Trellix

EXECUTIVE BRIEF

Trellix Collaboration Security

Evolve beyond email-only to complete enterprise collaboration security

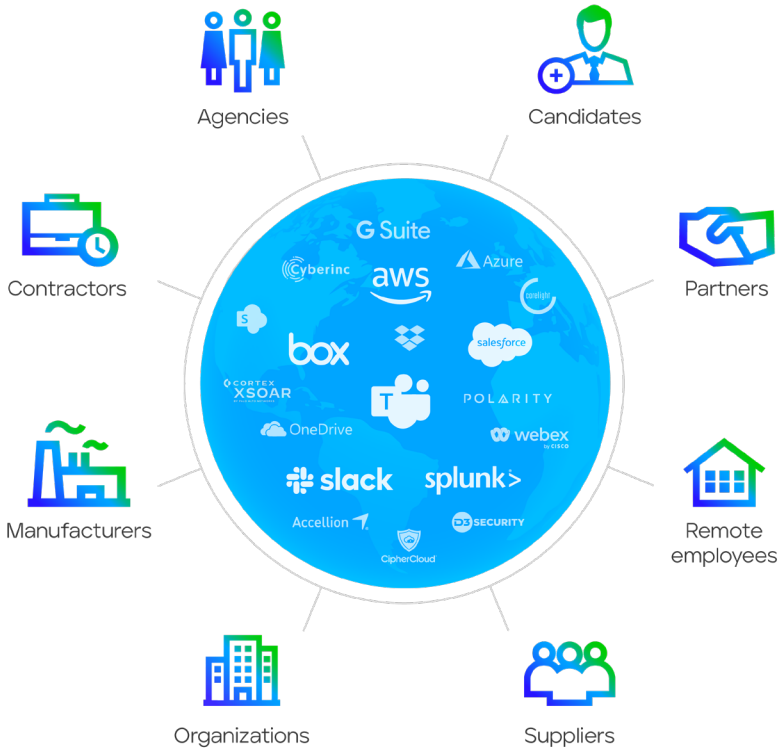
Collaboration: The least-protected attack vector

As organizations strive to innovate and grow, they create highly complex, interconnected global networks of external partners: suppliers, vendors, contractors, and customers.

Remote work, virtual teaming, and cloud-based collaboration platforms such as Slack, Box, Microsoft Teams, and Google Workspace have transformed both the nature and velocity of collaboration, encouraging us to freely share information with coworkers and external stakeholders.

Digital transformation initiatives further extend enterprise relationships, opening applications that were once securely within the perimeter to a growing number of external stakeholders. In fact, a 1,000-person company may share data with up to 15,000 external partners.[1]

But any new freedom will be compromised if not guarded, and threat actors are already exploiting this largely unprotected attack vector.



1. Quantifying the Risk of Unmanaged SaaS Data Access, DoControl, August 2021

New attack vectors, new challenges

Today's extended enterprise presents a range of new challenges for security leaders.

Third-party

59% of surveyed organizations have experienced a data breach caused by a third-party vendor or contractor[3]

Email

83% of organizations surveyed indicated they had experienced phishing attacks[4]

Collaboration

20% of an organization's SaaS files are shared internally to anyone with a link[5]

Digital transformation

82% of surveyed organizations reported a breach as a result of digital transformation[6]

Third-party risks

Security leaders are hard pressed to maintain ongoing visibility into who has access to sensitive data and systems across the extended enterprise. In a 2021 Ponemon Institute study, 65% of organizations surveyed had not identified the third parties that have access to their most sensitive data.[2]

Email infrastructure detection gaps

Many email security solutions today use antispam filters and antivirus software that don't respond fast enough and leave organizations open to threats like dynamic malwareless techniques. To keep up, organizations end up adopting multiple solutions, creating an overly complex security environment.

Collaboration threats

Collaboration platforms are essential to the day-to-day operations of most enterprises. While these systems allow us all to freely share information, they do not ensure the integrity of what is shared. Today, collaboration and file-sharing tools are attack vectors that are being actively exploited.

Increased access, increased risk

Digital transformation initiatives have led to suppliers, vendors, contractors, and customers being granted access to enterprise applications like ERP, CRM, HR, and procurement systems. But these enterprise applications don't inspect files on ingest to block threats before they enter the environment.

2. A Crisis in Third-Party Remote Access Security, Ponemon Institute, July 2021
3. Data Risk in the Third-Party Ecosystem, Ponemon Institute, October 2022
4. 2023 State of the Phish, Proofpoint, March 2023
5. Data Risk in the Third-Party Ecosystem, Ponemon Institute, October 2022
6. Digital Transformation is Increasing Cyber Risk, Ponemon Institute, June 2020

Go beyond email security

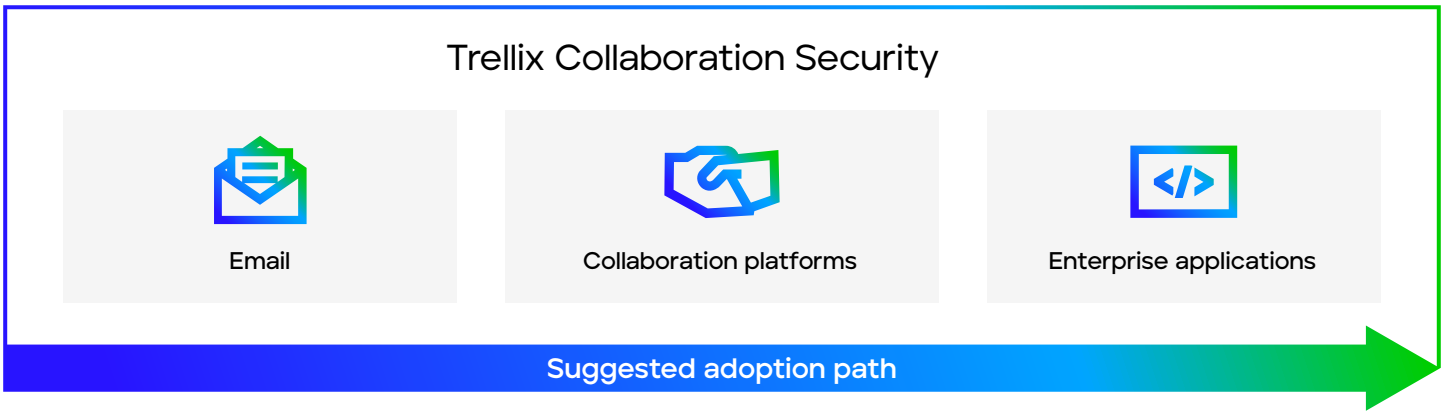
Modern enterprises must think beyond simply securing their email and consider the full spectrum of infrastructure that supports internal and external stakeholder collaboration.

> Phishing and BEC attacks are no longer limited to email. Communication and collaboration applications like Teams and Slack are growing as attack vectors. … To protect the future of business communication comprehensively, enterprise email security vendors must become enterprise communication and collaboration security vendors or risk obsolescence."
>
> —The Enterprise Email Security Landscape, Q1 2023, Forrester, February 2023

Trellix has long viewed digital collaboration as a critical attack vector with three main fronts to defend. That's why Trellix Collaboration Security offers a suite of protection technologies spanning email, collaboration tools, and SaaS applications used across the extended enterprise.

3 steps to collaboration security

Most enterprises will take a step-by-step approach to collaboration security. Trellix recommends the following path:



1. **Optimize email security.** Audit and improve your email security immediately. Existing tools have fallen behind attackers' techniques and miss emerging, multistage attacks. Some enterprises may choose to leave the current solution in place and add an additional hop to deploy newer technologies.
2. **Protect collaboration platforms.** Implement threat detection in collaboration and file-sharing tools to ensure you and your partners don't accidentally share malware. Use the same core detection, analysis, and blocking tools used by your email security to leverage a larger dataset of known threats.
3. **Extend security across all applications.** Protect your apps, built or bought, ensuring the continuous inspection of objects on intake. Inspecting incoming content and URLs helps you block threats before they enter your environment.

Mapping out your journey

First things first

Optimize email security

Modern extended enterprises need email security solutions that are:

Effective

Catch advanced threats that email infrastructure solutions miss.

- Detect and defend against multistage campaigns
- Activate multiple layers of detection, powered by innovative AI, ML, and security analytics
- Gain real-time detection and prevention against credential harvesting, impersonation, and spear-phishing attacks

Integrated

Integrate with your existing security operations workflows.

- Empower SOC analysts to claw back emails that are weaponized post-delivery
- Provide alerts with rich metadata to enable analysts to quickly identify the source of compromise
- Use newly identified IOCs to search previously received emails and perform retrospective analysis

Flexible

Deploy with secure email gateway (SEG) or integrated cloud email security (ICES) solution.

- Integrate via API with Microsoft 365 and Google Workspace
- Deploy in-line or in bcc/monitor mode
- Gain high availability (99.995% or better)
- Benefit from active-active AWS cloud deployment

Mapping out your journey

A step forward

Protect collaboration platforms

Best-in-class collaboration and file-sharing security solutions are:

Comprehensive

Leverage a single detection solution across your tools.

- Reduce cost and increase detection efficacy using a consistent, proven detection solution across collaboration platforms such as Slack, Microsoft 365, and Google Workspace
- Ensure quick time to value with robust APIs that enable continuous inspection and require no infrastructure changes
- Enhance overall effectiveness and streamline security tooling with the same proven detection and analysis engines trusted by our 40,000 enterprise customers

Frictionless

Ensure confident, secure collaboration with minimal end user impact.

- Provide seamless integration with existing platforms so users aren't slowed down
- Inspect shared files and URLs continuously and unobtrusively, with verdicts in seconds
- Notify users only when a malicious object has been inadvertently shared

Easy

Integrate out of the box with minimal configuration, without creating more work for your SOC and Enterprise Applications teams.

- Minimize the impact on SOC analysts with high-fidelity alerts
- Support a broad range of response actions, including quarantine, block, and notify
- Inform SOC investigation and response with detailed logging of threat actor activities

Mapping out your journey

Advanced-level protection

Extend security across all applications

Securing apps across the extended enterprise requires a solution that is:

Unified

Leverage a single solution across all enterprise applications.

- Reduce cost using a consistent, proven detection solution across a broad range of enterprise applications, built or bought
- Secure digital collaboration across the extended enterprise by inspecting objects shared by popular applications such as Salesforce, Ariba, Microsoft Azure, and Workday
- Ensure quick time to value with robust APIs that enable continuous inspection and require no infrastructure changes

Transparent

Provide a pain-free experience to your application end users.

- Inspect and verify files shared by enterprise applications without end user involvement
- Inspect shared files and URLs continuously, using the same intelligence-driven detection engines protecting Trellix enterprise security customers worldwide

Effective

Increase protection with minimal impact on SOC workloads.

- Gain consistent protection across all enterprise applications with simplified integration into existing SOC workflows
- Stop threats on entry with high-fidelity, low false-positive verdicts
- Gain alerts enriched with contextual insights to accelerate investigation and response

EXECUTIVE BRIEF

Trellix Email Security

Securing collaboration across the extended enterprise

Trellix Collaboration Security provides a single solution to secure email infrastructure, collaboration platforms, and SaaS applications, ensuring people can work together securely across the extended enterprise.

Ready to get started? Sign up now for a free demo—and see what our Trellix Email Security solution looks like in action.

Trellix
6000 Headquarters Drive
Plano, TX 75024
www.trellix.com

Trellix

About Trellix
Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at trellix.com.