Enterprise Strategy Group™ by TechTarget

THE FREEDOM TO COMMUNICATE AND COLLABORATE

Challenges in Securing an Overabundance of Tools

Dave Gruber, Principal Analyst

APRIL 2023

Research Objectives

As more workers collaborate virtually, many organizations now depend on additional digital communication tools beyond email. New collaboration tools provide attackers the opportunity to engage with humans to evade automated controls, extending phishing, BEC, credential theft, and other socially engineered attacks beyond email. Advanced attacks leverage multiple attack vectors, requiring individual, core security controls to work together to detect and prevent advanced attacks. This extends beyond traditional security operations tools (e.g., SIEM, SOAR, EDR, and XDR) to core network, cloud, endpoint, and identity controls.

As IT and security teams focus on risk-driven security strategies, consistency of policies and priorities across all enterprise communication channels becomes critical to strengthening security posture. More education is needed to motivate security architects to embrace this higher-level perspective. To gain further insight into these trends, TechTarget's Enterprise Strategy Group (ESG) surveyed 490 IT and cybersecurity professionals at organizations in North America (US and Canada) and Western Europe (UK, France, and Germany) involved with securing enterprise communication and collaboration technology and processes.

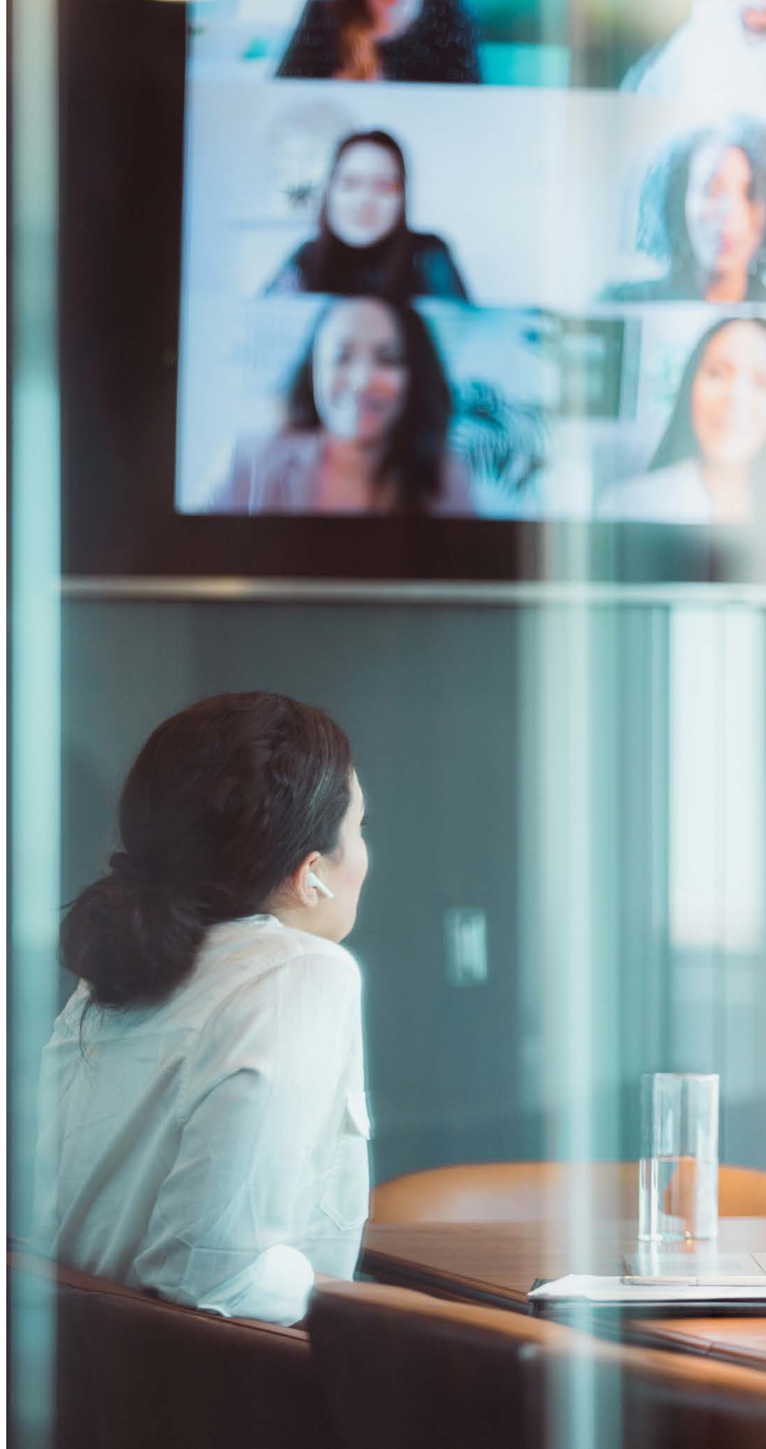
In terms of the risk and security of the many electronic communication and collaboration tools in use, this study sought to:

Assess how much of a concern this threat vector is for IT and security leaders.

Understand where and how organizations are currently securing this threat vector.

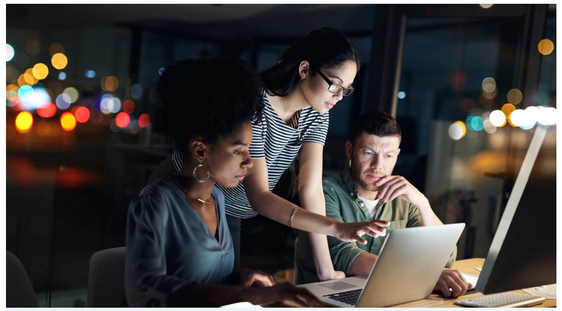
Determine where this expanding threat vector fits into modern security strategies and practices.

Identify key challenges, objectives, and opportunities to mitigate risk.



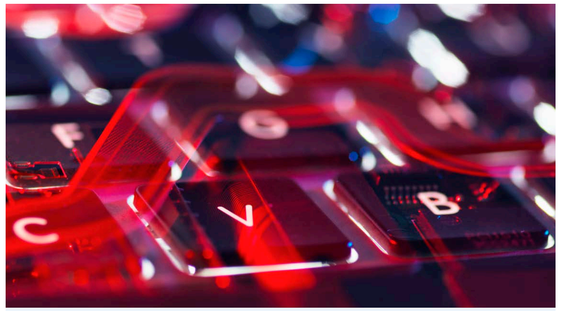
KEY **FINDINGS**

CLICK TO FOLLOW



Communication and Collaboration Tools Proliferation Is Driving Consolidation

PAGE 4

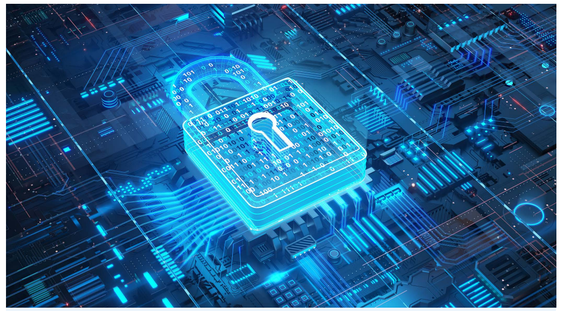


Communication and Collaboration Tools Are Considered a Significant Risk Vector for Most, Driving Continued Investments

PAGE 8

While Confidence in Native Communication and Collaboration Security Controls Is High, Gaps Persist

PAGE 12

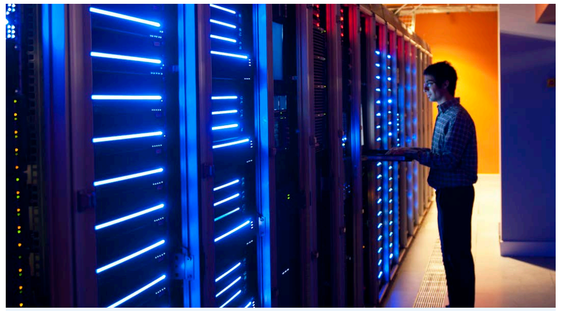


Weaknesses Endure Despite the Maturity of Email Security

PAGE 15

There Is Opportunity to Improve the Security of Sensitive Data within Communication and Collaboration Tools

PAGE 19



IT and Security Operating Models for Securing Communication and Collaboration Tools Are Still Evolving

PAGE 22

Communication and Collaboration Tools Proliferation Is Driving Consolidation

Communication and Collaboration Tools Abound

Modern IT environments were becoming far more distributed even before pervasive work-from-home initiatives stemming from the pandemic caused a spike in remote work and an increased dependence on multiple communication and collaborations channels. As workers strive to work efficiently with other team members in this highly distributed environment, electronic collaboration tools have become a cornerstone of their operating model, for both internal and external communication and collaboration. In addition to email, workers depend on many tools to communicate and collaborate, such as video conferencing and file sharing technologies, so the use of more than 10 such tools is no longer uncommon.

Number of formally sanctioned communication and collaboration tools.

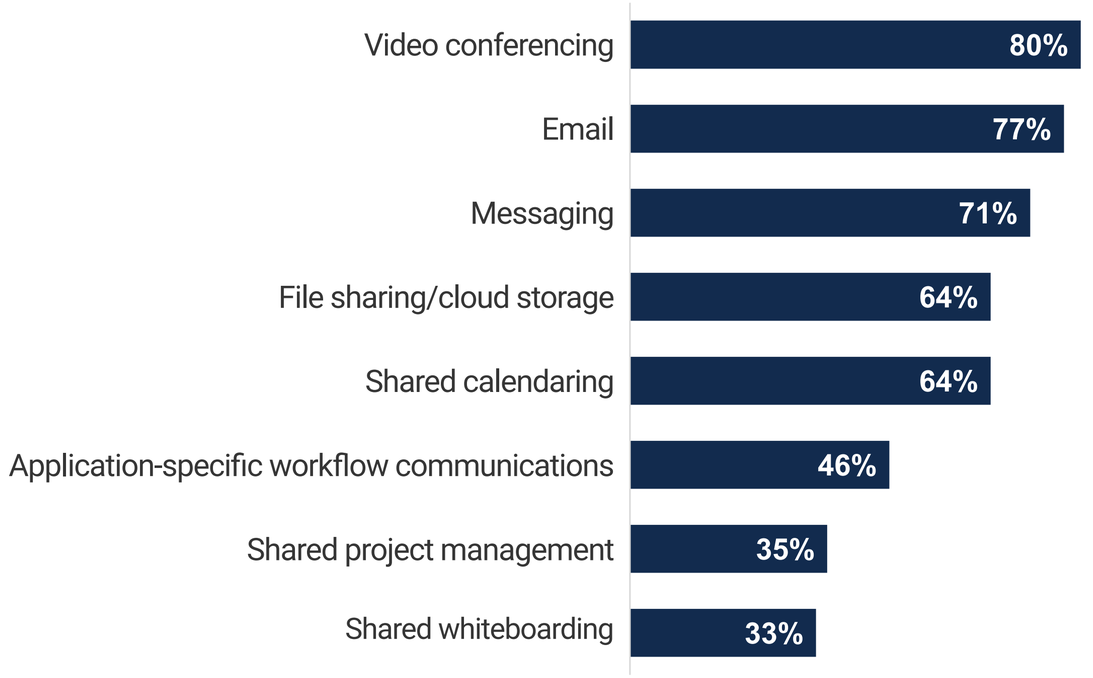
17%
1 to 5 communication and collaboration tools used

47%
6 to 10 communication and collaboration tools used

28%
11 to 15 communication and collaboration tools used

7%
16 to 20 communication and collaboration tools used

Types of formally sanctioned communication and collaboration tools.

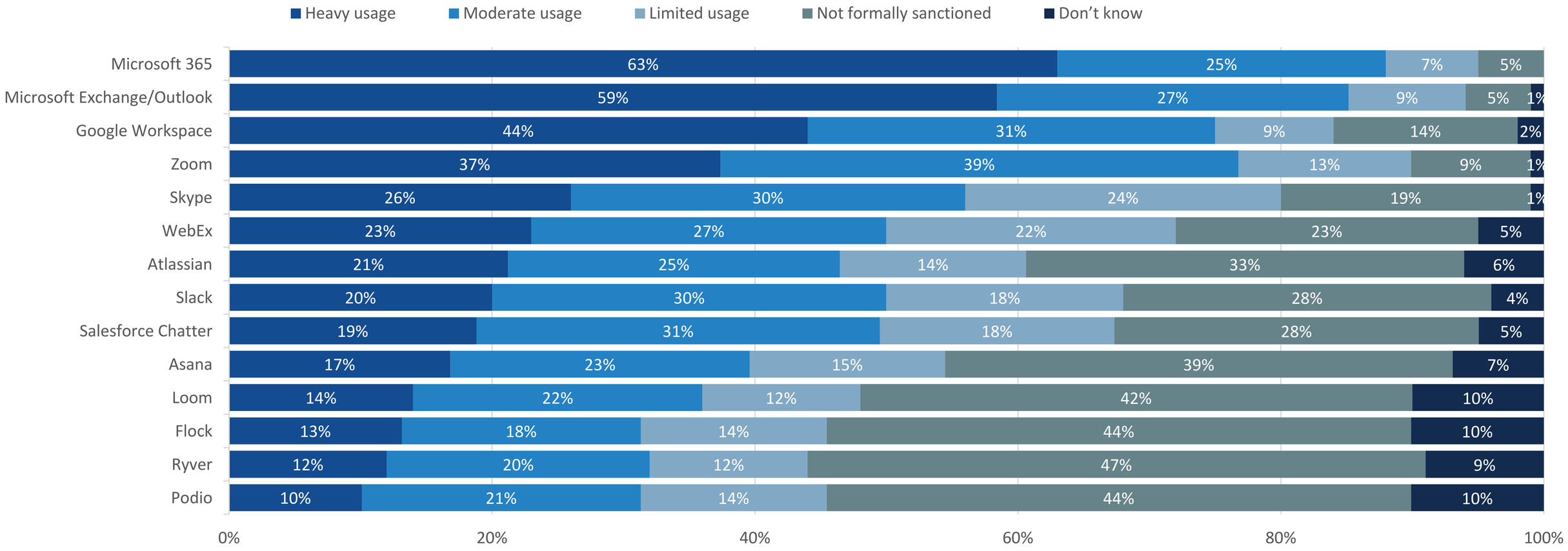


BACK TO CONTENTS

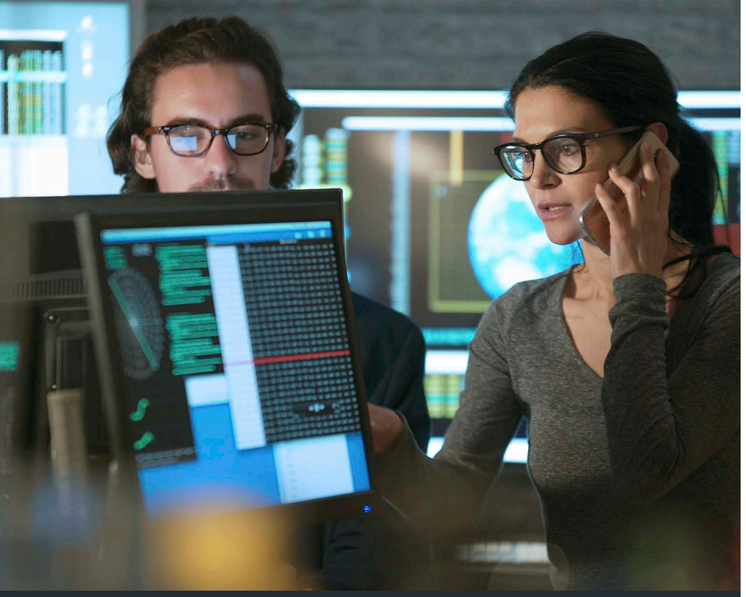
Usage Varies, but Integrated Platforms Have Emerged as the Leaders, with Video Conferencing Tools Following

As integrated communication platforms have emerged and continue to mature, many organizations have seized the opportunity to consolidate communication and collaboration mechanisms, aligning usage policies and simplifying operational management. Despite consolidation, there is still widespread use of additional solo tools, fulfilling specialty use cases or providing integration application workflows. ESG expects this model to continue as innovative solutions emerge, forcing security and IT teams to develop strategies to secure new mechanisms.

Usage trends of formally sanctioned communication and collaboration tools.



BACK TO CONTENTS



Many Plan to Consolidate Communication and Collaboration Tools

With proven benefits tied to the consolidation of solutions, many have already committed to or are investigating consolidation initiatives. Security leads the list in terms of *primary* consolidation drivers, along with the goal to further increase productivity, and simplify usage and administration. A lesser number of organizations are seeking improvement to user experience, better support for remote workers, and cost savings.

Plan to consolidate communication and collaboration tools into a common platform over the next 12 months.

39%
We have a formal plan to consolidate to a single common communication/collaboration platform

46%
We are currently evaluating options to consolidate communication and collaboration tools, but have no formally committed plan yet

10%
We will consolidate communication and collaboration tools opportunistically, but do not have a plan to consolidate to a single platform

3%
We have no plans for or interest in consolidating communication and collaboration tools

Primary consolidation drivers.

30%
Security improvements

22%
Increased user productivity

14%
Simplification (i.e., reduced complexity)

11%
User experience

11%
Support for remote workers

10%
Cost

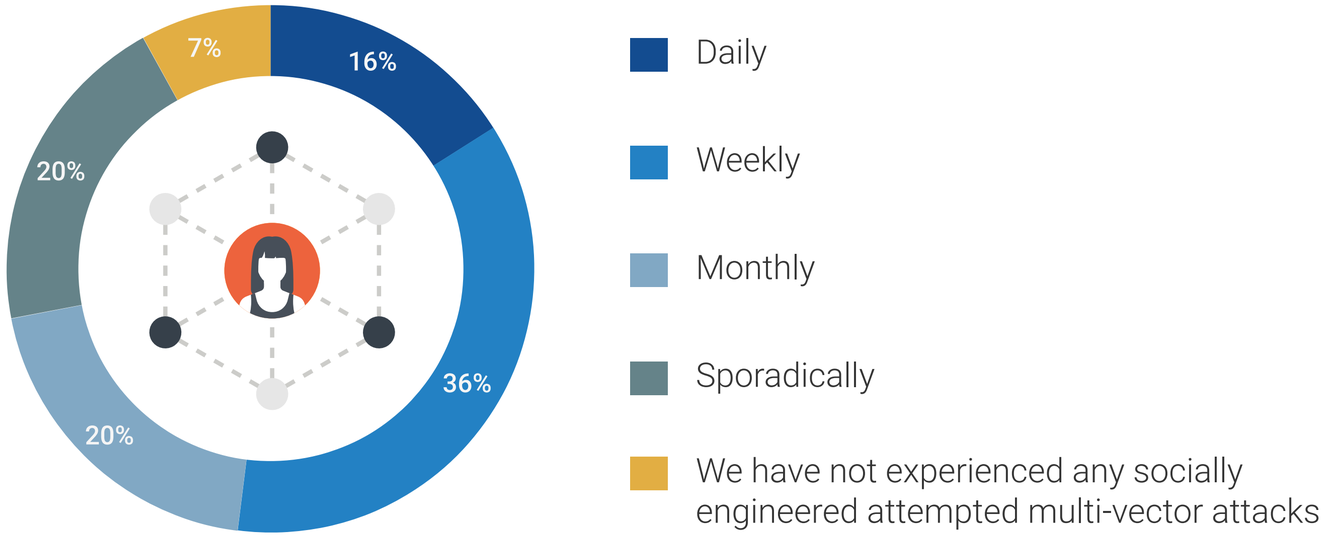
BACK TO CONTENTS

Communication and Collaboration Tools Are Considered a Significant Risk Vector for Most, Driving Continued Investments

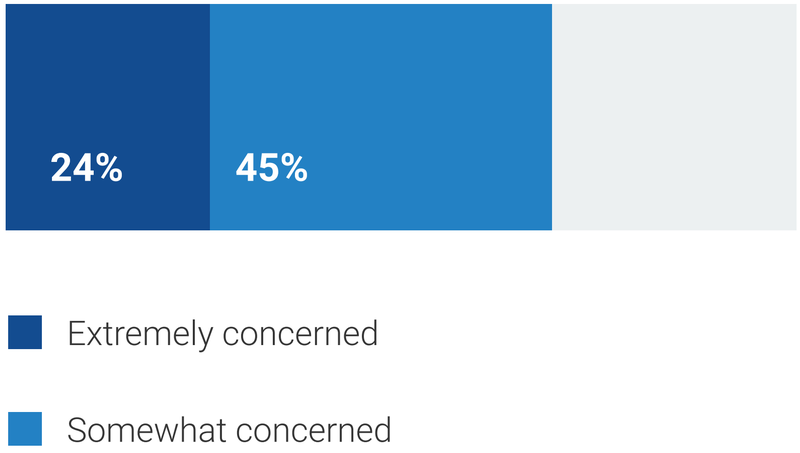
Multi-channel Attacks Are Gaining Momentum

Multi-vector, socially engineered attacks are becoming commonplace, with more than half reporting weekly (36%) or even daily (16%) frequency. As attackers seek to evade security controls by leveraging multiple, siloed communication and collaboration mechanisms, security and IT teams face a new level of complexity in gaining visibility across multiple tools. More advanced detection and response mechanisms are helping aggregate and correlate signals to uncover more complex attacks, but gaps will exist in policy alignment, sensitive data use, and identity misuse. More than two-thirds are concerned that attackers are leveraging other communication and collaboration channels beyond email to evade security controls, with 24% extremely concerned.

Frequency of socially engineered attacks involving multiple electronic communication mechanisms.



Level of concern that attacks will leverage communication and collaboration tools to evade security controls.



BACK TO CONTENTS

Types of threats that leverage communication and collaboration mechanisms that are most concerning to organizations.

38%
Ransomware

37%
Phishing

34%
Malware deployment

23%
Spam

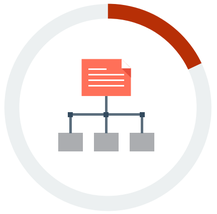
22%
Data leakage/exposure of sensitive data

21%
Credential theft

20%
Attacks leveraging social engineering

20%
Executive impersonation

18%
Business email compromise



18%
Attacks from compromised third parties

16%
Lateral movement of threats internally

15%
Reconnaissance activities

Specific Threat Concerns for Communication and Collaboration

When it comes to threats, ransomware is a top concern for communication and collaboration tools, along with the ongoing array of phishing and malware-based attacks. These concerns align with the same threats surrounding more traditional email communications, which brings up the question of whether this expanded set of communication and collaboration mechanisms is simply an expansion of the possible attack surface for adversaries. As security and IT teams strive to extend email security controls to other mechanisms, security solution providers are stepping up, with many able to secure multiple channels. ESG urges IT and security leaders to challenge solutions providers to expand coverage to include more channels, with the ability to support new channels as they emerge in the future.

BACK TO CONTENTS

> **The good news is that organizations are focused** on strengthening all communication and collaboration channels collectively, including email."

A High-risk Threat Vector and High Priority for Most

The good news is that organizations are focused on strengthening all communication and collaboration channels collectively, including email. Indeed, more than a quarter (27%) consider strengthening security controls across multiple communication and collaboration channels their top priority relative to other security threat vectors, with another 56% classifying it as a high priority. Not surprisingly, this prioritization corresponds to investment plans, with more that three-quarters (76%) anticipating an increase in spending compared with last year to strengthen multi-channel controls.

Priority level of communication and collaboration security.

27% Top priority (i.e., we are currently implementing additional security measures)

56% High priority (i.e., we have budget allocated and resources assigned to implement additional security measures)

Expected spending change for communication and collaboration security controls.

25% Increase signficantly

51% Increase slightly

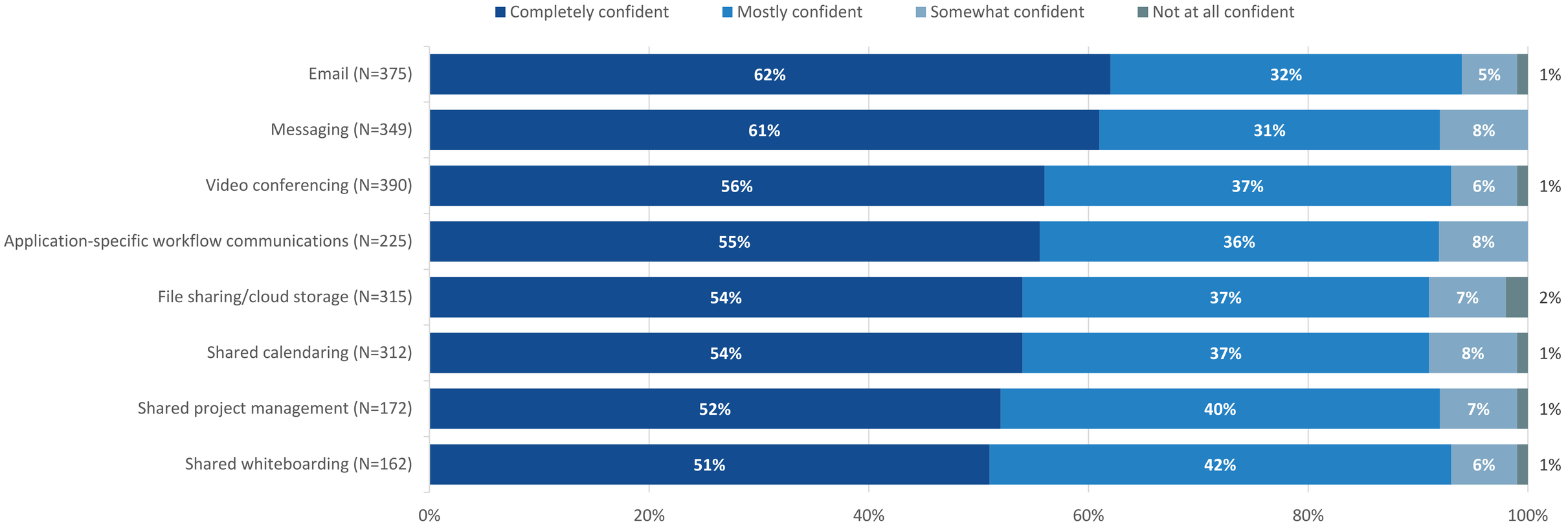
BACK TO CONTENTS

While Confidence in Native Communication and Collaboration Security Controls Is High, Gaps Persist

Confidence Is High in Native Communication and Collaboration Security Capabilities

Despite concerns and planned investments, most are relatively confident in the current native controls included by service providers. Specifically, more than half of organizations expressed complete confidence in all communication and collaboration tools, with email and messaging platforms garnering the highest percentage of organizations.

Level of confidence in the native security capabilities of formally sanctioned communication and collaboration tools.



BACK TO CONTENTS

Attacks Continue to Evade Automated Communication and Collaboration Security Controls

Looking back over the past 12 months, successful malware and phishing tactics continue to plague many across multiple channels. At first glance, this list seems to include the same concerns that have been widely reported as concerns specific to email security in the past and present. ESG believes that these concerns are better understood and therefore top of mind for many; however, more nuanced use of these threats and tactics need to be better explored and understood to determine the true threat associated multi-channel attacks.

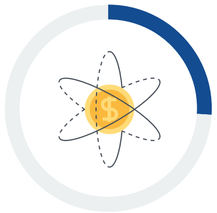
Threats that have likely penetrated communication and collaboration security controls in the past 12 months.

39%
Spam/malware filtering

34%
Phishing/spear phishing/ malicious link

27%
Misaddressed emails

27%
Ransomware/ extortion protection



26%
Wire transfer fraud, payroll fraud, payment fraud, and other BEC attacks

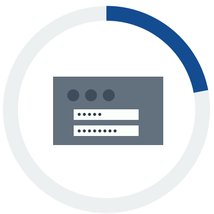
25%
Email domain spoofing/ impersonation

25%
Malicious third-party application integration

23%
Executive impersonation

23%
Internal email account compromise/account takeover

23%
Unintentional sensitive data leakage

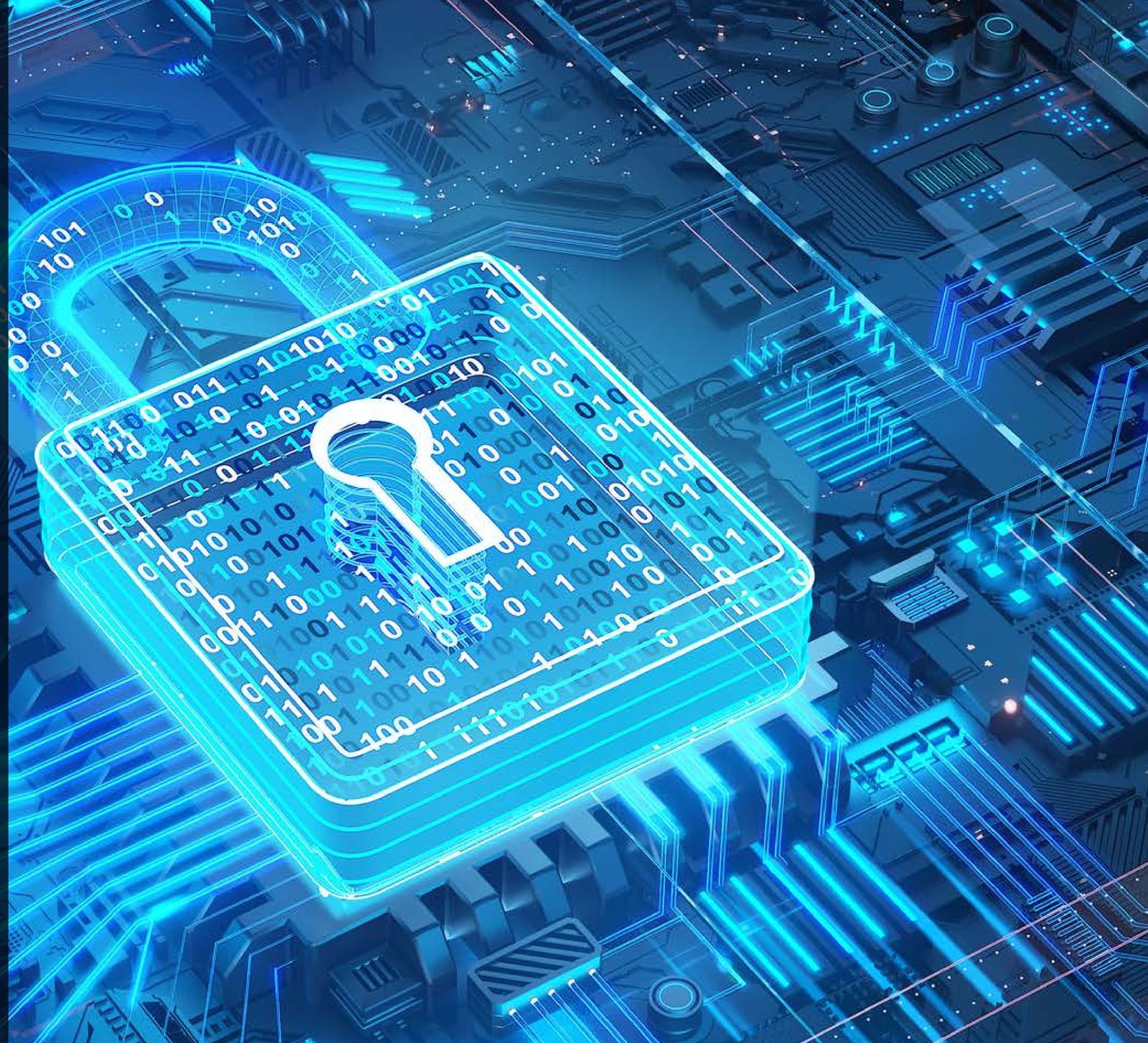


22%
Compromised vendor accounts

20%
Intentional data leakage

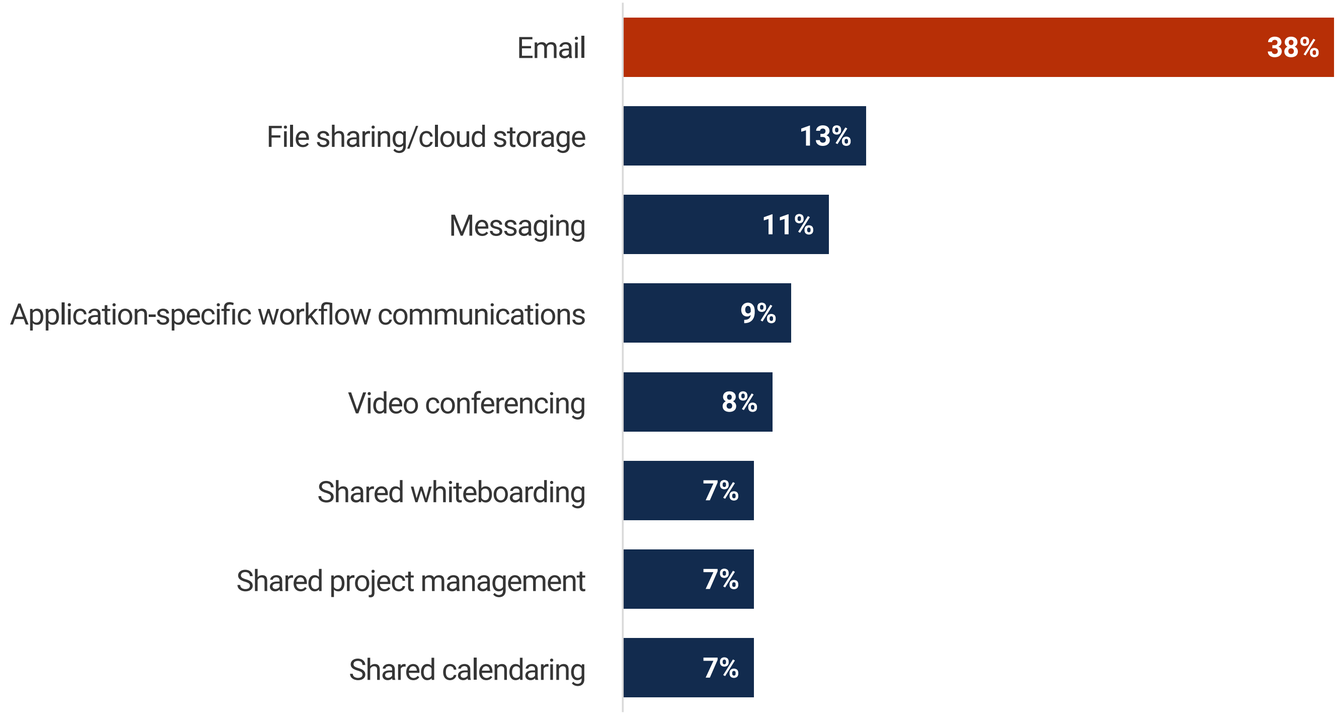
BACK TO CONTENTS

Weaknesses Endure Despite the Maturity of Email Security



“Email tops the list by a wide margin **as the channel considered *most vulnerable* to threat actors.”**

Communication and collaboration mechanisms considered *most vulnerable* to threats.



Email Is Considered Most Vulnerable to Threats

While most organizations are leveraging six or more tools for communication and collaboration, email tops the list by a wide margin as the channel considered *most vulnerable* to threat actors. ESG finds this interesting given the amount of dollars spent annually in the industry to secure the email channel. ESG believes that other channels are less understood and are less visible, obscuring the risk that they present. And while more have good things to say about their native email security controls when it comes to visibility, administration, and integration, there is room for improvement.

BACK TO CONTENTS

Gaps Persist for Many in Their Email Security Solution

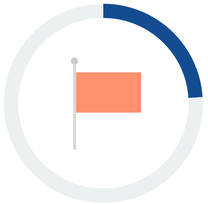
Digging into the challenges and gaps specific to email security, there is an expanded list beyond traditional security efficacy. Challenges with backup and recovery, regulatory compliance, and availability/reliability all center around operations more than security. This expands the lens of potential concerns for other communication and collaboration channels beyond security efficacy. As other tools are better understood, ESG expects IT and security leaders to also expand their perspective on the importance of similar capabilities.

Challenges experienced with current primary email security solution.

29%
Compliance issues

27%
Gaps in backup/recovery

24%
Inbound email attacks penetrating native security controls



24%
Incorrectly flagging too many messages as spam or suspicious

23%
Gaps in security awareness training and/or assessment

22%
Lack of add-ins on end-user client devices

22%
Automating response to user-reported phishing or other threats

21%
Data leakage getting through native email security controls

20%
Gaps in availability/reliability

20%
Gaps in security ecosystem integration

13%
Loss of configurability

BACK TO CONTENTS

Most Are Confident that Native Email Controls Will Improve, but Until Then, Third-party Controls Will Be Employed by Most to Mitigate Risk

Despite a lengthy list of concerns, most are confident (51%) or even completely confident (36%) that those challenges and shortcomings will eventually be addressed within the native security controls provided by their cloud email solution provider. Until then, more than a third (34%) report already implementing additional third-party security controls, with another 46% planning to do so in the next 12 months. A smaller percentage of organizations will look to managed service providers to fill the gaps.

Confidence level that email solution provider will *natively* address most or all security gaps.

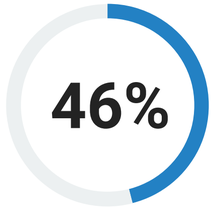
36%
Completely confident

51%
Mostly confident

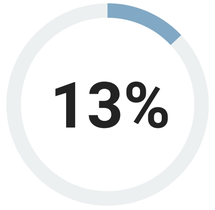
13%
Somewhat confident

Steps organizations will take until email provider fills native security control gaps.

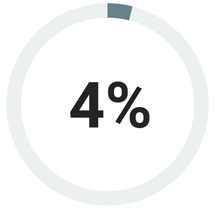
We have **already implemented** additional third-party controls



We **plan to implement** additional third-party controls in the next 12 months



We **plan to use a managed service** provider in the next 12 months to fill the gaps



We are **building our own** custom, internal solution

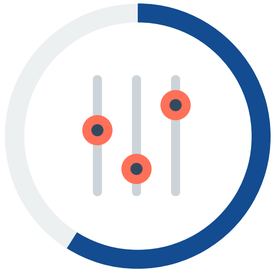
BACK TO CONTENTS

There Is Opportunity to Improve the Security of Sensitive Data within Communication and Collaboration Tools

Mitigating Sensitive Data Leakage from Communication and Collaboration Tools

When it comes to preventing the leakage of sensitive data, a combination of native controls and third-party controls are in use. More than half (59%) report leveraging native controls included in their email platform and/or deploying a purpose-built third-party solution to prevent sensitive data leakage. Surprisingly, more than half redact sensitive data from some number of these tools to prevent leakage. Outside of email, 52% depend on native controls to prevent leakage from other communication and collaboration tools.

Processes and/or technologies that prevent or protect sensitive data from being shared via email.



59%

Native controls included with our email solution

59%

A third-party email data leakage solution

54%

Sensitive data redaction

Policies and/or technologies that protect sensitive data in non-email collaboration tools.

56%

A third-party control for communication and collaboration tools

54%

Controls that redact sensitive data in communication and collaboration tools

52%

Native controls included within the communication and collaboration tools

BACK TO CONTENTS

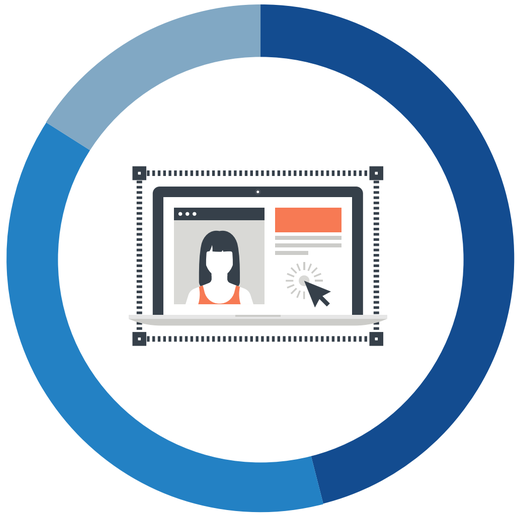
Sensitive Data Leakage Controls

Beyond these native automated controls, 60% have implemented mandatory and ongoing end-user training programs to inform employees about securing sensitive information policies, and 28% require this on a one-time basis. Furthermore, the majority of organizations leverage additional, specialized controls (46%) or alter the configuration of existing security tools (38%) for employees more likely to electronically communicate sensitive data.

Status of formal end-user security training programs.

- **60%** End-user security training programs are required on an ongoing basis (e.g., once per year, once per) quarter, etc.)
- **28%** End-user security training programs are required on a one-time basis
- **10%** End-user security training programs are not currently required, but we have plans to implement one in the next 12 months

Additional controls applied to employees likelier to be communicating sensitive data.



- **46%** We use additional, specialized controls for employees more likely to electronically communicate sensitive data
- **38%** We configure our existing security tools differently for employees more likely to electronically communicate sensitive data
- **14%** Everyone uses the same security regardless of role or likelihood of sending/receiving sensitive data

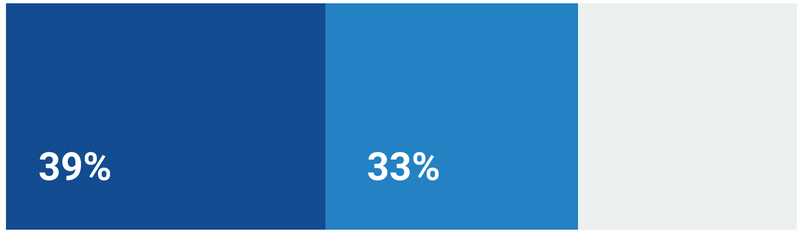
BACK TO CONTENTS

IT and Security Operating Models for Securing Communication and Collaboration Tools Are Still Evolving

Operating Models Are Still Evolving, Leaving the Door Open to Risk

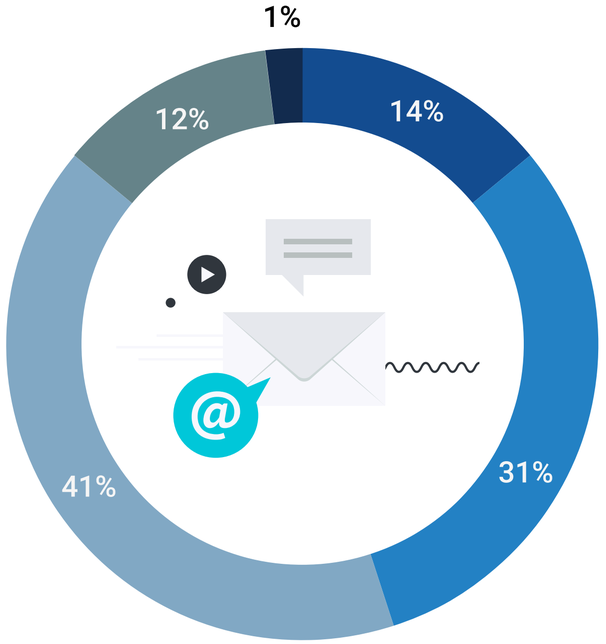
Securing communication and collaboration tools requires a team effort between IT and security teams. And while collaboration is happening, for many, silos still exist, leaving the door open for inconsistent controls and policy enforcement. For the plurality (41%) of organizations, IT teams are responsible for *all* aspects of communication and collaboration channels in use, with limited involvement of their security team. More work is needed in helping IT and security teams share visibility, policy, and management of this important threat vector.

Nature of relationship between IT and security to secure communication and collaboration channels.



- Highly collaborative
- Moderately collaborative

Staffing model used to manage the security of the communication and collaboration channels.



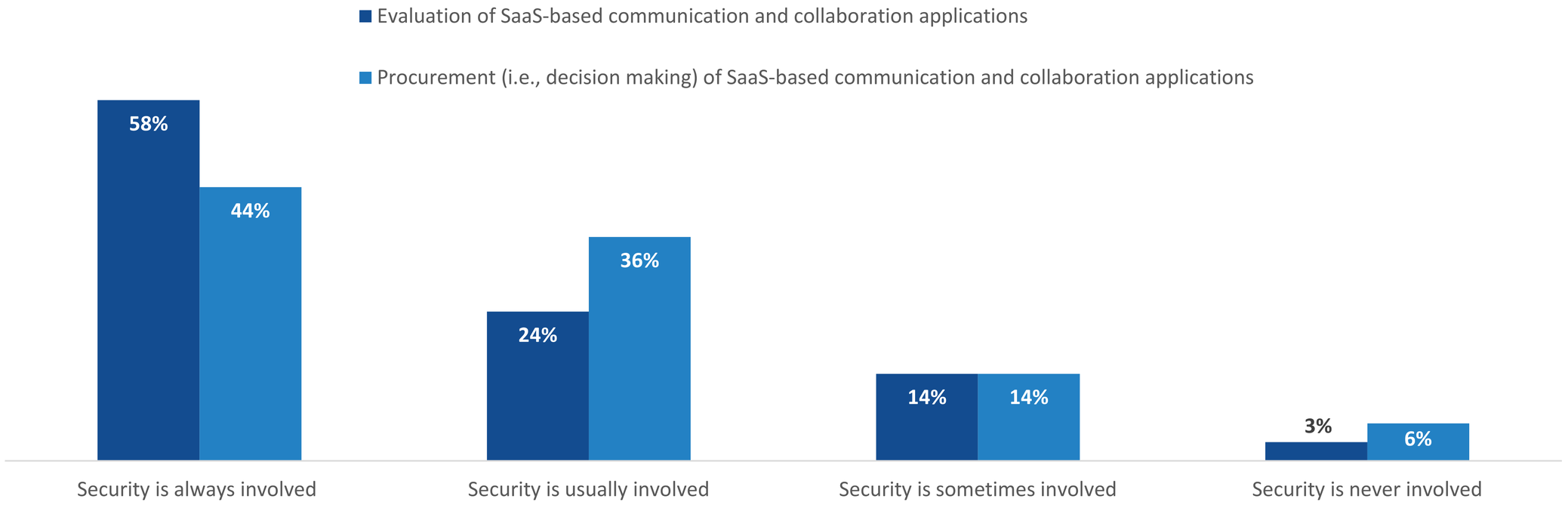
- Shared responsibility within our security operations team (i.e., no IT involvement)
- Specialized security personnel are assigned to managing the security of individual communication and collaboration channels
- IT team is responsible for all aspects of the communication and collaboration channels in use, with limited involvement of the security team
- We leverage a third-party service provider to manage the security of one or more of our tools, in addition to internal review or support
- We leverage a third-party service provider to manage the security of one or more of our tools, without internal review or support

BACK TO CONTENTS

What Role Does Security Play in SaaS-based Communication and Collaboration Tools Procurement?

When it comes to the evaluation and procurement of new communication and collaboration tools, IT and security teams often participate in different ways. While more than half (58%) report consistent security involvement in the evaluation process, only 44% say security is always involved in procurement.

Role security teams play in the evaluation and procurement of SaaS-based communication and collaboration applications supporting the business.



BACK TO CONTENTS

Abnormal

Abnormal Security provides the leading behavioral AI-based email security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails and messages in milliseconds—all while providing visibility into configuration drifts across your environment. You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly, with additional protection available for Slack, Teams, and Zoom.

LEARN MORE

ABOUT ENTERPRISE STRATEGY GROUP

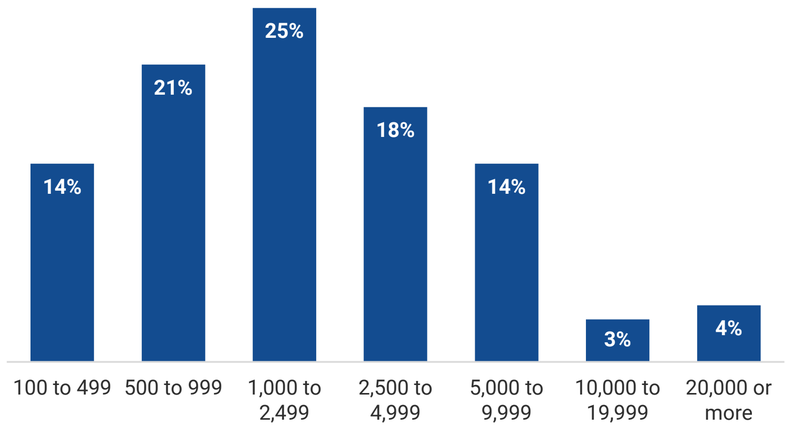
TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology and Demographics

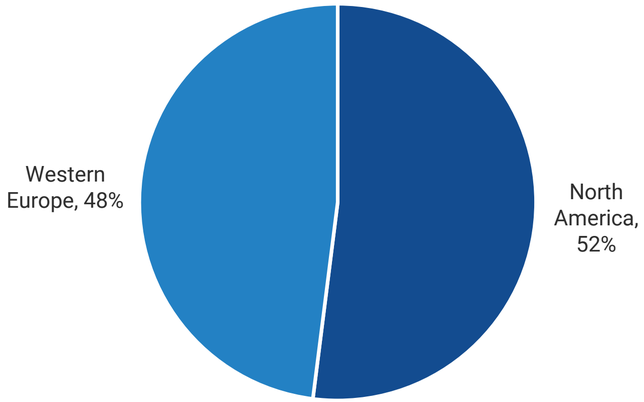
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America and Western Europe between February 14, 2023 and February 28, 2023. To qualify for this survey, respondents were required to be involved with securing their organization's enterprise communication and collaboration technology and processes. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 490 IT and cybersecurity professionals.

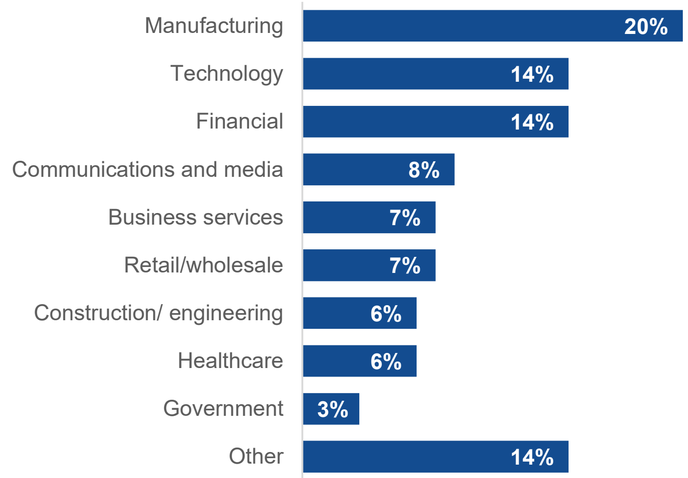
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY REGION



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.