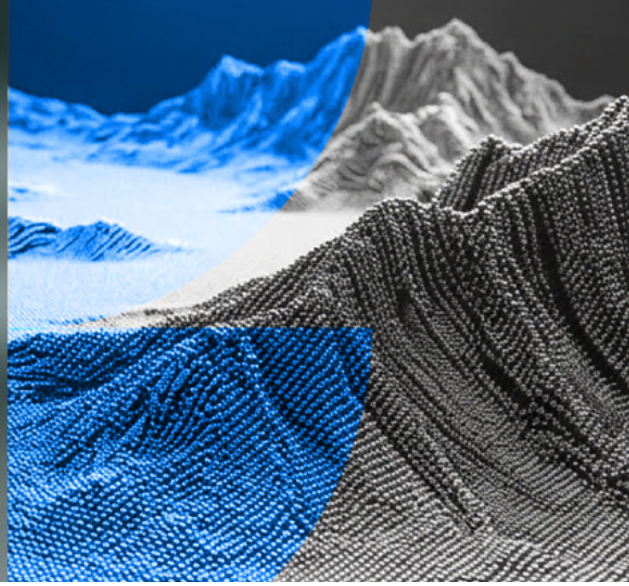
proofpoint.

SOLUTION BRIEF

Proofpoint Collaboration Security Prime

Complete and Continuous Collaboration Security for the AI Era



Key Highlights

- **Blocks the widest variety of threats with 99.999% efficacy**
- **Contains account compromise in minutes, whether the threat starts in email, across other vectors, or stems from a compromised supplier**
- **Cuts real-world malicious link clicks by 40% within six months of deployment**
- **Stops impersonation and shuts down lookalike domains before they reach your customers**
- **Lowers the total cost of ownership by 40% through platform consolidation**

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

Overview

AI has transformed the landscape for everyone. Attackers are using it to launch more novel and personalized attacks with greater sophistication and scale. Campaigns like business email compromise (BEC) have increased 27%, and AI-generated phishing now drives a 4.5X higher click rate than traditional phishing. Users have grown more susceptible to AI-generated content, while defenders are overwhelmed by alert triage and fragmented tools.

Organizations need a fundamentally different approach built for the agentic era, where AI-powered tools and assistants join the extended workforce across email, messaging, and cloud apps, expanding the attack surface attackers are already exploiting.

Unfortunately, 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:

- Detect novel, AI-generated threats earlier with greater visibility across the attack surface
- Block with confidence through industry-leading accuracy and low false positives
- Deliver continuous protection across pre-delivery, post-delivery, browser, and agentic coverage
- Protect business communications wherever they happen, across chat, apps, and agents
- Contain account compromise in minutes, not days

©Proofpoint, Inc. 2026

Detect novel threats earlier, with greater visibility

Novel, AI-generated attacks are moving faster than traditional defenses can catch them. As a result, they're slipping past legacy filters and reaching people across email, collaboration platforms, and cloud applications alike.

Collaboration Security Prime closes that gap with continuous protection across the full threat lifecycle, from pre-delivery to post-delivery email architecture, and from time of click to login, across every channel where people work.

Prime protects against the broadest range of threats, including:

- Advanced phishing, including credential phishing and callback phishing
- BEC and CEO impersonation
- Malware delivery
- QR code attacks
- Telephone-oriented attack delivery (TOAD)
- Email bombing
- Ransomware
- Account takeovers
- Legitimate service abuse
- AI-generated attacks and AI exploitation techniques, such as prompt injection

At the core of this protection is Proofpoint Nexus® AI, the industry's most advanced detection engine. Trained on one of the largest datasets in the in the industry, Nexus AI evaluates over 1,000 attributes per message. It combines five model types, language models, relationship graphs, machine learning, threat intelligence, and computer vision, working together and continuously learning from every verdict.

The result is 99.999% detection efficacy and the industry's lowest false positive rate, so real threats are stopped without burying teams in noise.

Defend against account compromise

Account compromise isn't limited to phishing emails. AI is making it easier for threat actors to scale credential attacks well beyond the inbox, from generating convincing, pixel-perfect lookalike login pages to defeating multifactor authentication through automated prompt bombing.

In a workspace driven by collaboration and assisted by agents, it's critical to stop these threats at every stage, before, during, and after compromise.

Collaboration Security Prime helps prevent compromise before it happens. Prime's SSO Password Guard detects when employees reuse their corporate password on non-corporate sites, closing off one of the most common entry points for credential-based attacks, and extending protection beyond email to the browser itself.

When prevention isn't enough, Prime detects compromise as it happens. It correlates identity and post-access signals across Microsoft 365, Google Workspace, and Okta to identify accounts that show signs of compromise.

Once a compromise is identified, Prime helps you investigate and contain it in minutes, not days, limiting the blast radius before an attacker can move further into the environment.

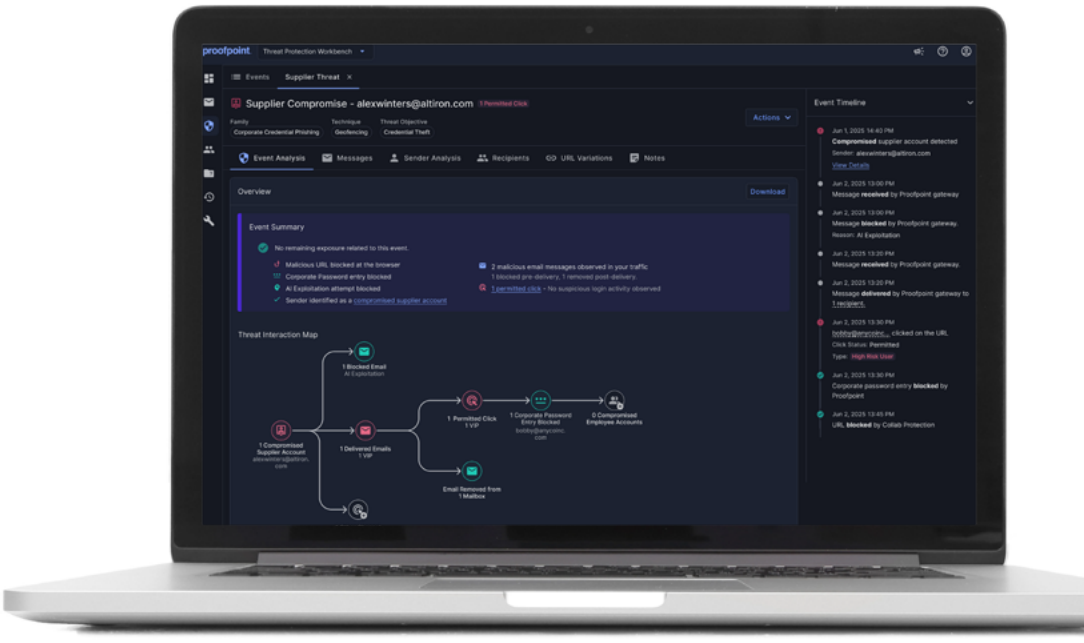


Figure 1. Collaboration Security Prime stops and correlates threats across email, messaging and collaboration, cloud and supplier channels.

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

©Proofpoint, Inc. 2026

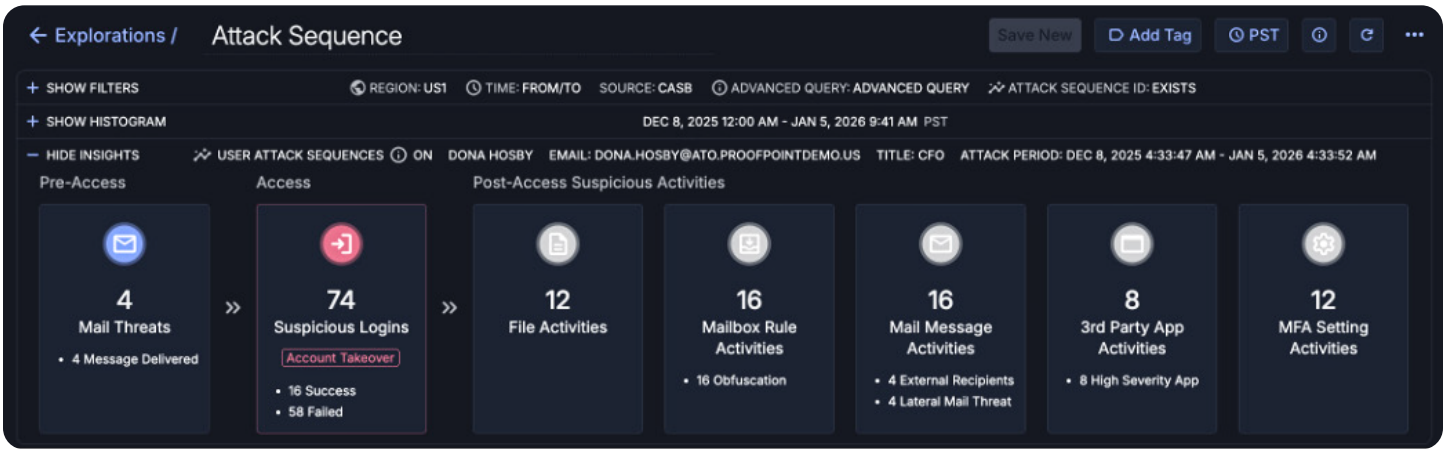


Figure 2. Collaboration Security Prime provides visibility into attack sequences and automates containment.

Protect your trusted business communications

Attackers often use impersonation tactics to insert themselves into trusted business communications, whether through direct domain spoofing, lookalike domains, or compromised supplier accounts. When your organization or its partners are impersonated or compromised, it puts your employees and customers at risk, and 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.

When it comes to supplier threats, Prime protects your employees from being exploited by attackers who are using compromised third-party accounts. It identifies suspicious activities that originate from supplier accounts and applies adaptive protections, such as warning indicators and URL isolation, to reduce risk without disrupting legitimate business communications.

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.

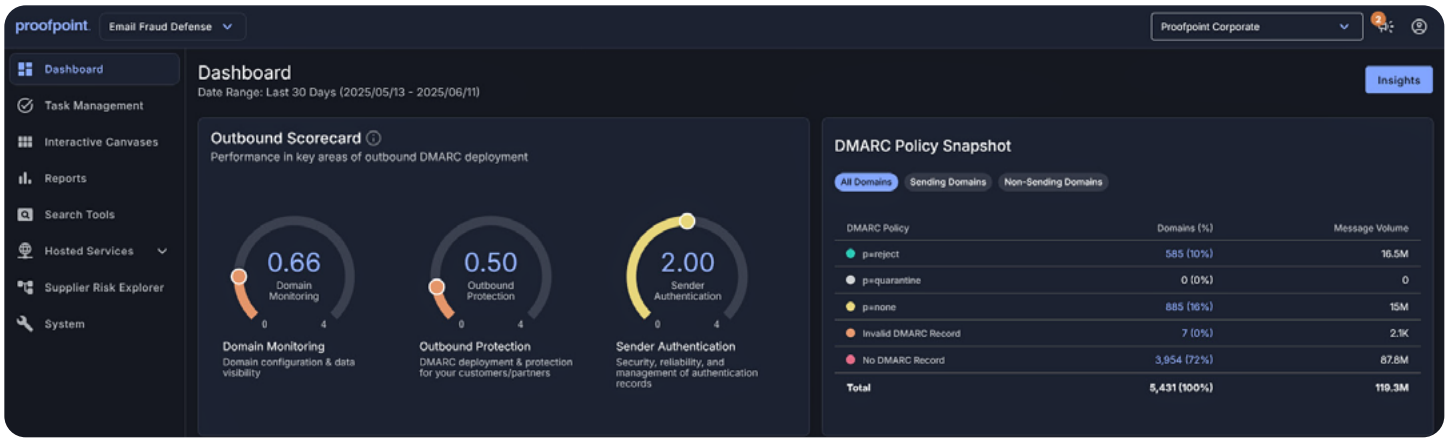


Figure 3. Collaboration Security Prime provides visibility into impersonation threats, such as domain spoofing and malicious lookalikes.

©Proofpoint, Inc. 2026

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—in-the-moment education that reflects how users work and the real risks that they face.

Collaboration Security Prime builds human resilience systematically, not through one-time training, but through a continuous cycle tied to real risk.

It starts with targeting. The Human Resilience Workbench draws in behavior and risk signals from across the platform, automatically identifying high-risk users, new hires, and repeat clickers so security teams can focus attention where it matters most.

From there, Prime reinforces safer behavior at the moment risk is highest. Using AI-powered ThreatFlip, it converts real, active threats into instant, one-click simulations, showing employees exactly what an attack looks like right after they encounter one, not weeks later in a generic training module.

Finally, Prime proves the impact. Risk scores and benchmarking give administrators clear visibility into where behavior is improving and where gaps remain. Organizations using this approach see 40% fewer real-world malicious link clicks within six months, evidence that resilience, not just awareness, is what drives lasting change.

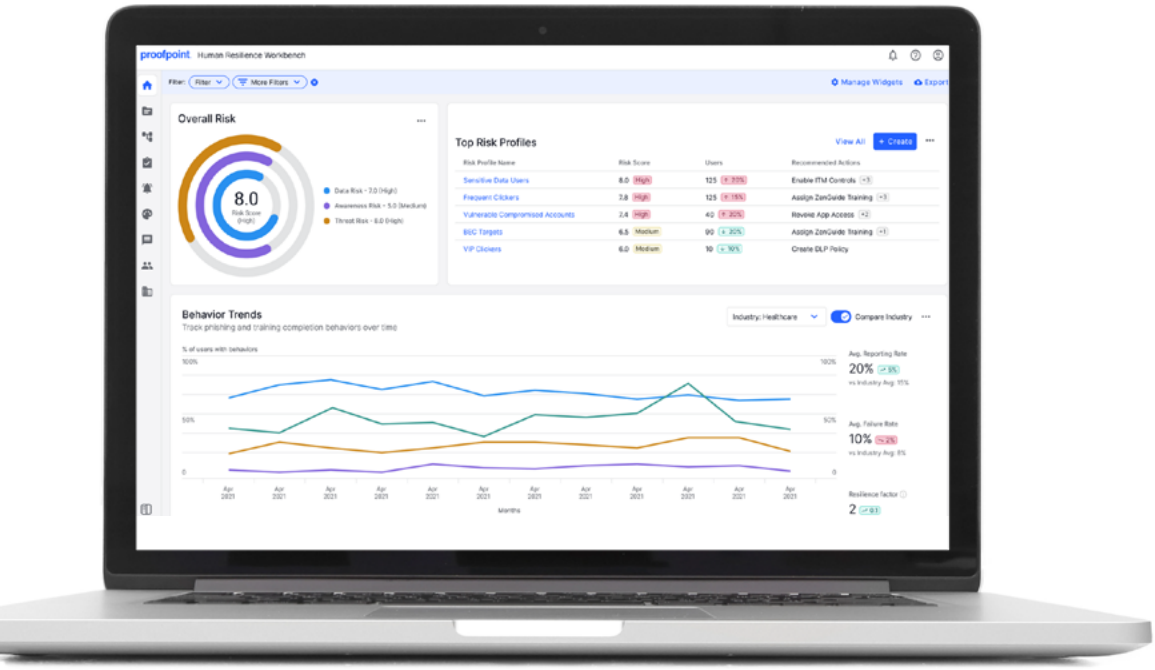


Figure 4. Collaboration Security Prime provides visibility into real user behavior, which enables targeted, risk-based learning.

©Proofpoint, Inc. 2026

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**

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com

Connect with Proofpoint: LinkedIn

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.

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 Tier 2	Collaboration Security Tier 3	Collaboration Security Prime
Email security	BEC, phishing, 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 email 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			✓	✓
	Build employee awareness with real-world, threat-based simulations			✓	✓
	Convert active threats into safe simulations			✓	✓
	Detect and prioritize at-risk users based on behaviors, threat telemetries, and roles			✓	✓
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.

©Proofpoint, Inc. 2026