

Q1 | 22



metrigy

Best Practices for Enabling Secure External Collaboration

*Federation provides the best choice for usability,
risk minimization, and policy enforcement*



Best Practices for Enabling Secure External Collaboration

*Federation provides the best choice for usability, risk
minimization, and policy enforcement*

Q1 2022

Irwin Lazar
*President and Principal Analyst
Metrigy*

Table of Contents

Executive Summary	3
The Rise of Team Collaboration	4
Business Benefits of Team Collaboration	5
Why Email isn't the Answer for B2B Collaboration	5
Safely Extending Team Collaboration to Business Partners	6
B2B Team Collaboration Approaches	6
Direct Federation	7
Guest Accounts	7
Third-Party Federation Services	7
Picking the Right Approach: What to Look For?	7
Vendor Comparisons	10
Conclusions and Recommendations	10

Executive Summary

Companies have ramped up their adoption of team collaboration over the last several years to support an increasingly distributed workforce. The widespread adoption of team collaboration enables a shift from email-based conversations to ones that provide context, and that enable integrations to eliminate app switching. Realizing the full benefits of team collaboration requires extending it to partners, suppliers, and customers to enable shared, cross-company workspaces. Doing so safely and securely requires both picking the right federation approach, and the right vendor that can meet security and compliance needs. Of all the available choices, direct federation between workspaces provides the highest level of security as well as support for integrations and workflow automations that enable the optimal collaboration experience.

To safely and securely implement team collaboration federation:

- Evaluate providers based on their security, governance, and compliance controls, especially in their ability to support regulatory environments such as HIPAA and FedRAMP
- Ensure the ability to implement granular controls for enabling or restricting establishment of federated channels in accordance with policies
- Look for solutions that enable distributed management and give workspace administrators the ability to manage their own federation
- Evaluate capabilities for integrating third-party applications, data sources, and automation into federated workspaces to achieve the highest business value

The Rise of Team Collaboration

Perhaps no technology has changed the collaboration landscape in as short a period of time as team collaboration. Metrigy began tracking adoption in 2017 as products like Slack gained mainstream attention, finding at the time that just under 20% of companies had adopted the technology. By the time we published our *Workplace Collaboration: 2021-22* study in early 2021, almost 68% of companies had either adopted the technology or planned to do so by the end of 2021.

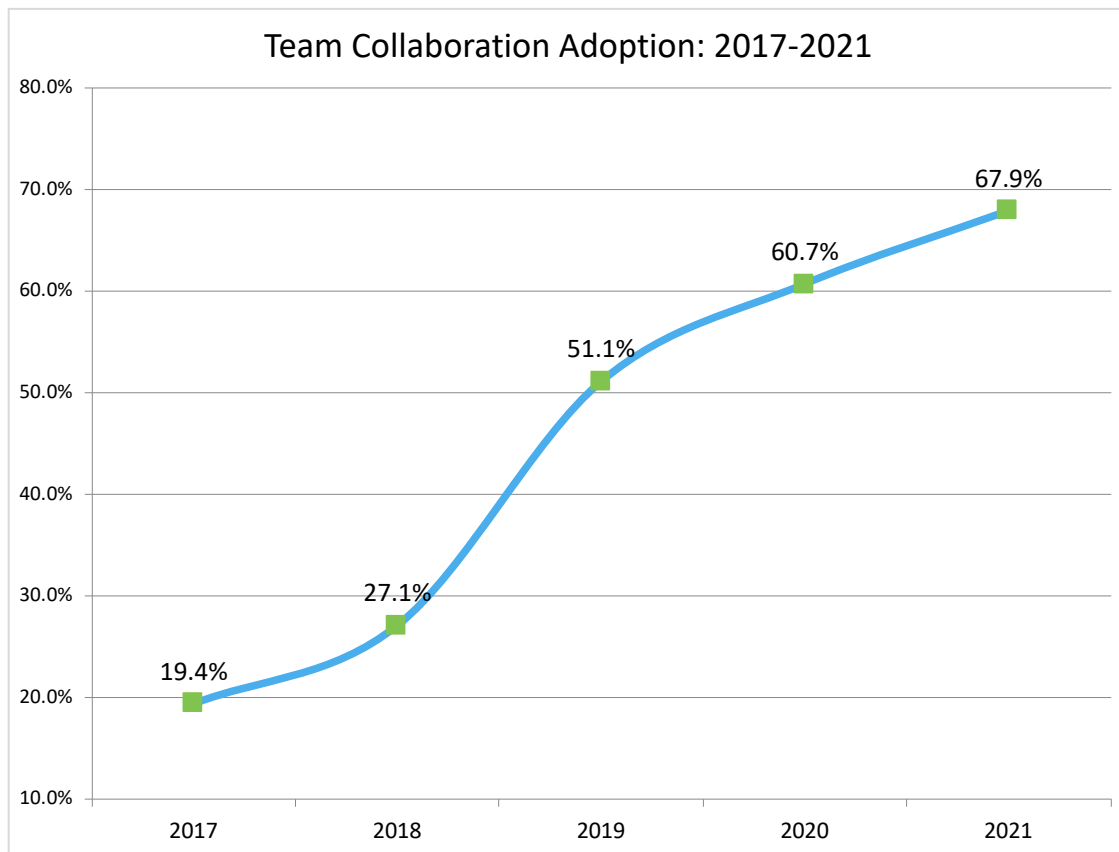


Figure 1: Team Collaboration Adoption: 2017-2021

What started as an app largely used within IT and application developer groups has quickly exploded into enterprise-wide adoption. Among the 476 companies that participated in our research, almost 72% of employees now use team collaboration apps.

The team collaboration market isn't just defined by the massive increase in adoption and utilization; team collaboration apps themselves have rapidly evolved beyond their messaging roots. Today, more than 57% of companies now view team collaboration applications as a hub for work, meaning that they integrate team collaboration apps with data sources, CRM, file sharing, help desk, and other business apps. These off-the-shelf and custom integrations, coupled with easy-to-create workflows, enable use cases ranging from management of employee onboarding to help desk and customer support, expense approval, and sales

opportunity management, all from within the team collaboration user interface. The end result is improved workflows, and simplified end-user experiences.

Business Benefits of Team Collaboration

Many adopters of team collaboration apps have documented measurable business benefit from their use. As shown in Figure 2, more than one-third have reduced meetings by almost 32% and have achieved productivity gains averaging 22.2%. Additional measured benefits come in the form of reducing cost by simplifying collaboration environments, reducing the use of email for internal collaboration, and increasing revenue by improving sales and customer support effectiveness.

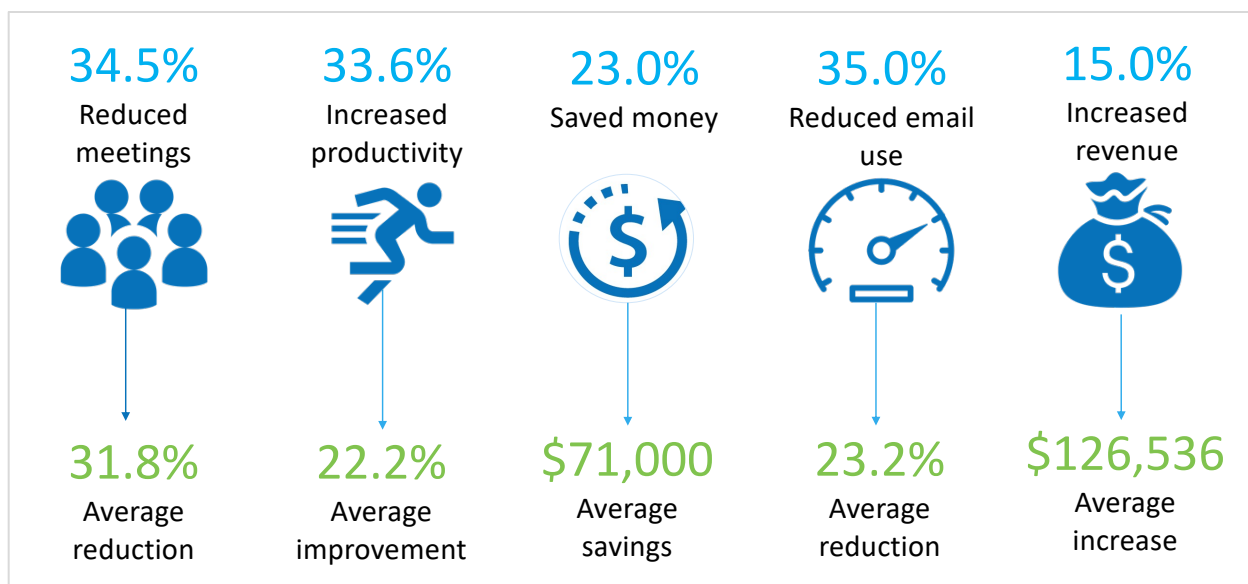


Figure 2: Team Collaboration Benefits

Why Email isn't the Answer for B2B Collaboration

Despite the clear benefits that team collaboration apps deliver, many companies still only rely on them for internal use, defaulting to email and file sharing to work with customers, partners, and suppliers. This means:

- Lack of context around communications, requiring individuals to search their inbox to find conversations rather than having them contained within a topic or project-based channel
- No ability for those joining into an engagement to easily catch up on past discussions
- No integrations with other applications or data sources that cross-company team members must rely on to do their work
- No ability to leverage automations and workflows to simplify processes and improve productivity

The end result is that companies that haven't yet extended their team collaboration to business-to-business (B2B) use cases are missing out on the quantifiable value that team collaboration apps deliver.

Beyond the inability to save money, increase revenue, and improve productivity, the use of email for B2B conversations creates potential security risk as companies lose control of the messages that leave their domain. Rather, they are dependent on the security controls of their partners. For example, an internal employee inadvertently sends an email with sensitive pricing and product information to a business partner. That business partner, in turn, could then potentially forward the email to its customers, without the knowledge of the originating sender. Or, a mistyped email address could result in information going to the wrong recipient.

In addition, email is a medium often clogged by junk mail and subject to phishing attacks. Legitimate and trusted messages may get lost in spam filters. And, users may not be able to validate identities of those who send them emails.

Safely Extending Team Collaboration to Business Partners

The business imperative for extending team collaboration applications beyond the enterprise boundaries is clear. But doing so safely requires adherence to security, governance, and compliance requirements. These typically include:

- **Data protection and control** to include data loss prevention (DLP) of company data, and the ability to quickly identify and mitigate inadvertent information sharing. In an ideal environment, each company participating in a cross-team collaboration workspace will maintain control over its own encryption keys to ensure that it can withdraw messages posted by an individual user all the way up to the entire organization
- **Access control and authentication** to ensure that only those approved to participate in a conversation are able to join a shared channel, and that organizations can implement access controls such as multi-factor authentication
- **Administrative approval** to establish B2B connections with only known and trusted external organizations
- **Ongoing administration** to ensure that B2B connections are terminated when no longer necessary to maintain

B2B Team Collaboration Approaches

Companies have several approaches for extending team collaboration outside of their organization. These include enabling guest access to existing team collaboration apps, investing in third-party gateway services, and leveraging a team collaboration vendor's native direct federation capability. The direct federation approach offers clear benefits in terms of security, data and information control, manageability, and user experience. Each approach is detailed further on the next page.

Direct Federation

Direct federation enables companies to connect their team collaboration apps to one another via shared channels. Direct federation only supports connectivity between the same app. Users remain within their own familiar workspace and communicate with external people via a shared channel. In direct federation, each company participating in the shared channel maintains complete control over user access and their own data. Direct federation allows team collaboration app users in all participating organizations to access all available features, integrations, and automations. And, it allows each company to enforce its own encryption, sharing, access, and DLP policies.

Guest Accounts

Guest accounts allow team space owners and managers to simply invite an external participant to join a channel or workspace. Guest accounts are useful when there's minimal need for external access, or when an external participant does not use the same team collaboration app within their own organization. Drawbacks of this approach include difficulty in managing guest access, including knowing when access is no longer required. Guest accounts also require guests to log into the workspace of their business partner rather than work from within their own company's workspace. This can be an inconvenience, requiring frequent switching between apps, or tenants in the Microsoft Teams world, to see and respond to new messages.

Third-Party Federation Services

Third-party federation services provide gateways between team collaboration applications. They can be useful when cross-company teams prefer to work within their own native team collaboration app. Drawbacks to this approach include the need to procure a separate gateway service, an inability to easily launch meetings and calls from within chats, a loss of features that team collaboration providers natively deliver within their own apps, and an inability to support end-to-end encryption.

Picking the Right Approach: What to Look For?

Not all team collaboration vendors offer equal federation capabilities. When evaluating potential solutions, it's important to assess security, governance, and compliance features. The following section provides a set of must-have features, and insight into the federation capabilities delivered by Slack, Webex by Cisco, and Google Chat. Note that while Microsoft has announced a federation capability for Teams, it is not yet available. Microsoft has announced plans to release a public preview in March of 2022, but has not shared feature details.

Key features and capabilities include:

- **Ability to control messages and revoke access** – Team space administrators must have the ability to withdraw messages and block access to shared spaces should a security incident occur. They must be able to maintain this level of control for the entire organization, or be able to delegate it out to team leaders managing specific channels.

- Both Slack and Webex offer the ability for administrators to revoke access to federated channels as well as messages posted within those channels. Google does not offer granular channel access controls.
- **DLP** – These controls prevent the sharing of unauthorized or potentially sensitive information into shared channels. Examples may include certain types of files based on type or keyword (e.g., “Business Plan,” “Sensitive,” “Confidential”). Federation DLP controls must support a company’s overall governance and DLP plan.
 - Google, Slack, and Webex support DLP capabilities both natively or through third-party partners. Slack, for Enterprise Grid customers, offers an API that customers can use to export data to a third-party DLP partner.
- **Mobile device controls** – Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) allows companies to control access to team apps from mobile devices. This allows organizations to mandate mobile device security controls such as long PINs, touch, or facial recognition to unlock the device. MDM features may also enable remote wipe of data, block copying of text and screen capture, or enforce the use of approved browsers for accessing a team workspace.
 - Only Slack provides native MDM controls for Android and iOS operating systems. Both Slack and Webex also support integration with third-party MDM providers.
- **Managed encryption keys** – Company-owned encryption keys ensure that no third-party participant can access encrypted data without approval. A company may store keys within their own data center or in a third-party escrow service such as AWS Key Management Service (KMS).
 - Slack supports customer-managed keys through AWS. Webex offers its own KMS through control hub, or support for third-party or on-premises KMS. Google does not support external key management.
- **Compliance support (e.g., HIPAA, FedRAMP) and eDiscovery** – For regulated industries such as financial services and healthcare, federation services must support required compliance controls and allow for the retention of messages containing personal health information (PHI) or personally identifiable information (PII) in accordance with regulatory requirements. Additionally, those operating in U.S. federal government environments are likely to require a solution that is FedRAMP moderate authorized at a minimum.
 - Google, Slack, and Webex all support eDiscovery, HIPAA, and FedRAMP at least up to moderate.
- **Access controls, including centralized and delegated permissions** – Federation services must provide organizations with the ability to control establishment and maintenance of shared channels. Automated approaches include creating approved and block lists, as well as generation of approval requests to the appropriate personnel when an employee creates a shared channel. Additional controls may include automated expiration, or a reauthorization request, after a period of time to ensure that shared channels end once they are no longer needed. Ideally companies should be able to delegate the approval

and revocation process to individual workspace administrators or lines of business, in accordance with centralized security policies.

- Google simply provides administrators with the ability to turn off external chat. Slack Connect and Webex provide administrative controls to approve external access and distribute access management. Slack offers granular controls allowing an administrator to withdraw messages from individual users, or the entire organization.
- **End-user controls** – Federation shouldn't open an attack vector into the enterprise. Instead, team collaboration vendors, either natively or through partners, should provide for the ability to protect conversations by implementing controls to prevent spam or phishing attacks, or the inadvertent or deliberate sharing of malware into team channels.
 - Google, Slack, and Webex provide malware and phishing protection, both natively as well as through partners.
- **Guest awareness** – External and internal participants should be clearly indicated to all federated channel members via both indicating that the channel contains external participants and the visual identification of individual external participants.
 - Google marks external users and spaces as external. Slack offers granular capabilities to confirm that invitations to join a channel are being sent to an external guest. Federated channels are both grouped and marked with a double-diamond icon, and external organizations are shown within the channel conversation. Individual user profile pictures display the participant's organization icon. Webex shows an external user's domain next to their name in a channel conversation and provides notification within a channel member list that external participants are in the channel.
- **Monitoring and logging** – Additional controls should allow companies to monitor and log conversations as a means of protecting against attack and minimizing the threat of data loss. Here again, team collaboration vendors should offer either native controls, or the ability to integrate external services that identify misuse of federated channels, attack attempts, or the use of abusive language.
 - Only Slack and Webex have conversation-monitoring capabilities available through third-party partners.

Vendor Comparisons

The below table provides a high-level overview of direct federation capabilities available today from leading team collaboration applications. Slack provides a dedicated federation service called Slack Connect, while Google and Webex allow for the management of external federation capabilities through existing administrative management controls.

As previously noted, Microsoft’s federation offering, Teams Connect, is not yet available. All other provider federation services are available today.

	Google Chat	Slack Connect	Webex by Cisco
Control and revocation	N/A	✓	✓
DLP	In beta	✓ (3 rd party; native in beta)	✓
MDM	N/A	✓ (native & 3 rd party)	✓ (3 rd party only)
Managed encryption keys	N/A	✓	✓
Compliance support	✓	✓	✓
Access controls	✓ (limited)	✓	✓
End-user controls	✓	✓	✓
Guest awareness	✓	✓	✓
Monitoring and logging	N/A	✓	✓

Conclusions and Recommendations

Team collaboration applications deliver measurable business value in terms of reducing costs, increasing revenues, and improving productivity. But team collaboration’s benefits shouldn’t stop at the company boundary. The benefits that team collaboration brings to internal communications and collaboration should also extend to interactions with partners, suppliers, and even customers. While companies have numerous options for extending team collaboration workspaces, direct federation offers the best approach for ensuring security and compliance, and enabling integrations with apps and data.

Today, only Slack Connect provides an out-of-the-box offering for external federation. Webex offers federation control and management embedded in its Webex Hub management console.

Google offers limited external federation control and management. Microsoft has not yet delivered a federation solution.

To safely and securely implement team collaboration federation:

- Evaluate providers based on their security, governance, and compliance controls, especially in their ability to support regulatory environments such as HIPAA and FedRAMP
- Ensure the ability to implement granular controls for enabling or restricting establishment of federated channels in accordance with policies
- Evaluate features designed to clearly convey identity of external participants within channels, as well as channels that contain external participants
- Look for solutions that enable distributed management and give workspace administrators the ability to manage their own federation
- Evaluate capabilities for integrating third-party applications, data sources, and automation into federated workspaces to achieve the highest business value

ABOUT METRIGY: Metrigy is an innovative research firm focusing on the rapidly changing areas of Unified Communications & Collaboration (UCC), digital workplace, digital transformation, and Customer Experience (CX)/contact center—along with several related technologies. Metrigy delivers strategic guidance and informative content, backed by primary research metrics and analysis, for technology providers and enterprise organizations.