Netskope Data Loss Prevention (DLP)

Data Sheet

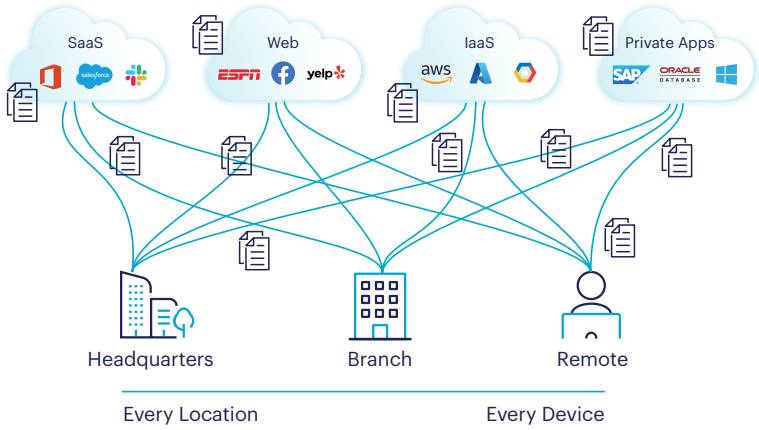
Data Protection for the Modern Enterprise

Comprehensive and advanced cloud-delivered DLP solution secures sensitive data everywhere across clouds, networks, email services, endpoints and users.

The Need for an Updated Data Protection Approach

Protecting sensitive data like personally identifiable information (PII), trade secrets, financial documents, and other intellectual property (IP) is a top priority for every organization today. Modern business trends expose data in unprecedented ways:

- **Hybrid work causes data to travel beyond the traditional boundaries** across cloud services, and anywhere a user wishes to connect, on- and off-premises.
- **Data is stored and shared across a growing number of SaaS applications** that can be accessed by any user and any device directly.
- **Data is booming in volume, variety and velocity.** As a result, sensitive data is increasingly harder to identify, and therefore, to protect.



Traditional DLP solutions can't adapt to cloud, hybrid work and exponential data sprawl. They are complex, anchored by their on-premises infrastructure, resource intensive, and use a costly bolt-on approach to scale.

Relentless data breaches, heightened compliance expectations (GDPR, PCI, HIPAA, GLBA etc.) and cost saving requirements drive the urgency for a new approach to data protection. Organizations need a reliable solution to protect their sensitive data regardless of where it is stored and flows - across clouds, web, email, private apps, or devices.

Netskope DLP is the answer for modern organizations of any size, thanks to its comprehensive coverage, unrivaled detection accuracy and easy management.

Key Benefits and Capabilities

Comprehensive

Achieve comprehensive data protection coverage: discover, monitor, and protect sensitive data across every network, cloud, endpoint, email service and user.

Precise

Attain the highest degree of data protection efficacy with the most accurate data detection and classification capabilities powered by machine-learning and artificial intelligence.

Effortless

Ensure the simplest and the most cost-effective enterprise DLP deployment and leverage unified policy and single management console.

Context and Risk Aware

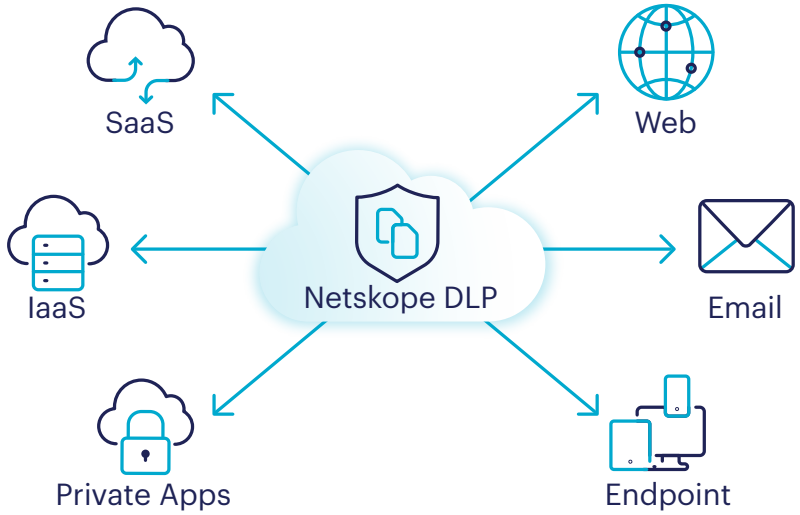
Automatically adapt to changing risks, behaviors, and organizational context In order to properly secure data with zero trust principles.

"When I moved to the cloud, finding the best DLP solution was my #1 priority. Netskope exceeded our requirements in every way."

- Security Architect, Fortune 100 Manufacturing

Netskope Data Protection Everywhere, Delivered From the Cloud

Netskope DLP is the industry's most comprehensive and most advanced cloud data loss prevention solution that secures sensitive data across clouds, networks, email services, endpoints and users consistently everywhere. Netskope DLP delivers zero trust data protection because it's risk-aware and context-aware, and is natively integrated into the Netskope market leading Security Service Edge solution.

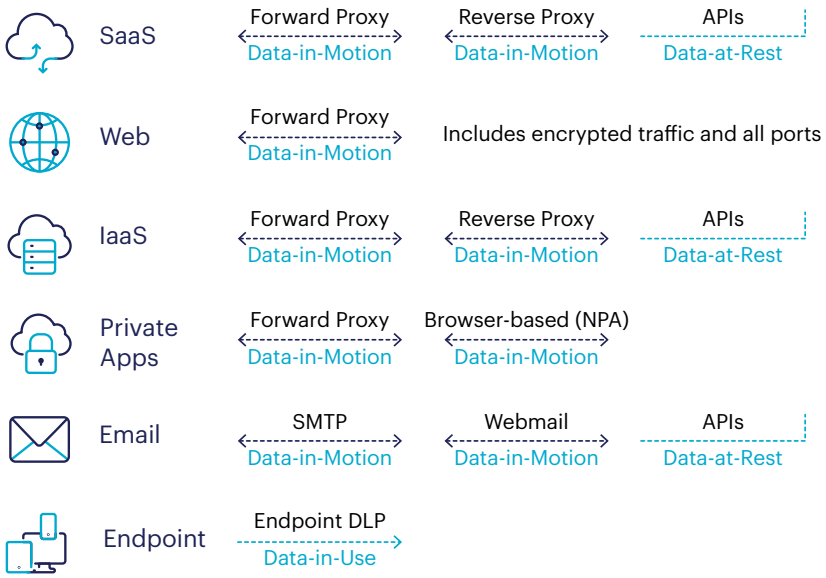


Capabilities

Full Coverage of all Critical Channels with Unified Policies

Sensitive data moving everywhere outside the traditional corporate premises becomes harder to track and protect, and is more prone to both intentional and unintentional exposure.

Netskope cloud DLP consistently discovers, monitors, and protects sensitive data in-motion, at-rest and in-use across SaaS applications, IaaS, corporate networks and branch offices, the mobile workforce, email services and through employees' endpoints. It provides unified data protection policies for every location where data is stored, used or transferred and delivered from a centralized cloud service. Single console, with role based access control, ensures that policy configurations, monitoring, reporting and incident response for all channels are all managed through a single pane of glass by the practitioners.



Unrivaled Detection and Classification Accuracy of All Sensitive Data

Data is growing in volume and is more diversified than ever. Netskope DLP delivers accurate and reliable detection and classification of all sensitive data in any form with the lowest degree of error possible, in order to minimize false positives and violation triage fatigue. This is achieved automatically through a broad set of detection technologies and advanced classification algorithms.

1. Described content matching uses over 3,000+ predefined data identifiers and personal identifiers specific to 80 countries, including regular expressions (regex), names, numbers, financial data, medical data, biodata, inappropriate terms, and industry focused information, in addition to localized languages and fully customizable identifiers. It is also possible to combine data identifiers and to granularly customize and fine-tune rules with proximity keywords, expressions, boolean logic, severity levels, thresholds and proximity ranges. The solution includes a wide variety of predefined data profiles supporting several use cases and compliance requirements such as GDPR, CCPA, PCI-DSS, HIPAA, and GLBA.

2. Exact data matching (EDM) is used to fingerprint actual data sets (eg: client lists, financial data, contracts, etc) and templates. It is a nearly infallible method designed to detect specific information that is sourced from structured data sources, such as individuals' full names, Social Security numbers, addresses, identification numbers, credit card numbers and bank accounts etc. Over two Billion records can be fingerprinted with Netskope DLP and multiple combinations of them. Such indexed information is then automatically discovered and protected across cloud repositories and anywhere the data flows are expected to happen.

3. In the present world, users find it very convenient to snap photos of documents, forms, ID cards, whiteboards, and even pictures of pictures. Optical character recognition (OCR) is an instrumental part of an overall data protection strategy. With OCR, Netskope DLP can extract textual information from images and PDFs and can then automatically look for sensitive data based on its classification algorithms and the detection policies that are in place.

4. Manually defined rules are the foundation of data detection, but automated engines supply invaluable assistance and make sensitive data detection very accurate. Artificial intelligence (AI) and machine learning (ML) -based image classification, available with Netskope DLP, uniquely supply with the ability to recognize sensitive files and document types without necessarily extracting the content that such assets contain, even when such images and documents are partially corrupted, crumpled, blurry and generally not clearly sharp. Built-in ML classifiers detect credit cards, resumes, patents, M&A documents, screenshots, passports, photo IDs, tax forms, medical cards, source code, etc. Netskope DLP also gives the ability to build custom ML-based classifiers.

5. Certain mission-critical documents and highly confidential files must be protected at all cost from complete or partial exfiltration and duplicate copies. File and document fingerprinting can index entire documents and then detect exact and partial copies of the information that they contain with certain degrees of similarity, when this content is found across environments and transmission channels.

6. Netskope DLP can scan over 1,600 different file types such as text formats, presentation, email, images, spreadsheet, design, communication, database, archive, compressed and many others. Detection is based on true file types, in order to prevent obfuscation and attempts to bypass detection, and includes contextual organizational awareness based on device, app, location, user activity etc.

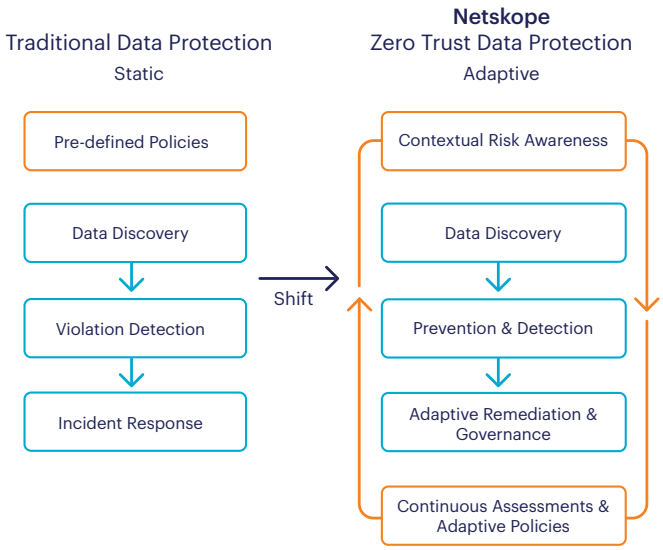
7. Netskope DLP integrates with third-party data classification technologies. It is able to read metadata and tagging in addition to content scans, in order to extend protection policies to data labeled as sensitive by the business users.

Integrated and Risk-aware Data Protection

False positives, incident response fatigue and business disruption are problems related to traditional DLP implementations. It's time for DLP to shift from a static protection model, made of fixed policies, to a dynamic and adaptive zero trust approach. Netskope DLP is the only solution that goes beyond merely discovering sensitive information and responding to a predefined violation, and factors in organizational context and security risks in order to dynamically enable the proper protection automatically based on changing conditions.

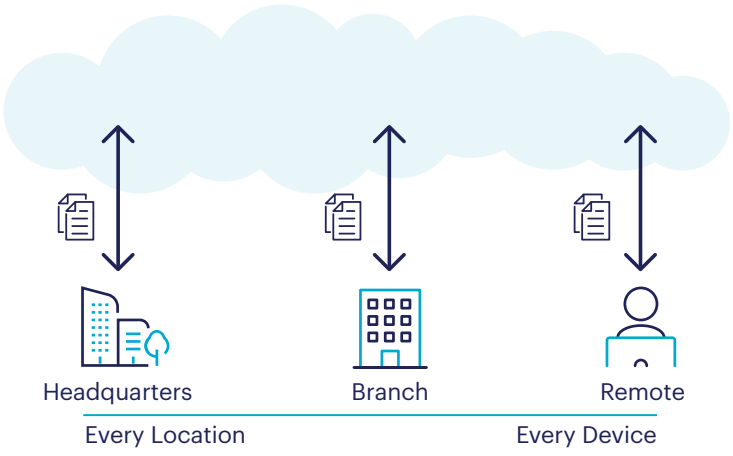
Netskope DLP is natively integrated to the comprehensive Netskope Security Service Edge (SSE) solution, a fully converged cloud-native security platform that consolidates security technologies, like SWG, CASB and UEBA, onto a unified, integrated cloud-native platform. This approach eliminates security blind spots, provides policy consistency, and dramatically reduces costs and complexity.

The platform is continually aware of users behavior, geolocation, security postures, device risks, application risks and reputations, personal application instances etc. and allows DLP to tailor incident response to true data security incidents, minimizing false positives, incident triage and business disruption.



Web Data Protection for all Networks and Work Anywhere

Corporate communications today happen effectively across a much broader spectrum of network connections than ever before. In fact, with hybrid work, users expose sensitive data as they access the web from remote locations in addition to the corporate networks. Moreover, corporate data can be accessed, uploaded and downloaded by managed and unmanaged endpoints, and



Netskope DLP ensures that sensitive data doesn't get leaked over untrusted and risky web traffic, including encrypted traffic. It detects, monitors and protects sensitive corporate data from being leaked and exposed over every web connection, from home offices, from public wifi locations and over cellular networks, in addition to the company campus network, the datacenter and the branch offices. It scans all corporate HTTP and HTTPS web traffic, it identifies sensitive information inline, and optionally removes sensitive HTML content or blocks requests. Netskope effectively provides protection and access control for web, application-based and non-web traffic, and additionally ensures that access to corporate assets from unmanaged devices is constantly verified and their traffic is scanned as well against the policies, while remote users are properly authenticated. Data exfiltration to unmanaged or personal devices can be also prevented and the users can be alerted and coached on security policies when performing risky activities. DLP is cloud-based and natively integrated with Netskope SWG, and doesn't require ICAP, SPAN, additional on-premises infrastructure, network configurations and traffic steering.

Protection	Data in-motion
Modes	Client-based, explicit proxy, proxy chaining
Web Categories	130+
Ports	All ports
Policy Actions	Alert, allow, bypass, block, forward, coaching etc.
Management	Unified console, policies and incident management across the entire DLP platform

Protect Data in the Cloud Across SaaS Applications

Software as a Service (SaaS) applications are a business enabler today by means of keeping all employees easily connected from any place they work, and making data conveniently available. With convenience comes risks, as data is exposed to new cloud threats, excessive sharing permissions, can be transmitted through thousands of unsanctioned apps, and can even be uploaded to personal instances of corporate SaaS apps. According to the Netskope Cloud and Threat Report, 2022, 83% of users use personal app instances on managed devices and average 20 file uploads each month.

Comprehensive Netskope DLP is an integral capability of Netskope multimode cloud access security broker (CASB), and seamlessly extends data protection policies to SaaS apps both inline and via APIs. The solution discovers, monitors and protects sensitive data in-motion and at-rest across corporate sanctioned SaaS apps like Microsoft 365, Salesforce, Google Workspace, and Slack. In addition, it discovers and protects sensitive data in-motion across more than 50,000+ SaaS apps, including data transmitted to personal app instances (i.e. corporate OneDrive to personal OneDrive) and risky apps. Sensitive information is discovered as part of more than 1,500 file types as well as within posts and asynchronous communications over collaboration apps like Slack, Teams and Zoom, and email.

The solution uses context and risk awareness to secure sensitive data with the proper protective action, based on conditions that may change over time, such as app risk scores through Cloud Confidence Index (CCI), security postures, user behavior and geolocation etc. Protections include unshare file, quarantine file, block file from leaving app, alert users about a violation, and apply strong encryption or digital rights management to data shared externally. Netskope also mitigates the risk of data loss via native controls like SaaS security posture management, threat prevention and behavioral analysis..

Protection	Data in-motion and at-rest
Modes	Multimode: inline and API-based
Web Categories	Sanctioned and unsanctioned SaaS applications, and IaaS
Policy Actions	Alert, block, change ownership, restrict access, encrypt, delete, quarantine, legal hold, restrict sharing, data classification, disable print and download, IRM protect, coaching etc.
Management	Unified console and policies across the entire DLP platform

Protect Data in the IaaS/PaaS Public Cloud

The increased data volumes collected and processed and the convenience of running data intensive applications in the cloud has led modern organizations to embrace infrastructure as a service (IaaS) data storage. Cloud native services for corporate data are highly scalable, available and durable, but if not properly protected and monitored, they can expose sensitive data in new ways outside the purview and control of security teams.

Netskope DLP extends discovery, monitoring and protection to sensitive data stored and shared within public cloud services including Amazon S3 buckets, Azure Blobs, and Google Cloud Storage. Industry-leading, machine learning-enhanced classification accurately uncovers sensitive data such as PII, source code, and access keys. Data protection, compliance and data privacy policies are consistently enforced across public cloud services and automatically synchronized across the entire Netskope DLP platform including SaaS apps, networks, email and users' endpoints.

The Netskope unified DLP solution is integrated as a service within the Netskope public cloud security platform in order to deliver data protection, threat prevention, cloud security posture management and behavioral analysis as a unified security strategy.

Protection	Data in-motion and at-rest
Modes	Inline and storage scan
Cloud coverage	Amazon Web Services, Microsoft Azure, Google Cloud Platform
Policy Actions	Alert, allow, bypass, block, forward, coaching etc.
Management	Unified console and policies across the entire DLP platform

Endpoint Data Loss Prevention

Endpoint devices are the means by which users access corporate resources and interface the web. More so today portable computing devices enable work from anywhere. Fundamentally endpoints allow users to do work, including creating sensitive corporate data and sharing it with others. As a consequence they represent a significant loss vehicle, often due to malicious user's behavior.

Netskope Endpoint DLP detects, monitors and protects sensitive data in-use through employees' endpoints, in order to prevent data loss and theft whether the device is online or even offline, regardless of its location. Netskope Endpoint DLP is integrated in the single Netskope client and will not require deploying a separate agent. Unlike traditional solutions, Netskope Endpoint DLP is designed to minimize resource utilization while featuring the full suite of capabilities, including ML-based classifiers, OCR, file fingerprinting, EDM, etc. In fact, it leverages the cloud DLP service, including the intelligence sourced across the entire DLP platform in order to avoid duplicate scanning if data originated in the cloud. This approach results in frictionless user experience and stronger protection outcomes. Endpoint DLP allows to:

- Leverage Netskope's full suite of DLP capabilities including ML classifiers, data fingerprinting and OCR.
- Detect and selectively prevent sensitive data transfers via USB.
- Enable USB device protection to prevent use of unsanctioned USB storage devices.
- Configure device control policies to manage how USB mass storage devices are allowed to operate on endpoints.
- Seamlessly extend predefined and custom-built profiles used elsewhere in the Netskope DLP platform to endpoint related content inspection
- Leverage existing scan results across every control point, such as inline and cloud apps, based on historical scans and content affiliation.
- Use new file origin capability to automatically protect files in use on the endpoint if those files have originated on certain corporate cloud apps (such as Salesforce).
- Achieve granular policy control using user and user group definition.

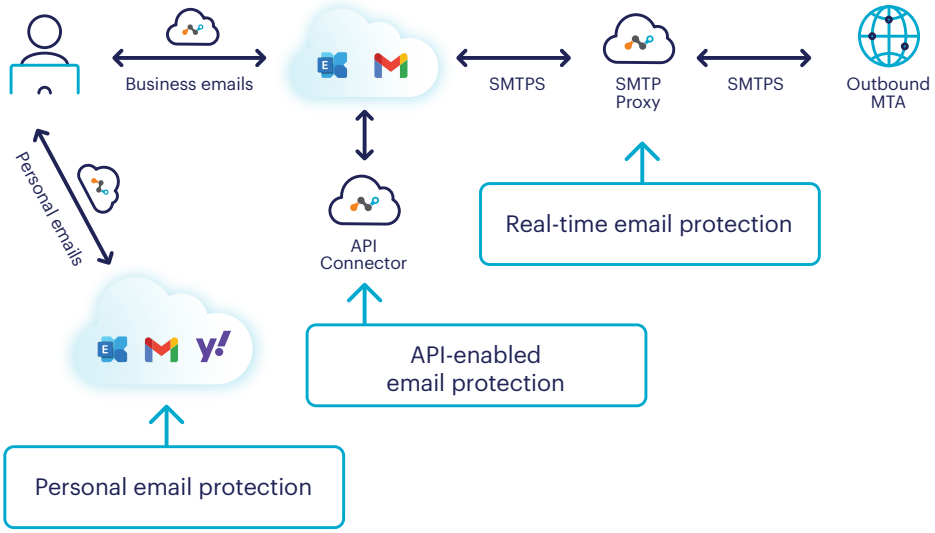
Protection	Data in-use
Agent	Part of Netskope Client single agent
Policy Actions	Allow; block, alert, user alert (coaching)
OS Support	Windows 10 x64, Windows 11 x64, macOS support for Big Sur and newer
Management	Unified console and policies across the entire DLP platform

Email

Email Data Protection

With business users today no longer meeting regularly in the office, virtual communications are expected to increase via email and collaboration apps. Email is used within the organization and externally and remains a predominant method of communication with customers, partners, and employees.

Netskope provides a very extensive DLP solution for email like Microsoft 365 and Gmail, and for both data in-motion and at-rest. The solution comprises:



- Real-time email protection inline for outbound sensitive emails sent via a corporate email account through SMTP proxy and webmail.
- Inline monitoring and prevention for sensitive data from leaving via a personal account (i.e. corporate Gmail vs. personal Gmail) or via private email services like Yahoo.
- API-enabled email protection to detect and respond to sensitive emails sent via corporate email services.
- Support for all email deployments including cloud email services, webmail and on-premises mail transfer agents (MTAs).
- Scan attachments, body, subject, and headers with the same DLP rules.
- Full suite of detection capabilities including file fingerprinting, EDM, OCR and ML based classification
- Limit DLP to only certain groups, users, or extend it to all users.

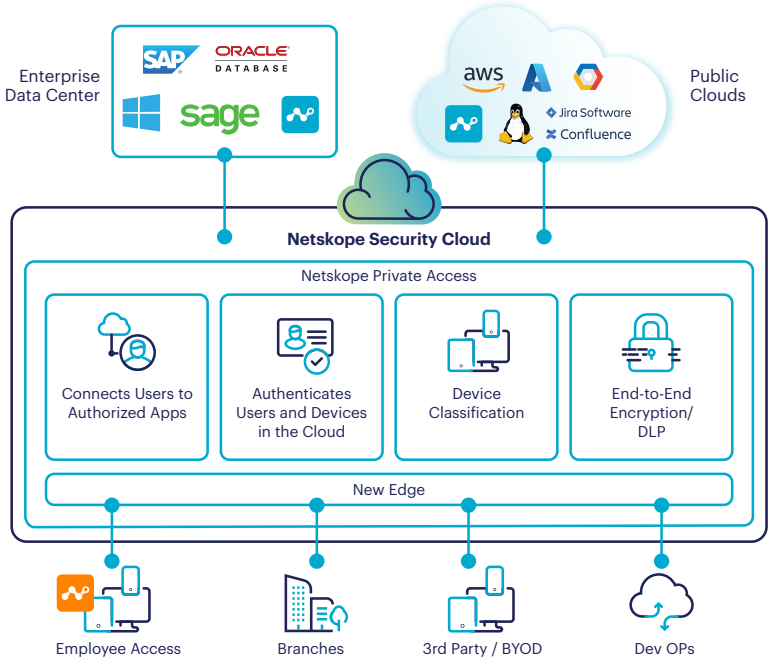
Netskope's single pass DLP approach simply extends unified DLP policies to email traffic, and conveys policy definition, incident management and reporting under a single DLP console for the entire solution.

Protection	Data in-motion and at-rest
Modes	Multimode: inline and API-based
Cloud coverage	Sanctioned and unsanctioned SaaS applications, and IaaS
Policy Actions	Alert, block, restrict access, encrypt, delete, quarantine, legal hold, restrict sharing, data classification, disable print and download, IRM protect, coaching etc.

Private Apps

Protect Data Accessed on Private Applications

Private resources hosted in data centers and public cloud environments are critical to the business for the sensitive data that they carry. It is paramount to secure access to private applications anywhere the users connect from, as well as monitor sensitive data movements, and prevent data exfiltration.



Netskope DLP is delivered via Netskope Private Access (NPA), remote access solution, in order to prevent data loss and exfiltration inline across private resources in the data center and in public cloud environments. Netskope DLP with NPA ensures data protection for browser-based access to private applications anywhere the users are, by inspecting both HTTP and encrypted traffic and automatically discovering, monitoring and protecting sensitive data in-motion. The solution is also built on the principles of Zero Trust Network Access (ZTNA), to connect users anywhere to private resources, providing authentication and secure access.

Protection	Data in-motion
Modes	Inline
Access Method	Browser
Policy Actions	Allow, block etc.
Management	Unified console and policies across the entire DLP platform

Protect Your Sensitive Data with Netskope DLP Today

92%

of IT organizations said Netskope's improved their data protection as compared to solutions they used in the past

Source: TechValidate

To learn more visit https://www.netskope.com/products/data-loss-prevention