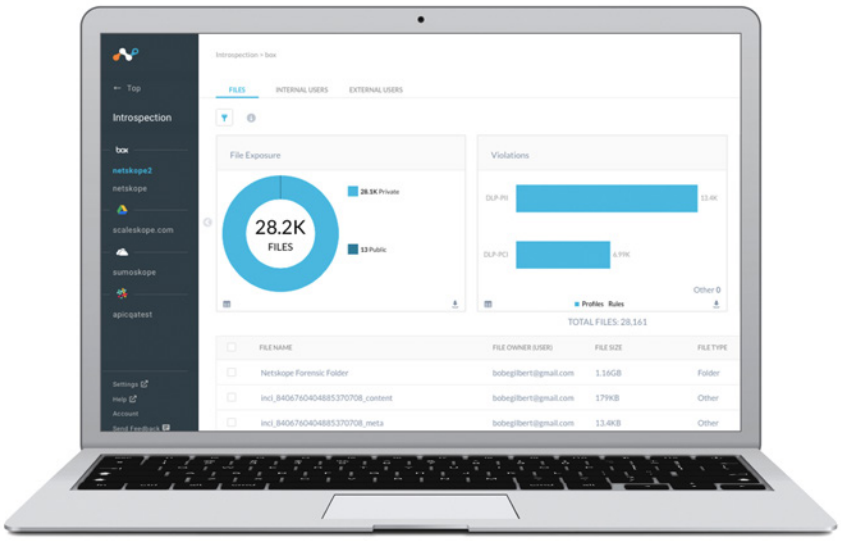
Netskope DLP

AT A GLANCE

- 360° data protection across SaaS, IaaS, and web
- Targeted data protection with Netskope Cloud XD™
- Advanced capabilities including fingerprinting, exact match, and optical character recognition



As data increasingly moves off-premises and into the cloud, you need data protection that is not just delivered from the cloud, but is architected from the ground up as a single engine that can be applied to SaaS, IaaS, and web, and can protect your data whether accessed from users on premises, mobile, or remote and from a browser, mobile app, or sync client.

PRODUCT OVERVIEW

Data is increasingly at risk as it moves outside the enterprise perimeter and beyond the reach of traditional security controls. This data movement started in the earliest days of the web, but is accelerating with the rapid adoption of cloud services, from IT-led services such as Office 365 and Amazon Web Services to the thousands of user- and business-led cloud services that are used in an average enterprise. With their ease-of-use and built-in capabilities for collaboration and sharing, these services make it all too easy for users to put sensitive information in the wrong place or share it with the wrong people.

You need a solution that can protect your data as it moves outside the enterprise perimeter to the cloud and web. Netskope DLP helps protect sensitive data wherever it is going – to SaaS applications, IaaS services, and to any destination on the web. Netskope has the most advanced DLP in the industry, designed for high accuracy and low false positives. Key capabilities include more than 3,000 data identifiers, support for more than 1,000 file types, custom regular expressions, proximity analysis, fingerprinting, exact match, optical character recognition (OCR), and more.

360º DATA PROTECTION FOR SAAS, IAAS, AND WEB

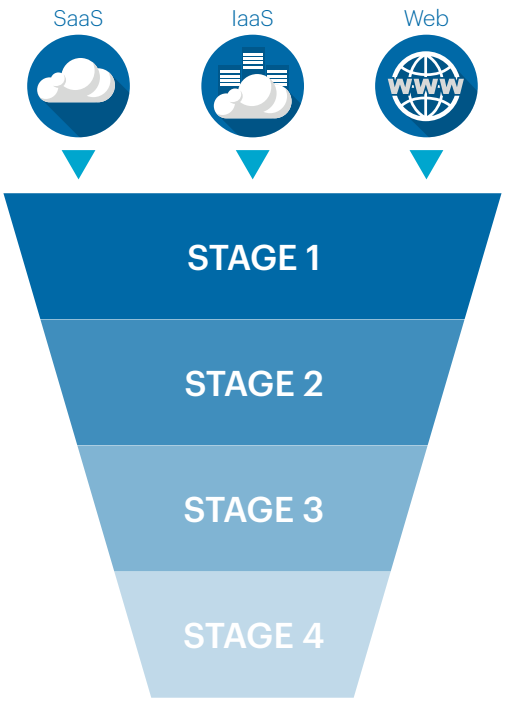
Netskope steers all Internet traffic through a centralized cloud enforcement point for SaaS, IaaS and web. From there, Netskope Cloud XD reduces data exposure by restricting risky cloud and web use based on a range of factors, including user, location, device, service, and activity. For necessary cloud and web activities, Netskope DLP provides an additional layer to detect and protect specific sensitive data moving to the cloud and web.

Stage 1: For risky cloud services that have a low security rating, Netskope blocks access to the cloud service or a specific cloud service instance. Netskope measures risk using the Netskope Cloud Confidence Index.

Stage 2: Netskope employs adaptive access controls that leverage identity, location and device information to determine the appropriate level of access. For example, allow view-only access from a risky location.

Stage 3: Using Cloud XD, Netskope enforces activity-level controls for risky activities like upload, download, share, create, post, publish, etc. It's important to enforce more stringent policies on the riskiest activities.

Stage 4: Netskope applies specific DLP policies to identify sensitive data and enforce data protection and compliance policies. Netskope reads data classification tags, performs exact match, fingerprints documents, and much more. And because Netskope only has to apply DLP policies to a subset of your data there are fewer false positives.



ADVANCED CLOUD DLP

Netskope DLP inspects all IT-led and business- and user-led cloud services, protecting sensitive data in the cloud and web with accuracy and precision. Sensitive content is detected across more than 1,000 file types and across structured and unstructured data, using more than 3,000 data identifiers, metadata extraction, proximity analysis, fingerprinting, exact match, OCR, and more.

- Control sensitive data resident in and en route to and from all cloud services
- Get the highest degree of accuracy with fingerprinting and exact match
- Further increase accuracy with keyword dictionaries, global data identifiers, and more
- Target DLP policies using Cloud XD to discern user, group, device, service, and activity

ONE DLP ENGINE AND CENTRAL POLICY INTERFACE FOR SAAS, IAAS, AND WEB

Unlike other products that attempt to combine disparate DLP systems to achieve functionality, Netskope DLP was architected from the ground up as a single engine that can be applied to SaaS, IaaS, and web. No separate management interfaces, special connectors, or policy collisions to deal with. This approach results in unparalleled coverage, efficacy, and streamlined incident management and operations.

FULL VISIBILITY

Detect DLP violations across all cloud services and web traffic with an all-mode architecture capable of covering all internet traffic whether your users are on premises or remote, using a web browser, mobile app, or sync client. This includes discovering sensitive data at rest in IT-led cloud services and en route to and from all cloud services and websites, IT-led, business-, or user-led.

- Detect DLP violations in all cloud services and web
- Gain visibility whether users are on premises or remote, using browsers, sync clients, or mobile apps
- Go beyond content by inspecting metadata, hidden fields, comments, and images
- Find violations in structured and unstructured data in webmail, social media posts, and instant messages

INCIDENT MANAGEMENT

Respond quickly and thoroughly to DLP policy violations. Take advantage of Netskope incident management capabilities for end-to-end workflows. Perform forensic analysis with comprehensive, deep activity audit trails. Assign owners, track progress, and mark as resolved.

- Closed-loop administrative and remediation workflows
- Detailed forensics for a comprehensive view of alerts
- Event-by-event activity audit trail
- Customizable role-based access controls

DLP INTEGRATION

Netskope DLP integrates with your on-premises DLP so you get the most out of your existing investment. You have the choice of detecting data violations and enforcing controls entirely in the cloud or funneling cloud violations to your on-premises DLP and incident management systems via secure ICAP and our REST API.

Top Use Cases

COMPLIANCE

Whether you need to comply with mandates such as HIPAA, GLBA, PCI/DSS, or another regimen, Netskope has you covered so you can pass audits and avoid fines. With Netskope DLP, you can construct activity audit trails, create summary compliance reports, protect sensitive data with strong encryption, and manage data incidents.

PREVENT DATA LOSS

Netskope provides a unique vantage point across all of your cloud services to help you detect data movement that could signal a data exfiltration attempt by an insider. Netskope anomaly detection combined with our DLP capabilities can correlate the download of sensitive data from a sanctioned cloud service like Salesforce or Box with the upload of the same data to a personal cloud service.

SECURE DATA

Uncover sensitive content using predefined (or custom) profiles for payment card industry data (PCI), protected health information (PHI), and many more. Protect with automated workflows to block, quarantine, or encrypt your data. With Netskope DLP, you can identify and secure all sensitive data in the cloud, whether it's in transit to and from a cloud service or already resident in a sanctioned cloud service like Box or Office 365 OneDrive.

DATA VISIBILITY

Whether it's to satisfy auditing requirements, compliance, or just corporate security policies, it's important to understand where your most sensitive data is flowing and how it's being used. Netskope gives you a comprehensive understanding of not only all cloud activity, regardless of device, network, or location, but also allows you to identify all sensitive data flowing in the cloud and detect DLP violations with an all-mode architecture capable of covering all cloud traffic whether users are on premises or remote or on a web browser, mobile app, or sync client. This includes discovering sensitive data at rest in sanctioned services and en route to and from all services, sanctioned or unsanctioned.

Netskope DLP Features

Netskope DLP is sold as a separate SKU and requires the purchase of the Netskope Security Cloud or at least one of Netskope's API Protection SKUs (e.g., Netskope for Office 365). Netskope DLP is available in standard and advanced options. Features marked with an * are not available in standard.

REAL-TIME AND API PROTECTION		
Options	More than 3,000 pre-defined data identifiers Fingerprinting and Exact Match capabilities* Perform secondary DLP analysis for content leveraging on-premises DLP solution Custom profiles & regular expressions Rules support global identifiers and severity levels	Multi-data identifier classification with Boolean operations Pattern & keyword matching Hundreds of industry standard DLP categories Further increase coverage with OCR to extend DLP policies to images*
File Types	Inspection for more than 1,000 file types	
Supported Regulations	Leverage dozens of pre-defined policy templates to identify sensitive data in accordance with regulations. Templates include (but are not limited to): AMRA, EC Directive, EU-GDPR, GLBA, HIPAA, PCI-DSS, PHI, PII, PHIPA,PIPEDA, SSN Confidentiality Act, US FTC Rules, etc.	
Non-regulated Data Types	Intellectual property data Financial and legal terms	National ID numbers International Bank Account Numbers (IBAN)
CONTEXT AWARE		
Policy Is Enforced On	Users, user groups, organization unit, custom user list Applications, application instances, application categories File sharing options File types and size Activity types: Upload, download, view, post, send and share	Device types: Desktop or mobile Device classification: Managed and unmanaged devices Location types: On-premises and remote Geo location: Source and destination Operating system and browser Sync client
INCIDENT MANAGEMENT AND REMEDIATION		
Complete Context and Visibility of the Violation	Forensic information of excerpts of the violation Get granular alerts of violations in SkopeIT DLP and Compliance based reports	
Incident Workflow	Assign incidents to investigate override severity Customizable status for workflows	
Remediation Workflow	Contact the owner Quarantine and restore Restrict file permissions	
Automatic Policy Actions	Alert, Block, Encrypt User Notification and Coaching (redirect to custom notice) Quarantine and Legal Hold	