8 Steps to Upgrade to Modern DLP

Why Stay with a Legacy DLP Deployment Anyway?

Traditional DLP deployments carry the legacy of accumulated components, maintenance time, patching and expansions, and don't solve well for modern hybrid work use cases. Moving away from such a composite infrastructures is never an easy task, but today's organizations that seek agility and scalability through their digital transformation can rely on Netskope. Cloud-delivered DLP from Netskope consistently protects all sensitive data across every on-premises and cloud environment by means of a consolidated data protection solution that is easy to deploy and scale.

There is no right or wrong way to migrate to Netskope DLP. Most organizations adopt the entire solution from the beginning, others transition step by step, leveraging current investments and building upon them, through their maturity stages. To make it easy, Netskope provides a single console and unified data protection policies for every location. The journey typically follows this course of action:

1

Reassess your data protection needs.

The first stage is to conduct a thorough assessment of your current technology environment, to identify and understand what data must be protected, which services and repositories are being used today by the organization to store and process sensitive information, and how these services are being used. This stage can also reveal that certain portions of legacy DLP deployment (like on-premises storage discovery) are perhaps less useful now and may not be as worth the investment as they were before because more data is stored in cloud repositories.

2

Protect data in motion through every web connection.

With hybrid work and more data in the cloud, sensitive data can now be accessed, uploaded, and downloaded beyond the oversight of IT. A traditional "proxy-connected" DLP solution sitting in the data center covered data in motion only through physical gateways. Netskope DLP leverages cloud SWG and ZTNA to cover the entire enterprise ecosystem to secure sensitive data anywhere people work when accessing web, SaaS apps, IaaS, and private apps using zero trust principles and without any constrictions.

3

Many organizations start with cloud apps.

Solving for new cloud data protection use cases is usually the motive that leads information security organizations to transition to modern cloud-delivered data protection. More and more data living across corporate SaaS applications, cloud email, and IaaS today is exposed to unintentional data sharing, malicious exfiltration, and other cloud-based cyber threats. Netskope's market-leading CASB solution embeds DLP as its core component. This approach solves for both data protection on corporate cloud applications and for the protection of sensitive data in motion, especially when data is moving across thousands of unsanctioned and possibly risky apps.

4

Cloud email is another starting point.

The corporate migration toward cloud-based email services requires the implementation of cloud-based DLP. Netskope provides a very extensive email DLP solution that includes services like Microsoft 365 and Gmail for both data in motion and at rest and also supports hybrid email environments. The solution comprises real-time protection for outbound sensitive emails sent via a corporate account through SMTP proxy and webmail, via a personal account (i.e., corporate Gmail vs. personal Gmail), or via private email services. It supports all email deployments including cloud email services, webmail, and on-premises mail transfer agents (MTAs).

5

Protect data on employees' endpoints.

Sensitive data can be created, downloaded, and transferred through users' endpoints. Endpoint DLP remains a fundamental control. Netskope cloud DLP is native to the Netskope unified client and does not require a separate endpoint agent. It is designed to minimize resource utilization while featuring the full suite of advanced DLP capabilities including ML classifiers, OCR, File Fingerprinting, Exact Data Match, etc. It provides device and content control to protect sensitive data whether the device is online or offline, on the corporate network, or anywhere else.

6

Apply the same policies to every channel for consistency.

Netskope DLP is a centralized cloud solution that supports all Netskope services as you extend data protection to additional environments including SaaS apps, IaaS, web, email, endpoint, etc. This means that Netskope DLP policies are created once and are easily portable, allowing a single DLP policy framework irrespective of the traffic vector being protected. When DLP rules are violated, a variety of actions can be taken for automatic remediation that are appropriate for the specific channel.

7

Build upon a solution that is working now.

If a recent investment was made toward SaaS-native DLP capabilities, and the solution is solving present needs, it's wise to augment it with Netskope advanced DLP. But as the organization is planning to extend data protection to multiple clouds, SaaS apps and on-premises, these siloed DLP environments could turn into too many consoles and disjointed policies. Plan to move to the entire Netskope DLP solution in order to ensure consistency, uniform policies, and single console. Netskope DLP also leverages existing data classification, DRM, and other adjacent data protection technologies.

8

Take advantage of newer capabilities offered by Netskope.

Modern use cases require an updated approach to data protection. Netskope DLP expands the scope of data protection by delivering advanced data detection technologies driven by ML, superior performance and computing scale, and more accurate risk mitigation. With Netskope, DLP is no longer a standalone solution, but it leverages the broadest organizational and risk context across all users, devices, networks, applications, and data to dynamically adapt to risks, behaviors, instances, and security postures across the entire organization. This integrated approach helps make better risk-based decisions and dramatically minimizes false positives, incident triage, and business disruption.

The experience built by the internal DLP practitioners (the policy admins, the incident response team, etc.) over the years with the existing legacy DLP solution is an extremely valuable asset that can be leveraged to adopt best practices and ensure that all the technological expectations are met, including producing compliance policy profiles and establishing the proper remediation workflows. As the Netskope DLP minimizes the program's efforts, security teams can spend less time on management and frustrating incident triage, and more on substantive security activities and proactive initiatives. Learn how Netskope helps customers be ready for anything at https://www.netskope.com/products/data-loss-prevention.