Solution Brief

Discovering and Protecting Your Data in the AI Era

By using integrated Netskope One DSPM and CASB, an organization can not only automate the continuous discovery and classification of sensitive structured and unstructured data on premises, in the cloud, and in hybrid environments, but can also see and control organizational AI and cloud app access and usage toward keeping sensitive data secure.

Quick Glance

- Single dashboard and policy framework across AI, SaaS, PaaS, IaaS, private apps, Web, Email, and Endpoints simplifies security management.
- Continuous scanning of data sources across all environments gives full visibility into sensitive data at rest and in motion.
- Real-time monitoring of data access and usage detects compliance risks, unauthorized activity, and potential exfiltration, reducing the risk of breaches.
- No-code policy engine automates data tagging, governance, and adaptive access control to align with regulatory standards.
- Automated data classification streamlines compliance management.

"Netskope One DSPM and CASB help us not only monitor data usage, but also prioritize and remediate real data risks to enhance our overall data security posture. Not only can we control data access better, but we can also see and understand our whole data landscape better."

CISO, Healthcare industry

The Challenge

Common Data Security Challenges Around AI and Cloud Usage

Organizations face significant challenges in today's AI and cloud-centric environment that can complicate data security and application access control. This leads to difficulties in managing unintentional or unapproved movement of sensitive structured and unstructured data across the cloud and on prem. Additionally, the rise in data breaches, with a large portion involving cloud data, highlights the need for better ways to protect sensitive information and manage its access and usage.

The Solution

Protect Your Data and Cloud Access Everywhere

Netskope One DSPM and CASB together provide full visibility and control over structured and unstructured data across cloud and on-prem environments. CASB focuses on securing AI and cloud apps and services, while DSPM automates the discovery, assessment, and classification of data at rest to proactively strengthen security posture so Netskope One DLP can stop the leakage of data in motion more intelligently. They combine to effectively address the challenges of securing data everywhere.

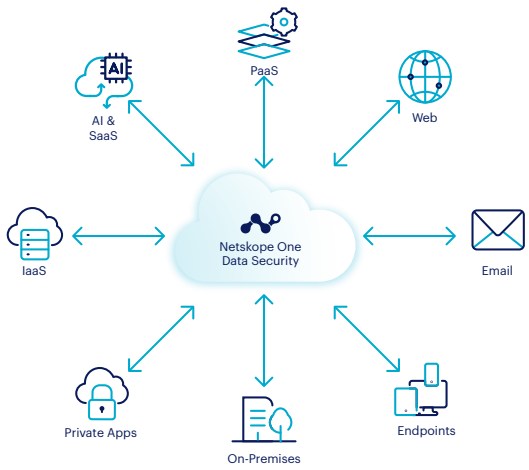
netskope

Automated and Comprehensive Data Discovery and Classification

Netskope One DSPM provides full data discovery and classification across various environments. Netskope One CASB offers visibility of the usage – or attempted usage – of AI and cloud apps and services, using tools like the Cloud Confidence Index (CCI), to assess risk and apply granular security rules. DSPM continuously scans structured and unstructured data in cloud, on-prem, and hybrid environments, automating classification of data to support regulatory compliance and data governance. The combination ensures organizations can see their whole data landscape to better identify and protect sensitive data effectively.

Advanced Data Loss Prevention (DLP)

Netskope One CASB includes DLP that prevents data exfiltration by monitoring and controlling data movement within AI and cloud apps. It uses contextual awareness and machine learning to identify sensitive data and risky activities, preventing unauthorized uploads, downloads, and external sharing. DSPM enhances DLP by providing deeper visibility into data at rest, identifying misconfigurations and analyzing usage patterns to detect and mitigate exfiltration risks. Altogether, they offer a holistic approach to protecting data in motion across the entire cloud and on-prem ecosystem.



Automated Compliance and Policy Enforcement

Neskope One DSPM automates compliance and policy enforcement to streamline data governance. It also automates data tagging, governance, and adaptive access control using a no-code policy engine to align with regulatory standards. Netskope One CASB allows for the definition of targeted security policies based on factors such as user, app, instance, risk, and activity. With both, organizations can enforce consistent policies across their cloud and on-prem environments to ensure compliance.

Proactive Risk Monitoring and Threat Prevention

Netskope One DSPM and CASB both monitor and prevent risks and threats to data security. CASB provides visibility and control over cloud activities while detecting and blocking malware, advanced threats, and risky AI usage. DSPM does real-time monitoring of data access and usage, proactively identifying potential unauthorized activity, compliance risks, and data exfiltration. The combination helps organizations quickly identify and respond to security incidents and reduce data breach risks.

BENEFITS	DESCRIPTION
Enhanced visibility	Provides a single view across data at rest and in motion.
Streamlined compliance	Automates data tagging and governance.
Proactive risk management	Monitors and detects unauthorized access.
Unified security	Integrates data security across multiple locations.
Scalable security	Supports on-prem, cloud, and hybrid environments.