Solution Brief

Netskope One Data Security

In the AI era, data security is more critical than ever. Netskope One provides a unified data security solution to protect your data wherever it lives or moves. Netskope One Data Security brings together DSPM and context-aware DLP capabilities to mitigate data risks, ensure compliance, and enable data privacy, all while reducing costs and complexity.

Quick Glance

- Discover and protect data everywhere while minimizing data exfiltration risk
- Secure usage of genAI by preventing sensitive data leak and managing data flowing through the genAI infrastructure
- Manage data security posture with discovery, classification, access, and usage risk
- Achieve compliance to regulations like GDPR, HIPAA, and CCPA with built-in compliance frameworks and automated policy enforcement
- Consolidate security operations with a unified data security platform with one engine, one client, one gateway, and one network

"Cybersecurity is a competitive differentiator for us, helping us to attract new clients, particularly from industries that value robust data protection."

CISO, Global Services Industry

The Challenge

Cloud computing and the distributed workforce have increased productivity but also introduced data security challenges. The traditional perimeter-based security model is now insufficient, requiring a new approach to protect sensitive data spread across various locations and devices. Generative AI adds another layer of complexity, as it could lead to unintentional data leaks. Organizations must adopt a multi-faceted data security strategy to address these evolving threats and protect sensitive information while minimizing risks.

The Solution:
Netskope One Data Security

Netskope's unified data security solution safeguards sensitive data in cloud applications, endpoints, and collaboration tools, extending beyond traditional security perimeters. Netskope One Data Security combines DSPM and DLP in a single platform, reducing cost and complexity while improving visibility and control. This comprehensive protection helps organizations prevent data breaches, unauthorized access, and data loss, ensuring compliance, maintaining customer trust, and safeguarding intellectual property.

Discover and protect data everywhere

As data proliferates across an organization's environment, answering the question "Where is all the data?" becomes increasingly challenging. Netskope One addresses this challenge by providing deep insights into all data, enabling organizations to achieve comprehensive data protection and control. This provides organizations with complete visibility and control over all their data, including sensitive data, regardless of location. This comprehensive solution safeguards both structured and unstructured data at rest, in motion, and in use across all channels, including web traffic, email, cloud applications (SaaS), endpoints, private apps, and IaaS infrastructure, ensuring consistent protection across the entire digital ecosystem. Key capabilities include:

- Discover sensitive data at rest in managed cloud services such as Microsoft 365 and AWS using API-enabled controls.
- Continuously scan IaaS storage services like AWS for data movement or inadvertent exposure.
- Detect and monitor data in motion between thousands of cloud apps and services, including instances, using inline controls.
- See and control data propagation between cloud apps and instances, as well as in the context of cloud app risk and user risk, without relying on tenant restrictions.
- Gain visibility into whether users are on premises or remote, using browsers, sync clients, or mobile apps.
- Go beyond content analysis by inspecting metadata, hidden fields, and comments.

With Netskope you can protect your data wherever it lives and moves

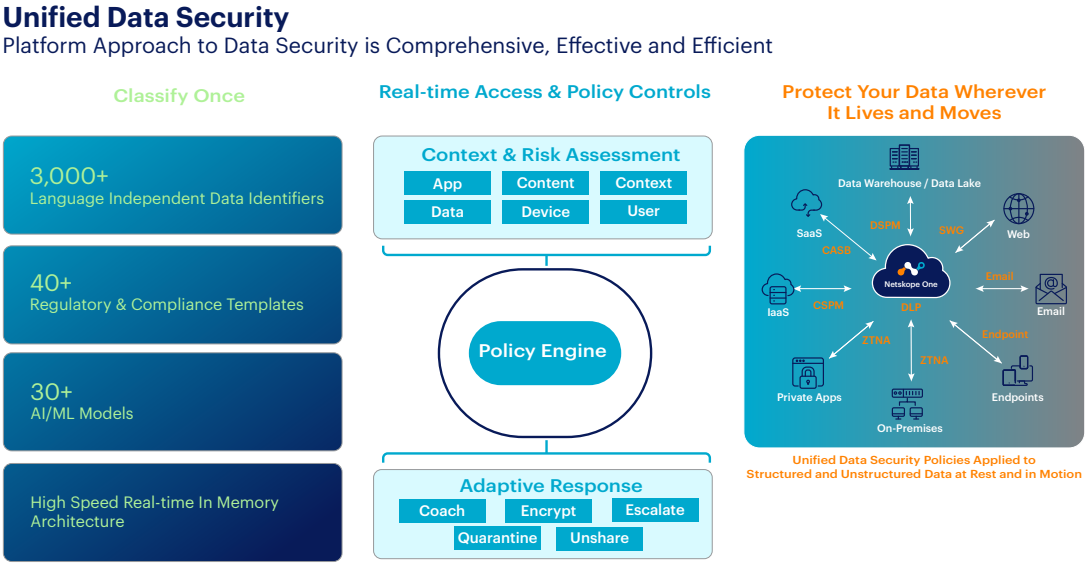
Can you answer these 4 key questions:

- Where is your data?
- What type of data do you have?
- Who has access to it?
- How risky are the data interactions?

Secure genAI usage

Security leaders are struggling to keep corporate data safe as organizations increasingly use generative AI to achieve their business goals. With this trend showing no signs of slowing down, we have to address the security concerns brought about by this new reality. Organizations can now drive innovation without sacrificing protection or performance. Netskope One provides unparalleled visibility and granular control over AI-powered SaaS applications, allowing security teams to monitor access, enforce real-time data protection, and prevent sensitive information from being exposed. Key capabilities include:

- Secure deployment of genAI applications through implementing controls, enforcing secure API connections, and unifying SaaS protection
- Data loss prevention in genAI workflows by monitoring sensitive data usage and leveraging data classification and masking
- Threat detection and response using AI-driven threat protection, proactively addressing vulnerabilities, and uncovering insider threats
- Policy enforcement and user coaching through automated, real-time guidance and enforcing data usage policies
- Compliance and risk mitigation by aligning genAI use with industry-specific regulations, maintaining audit trails, and consolidating security capabilities



Manage data security posture

As data environments grow more complex and cyber threats evolve, the need for unified data security across cloud and on-prem systems has never been greater. Where is all your data? What is the nature of that data? Who has access to it? How risky is our data usage? Netskope One with its DSPM capabilities provides continuous, real-time visibility into your data's security posture. The DSPM score and risk indicators highlight critical risks in data stores, user access, and interactions while continuously scanning for risky behaviors, sensitive data violations, and potentially harmful queries. Key capabilities include:

- Gain visibility: Discover and classify data across all environments, including shadow data stores, ensuring compliance with data sovereignty laws.
- Control access: Manage permissions, monitor access, and enforce strict controls so sensitive data remains accessible only to authorized users.
- Monitor usage: Secure every data interaction by setting alerts, enforcing governance standards, and ensuring end-to-end encryption.

Support privacy and compliance

Maintain data privacy and meet regulatory compliance mandates with GDPR, CCPA, HIPAA, GLBA, PCI DSS, and others through advanced DLP, granular access controls, audits, reporting, and strong encryption of sensitive data. Key capabilities include:

- Granular auditing for all user activity in the cloud and web, including what cloud service was used, website accessed, the activities performed, the data, location, device, and more
- File encryption in real time without impacting user productivity
- More than 40 compliance templates for global data protection regulations
- Compliance reporting on service usage regularly to inform cloud security policies
- Govern the usage of cloud services and websites based on contextual details such as user, app, device, location, activity, and content to meet compliance and risk standards

Minimize exfiltration risk along with malicious and negligent data exposure

Organizations are constantly threatened by data breaches due to the ingenuity of attackers and the unintentional actions of their own employees. A single click or response can lead to unauthorized access, making insider threats and negligent user behavior major concerns. Netskope's unified data security offers a solution by monitoring and mitigating data exposure, oversharing, and personal app and shadow IT usage. Security teams can utilize unified policy controls and UEBA-driven data protection to minimize risk across email, USB, and bulk downloads. Key capabilities include:

- Restrictions on personal app and shadow IT usage
- Prevention of oversharing and transfers in bulk or email
- Defense against C2 and other targeted attacks
- Proactive identification of malicious outsiders

BENEFITS	DESCRIPTION
Mitigate data security risks	Protect your valuable data across all states: whether it's stored (at rest), being transferred (in motion), actively processed (in use), or traversing any potential risk point (across all key vectors). This comprehensive approach ensures that your data remains secure and protected at all times, mitigating potential threats and vulnerabilities.
Enhance security through context and advanced analytics	Shared context enhances analytics and security by correlating user actions with data and application usage. This allows for proactive threat detection, anomaly detection, and tailored security policies, improving effectiveness and reducing disruptions.
Reduce cost and complexity	Organizations can achieve substantial cost savings, potentially reaching up to 50%, by transitioning from a disjointed collection of legacy security tools to the unified Netskope One Platform. This consolidation streamlines operations and eliminates the expenses associated with maintaining multiple disparate systems.
Achieve compliance	Simplify adherence to data protection regulations with built-in compliance frameworks and automated policy enforcement that helps organizations meet the requirements of various data protection regulations, including but not limited to GDPR, HIPAA, and CCPA. This includes identifying and classifying sensitive data, monitoring data access and usage, and enforcing policies to prevent unauthorized access or disclosure.