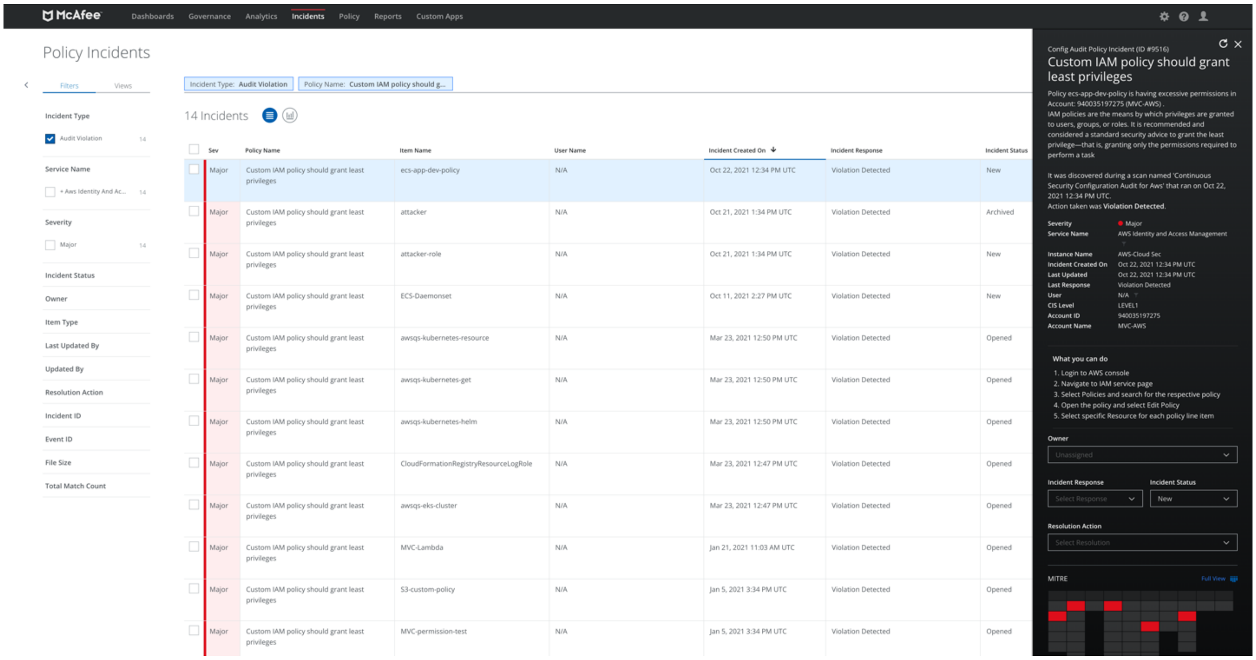
An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A malicious application may cause a denial of service or potentially disclose memory contents.

CVSS Score Version 2	5.8
CVSS Score Version 3	8.1
Package	sqlite3:3.31.1-4ubuntu0.2
Namespace	ubuntu:20.04

View Entry

Once a cyberattacker has completed a successful landing, they will expand and discover other IaaS resources by leveraging the exploit in the compromised node to query a metadata service to obtain sensitive keys and tokens. This allowed the adversary to obtain broad privileges, including the ability to query and read storage objects.

It is a best practice to protect access to cloud infrastructure by ensuring that developers and other users have only the permissions they need to do their jobs—and no more. Lock root account credentials that can provide an attacker access to all resources, and deprovision inactive accounts. MVISION CNAPP analyses activity within IaaS platforms and custom applications. Based on User Entity Behaviour analytics powered by machine learning, MVISION CNAPP identifies anomalous usage indicative of compromised accounts, insider threat, and privileged user threat.



Policy Incidents

Incident Type: **Audit Violation** Policy Name: **Custom IAM policy should g...**

14 Incidents

Sev	Policy Name	Item Name	User Name	Incident Created On	Incident Response	Incident Status
Major	Custom IAM policy should grant least privileges	ecs-app-dev-policy	N/A	Oct 22, 2021 12:34 PM UTC	Violation Detected	New
Major	Custom IAM policy should grant least privileges	attacker	N/A	Oct 21, 2021 1:34 PM UTC	Violation Detected	Archived
Major	Custom IAM policy should grant least privileges	attacker-role	N/A	Oct 21, 2021 1:34 PM UTC	Violation Detected	New
Major	Custom IAM policy should grant least privileges	ECS-Daemonset	N/A	Oct 11, 2021 2:27 PM UTC	Violation Detected	New
Major	Custom IAM policy should grant least privileges	awsqs-kubernetes-resource	N/A	Mar 23, 2021 12:50 PM UTC	Violation Detected	Opened
Major	Custom IAM policy should grant least privileges	awsqs-kubernetes-get	N/A	Mar 23, 2021 12:50 PM UTC	Violation Detected	Opened
Major	Custom IAM policy should grant least privileges	awsqs-kubernetes-helm	N/A	Mar 23, 2021 12:50 PM UTC	Violation Detected	Opened
Major	Custom IAM policy should grant least privileges	CloudFormationRegistryResourceLogRole	N/A	Mar 23, 2021 12:47 PM UTC	Violation Detected	Opened
Major	Custom IAM policy should grant least privileges	awsqs-eks-cluster	N/A	Mar 23, 2021 12:47 PM UTC	Violation Detected	Opened
Major	Custom IAM policy should grant least privileges	MVC-Lambda	N/A	Jan 21, 2021 11:03 AM UTC	Violation Detected	Opened
Major	Custom IAM policy should grant least privileges	S3-custom-policy	N/A	Jan 5, 2021 3:34 PM UTC	Violation Detected	Opened
Major	Custom IAM policy should grant least privileges	MVC-permission-test	N/A	Jan 5, 2021 3:34 PM UTC	Violation Detected	Opened

Config Audit Policy Incident (ID #9516)

Custom IAM policy should grant least privileges

Policy ecs-app-dev-policy is having excessive permissions in Account: 940035197275 (MVC-AWS) .
IAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended and considered a standard security advice to grant the least privilege—that is, granting only the permissions required to perform a task

It was discovered during a scan named 'Continuous Security Configuration Audit for Aws' that ran on Oct 22, 2021 12:34 PM UTC.
Action taken was **Violation Detected**.

Severity	● Major
Service Name	AWS Identity and Access Management
Instance Name	AWS-Cloud Sec
Incident Created On	Oct 22, 2021 12:34 PM UTC
Last Updated	Oct 22, 2021 12:34 PM UTC
Last Response	Violation Detected
User	N/A
CIS Level	LEVEL1
Account ID	940035197275
Account Name	MVC-AWS

What you can do

1. Login to AWS console
2. Navigate to IAM service page
3. Select Policies and search for the respective policy
4. Open the policy and select Edit Policy
5. Select specific Resource for each policy line item

Owner: Unassigned

Incident Response: Select Response

Incident Status: New

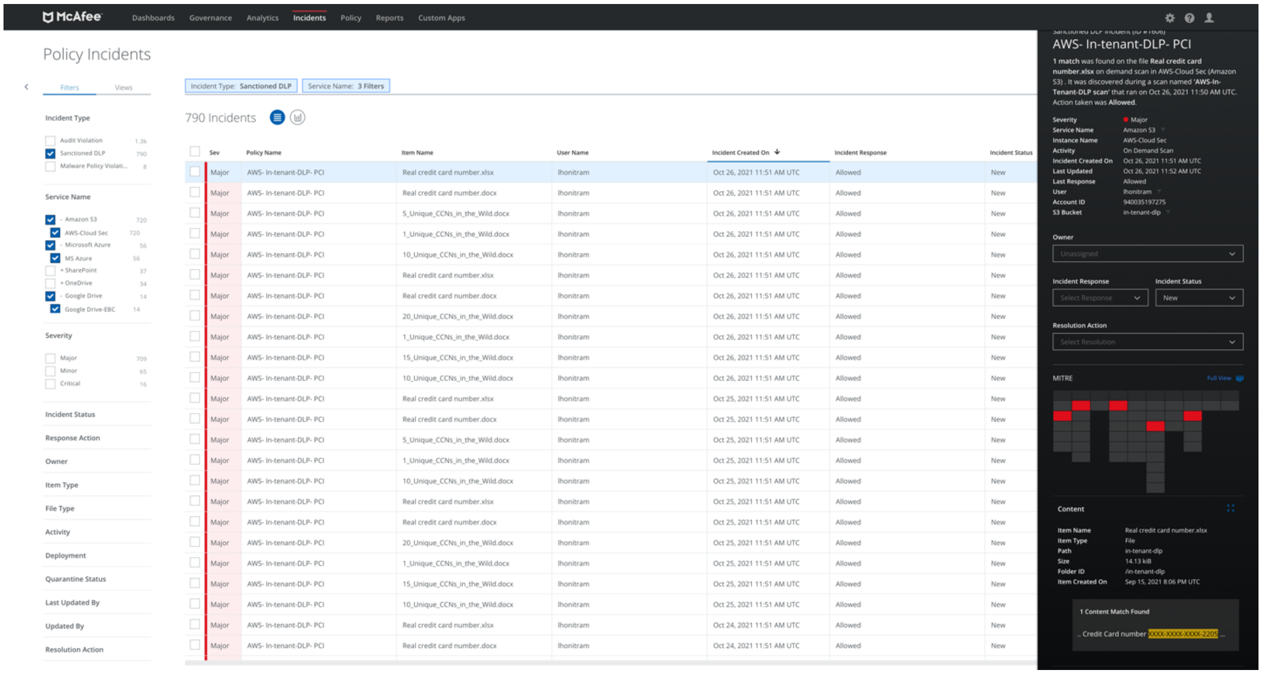
Resolution Action: Select Resolution

MVISION CNAPP can prevent unauthorized regulated data or malware from being stored in AWS, Azure and GCP storage services. DLP and malware scanning can be applied in three different ways:

1. First, as a response to a configuration audit incident. Highly vulnerable categories, DLP and/or malware scan can be a configured as a response action to the policy for trigger.

2. Near real-time (NRT) will applies to changes in the data set and evaluates the policies in near real time.

3. On-demand scan applies to pre-existing data and executes on a scheduled interval.



Policy Incidents

Incident Type: Sanctioned DLP | Service Name: 3 Filters

790 Incidents

Incident Type

- ☐ Audit Violation 1.3k
- ☑ Sanctioned DLP 790
- ☐ Malware Policy Violati... 8

Service Name

- ☑ - Amazon S3 720
  - ☑ AWS-Cloud Sec 720
- ☑ - Microsoft Azure 56
  - ☑ MS Azure 56
- ☐ + SharePoint 37
- ☐ + OneDrive 34
- ☑ - Google Drive 14
  - ☑ Google Drive-EBC 14

Severity

- ☐ Major 709
- ☐ Minor 65
- ☐ Critical 16

Incident Status

Response Action

Owner

Item Type

File Type

Activity

Deployment

Quarantine Status

Last Updated By

Updated By

Resolution Action

☐	Sev	Policy Name	Item Name	User Name	Incident Created On	Incident Response	Incident Status
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.xlsx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.docx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	5_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	1_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	10_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.xlsx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.docx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	20_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	1_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	15_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	10_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 26, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.xlsx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.docx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	5_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	1_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	10_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.xlsx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.docx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	20_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	1_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	15_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	10_Unique_CCNs_in_the_Wild.docx	lhonitram	Oct 25, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.xlsx	lhonitram	Oct 24, 2021 11:51 AM UTC	Allowed	New
☐	Major	AWS- In-tenant-DLP- PCI	Real credit card number.docx	lhonitram	Oct 24, 2021 11:51 AM UTC	Allowed	New

Sanctioned DLP Incident (ID #1606)

AWS- In-tenant-DLP- PCI

1 match was found on the file **Real credit card number.xlsx** on demand scan in AWS-Cloud Sec (Amazon S3) . It was discovered during a scan named **'AWS-In-Tenant-DLP scan'** that ran on Oct 26, 2021 11:50 AM UTC. Action taken was **Allowed.**

Severity	● Major
Service Name	Amazon S3
Instance Name	AWS-Cloud Sec
Activity	On Demand Scan
Incident Created On	Oct 26, 2021 11:51 AM UTC
Last Updated	Oct 26, 2021 11:52 AM UTC
Last Response	Allowed
User	lhonitram
Account ID	940035197275
S3 Bucket	in-tenant-dlp

Owner: Unassigned

Incident Response: Select Response

Incident Status: New

Resolution Action: Select Resolution

Content

Item Name	Real credit card number.xlsx
Item Type	File
Path	in-tenant-dlp
Size	14.13 kiB
Folder ID	/in-tenant-dlp
Item Created On	Sep 15, 2021 8:06 PM UTC

1 Content Match Found

.. Credit Card number XXXX-XXXX-XXXX-2205 ...

Key Takeaways

MVISION Unified Cloud Edge is unified cloud architecture that deliver data and threat protection across SaaS, IaaS and PaaS.

MVISION UCE delivers data and threat protection to any location so you can enable fast and secure direct-to-internet access for your distributed workforce. This results in a transformation to a cloud-delivered Security Service Edge (SSE) that converges connectivity and security to reduce cost and complexity while increasing the speed and agility of your workforce.

MVISION CNAPP defend against cloud threats and vulnerabilities by combining granular application and data context with CSPM and CWPP protections. Cloud security posture management provides broad assessment of vulnerabilities and security posture across your multi-cloud environment (AWS, Azure and GCP), while cloud workload protection goes deep to secure your VMs, containers, and serverless functions.

To learn more please contact the McAfee team **here** or refer to our website on MVISION Unified Cloud Edge **here**.