



TRELLIX COLLABORATION SECURITY

Evolving beyond
email-only cybersecurity

Trellix

Collaboration: The least-protected attack vector

In today's fast-paced business world, innovation and growth are paramount.

To sustain growth and fuel innovation, organizations have created vast and intricate networks of external partners, including suppliers, vendors, contractors, and customers. These networks often span the globe and are highly interconnected—which makes collaboration essential.

To further fuel growth, many organizations have embarked on digital transformation initiatives. This has opened up previously secure applications to an ever-growing number of external stakeholders, with some 1,000-person companies sharing data with up to 15,000 external partners.¹

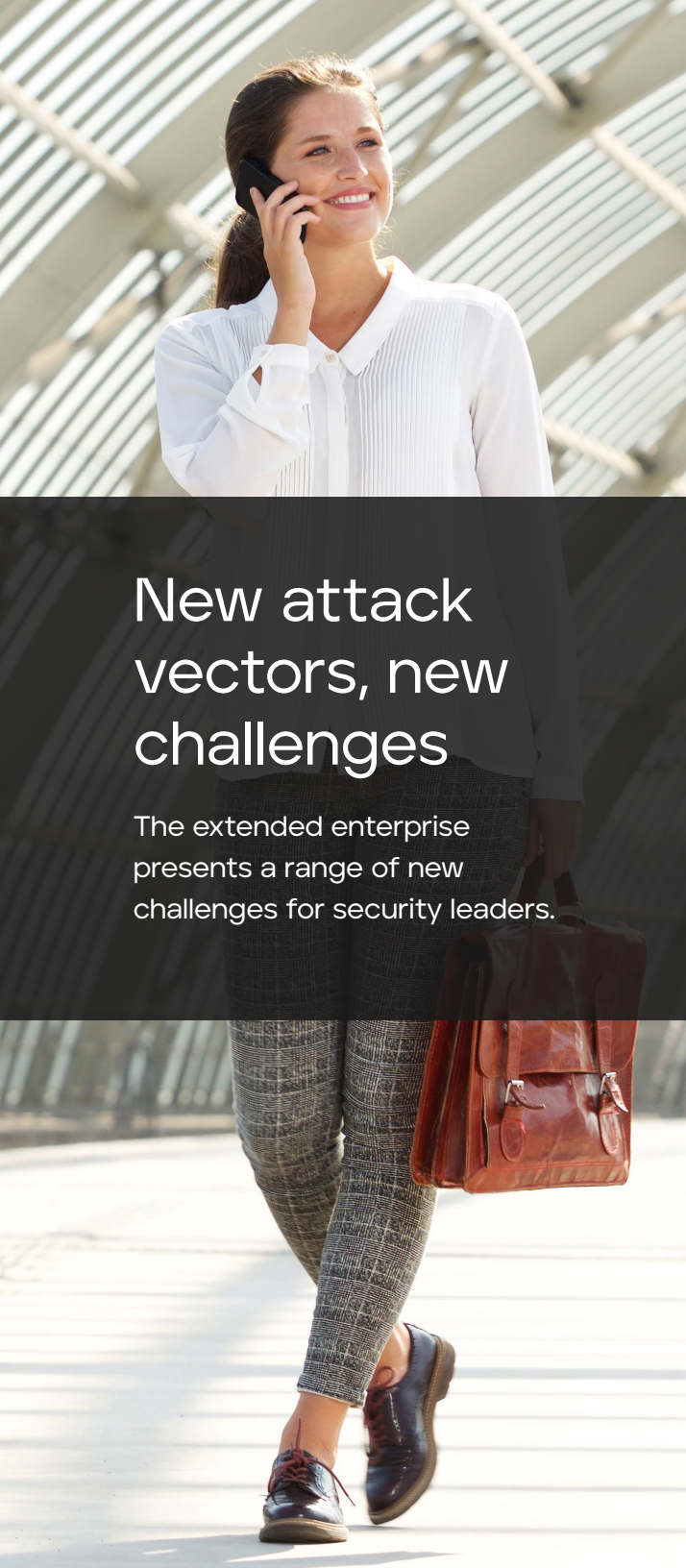
The advent of remote work, virtual teaming, and cloud-based collaboration platforms has revolutionized the way we work. Tools like Slack, Box, Microsoft Teams, and Google Workspace have made it easier than ever to share information freely with coworkers and external stakeholders, enabling collaboration to move at lightning speed.

But new freedom and new tools bring new risk.

The largely unprotected collaboration attack vector is already being exploited by threat actors, putting organizations at risk of data breaches.



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



New attack vectors, new challenges

The extended enterprise presents a range of new challenges for security leaders.

Managing third-party risk

When it comes to managing third-party risk, many organizations rely on paper-based processes to assess the security posture of their partners in order to ensure the protection of sensitive data.

But here's the problem: these processes are often subjective and rely on the supplier to provide an accurate assessment of their own risk exposure.

What's more, these processes rely on ongoing assessment and transparency between partner organizations.

According to research conducted by the Ponemon Institute and Mastercard's RiskRecon in 2022, only 34% of organizations are confident that their suppliers would notify them of a breach of their sensitive information.²

This lack of trust is perhaps why 44% of executives surveyed admitted that their growing use of partners and suppliers exposes them to significant security risks.³

2. The 2022 Data Risk in the Third-Party Ecosystem Study, Ponemon Institute, October 2022

3. Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know, Forbes, June 2022

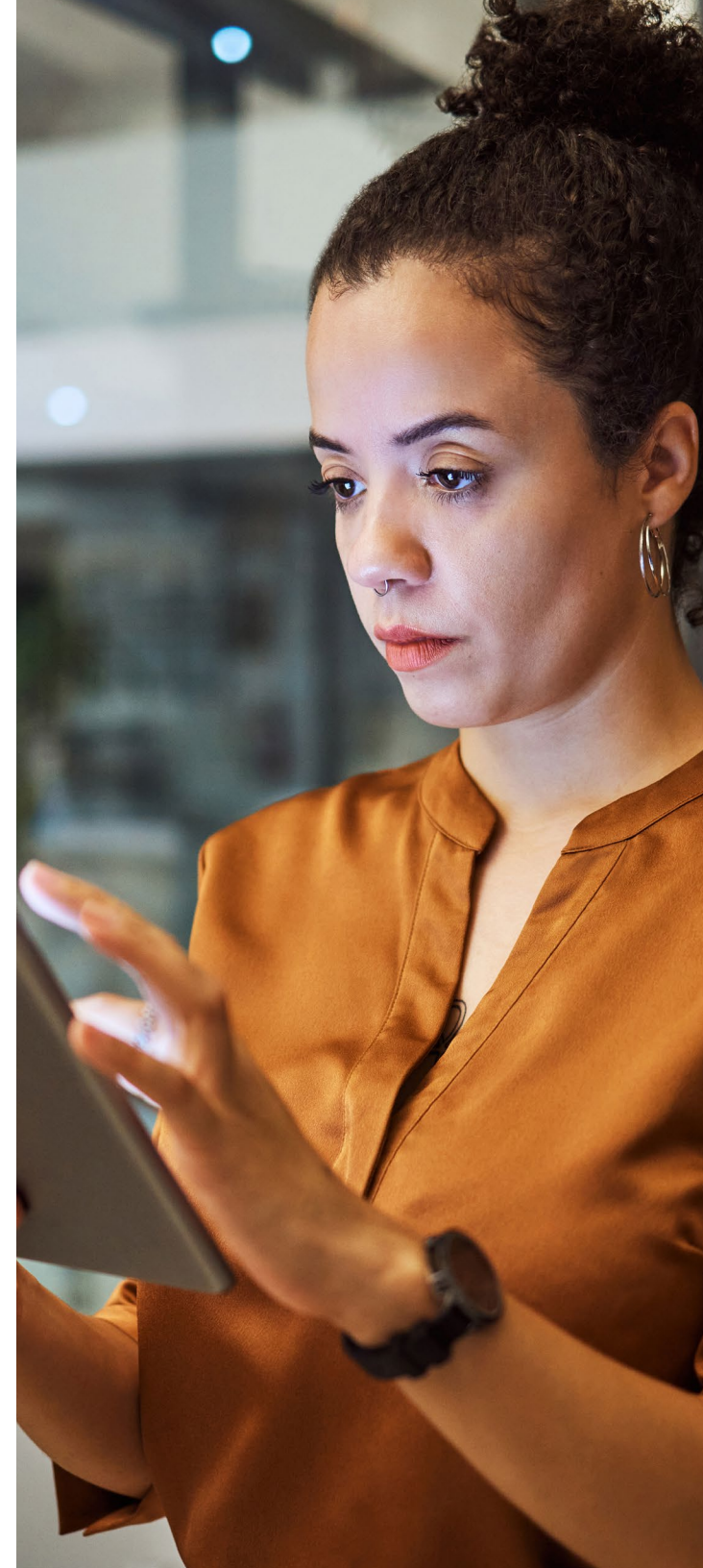
Lack of third-party visibility

But even with rigorous third-party risk management programs in place, it's crucial to know exactly who you're doing business with. This is no small feat given the dynamic nature of the partner ecosystem. Security leaders are hard-pressed to maintain ongoing visibility into who has access to sensitive data and systems across the extended enterprise.

Despite companies' best efforts, a 2021 study by the Ponemon Institute revealed that 65% of organizations surveyed had not identified the third parties that have access to their most sensitive data.

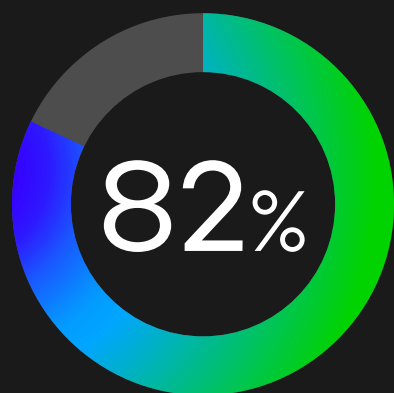
Even more concerning, 54% of organizations surveyed did not have a complete list of all the third parties who have access to their network.⁴

4. A Crisis in Third-Party Remote Access Security, Ponemon Institute, July 2021



Real CEO email or BEC attack?

In the [February 2023 Threat Report](#), the Trellix Advanced Research Center reported a significant surge in malicious emails impersonating CEOs and other business leaders. In this BEC tactic, employees receive a fake email from an executive asking them to confirm their direct phone number, so attackers can execute a voice phishing—or vishing—scheme.



of all CEO fraud emails were sent using free email services⁶

Email infrastructure detection gaps

The advent of email transformed business communication, enabling people to exchange information 24/7, regardless of location. But fast forward to today, and email has become the top attack vector, with a staggering 83% of organizations surveyed in the 2022 State of the Phish report indicating they have experienced phishing attacks.⁵

The widespread use of email and the ease with which threat actors can create and evolve phishing attacks make business email compromise an inexpensive and highly effective attack technique.

Cybercriminals can easily trick users into clicking malicious URLs or opening compromised attachments through targeted social engineering. They can even make well-intentioned employees believe that an urgent financial transfer request is coming from the CEO.

In the face of these increasingly sophisticated threats, the rudimentary security capabilities offered by many email infrastructure providers are not up to the task. Antispam filters and antivirus software simply don't respond fast enough and can't accurately detect threats the first time they're seen. This leaves organizations vulnerable to dynamic malwareless techniques and other advanced attacks.

To keep up, organizations often end up adopting multiple solutions, creating an overly complex security environment that results in an overwhelming uptick in alert volume.

5. 2022 State of the Phish, Proofpoint, January 2022

6. The Threat Report, Trellix Advanced Research Center, February 2023

Collaboration threats

Collaboration platforms like Microsoft Teams, Slack, and Google Workspace are essential to the day-to-day operations of most enterprises. They allow teams to work together and share information seamlessly, but they do a poor job of ensuring the integrity of what is shared. Today, attackers are increasingly targeting collaboration and file-sharing tools to gain access to sensitive data and systems.

One notable example was the 2020 Microsoft Teams hack, where attackers compromised employee accounts by tricking them into downloading a malicious file. The file was disguised as a legitimate Excel document, but it led users to a fake login page where attackers could steal their credentials.

Google Drive users also fell victim to a social engineering scam in late 2020. Attackers created a document with malicious links and tagged victims, asking for feedback. When flattered victims clicked on links to a phishing site and entered their login credentials, the attackers gained access to their accounts and sensitive information.

Similarly, in 2019, attackers were able to gain access to the GitHub repositories of several companies by using a malicious file that was shared on the platform. The file contained code that allowed the attackers to gain control of the affected systems and steal data.

All these incidents highlight the need for security leaders to intercept and inspect potentially malicious files shared via collaboration platforms.



THIRD-PARTY

59%

of surveyed organizations have experienced a data breach caused by a third-party vendor or contractor⁷

EMAIL

83%

of organizations surveyed indicated they had experienced phishing attacks⁸

DIGITAL TRANSFORMATION

82%

of surveyed organizations reported a breach as a result of digital transformation⁹

Increased access, increased risk

In the era of digital transformation, businesses have expanded their reach by granting application access to their suppliers, vendors, contractors, and customers. But with improved reach comes additional risk—enterprise applications like ERP, CRM, HR, and procurement systems don't inspect files on intake, leaving larger organizations particularly vulnerable to attacks.

These vulnerabilities are often exploited by threat actors who take advantage of file-sharing mechanisms to introduce malicious files.

Just as job seekers submit resumes through employment portals and users attach files to customer support requests, adversaries use the same means to infiltrate enterprise systems.

Application shared-responsibility models pose a major challenge, and both enterprises and application vendors often lack the necessary monitoring tools to identify and prevent attacks.

Security leaders must address this emerging attack vector by continuously inspecting objects on intake to block threats before they enter the enterprise environment.

7. The 2022 Data Risk in the Third-Party Ecosystem Study, Ponemon Institute, October 2022

8. 2022 State of the Phish, Proofpoint, January 2022

9. Digital Transformation is Increasing Cyber Risk, Ponemon Institute, June 2020

Email security alone won't work

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

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



// 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

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.



Optimize email security



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

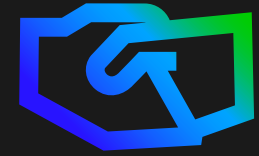
Integrate with your existing security operations workflows.

- 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 as a 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



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 email and 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



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

TRELLIX COLLABORATION SECURITY

Living security for today's dynamic threats

Trellix offers multiple detection techniques. Powered by innovative machine learning, artificial intelligence, and security analytics, they provide unparalleled defense against multistage campaigns, including:

Phishing. Multiple advanced URL defense techniques identify malicious URLs, protecting your organization from credential harvesting and spear-phishing attacks.

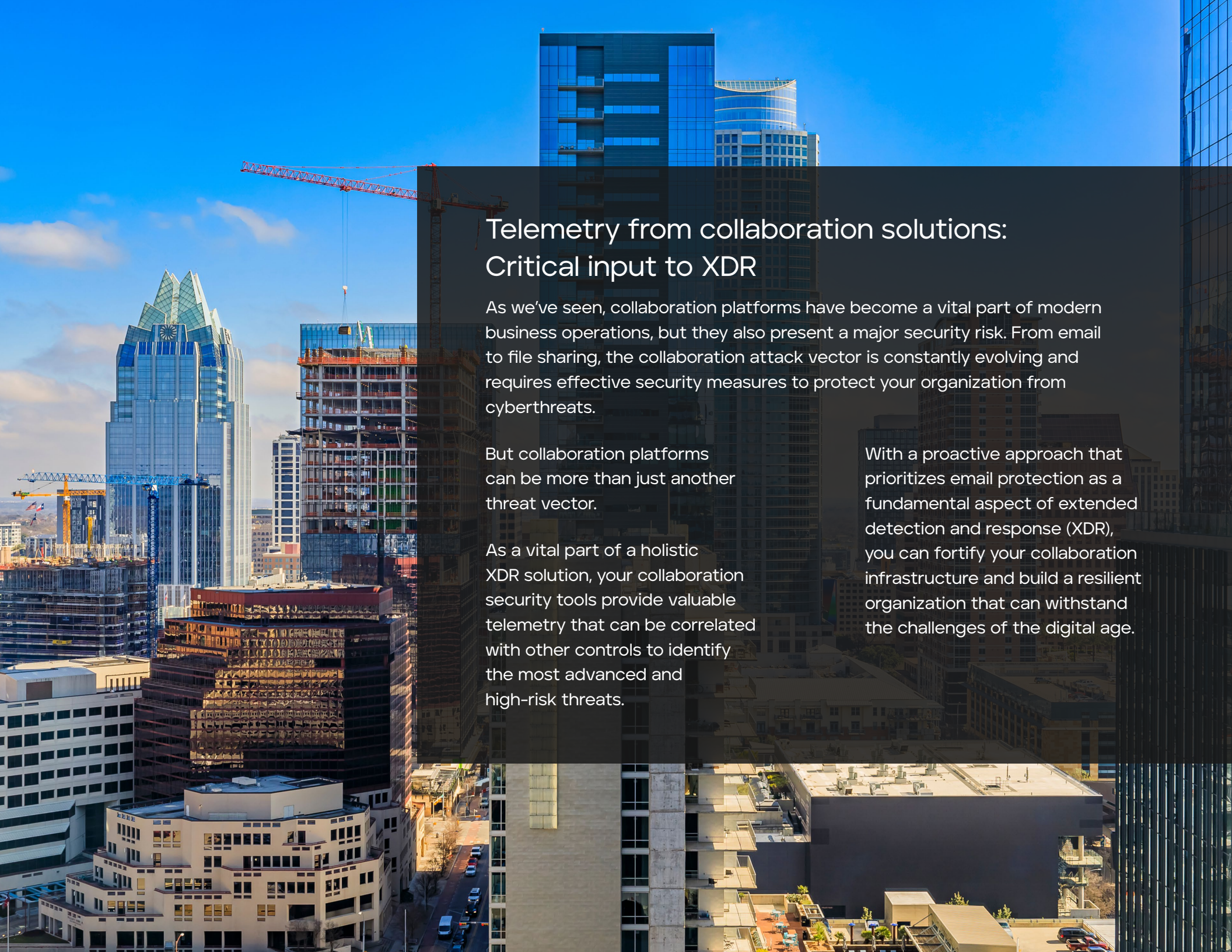
Deferred phishing. Emails containing URLs weaponized post-delivery are automatically extracted.

Impersonation and spoofing. Emails with newly observed domains or fraudulent sender information are flagged for further inspection.

Malware. Signatureless, dynamic, intelligence-driven analysis provides real-time inspection of suspicious attachments and URLs.

Black-listed URLs. Block specific traffic from an extensive, evolving list of black-listed URLs by quickly identifying objects with malware payloads and known-bad commands.





Telemetry from collaboration solutions: Critical input to XDR

As we've seen, collaboration platforms have become a vital part of modern business operations, but they also present a major security risk. From email to file sharing, the collaboration attack vector is constantly evolving and requires effective security measures to protect your organization from cyberthreats.

But collaboration platforms can be more than just another threat vector.

As a vital part of a holistic XDR solution, your collaboration security tools provide valuable telemetry that can be correlated with other controls to identify the most advanced and high-risk threats.

With a proactive approach that prioritizes email protection as a fundamental aspect of extended detection and response (XDR), you can fortify your collaboration infrastructure and build a resilient organization that can withstand the challenges of the digital age.



[Trellix Email Security](#)

Take the next step toward secure email and collaboration

Ready to get started? [Sign up now](#) for a free demo—and see what our Trellix Collaboration Security solution looks like in action.

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.

Copyright © 2023 Musarubra US LLC 042023-01

Trellix

6000 Headquarters Drive
Plano, TX 75024

www.trellix.com