netskope

SOLUTION BRIEF

Netskope for Microsoft Information Protection

Industry experts agree that email is the most commonly used data-loss vector today. Even as collaboration tools are increasingly popular and IT security teams focus on safeguarding data shared in this way, traditional email communications must be also vigilantly protected. Netskope and Microsoft Information Protection (MIP) provide security solutions that can help.

KEY USE CASES

- **Secure critical data in storage.** Detect and protect sensitive data stored in managed cloud applications like Microsoft OneDrive.
- **Prevent data loss through email.** Stop sensitive content from being emailed outside of your organization.
- **Protect sensitive collaborative content.** Ensure that sensitive data is labeled and encrypted before it moves between cloud apps like Microsoft Teams and SharePoint.
- **Facilitate consistent policies.** Create and enforce data protection policies across SaaS, IaaS, web, and email by using labels.

"The MIP integration with Netskope means consistent and appropriate management and usage of data wherever it goes for our company and our customers."

Leading Technology Company

THE CHALLENGE

With the rapid adoption of cloud applications and services, sensitive data is increasingly at risk as it moves outside the enterprise perimeter and beyond the reach of traditional security tools. Continuous and consistent data protection policies are now required across IT-managed cloud applications, plus thousands of user- and business-led cloud services, email, and websites that allow uploading or posting of data. Despite having native security controls, today's cloud applications provide limited protection against data loss and exposure, putting your sensitive information at risk. And, while general cloud apps remain a concern, traditional email is recognized as a common vector for sensitive-data loss. You need an integrated, comprehensive security solution that's easy to use and helps you maintain control over content throughout its lifecycle.

NETSKOPE WITH MICROSOFT MIP

Netskope and Microsoft Information Protection (MIP) together provide a solution that addresses modern cloud security challenges and secures your data regardless of user location, application, or device type. Netskope, the leading security cloud company, provides deep visibility and granular control of cloud applications and the web, as well as advanced data and threat protection.

Microsoft Information Protection is the unification of Microsoft's classification, labeling, and protection services. Unified administration is provided across Microsoft 365, Azure Information Protection, Windows Information Protection, and other Microsoft services. It works by labeling and encrypting files and email messages (attached documents) created by or shared to or from any user on any device, so only authorized users can read the information. MIP complements Netskope and empowers customers by offering enhanced protection and integrated workflows to optimize their security posture and operations.

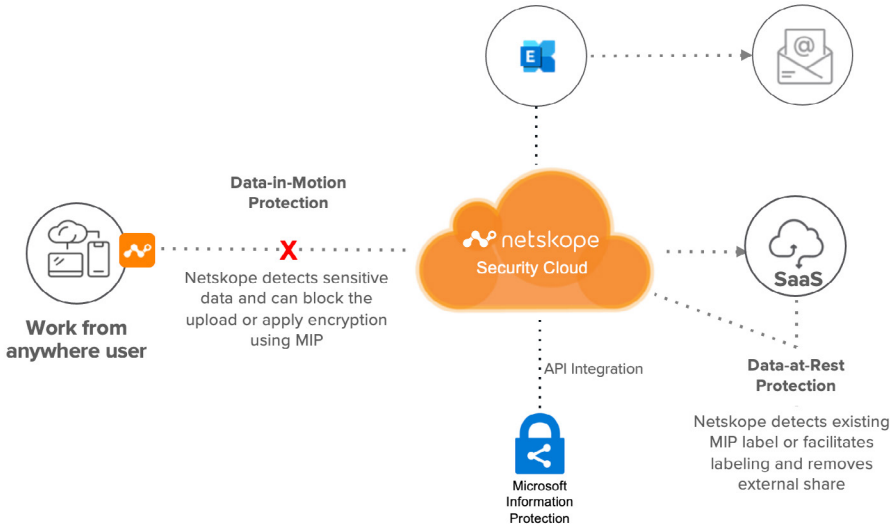
CAPABILITIES

360° DATA PROTECTION WITH NETSKOPE AND MIP

The integration of Netskope with MIP supplies a powerful, extensible platform for securing email, cloud applications, and web access. Netskope can prevent sending and sharing of files via email that have not been encrypted or tagged by MIP, or it can trigger MIP to apply or override encryption settings on matching email and its data-sensitive attachments. This enables Netskope to work with MIP and Exchange Online controls to prevent email from being used in combination with MIP to exfiltrate confidential information.

Netskope can block encrypted email from flowing until it is able to see the content, scan the content, and then trigger MIP if it is necessary or simply flag Exchange to block the content. Only content that is allowed to be shared is forwarded on by Netskope to the email service.

Using granular visibility and contextual controls and data across web, email, and cloud applications, the integrated solution offers a modern defense with an in-depth design that benefits organizations of all sizes.



Joint solution benefits

- **Take MIP and apply it consistently to every cloud service and data exchange**
- **Prevent sharing of files that have NOT been MIP encrypted or tagged**

Netskope integrates with Microsoft Information Protection to protect cloud data.

Netskope evaluates content and triggers Microsoft Information Protection for data at rest and examines data in motion to ensure that it is labeled and encrypted appropriately to match conditional access requirements.

INITIATING THE LABELING AND ENCRYPTION OF DATA AT REST

Together, Netskope and MIP provide a machine learning-enhanced 4-in-1 data loss prevention (DLP) for web, SaaS, IaaS, and Email as an approach to detecting and protecting sensitive information across your evolving cloud environment. The solution enables security teams to ensure that sensitive content is not sent outside the organization or shared with unauthorized users.

Netskope scans content at rest. Even if it is encrypted by MIP, Netskope has the credentials to open and scan that content for sensitive data. If sensitive data is found, Netskope can invoke MIP labeling and trigger subsequent encryption that is appropriate for the content. When or if these files are sent outside of a Netskope protected collaboration solution, the files remain protected by MIP throughout their lifecycle and despite how many times the files change hands. Security teams can worry less, knowing that the data is being scanned and protected consistently and programmatically without having to concern themselves with losing control over data that is eventually shared outside of the cloud.

PREVENTING UNPROTECTED SHARING OF SENSITIVE DATA

Netskope Cloud XD—the "engine" of the Netskope platform—can understand and decode the modern language of the cloud, so that specific details of users, actions, applications, instances, and more can be used to enforce policies. This visibility enables Netskope to look for the presence or absence of labels or encryption, and can leverage this in policy to restrict files with no MIP protections to only certain activities, users, or destinations. For example, you can use it to identify attempts at sending unprotected data between business and personal email (john-work@corporate.com → john-personal@gmail.com). Likewise, it can identify and prevent attempts at moving unprotected data between business and personal instances of OneDrive, becoming the enforcer for global application of MIP to real-time traffic. Similarly, Netskope can prevent data from being used in certain cases when it has been encrypted, but Netskope has not been able to see the content.

Whether your organization is collaborating with business partners via email, using SaaS applications like Slack or IaaS services like Amazon S3 buckets, Netskope and MIP protect your classified data from unauthorized access and inadvertent exposure by validating data sensitivity and then triggering labeling and encryption on data at rest in accordance with company policy.

Netskope's robust policy engine offers many means to ensure the right data is shared with the right applications and instances and with the right MIP labels and encryption settings.

CONCLUSIONS

ABOUT MICROSOFT INFORMATION PROTECTION

Microsoft Information Protection encrypts email messages and attached documents that are sent to any user on any device, so only authorized recipients can read emailed information. It protects against viewing of data by unauthorized systems or personnel, and complements BitLocker disk encryption in Microsoft datacenters.

ABOUT NETSKOPE

The network perimeter is dissolving. A new perimeter is needed that can protect data and users everywhere, without introducing friction to the business. The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, 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.