SOLUTION BRIEF

Netskope for Microsoft Teams

Netskope for Microsoft Teams helps organizations safely collaborate from anywhere to boost productivity, while ensuring that sensitive data is protected from misuse and unauthorized access.

> “In enterprises today, 33% of workers are remote on any given day, and are spread across more than 8 locations, on average.”

Netskope Cloud and Threat Report
February 2020

KEY USE CASES

- **Refine collaboration controls.** Enforce granular access policies and restrict sharing of sensitive data in Microsoft Teams to unauthorized parties or unmanaged devices.
- **Enforce data loss protection policies.** Prevent sensitive files and data from being downloaded or uploaded within Microsoft Teams.
- **Detect and prevent threats.** Detect malware and cloud-enabled threats, including insider threats, compromised accounts and anomalous user behaviour.
- **Monitor, investigate and audit.** Examine a complete audit trail of all user and application activity in Microsoft Teams.

THE CHALLENGE

Microsoft Teams is a popular collaboration solution to boost productivity in enterprises worldwide. As part of the Office 365 suite of applications, Microsoft Teams helps increase productivity and collaboration in businesses of all sizes, combining workplace chat, video meetings and file storage. While this innovative collaboration proves to be extremely beneficial to users, it presents new challenges for IT Security Operations teams in identifying, monitoring and securing the data that is shared amongst users and employees. Security teams must ensure that sensitive data is only accessible to those individuals that are authorized to see it, to ensure that data is not exfiltrated or shared outside the organization, to ensure regulatory compliance and, lastly, to detect and stop threats from penetrating the system.

Enterprises need a holistic, consistent approach to monitoring and protecting users and data in Microsoft Teams, as well as across the entire Office 365 suite of applications.

NETSKOPE FOR MICROSOFT TEAMS OVERVIEW

Netskope for Microsoft Teams is an advanced Cloud Access Security Broker (CASB) solution to protect sensitive data and files within Microsoft Teams environments. Netskope provides organizations with a comprehensive approach to cloud security, by enabling granular visibility and control across all Microsoft Teams accounts within an organization. Security Operations can obtain deep insight and context into Microsoft Teams collaboration activity with granular data and file access controls, as well as the ability to detect anomalous behaviour that might pose a serious threat to the organization. Real-time security controls can block malicious or unauthorized activity as it occurs, installing security protections in between your Microsoft Teams deployment and users, regardless of where they are located.

Netskope for Microsoft Teams is Microsoft Certified as a result of Netskope joining the Microsoft Teams Certification and Licensing Program and meeting its certification criteria.

KEY CAPABILITIES

CENTRALIZED, CONSISTENT MANAGEMENT

Netskope provides a single point of control for managing cloud security and compliance across the web and thousands of cloud applications. IT Security can now use a single console and platform to gain in-depth visibility for activities within their instances of Microsoft Teams, allowing them to define granular, contextual controls to protect sensitive data. Netskope offers unified policy management for Microsoft Teams and other Office 365 applications, including OneDrive, Outlook, and SharePoint, as well as Azure public cloud environments—providing consistent, intuitive workflows and reporting for securing Microsoft environments.

GRANULAR VISIBILITY AND CONTROL

Netskope provides deep visibility into Microsoft Teams and other Office 365 apps as well as the interaction between these cloud applications. Security admins can obtain risk-based insights that identify sensitive files and expose how they are being shared. Netskope for Microsoft Teams allows IT Security to set fine-grained policies to control activities and ensure protection. Powered by Cloud XD™, Netskope can enforce detailed security policies based on contextual information such as cloud app, user, instance, activities, and device. Cloud XD™ provides real-time decoding of cloud app traffic, discovering contextual information that can be utilized for controlling managed and unmanaged cloud applications. By distinguishing between corporate and personal instances of cloud application use, IT security teams can choose to block the upload of a sensitive document accessed from Microsoft Teams into an unmanaged cloud app. For employees who use their personal devices to access corporate data stored in associated Microsoft applications like OneDrive or SharePoint, Netskope can enforce conditional access that restricts access to view-only and prevents the download of sensitive files to personal, unmanaged devices. Custom policies can also detect and restrict activities—such as the sharing of personally identifiable information (PII) in Microsoft Teams channels—and custom warning messages help coach employees on certain, high risk activities.

> **“20% of users have sensitive data moving between cloud apps and 37% of that data is involved in DLP violations.”**
>
> Netskope Cloud and Threat Report
> February 2020

ADVANCED DATA PROTECTION

Netskope offers advanced data loss prevention (DLP) capabilities to identify and protect sensitive data no matter where it’s located or where it goes—out to any SaaS application, IaaS service, or to the web. This includes protecting data-at-rest as well as data-in-motion. Security teams can have Microsoft Teams messages and files inspected in real-time for sensitive data exfiltration to help reduce the risk of insider threats due to increased collaboration. Built from the ground up, Netskope has the most advanced DLP capability in the industry, architected for high accuracy and low false positives. Supporting over 3,000 data identifiers, over 1,000 file types, custom regular expressions, proximity analysis, fingerprinting, exact match, and optical character recognition (OCR), Netskope DLP effectively protects data across your

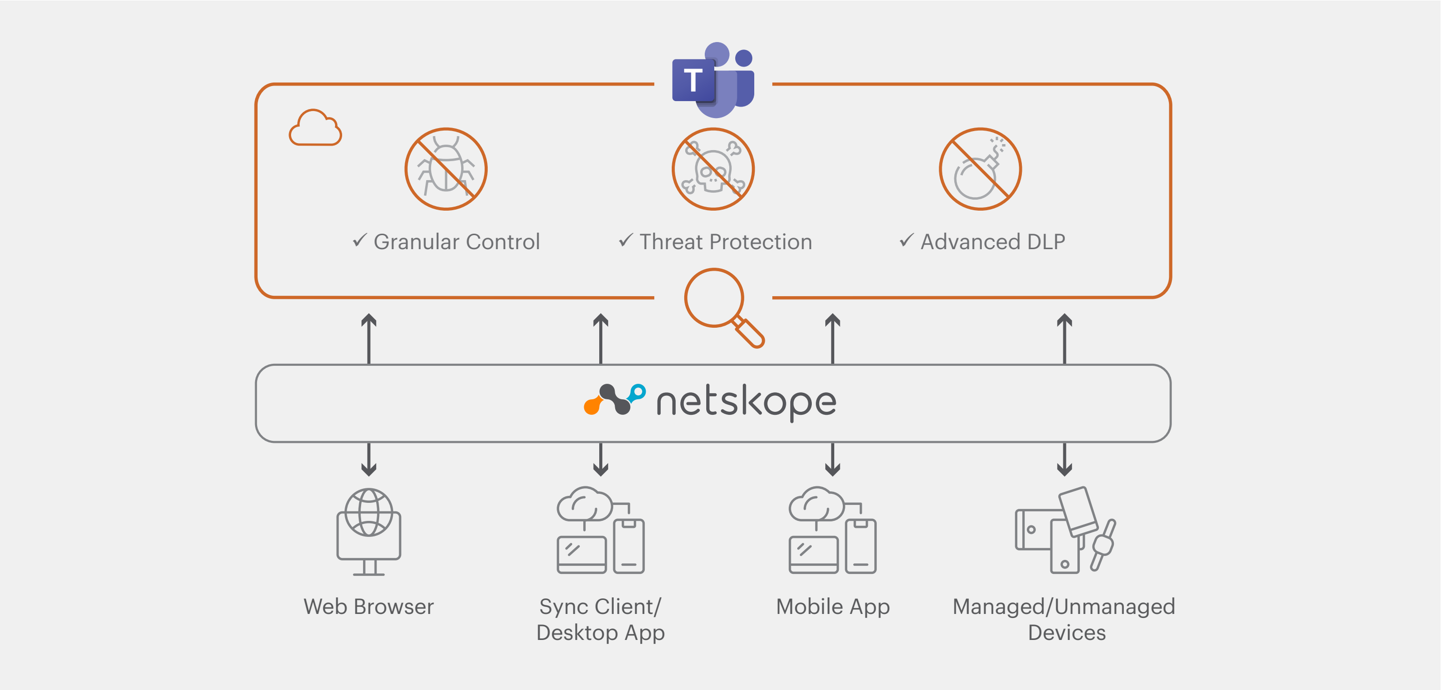

FIGURE 1: Netskope for Microsoft Teams

Office 365 suite. Netskope also helps IT Security achieve compliance by providing over 40 pre-built policy templates (e.g. PCI, HIPAA, GDPR) as well as customizable templates to fit their unique industry requirements.

CLOUD THREAT AND MALWARE PROTECTION

Netskope offers advanced threat protection to ensure malware and cloud-enabled threats do not harm your environment and hinder productivity. Netskope detects threats in data-at-rest as well as sees directly into cloud traffic and data-in-motion, exposing new cloud threats that often evade legacy security solutions, courtesy of a multi-layer threat engine, combined with threat intelligence feeds across 40 different sources. Netskope offers machine learning enabled User and Entity Behaviour Analytics (UEBA) to monitor user behaviour. Furthermore, a rules-based anomaly detection engine alerts Security Operations to suspicious logins, excessive activity, data exfiltration, and compromised credentials to help resolve incidents faster while providing flexible remediation options.

Security admins can readily detect and remediate cloud malware or in files shared with Microsoft Teams. Files that contain known malware can be quarantined and replaced with tombstone files that are instead propagated throughout the organization, reducing the risk of further infection. Combined with the aforementioned Cloud XD granular visibility, Security Operations can also prevent rogue and personal instances from delivering cloud phishing and cloud-enabled threats—which are now the top threats facing enterprises. Lastly, Netskope helps Incident Response teams by collecting rich metadata for 90 days—and up to 1 year—for web and cloud traffic for further investigation and analysis.

BENEFITS	DESCRIPTION
DEEP VISIBILITY AND CONTROL	**OBTAIN DEEP VISIBILITY AND CONTROL INTO MICROSOFT TEAMS:** • Detect creation of new Teams • Detect changes in Team privacy settings (e.g. 'Private' to 'Public') • Detect addition or removal of users within Teams • Detect/Scan content (messages and file attachments) in Teams • Block/Allow/Alert as content is updated/uploaded/downloaded into/from Teams • Replace offending or non-compliant messages with a warning (tombstoning)
GRANULAR SECURITY ACCESS POLICIES	**CREATE GRANULAR SECURITY POLICIES IN MICROSOFT TEAMS:** • Based on user, device, cloud application, activity, instance and more, using Cloud XD™ • Scan certain Team types • Scan direct, channel and meeting chat messages
ADVANCED DATA PROTECTION	**DEVELOP GRANULAR DLP POLICIES:** • Define keywords and phrases to detect sensitive or regulated data • Build granular custom regular expression to identify alpha-numeric patterns • 3,000 out-of-the-box data identifiers (e.g. Credit Card Number, Personal Names, address) • 40+ compliance and regulatory templates (e.g. PCI-DSS, HIPAA) • Fingerprint of unstructured files and structured files with exact or partial match • Optical character recognition (OCR) with Machine Learning (ML)-enabled image classification and scanning **DLP ACTIONS:** • Alert on DLP violations • Block violating message or attachments
CLOUD THREAT AND MALWARE PROTECTION	**PROTECT AGAINST THE LATEST CLOUD-BASED THREATS:** • **User and Entity Behavior Analytics (UEBA):** Offers batch and stream ML analysis, and pre-defined and customizable sequential rules to detect bulk uploads, downloads, deletes, failed logins, etc. • **Insider threats:** Detect anomalous behavior by unusual amounts of data uploaded/data, changes in user behavior, login frequency of cloud service accounts • **Compromised Accounts:** Evaluate access attempts by identifying suspicious geographic login-access, brute-force attacks, and unusual login patterns • **Integrate with third-party tools:** Connect with Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), sandbox solutions and more • **Privileged user threats:** Identify sudden user privilege escalations, dormant accounts, and unusual user system access • **Malware:** Block known malware, discover unknown files, and identify command and control (C2) behavior signaling data exfiltration • **Threat Intelligence:** Gather and utilize threat intelligence feeds from over 40 sources. Netskope Cloud Threat Exchange (CTE) enables threat intel sharing with EPP, EDR, SIEM, etc.

REQUEST A LIVE DEMO:

https://www.netskope.com/request-demo

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.