netskope

TOP QUESTIONS TO ASK YOUR CLOUD DLP VENDOR

Data Protection remains a top priority for organizations worldwide. As new communication and collaboration norms evolve, it's imperative to ensure your organization's security posture is up-to-date and capable of reducing risk of data loss, exposure and exfiltration across your multi-cloud, web and email environment. This check list will provide guidance on how to choose the right data protection solution for your organization.

QUESTION:

CAN I PROTECT SENSITIVE DATA FROM ALL THE WAYS IT CAN LEAVE MY ORGANIZATION?

EXPLANATION:

With the explosive growth of cloud applications and services, combined with an increasing number of remote workers, data loss vulnerabilities are more prevalent than ever before. Security teams must be able to discover, monitor and protect sensitive data regardless of location, application, and device type.

Over 20% of users have sensitive data moving between cloud apps

37% of this data is involved in DLP violations

97% increase for personal use of managed devices

– Netskope Cloud and Threat Report, 2020

The top two causes of data breaches:

1) **Hacking / malware** from an outside party, (32%), and

2) **Insider Threats** maliciously and inadvertently from employees and contractors (24%)

– CSI Data Security Report, April 2020

NETSKOPE ADVANTAGE:

The Netskope Security Cloud facilitates the most comprehensive monitoring and control at the activity and content level, whether users are on-premises or remote, on a mobile device or even using mobile apps, browsers, or sync clients. Moreover, Netskope lets you differentiate your policy enforcement between managed (corporate) and unmanaged (personally-owned) devices. Netskope is the only cloud security solution that covers all possible cloud traffic regardless of location, device, or network.

TEST FOR IT:

Attempt to trigger a DLP policy using a cloud application's sync client. Place a trigger file in the local sync folder and confirm the policy is enforced and a coaching message is displayed to the user when sync is attempted. Separately, test that a DLP policy can prevent both upload from a managed device and also download to an unmanaged (personal) device.

QUESTION:

CAN I SEE AND SECURE DATA IN ALL CLOUD APPLICATIONS AND SERVICES, WHETHER MANAGED OR UNMANAGED (SHADOW IT)?

EXPLANATION:

Many security solutions only allow for DLP policy enforcement for managed cloud services like Microsoft Office 365, Google Workspace (formerly G Suite), Salesforce, Box, and the like. For unmanaged, shadow IT services, most security solutions either cover a limited amount of services (<20) or none at all, creating a gap in your overall security posture.

The average company uses **2,415 cloud apps**

Over 95% of these apps are unmanaged and unapproved by IT

– Netskope Cloud and Threat Report, 2020

NETSKOPE ADVANTAGE:

Netskope protects and manages the leading cloud services as well as thousands of unmanaged ones, unlike other solutions. With managed application suites like Microsoft Office 365, the Netskope Security Cloud allows for DLP policies to be set across the entire suite, not just Teams, SharePoint, OneDrive, and Outlook, but also services like Dynamics, Power BI, and more. Netskope detects and protects sensitive data traversing these cloud applications within Office 365 as well as between its ecosystem applications. Whether shared via a chat in Teams, emailed via Outlook, posted to OneDrive or copied from SharePoint to Dropbox, Netskope DLP sees and stops sensitive content from leaving your organization through unauthorized means. For shadow IT, with comprehensive deployment options and a granular extensive policy engine, Netskope protects thousands of unmanaged cloud services in real time.

TEST FOR IT:

Set a DLP policy for sensitive information such as PII or PCI. Use this policy to restrict uploads of sensitive information to the top shadow IT cloud services used in your organization. Be sure to test the policy for employees that are both on-premises and working remotely.

QUESTION:

CAN I DETECT AND PROTECT SENSITIVE DATA IN MY PUBLIC CLOUDS (IAAS/PAAS)?

EXPLANATION:

Enterprises are now deploying more than half of their workloads in the cloud - which means that their data is also following suit. As there is a shared responsibility model between users and cloud providers for securing public clouds, its imperative that Security teams understand where all of their sensative content resides within their multi-cloud environment and secure it effectively. This includes ensuring that data in their storage buckets and blobs is not inadvertantly exposed to public, unauthorized access.

"By 2021, 50% of enterprises will unknowingly and mistakenly have some IaaS storage services, network segments, applications or APIs directly exposed to the public internet"

"Through 2023, at least 99% of cloud security failures will be the customer's fault"

– Gartner, Innovation Insight for Cloud Security Posture Management, January 2019

NETSKOPE ADVANTAGE:

Netskope is the only security platform that can set DLP policies consistently and uniformly across cloud storage resources like Amazon S3 buckets and Microsoft Azure blobs, simplifying data protection in multi-cloud environments. Utilizing API-enabled controls, Netskope scans terabytes of cloud storage for misconfigurations (such as open SSH access), embedded threats (such as malware) and sensitive data to ensure content is identified and protected based on best practices and industry standard guidelines. Additionally, inline, real time controls are provided to protect data moving between cloud storage services with granular capabilities based on users, groups, activities, app instance and more.

TEST FOR IT:

Create a DLP policy for sensitive information such as PII or PCI and use it to restrict the upload of sensitive files to an AWS S3 bucket or Azure Blob storage. Combine the DLP policy with a granular access policy to allow only a specific group of employees to upload the sensitive data.

QUESTION:

CAN I SECURE SENSITIVE DATA IN UNMANAGED, SHADOW IT CLOUD APPLICATIONS INSTEAD OF HAVING TO BLOCK USEFUL APPLICATIONS ALTOGETHER?

EXPLANATION:

Most cloud security tools provide archaic "allow" or "block" policies for unmanaged applications. This is an extreme approach that can hinder business productivity. Instead, consider an approach that allows select access and activities with restrictions so that your outlier app users can maintain their work while doing so safely. For example, setting policies to "block sharing of sensitive data in any cloud storage service if the recipient is outside of the company" mitigates risk while allowing employees to use their preferred storage apps. Likewise, allowing employees to use personal email accounts like Gmail for non business matters — with restrictions on specific activities like uploading / sending sensitive content — would enable your workforce while reducing risk.

The first half of 2020, saw a **161% increase in visits** to high-risk apps and sites

83% of users use personal app instances on managed devices and average 20 file uploads each month.

Top personal apps users upload sensitive data to via managed devices include:

1. Microsoft OneDrive
2. Google Drive
3. Google Gmail
4. iCloud
5. WeTransfer

– Netskope Cloud and Threat Report, 2021

NETSKOPE ADVANTAGE:

The average enterprise has more than 2415 cloud applications and services, with over 95% of these typically not managed and secured by IT. While some of these apps are not appropriate for your business, many are useful or even critical. The Netskope Security Cloud lets you understand and secure sensitive data granularly at an activity-level (and based on other factors like AD group, geo- location of app or user, device type, application, and app instance, or ownership status, and content type or classification), enabling you to restrict flow of sensitive data while still allowing the cloud service, even if it's shadow IT.

TEST FOR IT:

Apply a DLP policy to inspect uploads to an unmanaged, higher risk cloud service like Zippyshare or WeTransfer. Prevent the upload from completing and present a coaching message to the employee recommending the use of a corporate-managed cloud storage app instead.

QUESTION:

HOW ROBUST AND ADVANCED ARE YOUR DLP CAPABILITIES?

EXPLANATION:

Finding and securing sensitive content across the web and cloud is critical, yet cumbersome and inaccurate with outdated tools. Many organizations, including highly-regulated ones, have sensitive data that goes beyond what can be found with pre-defined DLP profiles. To optimize your organization's security posture, your cloud DLP needs to have advanced DLP features like exact match, fingerprinting of documents, support for custom keywords with weighted dictionaries, and more. Furthermore, modern technologies like machine-learning can enhance and expedite data scanning and classification, while reducing false positives and time-consuming incident response.

NETSKOPE ADVANTAGE:

Netskope detects and protects your sensitive data no matter where it is. Supporting 3,000+ language-independent data identifiers, 1500+ file types, proximity analysis, volume thresholds, international double-byte characters, document fingerprinting, content exact match, “and” and “or” rules, optical character recognition (OCR) and validation mechanisms such as Luhn check for credit cards, Netskope has the most comprehensive cloud DLP in the market. Machine learning-enhanced data scanning and classification also accurately identifies and protects sensitive content in documents like financial forms and patents, as well as images, including passports, driver licenses, screen shots, whiteboard images, and more. This significantly reduces false positives and provides no-touch protection that simplifies operations.

TEST FOR IT:

Create a document fingerprint using the DLP solution and use it to prevent copies of the source document being uploaded to any cloud storage application. Enable the machine learning capabilities of the DLP solution and use them to prevent sensitive data being uploaded to unmanaged cloud applications by automatically classifying data such as source code, screenshots or whiteboard images.

QUESTION:

CAN I REDUCE COMPLEXITY AND MANAGEMENT OVERHEAD BY APPLYING ONE DLP POLICY THAT COVERS SAAS, IAAS, WEB, AND EMAIL?

EXPLANATION:

Many security vendors require multiple DLP systems: One DLP system to cover SaaS applications, another DLP system to cover web, and yet another for email and/or public clouds. This approach is not only challenging operationally, but also impacts your ability to effectively implement incident management workflows that track DLP policy hits across all inspection targets.

NETSKOPE ADVANTAGE:

The Netskope Security Cloud is a scalable and extensible platform that provides a single, consistent cloud DLP for SaaS, IaaS, web, and email and requires no special aggregation or connectors, since the DLP engine and associated policies are unified from the start. This 4-in-1 consolidation dramatically simplifies and streamlines DLP policy administration, operations, and incident management.

TEST FOR IT:

Configure a DLP policy that classifies sensitive data such as PCI or PII. Apply that DLP policy across managed and unmanaged SaaS (e.g. OneDrive corporate and personal), IaaS (e.g. AWS S3 or Azure blob storage), websites (e.g. posts in forums or social media) and corporate email (e.g. SMTP from Exchange Online). Confirm that the DLP incidents generated can, in all cases, be investigated within the same administrative console.

THE ADVANTAGE OF NETSKOPE DATA PROTECTION

Eliminate blind spots

Netskope Cloud XD™ understands the modern language of the cloud and web (i.e. APIs, JSON, Protobuf) in extreme definition to eliminate blind spots throughout your cloud and web environment.

Detect and protect data everywhere

4-in-1 data protection for data -at-rest and data-in-motion across your SaaS, IaaS, web and email environments using machine-learning enhanced classification and consistent, uniform and intuitive policies.

Stop elusive attacks

Advanced threat detection exposes malware hidden in data-in-storage, while user and entity behavior analytics (UEBA) detects and prevents insider threats like bulk data movement and downloads.

Full control, with one console and one global cloud

Take full control of securing your cloud applications, web and email using the Netskope Security Cloud, its single, comprehensive admin console, a single-pass policy enforcement engine, as well as, NewEdge, am optimized carrier-grade, high-performance global cloud that brings security close to you.

SASE-ready architecture

The Netskope Security Cloud is future-proof and based on the Secure Access Service Edge (SASE) model, providing an extensive platform that consolidates DLP, CASB, SWG, ATP, ZTNA technologies and more utilizing the NewEdge optimized global private cloud for high-availability and scale.

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, email and private apps from anywhere, on any device. Only Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks, empowering the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey. Reimagine your perimeter with Netskope.

To learn more about how the Netskope Security Cloud can protect your data, visit **https://www.netskope.com/products/capabilities/data-protection.**

netskope

netskope.com