

SASE



SOLUTION  
GUIDE

# Securing SaaS with the Next-Generation CASB

Part of the “SASE for Securing Internet” reference architecture

SEPTEMBER 2023

# Table of Contents

---

Preface .....	1
Purpose of This Guide.....	3
Objectives .....	3
Audience .....	3
Related Documentation .....	4
Introduction .....	5
Security Challenges .....	6
Security Foundation .....	7
Design Details .....	13
Design Overview.....	14
Security for All SaaS Applications.....	15
Security for Sanctioned SaaS Applications .....	32
Data Security for All SaaS Applications .....	45
Deployment Details.....	54
Assumptions and Prerequisites.....	54
Deploying Security for All SaaS Applications .....	54
Configuring SaaS Usage Visibility and Reporting.....	54
Blocking Unsanctioned SaaS Applications.....	61
Controlling Tolerated SaaS Applications.....	68
Deploying Security for Sanctioned SaaS Applications .....	72
Configuring Security for Sanction SaaS Applications.....	72
Summary.....	76

# Preface

---

## GUIDE TYPES



*Overview guides* provide high-level introductions to technologies or concepts.

*Design guides* provide an architectural overview for using Palo Alto Networks® technologies to provide visibility, control, and protection to applications built in a specific environment. These guides are required reading prior to using their companion deployment guides.

*Deployment guides* provide decision criteria for deployment scenarios, as well as procedures for combining Palo Alto Networks technologies with third-party technologies in an integrated design.

*Solution guides* provide add-on solutions for post-deployment use cases.

## DOCUMENT CONVENTIONS



*Notes* provide additional information.



*Cautions* warn about possible data loss, hardware damage, or compromise of security.

**Blue text** indicates a configuration variable for which you need to substitute the correct value for your environment.

In the IP box, enter **10.5.0.4/24**, and then click **OK**.

**Bold text** denotes:

- Command-line commands.

**# show device-group branch-offices**

- User-interface elements.

In the **Interface Type** list, choose **Layer 3**.

- Navigational paths.

Navigate to **Network > Virtual Routers**.

- A value to be entered.

Enter the password **admin**.

*Italic text* denotes the introduction of important terminology.

An *external dynamic list* is a file hosted on an external web server so that the firewall can import objects.

**Highlighted text** denotes emphasis.

Total valid entries: **755**

## ABOUT PROCEDURES

These guides sometimes describe other companies' products. Although steps and screen-shots were up-to-date at the time of publication, those companies might have since changed their user interface, processes, or requirements.

## GETTING THE LATEST VERSION OF GUIDES

We continually update reference architecture guides. You can access the latest version of this and all guides at this location:

<https://www.paloaltonetworks.com/referencearchitectures>

## WHAT'S NEW IN THIS RELEASE

Since the last version of this guide, Palo Alto Networks made the following changes:

- Updated for Prisma® Access 4.0 preferred release
- Updated capabilities for SaaS application visibility
- Added design considerations for using explicit proxy
- Made minor navigational and procedure updates



# Purpose of This Guide

---

This solution guide builds on the reference architecture described in the [SASE for Securing Internet: Design Guide](#) and [SASE for Securing Internet: Deployment Guide](#).

This solution guide provides design and deployment guidance for the Palo Alto Networks Next-Generation cloud-access security broker (NG-CASB). This is the industry's first Secure Access Service Edge (SASE)-native NG-CASB that enables the use of SaaS applications with complete visibility, real-time data protection, and best-in-class security.

This guide:

- Describes the security challenges associated with SaaS-based applications and how Palo Alto Networks NG-CASB addresses those challenges.
- Provides a technical overview of the capabilities of the NG-CASB solution.
- Provides design considerations for using NG-CASB in order to secure SaaS applications and enforce data security.
- Provides decision criteria for deployment scenarios, as well as procedures for configuring features of the Palo Alto Networks NG-CASB in order to achieve an integrated design.

## OBJECTIVES

Completing the procedures in this guide, you are able to successfully secure applications and data in a SaaS environment. You also enable the following functionality:

- SaaS application visibility and control
- SaaS security posture management (SSPM)
- Advanced threat protection
- Data security

## AUDIENCE

This guide is written for technical readers, including solution architects and design engineers, who want to deploy the Palo Alto Networks NG-CASB solution in order to secure SaaS applications. It assumes the reader is familiar with the basic concepts of SaaS applications, data security, networking, and web security.

## RELATED DOCUMENTATION

The following documents support this guide:

- **SASE Overview**—Describes components and benefits of a SASE solution and how Palo Alto Networks delivers a full-featured SASE solution with the combination and integration of Prisma Access, Prisma SD-WAN, and cloud-delivered security services.
- **SASE for Securing Internet: Design Guide**—Presents a detailed discussion of the available design considerations and options for Prisma Access and Prisma SD-WAN when used for securing access to the internet.
- **SASE for Securing Internet: Deployment Guide**—Details deployment scenarios and step-by-step guidance for the Securing Internet design. This design includes securing internet for mobile-users and for remote-sites.
- **Securing Internet Access by Using Explicit Proxy: Solution Guide**—Provides design and deployment guidance for securing internet access by using Palo Alto Networks Prisma SASE explicit proxy. This solution allows you to apply security controls for mobile users accessing the internet and web-based applications by directing all web requests to a cloud-delivered explicit proxy without an agent installed on the endpoint.
- **SASE Secure Internet Policy Design: Solution Guide**—Describes best-practice policy design and deployment detail for securing internet services by using Cloud Managed Prisma Access.
- **Identity-Based and Posture-Based Security for SASE: Solution Guide**—This solution guide provides an overview of how the Palo Alto Networks SASE platform obtains and uses identity and device posture information and provides design and deployment guidance for applying identity-based and posture-based policies in a SASE environment.

# Introduction

---

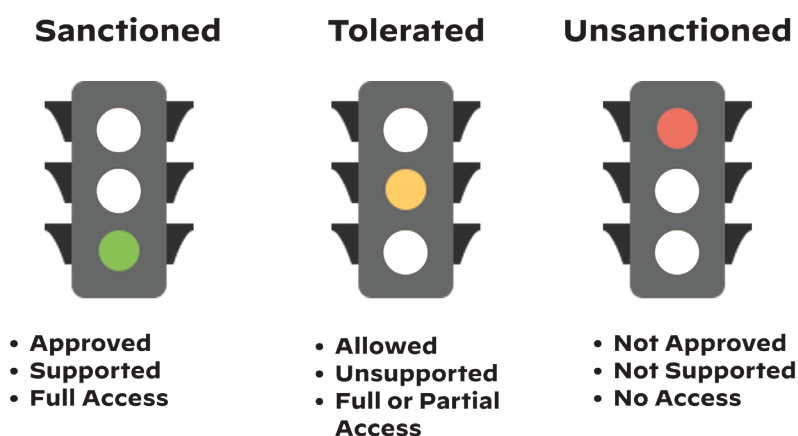
With the emergence of the hybrid workforce, the number of SaaS applications used in enterprises has increased dramatically. Instead of purchasing applications and running them in their data centers, organizations are increasingly subscribing to applications that external vendors host and maintain. These SaaS applications, originally used for niche purposes, are now used for mission-critical business functions, such as documentation, data storage, collaboration, payroll, human resources, customer resource management, service tracking, and more.

SaaS applications are easy to access. They simplify maintenance and support while reducing time-to-value. The following are some of the main reasons why organizations are transitioning to a SaaS-based application model:

- Users access SaaS applications from the internet, allowing users to work from anywhere.
- Users can onboard easily and authenticate seamlessly using corporate credentials.
- SaaS applications provide enhanced collaboration capabilities inside and outside the organization.
- Because their providers commonly deploy the infrastructure with auto-scaling capability, SaaS applications scale up rapidly.
- Because SaaS vendors operate and support their platform, they can better maintain, patch, and upgrade their infrastructure.

There are three levels of SaaS application adoption that organizations use. When discussing SaaS application policy, this guide uses the following terminology:

*Figure 1 Levels of SaaS application adoption*



*Sanctioned applications* are chosen and approved to fulfill a business need. They are critical to the business and typically allowed without restrictions on application functionality. They include applications such as Salesforce, Microsoft 365, or Slack. The organization typically subscribes to and supports the use of these applications, often tying them into the business's directory services for single sign-on.

*Tolerated applications* are important to the organization or a subset of users within the organization but are not officially supported by the organization. Tolerated applications typically fall into two main categories:

- **Non-enterprise applications**—Users rely on these applications, but the IT Help Desk does not support them. For example, an organization might allow users to access a SaaS flowcharting application but not officially support its use.
- **External partner applications**—Users rely on these applications to share and collaborate, but they are controlled by a third party or partner who shares data with internal users. For example, a organization might allow box.com for the marketing department because an external vendor uses it to deliver their projects even though the organization sanctions a different filesharing application.

Organizations might allow full access to tolerated applications to all users, or they might limit access to a subset of functionality (such as download only) or a subset of users (such as the marketing department).

*Unsanctioned applications* are known to be detrimental to the organization and are blocked without exception. There are many reasons to classify an application as unsanctioned, such as being known threat vectors, hosting in dangerous geographic regions with poor security and governance controls, having bad end-user license agreements or service-level agreements, or simply not being relevant to the business.

## SECURITY CHALLENGES

Even though SaaS-based applications provide many benefits over traditional applications, the SaaS applications can be harmful and introduce new risks. As sensitive data is increasingly uploaded, created, shared, and exposed across multiple SaaS applications, it becomes more vulnerable to loss and theft. Such sensitive data is also more unstructured than ever, making data privacy and compliance exceedingly difficult tasks.

Some of the most common security challenges associated with SaaS-based applications include the following:

- **Shadow IT**—When users have a specific task that their sanctioned application does not support, they introduce risk by using an unsanctioned SaaS application.
- **Non-compliance**—To meet data governance requirements, many organizations must comply with external standards and regulations. When users use SaaS-based applications, their organization might inadvertently become non-compliant and subject to penalties and fines.
- **Securing unstructured data**—Collaboration tools promote new communication styles. To quickly convey ideas and information, employees are using shorter, more frequent messages and sharing screenshots instead of traditional documents. As a result, sensitive data can be unstructured and increasingly difficult to protect with legacy tools.
- **Malware propagation**—When SaaS users download an infected file to their computers, the malware can infect other files shared by these users. Because of the automated file-syncing capabilities between SaaS and endpoints, malware can easily propagate over an entire organization.
- **Security posture management**—SaaS application configuration parameters change over time and administrators can inadvertently misconfigure the applications or fail to implement security best practices. These incorrect settings can impact data security.

Securing SaaS applications is challenging. Organizations must manage the risk of not having control of the infrastructure or the application itself. Users can access the applications from unmanaged devices, bypassing endpoint security controls. Users can also access the applications from outside the corporate network, bypassing standard inline protections and controls. However, organizations are still responsible for the SaaS application configuration and securing the data inside it.

## SECURITY FOUNDATION

CASB is the most recognized security solution for SaaS applications. It delivers visibility and security controls across SaaS applications. Legacy CASBs are proxy-based standalone products, disjointed from the security infrastructure. When deployed with other security controls, they can require complex traffic redirection and introduce network complexity.

Legacy CASB solutions suffer from the following three limitations:

- **Limited application visibility**—Because they rely on signature-based recognition developed in retrospect, legacy CASB solutions cannot provide visibility of new applications.
- **Inadequate data protection**—They provide inaccurate and limited coverage for data protection. They discover sensitive data-at-rest via regular expression (regex) and other traditional methods that are prone to errors. They don't offer a real-time mechanism to detect data in the context of user conversations on collaboration applications.
- **Poor security**—Originally designed to be used as compliance tools, legacy CASB solutions offer limited security controls compared to network security solutions. They deliver basic detection of known malware and miss prevention of unknown and zero-day threats.



## Palo Alto Networks NG-CASB

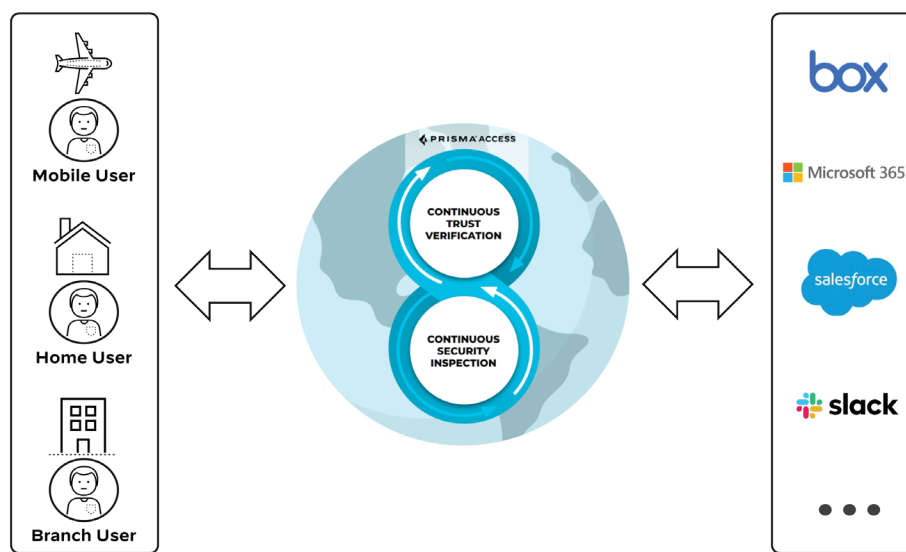
Prisma Access is a complete next-generation security platform delivered as a cloud-native service. It provides secure access to internet, SaaS, and private applications for both mobile users and remote sites. Prisma Access supports Zero Trust Network Access (ZTNA) 2.0, delivering least-privilege application access, continuous trust verification, and continuous security inspection. To protect all data and secure all applications, Prisma Access supports threat prevention, malware prevention, URL filtering, DNS security, SSL decryption, and application-based policy capabilities, providing the same level of security no matter where users are or what resources they are accessing. To support centralized analysis, reporting, and forensics across users, applications, and locations, Prisma Access stores logs in Cortex® Data Lake (CDL).

Prisma Access delivers protection at scale with global coverage. You do not have to worry about sizing and deploying hardware firewalls at branches or building out and managing appliances in colocation facilities. Prisma Access provides the network infrastructure to connect remote branches, headquarters sites, data centers, and mobile users without requiring you to build new global security infrastructure and expand operational capacity. Prisma Access is built in the cloud, leveraging the combined infrastructures of Amazon Web Services (AWS) and Google Cloud, delivering the first security fabric that provides resilience by using a multi-cloud architecture.

NG-CASB is a Prisma Access add-on that elevates the state of cloud-delivered SaaS security. With complete visibility, real-time data protection, and best-in-class security, NG-CASB is the industry's only solution that automatically keeps pace with the explosive SaaS growth. In addition to the continuous trust verification and security inspection provided by Prisma Access, the NG-CASB solution helps secure SaaS application use in the following four ways:

- **Visibility and control**—Identify all SaaS applications in use, assess risk, and control access and features
- **Security posture management**—Protect sanctioned SaaS applications from misconfigurations that put users and data at risk
- **Data security**—Prevent exposure of sensitive data-in-motion to all SaaS applications and data-at-rest inside sanctioned SaaS applications
- **Advanced threat protection**—Stop evasive malware inside SaaS applications and detect suspicious user activities associated with compromised accounts and malicious insiders

Figure 2 Palo Alto Networks NG-CASB



### Visibility and Control

Palo Alto Networks NG-CASB solves the shadow IT challenge by automatically discovering and preventing risks associated with thousands of new SaaS applications, using the following capabilities:

- **Inspects all traffic, ports, and protocols**—In addition to inspecting HTTP/HTTPS, the solution includes inspection for all types of applications, such as Tor, FTP, and PrivateVPN.
- **Application Cloud Engine (ACE)**—ACE technology leverages the power of the broad global community and uses machine learning (ML) models to automatically provide continuous identification, categorization, and granular risk-based control of known and previously unknown SaaS applications.
- **SaaS application analysis**—For each SaaS application, NG-CASB supports more than 10 descriptive and 30 compliance-related attributes. Applications are classified across more than 400 categories in the catalog.
- **SaaS risk assessment**—NG-CASB provides default risk scores that you can customize based on the attributes that matter most to your organization.
- **SaaS reporting**—NG-CASB generates detailed reports that provide information on user access, volume, and risk associated with SaaS applications. These reports can help you maintain SaaS security policies, establish priorities, and monitor compliance.
- **Risk mitigation controls**—You can automate policy recommendations for existing and future applications, eliminating time-consuming manual policy definitions.
- **Granular access control**—NG-CASB conditionally allows access to specific application functions (such as file upload, download, or sharing), depending upon the application. In addition, you can restrict access based on user and group information, who has access to an application, or application function.

**Note**

Many organizations have architecture or compliance requirements that necessitate the use of a proxy. When user traffic is predominantly web-based HTTP and HTTPS, you can use a web proxy in order to provide security and visibility for this traffic. Although using Prisma Access as a web-proxy eliminates the requirement of GlobalProtect® agent, you must secure non-web traffic separately from the web proxy.

## Security Posture Management

You can inadvertently misconfigure sanctioned applications or fail to implement security best practices. Incorrect settings and configuration drift between applications can impact data security. (For example, a SaaS application might not have multi-factor authentication (MFA) enabled. Password-only authentication can allow access to attackers with stolen credentials.) SSPM helps prevent data loss and reduces the risk of security breaches, and it includes the following capabilities:

- **Continuous monitoring and analysis**—Continuous monitoring eliminates the ongoing risk of data loss due to human misconfigurations.
- **Common security framework**—Going beyond basic compliance checks, this solution aligns thousands of application-specific best-practices configurations to a common security framework that security teams can easily understand and manage.
- **Remediation flows**—SSPM allows users to fix misconfigurations with a single click and avoid configuration drift by locking critical security settings in place.

## Data Security

With the industry's first cloud-delivered Enterprise Data Loss Prevention (DLP) service, this solution provides data protection and compliance controls consistently across SaaS applications. This solution delivers the following data-security capabilities:

- **Single cloud engine**—This solution delivers unified policies for sensitive data everywhere, both at rest and in transit.
- **Highest levels of detection accuracy**—This solution automatically detects sensitive content via ML data classification and an extensive number of described data identifiers using regex or keywords (examples: credit card or ID numbers, financial records, General Data Protection Regulation (GDPR), or other data privacy and compliance-related information) and applies customizable data profiles and Boolean logic to scan for collective types of data.
- **Scanning, classification, and protection**—This solution analyzes all data stored within SaaS applications in order to make sure policy violations, exposures, and regulatory compliance are properly addressed.
- **Exposure analysis**—To reduce incidents and inaccurate detection, this solution analyzes public, external, and internal sharing of files, as well as precise context criteria (example: number of occurrences and pattern logic).
- **Exact data matching**—An advanced data-fingerprinting method detects specific sensitive data and prevents exfiltration.
- **Secure collaboration applications**—Ensuring high accuracy and fewer false positives, this solution automatically identifies sensitive information even within the context of unstructured users' conversations by using deep learning, natural language processing, artificial intelligence models, and advanced optical character recognition (OCR).
- **Detection of flexible document properties**—Third-party data tagging augments the identification of sensitive data. This solution also includes file blocking profiles that you can use to prevent file types from being downloaded, which is an important part of a cloud data protection strategy.
- **Automated incident workflows**—Policy-based response actions include user alerts and auto-remediation.

## Advanced Threat Protection

SaaS applications introduce new risks that you need to understand and control. To help mitigate the risks from advanced threats, NG-CASB provides the following capabilities:

- **Protection from malware**—Many SaaS applications automatically synchronize files with users and third parties, so malware can also spread across the organization. This solution prevents infected files from residing in the sanctioned SaaS application, whether the malware is known or unknown and regardless of the source of the file. This solution stops the threat at the source, before the threat propagates to other locations.
- **Monitoring and detection of suspicious user activity**—This solution provides detection of suspicious activities that could indicate a compromised account or malicious insider.
- **Behavioral analytics**—This solution identifies high-risk activities such as shared credentials, bulk data access, suspicious logins, impossible traveler, and more.
- **User activity auditing**—This solution enables quick and simple investigation and remediation workflows.



# Design Details

Prisma Access is a complete next-generation security platform delivered as a cloud-native service. It provides secure access to internet, SaaS, and business applications for both mobile users and remote sites. To deliver SaaS security that is tightly coupled with the security infrastructure, NG-CASB capabilities are integrated into Prisma Access.

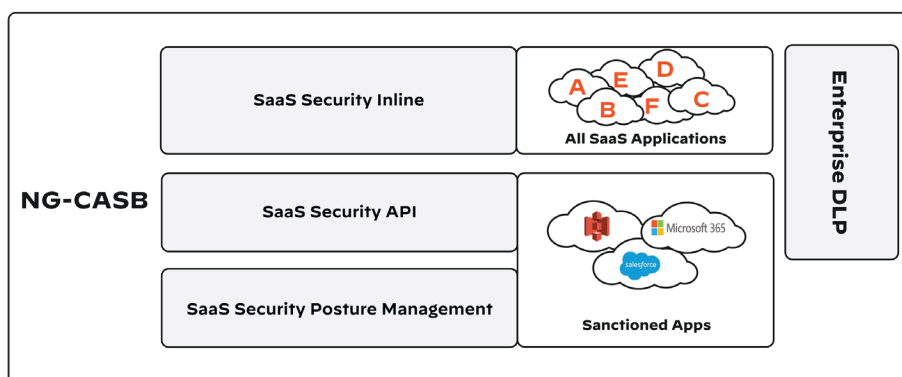
You have two options for provisioning and managing Prisma Access:

- Cloud-managed Prisma Access (through Strata Cloud Manager)
- Panorama® managed Prisma Access (through the Cloud Services plugin)

The NG-CASB design uses cloud-managed Prisma Access in order to provide the following set of capabilities, which are all integrated into a single management console:

- **SaaS Security Inline**—Uses ACE to retrieve SaaS application information and enforce access controls. ACE contains over 60,000 SaaS application IDs and is adding to the list constantly. To identify new SaaS applications as they become available, ACE uses ML and crowdsourcing.
- **SaaS Security API**—Cloud-based service that connects directly to sanctioned SaaS applications by using the cloud application's API. The service provides asset discovery, data classification, sharing/permission visibility, user-activity monitoring, and threat detection.
- **SSPM**—Cloud-based service that connects directly to sanctioned SaaS applications by using the cloud application's API. Through continuous monitoring, the service helps detect and remediate misconfigured security settings and best practices in SaaS applications.
- **Enterprise DLP**—Cloud-delivered solution that comprehensively protects sensitive data across all networks, clouds, and users. Enterprise DLP easily enables data protection and compliance in minutes, eliminating appliance deployment and ongoing management cycles in order to ensure the most cost-effective enterprise data-loss prevention on the market.

Figure 3 NG-CASB capabilities



## DESIGN OVERVIEW

To protect all types of SaaS applications, the NG-CASB design incorporates a multi-mode architecture. The combination of the modes solves the shadow IT problem while supporting granular security controls for sanctioned applications. The supported modes are as follows:

- **Inline security**—Provides visibility, access control, and feature control across thousands of SaaS applications delivered via Prisma Access inline traffic inspection.
- **API security**—Provides visibility, local scanning, and granular security controls for SaaS applications, delivered via cloud-based API connectors. Because it requires administrator access to the SaaS applications, this mode is available only for sanctioned applications.

For all SaaS applications, this design recommends inline security mode for implementing the following:

- **Visibility and control**—Unsanctioned applications are completely blocked while tolerated applications can be restricted by user, user group, and/or functionality.
- **Data loss prevention**—Enterprise DLP monitors and controls uploads of sensitive data to SaaS applications.
- **Threat protection**—Prisma Access inspects all SaaS traffic for vulnerability exploits, malware, spyware, command-and-control (C2) communication, and even unknown threats.

For sanctioned SaaS applications, the design recommends API security mode to complement inline security with advanced, granular controls for implementing the following:

- **Asset discovery and visibility**—Discovers all files, also called *assets*, contained in the managed SaaS application and provides visibility into how users are using the SaaS application.
- **Exposure risk assessment**—Provides visibility into how assets are shared in order to identify exposure level, user activity, and external collaborators.
- **Data security**—Discovers and analyzes content when it's stored and shared on SaaS applications, providing data governance and compliance assurance.
- **Security posture management**—Monitors and configures security settings for multiple SaaS applications in one place, making them both compliant and protected.
- **Threat protection**—Stops evasive malware stored in SaaS applications and identifies compromised accounts and malicious insiders.

Table 1 Recommended control settings for each type of SaaS application

Control	Sanctioned	Tolerated	Unsanctioned
Inline Visibility	Yes	Yes	Yes
Inline Control	No—full access	Yes—allow user group and/or functionality	Yes—block application
Inline DLP	Yes—inspect uploads to SaaS	Yes—inspect uploads to SaaS	No—application is blocked
Inline Threat Protection	Yes—secure traffic to SaaS	Yes—secure traffic to SaaS	No—application is blocked
SaaS Security API	Yes—asset discovery, risk assessment and threat protection	No—requires admin access	No—application is blocked
SSPM	Yes—config management and drift prevention	No—requires admin access	No—application is blocked
Data Security	Yes—data governance and compliance	No—requires admin access	No—application is blocked

## SECURITY FOR ALL SAAS APPLICATIONS

Solving the shadow IT security challenge requires granular visibility into which applications are being used and how. This information is essential for defining effective SaaS security policies.

### About Decryption

Organizations secure access to most of their applications and services with encryption, and over 85% of their internet traffic is encrypted. This has become an opportunity for adversaries who are taking advantage of encryption in order to hide their malicious activities in encrypted sessions and evade detection. Because malware can be disguised inside encrypted traffic, it is important to be able to decrypt as much internet traffic as possible (within compliance regulations).

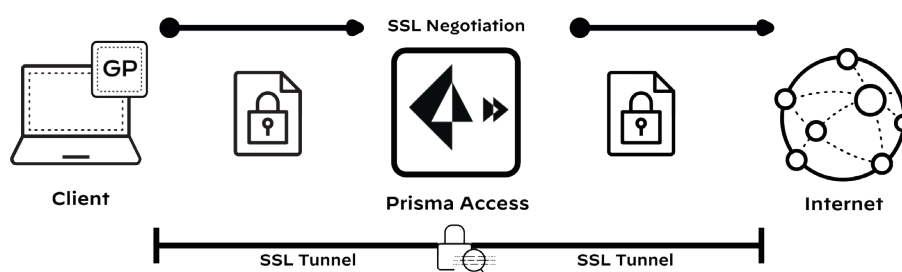
Prisma Access supports decryption of inbound and outbound SSL/TLS connections. After Prisma Access decrypts the traffic specified in your decryption policy, it enforces the security policy rules, providing protection against threats while enabling users to access their data and applications. Prisma Access then re-encrypts the traffic before the traffic exits the system. You can define sensitive traffic types as exempt from decryption policies.

Prisma Access preserves the integrity of the SSL/TLS session by using the cryptographic settings of the original SSL/TLS negotiation as mandated by the client and the server. It does not change the cryptographic parameters after the session has been negotiated. Further, to reduce risks associated with older versions of the protocols, Prisma Access allows you to specify the supported SSL/TLS protocol versions and cipher suites. Certificate Revocation List/Online Certificate Status protocol checks ensure that certificates presented during SSL decryption are valid.

## Decryption Settings

In this design, you use the SSL forward proxy default configuration to decrypt all outbound internet traffic from all users. To secure the connection, SSL uses certificates to establish trust between the client and server. Most commonly, to establish this trust, an organization uses its own public key infrastructure to generate a trusted signing certificate for Prisma Access. The endpoints must install the Prisma Access Root CA certificate into their certificate store so that the client session to Prisma Access can be established. You can use GlobalProtect to install the Trusted Root CA certificate on Windows and macOS clients. Alternatively, Prisma Access includes built-in signing certificates that you can use for testing.

Figure 4 SSL forward proxy



To ensure compatibility across all websites, Prisma Access includes both RSA and ECDSA signed certificates. Two sets of certificates, one trusted and one untrusted by the client, ensure that the end user gets a browser error when the target website has a certificate signed by a certificate authority that Prisma Access does not trust.

Figure 5 Certificate settings

Certificate Settings		
Certificate When Proxying for Trusted Sites		
RSA	Forward-Trust-CA	<a href="#">Export</a>
ECDSA	Forward-Trust-CA-ECDSA	<a href="#">Export</a>
Certificate When Proxying for Untrusted Sites		
RSA	Forward-UnTrust-CA	<a href="#">Export</a>
ECDSA	Forward-UnTrust-CA-ECDSA	<a href="#">Export</a>



### Note

SAML authentication for explicit proxy requires decryption. When using explicit proxy, it is a best practice to decrypt all traffic. For a detailed description, see the [Securing Internet Access by Using Explicit Proxy: Solution Guide](#).

If decryption breaks an important website or application, you can add the hostname or use a wildcard domain as a custom decryption exclusion. If for compliance regulation you want to prevent decryption for a specific type of application (examples: financial services, government, health, and medicine), you can configure a bypass based on URL categories. Prisma Access does not decrypt, inspect, and enforce security policy on traffic that the SSL decryption exclusion list allows or the URL category that is bypassed. The main reasons that websites and applications break when decryption is applied include pinned certificates, client authentication, incomplete certificate chains, and unsupported ciphers. Pinned certificates are commonly associated with mobile apps. To eliminate the need to maintain exclusions for the most common websites and applications that cannot be decrypted, Prisma Access contains a list of predefined exclusions.

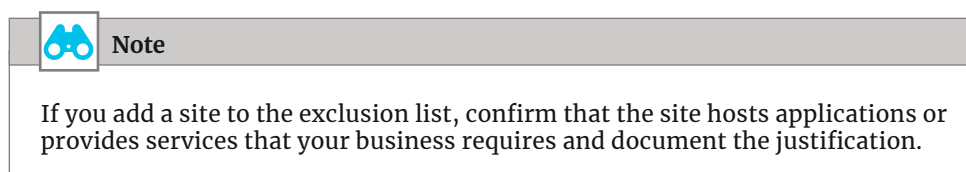


Figure 6 Decryption exclusions



You can use the default best-practice settings in order to enforce the recommended TLS versions, cipher suites, and certificate validations. The best-practice settings enforce the following:

- Block sessions based on certificate status, including blocking sessions with expired certificates, untrusted issuers, unknown certificate status, and restrict certificate extensions
- Block sessions with unsupported versions and cipher suites and that require using client authentication
- Minimum protocol version of TLS 1.2 and key exchange, encryption, and authentication algorithms allowed



## SaaS Security Inline

SaaS Security Inline provides complete visibility and control of SaaS application usage from corporate networks and managed devices. To provide a consistent management experience, it integrates with Prisma Access web-security policies.

The process for using SaaS Security Inline for securing applications is as follows:

1. Analyze usage visibility of SaaS applications in order to establish a starting point for application-control policies.
2. Establish risk scores that align with your organization's security requirements.
3. Tag discovered applications to match SaaS adoption usage level. This helps manage the application evaluation progress and generates accurate reports.
4. Generate and review SaaS security reports.
5. SaaS administrators can generate policy recommendations for blocking unsanctioned SaaS applications.
6. Web-security administrators can import and deploy policy recommendations from SaaS administrators, or they can generate their own custom web-security policies.

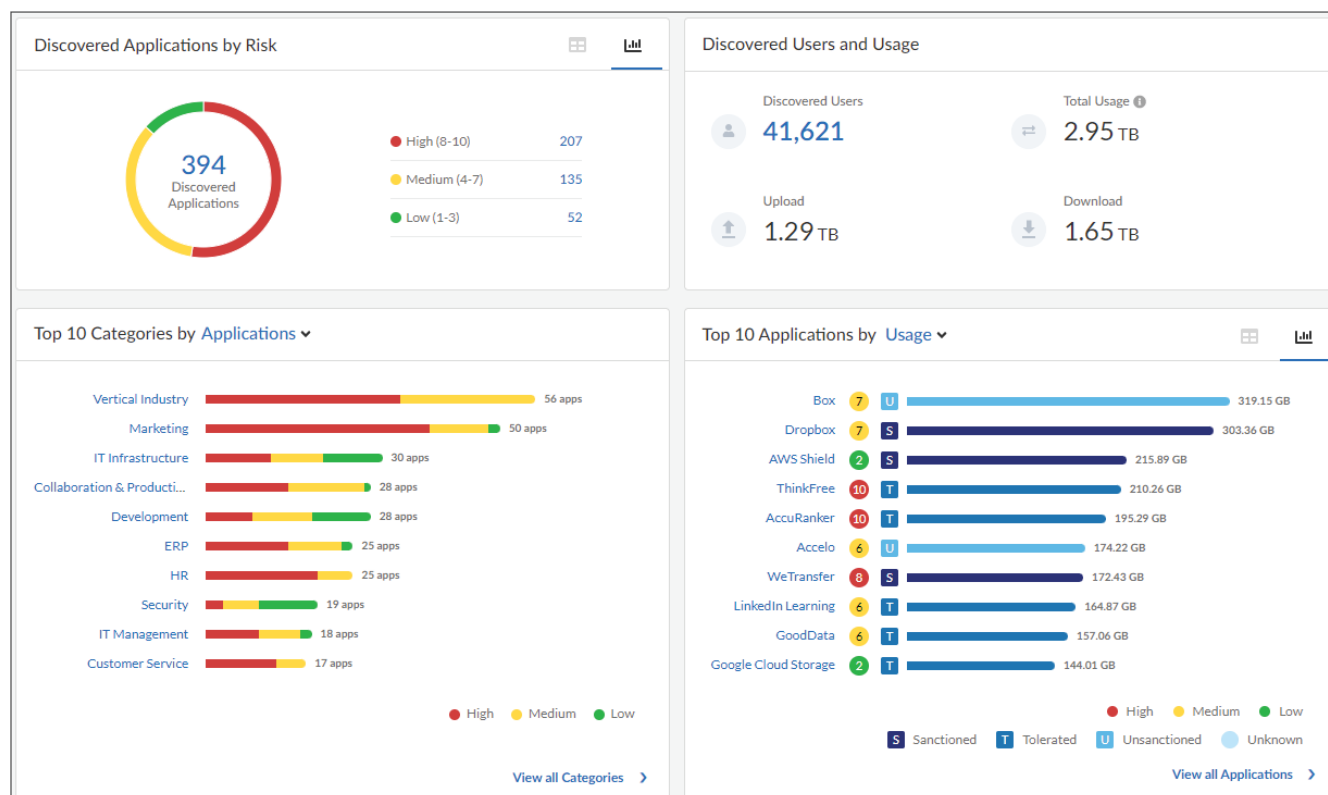
Figure 7 Securing all SaaS



## Usage Visibility

In the Discovered Applications dashboard, SaaS Security Inline provides a summary view where administrators can examine SaaS application usage. The dashboard provides information about the total number of SaaS applications discovered on the network, the total number of users, and how much, overall, SaaS applications are used by volume. The dashboard also displays top 10 categories by applications and top 10 applications by users. The dashboard enables administrators to drill-down into application and usage details.

Figure 8 Discovered Applications dashboard



SaaS Security Inline uses the ACE service to download App-IDs from the cloud and to identify unknown SaaS applications that do not have specific predefined App-IDs from the Palo Alto Networks content team. These are the applications that Prisma Access identifies as SSL or web-browsing. ACE collects a small initial portion of certain categories of network session payloads (up to four first packets) and uses ML and crowdsourcing to identify new SaaS applications and maintain a cloud database of App-IDs. With a catalog of over 60,000 SaaS applications and growing constantly, ACE vastly increases the number of known App-IDs in order to identify and control SaaS applications.

Figure 9 Application Dictionary dashboard

Application Dictionary (60,147)			
<input type="text" value="Search Application Name or Category"/>		<a href="#">Add Filter</a>	<a href="#">Reset</a>
Application Name ↑	Risk ↓	Category ↓	Actions
#paid	9	Marketing	<a href="#">View Details</a>
&frankly	9	HR	<a href="#">View Details</a>
.page	9	Hosting	<a href="#">View Details</a>
000webhost	7	Hosting	<a href="#">View Details</a>
01Com	10	Security	<a href="#">View Details</a>
OPing	10	Hosting	<a href="#">View Details</a>
Opatch	9	Vertical Industry	<a href="#">View Details</a>
Oxcareer	9	Vertical Industry	<a href="#">View Details</a>
1 SPOT Tech	9	ERP	<a href="#">View Details</a>
1-800-TIMECLOCK	4	Commerce	<a href="#">View Details</a>
Displaying 10 results of 60,147           Rows <input type="text" value="10"/> Page <input type="text" value="1"/> of 6015			

## Risk Assessment

When deciding how to classify a SaaS application, you should consider how critical the application is to your organization, what data is stored in the application, the security risk of the application, and how much visibility into the application is possible. The application detailed view provides basic information about the discovered SaaS applications. This information includes vendor name, product URL, whether the application is open source, category, employee count, net promoter score (NPS), the vendor's headquarters location, and application's domains.

By assigning each a risk score, SaaS Security Inline helps determine which applications pose a risk. This risk score is based on security, privacy, and compliance attributes of the SaaS application. Some attributes have a higher weight than others. The more compliance attributes that an application supports, the lower the risk score is for that specific application.

Figure 10 Application detailed view (basic info)

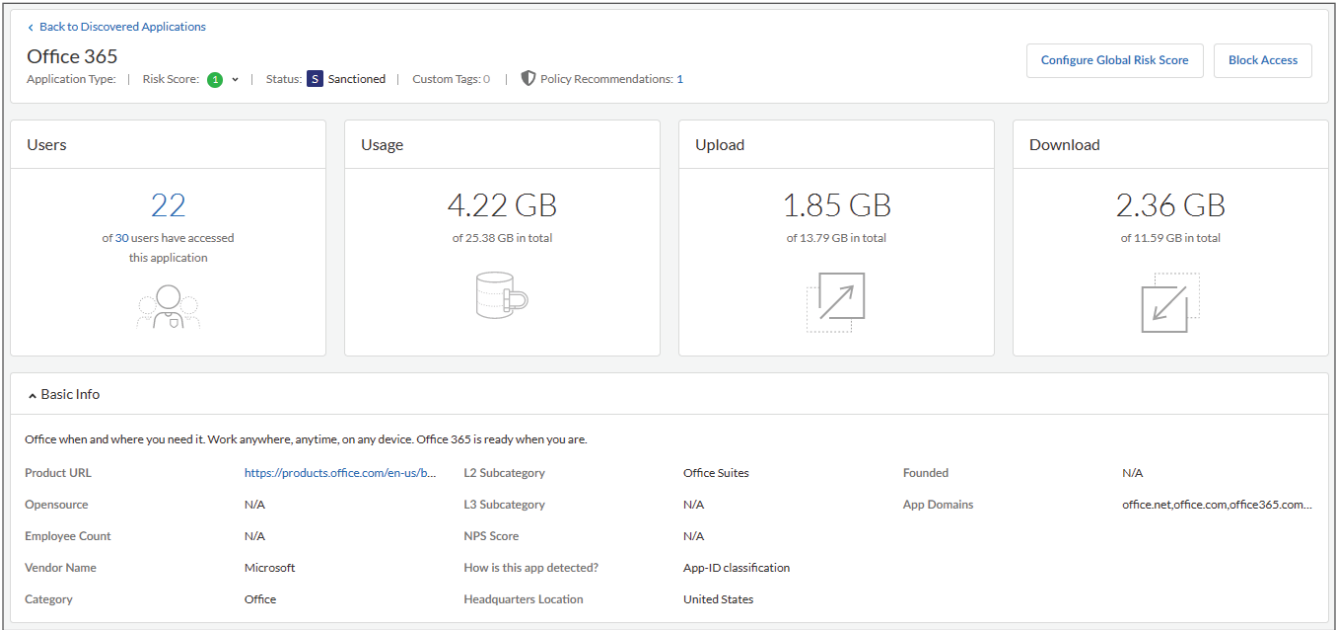


Figure 11 Application detailed view (detailed attributes)

Security and Privacy
Attributes Total 13 12

Security and Privacy information helps you assess if this application meets your organization's security policies.

Data Retention

✓

HTTP Security Headers

✓

Encryption at Rest

✓

Encryption in Transit

✓

Disaster Recovery

✓

Native Data Classification

✓

Data Ownership

Customer Ownership

Audit Log

✓

Privacy Policy

✓

File/Content Sharing

✓

Session Timeout

✓

Third Party Data Sharing

✓

Terms and Conditions

✓

Identity Access Management
Attributes Total 5 5

Identity Access Management information helps you assess the authentication and access-control capabilities of this application.

IP Based Restrictions

✓

Password Policy

✓

RBAC

✓

MFA

✓

SAML

✓

Compliance
Attributes Total 34 29

Compliance information helps you assess if this application meets the requirements of the standards, regulations, and policies listed.

✓ C5 Compliance

✓ FISMA

✓ ISO 27017

✗ PrivacyMark (Japan)

✓ CJIS

✗ GAPP

✓ ISO 27018

✓ Safe Harbor

✓ COBIT

✓ GDPR

✗ ISO 9000

✓ SOC1

✓ COPPA

✓ GLBA

✓ ISO 9001

✓ SOC2

✓ CSA STAR

✓ HIPAA

✓ ITAR

✓ SOX

✓ FEDRAMP

✓ HITRUST CSF

✓ Jericho Forum Commandments

✓ SSAE 18

✓ FERPA

✓ ISAE 3402

✓ NIST SP 800-53

✗ TrustArc

✓ FFIEC

✓ ISO 27001

✓ PCI

✓ FINRA

✗ ISO 27002

✓ Privacy Shield

In Figure 11, the application met several compliance standards such as GDPR, Federal Risk and Authorization Management Program (FedRAMP), and System and Organization Controls 1 and 2 (SOC1, SOC2). As a result, the overall risk score of this application is low. Application risk score is a value from 1 to 10. Applications with a risk value of 8 or higher are considered high risk applications.



You can adjust the weights assigned to each of the attributes in order to reflect a risk score that is better aligned to your organization's requirements. The total assigned weights across all attributes must total 100, and the new weights impact the score of all SaaS applications. The attributes available for scoring risk include the following:

- **Security and privacy**—Product capabilities and terms and conditions that can improve your organization's security and privacy. For example, MFA and role-based access control (RBAC).
- **Compliance**—Adherence to regulatory standards or framework. For example, GDPR and CJIS (Criminal Justice Information Services).

Figure 12 Custom global risk score

Configure Global Risk Score

You can assign weights to each attribute in order to re-calculate the SaaS Risk Score for all the applications. If an attribute is more important to your organization, assign it a higher weightage. The new scores will be calculated based on what you input here. Note: Global Risk Score doesn't affect Under Research applications.

☒ Use Custom Weights

Your risk weighting: 100  
This number has to equal 100.

Set All Fields to Zero

Security and Privacy

Data Retention	2	Encryption at Rest	5	File/Content Sharing	5
Audit Log	2.5	Encryption in Transit	6	Data Ownership	2
HTTP Security Headers	2.5	Terms and Conditions	1	Native Data Classification	2.5
Privacy Policy	1	Disaster Recovery	3		
Third Party Data Sharing	2	Session Timeout	2.5		

Identity Access Management

RBAC	4
MFA	6
Password Policy	6
SAML	4
IP Based Restrictions	3

Compliance

ISO 9000	0	COPPA	0	ISO 27017	1	CJIS	0
GAPP	0	HITRUST CSF	1	C5 Compliance	0	GDPR	4
ISO 9001	1	COBIT	1	CSA STAR	1	FISMA	1
PrivacyMark (Japan)	1	FINRA	1	SOC1	1	ISAE 3402	3
SOC2	3	TrustArc	1	SSAE 18	1	GLBA	1
Privacy Shield	1	ISO 27018	1	Jericho Forum Commandments	0	PCI	4
FERPA	0	FFIEC	1	SOX	1	ISO 27002	1
ITAR	1	FEDRAMP	1	HIPAA	3		
Safe Harbor	0	ISO 27001	3	NIST SP 800-53	1		

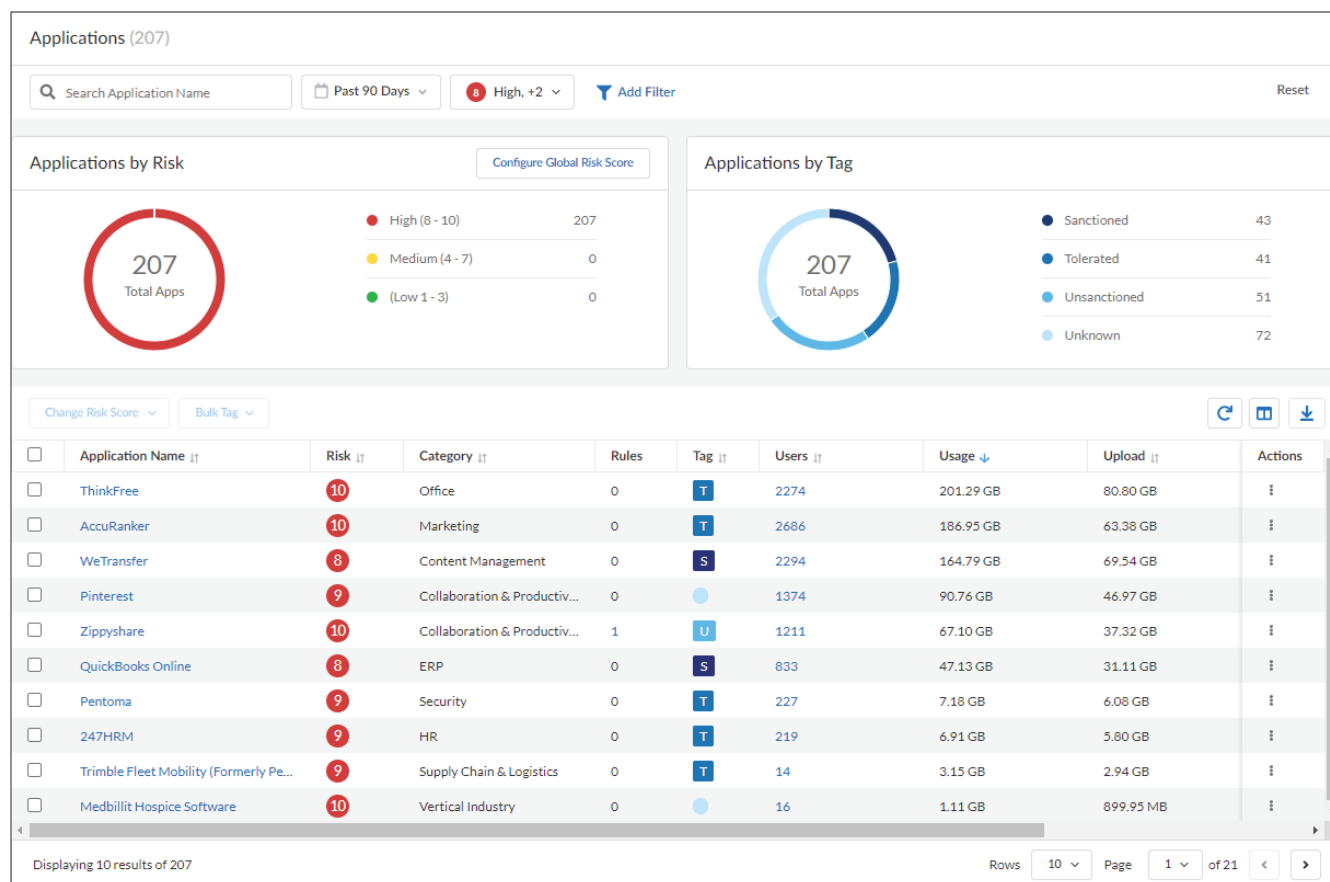
The new scores will impact all applications.

Cancel

Save

The following figure shows a significant number of high-risk applications being accessed. The high-risk portion of the Applications by Risk chart in the dashboard reveals the specific applications being accessed. You can use this information to identify applications to block and to recommend less risky applications to your users.

Figure 13 High-risk applications



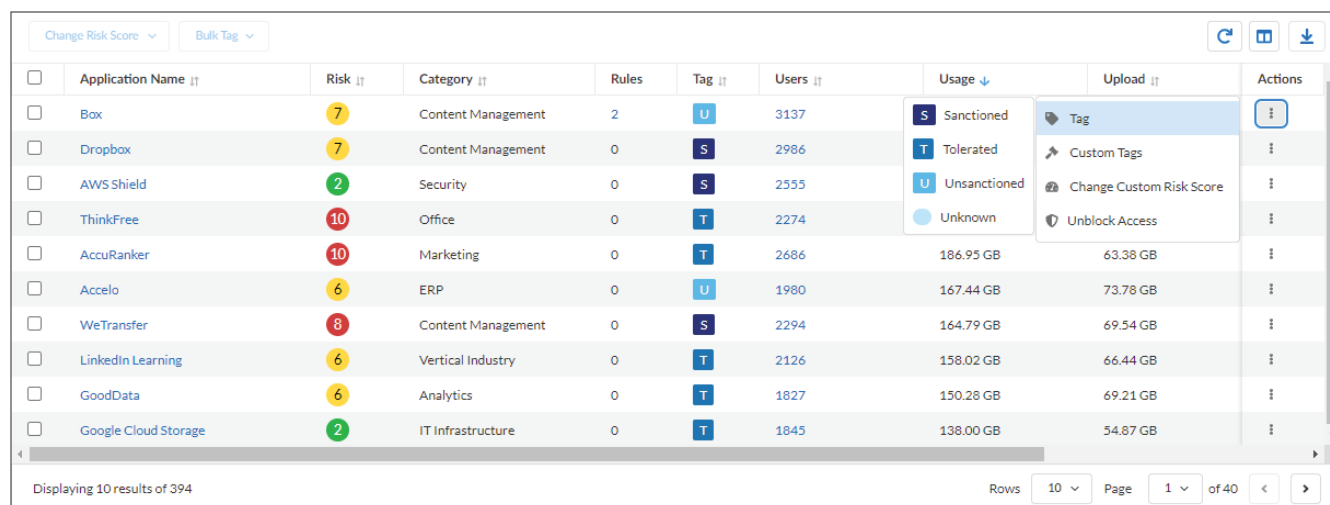
## Tagging Applications

To facilitate monitoring and reporting on discovered applications, you should assign tags to applications within SaaS Security Inline. When an application is discovered, it is automatically assigned a tag of “Unknown.” There are four default tags available to assign, which correspond to the SaaS application usage levels:

- Sanctioned
- Tolerated
- Unsanctioned
- Unknown

You can also create custom tags, such as “Engineering,” to group applications. This lets you filter the display and investigate SaaS application usage, as well as create policy recommendations based on tags.

Figure 14 Tagging applications



<input type="checkbox"/>	Application Name	Risk	Category	Rules	Tag	Users	Usage	Upload	Actions
<input type="checkbox"/>	Box	7	Content Management	2	U	3137			
<input type="checkbox"/>	Dropbox	7	Content Management	0	S	2986			
<input type="checkbox"/>	AWS Shield	2	Security	0	S	2555			
<input type="checkbox"/>	ThinkFree	10	Office	0	T	2274			
<input type="checkbox"/>	AccuRanker	10	Marketing	0	T	2686	186.95 GB	63.38 GB	
<input type="checkbox"/>	Accelo	6	ERP	0	U	1980	167.44 GB	73.78 GB	
<input type="checkbox"/>	WeTransfer	8	Content Management	0	S	2294	164.79 GB	69.54 GB	
<input type="checkbox"/>	LinkedIn Learning	6	Vertical Industry	0	T	2126	158.02 GB	66.44 GB	
<input type="checkbox"/>	GoodData	6	Analytics	0	T	1827	150.28 GB	69.21 GB	
<input type="checkbox"/>	Google Cloud Storage	2	IT Infrastructure	0	T	1845	138.00 GB	54.87 GB	

Displaying 10 results of 394

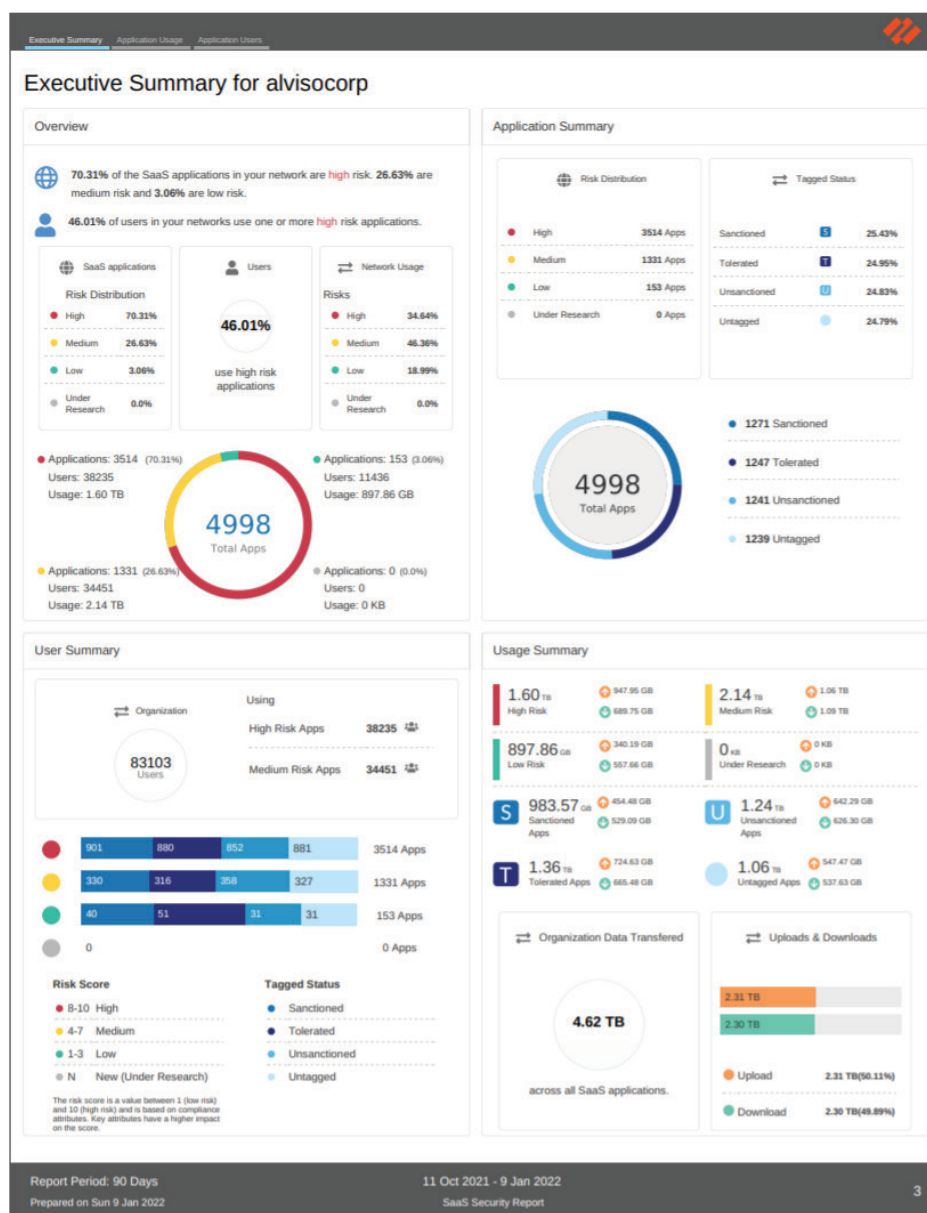
Rows: 10 Page: 1 of 40

## SaaS Security Reports

The SaaS security report provides visibility (as seen by SaaS Security Inline) into the SaaS application usage. The report is generated as needed and should be a part of regular SaaS security posture audits. The report can also be used to brief executives on SaaS application usage.

The report lists the total number of SaaS applications discovered, the risk levels of those applications, and whether those applications are sanctioned, tolerated, or unsanctioned, based on how the applications are tagged. The report provides a summary of user activity but does not provide detailed user access information. Additionally, it provides usage information by category, such as office applications, content management, ERP, and collaboration, and the top high-risk and high-volume applications in use.

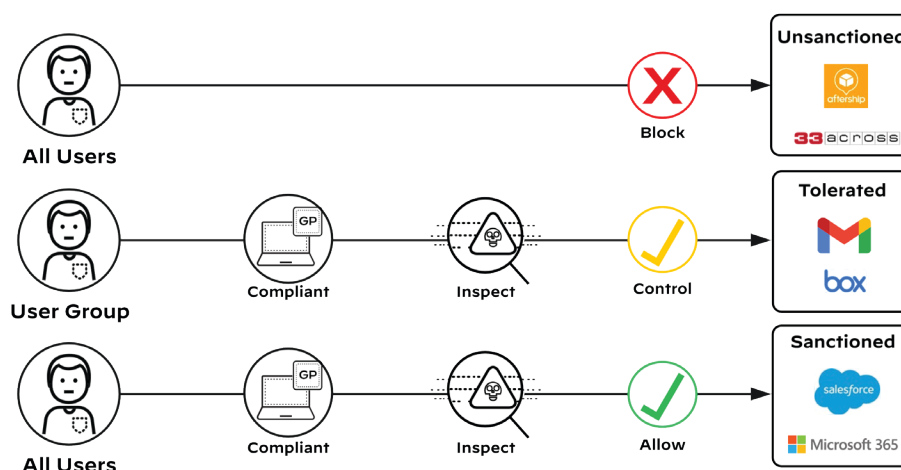
Figure 15 SaaS security report



## Controlling SaaS Application Use

After gaining visibility into the applications being used, who is using them, and the risks associated with them, you can establish controls for accessing SaaS applications. In this design, you completely block unsanctioned applications, and you can restrict tolerated applications by user/user group or functionality. When using GlobalProtect, you can perform additional posture checks that ensure device compliance before granting access.

Figure 16 SaaS inline security policy



## Policy Recommendations

NG-CASB supports a policy recommendation model that allows split responsibility between SaaS administrators and web-security administrators. A SaaS administrator can initiate the process of controlling access to an application by creating SaaS security policy recommendations to block or partially block SaaS applications. Partial blocking recommendations are supported if the application has a supported user activity, such as download, upload, and share. To initiate enforcement, web-security administrators and superusers can import and deploy the policy recommendations.



### Note

Policy recommendations follow a negative-enforcement security model that support blocking rules only. Global web-access policies are built-in by default to block high-risk applications and URL categories while enabling threat inspections for remaining allowed web-based traffic.

SaaS Security Inline has five default policy recommendations that you can enable:

- **Prevent share**—Blocks users from sharing content on a SaaS application
- **Block upload**—Blocks users from uploading content to a SaaS application
- **Block personal access**—Blocks access to personal accounts
- **Block download**—Blocks users from downloading content from a SaaS application
- **Block access**—Blocks users from accessing a specific SaaS application

Figure 17 Policy recommendations

Policy Recommendations (5)						
<input type="text" value="Search Rule Name"/>			<a href="#">Add Filter</a>		<a href="#">Reset</a>	
Synced	Name	Default	Description	Last Modified	Enabled	Actions
-	Block Access	Default	Default rule: block users from accessing unsan...		Disabled	
-	Block Download	Default	Default rule: prevent users from downloading ...		Disabled	
-	Block Upload	Default	Default rule: prevent users from uploading con...		Disabled	
-	Prevent Share	Default	Default rule: prevent users from sharing conte...		Disabled	
-	Block Personal Access	Default	Default rule: prevent users from accessing thei...		Disabled	

In addition to these default policy recommendations, you can create custom policy recommendations. For more granular controls, use custom policy recommendations that include one or more of the following:

- **Users & groups**—Block application or functional access to a subset of users and/or user groups.
- **Device posture**—Perform additional security checks based on device specific attributes.
- **Data profile**—Assign a data-security profile to block uploads of sensitive data.



#### Caution

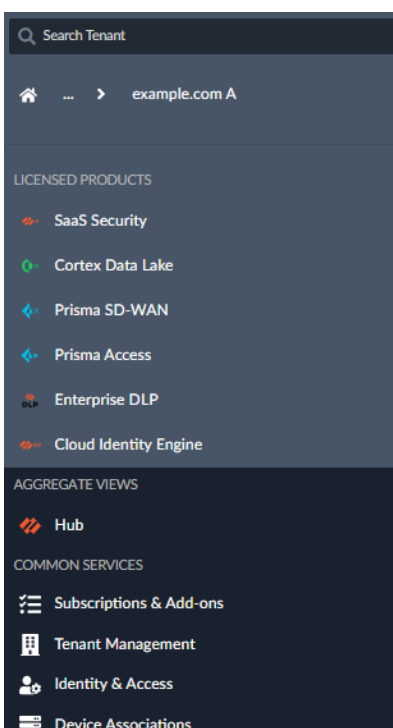
When you define a policy recommendation in SaaS Security Inline, the enforcement does not take effect immediately on Prisma Access. Instead, the policy recommendation is sent to the web-access policy recommendations page for reviewing and committing.

## Roles and Administrator Privileges

In many large organizations, the administrators responsible for configuring the security infrastructure, such as Prisma Access, might not be the same administrators monitoring and deciding which SaaS application traffic to block. NG-CASB supports this division of responsibility when controlling SaaS applications by using RBAC and the policy recommendation workflow.

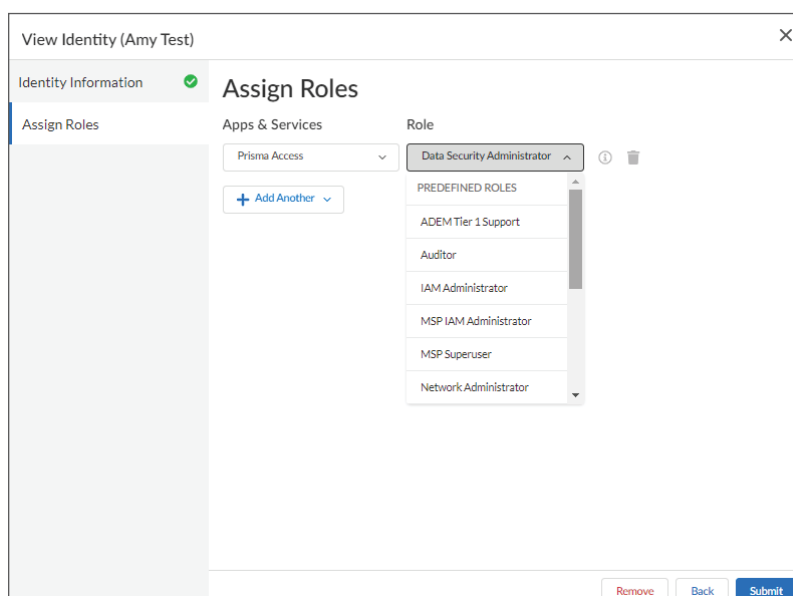
Cloud Manager provides a single cloud-based management pane that combines both Prisma Access and Prisma SD-WAN. The Prisma SASE platform supports a multitenant architecture that enables you to create and manage a hierarchy of business organizations. Common services allow license management, device associations, identity, and access controls across all tenants.

Figure 18 Common services



*Enterprise roles* are predefined sets of permissions for managing enterprise applications and services. You can assign administrator users to roles that match your organization's roles and responsibilities. For example, a data-security administrator can make policy recommendations but does not have the permissions to deploy the recommendations in Prisma Access. Supported roles include view only, superuser, security administrators, data-security administrators, and more. For a complete list of roles and associated permissions, see [About Roles and Permissions Through Common Services](#).

Figure 19 Role assignment



## Web-Security Policies

Web security is an optional policy management interface that provides a simplified and consolidated management experience for administrators who are focused on securing access to the internet and SaaS applications. This policy management interface provides a clear separation of web-security policies from the rest of the Prisma Access settings. Role-based access control can be used to restrict administrator access to only web-security policies.

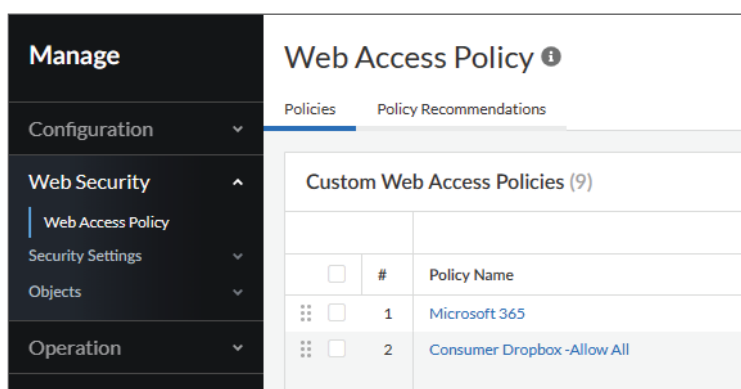
To review web-security policies, select **Prisma Access > Manage > Web Security > Web Access Policy**. The page default tab contains the web-access policies, and you use a second tab to review and deploy SaaS policy recommendations.



### Note

Policy recommendations can only be imported by using web access policies.

Figure 20 Web security



Web-security policies have built-in security rules that protect all users' web traffic with best-practices security profiles. After web security is enabled, the following are automatically enforced:

- **Decryption for all web traffic**—Decrypts all web traffic except that for which you define exclusions.
- **Threat inspection**—Protects against vulnerabilities, detects and controls C2 communication, uses WildFire® to detect unknown malware, and provides DNS security.
- **Global web access**—With all threat inspections enabled, allows all web traffic and blocks high-risk applications and URL categories.



Figure 21 Default web-access policies

Default Web Access Policies (2)								Enable	Disable
<input type="checkbox"/>	Policy Name	State	Logs	Description	Web Applications	URL Categories			
<input type="checkbox"/>	Global Web Access			Allow and Block Web Applications and URL categories for all users	High Risk Applications New Web Applications	High Risk Abused Drugs Adult Command and Control Copyright Infringement <a href="#">more...</a>			
<input type="checkbox"/>	Global Catch All Policy			Default Action for all outbound traffic to any Web Application and URL Category	any	any			

You can use custom web-access policies for creating user/user group specific policies. Some key features of web security are:

- **Consolidated policy management**—Define URL and application access policies for users and security protections, all from a single location. You apply threat-protection settings globally to all web traffic, which eliminates the need to configure them on a per-policy basis. You can easily manage SSL decryption from a central location.
- **Built-in best practices**—The ready-to-use default policy configurations adhere to Palo Alto Networks best-practice recommendations. To secure web traffic right away, simply enable web security and push the configuration. You can use the default policies as-is or customize your own.
- **Separation of roles and responsibilities**—A web-security administrator can manage web-bound traffic from the web-security policies page, while other traffic is enforced according to the policies set in the Prisma Access security policy. Web-security policies are evaluated before any other security rule.

Figure 22 Security policies evaluation sequence

Security Policy Rules (16)					<div><div><div></div></div><div>Search</div></div>	<div><div><div></div></div><div></div></div>	<div>Delete</div>	<div>Enable</div>	<div>Disable</div>	<div>Clone</div>	<div>Move</div>	<div>Add Rule</div>
<div><div></div></div>	<div></div>	<div>Name</div>	<div>BPA Verdict</div>	<div>Cleanup</div>	<div>Zone</div>	<div>Address</div>	<div>User</div>	<div>Device</div>	<div>Zone</div>	<div>Destination</div>		
<div>▼ Web Security Policies (5) ⓘ</div>												
<div><div></div></div>	<div>1</div>	<div>Web Security Policies</div>	<div><div><div></div></div><div>-</div></div>	<div>-</div>	<div><div><div></div></div><div>-</div></div>	<div><div><div></div></div><div>-</div></div>	<div><div><div></div></div><div>-</div></div>	<div><div><div></div></div><div>-</div></div>	<div><div><div></div></div><div>-</div></div>	<div>-</div>		
<div>▼ Prisma Access - Pre Rules (7)</div>												
<div><div></div></div>	<div>2</div>	<div>Drop Traffic to Known Malicious IP Addresses</div>	<div><div><div></div></div><div>Pass</div></div>	<div>Zero Hit Rule</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>		
				<div>Zero Hit Obje</div>								
<div><div></div></div>	<div>3</div>	<div>Drop Traffic to Potential High Risk IP Addresses</div>	<div><div><div></div></div><div>Pass</div></div>	<div>Zero Hit Rule</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>		
				<div>Zero Hit Obje</div>								
<div><div></div></div>	<div>4</div>	<div>Drop Traffic to Bulletproof hosting providers</div>	<div><div><div></div></div><div>Pass</div></div>	<div>Zero Hit Rule</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>		
				<div>Zero Hit Obje</div>								
<div><div></div></div>	<div>5</div>	<div>Drop Traffic from Known Malicious IP Addresses</div>	<div><div><div></div></div><div>Pass</div></div>	<div>Zero Hit Obje</div>	<div>any</div>	<div><div><div></div></div><div>panw-kno...</div></div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>		
<div><div></div></div>	<div>6</div>	<div>Drop Traffic from Potential High Risk IP Addresses</div>	<div><div><div></div></div><div>Pass</div></div>	<div>Zero Hit Obje</div>	<div>any</div>	<div><div><div></div></div><div>panw-high...</div></div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>		
<div><div></div></div>	<div>7</div>	<div>Drop Traffic from Bulletproof hosting providers</div>	<div><div><div></div></div><div>Pass</div></div>	<div>Zero Hit Rule</div>	<div>any</div>	<div><div><div></div></div><div>panw-bull...</div></div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>		
				<div>Zero Hit Obje</div>								
<div><div></div></div>	<div>8</div>	<div>Deny Quic</div>	<div><div><div></div></div><div>Pass</div></div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>	<div>any</div>		

## SECURITY FOR SANCTIONED SAAS APPLICATIONS

*Sanctioned* SaaS applications are those your organization has chosen to fulfill specific business needs. These applications are critical to the business and might host sensitive data that users can access from any device and location. For sanctioned SaaS applications, this design recommends API-based security to complement inline security for managing the security posture of the applications and securing the data stored inside them.

The process for securing sanctioned SaaS applications is as follows:

1. Configure internal domains, which are used by SaaS Security API, to identify the exposure level of shared assets
2. Review data security policy rules, adding additional rules if needed
3. Using an administrator account, onboard applications for SaaS Security API and SSPM
4. Initiate a retroactive scan of the stored assets
5. Explore discovered and quarantined assets, exposure levels, file types, and user and application ownership
6. Review and manage incidents triggered by policies
7. Review and manage SaaS configuration recommendations

### SaaS Security API

SaaS Security API is a cloud service that connects directly to sanctioned SaaS applications by using the SaaS application's API. This connection provides visibility and control over the data and activities within the application. Deploying SaaS Security API does not require deploying hardware or software on the network or endpoints. Traffic doesn't need to be steered to SaaS Security API through agents or proxy PAC file deployments. In fact, all endpoints are supported, including mobile devices and personal and partner endpoints. Because there is no added latency in using the SaaS application, the user experience of using the SaaS applications is unchanged.

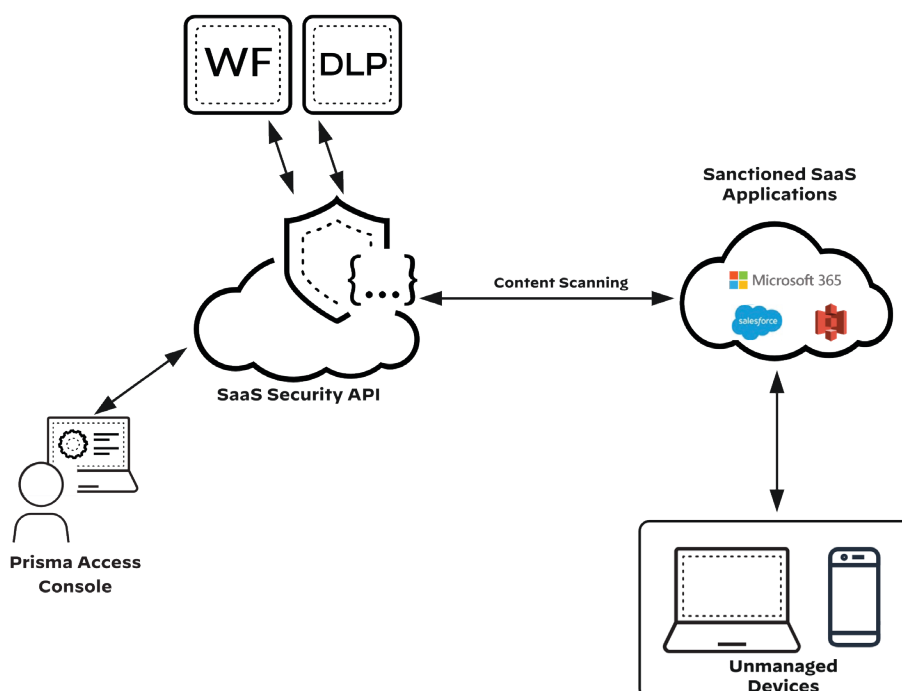
SaaS Security API is available globally and can manage multiple SaaS applications, providing consistent visibility and control across each. Within the managed SaaS application, SaaS Security API visibility and control even extend to data and activities that originate on personal devices and collaborators who aren't part of your organization.



#### Note

Supported visibility and controls are dependent on API capabilities of the individual SaaS applications.

Figure 23 SaaS Security API integration with SaaS applications



SaaS Security API connects and maintains a connection to SaaS applications without storing the administrator password. However, to configure SaaS Security API to connect, you need an administrator account in the SaaS application. When you add a SaaS application to SaaS Security API, you are asked to log in to the SaaS application as an administrator. SaaS Security API does not store the login information. Instead, the administrator account is used to grant an OAuth token to SaaS Security API, which stores the token and uses it to access the SaaS application.















### Asset Discovery and Visibility

Assets are the content stored in each cloud application. To help you uncover accidental or malicious data exposure, SaaS Security API provides visibility into the asset inventory. SaaS Security API discovers the assets stored in the cloud application, assesses the shared or exposed data within and outside your organization, and identifies the impact or risk to intellectual property and regulatory non-compliance. In addition to creating an incident and alerting the administrator, the service provides auto-remediation capabilities, including the option to quarantine, change sharing, or notify the owner.

After connecting a sanctioned application, to discover all assets inside the SaaS application, you must initiate a retroactive scan. After the initial scan, SaaS Security API continuously monitors the application and applies policy against new or modified assets (changes in permissions, location, owners, collaborators, etc.). If you modify your policies, the new policies apply only to new assets and activities in the application. To apply new policies to historical data, you must re-authenticate the application.

Giving priority to new assets and activities, the SaaS Security API policy engine evaluates the files and metadata against the rules and displays the results on the dashboard. Depending on the amount of data stored in the SaaS application, the scan of historical data and activities might take a while. All discovered assets are shown in the SaaS Security API data assets screen.

Figure 24 SaaS Security API data assets screen

All Data Assets		Quarantined Data Assets						
 Search data assets or owner		 Past 30 Days ▾	 Add Filter				Reset	
Exposure 	Data Asset Name	Data Type	Owner	Application (Instance)	Data Profile			
Internal	<a href="#">XSOAR_Document.docx</a>	 DOCX	xsoar	Office 365 Example				
Internal	<a href="#">XSOAR_Presentation.pptx</a>	 PPTX	xsoar	Office 365 Example				
Internal	<a href="#">XSOAR_Book.xlsx</a>	 XLSX	xsoar	Office 365 Example				
Internal	<a href="#">XSOAR_Private</a>		xsoar	Office 365 Example				
External	<a href="#">XSOAR_External_Share</a>		xsoar	Office 365 Example				
Public	<a href="#">XSOAR_Public_Share</a>		xsoar	Office 365 Example				
Company	<a href="#">XSOAR_Company_Share</a>		xsoar	Office 365 Example				

To find specific assets, you can use the search bar to search by asset name or owner. To identify assets with common attributes, you can use filters to narrow down the scope of the results. The following filter criteria is available to search for assets:

- Creators
- Application instance
- Exposure
- Policy
- Data profile

The detailed view of the asset summarizes file name, type, exposure, owner, and last updated. Additional detailed information on exposure, incidents, and user activity can help you monitor and investigate user activity.

Figure 25 Asset detailed view

The screenshot displays the detailed view of an asset named 'XSOAR\_Document.docx'. The interface is divided into several sections:

- DETAILS:** A list of metadata including Application (Instance) 'Office 365 Example', Exposure level 'Internal' (highlighted in red), Owner 'xsoar', Last Updated '05 Dec 2022, 01:39 PM', Malware Verdict 'Not Analyzed', and Data Type 'DOCX'. A 'Show More' link is present.
- INCIDENTS:** A table with columns: Severity, Policy, Detected, Status, and Assigned To. Below the table, a message states 'No Results Available' with a search icon.
- EXPOSURE DETAILS:** A section showing various exposure settings:
  - Expiration-date: Public-Write-URL
  - Exposed-by-parent-folder: Sign-in required
  - Password-protected-link: Vanity-link-or-Custom-URL
  - Public-Read-URL: (empty)
  - Link: [https://\[redacted\].sharepoint.com/personal/xsoar\\_test-example\\_com/\\_layouts/15/Doc.aspx?sourcedoc=%7B674E122B-1B7F-4043-B4FA-919850654562%7D&file=XSOAR\\_Document.docx&action=default&mobileredirect=true](https://[redacted].sharepoint.com/personal/xsoar_test-example_com/_layouts/15/Doc.aspx?sourcedoc=%7B674E122B-1B7F-4043-B4FA-919850654562%7D&file=XSOAR_Document.docx&action=default&mobileredirect=true)
  - Sign-In Required: Yes
- USER ACTIVITIES:** A table with columns: Date, Event, User Name, IP Address, and Location. A 'View all user activities' link is at the top right.

## Identifying Internal and External Users

SaaS Security API defines a *collaborator* as any person who can access, view, preview, download, comment, or edit a managed asset. SaaS Security API uses the defined internal domains in order to determine whether the collaborators on an asset are internal to your organization or if the owner has shared the asset with external users. SaaS Security API determines this by matching the domain name in each collaborator's email address against a defined list of internal domains. You also can configure external users and domains as trusted, which helps distinguish business partners, contractors, and other third parties who should be treated differently from generic external users.



### Note

Because SaaS Security API uses the internal domains list in order to determine the exposure level of an asset during the scan process, you must define the internal domains list before scanning cloud applications.

## Exposure Risk Assessment

Gaining visibility into how data is shared allows you to identify data that has been shared publicly, with the wrong person, or with someone who should no longer have access. Additionally, when you do identify an issue with sharing, SaaS Security API allows you to look back and see who accessed the data and when.

The exposure level describes how an asset is shared. SaaS Security API uses the following exposure levels to classify scanned assets:

- **Public**—SaaS Security API considers an asset *public* if the repository is public or if the owner created a public link, vanity URL, or password-protected link for direct access to the asset.
- **External**—The owner invited one or more users outside the organization to collaborate on the asset. These are domains that are not configured as internal domains.
- **Company**—The owner created an organization-wide URL that gives anyone in the organization direct access to the asset.
- **Internal**—This exposure level includes assets the owner has not shared. Also, it includes assets that the owner has shared but only with specific users within the organization. These users have an email address in the enterprise domain name.

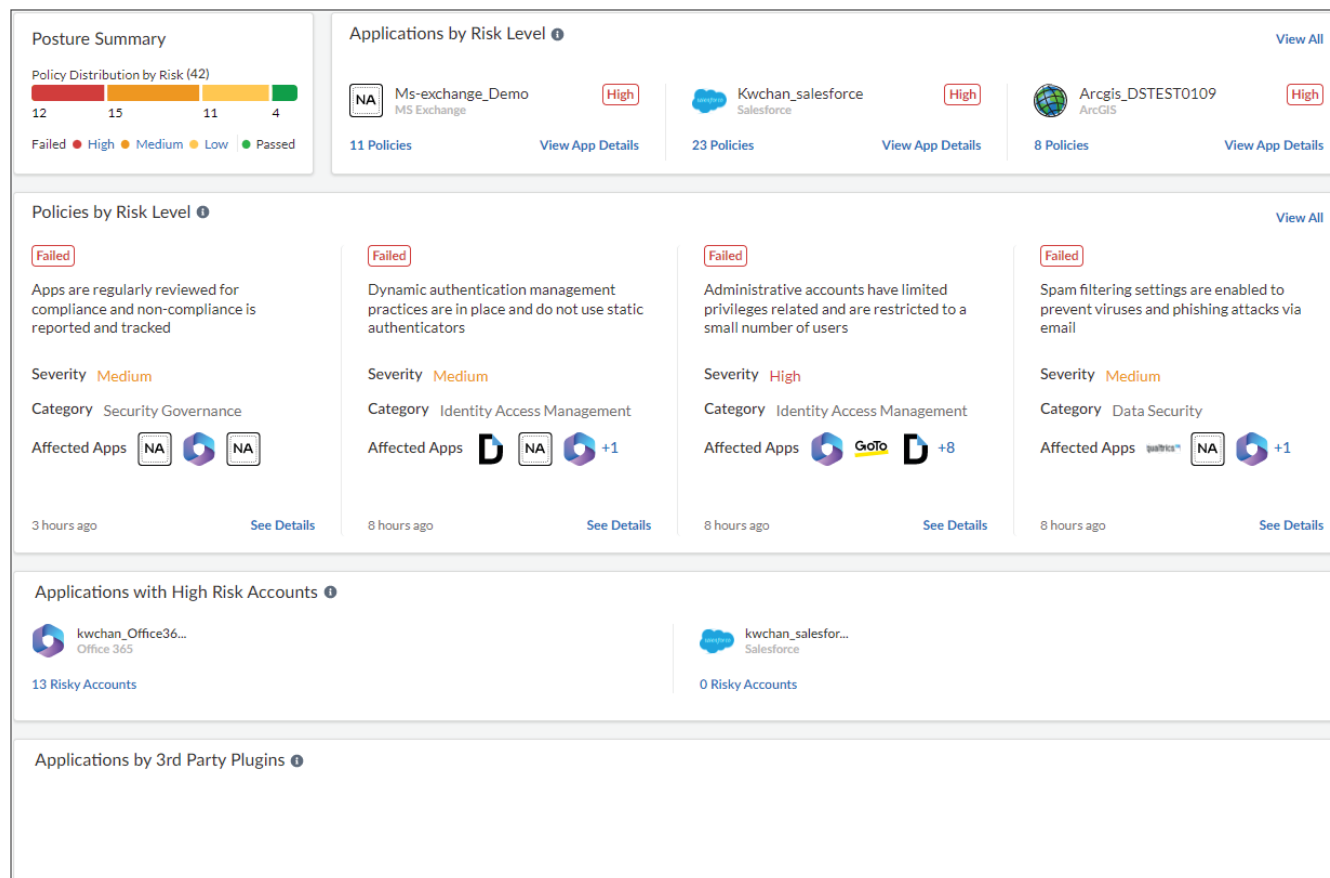
## SaaS Security Posture Management

Human misconfiguration is the most common cause of cloud breaches. The more SaaS applications used by an organization, the more difficult it is to maintain the security posture across all applications. With over 90 applications supported and growing, SSPM helps prevent data loss and reduces the risk of security breaches with the following capabilities:

- **Detection of misconfigurations**—Finds misconfigurations by using built-in best practices and categorizes misconfigurations by severity in order to help you prioritize risks.
- **Comprehensive and effortless remediation**—Provides misconfiguration alerts and the ability to remediate issues quickly across applications with one click of a button or manually using straightforward instructions. Enables you to lock a configuration so that the setting does not become a misconfiguration in the future.

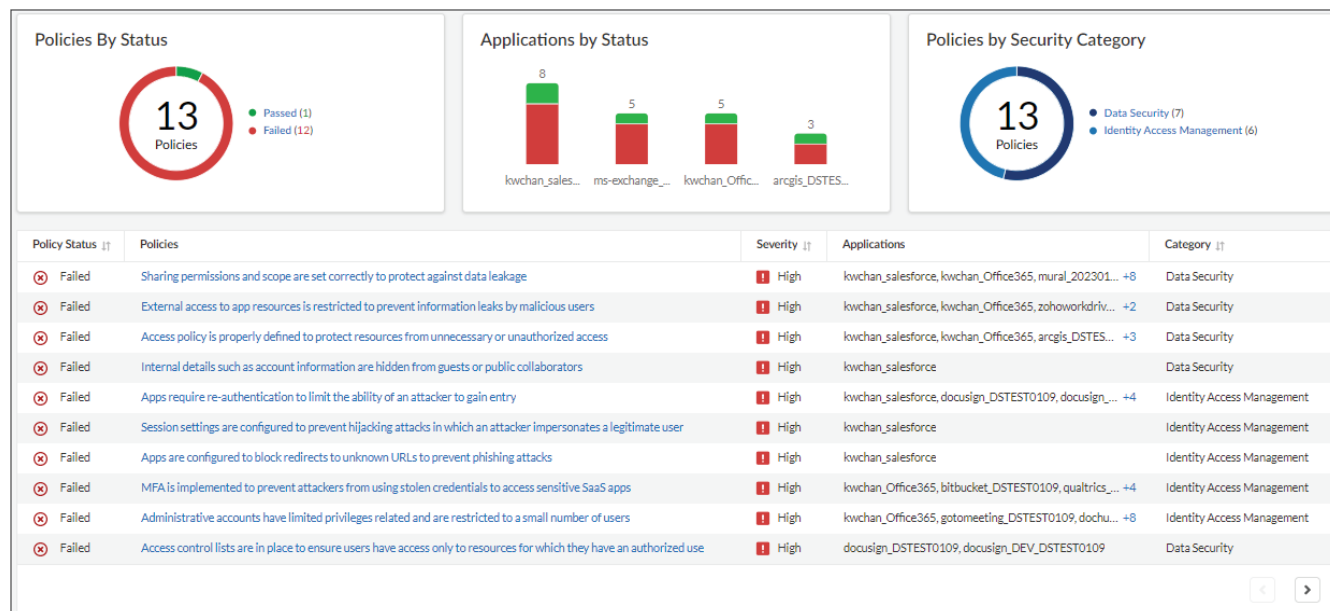
The SSPM dashboard provides a summary view that allows you to quickly identify the most critical risks. The dashboard provides information about the total number of failed policies by risk, applications with the riskiest policy violations, high-risk policy violations, and applications with high-risk accounts.

Figure 26 SSPM dashboard



The policy rules are already built-in. To reduce the alert noise and enable easy prioritization of settings that require remediation, the results of the policies are grouped by security areas and applications.

Figure 27 Policy status





Each policy provides details into how it maps to application-specific settings. Details for each application include:

- Configuration setting for each SaaS application instance
- Status of the configuration setting for each SaaS application instance
- Compliance requirement mapping to security standards
- Remediation type (manual or system)
- Links to the application site for additional reference

Figure 28 Detailed policy information

High

Apps require re-authentication to limit the ability of an attacker to gain entry

×

Policy Information

You can mitigate the amount of damage an attacker can do with stolen credentials or session tokens by forcing users to re-authenticate after a user logs out or the session expires. You can define session expiration based on things such as a user inactivity timeout, a given time of day, or a specific event.

Settings (12)

Compliance Mapping

↓

Application ⓘ	Setting Name ⓘ	Remediation Type ⓘ ⓘ	Status ⬆
kwchan_salesforce	Gmail integration users log in to Salesforce from Gmail each time their sessions expires.	Manual	Violation
docuSign_DSTEST0109	Web App Session Timeout	System	Violation
terraform_Demo	Idle Session Timeout	Manual	Violation
terraform_Demo	Remember User Session	Manual	Violation
ms-exchange_Demo	Idle session timeout	Manual	Violation
ms-office-365_Demo	Idle session timeout	Manual	Violation
ms-teams_Demo	Idle session timeout	Manual	Violation
kwchan_salesforce	Force logout on session timeout	System	Passed
kwchan_salesforce	Session timeout value	System	Passed
docuSign_DSTEST0109	Mobile App Session Timeout	Manual	Passed
docuSign_DEV_DSTEST0109	Web App Session Timeout	System	Passed
docuSign_DEV_DSTEST0109	Mobile App Session Timeout	Manual	Passed

For each of the SaaS application-specific settings, detailed information, references, and remediation instructions help you to quickly remediate the failed policies. To prevent configuration drift, SSPM performs continuous monitoring for all settings across all apps. If the best-practice settings do not align with your policies, you have the option of disabling monitoring for individual settings with application-instance granularity.

Figure 29 Detailed setting information

High

Apps require re-authentication to limit the ability of an attacker to gain entry

×

Policy Information

You can mitigate the amount of damage an attacker can do with stolen credentials or session tokens by forcing users to re-authenticate session expiration based on things such as a user inactivity timeout, a given time of day, or a specific event.

Settings (12)

Compliance Mapping

Application	Setting Name
kwchan_salesforce	Gmail integration users log in to Salesforce from Gmail each time their sessions expires.
docuSign_DSTEST0109	Web App Session Timeout
terraform_Demo	Idle Session Timeout
terraform_Demo	Remember User Session
ms-exchange_Demo	Idle session timeout
ms-office-365_Demo	Idle session timeout
ms-teams_Demo	Idle session timeout
kwchan_salesforce	Force logout on session timeout
kwchan_salesforce	Session timeout value
docuSign_DSTEST0109	Mobile App Session Timeout
docuSign_DEV_DSTEST0109	Web App Session Timeout
docuSign_DEV_DSTEST0109	Mobile App Session Timeout

Idle session timeout

Monitored

ⓘ

Status: Violation

Idle session timeout signs users automatically out of Office web apps after a period of inactivity.

[Go to admin console](#)

Current Value

60

Suggested Value

30

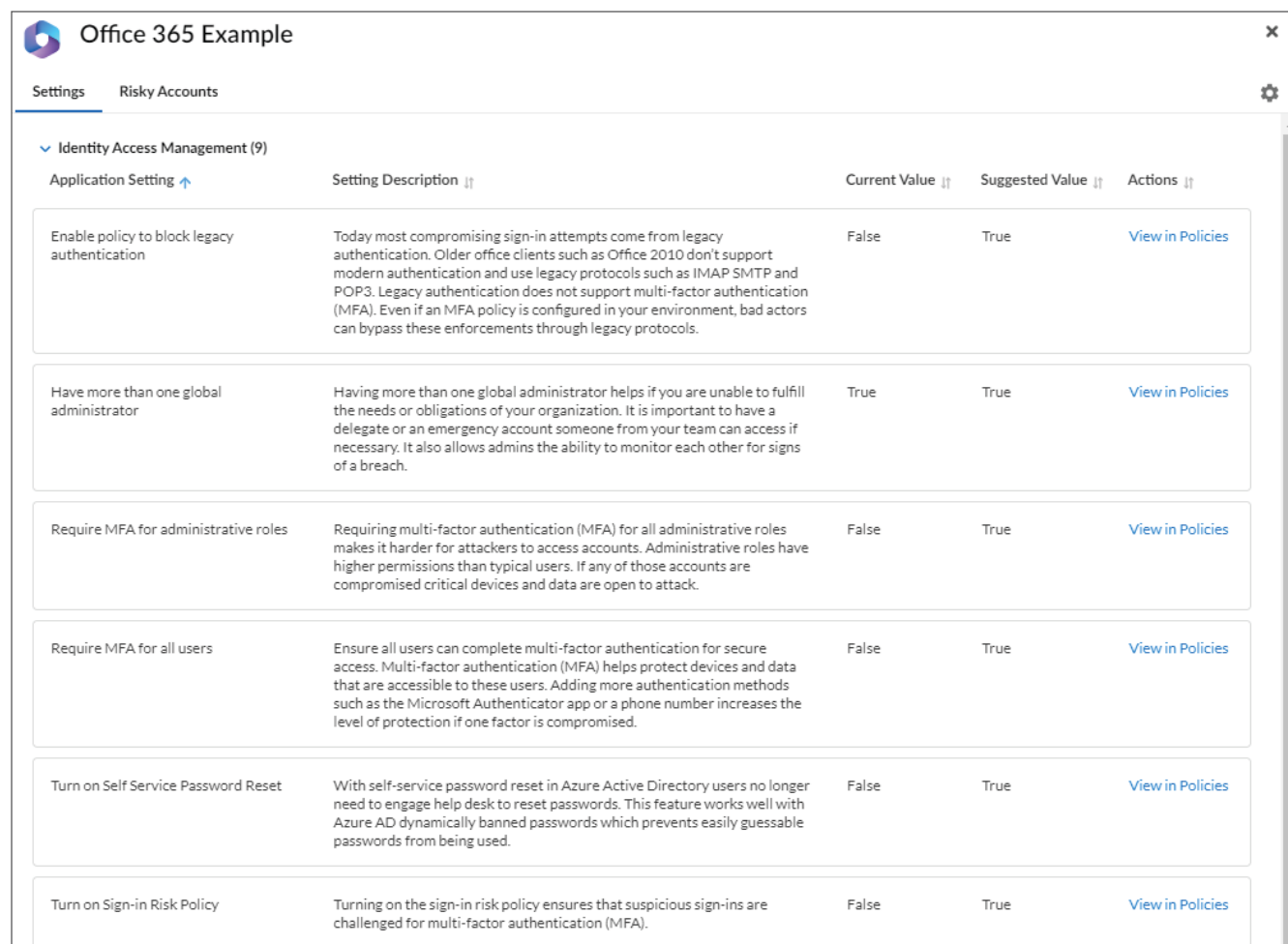
Remediation Instructions

1. Log into the application.
2. Click on the 'Admin' option from the 'Candy box' icon on the left.
3. Click on the 'hamburger' icon from the top left.
4. Click on 'Show all' from the left panel.
5. Click on 'Settings' in the left panel.
6. Click on 'Org settings' under the setting submenu.
7. Click on the 'Security & Privacy' tab.
8. Click on 'Idle session timeout'.
9. Select the checkbox for 'Turn on to set the period of inactivity for users to be signed off of Office web apps'.
10. Select the suggested value 'When do you want users signed out?' dropdown in minutes.
11. Click on the 'Save' button.

Close

SSPM provides an application-specific view that allows you to evaluate the security posture of an individual application. The application settings are organized by category and show the current value and suggested value.

Figure 30 SaaS application posture



Application Setting ↑	Setting Description ⌵	Current Value ⌵	Suggested Value ⌵	Actions ⌵
Enable policy to block legacy authentication	Today most compromising sign-in attempts come from legacy authentication. Older office clients such as Office 2010 don't support modern authentication and use legacy protocols such as IMAP SMTP and POP3. Legacy authentication does not support multi-factor authentication (MFA). Even if an MFA policy is configured in your environment, bad actors can bypass these enforcements through legacy protocols.	False	True	<a href="#">View in Policies</a>
Have more than one global administrator	Having more than one global administrator helps if you are unable to fulfill the needs or obligations of your organization. It is important to have a delegate or an emergency account someone from your team can access if necessary. It also allows admins the ability to monitor each other for signs of a breach.	True	True	<a href="#">View in Policies</a>
Require MFA for administrative roles	Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised critical devices and data are open to attack.	False	True	<a href="#">View in Policies</a>
Require MFA for all users	Ensure all users can complete multi-factor authentication for secure access. Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods such as the Microsoft Authenticator app or a phone number increases the level of protection if one factor is compromised.	False	True	<a href="#">View in Policies</a>
Turn on Self Service Password Reset	With self-service password reset in Azure Active Directory users no longer need to engage help desk to reset passwords. This feature works well with Azure AD dynamically banned passwords which prevents easily guessable passwords from being used.	False	True	<a href="#">View in Policies</a>
Turn on Sign-in Risk Policy	Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication (MFA).	False	True	<a href="#">View in Policies</a>

## Advanced Threat Protection

Advanced threat prevention capabilities for SaaS Security API help you protect against evasive malware inside SaaS applications and detect suspicious user activities associated with compromised accounts and malicious insiders.

### Malware Detection

SaaS Security API uses WildFire to detect both known and unknown malware stored in managed SaaS applications. SaaS Security API scans assets and submits files to WildFire for analysis.



#### Note

SaaS Security API does not submit any files for processing by default, and you control which file type categories apply to the WildFire service.

Figure 31 WildFire settings

WildFire Analysis

Status

☒ Enabled

Action

<input type="checkbox"/>	File to Submit	Status
<input type="checkbox"/>	Portable executable (PE, EXE)	Disabled
<input type="checkbox"/>	Microsoft Office	Disabled
<input type="checkbox"/>	Portable Document Format (PDF)	Disabled
<input type="checkbox"/>	Mac OS X	Disabled
<input type="checkbox"/>	Linux (ELF)	Disabled
<input type="checkbox"/>	Script (BAT, JS, VBS, PS1, and Shell script)	Disabled
<input type="checkbox"/>	Android application package (APK)	Disabled
<input type="checkbox"/>	Adobe Flash	Disabled
<input type="checkbox"/>	Java Archive (JAR)	Disabled
<input type="checkbox"/>	Archive (RAR and 7-Zip)	Disabled

Action

<input type="checkbox"/>	Contextual Information	Status
<input type="checkbox"/>	Cloud App	Disabled
<input type="checkbox"/>	File URL	Disabled
<input type="checkbox"/>	Timestamp	Disabled
<input type="checkbox"/>	File Directory Path	Disabled
<input type="checkbox"/>	User ID	Disabled

## Suspicious User Activity

SaaS Security API uses a combination of tools, including ML, predefined and user-defined data patterns, security configuration controls, and access to event logs auditing user access and activity on each cloud application. With these tools, it builds context on sensitive data within your environment, identifies thresholds for expected and unexpected behavior, and uses this intelligence to log a violation or alert you to risky user behavior and possible data leaks from accidental or malicious user activity.

SaaS Security API offers built-in user-activity policies like the following:

- **Risky IP**—Detects user activities from IP addresses that are deemed to be malicious. These IP addresses are determined by threat intelligence from Palo Alto Networks and reputable third-party feeds. IP addresses include Tor exit nodes and IP addresses from Bulletproof hosting providers. These services can host and distribute malicious, illegal, and unethical material.
- **Bulk Upload**—Detects users who are uploading large numbers of files or folders within a short timeframe, likely indicating malicious intent to compromise your organization's sensitive data.
- **Impossible Traveler**—Detects a user accessing an application from two different physical locations within a timeframe that would be impossible for the user to physically travel.

Figure 32 Pre-defined user-activity policies

Data Asset Policies   User Activity Policies   Security Control Policies								
<input type="text" value="Search by policy name"/> Status: Enabled <a href="#">Reset</a>								
Severity	Policy Name	Detect	Activity	Sanctioned Applications	Frequency	Status	Actions	Actions
Medium	Malware	Suspicious Activity	View, & 4 more	All		Enabled	Log Only	⋮
Medium	Bulk Sharing	Suspicious Activity	Share	All		Enabled	Log Only	⋮
Medium	Bulk Download	Suspicious Activity	Download, & 2 more	All		Enabled	Log Only	⋮
Medium	Bulk Upload	Suspicious Activity	Upload	All		Enabled	Log Only	⋮
Medium	Bulk Deletion	Suspicious Activity	Delete	All		Enabled	Log Only	⋮
Medium	Login Failure	Suspicious Activity	Failed Login	All		Enabled	Log Only	⋮
Medium	Unsafe Location	Suspicious Activity	Login	All		Enabled	Log Only	⋮
Medium	Inactive Account Access	Suspicious Activity	Login	All		Enabled	Log Only	⋮
Medium	Risky IP	Suspicious Activity	Login	All		Enabled	Log Only	⋮
Medium	Unsafe VPN	Suspicious Activity	Login	All		Enabled	Log Only	⋮
Medium	Impossible Traveler	Suspicious Activity	Login	All		Enabled	Log Only	⋮
Medium	Activities From Personal Domains	Users	Any	All	1 Day	Enabled	Log Only	⋮
High	Anonymous Access	Assets	Download, & 1 more	All	1 Month	Enabled	Log Only	⋮
High	Bulk Sharing Of Data	Users	Share	All	1 Month	Enabled	Log Only	⋮
High	Bulk Upload Of Data	Users	Upload	All	1 Month	Enabled	Log Only	⋮

Figure 33 “Risky IP” security policy

Edit User Activity Policy

Back to Policies

General

Policy Name

Risky IP

Severity

3 (Medium)

Description

Detects a user accessing an application from a suspicious IP address, as determined by an IP address that is known to be malefic by Palo Alto Networks Unit-42 research team or is a known Tor exit node or an IP address of a Bulletproof

Status

Enabled

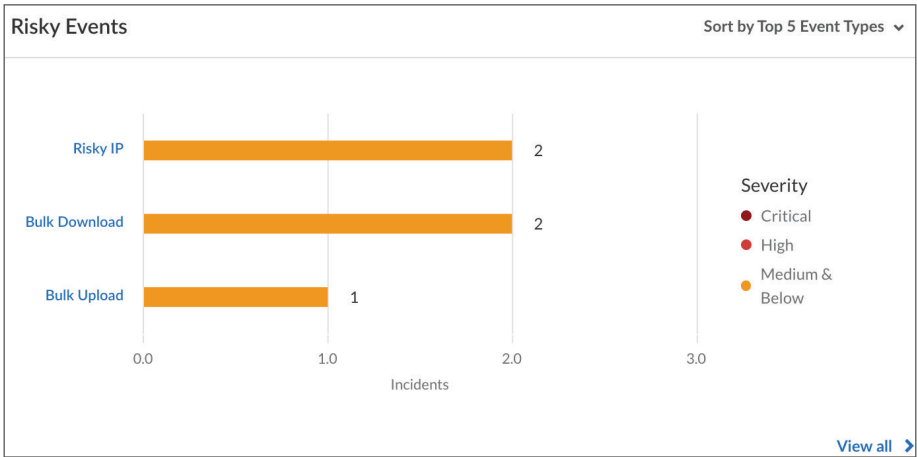
Actions

Send admin alert and log as an incident

Log as an incident only

To view the top events for user-activity policies, the SaaS Security API dashboard presents data analytics of suspicious user activities.

Figure 34 Risky events reported by SaaS Security API



Using the above information, you can drill down on any of them to find out which users have triggered the policies.

Figure 35 User-activity details matching the “Risky IP” policy

Data Asset

User Activity

Security Control

Search By Policy

Past 7 Days

Suspicious User Activity

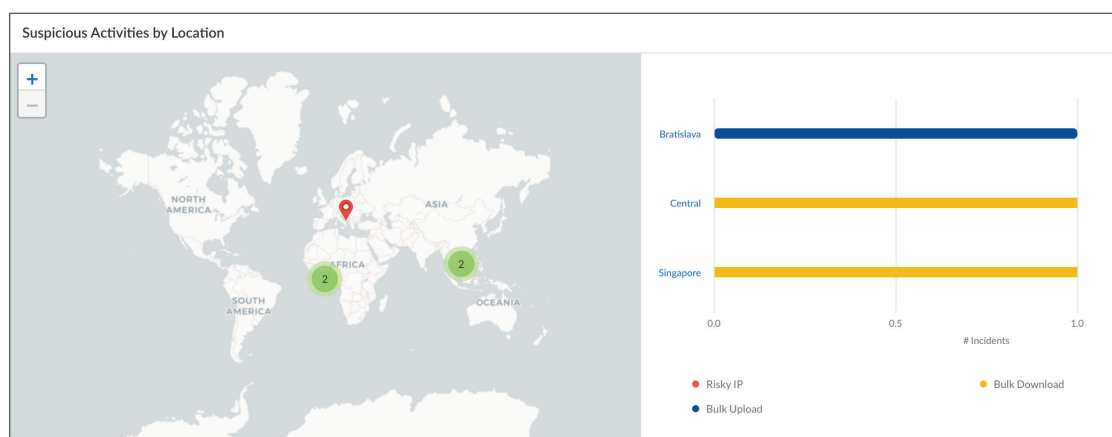
1 (Very Low), +2

Add Filter

Reset

Severity	Date Found	Policy	Target Type	Policy Type	User Activities Count	Matched Target	User Name
Medium	16 Dec 2022, 15:10 pm	Risky IP	Suspicious Activity	Suspicious User Activity	1	Nfury@Crispyprata.Com	Nick Fury
Medium	16 Dec 2022, 15:11 pm	Risky IP	Suspicious Activity	Suspicious User Activity	1	Nfury@Crispyprata.Com	Nick Fury

Figure 36 Geographic locations with suspicious user activities



## DATA SECURITY FOR ALL SAAS APPLICATIONS

To evaluate the content of data being sent to (data-in-motion) or stored (data-at-rest) in SaaS applications, the next-generation CASB solution uses Enterprise DLP. *Enterprise DLP* is a cloud-based service that is natively integrated into existing security control points, including SaaS Security Inline (Prisma Access and NGFW), SaaS Security API, and Prisma Cloud. It provides instantaneous protection for data by applying consistent data-security policies at scale.

To avoid data loss and data theft, Enterprise DLP discovers, monitors, and protects your sensitive data. The service detects sensitive data by using a combination of techniques that include regex, keywords, and ML. The service applies customizable data profiles by using Boolean logic, which provides much more granular data-matching options and accuracy than just using search patterns. The service contains 1000+ data patterns and 20+ data profiles, including profiles for GDPR, California Consumer Privacy Act (CCPA), personally identifiable information (PII), and you can create your own.

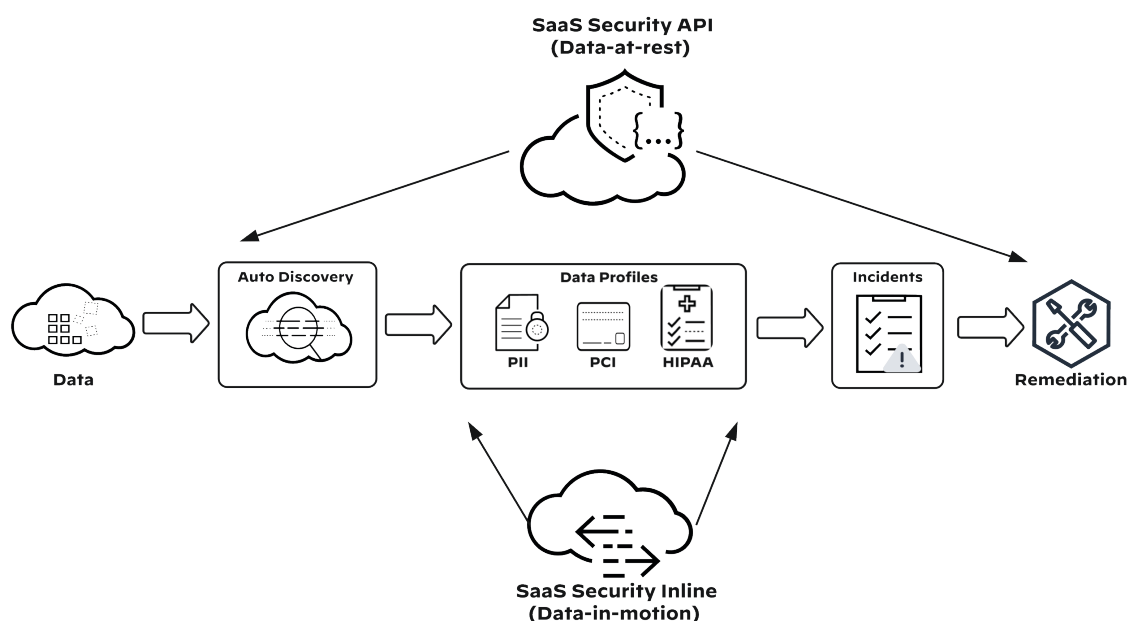
Data security is an important aspect of SaaS security, one of the key outcomes of data security is to protect sensitive data from being exposed. The design goals for SaaS data security are as follows:

- Prevent disclosure of PII
- Prevent theft of intellectual property information
- Meet compliance with external standards such as GDPR, CCPA, Payment Card Industry Data Security Standard, Health Insurance Portability and Accountability Act (HIPAA), and Sox agencies
- Protect sensitive data from malicious or well-meaning insiders

The process for securing SaaS data is as follows:

1. Identify business critical and/or PII data
2. Identify business-required regulatory compliance standards
3. Identify file types and storage locations
4. Choose data profiles based on data patterns and matching logic that meet your requirements
5. Using the data profiles identified, create data-asset policies in order to secure data stored in sanctioned SaaS applications
6. Apply data profiles identified in web-access policies in order to secure data uploads to sanctioned and tolerated SaaS applications
7. Monitor and remediate incidents

Figure 37 Data security process



## Data Types

NG-CASB supports a wide variety of applications and the most used file types, such as .csv, .json, .txt, .doc, .docx, .xls, and more. You should also evaluate the maximum supported file size. For SaaS Security API support, see [Support on SaaS Security API](#). For SaaS Security Inline support, see [What's Supported with Enterprise DLP](#).



## Detection Methods

Sensitive data is often stored or transferred in assets such as files, images, databases, and other forms where data is typically stored. To determine the presence of sensitive data, NG-CASB performs deep-scanning techniques on these assets. To that end, NG-CASB uses detection methods such as data patterns, exact data matching, and optical character recognition.

Data patterns can match API credentials, addresses from different countries, credit card numbers, Tax IDs, and many other forms of information. To identify content, the data patterns use regex, ML techniques, and proximity analysis. For instance, NG-CASB uses regex to identify addresses from different countries and ML techniques to identify legal documents. NG-CASB has more than 1000+ pre-defined data patterns that you could use individually or combined with other data patterns in order to create a data profile that is then applied to a DLP policy. When the pre-defined data patterns do not provide the required granularity, you can define custom data patterns that scan content based on regex and proximity keywords.

The second detection method is exact data matching (EDM). This capability allows NG-CASB to match exact data values for detection. With extremely high accuracy, EDM detects sensitive information (such as passwords) and PII (such as social security numbers, medical record numbers, bank account numbers, and credit card numbers) stored in a structured data source such as databases, directory servers, or structured data files (.csv and .tsv). The key difference between EDM and data patterns is that the data patterns look for sensitive information whereas EDM looks for specific information. To leverage EDM, you must create an encrypted hash of the sensitive data and upload it to the DLP engine. After sensitive data is uploaded, the DLP engine indexes the encrypted hash of uploaded EDM data sets. EDM capability supports certain file types, and there are restrictions on the size of the files. For supported data set formats, see [\*\*Supported EDM Data Set Formats\*\*](#).

OCR is the last detection method. After you enable OCR, the DLP engine scans images (such as .jpg, .jpeg, .png, .tif, and .tiff) that are embedded in container files (such as .pdf, .pptx or .docx). The DLP engine then extracts text with sensitive information and applies data profiles.

## Data Profiles

NG-CASB has built-in data profiles that include match criteria based on data patterns (such as credit card or ID numbers, financial records, GDPR, or other data privacy-related and compliance-related information), Boolean logic and match count. Both SaaS Security Inline and SaaS Security API use the data profiles to protect data. You can use the profiles as-is, or you can create your own.

Figure 38 Data profiles in NG-CASB

Data Profiles (24)					
				Search <input type="text"/>	<a href="#">Add Data Profile</a>
DATA PROFILE ▾	MODE ⚙	TYPE ⚙	LAST MODIFIED ⚙	LAST UPDATED BY ⚙	ACTIONS
Bulk CCN	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
CCPA	Predefined	Advanced	October 24, 2022, 3:31 PM EDT	System	⋮
CommonwealthAustralia-PrivAct88	Predefined	Advanced	October 24, 2022, 3:31 PM EDT	System	⋮
Corporate Financial Docs	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
Financial Information	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
GDPR	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
GLBA	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
Healthcare	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
HIPAA	Predefined	Advanced	October 24, 2022, 3:31 PM EDT	System	⋮
Intellectual Property	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
Intellectual Property - Basic	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
Legal	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
PHI	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
PHIPA	Predefined	Advanced	October 24, 2022, 3:31 PM EDT	System	⋮
PII	Predefined	Basic	October 24, 2022, 3:31 PM EDT	System	⋮
Displaying 15 results of 24				Rows <input type="text" value="15"/>	Page <input type="text" value="1"/> of 2 <input type="button" value="⏪"/> <input type="button" value="⏩"/>

## Securing Data-in-Motion

SaaS Security Inline secures data-in-motion, enabling content inspection for assets that are uploaded to both sanctioned and tolerated applications. When a user uploads an asset to any SaaS application, Prisma Access inspects the asset in-line by using the DLP data profile assigned to a web-security policy. After a DLP data profile matches, a DLP rule with the same name defines the action (alert or block), and log severity for the incident. You use the DLP incidents page to monitor information such as time, file, data profile and user associated with each incident.

## DLP for Sanctioned and Tolerated Applications

To enable DLP, you need to apply a data profile to the web-security policy. In the example shown in Figure 39, the data profile “PII-Basic” is applied, for inspecting files uploaded to Microsoft 365 through SharePoint.

Figure 39 Sample custom web-access policy

Allowed Web Applications (2)				
Explicitly allow the applications you require for enterprise use.				
<input type="text" value="Search"/> <input type="button" value="Delete"/> <input type="button" value="Set DLP"/> <input type="button" value="Add"/>				
<input type="checkbox"/>	Name	SaaS Enterprise Control	App Functions	File Control
▼	Applications (2)			
<input type="checkbox"/>	Sharepoint		<input checked="" type="checkbox"/> Admin <input checked="" type="checkbox"/> Posting(sharepoint Blog) <input checked="" type="checkbox"/> Calendar <input checked="" type="checkbox"/> Wiki	Upload: All File Types Download: All File Types
				PII - Basic

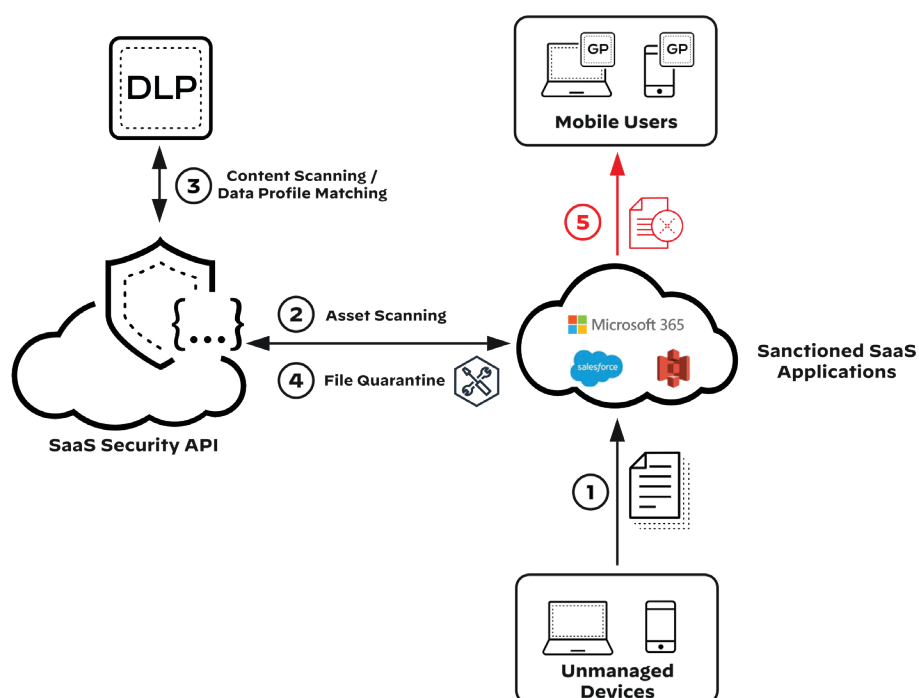
## Securing Data-at-Rest

For sanctioned SaaS applications, users can upload files from their unmanaged devices, bypassing inline protections. To protect data assets in the sanctioned SaaS applications, NG-CASB continuously scans assets by using pre-defined or custom data-asset policies. Data-asset policies detect and remediate any sensitive information present in SaaS stored assets. The data-asset policies can not only generate alerts but also can take auto-remediate actions.

The following sequence describes how NG-CASB can quarantine a sensitive file uploaded from an unmanaged device:

1. A user mistakenly uploads sensitive information to a SaaS application.
2. SaaS Security API discovers the file during asset scanning.
3. SaaS Security API sends the file to Enterprise DLP for content scanning and matching configured data profiles.
4. SaaS Security API quarantines the file according to the configured data-asset policy.
5. Mobile or branch office users are prevented from accessing the quarantined file.

Figure 40 Securing data-at-rest



## Data-Asset Policy Definition

For scanning content and assessing risk, NG-CASB includes default data-asset policies profiles. The data-asset policies match on existing data profiles and define actions for notifications and incident creation. Some of the built-in asset policies include the following:

- **Intellectual Property**—Scans files for RSA and AWS secret keys and confidential documents that are at risk of being stored or shared in a way that could result in a loss of intellectual property.
- **Financial Information**—Scans for financial data including credit card numbers, credit card magnetic stripe data, international bank account numbers, financial accounting, bank statements, personal finance, invoices, and other financial documents. By default, the SaaS Security API performs strict checking on credit card numbers in order to reduce false positives.
- **PII Compliance**—Scans for PII data, such as U.S., Canadian, and international social security numbers. It also scans for Tax IDs from the U.S., Australia, Canada, Germany, and the UK for both the Unique Taxpayer Reference and National Insurance Number formats. For each type of personally identifiable information for which SaaS Security API scans, you can specify the minimum number of occurrences required to trigger a match. As the number of violations for a specific asset exceeds the specified threshold, the severity of the risk increases.
- **Healthcare Information**—Scans healthcare documents for exposure to sensitive or confidential information, related to Clinical Laboratory Improvement Amendments number, Drug Enforcement Administration number, and other healthcare documents. SaaS Security API uses ML to classify information and to detect sensitive information.
- **Legal Information**—Scans legal documents for exposure to sensitive or confidential information related to bankruptcy filings, lawsuits, business agreements, mergers and acquisition information, patents, and other legal documents. SaaS Security API uses ML to classify information and to detect sensitive information.
- **Sensitive Credentials**—Scans for key words, phrases, or regex strings that match a specific pattern or character combination. For example: **imported-openssh-key** or **-----BEGIN RSA**

Figure 41 Built-in data-asset policies

Data Asset Policies							
User Activity Policies							
Security Control Policies							
<input type="text" value="Search by policy name"/> <span>Status: Enabled</span> <span>Reset</span>							
Severity	Policy Name	Exposure	Sanctioned Applications	Status	Actions	Mode	Actions
Critical	Risky Untrusted Sharing	external	-	Enabled	Create Incident	Basic	⋮
Critical	Bulk CCN	public, & 1 more	-	Enabled	Create Incident	Basic	⋮
Critical	WildFire	All	-	Enabled	Create Incident	Basic	⋮
High	U.K. PIOC	public, & 2 more	-	Enabled	Create Incident	Basic	⋮
High	GLBA	public, & 2 more	-	Enabled	Create Incident	Basic	⋮
High	PCI-DSS	public, & 2 more	-	Enabled	Create Incident	Basic	⋮
High	HIPAA	public, & 2 more	-	Enabled	Create Incident	Basic	⋮
High	Intellectual Property	public, & 2 more	-	Enabled	Create Incident	Basic	⋮
High	PII	public, & 2 more	-	Enabled	Create Incident	Basic	⋮

You can also create custom data-asset policies using built-in or custom data patterns and profiles. The data-asset policies are DLP rules that can match on cloud application, exposure, asset type, and data profile. After you create a policy, when the data matches the policy, the action could be to create an incident or take any of the following auto-remediation actions:

- Quarantine
- Change sharing
- Notify file owner

**Figure 42** Custom data-asset policy

### Add Data Assets Policy

[← Back to Policies](#)

#### General

Policy Name

Severity  
1 (Very Low)

Description (Optional)

Status  
☒ Disabled

#### Match Criteria

☐ Cloud Apps  
☐ Exposure  
☐ File Extension  
☐ Account  
☐ Activity  
☐ Asset Name  
☐ Data Pattern/Data Profile  
☐ File Hash(SHA256)  
☐ Owner  
☐ Trust States

#### Action

Basic Action

☐ Send admin alert and log as an incident  
 ☐ Log as an incident only

☐ Alert end-user(Configure [Workflow Settings](#) and enable proactive training to enable Slack bot notifications)

Autoremediate Actions

None

## Data Security-Control Policy Definition

To monitor rules in email applications, SaaS administrators can create security-control policies. When enabled, certain rules can cause data leakage to the outside world. For instance, if there are public email folders in an application, then users in the same organization (or sometimes belonging to different organizations) can access it. Having visibility into the existence of such folders reduces the risk of exposure.

By default, SaaS Security API provides the following policies:

- **Public Folders in Email**—This policy checks whether there are public folders present in email.
- **High Risk Email Forwarding Rules**—This policy checks whether there are any rules that forward emails to high-risk email groups.
- **Administrative Access of End Users Inbox**—This policy checks whether an email administrator has access to end-user email boxes.

Figure 43 Built-in security-control policies

Data Asset Policies   User Activity Policies <b>Security Control Policies</b>					
<input type="text" value="Search by policy name"/>		Status: Enabled ▾		Reset	
Severity	Policy Name	Sanctioned Applications	Status	Actions	Actions
⚠ Medium	Public Folders In Email	All	✔ Enabled	Log Only	⋮
✖ Critical	High Risk Email Forwarding Rules	All	✔ Enabled	Log Only	⋮
⚠ Medium	Administrative Access Of End Users Inbox	All	✔ Enabled	Log Only	⋮

# Deployment Details

This section illustrates how you can deploy NG-CASB. You should adjust SaaS security policies and DLP profiles to your organization's business needs, data privacy requirements, and security requirements. For information about capabilities per application, see the [SaaS Security Administrator's Guide](#).

## ASSUMPTIONS AND PREREQUISITES

These procedures assume that you have deployed your Prisma Access infrastructure (as described in [SASE for Securing Internet: Deployment Guide](#)) and activated all required licenses for NG-CASB.

The Prisma Access deployment should consist of the following:

- Cloud-managed Prisma Access 4.0 preferred release
- A Business premium or Enterprise license for Prisma Access
- NG-CASB bundle for Prisma Access
- Web-security management
- GlobalProtect network security clients on endpoints

## DEPLOYING SECURITY FOR ALL SAAS APPLICATIONS

For all SaaS applications, this design recommends inline security for the following:

- **Visibility and control**—Unsanctioned applications are completely blocked. Tolerated applications can be restricted by user, user group, and/or functionality.
- **Data loss prevention**—DLP monitors and controls uploads of sensitive data to SaaS applications.
- **Threat protection**—Threat protection inspects all SaaS traffic for vulnerability exploits, malware, spyware, C2 communication, and even unknown threats.

### Procedures

#### Configuring SaaS Usage Visibility and Reporting

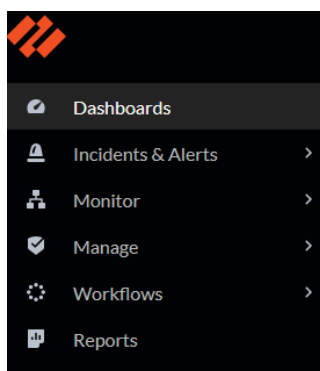
- 1.1 Access Cloud Manager
- 1.2 Configure Global Risk Scores
- 1.3 Tag Discovered SaaS Applications
- 1.4 Generate SaaS Security Report



To identify your policy needs, you must first have visibility into SaaS applications usage and identify the associated risks. To assess your SaaS security posture and maintain policies, ongoing reporting is required.

## 1.1 Access Cloud Manager

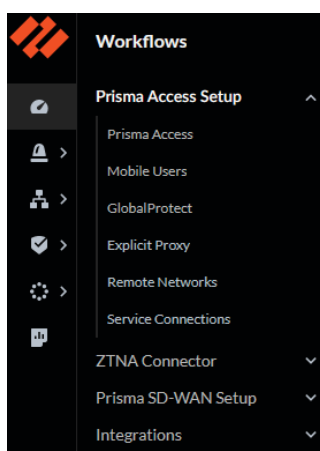
Strata Cloud Manager provides a single management pane that combines both Prisma Access and Prisma SD-WAN tasks. In Cloud Manager, you use the left panel to navigate to specific Prisma Access and Prisma SD-WAN functions. If the left panel is collapsed, to see the text labels that describe each function, you can expand it by clicking the chevron at the bottom of the left panel.



For effective navigation within Cloud Manager, familiarize yourself with the icons. You access initial setup tasks using Workflows functions. After the initial setup is complete, you access most operational tasks by using Manage functions.

**Step 1:** Log in to Cloud Manager.

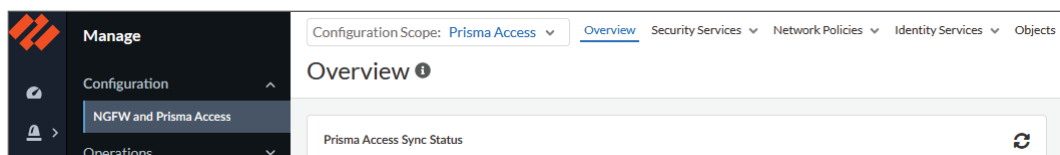
**Step 2:** Familiarize yourself with Cloud Manager, and then click **Workflows**. The left panel collapses.



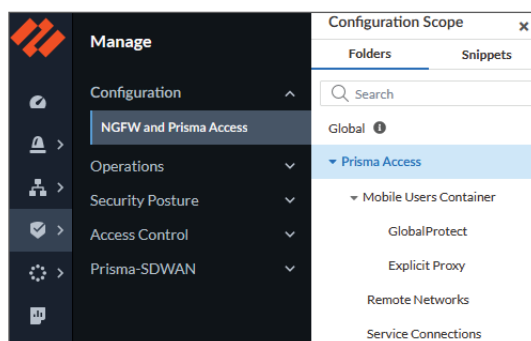
When using Manage functions for Prisma Access, Cloud Manager uses inheritance to maintain certain configuration parameters. Settings you make at a higher level configuration scope (Prisma Access), are also available as read-only within lower level scopes (example: GlobalProtect and Service Connections). Each time you start a session with Cloud Manager, your configuration scope is set to the scope selected in

the previous session. If you choose a different configuration scope, Cloud Manager maintains this choice across all configuration screens that rely on a configuration scope. To simplify access to the configuration scope pane, you can pin it and make it persistent. All following procedures in this guide assume that you have pinned the configuration scope pane. By default, Cloud Manager uses the Folders tab, which allows you to select configuration scopes for Prisma Access. For all procedures, this guide assumes you choose scopes from the Folders tab. You do not use the Snippets tab in this guide.

**Step 3:** Continuing in Cloud Manager, click **Manage > Configuration > NGFW and Prisma Access**. The Overview pane appears.



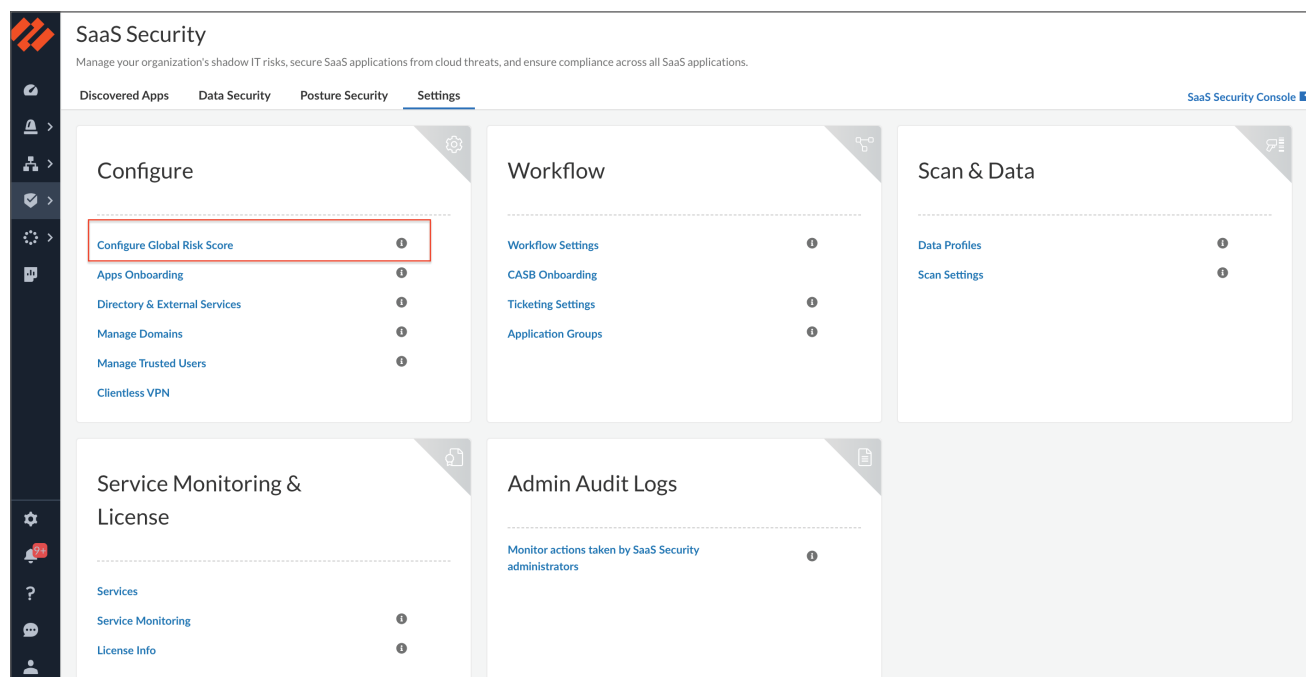
**Step 4:** To pin the Configuration Scope pane to the left, click in the Configuration Scope box, and then click the thumbtack. The Configuration Scope now remains visible in this position for all configuration screens.



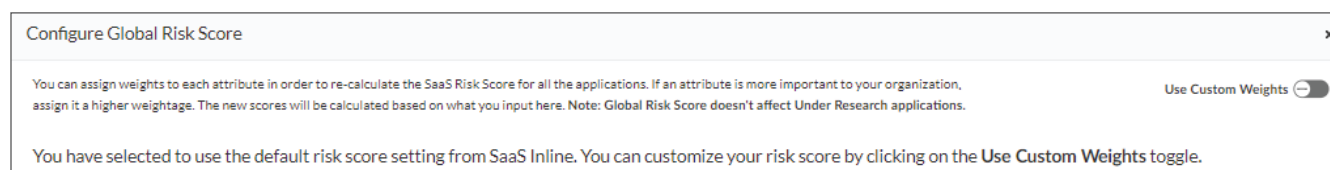
## 1.2 Configure Global Risk Scores

SaaS Security Inline helps determine which applications pose a risk by assigning each a risk score. This risk score is based on security, privacy, identity access management, and compliance attributes of the SaaS application. In this procedure, you adjust the weights of the attributes to recalculate the risk score of all SaaS applications in order to align the risk score with your organization's security requirements.

Navigate to **Manage > Configuration > SaaS Security > Settings**, and then click **Configure Global Risk Score**.



**Step 1:** On the Configure Global Risk Score dialog box, enable **Use Custom Weights**.



**Step 2:** Adjust the weights of the assigned attributes to your preferences. The total number assigned must equal 100.

Configure Global Risk Score

You can assign weights to each attribute in order to re-calculate the SaaS Risk Score for all the applications. If an attribute is more important to your organization, assign it a higher weightage. The new scores will be calculated based on what you input here. Note: Global Risk Score doesn't affect Under Research applications.

☒ Use Custom Weights

Your risk weighting: 100  
This number has to equal 100.

Set All Fields to Zero

Security and Privacy

Data Retention	2	Encryption at Rest	5	File/Content Sharing	5
Audit Log	25	Encryption in Transit	6	Data Ownership	2
HTTP Security Headers	25	Terms and Conditions	1	Native Data Classification	25
Privacy Policy	1	Disaster Recovery	3		
Third Party Data Sharing	2	Session Timeout	25		

Identity Access Management

RBAC	4
MFA	6
Password Policy	6
SAML	4
IP Based Restrictions	3

Compliance

The new scores will impact all applications.

Cancel

Save

**Step 3:** Click Save.

**Step 4:** On the SaaS Risk Weight Modification message, click Yes.

## 13 Tag Discovered SaaS Applications

To facilitate monitoring and enable accurate reporting, you assign tags to discovered applications. In this procedure, you tag the discovered applications to one of the following:

- Sanctioned
- Tolerated
- Unsanctioned

You can modify the discovered applications table by using sort and filtering functions to display the most important attributes for your organization. In environments that have many unclassified applications, sorting by users and usage allows you to prioritize the tagging of the most-used applications by users or volume.

**Step 1:** In **Manage > Configuration > SaaS Security > Discovered Apps > Applications**, in the Applications pane, click the arrow in the Users column.

Change Risk Score ▾		Bulk Tag ▾											
<input type="checkbox"/>	Application Name ⌵	Risk ⌵	Category ⌵	Rules	Tag ⌵	Users ⌵	Usage ⌵	Upload ⌵	Actions				
<input type="checkbox"/>	Box	7	Content Management	3	U	3127		77.78 GB	⋮				
<input type="checkbox"/>	Dropbox	7	Content Management	0	S	2979	264.74 GB	78.83 GB	⋮				
<input type="checkbox"/>	AccuRanker	10	Marketing	0	T	2675	170.52 GB	57.87 GB	⋮				
<input type="checkbox"/>	AWS Shield	2	Security	0	S	2545	187.58 GB	67.39 GB	⋮				
<input type="checkbox"/>	WeTransfer	8	Content Management	0	S	2286	149.77 GB	63.32 GB	⋮				

**Step 2:** Click **Add Filter**, and then select **Tags**.

Applications (394)

Past 90 Days ▾

⚙ Add Filter

Reset

**Step 3:** In the **Tags** list, select **Unknown**.

Applications (394)

Past 90 Days ▾

Tags ^

⚙ Add Filter

Applications by Risk

394 Total Apps

High (8 - 10)

Medium (4 - 7)

Low (1 - 3)

☐ Select All (4 results)
 ☐ Sanctioned
 ☐ Tolerated
 ☐ Unsanctioned
 ☒ Unknown

**Step 4:** Select a single or a group of applications that you want to assign the same SaaS adoption usage level, and then click **Bulk Tag**.

Change Risk Score ▾		Bulk Tag ▴								↺	📄	⬇
<input type="checkbox"/>	Application Name	Sanctioned	Tolerated	Unsanctioned	Unknown	Category	Rules	Tag	Users	Usage	Upload	Actions
<input type="checkbox"/>	DigitalOcean Spa					IT Infrastructure	0	●	1514	92.65 GB	46.57 GB	⋮
<input type="checkbox"/>	Pinterest					Collaboration & Productiv...	0	●	1366	82.37 GB	42.72 GB	⋮
<input type="checkbox"/>	Blockly					Development	0	●	684	31.32 GB	21.88 GB	⋮
<input type="checkbox"/>	Chrome Mobile DevTools				7	Development	0	●	609	27.90 GB	20.08 GB	⋮
<input type="checkbox"/>	Google App Maker				6	Development	0	●	453	19.66 GB	14.59 GB	⋮
<input type="checkbox"/>	Abara LMS				7	HR	0	●	147	10.47 GB	5.09 GB	⋮
<input checked="" type="checkbox"/>	VL OMNI				10	Commerce	0	●	29	538.15 MB	412.75 MB	⋮
<input type="checkbox"/>	Google Cloud Dataproc				4	IT Infrastructure	0	●	23	686.01 MB	495.71 MB	⋮
<input type="checkbox"/>	Artivatic				9	Artificial Intelligence	0	●	23	890.27 MB	691.54 MB	⋮
<input checked="" type="checkbox"/>	ChatSupport				10	Customer Service	0	●	21	653.27 MB	494.55 MB	⋮

**Step 5:** In the **Bulk Tag** list, choose the appropriate tag for your organization (example: Unsanctioned).

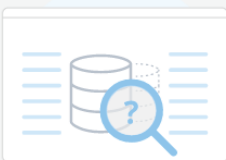
**Step 6:** Repeat Step 4 through Step 5 until all unknown applications have been tagged.

## 1.4 Generate SaaS Security Report

The SaaS security report provides visibility into the SaaS application usage. You should generate this report as part of regular security audits.

**Step 1:** Navigate to **Manage > Configuration > SaaS Security > Discovered Apps > Reports**.






**Step 2:** On the Discovered Apps tab, in the SaaS Security Reports pane, click **Generate Report**.

SaaS Security Reports (0)				↺	📄	Generate Report ▾
Report	Generated By	Date	Actions			
<div>  <p>No Results Available</p> </div>						
Displaying 0 results of 0 <div>             Rows 10 ▾             Page 1 ▾ of -             &lt; &gt;           </div>						

**Step 3:** In the **Generate Report** list, select the duration of the report (example: 7, 30, or 90 days).

**Step 4:** Click the generated report that you want to download and review.

**Step 5:** You also receive an email notification with download instructions.

SaaS Security Reports (1)				  Generate Report ▾
Report ⓘ	Generated By ⓘ	Date ↓	Actions	
 2023-01-06 SaaS Security Report - Last 90 days		06 Jan 2023 14:06:47 UTC	 Delete	

## Procedures

### Blocking Unsanctioned SaaS Applications

- 2.1 Enable Web-Security Management
- 2.2 Create New Policy Recommendation for Blocking Unsanctioned Applications
- 2.3 Import and Deploy New Policy Recommendation
- 2.4 Update Policy Recommendation for Blocking Unsanctioned Applications
- 2.5 Import and Deploy Updated Policy Recommendation

After gaining visibility into the applications being used, who is using them, and the risks associated with them, you can establish controls for accessing SaaS applications. In this design, unsanctioned applications are completely blocked.

As new applications are discovered and tagged, you can update the unsanctioned application policy by repeating these procedures.

#### 2.1 Enable Web-Security Management

Web Security management integrates with SaaS Security Inline in order to deploy policy recommendations.

**Step 1:** To enable Web Security for GlobalProtect, in the Cloud Manager, navigate to **Manage > Configuration > NGFW and Prisma Access**, and in the Configuration Scope pane, click **GlobalProtect**.

**Step 2:** In the Web Security pane, click **Enable**.

**Step 3:** On the Enable Web Security message, click **Enable**.

**Step 4:** Click **Push Config**, and then click **Push**.

**Step 5:** In the Push dialog box, enter a description, select **Prisma Access**, and then click **Push**.

	Container	Labels
<input checked="" type="checkbox"/>	Global	
<input checked="" type="checkbox"/>	Prisma Access	
<input checked="" type="checkbox"/>	Mobile Users Container	
<input checked="" type="checkbox"/>	GlobalProtect	
<input checked="" type="checkbox"/>	Explicit Proxy	
<input checked="" type="checkbox"/>	Remote Networks	
<input checked="" type="checkbox"/>	Service Connections	

**Step 6:** If you want to enable Web Security for Explicit Proxy, navigate to **Manage > Configuration > NGFW > Prisma Access > Overview**, and then in the Configuration Scope pane, select **Explicit Proxy** and repeat Step 2 to Step 5.

**Step 7:** If you want to enable Web Security for Remote Networks, navigate to **Manage > Configuration > NGFW > Prisma Access > Overview**, and then in the Configuration Scope pane, select **Remote Networks** and repeat Step 2 to Step 5.

## 2.2 Create New Policy Recommendation for Blocking Unsanctioned Applications

In this procedure, the SaaS administrator creates a new policy recommendation for blocking unsanctioned tagged applications. In Procedure 2.3, the web-security administrator deploys the policy recommendation.

**Step 1:** Navigate to **Manage > Configuration > SaaS Security > Discovered Apps > Policy Recommendations**.

**Step 2:** In the Policy Recommendations pane, click **Block Access**.

Policy Recommendations (5)						
<input type="text" value="Search Rule Name"/>			<a href="#">Add Filter</a>		<a href="#">Reset</a>	
Synced	Name	Default	Description	Last Modified	Enabled	Actions
-	Block Access	Default	Default rule: block users from accessing unsan...		Disabled	⋮
-	Block Download	Default	Default rule: prevent users from downloading ...		Disabled	⋮
-	Block Upload	Default	Default rule: prevent users from uploading con...		Disabled	⋮
-	Prevent Share	Default	Default rule: prevent users from sharing conte...		Disabled	⋮
-	Block Personal Access	Default	Default rule: prevent users from accessing thei...		Disabled	⋮



**Step 3:** In the Basic Information pane, click **Enabled**.

Basic Information

Default

Rule Name

Block Access

Enter a unique rule name (Ex: Block Unsanctioned Apps from HR).

Description (optional)

Default rule: block users from accessing unsanctioned SaaS apps.

64/72

Status

☒ Enabled
 ☐ Disabled

**Step 4:** In the Select Application pane, enable **View Selected Applications**. You should see all applications.

Select Application (53,395)

View Selected Applications

Search Application Name or Category

Add Filter

Reset

	Application ↑	Category ↓	Risk ↓	Application Capabilities	Tag ↓
<input type="checkbox"/>	000webhost	Hosting	9		
<input type="checkbox"/>	Opatch	Vertical Industry	10		
<input type="checkbox"/>	Oxcareer	Vertical Industry	10		
<input type="checkbox"/>	1000Minds Decision-Making Software	Collaboration & Productivity	9		
<input type="checkbox"/>	100AM	Marketing	10		
<input type="checkbox"/>	100mentors	Collaboration & Productivity	10		
<input type="checkbox"/>	100ms	Collaboration & Productivity	10		
<input type="checkbox"/>	100Plus	Vertical Industry	10		
<input type="checkbox"/>	100WebSpace	Hosting	10		

Displaying 10 results of 53,395

Rows

10

Page

1

of 5340

**Step 5:** Click **Add Filter**.







**Step 6:** In the **Add Filter** list, select **Tags**.

**Step 7:** In the **Tags** list, select **Unsanctioned**.

**Step 8:** Select all unsanctioned applications, and then click **Save**.

Select Application (11) View Selected Applications

Search Application Name or Category U Unsanctioned Add Filter Reset

<input checked="" type="checkbox"/>	Application ↑	Category ↑	Risk ↑	Application Capabilities	Tag ↑
<input checked="" type="checkbox"/>	101 Blockchains	Vertical Industry	10		U
<input checked="" type="checkbox"/>	33Across	Digital Advertising	10		U
<input checked="" type="checkbox"/>	Dianomi	Marketing	10		U
<input checked="" type="checkbox"/>	Iterate	Office	10	 	U
<input checked="" type="checkbox"/>	Kimola Analytics	Marketing	10		U
<input checked="" type="checkbox"/>	MachineryHost	Marketing	10		U
<input checked="" type="checkbox"/>	Meetup Pro	Marketing	10		U
<input checked="" type="checkbox"/>	Quora	Collaboration & Productivity	10	 	U
<input checked="" type="checkbox"/>	RetentionEngine	Customer Service	10		U

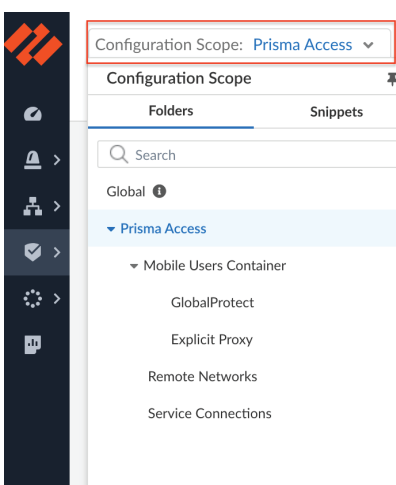
Displaying 10 results of 11

Rows 10 Page 1 of 2

## 2.3 Import and Deploy New Policy Recommendation


In this procedure, the web-security administrator imports the recommended policy into web security in order to deploy and enforce it.

**Step 1:** Navigate to **Manage > Configuration > NGFW and Prisma Access**, and in the Configuration Scope pane, click **Prisma Access**.



**Step 2:** Navigate to **Security Services > Web Security > Policy Recommendations**.

**Step 3:** In the New SaaS Rule Recommendations pane, in the Actions column, click the import icon.

New SaaS Rule Recommendations (1)			
Name	Description	Last Updated	Actions
Block Access	Default rule: block users from accessing unsanctioned SaaS apps.	2023-Jan-06 11:08:51 EST	

**Step 4:** In the Imported Tolerated SaaS Apps dialog box, select the desired order for the rule, and then click **Import**.

Import Tolerated SaaS Apps

Import Rule Name

Block Access

RULE ORDER

☒ Top
 ☐ Bottom
 ☐ Before Rule
 ☐ After Rule

\* Required Field

Cancel

Import

**Step 5:** On the Success message, click **Close**.

**Step 6:** Verify that the rule appears in the Imported SaaS Rule Recommendations pane.

**Step 7:** Click **Push Config**, and then click **Push**.

**Step 8:** In the Push dialog box, enter a description, and then click **Push**.

## 2.4 Update Policy Recommendation for Blocking Unsanctioned Applications

In this procedure, the SaaS administrator updates an existing policy recommendation to block additional unsanctioned tagged applications. In Procedure 2.5, the web-security administrator deploys the new policy recommendation.

**Step 1:** Navigate to **Manage > Configuration > SaaS Security > Discovered Apps > Policy Recommendations**, and then click **Block Access**.

Policy Recommendations (5)							Add Policy
<input type="text" value="Search Rule Name"/>		Add Filter		Reset			
Synced	Name	Default	Description	Last Modified	Enabled	Actions	
-	Block Download	Default	Default rule: prevent users from downloading ...		Disabled		
-	Block Upload	Default	Default rule: prevent users from uploading con...		Disabled		
-	Prevent Share	Default	Default rule: prevent users from sharing conte...		Disabled		
✓	Block Personal Access	Default	Default rule: prevent users from accessing thei...	06 Jan 2023, 16:08:51 UTC	Enabled		
✓	Block Access	Default	Default rule: block users from accessing unsan...	06 Jan 2023, 14:36:47 UTC	Enabled		

**Step 2:** In the Select Application pane, enable **View Selected Applications**. You should see all applications.

Select Application (53,395)						View Selected Applications
<input type="text" value="Search Application Name or Category"/>		Add Filter		Reset		
<input type="checkbox"/>	Application	Category	Risk	Application Capabilities	Tag	
<input type="checkbox"/>	000webhost	Hosting	9			
<input type="checkbox"/>	Opatch	Vertical Industry	10			
<input type="checkbox"/>	Oxcareer	Vertical Industry	10			
<input type="checkbox"/>	1000Minds Decision-Making Software	Collaboration & Productivity	9			
<input type="checkbox"/>	100AM	Marketing	10			
<input type="checkbox"/>	100mentors	Collaboration & Productivity	10			
<input type="checkbox"/>	100ms	Collaboration & Productivity	10			
<input type="checkbox"/>	100Plus	Vertical Industry	10			
<input type="checkbox"/>	100WebSpace	Hosting	10			
<div> Displaying 10 results of 53,395 </div> <div> Rows 10 Page 1 of 5340 </div>						







**Step 3:** Click **Add Filter**, and then in the **Add Filter** list, select **Tags**.

**Step 4:** In the **Tags** list, select **Unsanctioned**.

**Step 5:** Select all unsanctioned applications, and then click **Save**.

Select Application (11) View Selected Applications

Search Application Name or Category U Unsanctioned Add Filter Reset

<input checked="" type="checkbox"/>	Application ↑	Category ↑↓	Risk ↑↓	Application Capabilities	Tag ↑↓
<input checked="" type="checkbox"/>	101 Blockchains	Vertical Industry	10		U
<input checked="" type="checkbox"/>	33Across	Digital Advertising	10		U
<input checked="" type="checkbox"/>	Dianomi	Marketing	10		U
<input checked="" type="checkbox"/>	Iterate	Office	10	 	U
<input checked="" type="checkbox"/>	Kimola Analytics	Marketing	10		U
<input checked="" type="checkbox"/>	MachineryHost	Marketing	10		U
<input checked="" type="checkbox"/>	Meetup Pro	Marketing	10		U
<input checked="" type="checkbox"/>	Quora	Collaboration & Productivity	10	 	U
<input checked="" type="checkbox"/>	RetentionEngine	Customer Service	10		U

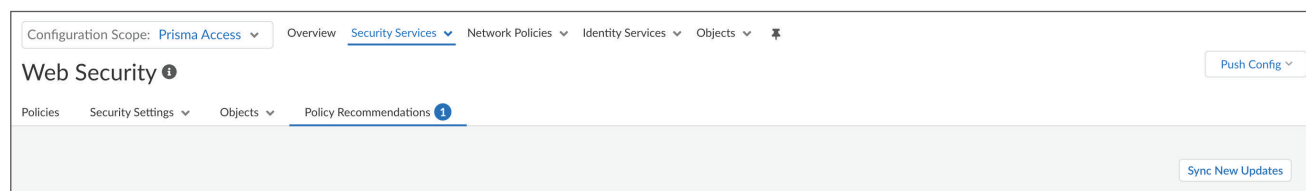
Displaying 10 results of 11

Rows 10 Page 1 of 2

## 2.5 Import and Deploy Updated Policy Recommendation

In this procedure, the web-security administrator imports the updated recommended policy into web security in order to deploy and enforce it.

**Step 1:** Navigate to **Manage > Configuration > NGFW and Prisma Access > Security Services > Web Security > Policy Recommendations**, and then click **Sync New Updates**.



**Step 2:** On the Success message, click **Close**.

**Step 3:** In the Imported SaaS Rule Recommendations pane, verify that the status of the Block Access rule is Update Available, and then in the Actions column, click the refresh icon.

The screenshot shows the Palo Alto Networks Web Security interface. The top navigation bar includes 'Configuration Scope: Prisma Access', 'Overview', 'Security Services', 'Network Policies', 'Identity Services', 'Objects', and a star icon. The 'Web Security' section is active, with a 'Push Config' button. Below this, the 'Policy Recommendations' tab is selected, showing a 'Sync New Updates' button. The main content area is divided into two sections: 'New SaaS Rule Recommendations (0)' and 'Imported SaaS Rule Recommendations (2)'. The 'Imported SaaS Rule Recommendations' section contains a table with the following data:

Name	Description	Status	Last Updated	Actions
Block Access	Default rule: block users from accessing unsanctioned SaaS apps.	Update Available	2022-Oct-24 11:15:49 PDT	
Block Personal Access	Default rule: prevent users from accessing their personal accou...	Imported	2023-Jan-09 15:14:48 PST	

**Step 4:** On the Success message, click **Close**.

**Step 5:** Click **Push Config**, and then click **Push**.

**Step 6:** In the Push dialog box, enter a description, and then click **Push**.

## Procedures

### Controlling Tolerated SaaS Applications

- 3.1 Control SaaS Applications by Using Custom Web-Access Policy
- 3.2 Apply DLP Profile to Inspect Data Uploads

After gaining visibility into the applications being used, who is using them, and the risks associated with them, you can establish controls for accessing SaaS applications. In this design, you can use web-access policies to restrict tolerated applications by user/user group or functionality.

You can create custom web-access policies without the need of policy recommendations. In these example procedures, you restrict an external partner file-sharing application to allow only uploads from a user group, and you assign a DLP profile to inspect the content and prevent PII data leakage.

**Caution**

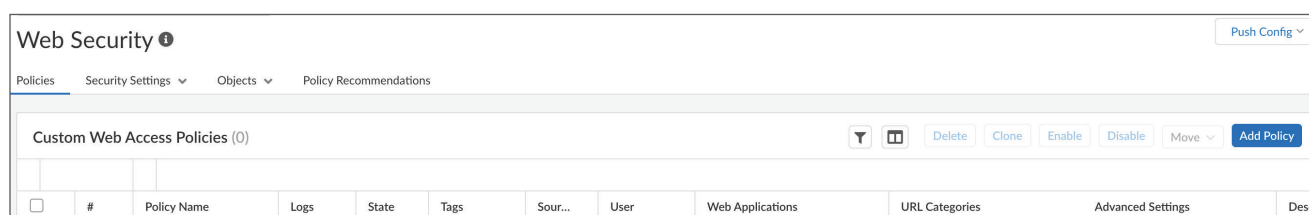
This is an allow rule for a specific user group. In order to block access to the same application for other user groups, an application block policy for all users is required after this policy. Otherwise, the default Global Web Access allows the file-sharing application for other groups.

### 3.1 Control SaaS Applications by Using Custom Web-Access Policy

In this procedure, you allow uploads to the Enterprise version of box.com from users in the engineering group and deny all other functions for that same app.

**Step 1:** Continuing in Cloud Manager, navigate to **Manage > Configuration > NGFW and Prisma Access > Security Services > Web Security > Policies**.

**Step 2:** In the Custom Web Access Policies pane, click **Add Policy**.

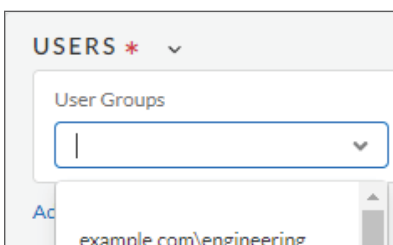


**Step 3:** In the Name box, enter **Box Allow only Uploads**.

**Step 4:** In the Description box, enter **Control tolerated application box.com**.

**Step 5:** In the Source pane, in the Users section, click **Add User Groups**.

**Step 6:** In the User Groups list, select **example.com\engineering**.



**Step 7:** In the Allowed Web Applications pane, click **Add**.

**Step 8:** In the Add list, select **Add Application**.

The screenshot shows the 'Allowed Web Applications' interface with 0 applications. A dropdown menu is open from the 'Add' button, showing options: 'Add Application', 'Add Custom Application Group', and 'Add Application Category'. The interface includes columns for Name, SaaS Enterprise Control, App Functions, File Control, and DLP.

**Step 9:** In the application name list, type *boxnet*, and then choose **Boxnet**.

The screenshot shows the 'Allowed Web Applications' interface with 1 application. A search bar contains the text 'boxnet'. Below the search bar, a dropdown menu shows 'Boxnet' as the selected application. The interface includes columns for Name, SaaS Enterprise Control, App Functions, File Control, and DLP.

**Step 10:** In the SaaS Enterprise Control column, select **Enterprise access**, and then clear **Consumer access**.

The screenshot shows the 'Allowed Web Applications' interface with 1 application. The 'Boxnet' application is selected. In the 'SaaS Enterprise Control' column, the 'Enterprise access' checkbox is checked, and the 'Consumer access' checkbox is unchecked. The interface includes columns for Name, SaaS Enterprise Control, App Functions, File Control, and DLP.

**Step 11:** In the App Functions column, click **Downloading**, clear all functions except for **Uploading**, and then click **Save**.

The screenshot shows the 'App Functions' dropdown menu. The 'Uploading' checkbox is checked, and all other checkboxes ('Allow All App Functions', 'Downloading', 'Editing', 'Sharing') are unchecked.



**Step 12:** Click **Push Config**, and then click **Push**.

**Step 13:** In the Push dialog box, enter a description, and then click **Push**.

## 3.2 Apply DLP Profile to Inspect Data Uploads

After you verify the access control policy is working for your SaaS application, you can apply a DLP profile to perform content inspection. In this procedure, you apply the default PII profile to the web-access policy configured in Procedure 3.1.

**Step 1:** Navigate to **Manage > Configuration > NGFW and Prisma Access > Security Services > Web Security > Policies**.

**Step 2:** In the Custom Web Access Policies pane, click the policy name **Box Allow only Uploads**.

**Step 3:** In the Allowed Web Applications pane, select the Boxnet row, and then click the DLP column.

**Step 4:** From the **DLP** list, type *PII*, select **PII**, and then click **Save**.

**Step 5:** Click **Push Config**, and then click **Push**.

**Step 6:** In the Push dialog box, enter a description, and then click **Push**.

## DEPLOYING SECURITY FOR SANCTIONED SAAS APPLICATIONS

For sanctioned SaaS applications, this design recommends API security mode in order to complement inline security with advanced granular controls for implementing the following:

- **Asset discovery and visibility**—Discovers all files, also called *assets*, contained in the managed SaaS application, and provides visibility into how users are using the SaaS application.
- **Exposure risk assessment**—Provides visibility into how assets are shared in order to identify exposure level, user activity, and external collaborators.
- **Data security**—Discovers and analyzes content when it's stored and shared on SaaS applications, providing data governance and compliance assurance.
- **Security posture management**—Monitors and configures security settings for multiple SaaS applications in one place to make them both compliant and protected.
- **Threat protection**—Stops evasive malware stored in SaaS applications and identifies compromised accounts and malicious insiders.

### Procedures

#### Configuring Security for Sanction SaaS Applications

- 4.1 Configure Internal Domains
- 4.2 Create Data-Asset Policy Rule
- 4.3 Create User-Activity Policy

#### 4.1 Configure Internal Domains

To allow you to identify data assets that are internal and external to your organization, you configure internal domains in SaaS Security API.

**Step 1:** Continuing in Cloud Manager, navigate to **Manage > Configuration > SaaS Security > Settings**, and then select **Manage Domains**.

**Step 2:** In Internal Domains pane, click **Edit**.

**Step 3:** In the Edit Internal Domains dialog box, enter [example.com](https://example.com), and then click **Save**.

## 4.2 Create Data-Asset Policy Rule

Data-asset policies detect whether there is sensitive data present in SaaS applications. To detect sensitive data, SaaS Security API provides default policies. In addition to the default policies, SaaS Security API allows you to create custom policies.

In this procedure, you create a custom data-asset policy. This policy is a medium-severity policy, and it alerts an administrator and logs an incident when HIPPA violation occurs on Microsoft 365 SaaS application.



### Note

This procedure assumes that Microsoft 365 is already onboarded to Prisma Access.

**Step 1:** Navigate to **Manage > Configuration > SaaS Security > Data Security > Policies**.

**Step 2:** On the Data Asset Policies tab, click **Add Policy**.

**Step 3:** In the General pane, in the **Policy Name** box, enter **Alert on HIPAA Violations**.

**Step 4:** In the **Description** box, enter **Alert on HIPAA Violations Data Asset Policy**.

**Step 5:** In the **Severity** list, choose **Medium**.

**Step 6:** Set **Status** to **Enabled**.

[< Back to Policies](#)  
**General**

<b>Policy Name</b> <input type="text" value="Alert on HIPAA Violations"/>	<b>Severity</b> <input type="text" value="3 (Medium)"/>
<b>Description (Optional)</b> <input type="text" value="Alert on HIPAA Violations Data Asset Policy"/>	<b>Status</b> <input checked="" type="checkbox"/> Enabled

**Step 7:** In the Match Criteria pane, select **Cloud Apps**.

**Step 8:** In the **Any Cloud App** list, select **Choose**.

**Step 9:** In the Select Cloud App list, select **Office 365 Example**.

The screenshot shows the 'Match Criteria' panel. The 'Cloud Apps' checkbox is checked. Below it, a 'Choose...' dropdown is open, showing a list of cloud applications. 'Office 365 Example' is selected and highlighted in blue. Other applications listed include Amazon S3 1, GitHub 1, and Office 365 Example (which is also checked with a blue box). Other criteria like Exposure, File Extension, Account, Activity, Asset Name, Data Pattern/Data Profile, File Hash(SHA256), Owner, and Trust States are unchecked.

**Step 10:** Select **Data Pattern/Data Profile**.

**Step 11:** In the **Type** list, choose **Data Profile**.

**Step 12:** In the Select a Data Profile list, choose **PII**.

The screenshot shows the 'Match Criteria' panel. The 'Data Pattern/Data Profile' checkbox is checked. Below it, the 'Type' dropdown is set to 'Data Profile'. A 'Select a Data Profile' dropdown is open, showing a list of data profiles. 'PII' is selected and highlighted in blue. Other profiles listed include Malware and PII - Basic. The 'Cloud Apps' section remains unchanged from the previous step.

**Step 13:** In the Action pane, select **Log as an incident only**, and then click **Create**.

The screenshot shows the 'Action' pane. Under 'Basic Action', the 'Log as an incident only' radio button is selected. The 'Assign to' dropdown is set to 'None'. The 'Alert end-user' checkbox is unchecked. Under 'Autoremediate Actions', the dropdown is set to 'None'.

## 4.3 Create User-Activity Policy

User-activity policies highlight any suspicious activities in SaaS applications. Such activities include risky IP addresses, bulk uploads, bulk downloads, and more. SaaS Security API has in-built policies to detect such activities and has options for you to create custom policies. The custom policies allow you to match on granular conditions in order to define specific user behaviors.

In this procedure, you create a custom user-activity policy that matches uploads to the GitHub application.

**Step 1:** Navigate to **Manage > Configuration > SaaS Security > Data Security > Policies**.

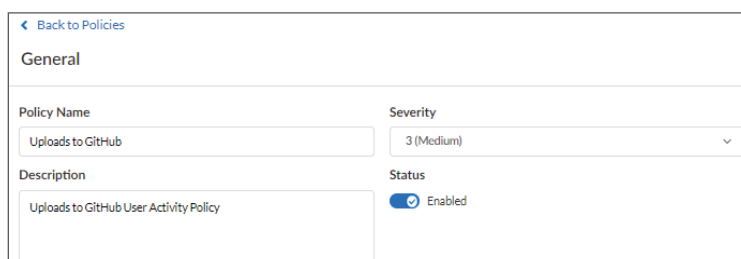
**Step 2:** On the User Activity Policies tab, click **Add Policy**.

**Step 3:** In the General pane, in the **Policy Name** box, enter **Uploads to GitHub**.

**Step 4:** In the **Description** box, enter **Uploads to GitHub User Activity Policy**.

**Step 5:** In the **Severity** list, select **3 (Medium)**.

**Step 6:** Set **Status** to **Enabled**.



General

Policy Name: Uploads to GitHub

Severity: 3 (Medium)

Description: Uploads to GitHub User Activity Policy

Status: ☒ Enabled

**Step 7:** In the Items to Detect pane, select **Users**.

**Step 8:** In the Match Criteria pane, in the **Sanctioned Applications** list, select **GitHub1**.

**Step 9:** In the **User Activity** list, select **Upload**, and then click **Create**.



Match Criteria

Sanctioned Applications: GitHub 1 x

User Activity: Upload x

# Summary

---

The Palo Alto Networks next-generation CASB solution elevates the state of cloud-delivered SaaS security. With complete visibility, real-time data protection, and best-in-class security, it's the industry's only solution that automatically keeps pace with the explosive SaaS growth. In addition to the continuous trust verification and security inspection provided by Prisma Access, the NG-CASB add-on helps secure SaaS application usage in the following four ways:

- **Visibility and control**—Identify all SaaS applications in use, assess risk, and control access and features.
- **Security posture management**—Protect sanctioned SaaS applications from misconfigurations that put users and data at risk.
- **Advanced threat protection**—Stop evasive malware inside SaaS applications and detect suspicious user activities associated with compromised accounts and malicious insiders.
- **Data security**—Prevent exposure of sensitive data-in-motion to all SaaS applications and data-at-rest inside sanctioned SaaS applications.

The NG-CASB design uses cloud-managed Prisma Access in order to provide the following set of capabilities, which are all integrated into a single management console:

- **SaaS Security Inline**—SaaS Security Inline uses ACE to retrieve SaaS application information and enforce access controls. ACE contains over 60,000 SaaS application IDs and is adding to the list constantly. To identify new SaaS applications as they become available, ACE uses ML and crowdsourcing.
- **SaaS Security API**—Cloud-based service that connects directly to sanctioned SaaS applications by using the cloud application's API. The service provides asset discovery, data classification, sharing/permission visibility, user-activity monitoring, and threat detection.
- **SSPM**—Cloud-based service that connects directly to sanctioned SaaS applications by using the cloud application's API. Through continuous monitoring, the service helps detect and remediate misconfigured security settings and best practices in SaaS applications.
- **Enterprise DLP**—Enterprise DLP is a cloud-delivered solution that comprehensively protects sensitive data across all networks, clouds, and users. It easily enables data protection and compliance in minutes, eliminating appliance deployment and ongoing management cycles and ensuring the most cost-effective enterprise DLP on the market.

## HEADQUARTERS

Palo Alto Networks	Phone: +1 (408) 753-4000
3000 Tannery Way	Sales: +1 (866) 320-4788
Santa Clara, CA 95054, USA	Fax: +1 (408) 753-4001
<a href="https://www.paloaltonetworks.com">https://www.paloaltonetworks.com</a>	<a href="mailto:info@paloaltonetworks.com">info@paloaltonetworks.com</a>

© 2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.



You can use the [feedback form](#) to send comments about this guide.

