netskope

Best Practices Guide:

Securing Collaboration Tools

Netskope Best Practices Guide: Securing Collaboration Tools

Organizations today are deploying collaboration tools like **Slack** and **Microsoft Teams** at a rapid pace, driven by the unprecedented challenges of maintaining productivity while transitioning to a remote workforce. Microsoft reported that daily usage for Microsoft Teams more than doubled (from 20m to 44m users) in the time period from November 2019 to March 2020[1]. Slack has witnessed similar growth, although the specific numbers have not been publicly disclosed.

As the adoption of collaboration tools skyrockets, the risks that organizations face are also running at an all time high. The need for the tools cannot wait, and concerns for security must be addressed. Netskope has years of experience working with customers deploying cloud security, and in this guide, our experts provide practical and detailed recommendations for the best practices for implementing security for deploying Slack and Microsoft Teams across your organization.

[1] Microsoft says Teams communication app has reached 44 million daily users”, CNBC, retrieved 3/19/20, https://www.cnbc.com/2020/03/18/microsoft-teams-app-reaches-44-million-daily-users.html

Best Practices for Securing Collaboration Tools

Control Access

- Ensure that your users have access to sanctioned applications while staying in control over unsanctioned applications and instances.
- Make sure that applications are configured to use the proper functions necessary for adherence to your policies for ediscovery, legal hold, and archive.
- Maintain and enforce policies for BYOD and unmanaged access to applications. Your organization may choose to block access, or permit access with specific controls in place to protect data.
- Maintain strict controls over 3rd party access, such as authorized partners, while blocking guest access to collaboration messages and files.

Protect Data

- Make sure that data is not accidentally or maliciously shared globally. Enforce policies that limit permissions to specific users and groups.
- Make sure that the collaboration application uses encryption properly, and in accordance to your organization's policies for protection and compliance.
- Find sensitive data stored in your collaboration applications, based on categories of sensitivity relevant to your organization's business or industry.
- Take action to enforce policies for data at rest (within the collaboration platform or cloud storage) and data in motion.

Stop Malware

- Inspect content with the application's channels, as well as within direct person-to-person messages, to look for malware.
- Enforce threat protections both inline (for real time protection of content), as well as scan for malware stored within the application.

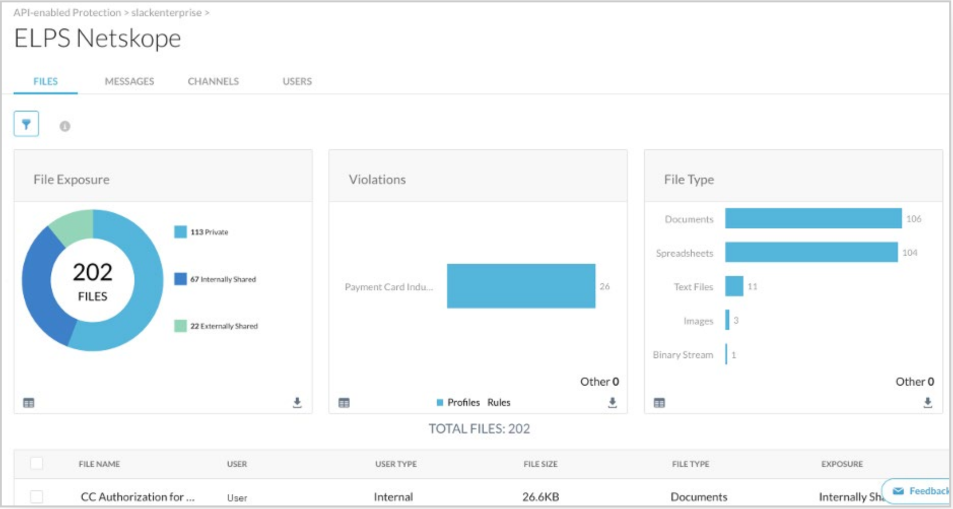
Netskope's patented Cloud Security Platform provides multi-layered inline and API protections for leading cloud applications. To properly secure users and protect data shared via these collaboration tools, customers should apply the layered security approach:

- Netskope API-enabled Protection for **Slack** and **Microsoft Teams**
- Netskope Inline Protection

Using Netskope API-enabled Protection

Netskope recommends that customers deploy API-enabled protection for collaboration applications. Enabling API-enabled protection allows customers to have a comprehensive view of their collaboration platform and easily assess the security posture of data sharing (for data-at-rest stored within the collaboration application as well as the connected cloud storage). You will have a comprehensive view of how your collaboration platform is used, with detailed reports that include information such as the number of users, channels, files shared, exposure of data to external entities.

Netskope recommends that you set up API-enabled policies to scan for sensitive data in private and public teams/channels, as well as private messages. Netskope provides a wide variety of prebuilt DLP profiles to accurately identify sensitive information message posts and files uploaded to your collaboration platform.



□	FILE NAME	USER	USER TYPE	FILE SIZE	FILE TYPE	EXPOSURE
□	CC Authorization for ...	User	Internal	26.6KB	Documents	Internally Sh

Depending on your organization's industry and security requirements, you should consider deploying DLP profile scanning for:

- PCI data such as credit card numbers, bank account numbers, Swift codes.
- PII data such as employee identification numbers, social security numbers, dates of birth, and Medicare Beneficiary Identifiers.
- Company confidential data that is either explicitly classified using a data classification tool or is dynamically detected using Netskope's powerful and flexible data identifier library.
- Any data that the company desires for classification such as data related to intellectual property, proprietary data, customer databases, etc.

> **"More than 50% of data policy violations come from cloud storage, collaboration, and webmail apps."**
>
> Netskope Threat Labs,
> *The Dark Side of the Cloud,*
> February 2020

After scanning the data for classification, use Netskope to set up a policy to secure sensitive data. Possible actions include: Delete file/post due to its sensitivity, copy data into legal hold, restrict sharing with external entities by quarantining the file to an internal-only repository, etc. Regardless of the action taken, you will always have an accurate reporting picture of the sensitive data and its exposure in your collaboration platform.

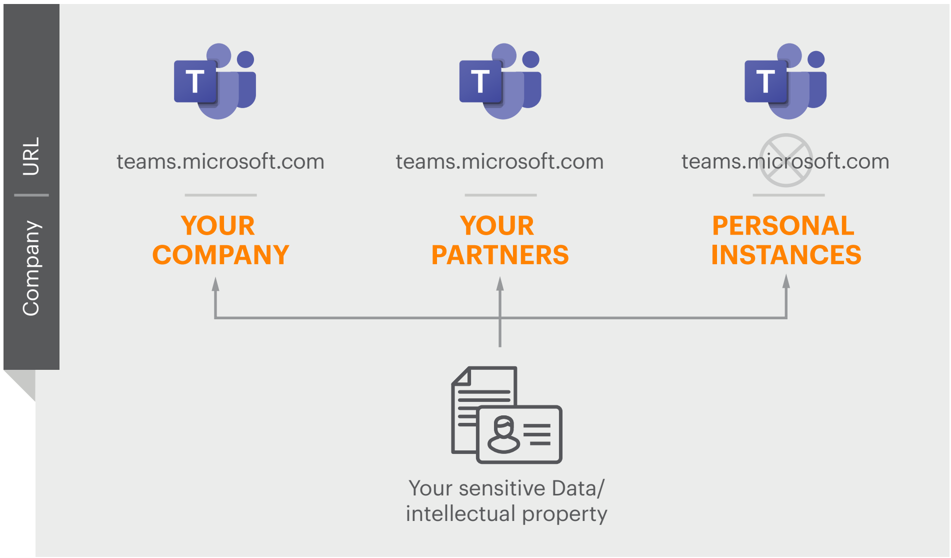
You should use Netskope Threat Protection to ensure your collaboration platform is free of malware that may reside within the application or cloud storage is accidentally shared with your employees, or uploaded from an unmanaged 3rd party device. Netskope threat protection is available via both API-enabled protection and inline protection modes.

Using Netskope Inline Protection

Netskope Inline protection should be deployed to provide access controls, inline threat protection and enforce data protection policies in traffic. This is achieved by deploying the Netskope lightweight client on managed endpoints to steer traffic to the Netskope Cloud Security Platform.

As the proliferation of the collaboration platforms rises, your users may need to extend communication with business partners as well. Some users may try to use unsanctioned or personal instances of these collaboration tools. Netskope identifies and governs access to applications and enforces instance aware policies to keep data where it belongs.

Consider the picture below:

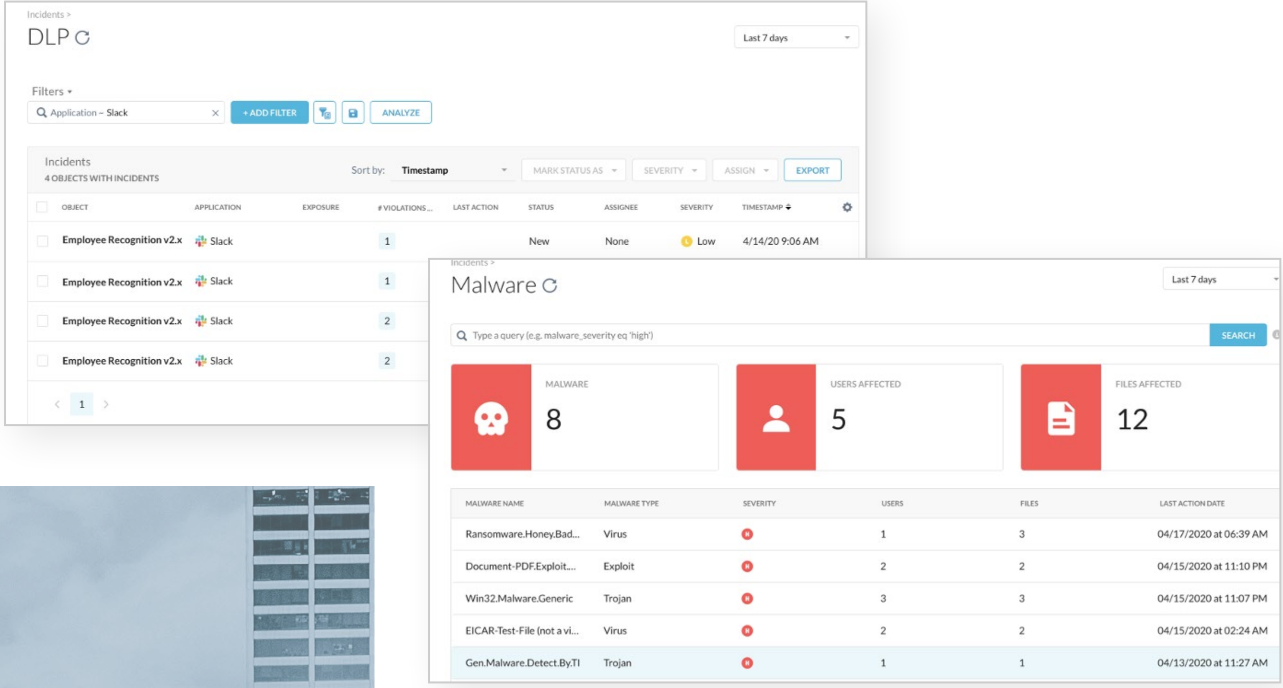


Inline Protection can be deployed in multiple ways:

- Deploy Netskope Inline Protection security policies to prohibit logins to unauthorized instances of cloud SaaS applications. This will ensure that your users only use the sanctioned application instance, and will not be able to access unauthorized instances (such as personally owned or hacker controlled).

- An alternative approach is to use a policy that permits users to login to any instance of the application, while still enforcing DLP profiles to protect data. This approach stops your proprietary or sensitive information from being uploaded to an unsanctioned instance of the collaboration application.
    - Furthermore, the same policy protects data if a user accidentally or maliciously tries to exfiltrate data from their endpoint to risky file sharing applications such as WeTransfer, personal cloud storage applications such as Dropbox, or using an email service like personal Gmail.
    - Netskope Inline Protection also provides full audit of user activity, such as user logins/logouts, as well as granular controls and reporting on creating, editing, deleting, uploading, and downloading data. These protections provide you with full audit and eDiscovery capabilities.

Netskope Inline Protection also gives you the ability to control and govern use of BYOD/unmanaged devices accessing your sanctioned cloud collaboration applications such as Slack or Microsoft Teams. This is achieved by integrating your identity provider (such as Okta) with Netskope reverse-proxy steering mode. You can then apply separate access and DLP policies to users with unmanaged devices and prevent them from downloading sensitive or proprietary data. Maintain collaborative exchange with other employees and partners, mitigating the risk of data loss, and prevent malware from infiltrating your collaboration platform.



Application – Slack

Incidents
4 OBJECTS WITH INCIDENTS

Sort by: Timestamp

OBJECT	APPLICATION	EXPOSURE	# VIOLATIONS ...	LAST ACTION	STATUS	ASSIGNEE	SEVERITY	TIMESTAMP
Employee Recognition v2.x	Slack		1		New	None	Low	4/14/20 9:06 AM
Employee Recognition v2.x	Slack		1					
Employee Recognition v2.x	Slack		2					
Employee Recognition v2.x	Slack		2					

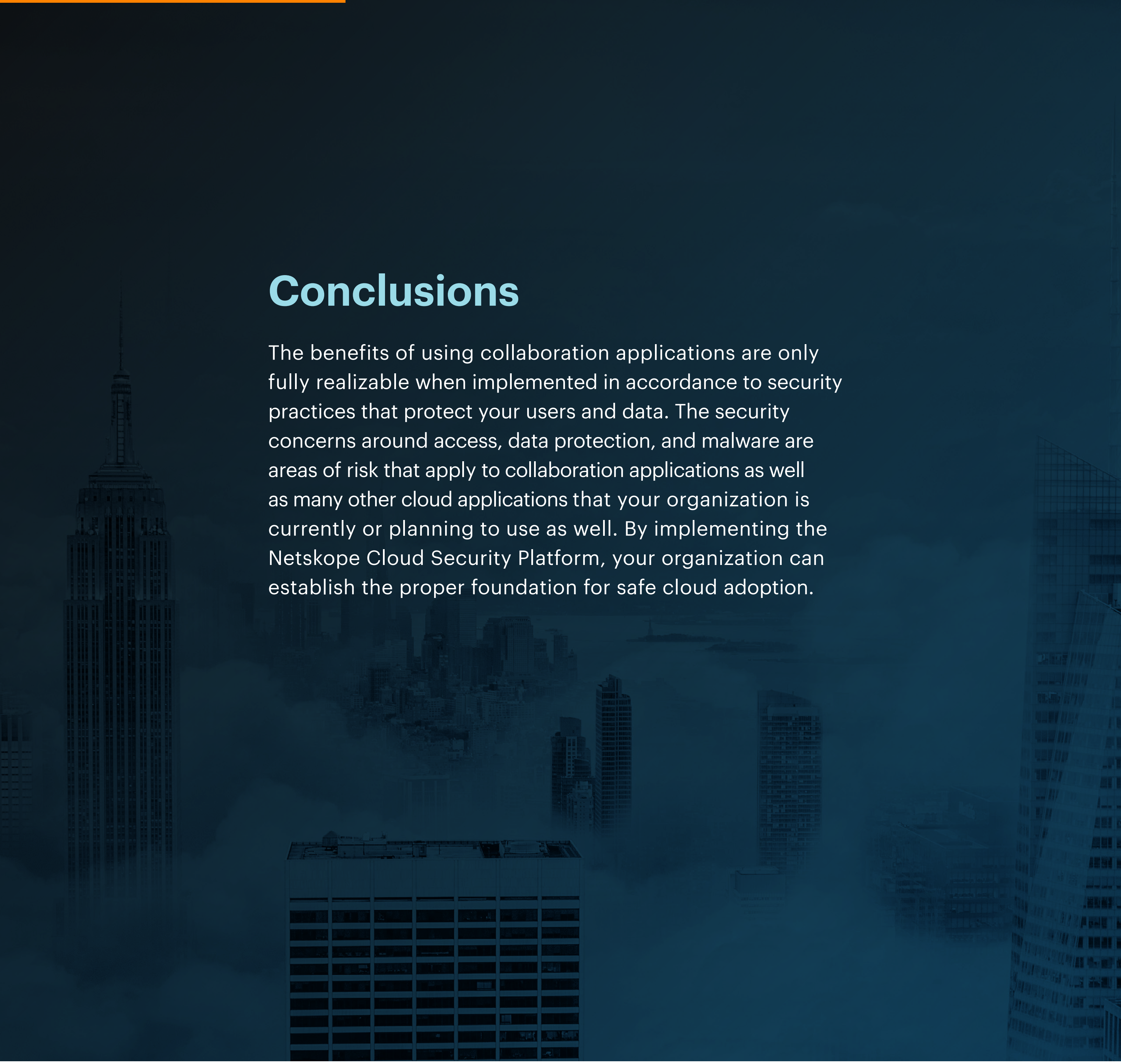
Type a query (e.g. malware_severity eq 'high')

MALWARE 8

USERS AFFECTED 5

FILES AFFECTED 12

MALWARE NAME	MALWARE TYPE	SEVERITY	USERS	FILES	LAST ACTION DATE
Ransomware.Honey.Bad...	Virus	H	1	3	04/17/2020 at 06:39 AM
Document-PDF.Exploit....	Exploit	H	2	2	04/15/2020 at 11:10 PM
Win32.Malware.Generic	Trojan	H	3	3	04/15/2020 at 11:07 PM
EICAR-Test-File (not a vi...	Virus	H	2	2	04/15/2020 at 02:24 AM
Gen.Malware.Detect.By.TI	Trojan	H	1	1	04/13/2020 at 11:27 AM



Conclusions

The benefits of using collaboration applications are only fully realizable when implemented in accordance to security practices that protect your users and data. The security concerns around access, data protection, and malware are areas of risk that apply to collaboration applications as well as many other cloud applications that your organization is currently or planning to use as well. By implementing the Netskope Cloud Security Platform, your organization can establish the proper foundation for safe cloud adoption.

netskope

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 takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.

To learn more visit, https://www.netskope.com.