Netskope SaaS Security Posture Management (SSPM)

Data Sheet +

SaaS Visibility, Security, and Compliance

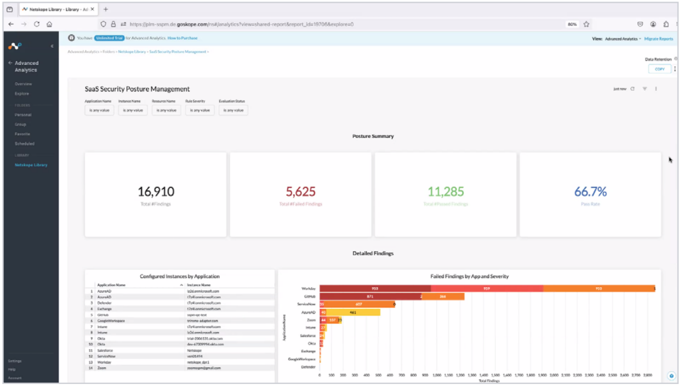
Enterprises use 125 SaaS apps, but IT only sees a third. This blind spot leads to dangerous misconfigurations, privilege sprawl, and data breaches. Get full visibility and control for secure SaaS productivity with Netskope SSPM, part of the industry's most unified CASB platform.

Why is Netskope the best choice?

Netskope SSPM enhances our industry-leading CASB, providing organizations with comprehensive in-line and API-based protections. Powerful graph-based detections and visualizations leverage cross-app rules, correlating context between different apps to expose hidden risks. Alerts and notifications have guided remediation built-in to fix security misconfigurations and ensure compliance with industry standards including CIS, PCI-DSS, NIST, HIPAA, CSA, GDPR, AIPCA, ISO, and more.

Netskope SSPM value

- **Predefined security and compliance rules** across industry benchmarks and standards enable adoption and improvement of SaaS security and compliance initiatives.
- **Graph-based detections and visualizations** support cross-app rules that stitch together context between different SaaS apps.
- **Deep visibility into connected and 3rd Party Apps** to uncover and mitigate additional risks.
- **Define custom rules and profiles** to fit your organization's specific needs in addition to best of breed out-of-the-box rules & detections.
- **Accelerate remediation** with step-by-step guidance to quickly resolve security risks.
- **Comprehensive set of APIs** enables easy integration into existing security and automation workflows to prevent business disruption.
- **Unified view of alerts and events** from across the entire Netskope platform.



https://plm-sspm.de.goskope.com/ns#/analytics?view=shared-report&report_id=19706&explore=0

You have Unlimited Trial for Advanced Analytics. How to Purchase

Advanced Analytics > Folders > Netskope Library > SaaS Security Posture Management >

SaaS Security Posture Management

Application Name: is any value
Instance Name: is any value
Resource Name: is any value
Rule Severity: is any value
Evaluation Status: is any value

Posture Summary

16,910 Total #Findings

5,625 Total #Failed Findings

11,285 Total #Passed Findings

66.7% Pass Rate

Detailed Findings

Configured Instances by Application

	Application Name	Instance Name
1	AzureAD	lz2d.onmicrosoft.com
2	AzureAD	t7z4l.onmicrosoft.com
3	Defender	t7z4l.onmicrosoft.com
4	Exchange	t7z4l.onmicrosoft.com
5	GitHub	sspm-qe-test
6	GoogleWorkspace	trireme-adapter.com
7	Intune	t7z4l.onmicrosoft.com
8	Intune	lz2d.onmicrosoft.com
9	Okta	trial-2006131.okta.com
10	Okta	dev-67309994.okta.com
11	Salesforce	Netskope
12	ServiceNow	ven01494
13	Workday	netskope_dpt1
14	Zoom	zoomsspm@gmail.com

Failed Findings by App and Severity

Key Benefits and Capabilities

Graph-based Detections and Visualizations

Expose hidden risk with cross-app rules that correlate context between different SaaS apps.

SaaS Visibility Including 3rd Party OAuth Apps

Continuously discover and monitor SaaS configurations, users, and 3rd Party OAuth apps to eliminate blind spots and manage risk.

SaaS Compliance

Uncover and mitigate misconfigurations and overly permissive user access by verifying against predefined best practices and industry standards.

Guided Remediation

Alerts include step-by-step instructions and automations for quick remediation of SaaS misconfigurations.

Customizable Rules and Configuration

SSPM includes the ability to define custom rules and profiles to fit your SaaS security needs.

Quickly Convert Anomalies to New Detection Rules

Powerful query language allows you to search for anomalies and easily build new detection rules from findings.

Extensive Reporting and Integrations

Netskope Cloud Exchange enables RESTful API integration with Snowflake and Jira for ticketing and SIEM/SOAR tools for automation and orchestration.

Part of an Integrated SASE Architecture

SSPM complements Netskope CSPM, NG-SWG, CASB, DLP, ZTNA, CFW, RBI, and Advanced Analytics, all delivered on one platform, one console, and one policy engine.

> "Netskope provides visibility into SaaS usage and risk exposures we didn't have previously."
>
> – Manager, Information Security
> Large Enterprise Diversified Consumer
> Services Company

Discover and Control 3rd Party SaaS Apps and Plug-Ins

Users are connecting untrusted 3rd Party OAuth apps to managed apps such as Microsoft 365, Google Workspace, Salesforce, Okta and Workday. at an exponential rate. While useful and easily connected by users, these unmanaged "plug-ins" can be compromised by attackers and used to access managed resources or exfiltrate data. Since governance and data movement on these apps happens in the cloud beyond the enterprise perimeter, they can't be discovered or monitored using CASB or SWG solutions. Likewise, security tools such as EDR, XDR, and related SIEMs are also blind to these apps. Here are a few of the risks that organizations inherit with these apps:

- **OAuth vulnerabilities:** 3rd Party Apps are often connected using OAuth, a widely used protocol for enabling 3rd Party access to resources. Vulnerabilities can arise from implementation on main and 3rd Party Apps and the OAuth service itself.

- **Data breaches:** Granting access to 3rd Party Apps might expose sensitive data to potential security breaches. If a 3rd Party App is not properly secured or configured, attackers could gain unauthorized access to sensitive data.

- **Data misuse:** Some 3rd Party Apps might collect and use data for purposes other than what you intended or disclosed.

- **Compliance violations:** 3rd Party Apps could potentially access more data than they need for their intended functionality, violating compliance or privacy regulations.

- **Loss of control:** 3rd Party Apps might be able to control certain aspects of accounts or data, potentially compromising additional resources.

- **Vendor risks:** If a 3rd Party App provider is compromised, the app could be used as a Trojan horse to access data or initiate a supply chain attack.

Netskope SaaS Security Posture Management (SSPM) reduces risk associated with 3rd Party Apps by discovering and controlling any connections made to an organization's managed apps by add-ons or plug-ins. Netskope SSPM continuously monitors configuration settings for any connections to 3rd Party Apps and automatically assigns a risk score to these apps so that you can take action—for example block the riskiest apps.

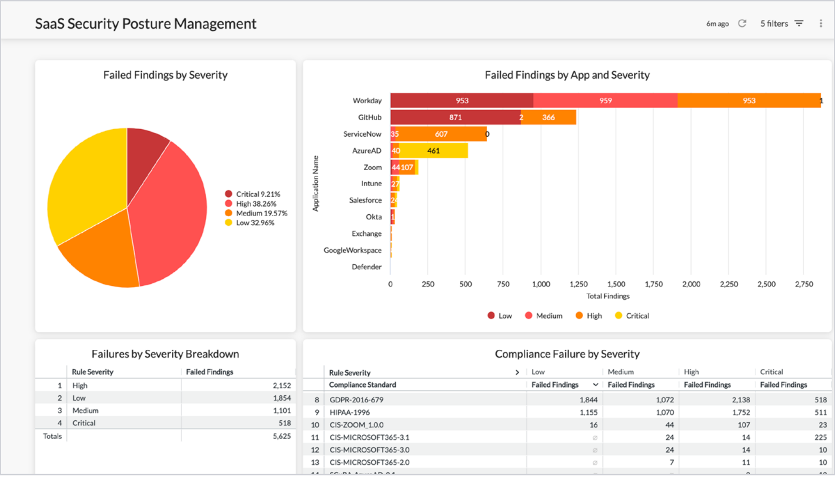
SSPM Benefits

- **Increased visibility:** Broad visibility and monitoring of the SaaS ecosystem.

- **Safeguard SaaS data:** Keep sensitive data within your SaaS ecosystem by preventing exfiltration to unknown locations and apps.

- **Reduced risk and attack surface:** Gain control over unknown SaaS apps and reduce risk by revoking dangerous connections.

- **Maintain compliance:** Prevent users from jeopardizing audits or exposing sensitive data by connecting risky apps and plug-ins.



Failures by Severity Breakdown

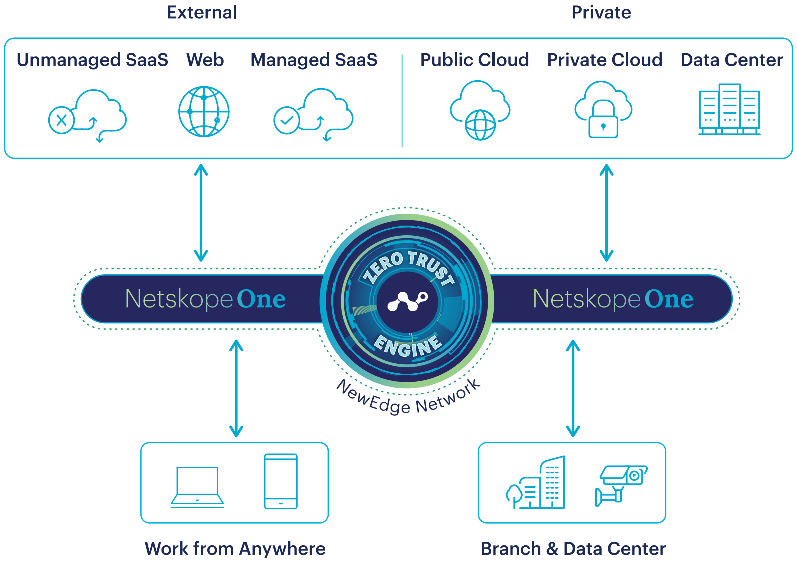
	Rule Severity	Failed Findings
1	High	2,152
2	Low	1,854
3	Medium	1,101
4	Critical	518
Totals		5,625

Compliance Failure by Severity

	Rule Severity ›	Low	Medium	High	Critical
	Compliance Standard	Failed Findings ⌄	Failed Findings	Failed Findings	Failed Findings
8	GDPR-2016-679	1,844	1,072	2,138	518
9	HIPAA-1996	1,155	1,070	1,752	511
10	CIS-ZOOM_1.0.0	16	44	107	23
11	CIS-MICROSOFT365-3.1	∅	24	14	225
12	CIS-MICROSOFT365-3.0	∅	24	14	10
13	CIS-MICROSOFT365-2.0	∅	7	11	10

The Netskope Difference

Netskope One is a converged security and network as a service platform. Through its patented Zero Trust Engine, AI innovation, and the largest private security cloud we make it easy for our customers to defend their businesses and data while delivering a phenomenal end user experience and simplified operations. The platform delivers AI-powered data and threat protection that automatically adapts to the ever growing data landscape, including the widespread adoption of generative AI and new AI-driven attacks.



YOUR NEEDS	THE NETSKOPE SOLUTION
Support Compliance Initiatives	Verify security posture against predefined best practice rules and industry standards including CIS, NIST, HIPAA, PCI, CSA, GDPR, AIPCA, ISO, and more.
Prevent Misconfiguration and Reduce Risk	Misconfiguration remains the most common security problem for SaaS apps. Netskope SSPM uses graph-based detections and visualizations to streamline security posture management and compliance.
Discover and Control 3rd Party SaaS Apps	Netskope SSPM continuously monitors the configuration settings of your managed apps for any connections to 3rd Party Apps, and when discovered, automatically assigns a risk score to them so you can block or control them to reduce risk.
Remediation	Step-by-step instructions and automations for quick resolution of security risks. Alerts and compliance results can be exported via RESTful API for integration into ticketing and remediation orchestration workflows.
Integrated SASE Architecture	Netskope SSPM is integrated with Netskope CASB, SWG, DLP, ZTNA, and other Netskope products to offer a seamless and unified management, visibility, and security solution.
SaaS Application Support	Support for SaaS applications including GitHub, Google Workspace, Okta, Microsoft 365, Salesforce, ServiceNow, Workday, Azure AD, JIRA, Confluence, Microsoft Defender, Zoom, Microsoft SharePoint, Intune, and Microsoft Exchange
Global Coverage and Performance	Netskope SSPM is just one of many services delivered from Netskope NewEdge, our security private cloud with global coverage that is built from the ground up for maximum performance and service resilience.

netskope

Interested in learning more? Request a demo

Netskope, a global SASE leader, uses zero trust principles and AI/ML innovations to protect data and defend against cyber threats, optimizing both security and performance without compromise. Thousands of customers trust the Netskope One platform and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity. Learn more at netskope.com.