Solution Brief

Securing Your Data in SaaS Apps

The adoption of AI is rapidly and fundamentally reshaping cybersecurity. Enterprises are left struggling to manage when and how employees use new AI SaaS applications that evolve faster than traditional safeguards. It's never been more essential to strengthen oversight, data loss prevention (DLP) controls, and update overall security posture.

Findings from Netskope's 2026 cloud and threat report:

- The number of people using SaaS AI apps, such as ChatGPT and Gemini, increased 3x in 2025.
- 60% of insider threat incidents involve personal cloud app instances.
- The average organization sees 223 incidents of sensitive data uploaded to an AI app per month, a 2x increase year-on-year.
- Shadow AI remains a significant challenge, with 47% of AI users using personal AI apps.
- 42% of genAI policy violations in 2025 were source code uploads, followed by regulated data uploads (32%) and IP uploads (16%)

"It's rare that anybody gets the opportunity to make life easier for users and make data more secure, and I feel we've done an excellent job succeeding at that [with Netskope]."

Tyler Warren
Deputy Information Security Officer
Prologis

The challenge

Besides your people, data is arguably the most valuable asset for your organization. Some of it is structured, but the majority is not, and AI outputs expand the volume of this unstructured data further. To keep data safe when at rest or in use within SaaS apps (or in motion between them), you need to have the right security tools and controls in place. This includes automated visibility and tracking that help you understand:

- Where all your data is located
- Where it has been and where it is going
- Who has interacted with it (and why and when)
- How it has mutated along its lifecycle journey
- What security policy adjustments you need to make

Netskope One for securing data in SaaS apps

The foundation for total security of your data—both within and when in transit to and from SaaS apps—is Netskope One DSPM, which automates discovery and classification of your data at rest in those apps. Further value can be realized by adding Netskope One Data Lineage, Netskope One SaaS Security Posture Management (SSPM), and Netskope One CASB, which includes advanced DLP. Netskope One delivers all of this in a single platform that is integrated and unified from the ground up.

Automate data discovery and classification, alongside journey and mutation tracking

InLet's say you're a data security leader looking to ensure your policies will find and classify all the sensitive data stored in SaaS apps in use in your environment. Your employees and contractors constantly produce, consume, and share a ton of this data, often using shadow AI, further complicating the situation. Those users will also change or move the data in ways that create a disconnected series of events related to that data. This disrupts your ability to understand how and where it has mutated during its lifecycle.

Netskope One DSPM automates the discovery and classification of all your data at rest, no matter its nature, location, who has access, or how your people and systems interact with it. DSPM uses your security policies to protect that data before it is used or moved, with those same policies extending to Netskope One DLP.

Netskope One Data Lineage provides visibility with context, tracking a file's entire journey from origin to destination. By documenting every user modification, rename, and movement across SaaS, endpoints, and AI tools, it creates a definitive visual chain of custody. This visibility enables security teams to investigate insider risks in minutes and simplify compliance audits. It ensures sensitive IP remains protected and governed, regardless of how it transforms or where it travels.

Ensure proper security configurations and identity and access management settings

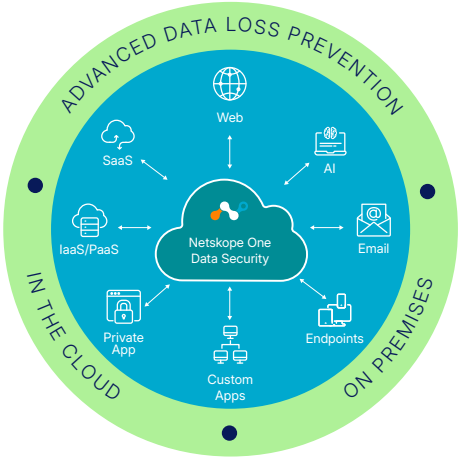
Remote work has accelerated the use of both managed and unmanaged SaaS apps. While helpful for user productivity, many information security teams can't discover or monitor unmanaged SaaS apps, since they run in the cloud outside their organizations' control perimeters. This lack of visibility can make unmanaged SaaS apps more easily compromised by attackers, and used to access managed resources or exfiltrate data.

> "With Netskope, we can lock down certain areas and prevent users from uploading certain data to AI platforms. So, they can use ChatGPT to help the business operate more efficiently, but they cannot upload proprietary data into ChatGPT."
>
> - Nik Miller,
> Partner and Chief Technology Officer for BDO UK

Netskope One SSPM continuously checks security posture by comparing SaaS app settings with security policies and industry benchmarks (CIS, PCI DSS, NIST, HIPAA, CSA, GDPR, AIPCA, ISO, and more). It complements Netskope One CASB by providing powerful graph-based detections and visualizations that add context to expose hidden risks and security gaps. When risky configurations or policy drift are detected, SSPM generates alerts with remediation instructions.

Unified SaaS Data Security in Netskope One

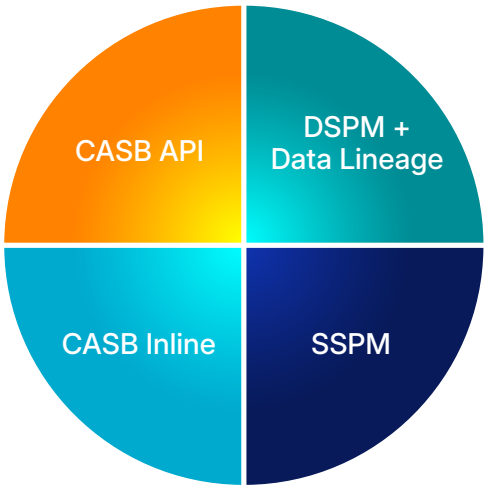
- Unified Contextual Visibility
- Unified Policy Controls
- Unified Data Analytics
- Data Journey Tracking
- AI-Powered Data Classification
  - 3K+ Data Identifiers
  - 30+ AI/ML Models
  - 40+ Regulatory and Compliance Templates



Data at Rest • Data in Use • Data in Motion
Structured and Unstructured

Get SaaS Data Security with 5 Trusted Tools

- Discover Data & Track Its Journey
- Classify Data for Compliance
- Configure Security
- Manage Identity & Access
- Block Sensitive Data Uploads
- Prevent External Sharing
- Protect Data in SaaS Apps
- Accelerate AI Readiness



Block sensitive data uploads and prevent external sharing

Many employees use AI to improve their productivity. Sometimes, they use managed SaaS apps provided by their employer. But they also sometimes use unmanaged SaaS apps, often described as shadow IT or shadow AI. These unmanaged apps introduce uncontrollable risks for security teams, including inadvertent or unauthorized transfer of sensitive information between cloud apps — including AI apps. This lack of oversight and control can lead to sensitive data exposure as a result of inadvertent oversharing and exfiltration by risky insiders or malicious cybercriminals.

Netskope One CASB empowers data security teams to quickly identify and oversee the use of SaaS apps, regardless of whether they are managed by the organization. It allows organizations to confidently adopt SaaS apps including AI to accelerate innovation without sacrificing security. Netskope One CASB ensures rapid risk categorization to automatically stay ahead of SaaS sprawl, leveraging cutting-edge algorithms and large language models (LLM) to expedite the automatic process of new SaaS app risk categorization.

Perhaps most importantly, Netskope One CASB monitors attempted transfers of data on its way to SaaS apps or to unapproved recipients outside the organization. It blocks these transfers through built-in advanced data loss prevention capability.

Protect data in SaaS apps and accelerate AI readiness

Netskope One makes security management effortless thanks to unified automated data security. Netskope One aggregates risk intelligence across CASB inline, CASB API, and SSPM controls to provide deep visibility into user identities and privileges. This streamlines security operations, simplifies policy definition and enforcement, and expedites incident response.

Netskope One CASB is the only solution that offers machine learning (ML)-based risk categorization of SaaS apps. It also protects your data that has been created in SaaS apps and is still stored in them. Even further, it intelligently discerns app instances (corporate vs. personal) and enables responsible use of AI, such as OpenAI ChatGPT, Anthropic's Claude, Google Gemini, and Microsoft Copilot by making it more secure and enabling your organization to leverage AI for its productivity advantages.

BENEFITS	DESCRIPTION
Broader visibility	Expanded and automated discovery of all your data at rest across all locations, including ones you might not know about.
Faster investigations	Quick, visual discovery of where and how data has mutated to support better understanding and control of your data's lifecycle.
Automated compliance	Simple, fast, and accurate tagging of sensitive data that reduces time and effort required to follow privacy laws.
Scalable confidence	Rapid and robust detection and response to hidden security risks and configuration gaps.
Sprawl and loss avoidance	Better detection and monitoring of new shadow apps usage expedites informed policy adjustments to keep data safer.
AI readiness	Controlled use of new and evolving AI apps inspires confidence that data stays secure and enables faster AI adoption.

netskope

Interested in learning more? Request a demo

Netskope (NASDAQ: NTSK), a leader in modern security and networking for the cloud and AI era, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for the AI ecosystem inclusive of agents, applications, tools, LLMs, people, devices, and data. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications – providing security and accelerating performance without trade-offs. Learn more at netskope.com, Netskope.ai, on LinkedIn, and Instagram.

©2026 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized "N" logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners.

05/26 SB-989-1