Advanced Email Security

Protect against known and unknown email threats and get actionable visibility into advanced attacks and users who are being targeted

Email is a fundamental feature of modern business. Yet it is also the number one threat vector. In fact, more than 90% of threats arrive via email.\(^1\) And email attacks are constantly evolving—from phishing attacks to new forms of email threats. Some attacks include business email compromise (BEC), supply chain attacks, ransomware and cloud account compromise. Proofpoint delivers the most effective integrated solution to protect your people and critical data from these advanced phishing threats.

Proofpoint protects your people from advanced attacks with a complete, extensible email security platform. We detect and block email threats and provide visibility into your greatest risk—your very attacked people (VAPs). With actionable insights, you can better understand the risk you face and respond to threats faster and more effectively.

Detect and block both known and unknown threats before they reach the inbox

Stop advanced threats with a robust integrated threat protection platform

Proofpoint provides better protection because we see more threats and detect them faster. We block email with malicious URLs or attachments, as well as malware-less threats like credential phishing and BEC. We dynamically classify impostor and phishing threats with our impostor classifier. And we assess the reputation of the sender with Advanced BEC Defense, our advanced machine-learning. Along with this information, we create a baseline by learning your organization’s normal flow and by aggregating data from other Proofpoint deployments. Having this baseline allows us to quickly identify email that falls outside of the norm.

We analyze email with multi-layered content analysis, reputation analysis and sandboxing. This effectively stops advanced email threats, including polymorphic malware and ransomware, before they hit your users. And we provide you with predictive and click-time URL sandboxing to detect and block malicious URLs. Re-writing URLs protects your users on any network and device and helps detect if a message has been weaponized after delivery.

Click safely with email and browser isolation

Attackers don’t just use one tactic to break into your organization. They’ll try various tactics and threat vectors. For example, they’ll target your users through corporate email and personal webmail. Or they attack users when they engage in personal browsing from their corporate devices. With email and browser isolation, we let your users access websites, personal webmail and corporate email safely. They can interact with websites in a secure environment. And you can disable uploads and downloads and restricting data input while the website is being analyzed. Our real-time anti-phish scan runs as soon as the page is opened. This determines whether the page could be a potential phishing site, which takes no more than a few seconds. This technology adds an additional layer to prevent credential theft, especially for those phishing emails that contain URLs poisoned post delivery.

Prevent email fraud with email authentication

Domain-based Message Authentication, Reporting and Conformance (DMARC) has proven to be the most effective way to protect against domain spoofing. And it prevents fraudulent emails using your domain. We help you fully deploy DMARC faster and with less risk of blocking legitimate email, so you can confidently protect your employees, partners and customers. We also give you the visibility, tools and services to authorize legitimate email and block fraudulent messages before they reach the inbox. And we help you enforce DMARC authentication quickly and safely to block fraudulent emails that spoof trusted domains at the Proofpoint gateway. What’s more, you can see all impostor threats from a single pane of glass—regardless of the tactic used or the person being targeted. In addition, we flag lookalike domains registered by third parties. This proactively prevents fraudulent lookalike domain email attacks before they strike. Our managed service includes an experienced consultant to guide you through every step of your deployment. We also work with you to identify all your trusted senders, including third-party senders, to ensure they authenticate properly.

Protect internal email and quickly contain threats

Protecting internal email is just as critical as protecting inbound email. Attackers use compromised accounts to send phishing, BEC or malware. Proofpoint scans internal emails for malicious content in the form of URLs and attachments. And when a malicious internal email has been detected, you can automatically pull and quarantine any unwanted messages, even if it was forwarded or received by other users. We also allow you to get reporting that indicates exactly which accounts may have been compromised, enabling you to quickly take action on those accounts.
Get unmatched visibility into attacks and your human attack surface

In today’s people-centric threat landscape, your users are your greatest asset and your biggest risk. To better mitigate and communicate risk to your management and board, you need to know:

- Who your VAPs are
- How they are being targeted
- Who are vulnerable to these threats

We give you unmatched visibility into targeted attacks and your human attack surface, so you know who is posing risk to your organization. Once you have that insight, you can then prioritize and mitigate risk by implementing adaptive controls for your risky users.

In addition, we provide detailed forensic information on threats and campaigns in real time. Our deep threat analysis shows you everything from who was being attacked, where the attack was coming from, and even what the attack looked like—with email samples and screenshots. Going beyond email, we also connect the dots between email attacks and suspicious logins, uncovering and stopping account compromise more effectively. We also provide you with visibility into which suppliers pose risk to your organization. With Nexus Supplier Risk Explorer, we automatically identify potentially impersonated and compromised suppliers and the domains they use to send email to your users. And with visibility across these attack vectors, you can address complex attacks comprehensively.

Improve operational effectiveness

One common challenge that most organizations have is shortage of security staff. On top of that, most security teams are overwhelmed with managing multiple security vendors and products that don’t always talk to each other. We provide you with an integrated solution that focuses on the threats that matter and that automates threat detection and remediation. This saves you time and money.
Protect against data loss via email

Email is the number one threat vector for both inbound threats and outbound data loss. So it’s important to secure your sensitive data and prevent data loss via email. We give you out-of-the-box visibility and enforcement to prevent intentional and accidental data loss during email communication. Email data loss prevention (DLP) and encryption are tightly integrated and can be centrally managed. We analyze confidential information within structured and unstructured data. And we provide you with fine-tuned policies and prebuilt dictionaries. These automatically find and classify data protected by regulatory compliance and data privacy laws. And they help you comply with data protection rules across a range of industries—including PCI DSS, SOX, HIPAA, GDPR and more—while reducing your manual work. When combined with encryption, you can define and customize unique policies to automatically encrypt sensitive data in email. This makes it easy for you to manage and secure sensitive data exchange.

Summary

Proofpoint Advanced Email Security effectively protects against the number one threat vector—email. It provides you with actionable visibility into your attacks and your most attacked people. Our solution:

- Blocks both known and unknown threats before they enter
- Provides unmatched visibility into threats targeting your people
- Improves operational effectiveness with automated threat response
- Trains your users to become part of your line of defense
- Protects against data loss via email

LEARN MORE

For more information, visit proofpoint.com.