proofpoint.

Proofpoint Prime Threat Protection for Enterprise

Key benefits

- Blocks the widest variety of threats with 99.99% accuracy
- Extends protection to people on any platform—email and beyond
- Strengthens human resilience with risk-based guidance and insights
- Accelerates response time for both employee and supplier account compromises
- Simplifies operations with industry-leading detection efficacy and automated workflow
- Maximizes cost efficiency through consolidation and preconfigured integration

Overview

Email remains a primary vector for cyber threats. However, in recent years the attack surface has expanded—bad actors target people across email and other digital channels like messaging platforms, collaboration tools, cloud apps, file-sharing services and more.

In response, many organizations are taking a fragmented, point-product approach to security. But this creates additional gaps in their defenses and leaves many risks unaddressed. And managing and integrating all these tools is complicated.

To defend against these evolving human-centric threats, you need to take a holistic approach. Proofpoint Prime Threat Protection (Prime) can help.

Prime enables you to defend your organization against multichannel, multistage attacks and secure your business communications. What's more, it provides risk-based guidance for your employees and streamlines your security operations at every level.

Enterprise Prime Threat Protection

USER PROTECTION

- Security Awareness & Behavior Change
- Account Takeover Protection
- Collaboration & Messaging Protection

IMPERSONATION PROTECTION

- Domain Spoofing Protection
- Secure App Email Relaying
- Supplier Threat Protection
- Malicious Domain Takedown Services

CORE EMAIL PROTECTION

Stop Threats Across Email and Other Digital Channels

Today's employees communicate and collaborate more efficiently than ever before. They work across Microsoft Teams, Slack, cloud-based applications, file-sharing services and more. While this boosts employee productivity, it also expands the attack surface. Human-centric cyberattacks are no longer confined to just email—and your defenses shouldn't be, either.

Prime protects your entire digital workspace. Whether threats are delivered through email, instant messages, social media networks or collaboration apps, Prime provides real-time protection against a wide variety of threats—BEC, ransomware, spear phishing and more.

Powered by Proofpoint's Nexus® AI technology, Prime delivers unmatched threat protection with 99.99% efficacy. It does this by leveraging 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.

With its expansive reach and powerful AI capabilities, Prime keeps your workforce secure—no matter where or how they work.
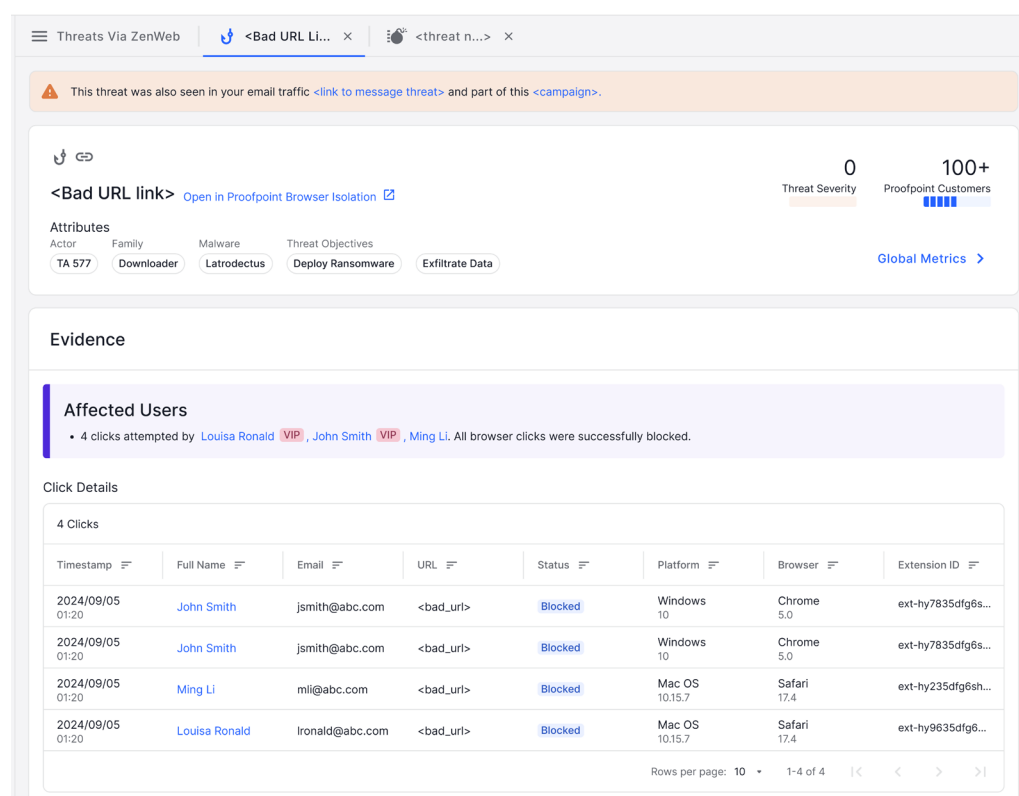

Figure 1: Proofpoint extends phishing protections beyond email. It also blocks malicious URLs that are shared in messaging, collaboration and communication platforms.

Defend Against Multistage Attacks

Attackers take over legitimate user accounts using a wide range of tactics. These include phishing, brute-force attacks, session hijacking and social engineering. Once an account is compromised, they often escalate privileges, access your data and establish long-term persistence. Even if you have multifactor authentication (MFA) in place, account takeovers (ATOs) are still a threat.

Prime defends against ATOs that bypass MFA. It enables security teams to quickly detect, investigate and respond to compromised accounts across major platforms such as Microsoft 365, Google Workspace and Okta.

Not only does it provide a centralized view of what attackers are doing post-compromise, but it also supports a variety of automated responses. Teams can choose to automatically suspend compromised accounts, enforce password resets, revert unauthorized changes and remove suspicious third-party applications.

It also protects you from multistage attacks that come from cybercriminals using compromised supplier accounts. Prime detects when third-party accounts might be compromised throughout the Proofpoint ecosystem, and it alerts your security team. It also empowers your team to apply adaptive security controls, such as URL isolation and email warning tags, without disrupting legitimate messages.
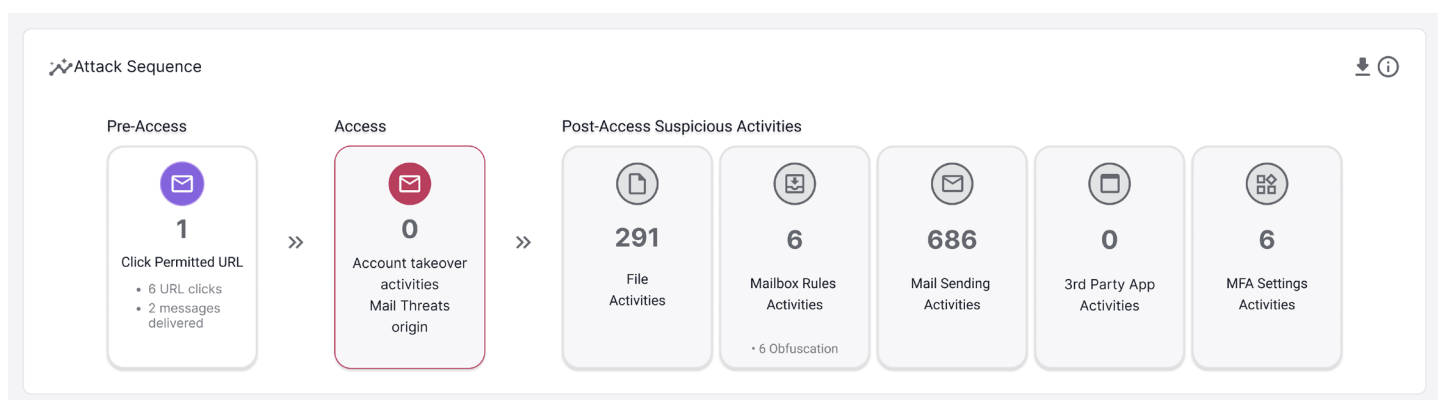

Figure 2: Proofpoint Prime shows you pre- and post-access malicious activities for affected accounts.

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, and can inflict serious damage on your brand.

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 and 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 provides detailed insights into their registration details as well as potential misuse. And we don't just stop at detection; we can work on your behalf to shut down malicious domains and URLs leveraging 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.
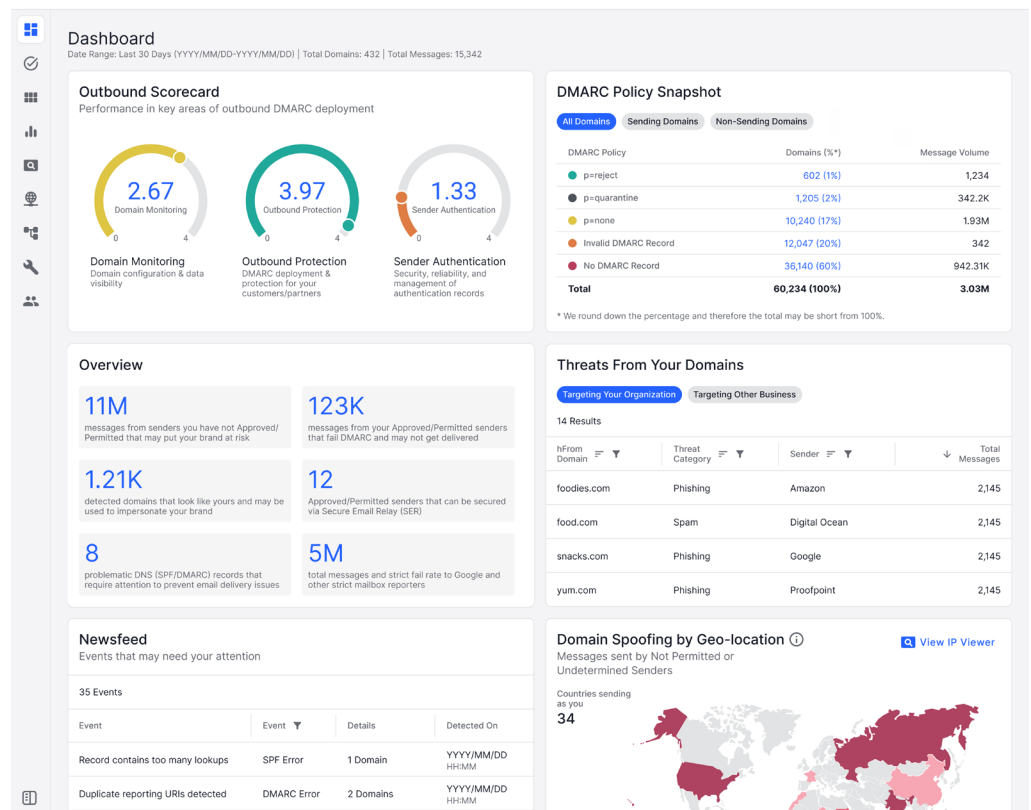

Figure 3: Prime gives you visibility into domain spoofing threats, malicious lookalikes of your domains, and emails being sent using your trusted domains.

Build Resilience Through Risk-Based Guidance and Insights

Cybercriminals target people. Unfortunately, once-a-year security training isn't enough to improve your overall security posture against their ever-evolving tactics.

Prime provides human risk insights and guidance that foster meaningful behavior change and helps build lasting human resilience. It uses adaptive, risk-based learning that goes beyond traditional approaches, making it far more effective than one-size-fits-all methods.

Prime helps organizations measure human risk and identify high-risk individuals by aggregating insights across the Proofpoint ecosystem. With its adaptive learning pathways feature, Prime enables security teams to automatically enroll risky users in tailored learning experiences based on

their behaviors, threat exposure, roles, security skills and business privileges. For example, a Very Attacked Person (VAP) can be automatically enrolled in targeted engagements—such as training assignments, notifications and phishing simulations—based on the specific types of threats targeting them. This empowers security teams to deliver more relevant threat-driven content, drive meaningful engagement, and scale behavior-change efforts more efficiently across the organization.

As your employees become more resilient against evolving threats, you not only reduce overall risk, but your workforce becomes a key line of defense. With Prime, you can measure the impact of your human resilience program and quantify exactly how much human risk has been reduced. This helps to show the effectiveness of your program, which means you're more likely to get continued support from your leadership and stakeholders.
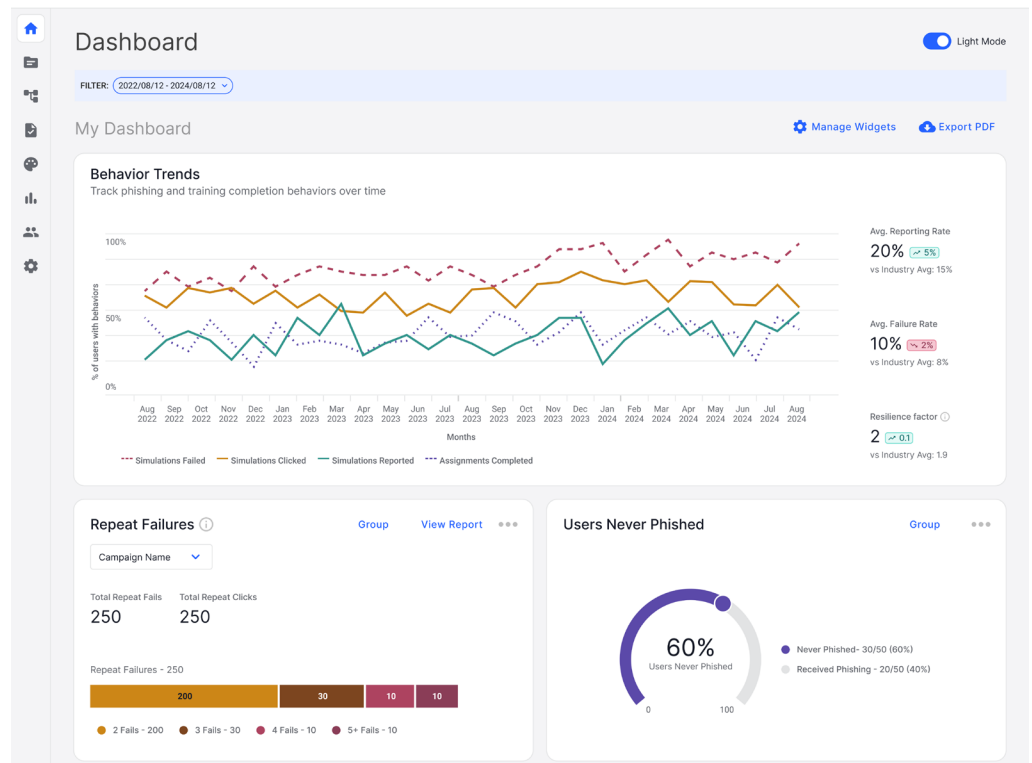

Figure 4: Informed by Proofpoint global threat intelligence, Prime gives you insights about the ever-changing threat landscape. You can guide and educate your users on new threats while capturing behavior trends over time.

Capitalize on the Benefits of Integrated Protection

It's increasingly challenging to protect the digital workspace from cyber threats. A patchwork of siloed point products isn't enough and leaves many risks unaddressed. There are issues with integration, management complexity, overspending and high operational costs.

Proofpoint Prime addresses these challenges with a comprehensive approach to threat defense, closing security gaps and reducing the complexity caused by fragmented, disconnected solutions. Our integrated threat protection enables your team to act faster and more effectively with automated workflows, shared threat intelligence and pre-configured integrations. Plus, Prime includes licensing benefits that can lower your operational costs and improve your return on investment. Best of all, you get an industry-leading, trusted partner that you can rely on.

Prime Threat Protection

Multi-Channel Defense with Nexus AI
- Defends threats across email, cloud apps, collab & messaging tools etc. Uses Nexus AI to ensure full-surface protection

Human Risk-Based Guidance and Insights
- Provides employees risk-based guidance & education and enables security teams to apply adaptive controls based on adaptive insights

Multi-Stage Attack Protection
- Detects & remediates both compromised employee and supplier accounts; get full visibility from one console for faster threat response

Impersonation Protection
- Protects trusted domains against spoofing with email authentication, brand protection, and takedown services

Comprehensive protection & resilience for multi-channel, multi-stage human-centric threats

proofpoint.

---

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →