Trustifi

WHITEPAPER

Closing The Collaboration Security Gap

How to Protect Sensitive Data and Reduce Risk Across Microsoft 365

©2026 Trustifi, All rights reserved.

Executive Summary

Microsoft Teams has more than 350 million monthly active users.[1] Together with OneDrive and SharePoint, Teams has become a central hub for daily work, where files, links, and sensitive data move beyond the reach of traditional email security.

Email and collaboration tools like Microsoft Teams are part of the same security problem. The same users, identities, data, links, and threats move across both, yet they are often protected through separate controls and workflows.

Protecting Microsoft 365 requires a connected approach across email and collaboration. Detection, access context, and response need to work across both email and collaboration.

This whitepaper provides a practical framework for evaluating whether security controls extend consistently across email, Teams, OneDrive, and SharePoint, and shows how Trustifi Collaboration Shield applies that approach.

1. One Security Problem, Multiple Channels

Email security does not automatically extend to Microsoft 365 collaboration tools. Files, links, and sensitive data shared through Teams, OneDrive, and SharePoint can fall outside traditional email security controls, creating a gap in detection, access context, and response.

That gap creates risk in two ways: attackers can use collaboration tools as part of an attack, and sensitive data can remain exposed through everyday sharing.

Threats Inside Collaboration Tools

Microsoft has documented multiple campaigns in which threat actors used Teams messages or calls as part of the attack chain.[2] [4] [5] In one campaign, attackers impersonated IT support through Teams and convinced users to grant remote access through Quick Assist, creating an opportunity to steal credentials and deploy ransomware.[2]

ReliaQuest documented a similar tactic associated with Black Basta.[3] Attackers flooded a user's inbox with subscription emails, then contacted the user through Teams while posing as IT support and offering to fix the problem. The attackers used that interaction to gain remote access and continue the attack.

In both cases, Teams became a critical part of the attack path, showing how attackers can reach users through collaboration channels rather than relying on email alone.

Sensitive Data Exposure

Collaboration risk is not limited to malicious attacks. Everyday sharing can also expose sensitive information.

A folder opened to an outside contractor for a short project can remain accessible after the project ends. Inherited permissions can give a file broader access than its owner intended. A sharing link created for one purpose can continue to provide access until it expires or is revoked.[8]

These scenarios may not create an obvious malicious event to investigate. The issue is often the current state of access: permissions or sharing links remain in place after the original business need has changed or ended.

©2026 Trustifi, All rights reserved.

2. A Threat Model for Microsoft 365 Collaboration

Before evaluating a collaboration security product, start by defining what needs to be protected. Teams, OneDrive, SharePoint, and meeting content each create different types of exposure.

Surface	What's exposed	Where additional visibility may be needed
Teams chats and channels	Sensitive data and links shared in messages, and communication with external users.	Microsoft provides DLP and URL-protection capabilities for Teams, but coverage varies by license, policy configuration, and content type. Organizations should evaluate whether those controls provide the cross-surface visibility and access context they need.[6 7]
SharePoint libraries	Sensitive files uploaded directly to libraries, along with inherited or broadly scoped permissions that may expand access beyond the file owner's intent.	SharePoint and OneDrive support DLP, sensitivity labeling, and sharing controls, but effective access can depend on inherited permissions, site settings, and policy configuration. Organizations should evaluate how easily they can see current access to sensitive content across sites.[6 8]
OneDrive for Business	External sharing and "anyone with the link" access that may remain active until an expiration policy applies or the link is revoked.[8]	Administrators can control link types and configure expiration policies for links. Organizations still need a practical way to understand which links are active and how those links affect access to sensitive content across the environment.[8]
Meetings and shared files	Meeting-related files and recordings whose access is governed by the Microsoft 365 services in which they are stored.	Coverage can vary by content type, storage location, licensing, and policy configuration. Organizations should verify which meeting-related messages, files, links, and recordings are covered by their DLP and threat-protection controls.[6 7]

The four surfaces leave security teams with the same unanswered question:

What sensitive information exists across these collaboration tools, and who can access it right now?

A practical coverage check

Before adding a new tool, test the controls you already have. Pick one sensitive file or message in each collaboration surface and answer four questions: Can you identify the content as sensitive? Can you see who can access it now? Can you determine how that access was granted? Can you take action from the same workflow used to investigate the finding?

Any question that requires a separate export, console, or manual reconstruction is a useful indicator of where your current operating model may have a gap.

©2026 Trustifi, All rights reserved.

3. Fragmented Security Creates an Accountability Gap

After a potential data exposure, security teams need to answer three questions quickly:

01	02	03
Who accessed this file?	**How was this data shared?**	**Who can access it now?**
Historical activity shows who interacted with the file in the past.	Audit activity can show how the file or link moved through the environment.	Current permissions, group memberships, and active sharing links show whether the exposure still exists.

Depending on the tools and configuration in place, a team may need to review audit activity, SharePoint permissions, group memberships, and active sharing links across multiple Microsoft 365 views to understand what happened and determine who still has access.

That can turn a simple question into a multi-step investigation.

For internal security teams and MSPs, those extra steps add systems and manual work to the investigation, particularly when a clear answer is needed for an auditor, regulator, or executive team.

Protecting collaboration separately from email can fragment the view of a single incident.

Accountability requires connecting detection with access and response across channels.

Run an incident-readiness test

Choose a recent sharing event involving sensitive data and document the steps required to answer: what was shared, who accessed it, who can access it now, and what action would contain the exposure. Record the number of systems and manual steps involved. That baseline gives you something concrete to improve and measure later.

©2026 Trustifi, All rights reserved.

4. What Unified Email and Collaboration Security Should Deliver

The goal is not another isolated product, but a security model that extends from email into collaboration. A useful way to compare solutions is to look at how far they take teams from visibility to action.

The maturity model

Stage	What it means	You know you're here when...
1. Visibility	You can see what happened: what was shared, who shared it, where it happened, and who received it.	You can build an activity timeline without manually exporting and combining logs.
2. Detection	The security platform inspects the content itself and identifies sensitive information, malicious links, and other risks.	You can see what sensitive information is inside a document, not just that it was shared.
3. Access mapping	A comprehensive access view accounts for who can access an item right now, including users, groups, inherited permissions, and active sharing links.	You can answer "who can access it now?" from a single view.
4. Automated remediation	Policies automatically take action when risk is detected.	Response actions can be triggered when risk is detected. Depending on the platform, those actions may include quarantine, reviewer notification, escalation, or changes to sharing and access.

Visibility and detection are only part of the model; access context and remediation complete the path from finding to action.

Five questions to ask any vendor

- [ ] **Does it inspect the actual content, or just activity logs?**
  Activity logs tell you that something happened. Content inspection tells you what was inside the file or message.

- [ ] **Does it show who currently has access?**
  Knowing that a file contains sensitive information is useful. Knowing exactly which users, groups, and external links can access it makes the finding actionable.

- [ ] **Can it deploy without agents or mail-flow changes?**
  Collaboration security should not require an endpoint rollout or changes to the organization's email architecture.

- [ ] **Can MSPs manage risk across multiple tenants?**
  Evaluate whether findings, policies, and response workflows can be managed across customer environments or require separate administration within each tenant.

- [ ] **Can email and collaboration use the same security policies?**
  Separate products can mean separate classification models, policies, consoles, and workflows. A unified approach can reduce the number of systems and policy sets teams need to maintain.

©2026 Trustifi, All rights reserved.

5. Why Access Mapping Matters

Detecting sensitive information establishes what is at risk. Access mapping establishes who can reach it now.

A file containing PII that is limited to authorized employees presents a different exposure than the same file accessible to external users through inherited permissions or an active sharing link.

Historical activity provides another part of the picture. Audit records can show who interacted with a file in the past. They do not necessarily answer whether that person, or someone else, can still access the file today.

Effective collaboration security needs to connect sensitive data detection with current access. Security teams need to understand not only what sensitive information exists, but who can currently reach it and how that access is granted.

From Detection to Resolution

Detection
An employee uploads a spreadsheet to SharePoint. The security platform identifies sensitive information in the file.

Current Access
A comprehensive access assessment accounts for who can reach the file now, including internal and external users, groups, inherited permissions, and active sharing links.

Remediation
Based on the finding, security teams can quarantine risky content, notify reviewers, or take appropriate steps in Microsoft 365 to address excessive access.

Audit Trail
The response is recorded, including what was detected, what action was taken, and when.

Historical Activity vs. Current Access

These answer two different questions:

Historical activity: Who accessed this file?
Audit activity shows who interacted with the file in the past.

Current access: Who can access this file now?

Determining current access requires accounting for permissions, groups, inherited access, and active sharing links.

Both matter during an investigation. A file can remain exposed even when no recent access appears in the activity history.

©2026 Trustifi, All rights reserved.

6. Compliance and Regulatory Alignment

Compliance and regulatory requirements extend across the Microsoft 365 environment, including Teams, OneDrive, and SharePoint. Organizations need controls that help identify regulated data, manage how it is accessed and shared, and maintain a record of how potential exposure is addressed.

Extending those controls into collaboration tools helps security teams align data protection across Microsoft 365 while supporting requirements under frameworks such as HIPAA, PCI-DSS, and GDPR.

Framework	Where collaboration coverage matters
HIPAA	Identifies PHI shared through Teams or stored in OneDrive and SharePoint, supports visibility into access, and maintains records of how that information was handled.
PCI-DSS	Cardholder data may be copied or shared into collaboration tools outside its intended environment. Visibility and policy enforcement identify and restrict that exposure.
GDPR	Organizations need to understand where personal data is stored, who can access it, and whether it has been shared externally.

Extending compliance controls into collaboration can help organizations maintain consistent data protection and response records across Microsoft 365. During an incident, that record can help teams establish exposure and response without reconstructing events across separate views. A consolidated access view can also bring information used for incident scoping into one place.

©2026 Trustifi, All rights reserved.

7. Operational and Security Outcomes

Extending email security into collaboration changes how security teams and MSPs manage Microsoft 365 risk.

Simplify investigation and response
When content inspection, access context, and remediation are connected, teams can move from identifying a risky file to understanding its exposure and taking action through a more consolidated workflow.

For MSPs, that same model can be applied across customer environments rather than managing collaboration risk through separate processes for each tenant.

Measure the impact
Organizations can establish a baseline before extending collaboration security and track operational and security outcomes over time, **including actions taken through security controls or Microsoft 365:**

- Sensitive data identified across collaboration tools
- Risky sharing links removed
- External access revoked
- Incidents remediated
- Time required to determine current access

For MSPs, collaboration security also creates an opportunity to extend existing Microsoft 365 security services and address a customer security question that email-only coverage does not answer:

"What is protecting our Teams, OneDrive, and SharePoint environments?"

©2026 Trustifi, All rights reserved.

8. Applying a Unified Security Model: Trustifi Collaboration Shield

Trustifi Collaboration Shield extends Trustifi's existing email security model into Microsoft Teams, OneDrive, and SharePoint.

Collaboration Shield brings DLP classification, URL and file analysis, policy-based actions, and reviewer workflows into Teams, OneDrive, and SharePoint. These capabilities are managed alongside Trustifi email security from the same console.

Mapped against the framework

Evaluation criterion	How Collaboration Shield addresses it
Inspects content at the source	Scans messages and files directly in Teams, OneDrive, and SharePoint through the Microsoft Graph API, including content that never passes through an email gateway.
Provides access visibility	Shows users and external users with access to protected resources, helping administrators investigate how sensitive content is exposed.
Deploys without agents	Connects directly to Microsoft 365 through API consent, with no software to install, mail-flow changes, or infrastructure changes required.
Scales across tenants	Provides multi-tenant management for MSPs to manage collaboration security across customer environments.
Unifies email and collaboration management	Protects email and Microsoft 365 collaboration from the same Trustifi console, with DLP and malicious-content detection, policy-based actions, and reviewer workflows.

Collaboration Shield covers Microsoft 365: Teams, OneDrive, and SharePoint. Organizations that also rely on Slack or other third-party file-sharing platforms should scope coverage to email plus Teams, OneDrive, and SharePoint rather than assume every collaboration channel is included.

©2026 Trustifi, All rights reserved.

9. Conclusion: One Security Model Across Email and Collaboration

Protecting Microsoft 365 requires looking beyond the inbox. Teams, OneDrive, and SharePoint introduce additional places where threats and sensitive data need to be detected, access understood, and risk addressed.

A connected security model brings those capabilities together across email and collaboration rather than treating each channel as a separate problem.

Trustifi Collaboration Shield applies that approach across Teams, OneDrive, and SharePoint, helping security teams and MSPs identify sensitive data, gain visibility into access, and take action from one platform.

Trustifi

See Collaboration Shield in Action

Request a demo – See how Trustifi protects sensitive data and identifies risky access across Teams, OneDrive, and SharePoint.

Contact Us

©2026 Trustifi, All rights reserved.

Sources

1. Microsoft, "Supercharge Your Business: Getting Small Businesses Ready for 2025 with Microsoft 365," Microsoft Community Hub, February 7, 2025.
https://techcommunity.microsoft.com/blog/microsoft_365blog/supercharge-your-business-getting-small-businesses-ready-for-2025-with-microsoft/4374723

2. Microsoft Threat Intelligence, "Threat actors misusing Quick Assist in social engineering attacks leading to ransomware," May 15, 2024, updated June 2024.
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

3. ReliaQuest, "ReliaQuest Uncovers New Black Basta Social Engineering Technique," October 25, 2024.
https://reliaquest.com/blog/black-basta-social-engineering-technique-microsoft-teams/

4. Microsoft Threat Intelligence, "Disrupting threats targeting Microsoft Teams," October 7, 2025.
https://www.microsoft.com/en-us/security/blog/2025/10/07/disrupting-threats-targeting-microsoft-teams/

5. Microsoft Defender Experts, "Help on the line: How a Microsoft Teams support call led to compromise," March 16, 2026.
https://www.microsoft.com/en-us/security/blog/2026/03/16/help-on-the-line-how-a-microsoft-teams-support-call-led-to-compromise/

6. Microsoft Learn, "Data loss prevention and Microsoft Teams," accessed September 2, 2026.
https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams

7. Microsoft Learn, "Microsoft Defender for Office 365 support for Microsoft Teams," accessed September 2, 2026.
https://learn.microsoft.com/en-us/defender-office-365/mdo-support-teams-about

8. Microsoft Learn, "Plan sharing and collaboration options in SharePoint and OneDrive," accessed September 2, 2026.
https://learn.microsoft.com/en-us/sharepoint/collaboration-options

About Trustifi

Trustifi gives MSPs and IT teams one AI-native platform to protect the email lifecycle—from inbound threats and account compromise to outbound data loss and human risk. Unified detection, policy, training, and archiving reduce security gaps and operational complexity without forcing teams to replace their existing Microsoft 365 or Google Workspace environment.

©2026 Trustifi, All rights reserved.