netskope

Netskope Active™ Cloud DLP

- Utilize accurate and efficient noise-cancelling cloud DLP
- Complement your on-premises DLP solution
- Prevent sensitive data leakage with adaptive workflows

Introduction

Organizations are adopting cloud apps in a big way. Cloud apps help people be more productive in their jobs, offer anywhere access to important business tools and data, and enable groups to collaborate more easily. Despite its benefits, the cloud also makes it easy for people to lose sensitive corporate data. For one thing, people can access cloud apps from multiple devices more easily. Another is that the cloud makes it easy to share data, including with people outside of a company. For these reasons, it is easy for data to get out of an organization's control.

You need to take the necessary steps to identify and protect sensitive data in the cloud while ensuring that employees continue to be productive and use the best tools for the job. Protect the data you can least afford to lose — your intellectual property, non-public financials, strategic plans, customer lists, customers or employee personally identifiable information (PII), and other data you deem sensitive.

One of the commonly known challenges with data loss prevention (DLP) is that it creates a lot of false alarms — noise — that makes it overwhelming for information security admins to manage on a daily basis. Also, most organizations have an existing on-premises DLP investment that they would like to leverage so it's important to find a complementary solution for the cloud.

Cloud DLP without the noise

It is evident that organizations need to identify and protect sensitive data in the cloud. However, simply using your existing DLP solution to scan all at-rest and en route cloud data will result in a significant number of false positives or false negatives. The challenge with trying to apply traditional DLP thinking to the cloud is that detection accuracy and efficiency have limited effect when performing DLP scans on cloud data.

Netskope's ability to incorporate proximity analysis, using predefined or custom proximity templates, and categorize the severity of a violation based on number of occurrences, is critical to making deterministic detections and enables you to focus on curtailing the most critical violations first.

With features such as Fingerprinting, Netskope allows organizations to catalog their documents and create a unique DNA for sensitive files. This DNA is used to more efficiently discover DLP violations of whole files or even trace amounts of sensitive data in files. When coupled with Netskope's ability to target DLP rules to content or metadata or a combination of both, this makes your results more precise.

Additionally, Netskope's Exact Match capability reduces misclassification by performing an extra pass of detected sensitive data against customer specific sensitive data. This helps further reduce the noise and make detection very custom to your organization. Based on the same Netskope machinery, you can whitelist certain enterprise data that you know will appear repeatedly in your files and cancel any additional false alarms that may be attributed to it.

Netskope's global identifiers allow you to find sensitive content in unstructured data. Using global identifiers makes it simpler to write effective DLP rules and, when used in combination with proximity templates, allows for superior accuracy in detecting sensitive content.

Each of these features is powerful on its own, but when combined together they make the solution formidable since they give Netskope its true competitive edge: Noise-Cancelling DLP — the ability to significantly reduce false positives and false negatives to create a high-fidelity DLP solution.

Complements Your On-Premises DLP

Another challenge is that many organizations have an existing on-premises DLP investment that they want to leverage for the cloud. Customers want to increase accuracy and efficiency and leverage their existing investment whenever possible. However, backhauling all of your cloud data to your premises for inspection is not the right solution.

Netskope Active Cloud DLP features the most elegant integration with on-premises DLP and incident management systems, performing a first pass of sensitive content discovery in the cloud for efficiency, and then directing suspected violations to your organizations' highly-tuned DLP solutions via secure ICAP.

Context and Activity Aware

With increasing amounts of your corporate data moving to and being created in the cloud, identifying and protecting what's truly sensitive is a challenge. Traditional content inspection techniques can lead to false positives or false negatives. Before you even begin inspecting content and enforcing policies to protect data, you should have the relevant context of the activity. The Netskope Active Platform enables you to incorporate cloud app and usage details such as the app, its category, its enterprise-readiness score per the Netskope Cloud Confidence Index™, the user or group, location of the user or app, time of day, device, browser, and user activity (e.g., upload, download, or view) into your policies, which helps you be precise in identifying potential data loss scenarios so you can protect data in a targeted way. This aids in reducing the surface area of potential DLP violations, which further increases the accuracy of sensitive data detection and protection.

Industry-leading Content Inspection

Once you have identified the context of potential cloud data loss for your organization, you can begin inspecting content and enforcing your DLP-enriched policies. Netskope Active Cloud DLP uses industry-standard content inspection incorporating more than 3,000+ language-independent data identifiers, more than 500 file types, with the added benefit of support for language agnostic double-byte characters, custom regular expressions, proximity analysis, and document fingerprinting. These come together to form DLP rules, which comprise profiles. From those profiles, you can set precise, contextual policies in the Netskope Active Platform that can be applied to data en route or at rest in the cloud. This translates to confidence that you are using proven, industry-standard DLP building blocks in your policies.

Adaptive Workflows

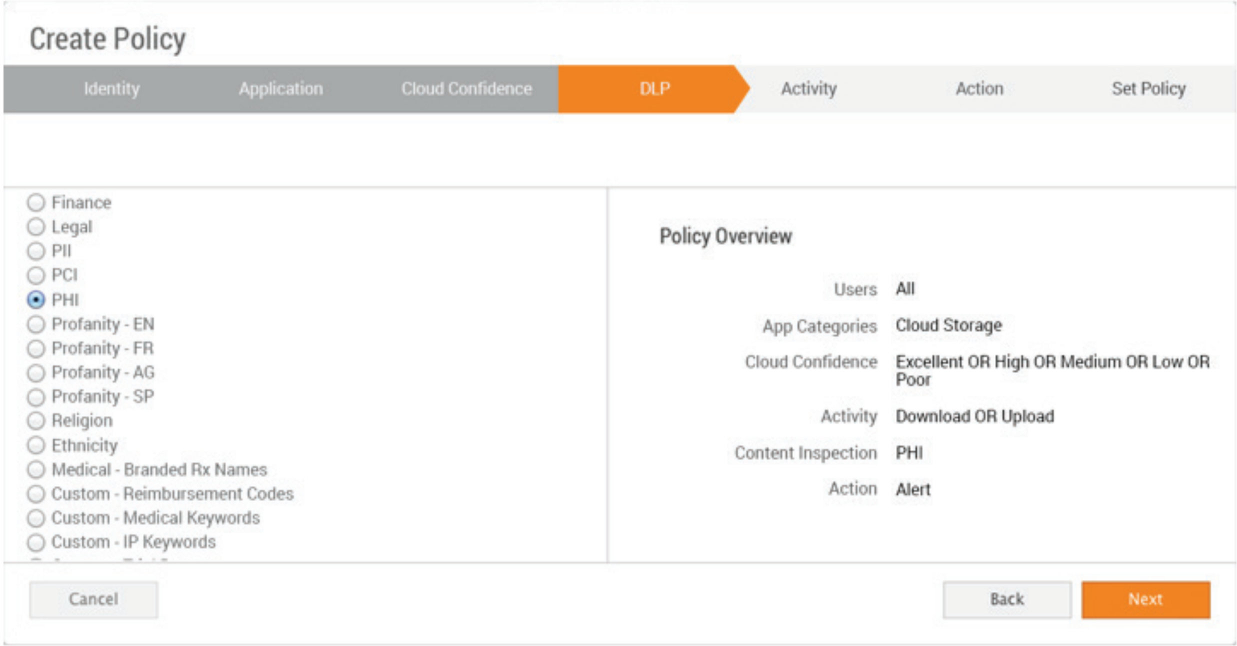
Only Netskope offers important DLP workflows such as quarantine, legal hold, content encryption, automatic elimination of public access to sensitive content, user notification, and event visualization in corporate SIEM systems. These capabilities ensure IT and legal have a way to make DLP actionable while keeping users in the loop.

Strong Encryption

Add an encryption action to DLP policies and ensure your sensitive data stored in the cloud is secure. Netskope Active Cloud DLP uses AES 256-bit encryption for data that is stored in your cloud apps. While Netskope has made a significant investment in ensuring your data is secure, we have also made a similar investment to ensure a seamless user experience while dealing with encrypted data.

Flexible and Easy to Use

Netskope Active Cloud DLP is flexible and easy-to-use. It offers a simple wizard for you to either define your own custom DLP profile or choose from industry-standard pre-defined profiles that were built based on standard combinations of data identifiers.



○ Finance
○ Legal
○ PII
○ PCI
● PHI
○ Profanity - EN
○ Profanity - FR
○ Profanity - AG
○ Profanity - SP
○ Religion
○ Ethnicity
○ Medical - Branded Rx Names
○ Custom - Reimbursement Codes
○ Custom - Medical Keywords
○ Custom - IP Keywords

Policy Overview

Users	All
App Categories	Cloud Storage
Cloud Confidence	Excellent OR High OR Medium OR Low OR Poor
Activity	Download OR Upload
Content Inspection	PHI
Action	Alert

The profile types you can choose from include:

- **Pre-defined profiles.** Profiles built from rules that incorporate standard combinations of data identifiers. This includes Payment Card Information (PCI); Personally-Identifiable Information (PII); Personal Health Information (PHI); Source Code and Profanity. Using pre-defined profiles lets you take advantage of established best practices and start preventing loss of critical data in the cloud immediately, out of the box, without having to be a DLP expert.

- **Custom profiles.** Custom profiles built from a library of more than 3,000 data identifiers arranged in an easy-to-navigate menu. You have the flexibility to set global identifiers, use Boolean expressions using AND plus OR operators, choose to scan content or metadata or a combination of both, and set severity thresholds for data identifiers seen, within DLP rules. Using custom profiles will allow you to be surgically specific about identifying sensitive data and preventing its loss from your organization. You can also clone and customize pre-defined profiles for rapid profile development.

- **Customized profiles.** You can customize your own profile based on keywords or a regular expression specific to your organization. Using custom expressions will help you protect data in a way that's specific to your organization, such as with a watermark.

Netskope Active Cloud DLP is also flexible in the way it provides you DLP intelligence. Within a couple of clicks, you can easily see the exact DLP profile that was triggered and how often it may have been matched in your policy.

Unlike other DLP solutions, which are either too basic or so arcane that they require dedicated security personnel, Netskope Active Cloud DLP is simple and flexible, letting you define DLP profiles and get your policies up-and-running in minutes, and then gain powerful intelligence about data loss in your environment — all within a simple workflow.

Real-time Across Any App

In the Netskope Active Platform, analytics and policy enforcement happen in real-time and across any app. Netskope's unique architecture, including the normalization of activities across cloud apps, ensures that you can set a policy once and it will be enforced immediately at the app, category, or global level. This is true whether your users are on-premises or remote, on a PC, laptop, or mobile device, and working in a web browser or native app. Netskope Active Cloud DLP takes advantage of this architecture. This means, for example, that when you set a policy blocking the download of PHI data from any Cloud Storage app onto a mobile device, you have the assurance that rather than have to do this app-by-app, you can set the policy once and it will take effect across all apps meeting those criteria in real-time, and at enterprise scale.

Find Stored Content and Secure It

Netskope Active Cloud DLP works in conjunction with Netskope's Introspection feature, which enables you to discover content resident in your cloud apps, no matter when it was uploaded. View the exposure of your sensitive files by finding out whether they are private, shared internally or publicly, understand who has access inside and outside of your organization, and get an activity audit trail for each file. You can see information such as DLP violations, encryption status, file type, file owner, who your biggest violators are, and you can take action immediately.

Requirements

Netskope Active Cloud DLP is sold as a separate SKU and requires the purchase of the Netskope Active Platform or one of the Featured Apps products.

INSPECTION AND INTROSPECTION	
Inspection and Introspection Options	› Over 3,000 pre-defined data identifiers › Fingerprinting › 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
File Types	› Inspection for over 500 file types
Supported Regulations	› PII, PHI, PCI, Source Code and Profanity
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 › Activity types – Upload, Download, View, Post, Send and Share › Device types – Desktop or mobile › Location types – On-premises and remote › Geo Location › Time
POLICY ENFORCEMENT	
Types	› Alert, Block, Encrypt › User Notification and Coaching (redirect to custom notice) › Quarantine and Legal Hold
Active Policies	› Simple and intuitive policy creation › Ease of use – built-in profiles
SkopeIT	› Separate event types › Number of policy violations are captured in log events
Reports	› Custom- and compliance-centric reporting

About Netskope

Netskope™ is the leader in safe cloud enablement. The Netskope Active Platform™ gives IT the ability to find, understand, and secure cloud apps. Only Netskope empowers organizations to direct usage, protect sensitive data, and ensure compliance in real-time, on any device, for any cloud app so the business can move fast, with confidence.