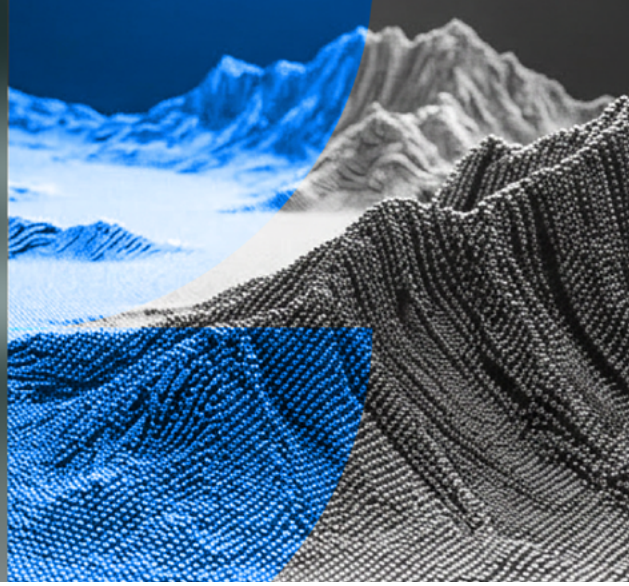
proofpoint.

SOLUTION BRIEF

Proofpoint Collaboration Security Prime

Protecting against AI-scaled attacks across email and beyond



Key Highlights

- **Blocks the widest variety of threats with 99.999% efficacy**
- **Extends protection to people across email and beyond**
- **Strengthens human resilience with risk-based guidance and insights**
- **Minimizes the impact of internal and supplier account compromise**
- **Simplifies operations with a unified platform that automates workflows**
- **Eliminates the cost and complexity of fragmented solutions through consolidation**

This solution set is part of Proofpoint' s integrated human-centric security platform, securing people and data in the agentic workspace.

Overview

As organizations enter the agentic era, they are adopting AI-powered tools and assistants to help people work more effectively. These AI agents are becoming part of the extended workforce, interacting with employees, applications, and other agents across email, messaging platforms, cloud apps, and more. As the workspace expands so does the attack surface, and attackers are already taking advantage of these trusted communication channels.

In response, many organizations are forced into taking a fragmented, point-product approach to security. But this creates additional gaps in their defenses, silos teams, and increases operational complexity.

To defend against today' s AI-scaled attacks across multiple channels and stages as well as protect trusted interactions—whether human-to-human, human-to-AI assistant, human-to-cloud application—organizations need a more holistic approach. Proofpoint Collaboration Security Prime can help. Prime unifies threat detection and response across the agentic workspace.

It helps you to:

- Defend against multichannel, multistage attacks with unmatched accuracy
- Minimize the impact of employee and supplier account compromise
- Secure trusted business communications with suppliers, partners, and customers
- Strengthen human resilience with targeted, human risk-based education
- Streamline security operations through automation

Protect people wherever they collaborate—across email and beyond

As work continues to evolve toward a more connected and AI-assisted workspace, Collaboration Security Prime protects people wherever they work. It stops multichannel attacks across email and collaboration and messaging tools such as Microsoft Teams, Slack, social media, and cloud-based applications. What' s more, it does this without disrupting how work gets done.

Prime protects people across this expanded workspace against the broadest range of threats, including:.

- Advanced phishing
- Business email compromise (BEC)
- Telephone-oriented attack delivery (TOAD)
- Email bombing
- Ransomware
- Account takeovers
- AI-generated attacks and AI exploitation techniques, such as prompt injection

Plus, it stops attacks at all stages of the threat lifecycle—from pre-delivery to post-delivery, and from time of click to login.

With flexible email security deployment options—including secure email gateway (SEG) and API-based architectures—it extends protection across environments while aligning with your existing infrastructure.

Powered by Proofpoint' s Nexus® AI technology, Prime delivers unmatched threat protection with 99.999% efficacy. It does this by using our rich threat intelligence, advanced language models, relationship graphs, machine learning, behavioral analysis, and computer vision. All these technologies work together to detect and stop threats before they can cause harm.

Defend against account compromise

Attackers use a range of techniques—from phishing and credential theft to brute-force and session hijacking—to gain access to legitimate accounts and launch multistage attacks. Once inside, they move across email, cloud apps, collaboration tools, and supplier relationships, exploiting trusted identities to expand their reach.

Collaboration Security Prime reduces this risk at every stage of the attack chain. It helps surface credential misuse early—such as corporate password reuse on unsanctioned or risky applications—giving security teams visibility into exposed identities before attackers can use them for account takeover.

When compromise does occur, Prime detects, investigates, and contains it quickly. By correlating identity and activity signals across platforms such as Microsoft 365, Google Workspace, and Okta, it identifies suspicious behavior, exposes attacker activity, and automates response—from session revocation to rollback of unauthorized changes.

This same identity-aware approach extends beyond your organization. Prime identifies compromised supplier accounts, detects subtle anomalies in trusted communications, and applies adaptive protections—such as warning indicators and URL isolation—to reduce risk without disrupting business operations.

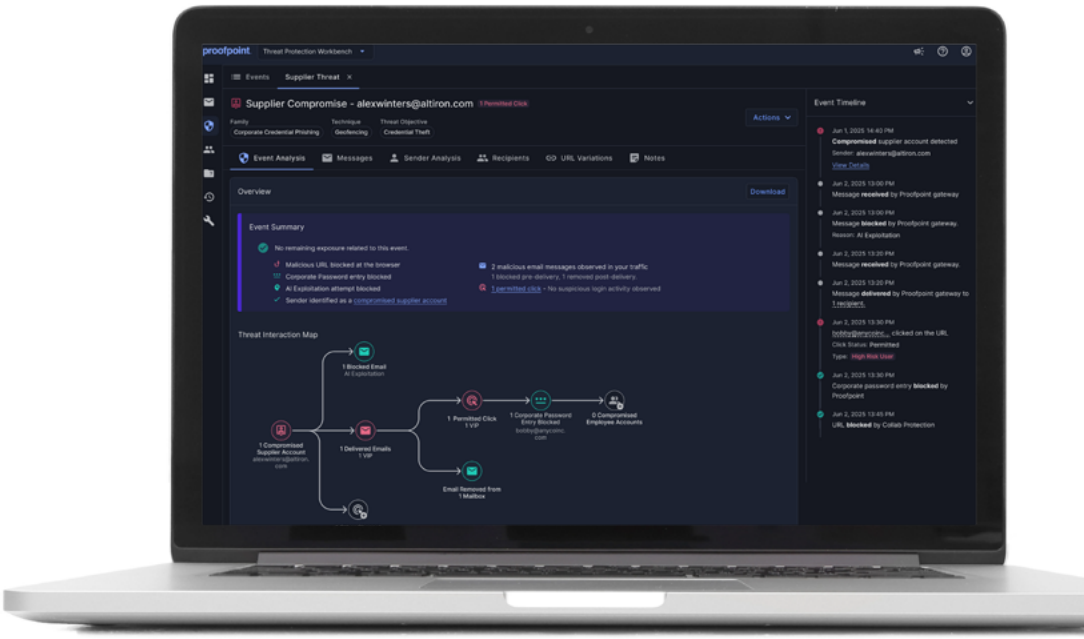


Figure 1. Collaboration Security Prime stops and correlates threats across email, messaging and collaboration, cloud and supplier channels.

Nexus® AI models are trained on one of the largest and most diverse datasets in all of cybersecurity.

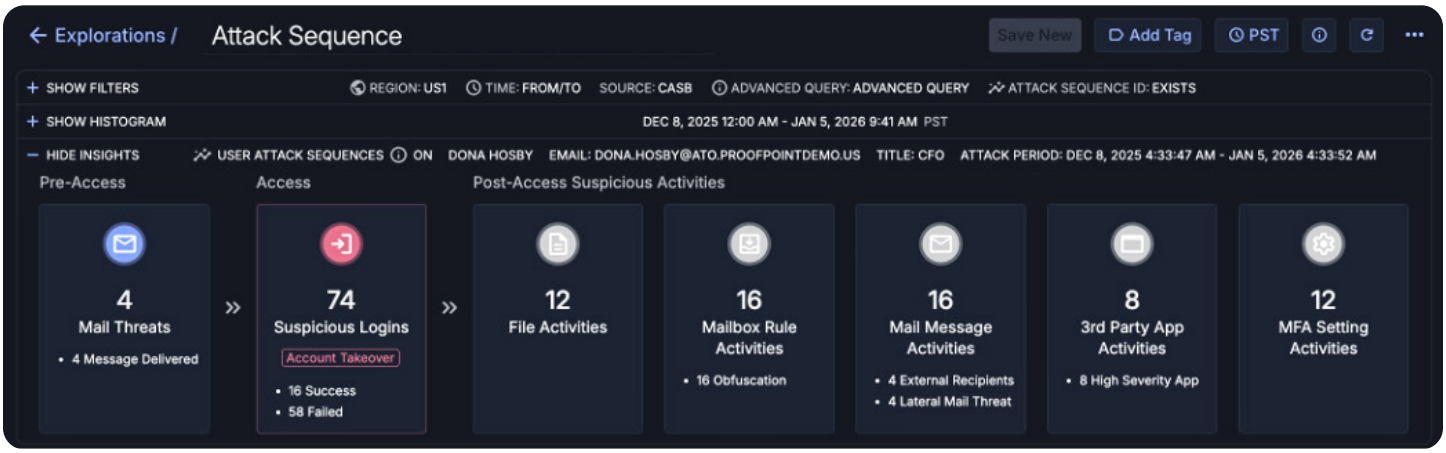


Figure 2. Collaboration Security Prime provides visibility into attack sequences and automates containment.

Protect your trusted business communications

Attackers often use impersonation tactics to insert themselves into trusted business communications. When your organization is impersonated—whether through direct domain spoofing or lookalike domains—it puts your employees, customers, and partners at risk. What' s more, it can inflict serious damage on your brand.

Collaboration Security Prime can help you proactively mitigate these impersonation risks. It gives you complete visibility into all emails sent using your trusted domains, including those sent by third parties. You gain access not only to powerful tools, but also to expert consultants who will guide you through every step of your email authentication rollout. This helps you achieve full DMARC compliance and prevents attackers from spoofing your domains.

Our protection extends beyond user-generated emails to include a secure, dedicated environment for relaying application-generated messages as well as emails sent by third-party SaaS providers on your behalf.

Additionally, Prime provides advanced lookalike domain discovery capabilities. It dynamically monitors the internet for domains that closely resemble your own. And it provides detailed insights into their registration details as well as potential misuse.

We don' t just stop at detection. We can work on your behalf to shut down malicious domains and URLs using our strong relationships with registrars, hosting providers, and top-level domain (TLD) authorities. Our professionals manage the entire process, allowing your teams to focus on core business operations.

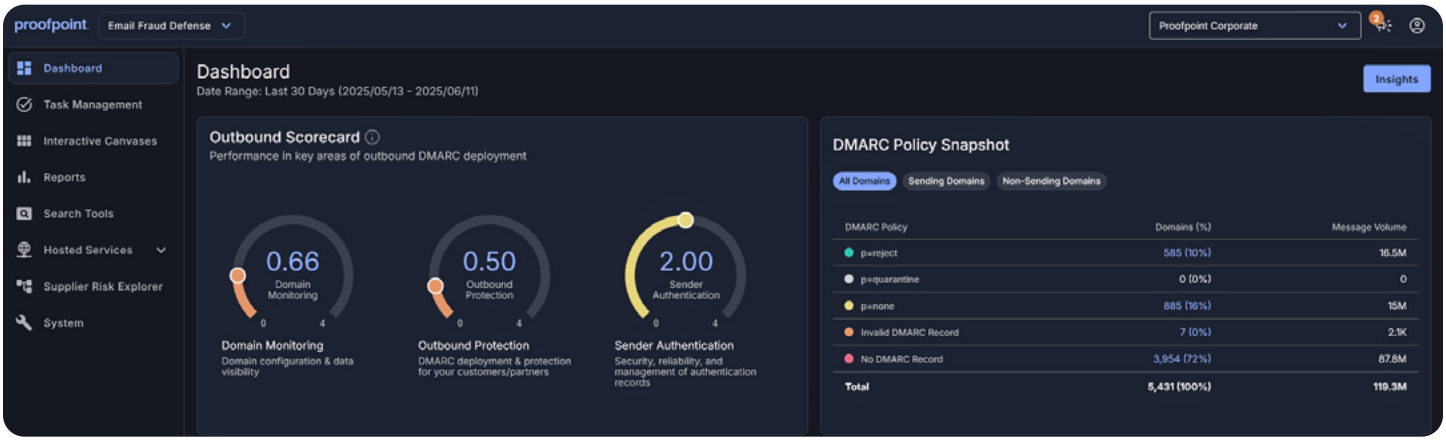


Figure 3. Collaboration Security Prime provides visibility into impersonation threats, such as domain spoofing and malicious lookalikes.

Strengthen human resilience with risk-based guidance

As work becomes more collaborative and dynamic, people must become more resilient against cyberattacks. This requires moving beyond compliance-driven training to human risk management that features education and controls that are aligned to how users actually work and the risks they face.

Collaboration Security Prime enables this shift by combining targeted learning with the Human Resilience Workbench. It provides a centralized view of user risk across behavior, role, and attack exposure. Security teams can identify high-risk users, understand why risk is changing, and take action with targeted interventions.

Prime delivers automated, risk-based learning that's tailored to each user's profile. Using AI, it converts real-world threats into simulations with a single click, ensuring education reflects active threats and reinforces safer decisions in context.

Learning adapts continuously based on user behavior and is delivered through engaging, in-the-moment experiences that drive participation and retention. Both users and administrators gain clear visibility into progress and risk reduction through intuitive dashboards.

The result is a closed-loop model: identify risk, act with targeted education and controls, and measure improvement over time—driving measurable behavior change and a stronger security culture.

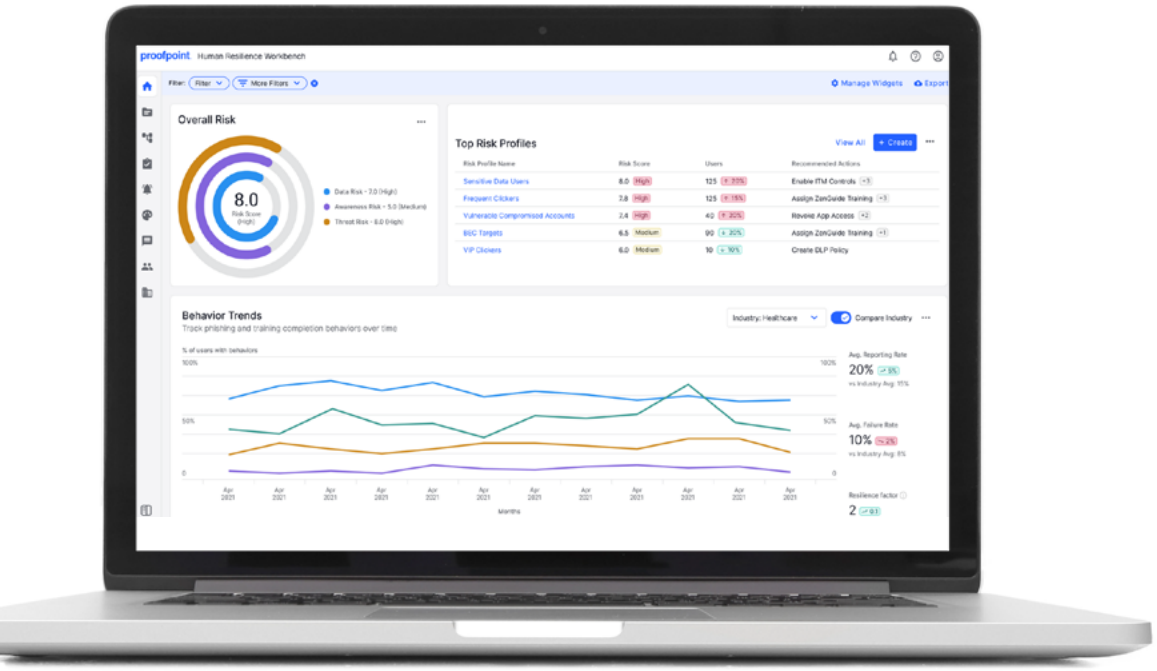


Figure 4. Collaboration Security Prime provides visibility into real user behavior, which enables targeted, risk-based learning.

Simplify security operations

As threats expand beyond email to collaboration tools, cloud platforms, and supplier ecosystems, security teams are under pressure to do more with less. In this environment, disconnected point solutions don' t make things easier. Not only do they increase complexity, but they also slow response times and drive up operational costs. All of which makes it harder to reduce risk at scale.

Collaboration Security Prime simplifies your security operations by unifying threat detection and investigation, and automating workflows and response. The Threat Protection Workbench uses native integrations to bring together detection insights and attack forensics from across email, messaging, collaboration platforms, cloud accounts, and supplier ecosystems. This enables teams to investigate incidents and take decisive action—all from a single, unified workspace for maximum efficiency.

Prime also helps teams prioritize effectively. The Threat Interaction Map correlates threats and security events across control points—and provides a visual map of attack paths. This enables analysts to quickly identify the most critical incidents. In parallel, it automatically inspects user-reported messages, remediates malicious content, and delivers feedback to users. As a result, manual effort is reduced while secure user behavior is reinforced.

The result is faster response and lower operational complexity. And your security team can do more with less—without sacrificing protection.

Choose the right level of protection

Collaboration Security Prime is available in multiple tiers. This enables you to align protection with your organization' s risk profile and operational needs. Each tier builds on the previous one. Coverage expands from core email threats to collaboration channels, account compromise, human risk reduction, and advanced brand protection.

See our available features on the next page.

Learn more at **proofpoint.com**

proofpoint.

All Collaboration Security solution tiers are available for both SEG and API deployments. Feature availability may vary by deployment model.

	Available Features	Core Email Protection	Collaboration Security Trier 2	Collaboration Security Trier 3	Collaboration Security Prime
Email security	BEC, phising, call-back phishing, and malware protection	✓	✓	✓	✓
	Multilayered detection stack powered by Nexus AI	✓	✓	✓	✓
	Unparalleled threat data from 2.8M+ customers	✓	✓	✓	✓
	Attachment and URL sandboxing	✓	✓	✓	✓
	URL re-write & click-time sandboxing	SEG	SEG	SEG	SEG
	Isolate suspicious clicks on rewritten URLs	VAPS*	All users*	All users*	All users*
	Anti-spam and graymail detection	✓	✓	✓	✓
	Contextual emerail warning tags	✓	✓	✓	✓
	Adaptive email hygiene self-learns based on user behavior	✓	✓	✓	✓
	Configurable mail routing policies	SEG	SEG	SEG	SEG
	Automated message remediation	✓	✓	✓	✓
	Automate abuse mailbox	✓	✓	✓	✓
	Very Attacked People (VAP)™, threat actor, and global intelligence	✓	✓	✓	✓
Multichannel, multistage threat protection	Detect and remediate compromised cloud accounts		✓	✓	✓
	Block malicious URLs sent via messaging and collaboration applications		✓	✓	✓
	Detect corporate password misuse on risky or unsanctioned websites		✓	✓	✓
	Compromised supplier account protection		✓	✓	✓
Human resilience and security awareness	Guide users with automated, risk-based education			✓	✓
	Identify and prioritize human risk with unified risk insights			✓	✓
	Build employee awareness with real-world, threat-based simulations			✓	✓
	Convert active threats into safe simulations			✓	✓
Impersonation Protection	Prevent brand abuse via email authentication				✓
	Detect and remediate malicious lookalike domains				✓
	Secure application email relay (250 GB)				✓

SEG = Secure email gateway deployment only
***** = Available for SEG deployments only.