WHITE PAPER

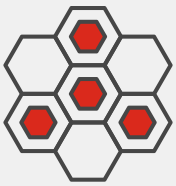
Securing the Modern Workspace

AI-Powered Browser, Collaboration, Data Loss Prevention, and Email Security

Executive Summary

Productivity increasingly relies on the interaction of users and sensitive data. At the same time, more sophisticated AI-enhanced threats target users directly through channels including email, web browsing activity, collaboration tools, and other SaaS applications. As a result, organizations need to move urgently to securing workspaces across their user and employee bases.

Workplace security should emphasize areas of employee engagement that are commonly targeted by threat actors and focus on critical areas where egress of sensitive data could occur.



Threat actors leverage AI for phishing, impersonation, extortion,and evasion tactics. Tools like FraudGPT, BlackmailerV3, and ElevenLabs are automating malware generation, deepfake videos, phishing websites, and synthetic voices, fueling more scalable, believable, and effective campaigns.[1]

How Users Engage with Data

Users and sensitive data are intrinsically linked. For example, human resources managers may access employee personally identifiable information (PII), finance employees use customer data to compile reports, and software developers can access sensitive source code. Users across the company have access to sensitive data, so security teams must simultaneously address user risks and risks to sensitive data from both outsider and insider perspectives.

Organizations are increasingly concerned about data breaches and disclosures, and 55% of incidents are caused by user or employee negligence[2]. These incidents result in an average $8.8 million to remediate annually, and the total cost rises to $17.4 million when accounting for all insider-related security incidents.[3]

Protecting users and data can be difficult. The term *workspace security* refers to all the security infrastructure or technologies, processes, and people involved in securing users from a user-centric viewpoint. Achieving comprehensive workspace security involves a large-scale commitment that can prove daunting for many organizations.

The Increase in AI-Based Threats

Today, cybercriminals use generative pre-trained transformers (GPTs) and other AI tools, changing the caliber of the threats directed at users. These threats may be email-based, such as phishing and impersonation, or web-based threats, such as malicious URLs and drive-by-downloads secretly deployed to a popular website that employees often access. Threats also can be collaboration-based, such as malware embedded in shared files.

Because user productivity increasingly requires employees and users to access sensitive information to do their jobs, securing users and data more effectively is vital. Organizations need to protect against risks from outside attackers but also against insider risks and threats, whether it's a bad actor with legitimate login credentials, a soon-to-be-departing employee seeking to take sensitive data, or an uninformed employee who doesn't appreciate the critical importance of properly handling sensitive data.

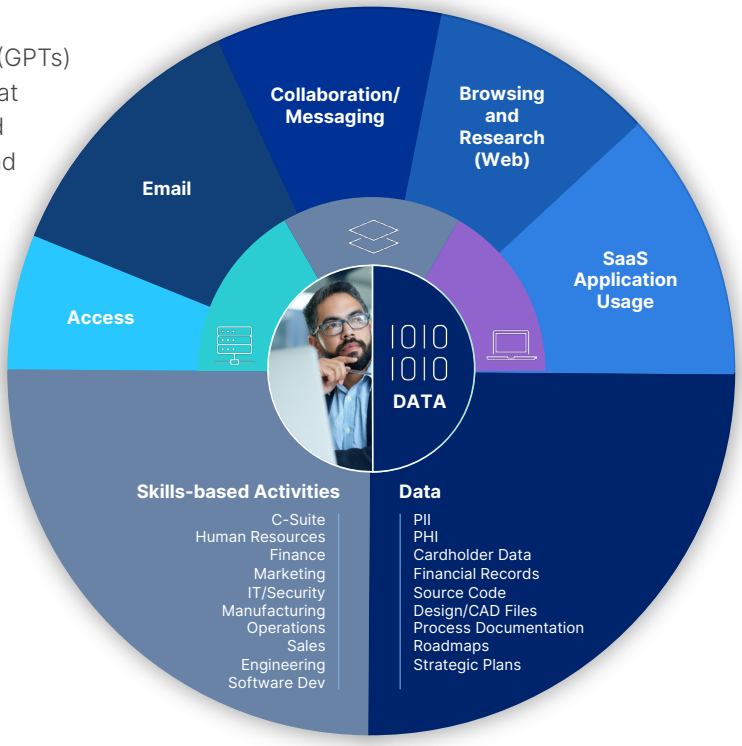


Figure 1: The links between users and data

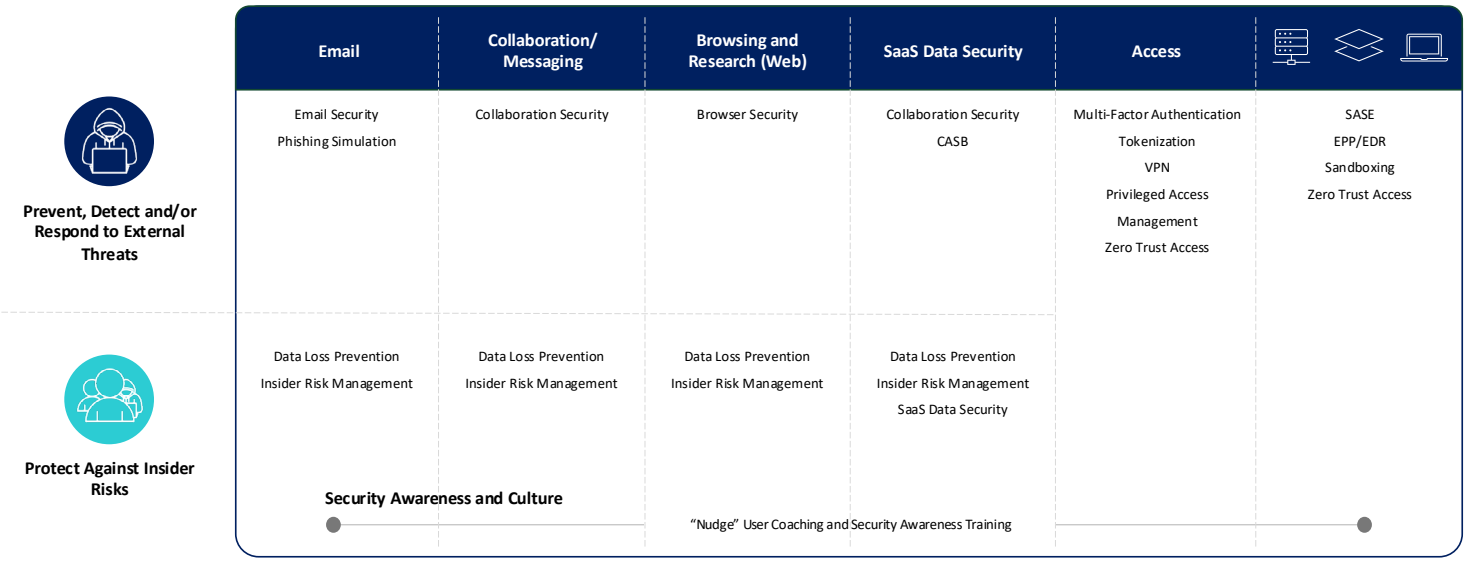


Figure 2: Common technologies included in workspace security frameworks

A Simple Strategy for Workspace Security

At Fortinet, we have developed a strategy for protecting users and data. Organizations can apply a simple approach to workspace security that goes from A to E.

- **A =** AI-powered
- **B =** Browser security
- **C =** Collaboration security
- **D =** Data loss prevention
- **E =** Email security

Our A to E approach emphasizes the most common areas where employees are engaged throughout their day. It also includes areas commonly targeted by threat actors and critical places where egress of sensitive data could occur. Many organizations are likely to have two or more security solutions at work, which can be incorporated as part of a more intentional workspace security strategy.

A = AI-powered

Organizations should capitalize on security innovations that include AI because AI technologies are finally delivering real, measurable value when incorporated into the security infrastructure. For instance, machine learning (ML) is used to more effectively detect and prevent emerging threats across a large volume of telemetry data. It also can be used for baselining and analysis of user behavior, or to facilitate threat hunting of previously unknown compromises. Generative AI (GenAI) and large language models (LLMs) may be applied to provide actionable insights to an analyst for an optimal network and security configuration, synthesize and summarize events related to an incident, and provide guidance on the appropriate steps to take to resolve an incident. With the advent of agentic AI, security teams can automate workflows to analyze logs, events, detections, incidents, or other information to flag anomalies and areas of potential risk and apply policy actions based on findings.

As part of your workspace security strategy, be sure to ask how AI is specifically being applied in your security solutions and how it benefits your overall security operations and the broader organization.

B = Browser security

Throughout the day, employees are online performing research, accessing applications, or catching up on industry news. Unfortunately, these activities are not without risk. With 44% of all breaches involving ransomware, protecting against drive-by downloads where ransomware could be present is critical.[4] But it's not just ransomware. To keep the workplace secure, organizations also need to protect against phishing, malicious browser plugins, session hijacking, and man-in-the-middle or man-in-the-browser attacks.

Organizations should deploy advanced browser security capabilities that protect users and organizations against these types of attacks. An effective solution can protect the browsers in use at your organization and Software-as-a-Service (SaaS) applications against external web threats, data breaches, and employee-related risks.

When considering browser security for your organization, be sure to determine how the security is deployed, the protection it provides, and the overall footprint and impact of the solution on the user experience.

C = Collaboration security

As the exchange of files and URLs moves to new channels, so does the potential for malicious content. In today's user workspaces, cloud collaboration, messaging, storage, and a multitude of SaaS apps are integral to daily operations. The adoption of tools such as Slack, Microsoft 365, and Salesforce has transformed these SaaS platforms into potential hotspots for advanced cyberattacks. Phishing links, sophis ticated malware, and zero-day exploits are increasingly being delivered through cloud-based collaboration tools, posing significant risks to end-users and the organization.

Collaboration security solutions protect users and organizations against a range of threats posed by collaboration and SaaS applications. A solid collaboration security solution provides a holistic approach to threat prevention. It can also enable security policy extension from the email domain to other communication channels, significantly enhancing the line of defense against sophisticated attackers securing enterprise collaboration workspace customer relationship management (CRM) applications, enterprise social networks, and shared virtual workspaces.

When considering adding collaboration security to further secure the workspace, make sure you understand the solution's threat prevention capabilities, evaluate how the solution is deployed, and any impact there may be on performance.

D = Data loss prevention

Data loss prevention (DLP) keeps sensitive data from leaving the organization through deliberate exfiltration or accidental or careless disclosure. In the context of workspace security, DLP performs a critically important role, protecting both users and sensitive data from risks.

Most organizations today employ some type of DLP solution, but they often have a number of challenges. They typically aren't suited for complex environments and require exhaustive data discovery and classification as a prerequisite. They also need policies to be formulated before providing visibility into data flows and usage. Next-generation DLP solutions have emerged to address these challenges by providing cloud-native endpoint-based DLP combined with insider risk management.

Next-gen DLP solutions can provide immediate visibility across all points of egress and SaaS applications, both sanctioned and unsanctioned. They also make it easier to understand business data flows, so administrators and analysts can construct policies based on actual behaviors. By integrating DLP and insider risk management solutions, organizations can gain broad and deep visibility into data usage and risks and ultimately discover how data may have been put at risk within an organization, who was involved, and why. Next-gen solutions can also incorporate user coaching with information about proper data handling at the point of access and the use of sensitive data.

If your organization relies on a traditional DLP solution, you should consider the additional benefits of advanced next-gen DLP and insider risk management solutions.

E = Email security

Most organizations already have an email security solution in place. But, you may be concerned about your solution's overall suitability and efficacy when securing users against sophisticated email-based threats. If so, consider the following:

- If your organization has a hybrid email environment (due to acquisition, disparate and separate business operations, or other reasons), you may now utilize multiple email services and security solutions. Consider how your organization can streamline its email services and consolidate security solutions. Engage a consultant or email security vendor to understand how your organization can benefit from a streamlined architectural approach to email services and related security controls.
- If you are using Microsoft 365 E3 or E5 licenses or Gmail Advanced Protection Program licensing and are concerned that malicious emails are still getting through or your organization has a heightened state of security, consider implementing a layered email security approach. Using integrated cloud email security (ICES) solutions can heighten efficacy against the most sophisticated threats. Hosted, API-based solutions can also provide additional protection for Microsoft Outlook and Google Mail.

- If you have concerns regarding the overall efficacy of your solution, consider engaging another email security vendor and conducting a proof-of-concept. If you are currently under contract for email security services, allow at least three months before your term expires to give your team plenty of time to research options, engage vendors, and evaluate and implement a new solution.
- Ask specific questions about how a new solution addresses the threats that matter most to your organization. Also, ask whether their email security solution integrates with other workspace security capabilities such as browser security and collaboration security.

Workspace Security from A to E

Securing modern digital workspaces can be a challenge. The breadth of areas that pose risk to an organization and the set of technologies to address them can be difficult for security teams to evaluate and implement. A simple staged approach to workspace security focuses on an A to E strategy: AI-powered, browser, collaboration, data loss prevention, and email security.

Types of browser-based threats:

- Phishing
- Malware, including ransomware
- Threats using evasive tactics
- Cross-site scripting (XSS)
- Malicious browser plugins
- Broken authentication and session hijacking
- Distributed denial-of-service (DDoS) attacks
- SQL injection
- Drive-by downloads
- Man-in-the-middle/man-in-the-browser attacks
- DNS poisoning attacks

1. Fortinet, Global Threat Landscape Report, May 1, 2025.
2. Ponemon Institute, Cost of Insider Risks Global Report, 2025.
3. Ibid.
4. Verizon, Data Breach Investigations Report, 2025.

July 11, 2025 10:32 AM / MKTG-1554-0-0-EN