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
- Minimises 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 organisations enter the agentic era, they're 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 organisations are forced into taking a fragmented, point-product approach to security. But this creates additional gaps in their defences, 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 or human-to-cloud application—organisations need a more holistic approach. Proofpoint Collaboration Security Prime can help. Prime unifies threat detection and response across the agentic workspace.

It helps you:

- Defend against multichannel, multistage attacks with unmatched accuracy
- Minimise 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

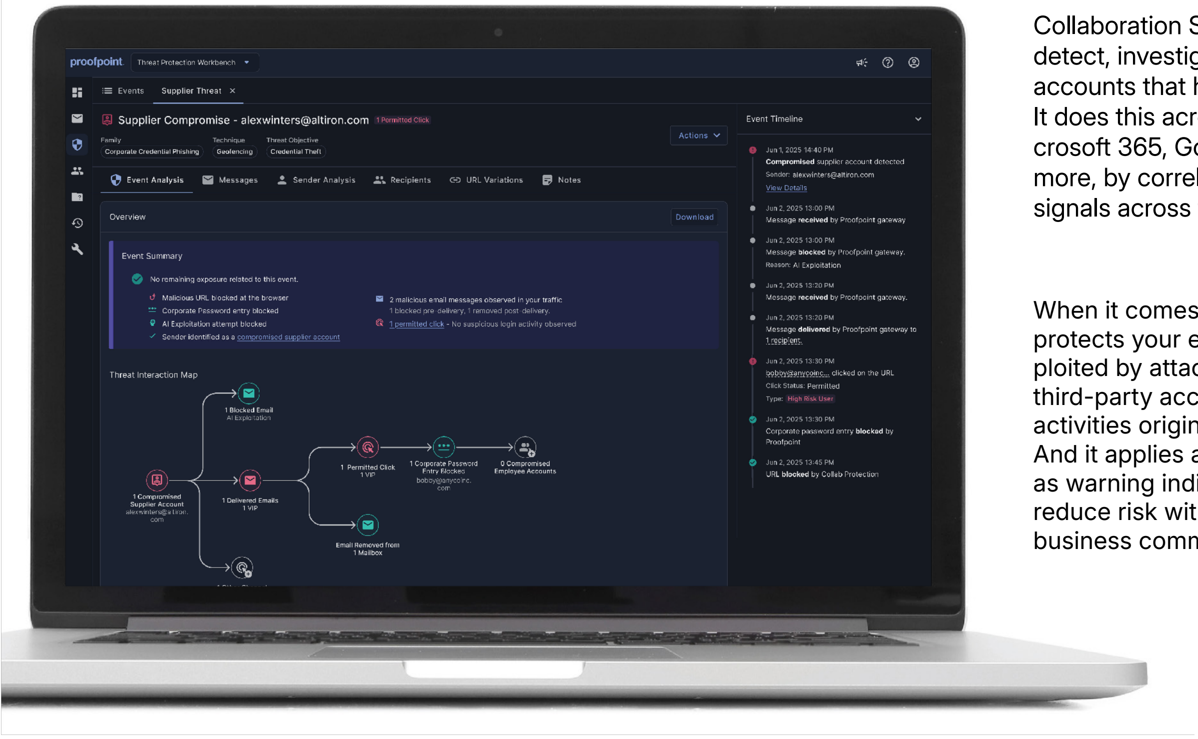
Protect people wherever they collaborate, across email and beyond

As work continues to evolve towards 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. It also achieves 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

It also stops attacks at all stages of the threat lifecycle: from pre-delivery to post-delivery and from time of click to login.



Supplier Compromise - alexwinters@altiron.com 1 Permitted Click

Event Summary

No remaining exposure related to this event.

- Malicious URL blocked at the browser
- Corporate Password entry blocked
- AI Exploitation attempt blocked
- Sender identified as a compromised supplier account

2 malicious email messages observed in your traffic
1 blocked pre-delivery, 1 removed post-delivery.

1 permitted click - No suspicious login activity observed

Jun 1, 2025 14:40 PM
Compromised supplier account detected
Sender: alexwinters@altiron.com
View Details

Jun 2, 2025 13:00 PM
Message **received** by Proofpoint gateway

Jun 2, 2025 13:00 PM
Message **blocked** by Proofpoint gateway.
Reason: AI Exploitation

Jun 2, 2025 13:20 PM
Message **received** by Proofpoint gateway.

Jun 2, 2025 13:20 PM
Message **delivered** by Proofpoint gateway to 1 recipient.

Jun 2, 2025 13:30 PM
bobby@anycoinc... clicked on the URL
Click Status: Permitted
Type: High Risk User

Jun 2, 2025 13:30 PM
Corporate password entry **blocked** by Proofpoint

Jun 2, 2025 13:45 PM
URL **blocked** by Collab Protection

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

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, behavioural analysis and computer vision. All these technologies work together to detect and stop threats before they can cause harm.

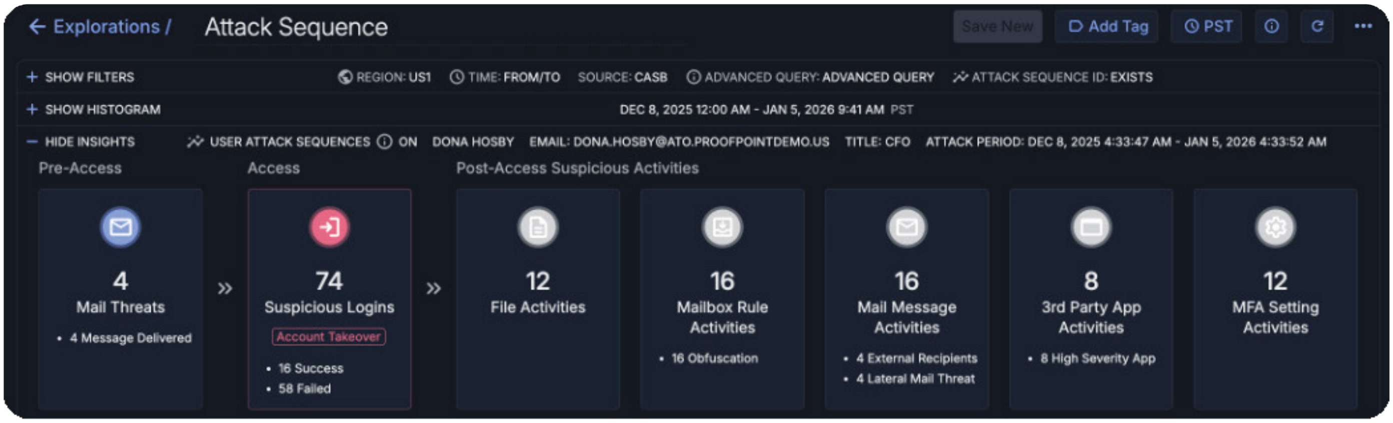
Nexus® AI models are trained on one of the largest and most diverse datasets in all of cybersecurity.

Defend against account compromise

Attackers use compromised identities to access legitimate accounts and launch multistage attacks. They abuse the compromised accounts of your employees as well as those of your trusted suppliers. In a workspace driven by collaboration and assisted by agents, minimising the impact of these threats is critical.

Collaboration Security Prime helps you detect, investigate and contain employee accounts that have been compromised. It does this across platforms, such as Microsoft 365, Google Workspace, Okta and more, by correlating identity and activity signals across the Proofpoint ecosystem.

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



REGION: US1 TIME: FROM/TO SOURCE: CASB ADVANCED QUERY: ADVANCED QUERY ATTACK SEQUENCE ID: EXISTS

DEC 8, 2025 12:00 AM - JAN 5, 2026 9:41 AM PST

USER ATTACK SEQUENCES ON DONA HOSBY EMAIL: DONA.HOSBY@ATO.PROOFPOINTDEMO.US TITLE: CFO ATTACK PERIOD: DEC 8, 2025 4:33:47 AM - JAN 5, 2026 4:33:52 AM

4 Mail Threats
- 4 Message Delivered

74 Suspicious Logins
Account Takeover
- 16 Success
- 58 Failed

12 File Activities

16 Mailbox Rule Activities
- 16 Obfuscation

16 Mail Message Activities
- 4 External Recipients
- 4 Lateral Mail Threat

8 3rd Party App Activities
- 8 High Severity App

12 MFA Setting Activities

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

Protect your trusted business communications.

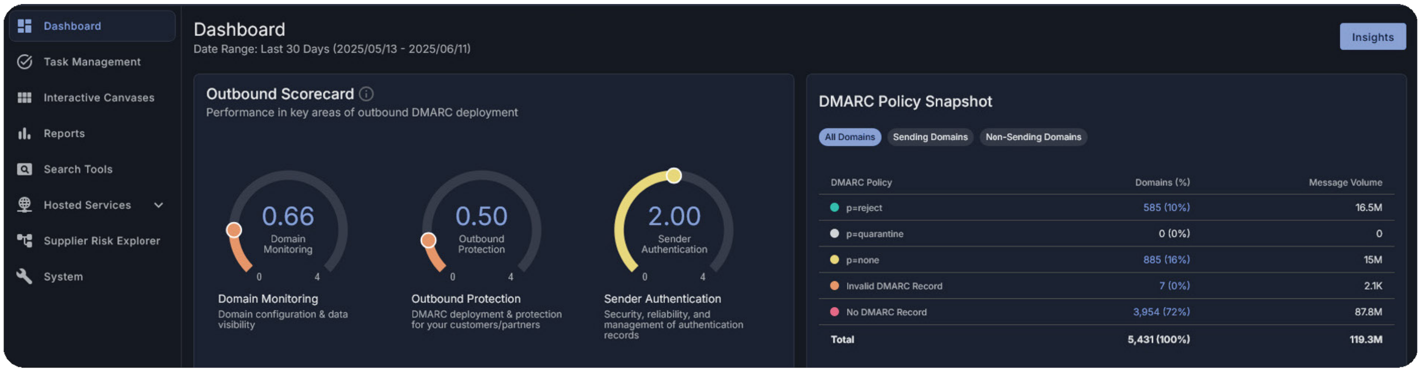
Attackers often use impersonation tactics to insert themselves into trusted business communications. When your organisation is impersonated—whether through direct domain spoofing or lookalike domains—it puts your employees, customers and partners at risk. It can also inflict serious damage to your brand.

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 closely resembling 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.



Dashboard
Date Range: Last 30 Days (2025/05/13 - 2025/06/11)

Outbound Scorecard
Performance in key areas of outbound DMARC deployment

Domain Monitoring
Domain configuration & data visibility

Outbound Protection
DMARC deployment & protection for your customers/partners

Sender Authentication
Security, reliability, and management of authentication records

DMARC Policy Snapshot

DMARC Policy	Domains (%)	Message Volume
● p=reject	585 (10%)	16.5M
● p=quarantine	0 (0%)	0
● p=none	885 (16%)	15M
● Invalid DMARC Record	7 (0%)	2.1K
● No DMARC Record	3,954 (72%)	87.8M
Total	5,431 (100%)	119.3M

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: in-the-moment education showing how users work and the real risks they face.

Collaboration Security Prime helps your organisation make this shift by guiding your employees to make safer choices. It provides automated, targeted, human risk–based learning that's tailored to each user's behaviour, role, attack exposure and unique risk profile. Using AI, Prime converts real-world threats into instant simulations with a single click. This ensures education is aligned with active risk signals to drive measurable, lasting behaviour change.

Not only do learning modules adapt to individual risk signals, but they're delivered through engaging, gamified experiences. As a result, users are motivated to participate, and their safer behaviour is reinforced over time. Learners gain clear visibility into their progress through intuitive dashboards, keeping them informed and accountable.

At the same time, administrators can easily tailor programmes to align with organisational risk priorities. The result is higher engagement, measurable behaviour change and a stronger security culture across your organisation.

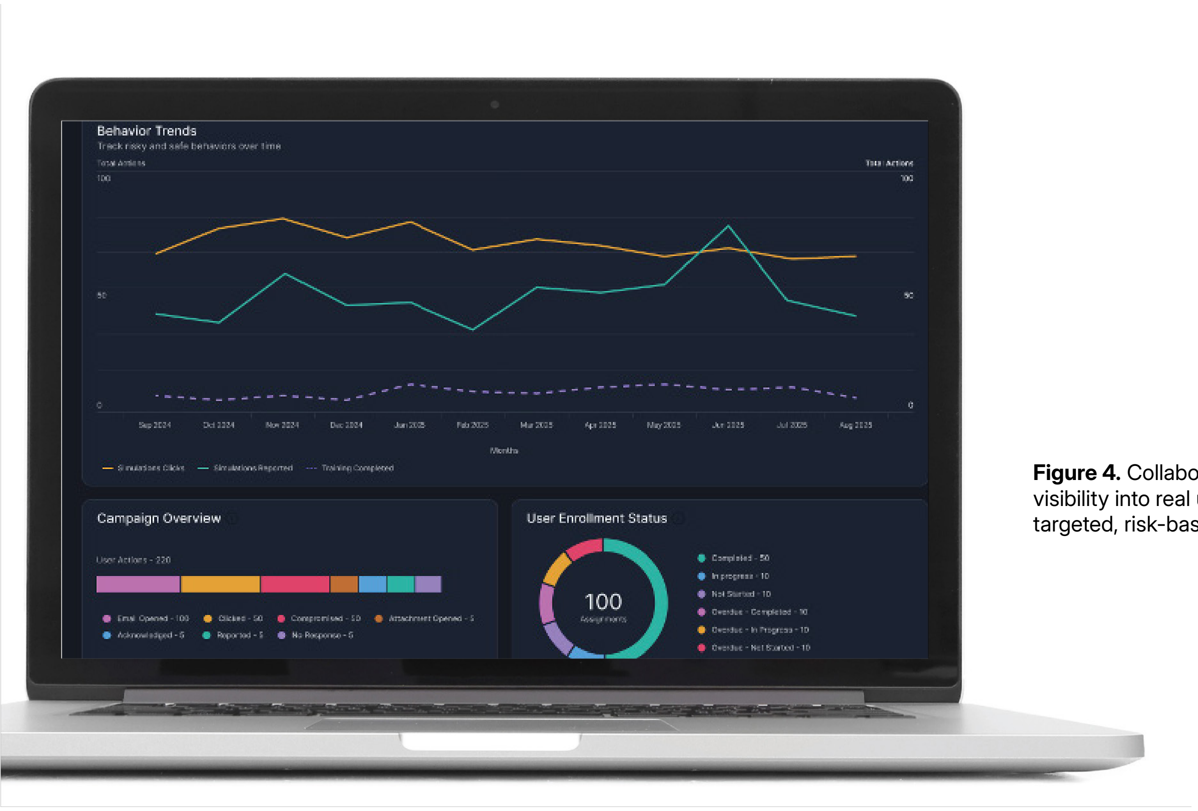


Figure 4. Collaboration Security Prime provides visibility into real user behaviour, which enables targeted, risk-based learning.

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 this 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 prioritise 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 behaviour 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 organisation'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.

proofpoint.

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 organisations in stopping threats, preventing data loss and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organisations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com/uk.

Connect with Proofpoint: Linke-

DISCOVER THE PROOFPOINT PLATFORM →

	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 rewrite & 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 behaviour	●	●	●	●
	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		●	●	●
	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			●	●
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.