WHITE PAPER

Skyhigh Security

Microsoft Teams: Top 10 Security Threats

TABLE OF CONTENTS

4 THREAT 1: Guest Users

5 THREAT 2: Access From Unmanaged Devices or Untrusted Locations

6 THREAT 3: Screen Sharing Displaying Confidential Information

6 THREAT 4: Malware Uploaded Via Teams

7 THREAT 5: Data Loss Via Teams Chat and File Shares

7 THREAT 6: Data Loss Via Other Apps

8 THREAT 7: Slow Security Is Worse Than No Security

8 THREAT 8: Inconsistent Control Across Applications

9 THREAT 9: Missing Risky Behavior Patterns

9 THREAT 10: Simple Controls for a Complex World

10 How Skyhigh Security Can Help

11 Conclusion

Microsoft Teams: Top 10 Security Threats

Cloud adoption plans have quickly accelerated as a result of the COVID-19 pandemic. As a result, projects to empower users, increase remote working capacity, and embrace the cloud have been executed in weeks instead of years. Users have rushed to join the cloud revolution with monumental increases in collaboration, communication, and sharing apps. One of the fastest growing apps has been Microsoft Teams. Teams combines messaging, file sharing, audio, and video calling and integrates with over 100 other cloud apps, often functioning as the core of new work methodologies.

Microsoft invests huge amounts in the security of their systems and is applauded for the security and capabilities of its services. However, it is the enterprise's responsibility to secure the data in the systems and how they are used.

The breadth of options can also be its weakest link. With almost unlimited communication capabilities the risk of misconfiguration, oversharing, or misuse is great. It takes just seconds to add an external party into an internal discussion without realizing the potential for data loss. IT security teams need the ability to manage and control use to reduce risk of data loss or malware entering through Teams.

After working with hundreds of enterprises and more than 40 million Skyhigh Security CASB users worldwide and discussing with IT security, governance, and risk teams on how they address their Teams security concerns, Skyhigh Security has identified the top 10 issues they face and how to address them.

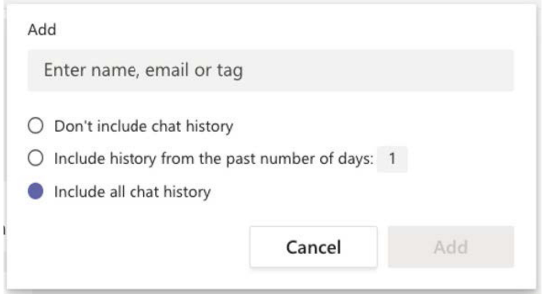
Addressing these threats requires a mix of responses from multiple groups in the organization, as no single group can address all possible threats; Tenant admins can review and make changes to Teams settings, IT security deliver broader defense capabilities, Team owners need to understand their role and never forget the ever-important user training to educate employees and guests on safe Teams usage. Skyhigh Security CASB complements Teams security by keeping features of the product available while addressing these risks and providing additional protection for customers.

Microsoft publish a lot of material about Teams security and compliance, a good place to start is here.

THREAT 1: Guest Users

Guests can be added and see internal/ sensitive content.

One of the great powers of Teams is the ability to add external users (guests) to a channel and share chat messages, files, have online meetings, live meetings, make calls, create tasks and shifts for users, and use other integrated apps between internal and external collaborators. Some companies are now using Teams for customer service agents to chat to customers. Any channel owner or administrator can add new members to a channel and, depending on settings, this can include external guests. Team channels can have multiple administrators—this is common when a channel has many members, especially across time zones. When guests are added, they can either be set to see all old chat history (including files) or just see new content.



Add

Enter name, email or tag

○ Don't include chat history

○ Include history from the past number of days: 1

● Include all chat history

Figure 1. Chat history in Teams.

Microsoft's security capabilities allow administrators to either enable or disable "guest access" for Microsoft Teams (the default is new teams are closed to guests).

The difficulty with implementing an enterprise-wide setting is that either all teams are open to all guests or all teams are closed to all guests. Then, tenant admins that want a different setting have to change this for their particular team. Most organizations want to use the full capabilities of Teams. Therefore, typically set all teams open to all guests.

What is really needed is flexibility; the ability to define internal-only teams, public teams, and those that allow only authorized external third parties. By setting allow list or block list domains, security can be implemented with the flexibility to allow employees to collaborate via Teams with authorized guests.

The optimal security options are to be able to:

- Detect and remove guest users from unauthorized domains joining team channels.
- Detect and remove all guest users joining teams meant for internal conversations.
- Control messages posted in channels and chat conversations that include guest users from (or not from) specified domains
- Control files posted in channels and chat conversations that include guest users from (or not from) specified domains
- Report on channels and all guest users to allow management of team members
- Control messages and files posted historically in channels having guest users from (or not from) specified domains.

Multiple actions should be available, depending on the severity of a policy trigger, such as removing files, quarantine files, tombstoning, alerting to channel owners and IT administrative staff, and ensuring that logs are collected for future investigation.

Being able to allow list trusted domains and monitor and remove sensitive content and messages allows Teams guest access while, at the same time, keeping data secure.

As new teams can be created at any time and members may be unsure of the individual team attributes, a security policy defined beforehand can be invaluable. For example, team names starting with "external" could be defined as allowing guests from specified domains, team names starting "open" could allow all guests, and "internal" disallowing guest access. This capability is available with Skyhigh Security CASB.

THREAT 2: Access From Unmanaged Devices or Untrusted Locations

Teams can be used by unmanaged devices resulting in data loss.

The standard controls for Teams access are the typical name/password pair with optional multifactor authentication. A valid user can log in from any device. A user with access from an unmanaged device could download files shared in a Teams channel and then either forward or lose those files after being a victim of a cyberattack.

The ability to set policies for unmanaged devices can safeguard Teams content, with useful options including:

- Block access from all unmanaged devices
- Allow access but block downloads
- Allow access but block file uploads (as unmanaged devices may have been infected with malware)
- Step up authentication (redirecting to another authentication mechanism)
- Add specific data loss prevention (DLP) policy for unmanaged devices
- Proxy unmanaged devices using browser-based access (for additional controls)
- Block unmanaged devices from using the native Teams client
- Force digital rights management (DRM) registration before access.

Access from devices in untrusted locations could risk data loss.

Device location could be an indicator of risk. Depending on the sensitivity of the data being exchanged, IT administrators may want to define locations that are or are not trusted, allow or disallow access, or set security policies based on location.

Allow lists and block lists of IP addresses/locations could include corporate offices and/or whole countries. The types of policies that could be useful include:

- Block access from specified block lists
- Allow access from IP range/geography, but block downloads
- Step up authentication (redirecting to another authentication mechanism)
- Add specific DLP policy for devices from IP range/geography
- Proxy devices from IP range/geography using browser-based access (for additional controls)
- Block devices from IP range/geography from using the native Teams client
- Force DRM registration before access.

THREAT 3: Screen Sharing Displaying Confidential Information

Screen sharing can inadvertently leak confidential information

Screen sharing during Teams meetings is a powerful feature; users can share single application files, full screens, and can jointly share a whiteboard feature. This can be made available both to internal users and to guests.

The risk is that a user overshares sensitive data. When sharing a complete screen there may be other applications on display that show confidential data. Many communication applications show message alerts even when running in background, therefore a new Teams, email, or any other message received may appear on the presenter's screen and be shared with other attendees.

IT admins can consider configuring the Teams application to disable screen sharing and only allow application sharing as then alerts do not appear on the other meeting member screens and there are multiple options for users and guest sharing that can be implemented. However, this removes a function that users like and use widely and if a speaker wants to show multiple applications they will have to stop and restart sharing of each app during the meeting.

Guest users can be allowed or disabled to request control of the shared screen and it is recommended to consider whether this is an appropriate risk—what is the company's position if an employee views confidential information from a third party?

Users can also share the common whiteboard, though data loss is less likely, again admins need to decide the appropriate organization policy.

This is an area where the user's behavior is the potential problem, so rather than the administrator trying to anticipate every eventuality, it is recommended that employee training for Teams use is prioritized—include examples and explanations of the upsides and downsides of this set of features so users can decide when to close messaging apps, when to share individual files and when to share a complete screen.

THREAT 4: Malware Uploaded Via Teams

File uploads from external users or unmanaged devices may contain malware.

Guest devices, by definition, are not managed by the organization, and so their status is unknown, including the presence of anti-malware technology. As Teams channels can include many internal users, any of those can be infected by malicious file uploads.

IT administrators need the ability to either block all file uploads from unmanaged devices or to scan content when it is uploaded and remove it from the channel, informing IT management of any incidents.

THREAT 5: Data Loss Via Teams Chat and File Shares

File shares in Teams can lose confidential data.

Teams is an easy way for users to share and collaborate on files as well as chat. Both could be conduits for data loss and should be controlled.

DLP technologies with strong sensitive content identification capabilities should be implemented on Teams chat and file shares, including features such as DLP standard data identifiers, specific organization dictionary matches, fingerprinting of files, proximity checking, Boolean logic to check multiple parameters, and exception logic.

Scans should be able to be conducted in near real time on messages and file uploads, but also on-demand scanning should be available to look at previous messages and files previously shared within the team.

Don't forget that external users could also upload sensitive data, so DLP scans need to be implemented to ensure that internal users don't receive sensitive data from an external guest.

THREAT 6: Data Loss Via Other Apps

Teams app integration can mean your data going to unknown destinations.

Microsoft Teams allows users to easily incorporate many third-party cloud-based apps into their Teams environment, providing facilities such as polling, analytics, business intelligence, education, HR, project management, and sales apps. While these apps can provide benefits to users, third-party apps can present administrators with security concerns and risk of data loss if data is passed outside the Teams system to these other service providers.

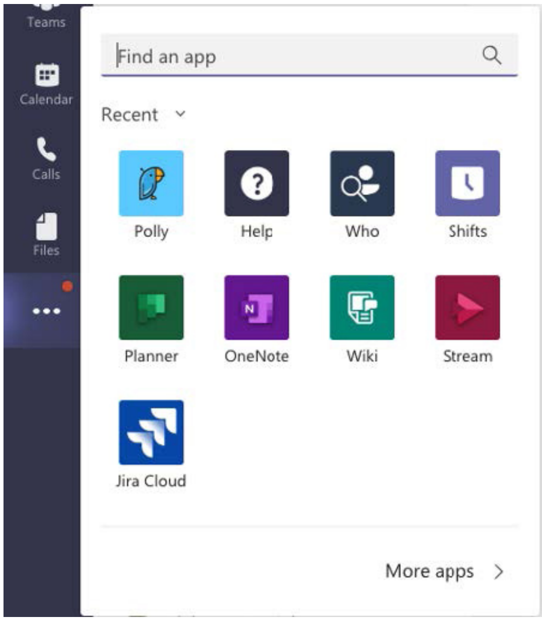


Figure 2. Apps integration in Teams.

As some of these apps may transfer data via their services, IT administrators need a system to discover third-party apps in use, review their risk profile, and provide a workflow to remediate, audit, allow, block, or notify users of an app's status and revoke access as needed.

THREAT 7: Slow Security Is Worse Than No Security

Security actions need to be near real time or the data is already gone.

Policies should be implemented in as near real time as possible to reduce risk. In fact, having a security system that is slow to respond could be worse than no security at all, as it leads to complacency.

The enforcement systems should support multiple actions depending on the severity of the violation and multiple actions be available, such as:

- Add incident to incident log
- Delete file or chat from Teams channel
- Remove shared link of file
- Quarantine file, allowing IT administrators to release it when safe
- Quarantine file, allowing user to release it when safe
- Remove user from channel
- Apply DRM or classification tags or encrypt the file
- Send notification to user, administrators, bot, and others

Microsoft has a large set of application programming interfaces (APIs) that can be used to implement security. However, some vendors do not prioritize this and, therefore, their response time to an incident can be measured in minutes or hours—during which time a data loss incident may have occurred. IT administrators need to check the general response time for incident remediation and ensure that the response is near real time.

THREAT 8: Inconsistent Control Across Applications

Teams policies should be consistent with data controls for other cloud apps and non-cloud controls such as file transfer via email, USB stick, and more.

Teams is just one of many ways to send and receive files. It can be an administration nightmare if each system is managed separately, as it will be very difficult to have consistent policies.

Administrators should be able to consolidate policies based on the data and user across all systems, no matter the method used for data transfer to ensure there are common policies and enforcement capabilities. This starts from the security we've known for years, such as encrypting and password protection on laptops and mobile devices, and USB stick and email controls. It continues with controls of other cloud services: "Shadow Cloud" use and sanctioned apps, along with internally developed apps on Infrastructure-as-a-Services (IaaS). Teams is just one application—albeit growing quickly—and IT security teams need to be able to review all possible data loss conduits and coordinate policies across them all.

As a warning to everyone; Teams files are kept within SharePoint, but it is easy for SharePoint and OneDrive to have pointers to the same file with different policies, where a user cannot share externally using a SharePoint link but can share the same file via OneDrive.

Of course, Teams shouldn't be the weakest link. Teams policies should take the best practices from existing policies but be implemented recognizing that Teams adds different ways of document and data sharing.

THREAT 9: Missing Risky Behavior Patterns

User behavior patterns can indicate lost credentials and rogue users, but these patterns are rarely reviewed.

Microsoft publishes APIs that allow security systems to look at user actions and the history of a particular user can be reviewed to compare current actions to prior history. If credentials are lost to an attacker, the behavior of the attacker could indicate an ongoing attack, so the Teams access can help identify a live attack on the organization.

As an example, an individual user may have a history showing that they access Teams from a dozen different IP addresses, all within a geographic radius; that they use a particular type of device; and that they typically engage with a certain number of Teams and files each day. If suddenly that user appears from a different country using a different device (and especially if this indicates impossible travel speeds), the account should be blocked until it is investigated—before a bad actor gets into the system and starts downloading files.

IT administrators should have a live system that automatically tracks and finds "normal" traffic patterns for each user and constantly watches for unusual patterns, allowing anomalies to be detected, alerts to be raised, and remedial action to be taken in high-risk situations.

THREAT 10: Simple Controls for a Complex World

Comprehensive and flexible controls are needed to ensure Teams security without losing functionality.

Microsoft Teams is a rich ecosystem that incorporates many functions used worldwide as the hub for instant messaging, audio and video calling, online meetings, and file and data collaboration with integration to other Microsoft Office 365 and partner applications.

Teams therefore needs to be considered as a whole. The feature list is long, and the capabilities require administrators to consider every way data can be shared and how best to implement policies to reduce risk and secure data. A simple block or allow is unlikely to work unless administrators are prepared to reduce the functionality available to the users.

A comprehensive set of policies is needed, including Boolean logic, such as "IF content AND guest NOT allow list THEN ACTION …" This logic may be different taking into account the user, their role, device, location, previous behavior patterns, and external user credentials data identifiers. It requires multiple possible response actions that are based on incident severity.

The Teams controls should be integrated and common with other systems for data security and logs kept within the corporate security information event management (SIEM) or other logging systems for future review.

How Skyhigh Security Can Help

Skyhigh Security has a wealth of experience helping customers secure their cloud computing systems, built around our Security Services Edge portfolio and other technology solutions. We were the first to announce and ship controls specifically for Microsoft Teams, even before Microsoft itself. Our 25-plus years of endpoint security experience, cloud controls, DLP and web gateway technologies, allow our customers to define and implement centralized management and actionable intelligence across device, network, and cloud.

Skyhigh Security offers leading cloud access security broker (CASB)—per Gartner, Forrester, and KuppingerCole—providing cloud security for Microsoft Teams. Capabilities include DLP, device control, user control, malware control, user behavior analytics with comprehensive flexible policy options, exceptions, Boolean logic, incident logs, and automated remediation actions.

The controls available for Microsoft Teams include controlling guest access, managing access based on device or location, malware defenses for file uploads, DLP for chat and files, and multiple remediation options—all integrated with controls that are used to manage non-cloud traffic.

Teams is just one of the many applications available as part of Microsoft Office 365. Skyhigh Security CASB provides management and control for the Office 365 Suite, as well as many other cloud-based applications, such as Salesforce, Box, Dropbox, Workday, Amazon Web Services (AWS), Azure, Google Cloud Platform, and customers' own internally developed cloud apps. Our CASB also provides visibility and control of user-defined “Shadow IT “services.

Integrating with the leading proxies, firewalls, single sign-on services, SIEM systems, and many other technology vendors, Skyhigh Security is committed to delivering the most flexible and open solutions to our customers.

Conclusion

Even before COVID-19, we saw significant increases in traffic from business collaboration applications such as Microsoft Teams. When the pandemic struck, this activity grew dramatically. There is no doubt that Teams is one of the main business applications of our age, with its wealth of functionality and the focus of Microsoft behind it. The third-party app plug-ins will continue to grow, and, no doubt, Microsoft will add more features.

IT security groups needed put more attention on Teams, as it is likely to be the next threat vector and conduit for data to leave the organization and attackers to enter. This in no way imputes any blame to Microsoft. Like any product or system, how it is used is the most important factor in its security. It is also not Microsoft's responsibility to allow users access and to control the data that they share and collaborate using Teams.

Truly comprehensive security for Teams can best be achieved with a purpose-built solution. Previous generations of security tools miss most cloud traffic and certainly do not have the flexibility to enforce the comprehensive policies needed in today's world.

Before implementing security technology, we recommend setting up workshops where different groups within your organization talk through various scenarios and decide the appropriate policy for each and where risk and compliance teams come together with IT security, HR, and user representatives.

Skyhigh Security is here to help you on your cloud journey, facilitating workshops, helping you evaluate your cloud maturity, and assisting you with the delivery of cloud traffic and risk assessments. Don't hesitate to contact us today to get started.

For more information on our cloud security product line, visit www.skyhighsecurity.com

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

Learn More

For more information visit us at skyhighsecurity.com

Skyhigh Security

6220 America Center Drive
San Jose, CA 95002
888.847.8766
skyhighsecurity.com