Next-Generation Cloud Access Security Broker (CASB)

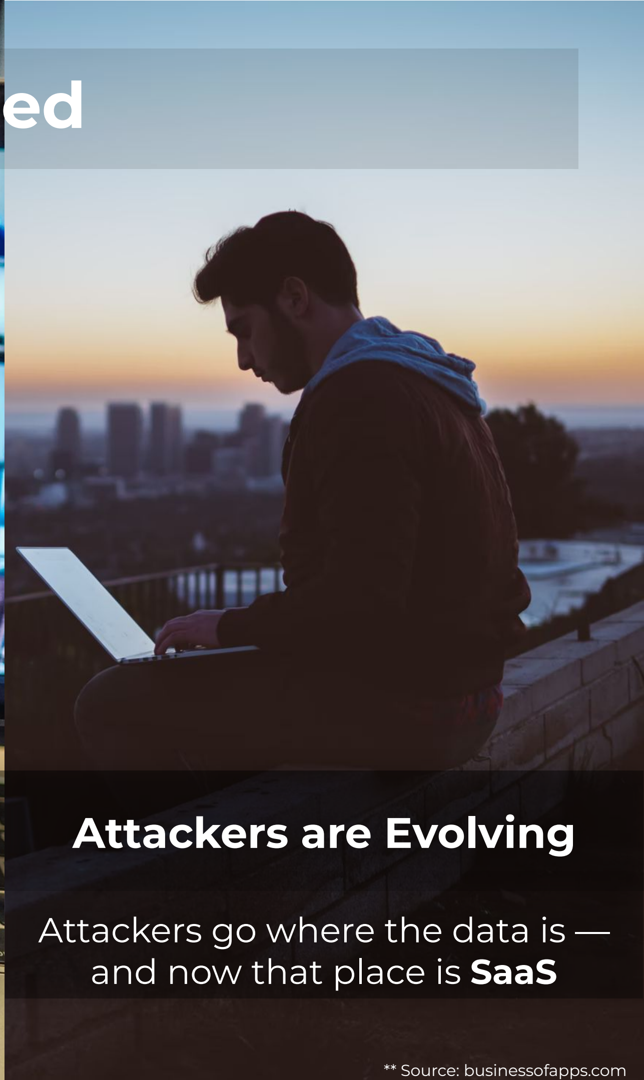
The World has Changed

SaaS Usage is Exploding

The typical enterprise now has over **1000** SaaS apps in use

Data is Changing

Sensitive data comes in **all forms** and is shared in **real-time**



Attackers are Evolving

Attackers go where the data is — and now that place is **SaaS**

** Source: businessofapps.com

These changes are creating new security challenges

Growing complexity of SaaS introduces new risks

Unmanaged **shadow IT apps** put users and data at risk

Dangerous misconfigurations create vulnerabilities within sanctioned SaaS apps

[Evidence]

Data is becoming harder to identify and secure

Sensitive data now shared using **real-time collaboration apps**

Corporate data increasingly found in **unstructured data**, not just files & databases

[Evidence]

SaaS is used to attack users and steal data

SaaS is used to **compromise users** & **steal credentials**

Compromised users and **malicious insiders** directly access SaaS from **anywhere**

[Evidence]

First-gen CASB is failing to solve these problems

App policies built around compliance, not security

App compliance attributes used to estimate risk & control access

New posture controls limited to compliance benchmarks

Outdated data protection as a compliance control

Legacy DLP based on compliance data patterns & profiles

Built for files & databases — can't understand chats, code snippets, other IP

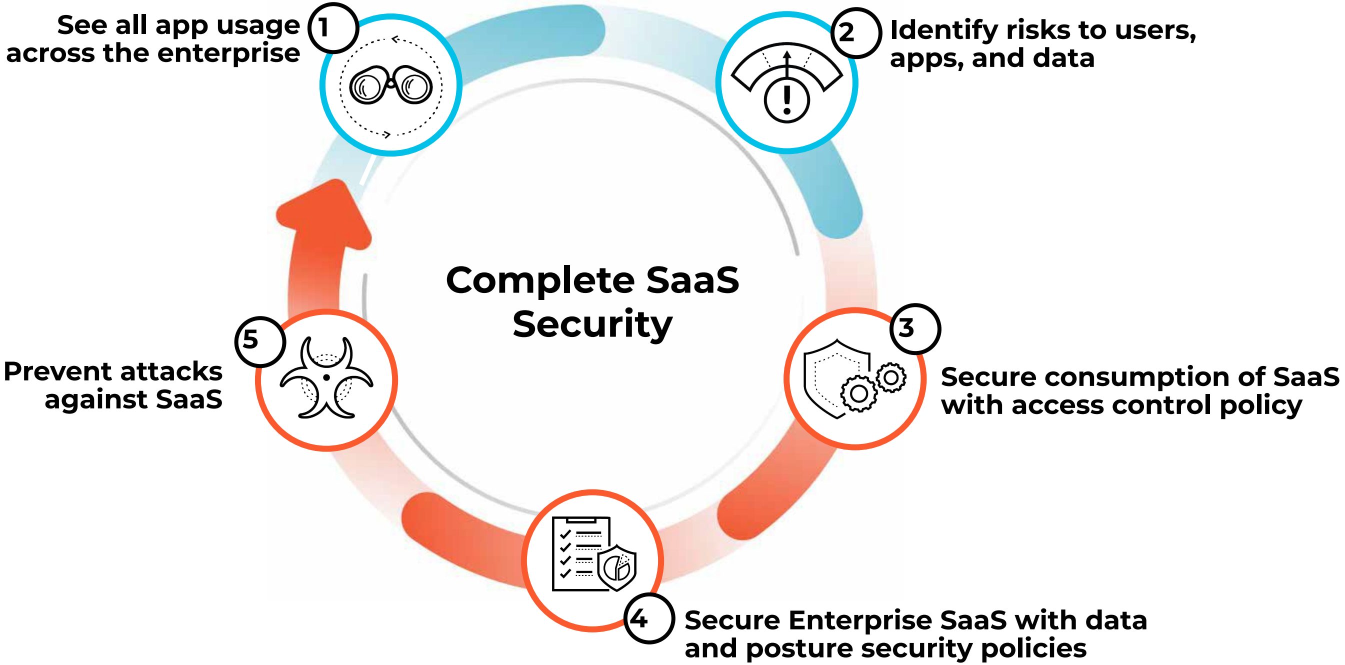
Threat protection that checks the box

Commodity antivirus and sandboxes can't detect today's evasive malware

Weak network security services can't stop the complete attack kill chain

CASB was **conceived** and **built** as a **compliance tool.**
It largely **remains** a **compliance tool.**

The right approach to securing SaaS


1
See all app usage across the enterprise
2
Identify risks to users, apps, and data
Complete SaaS Security
3
Secure consumption of SaaS with access control policy
4
Secure Enterprise SaaS with data and posture security policies
5
Prevent attacks against SaaS

Introducing Palo Alto Networks Next-Generation CASB

The industry's most complete, security-first CASB

Complete visibility and security for all apps

See and secure all SaaS applications in use

Real-time integrations with modern collaboration apps

Posture Security prevents dangerous misconfigurations

Data security for the modern enterprise

Discovery of all sensitive data, not just compliance controlled data

Advanced data detection in structured and unstructured data

User-led remediation and education

Protection from advanced threats

Integrated with WildFire for best-in-class antimalware

Detection of compromised accounts and insider threats

Natively integrated with SASE security stack

Complete visibility and security for all apps

Comprehensive access control for all SaaS

- Automatically discover, risk profile & control user actions on over **40k+** SaaS apps
- ML-based Application Cloud Engine (ACE) automatically discovers and catalogs new apps for rapid identification and control of apps as they emerge

Industry-leading API integrations with Enterprise SaaS apps

- Deep data protection and user monitoring for over **27+** sanctioned apps
- Near real-time connectors with modern collaboration apps provide immediate identification and remediation of data incidents

NEW

Posture Security prevents dangerous misconfigurations that put data at risk

- Comprehensive app coverage with automated benchmarking against security best practices and compliance frameworks
- Prevention-first approach with single-click remediation and drift prevention to stop problems before they occur

Data security for the modern enterprise

NEW

Advanced classification for all forms of sensitive data

- Comprehensive detectors, including EDM, OCR, ML classifiers, 1000s of built-in patterns
- Natural language processing (NLP) contextually understands chat and other unstructured data to find hard-to-detect secrets such as passwords and API keys

NEW

User-led remediation & data security education

- Proactive education for end-users during a data security violation
- End-users empowered to immediately remediate incidents themselves, reducing workload on the SOC

Consistent data security policy, across the enterprise

- Single, cloud-based DLP engine natively integrated with NG-CASB, NGFW, Prisma Access, and Prisma Cloud for enterprise-wide consistency

Industry-leading protection from advanced threats

Fully integrated with WildFire for best-in-class malware protection

- Advanced cloud-based detection & analysis of known and unknown malware
- Detects evasive malware hidden within sanctioned SaaS at-rest, and malware in-motion delivered from any SaaS app

NEW

Detection of compromised accounts and malicious insider activity

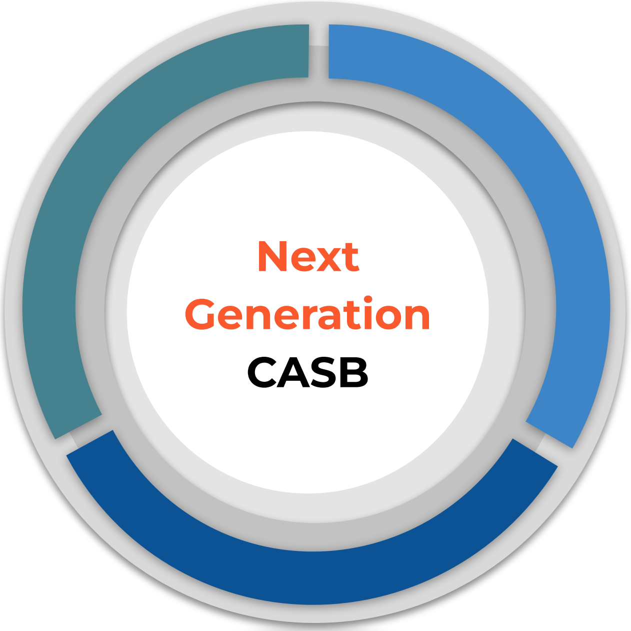
- New behavioral analytics detects high-risk and suspicious activity that can identify insider threats and compromised credentials or endpoints
- Comprehensive user activity auditing supports rapid investigation and remediation workflows

Natively integrated with the industry’s most advanced SASE security stack

- Advanced intrusion prevention, web security, and DNS security stop attackers and malware from successfully establishing footholds and exfiltrating data

Palo Alto Networks Next-Generation CASB

The industry's most complete, security-first CASB



Complete visibility and security for all apps

Comprehensive coverage over broadest app catalog (40k+ apps)

Industry-leading API integrations (27+ apps)

Posture security for over 20 apps with automated remediation

Data security for the modern enterprise

Advanced classification w/ EDM, OCR, and Deep Learning

User-led remediation & education

Consistent data security across the enterprise

Industry-leading protection from advanced threats

Best-in-class malware protection with WildFire

Suspicious User Activity Detection

Native integration with industry’s most advanced security stack

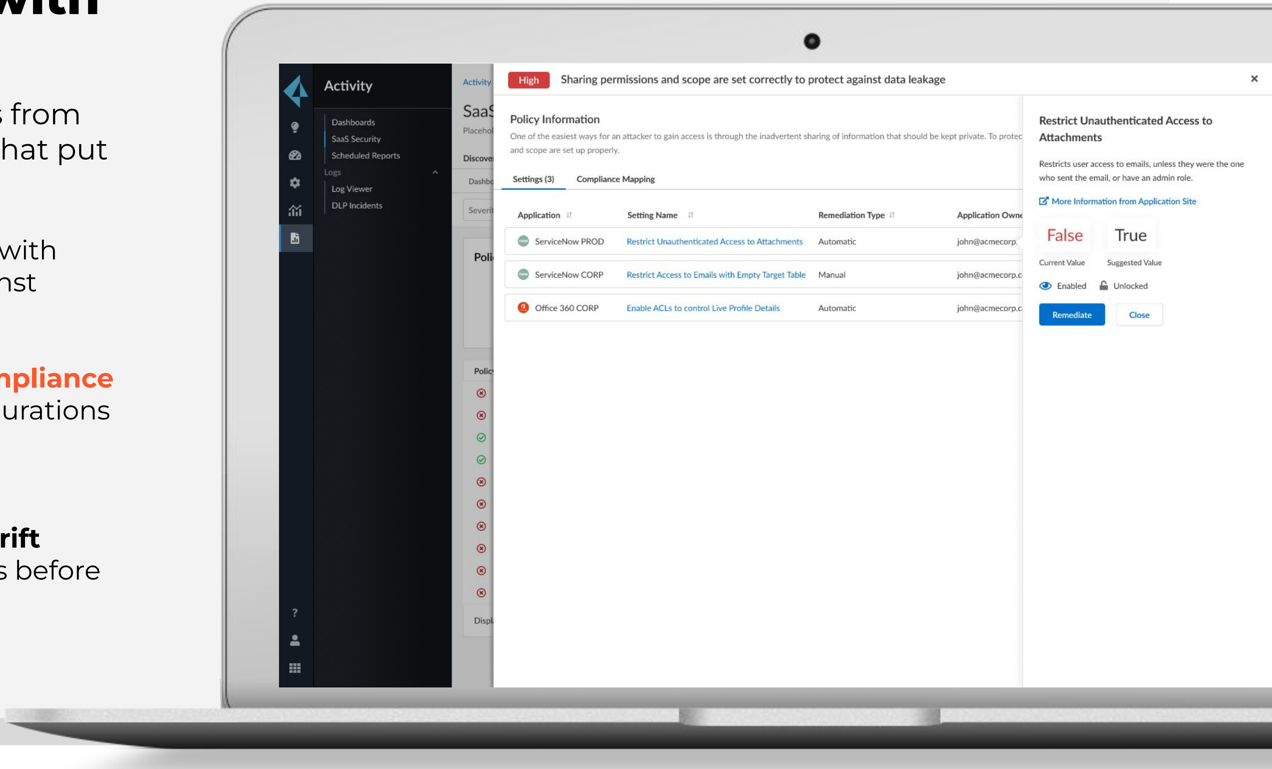
What’s new in NG-CASB

- Posture Security
- Data security for collaboration
- Suspicious User Activity Detection

Secure your apps with Posture Security

Protect your essential SaaS apps from **dangerous misconfigurations** that put users and data at risk.

- **Comprehensive app coverage** with automated benchmarking against security best practices
- **Security that goes beyond compliance** with best practices for **all** configurations that impact app security
- **Prevention-first approach** with **single-click remediation** and **drift prevention** to prevent problems before they occur



High Sharing permissions and scope are set correctly to protect against data leakage

Policy Information

One of the easiest ways for an attacker to gain access is through the inadvertent sharing of information that should be kept private. To protec
and scope are set up properly.

Application	Setting Name	Remediation Type	Application Owne
ServiceNow PROD	Restrict Unauthenticated Access to Attachments	Automatic	john@acmecorp.
ServiceNow CORP	Restrict Access to Emails with Empty Target Table	Manual	john@acmecorp.c
Office 360 CORP	Enable ACLs to control Live Profile Details	Automatic	john@acmecorp.c

Restrict Unauthenticated Access to Attachments

Restricts user access to emails, unless they were the one who sent the email, or have an admin role.

More Information from Application Site

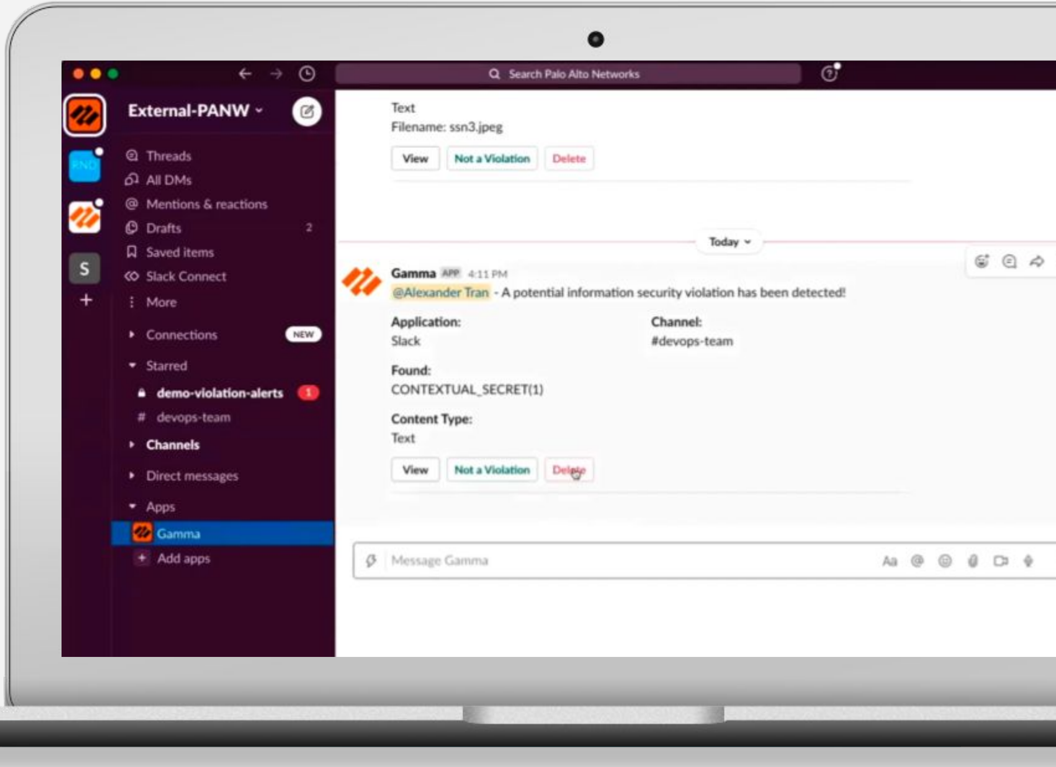
Current Value: False
Suggested Value: True

Enabled
Unlocked

Data security for modern collaboration

Prevent exposure of **sensitive data** commonly shared between employees within real-time collaboration apps.

- Natural language processing (NLP) finds **hard-to-detect secrets** such as passwords and API keys in unstructured chat data
- **Proactively educate end-users** about a data security violation they caused as it happens in real-time
- Enable end users to immediately **remediate incidents themselves**, reducing workload on the SOC



Text
Filename: ssn3.jpeg

Gamma APP 4:11 PM
@Alexander Tran - A potential information security violation has been detected!

Application:
Slack

Channel:
#devops-team

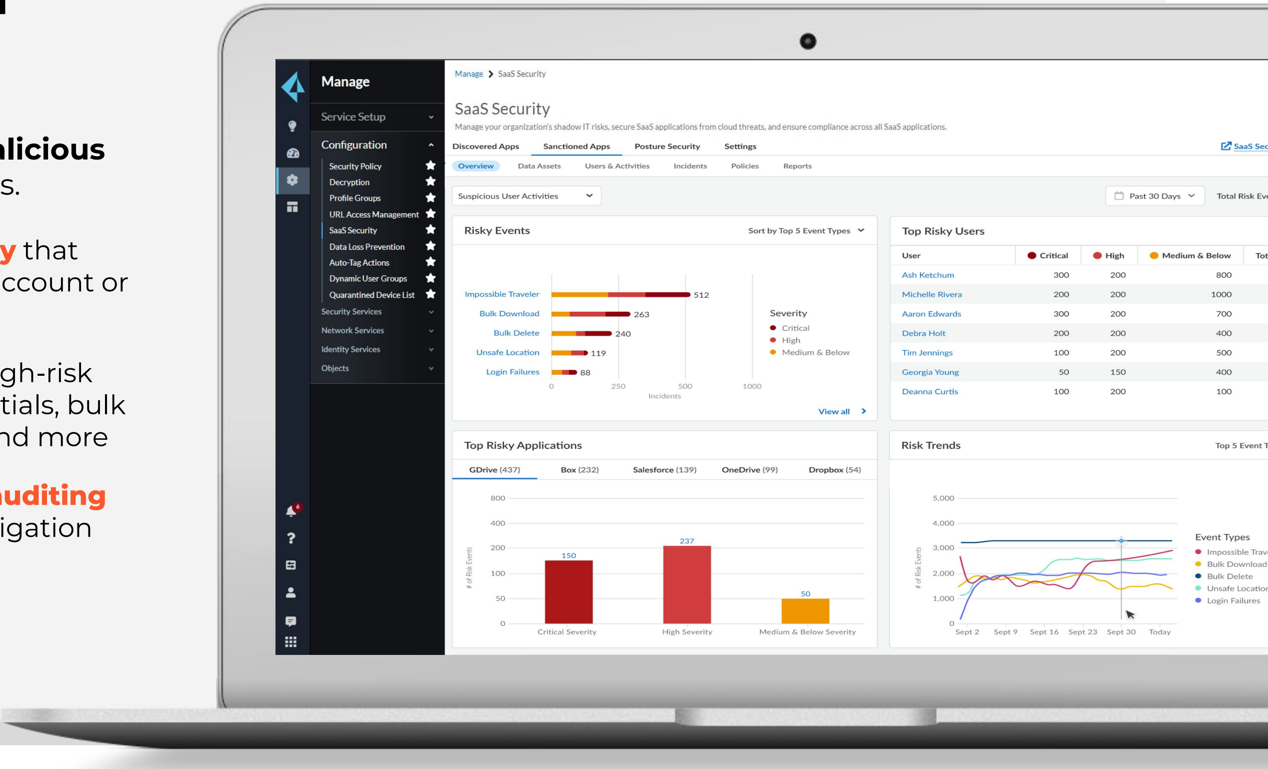
Found:
CONTEXTUAL_SECRET(1)

Content Type:
Text

Stop attackers and malicious insiders

Detect and stop activity from **compromised accounts** and **malicious insiders** with behavioral analytics.

- Detects **suspicious user activity** that could indicate a compromised account or malicious insider
- **Behavioral analytics** identify high-risk activity including shared credentials, bulk data access, suspicious logins, and more
- **Comprehensive user activity auditing** enables quick and simple investigation and remediation workflows



SaaS Security

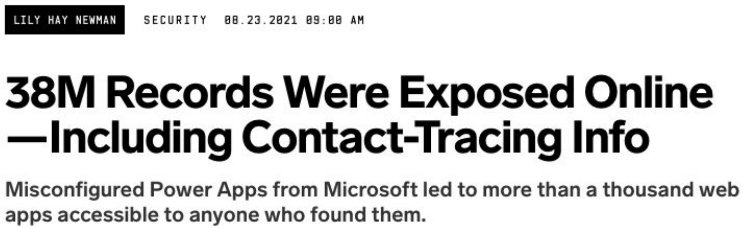
Manage your organization's shadow IT risks, secure SaaS applications from cloud threats, and ensure compliance across all SaaS applications.

Top Risky Users

User	● Critical	● High	● Medium & Below	Tot
Ash Ketchum	300	200	800	
Michelle Rivera	200	200	1000	
Aaron Edwards	300	200	700	
Debra Holt	200	200	400	
Tim Jennings	100	200	500	
Georgia Young	50	150	400	
Deanna Curtis	100	200	100	

Posture Security

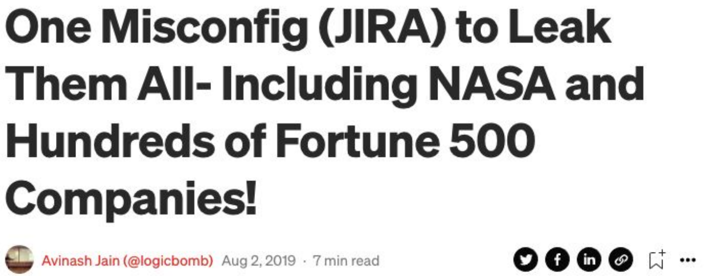
SaaS misconfigurations are a growing problem



LILY HAY NEWMAN SECURITY 08.23.2021 09:00 AM

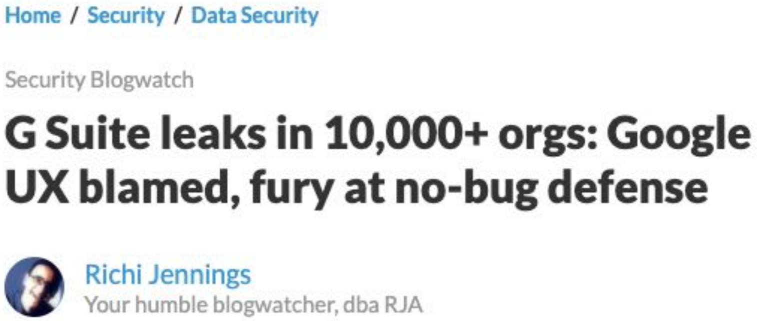
38M Records Were Exposed Online —Including Contact-Tracing Info

Misconfigured Power Apps from Microsoft led to more than a thousand web apps accessible to anyone who found them.



One Misconfig (JIRA) to Leak Them All- Including NASA and Hundreds of Fortune 500 Companies!

Avinash Jain (@logicbomb) Aug 2, 2019 · 7 min read

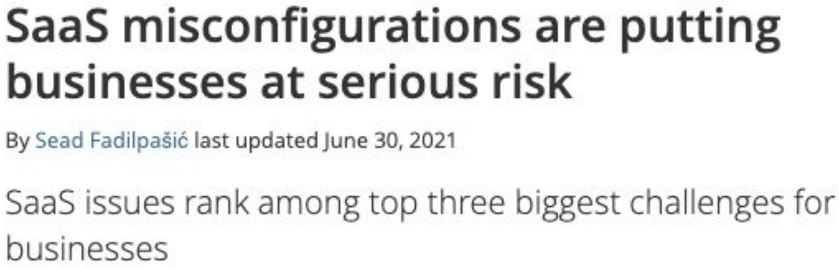


Home / Security / Data Security

Security Blogwatch

G Suite leaks in 10,000+ orgs: Google UX blamed, fury at no-bug defense

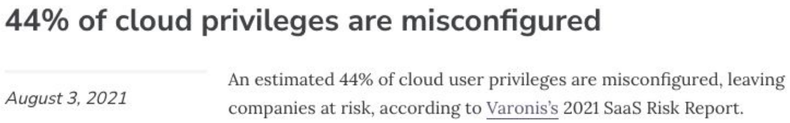
Richi Jennings
Your humble blogwatcher, dba RJA



SaaS misconfigurations are putting businesses at serious risk

By Sead Fadilpašić last updated June 30, 2021

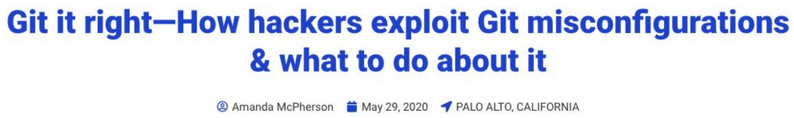
SaaS issues rank among top three biggest challenges for businesses



44% of cloud privileges are misconfigured

August 3, 2021

An estimated 44% of cloud user privileges are misconfigured, leaving companies at risk, according to Varonis's 2021 SaaS Risk Report.



Git it right—How hackers exploit Git misconfigurations & what to do about it

Amanda McPherson May 29, 2020 PALO ALTO, CALIFORNIA

Increased SaaS consumption is creating issues for enterprises

Typical large enterprise uses 50-100 sanctioned SaaS applications

99% cloud security failures will be caused by human error (Gartner)

Lack of best practices, app updates, new features, “on by default” settings

Specific challenges with securing SaaS

Keeping up with SaaS consumption is challenging

Enterprises are consuming an increasing number of sanctioned SaaS apps

Every SaaS apps has 10's-100's of security settings

New SaaS apps are often introduced without notice, creating blindspots

Fixing problems and keeping them fixed in SaaS is difficult

Ownership over SaaS config is spread across the enterprise

Admins make changes to apps, often unaware of security impact

Lack of coordination between InfoSec, IT, and GRC causes security and compliance issues

Securing SaaS is different from securing traditional software

SaaS apps are accessible from the Internet, significantly raising the stakes of any misconfigurations

Apps update themselves, adding new features and settings

SaaS is typically "open by default" to drive simplicity and user experience but adds risk

A better approach to SaaS Security Posture Management

Comprehensive app coverage

Automated security posture management for over 20 enterprise SaaS apps, with support for over 100 apps by the end of the year

Security that goes beyond compliance

Comprehensive security best practices of all security-impacting configurations, not just those on a compliance checklist

Prevention-first approach

Single-click remediation for application owners, and drift prevention that locks security-critical configurations in place to prevent problems before they occur

Natively integrated with NG-CASB for complete security of SaaS apps and data

Specific challenges with securing SaaS

Keeping up with SaaS consumption is challenging

Current processes make it impossible to keep up with the growing number of apps and unique settings

Apps that are compliant are not always secure

Application audits might have a select number of checks and quickly become outdated

Fixing problems and keeping them fixed in SaaS is difficult

Spread ownership and lack of coordination between security and IT teams makes it difficult to find and fix issues

Current SSPM solutions are siloed or not well integrated into a NG-CASB offering

An SSPM solution built to secure the new era of SaaS consumption

Comprehensive app coverage

Launching with 20+ enterprise SaaS apps

100 apps by the end of the year

Security that goes beyond compliance

Best practices for all security-impacting configurations

Continuous monitoring

Prevention-first approach

Single-click remediation

Drift prevention to lock security-critical configurations in place

Natively integrated with NG-CASB for complete security of SaaS apps and data

Product Highlights

Monitoring

Continuous monitoring to detect misconfigurations

Visibility

Operationalized dashboard helping users take the next step to fix issues

Policies

Best Practice Framework with compliance mappings that scales across apps

Local account detection for non-IdP provisioned accounts

Remediation

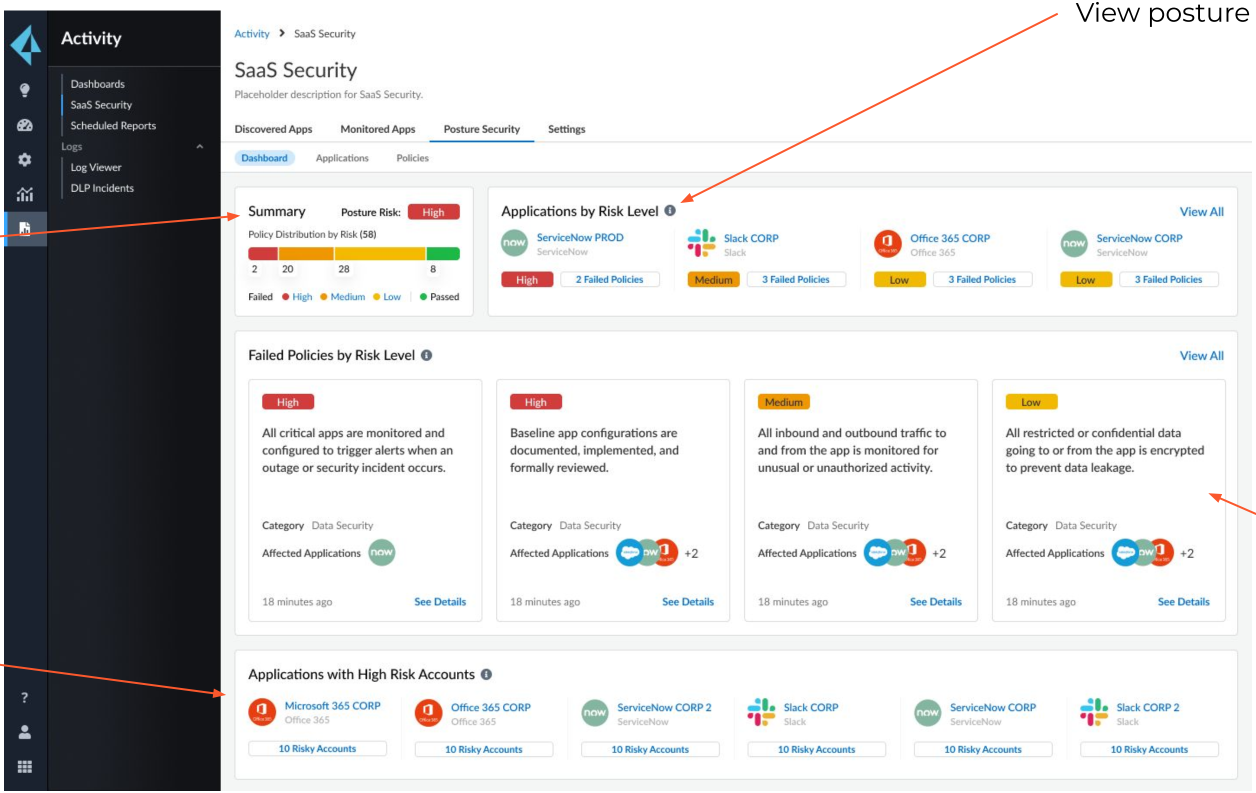
API-drive, “One-click” remediation where possible

Drift prevention to lock critical security settings

Real-time benchmarking of apps against security best practices

View posture across **apps**

Security posture summary against **best practices** and **compliance**



SaaS Security

Placeholder description for SaaS Security.

Summary Posture Risk: High

Policy Distribution by Risk (58)

2 20 28 8

Failed ● High ● Medium ● Low | ● Passed

Applications by Risk Level

Application	Type	Risk	Failed Policies
ServiceNow PROD	ServiceNow	High	2 Failed Policies
Slack CORP	Slack	Medium	3 Failed Policies
Office 365 CORP	Office 365	Low	3 Failed Policies
ServiceNow CORP	ServiceNow	Low	3 Failed Policies

Failed Policies by Risk Level

High

All critical apps are monitored and configured to trigger alerts when an outage or security incident occurs.

Category Data Security

Affected Applications

18 minutes ago See Details

High

Baseline app configurations are documented, implemented, and formally reviewed.

Category Data Security

Affected Applications +2

18 minutes ago See Details

Medium

All inbound and outbound traffic to and from the app is monitored for unusual or unauthorized activity.

Category Data Security

Affected Applications +2

18 minutes ago See Details

Low

All restricted or confidential data going to or from the app is encrypted to prevent data leakage.

Category Data Security

Affected Applications +2

18 minutes ago See Details

Applications with High Risk Accounts

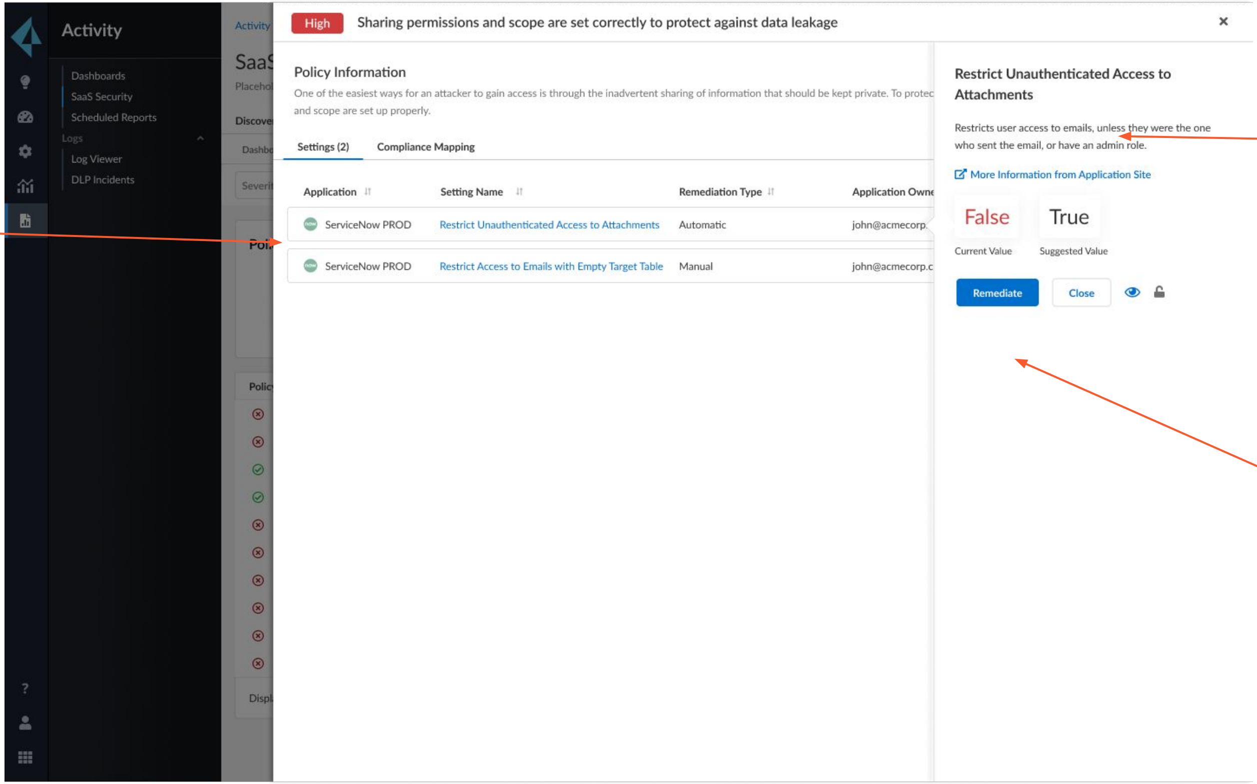
Application	Type	Risky Accounts
Microsoft 365 CORP	Office 365	10 Risky Accounts
Office 365 CORP	Office 365	10 Risky Accounts
ServiceNow CORP 2	ServiceNow	10 Risky Accounts
Slack CORP	Slack	10 Risky Accounts
ServiceNow CORP	ServiceNow	10 Risky Accounts
Slack CORP 2	Slack	10 Risky Accounts

Top security problems **prioritized for immediate action**

Advanced posture checks

Simple, single-click remediation of misconfigurations

Summarize issues across multiple apps



High Sharing permissions and scope are set correctly to protect against data leakage ×

Policy Information

One of the easiest ways for an attacker to gain access is through the inadvertent sharing of information that should be kept private. To protec
and scope are set up properly.

Settings (2) Compliance Mapping

Application	Setting Name	Remediation Type	Application Owne
ServiceNow PROD	Restrict Unauthenticated Access to Attachments	Automatic	john@acmecorp.
ServiceNow PROD	Restrict Access to Emails with Empty Target Table	Manual	john@acmecorp.c

Restrict Unauthenticated Access to Attachments

Restricts user access to emails, unless they were the one who sent the email, or have an admin role.

More Information from Application Site

False	True
Current Value	Suggested Value

Remediate Close

Security context allows users to remediate with **confidence**

Single-click remediation for multiple applications

Existing solutions do not solve the problem

App Vendors

salesforce servicenow

Scope limited to a single app

Not a complete CASB solution (no inline controls, data protection, or threat prevention)

No alignment to common security control frameworks

Capabilities vary across SaaS apps

SSPM Vendors

OBSIDIAN AppOmni ADAPTIVE SHIELD

Only solves part of the problem — not a complete SaaS security solution

Cannot provide full view of SaaS security posture and compliance

Basic basic remediation workflows that do not work for most enterprise users

Other CASB Vendors

netskope zscaler

Mostly a **settings aggregator** — simple combining of settings across multiple apps in a single console

Basic mapping of settings to compliance without full view of security framework or compliance attainment

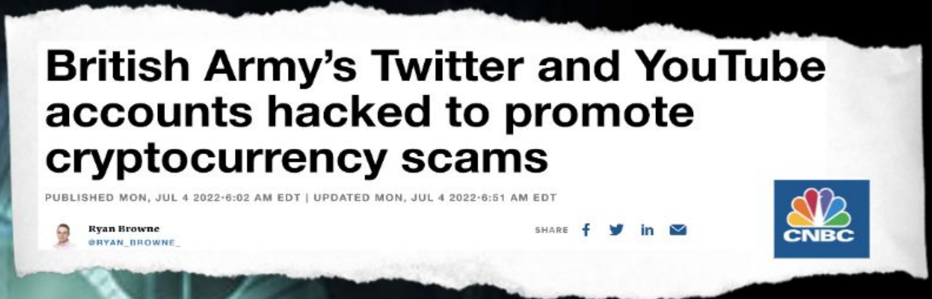
Basic remediation workflows that do not work for most enterprise users

Data security for collaboration

TBD

Suspicious User Activity Monitoring

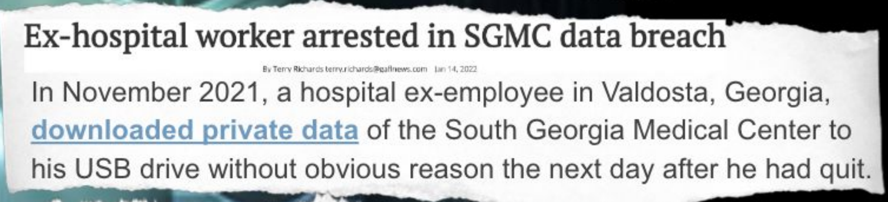
Insider Threats and Attacks are on the rise



British Army's Twitter and YouTube accounts hacked to promote cryptocurrency scams

PUBLISHED MON, JUL 4 2022·6:02 AM EDT | UPDATED MON, JUL 4 2022·6:51 AM EDT

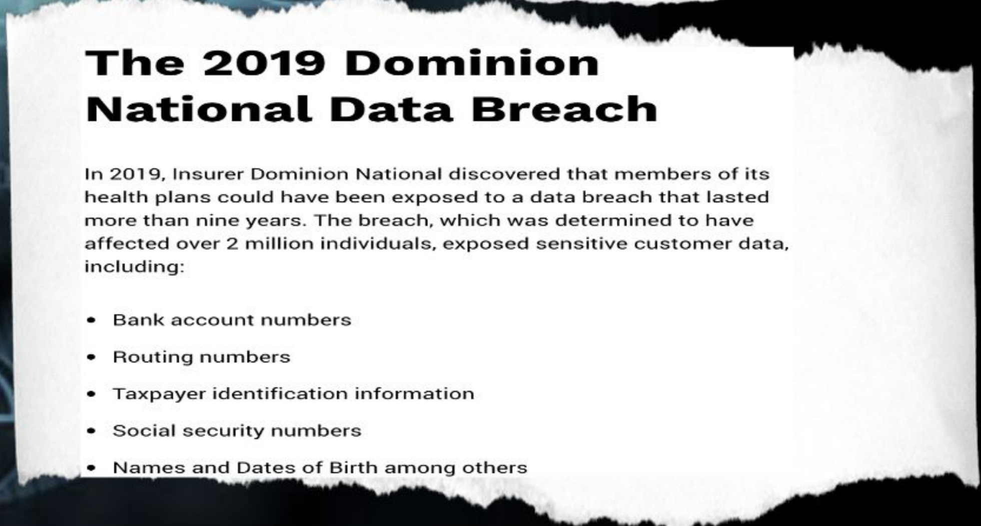
Ryan Browne
@RYAN_BROWNE_



Ex-hospital worker arrested in SGMC data breach

By Terry Richards terry.richards@gaflnews.com Jan 14, 2022

In November 2021, a hospital ex-employee in Valdosta, Georgia, downloaded private data of the South Georgia Medical Center to his USB drive without obvious reason the next day after he had quit.



The 2019 Dominion National Data Breach

In 2019, Insurer Dominion National discovered that members of its health plans could have been exposed to a data breach that lasted more than nine years. The breach, which was determined to have affected over 2 million individuals, exposed sensitive customer data, including:

- Bank account numbers
- Routing numbers
- Taxpayer identification information
- Social security numbers
- Names and Dates of Birth among others

Challenges in Monitoring SaaS Usage

Compromised Accounts

Complex to correlate user activities within/across applications

Hard to evaluate the business risk

Inability to assess all threat vectors to identify a compromised account.

Malicious Insider

Difficult to identify bad actors in the organization.

Data breaches go unidentified for a longer time causing significant loss to the organization.

Hard to detect abuse of access privileges.

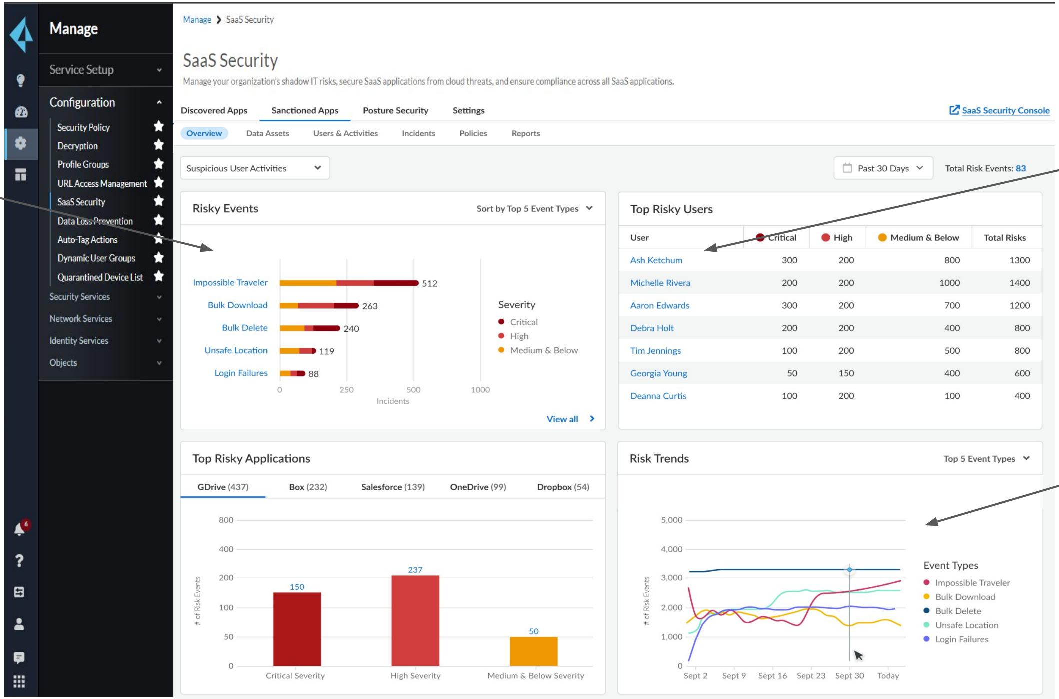
User Activity Auditing

Lack of monitoring user patterns, data usage trends in the organization.

Incidents may remain unresolved longer with the absence of correlative intelligence.

Suspicious User Activity Detection by Palo Alto Networks

Top security risks **prioritized for immediate action**



SaaS Security

Manage your organization's shadow IT risks, secure SaaS applications from cloud threats, and ensure compliance across all SaaS applications.

Total Risk Events: 83

Risky Events

Top Risky Users

User	● Critical	● High	● Medium & Below	Total Risks
Ash Ketchum	300	200	800	1300
Michelle Rivera	200	200	1000	1400
Aaron Edwards	300	200	700	1200
Debra Holt	200	200	400	800
Tim Jennings	100	200	500	800
Georgia Young	50	150	400	600
Deanna Curtis	100	200	100	400

Top Risky Applications

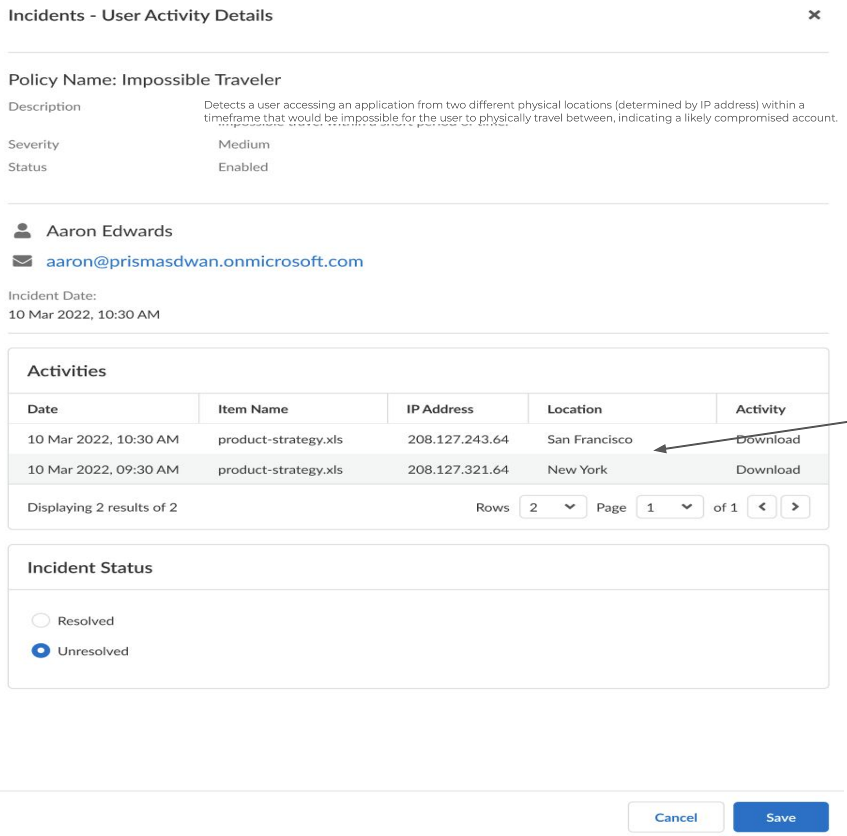
Risk Trends

Prioritized list of **Potentially Risky Users** to monitor!

Summarize details on How the organization's Security against insider threats and attacks looks like over a period of time.

Compromised Account - Impossible Traveler

Compromised Account: Identity
User Name and Email address



Incidents - User Activity Details

Policy Name: Impossible Traveler

Description	Detects a user accessing an application from two different physical locations (determined by IP address) within a timeframe that would be impossible for the user to physically travel between, indicating a likely compromised account. impossible travel within a short period of time.
Severity	Medium
Status	Enabled

Aaron Edwards
aaron@prismasdwan.onmicrosoft.com

Incident Date:
10 Mar 2022, 10:30 AM

Activities

Date	Item Name	IP Address	Location	Activity
10 Mar 2022, 10:30 AM	product-strategy.xls	208.127.243.64	San Francisco	Download
10 Mar 2022, 09:30 AM	product-strategy.xls	208.127.321.64	New York	Download

Displaying 2 results of 2

Incident Status

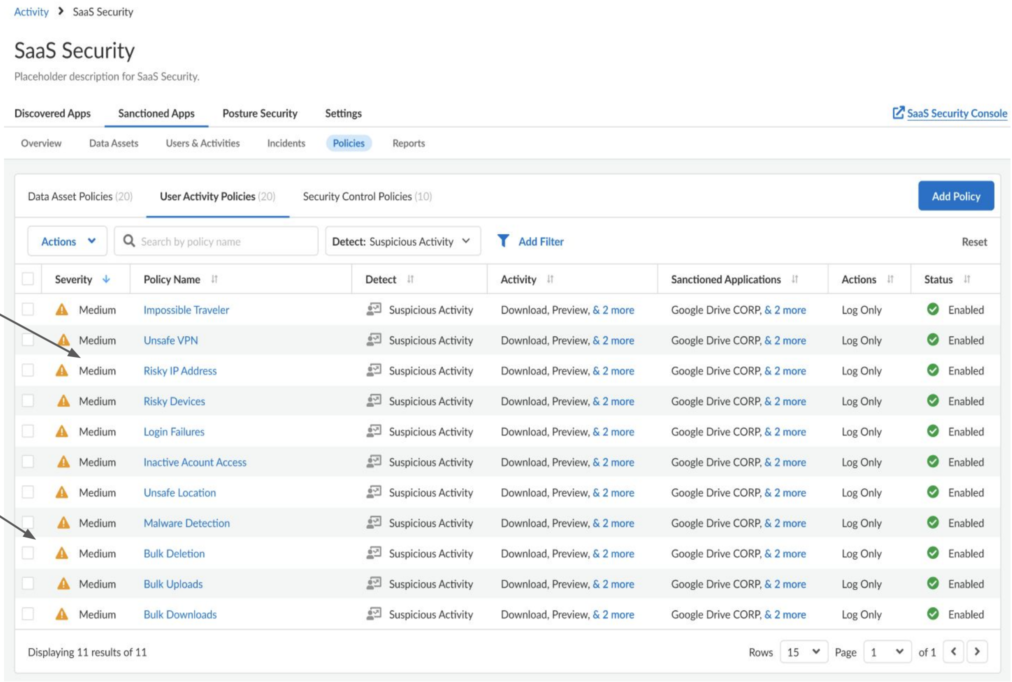
○ Resolved
● Unresolved

Activity Log
Two monitored access events from two different locations in a short time span - impossible to travel

Policies to quickly detect Insider Threats and Attacks

External Attack
Risky IP/Unsafe VPN policies to detect unauthorized access

Malicious Insider
Policies to track suspicious bulk activities indicating a bad actor



Activity › SaaS Security

SaaS Security

Placeholder description for SaaS Security.

Discovered Apps | Sanctioned Apps | Posture Security | Settings | SaaS Security Console

Overview | Data Assets | Users & Activities | Incidents | Policies | Reports

Data Asset Policies (20) | User Activity Policies (20) | Security Control Policies (10) | Add Policy

Actions | Search by policy name | Detect: Suspicious Activity | Add Filter | Reset

□	Severity	Policy Name	Detect	Activity	Sanctioned Applications	Actions	Status
□	⚠ Medium	Impossible Traveler	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Unsafe VPN	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Risky IP Address	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Risky Devices	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Login Failures	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Inactive Acount Access	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Unsafe Location	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Malware Detection	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Bulk Deletion	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Bulk Uploads	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled
□	⚠ Medium	Bulk Downloads	Suspicious Activity	Download, Preview, & 2 more	Google Drive CORP, & 2 more	Log Only	✓ Enabled

Displaying 11 results of 11 | Rows 15 | Page 1 of 1

paloalto®
NETWORKS

Thank you

paloaltonetworks.com