Proofpoint Email Protection

Detect and Block Both Malicious and Malware-less Email Threats

KEY BENEFITS

- Block BEC scams, phishing attacks and advanced malware at entry
- Raise user awareness with email warning tag
- Improve productivity with fast email tracing and email hygiene
- Scale for large enterprises with complete flexibility
- Provide operational efficiencies through automation of security operation and threat response
- Extend protection with integrated email authentication, email encryption, email DLP, Targeted Attack Protection and more
- Deliver industry-leading SLAs when deployed in the cloud:
  - 99.999% service availability
  - 100% virus protection
  - less than one-minute email latency
  - 99% blocked or redirected spam

Proofpoint Email Protection helps secure and control your inbound and outbound email. It uses machine learning and multilayered detection techniques to identify and block malicious email. It also dynamically classifies today's threats and common nuisances. And it gives you granular control over a wide range of email. This includes imposter email, phishing, malware, spam, bulk mail and more. It also offers complete flexibility with custom security policies and mail routing rules. It's also the most deployed email security solution by the Fortune 1000. And it scales for even the largest enterprise. What's more, it supports cloud, on-premises and hybrid installations.

Email is the No. 1 threat vector, with 96% of suspicious social actions arriving through email.[1] In addition to common email threats like phishing attacks and malware, emerging business email compromise (BEC) has posed a new threat to organizations. Email Protection catches both known and unknown threats that others miss. By processing billions of messages each day, Proofpoint sees more threats, detects them faster and better protects you against hard-to-detect malware-less threats, such as impostor email. With Email Protection, you can stop a vast majority of threats before they arrive in your user's inbox.

Catch Emerging Threats That Others Miss

Detect phishing, impostor and fraudulent email

Email Protection detects emerging threats before they can get to your user's inbox. Proofpoint Advanced BEC Defense powered by NexusAI is designed to effectively stop a wide variety of email fraud. That includes payment redirect and supplier invoicing fraud from compromised accounts. These types of threats require a more sophisticated detection technique, as there's often no malicious payload to detect.

Advanced BEC Defense is our ML and AI-powered detection engine. It is specifically designed to find and stop BEC attacks. It dynamically detects BEC by analyzing multiple

1 Data Breach Investigations Report, Verizon, 2020.

message attributes. Some examples include:

- Message header data
- Sender's IP address (x-originating IP, reputation)
- Message body for urgency and words or phrases

It determines whether a message is a BEC threat. And it detects various BEC actor tactics. Such as:

- Reply-to pivots
- Use of malicious IPs
- Use of impersonated supplier domains

Advanced BEC Defense also provides granular visibility into BEC threat details. That includes BEC theme, gift card, payroll redirect, invoicing, lure or task. It provides observations about why the message was suspicious and message samples. That way, your security team can better understand and communicate about the attack. Data from NexusAI is then fed into the Proofpoint Nexus Threat Graph. It analyzes and correlates threat information across email, cloud, network and social from all of our customers. And thus gives you the protection to stay ahead of the threat landscape.

Block malicious and unwanted email

We've built multilayered detection techniques into Email Protection to defend against constantly evolving threats. With signature-based detection, it blocks known threats like viruses, trojan horses and ransomware. And it uses dynamic reputation analysis to continually assess local and global IP addresses to determine whether to accept email connections. Our unique email classifier also dynamically classifies a wide variety of emails. This includes impostor, phishing, malware, spam, bulk mail, adult content and circle of trust. And it quarantines incoming email by types. Together, these features help protect you at the first signs of malicious activity.

Track Down Any Email in Seconds

Email Protection has the most powerful search capability. With the smart search feature, you can easily pinpoint hard-to-find log data based on dozens of search criteria. You can also swiftly trace where emails come from and go to. Email Protection provides you with granular details of search results, including metadata with over a hundred attributes. The search is complete in seconds, not minutes. You can download and export your search results by up to 1 million records. Moreover, several real-time reports are built into the product, giving you the detailed visibility into mail flow and trends. With this data, you can proactively address issues as they emerge.

Scales for Large Enterprise with Complete Flexibility

Email Protection supports the demands of the largest enterprises in the world. It allows you to create highly customizable email firewall rules at the global, group and user level. You can create any security policies and mail routing rules that fit your needs. And you can easily enforce them. Email Protection also provides the same benefits and greater flexibility with multiple deployment options. This includes on-premises hardware, virtual machine and SaaS.

Raise User Security Awareness

The email warning tag feature enables your users to make more informed decisions on the emails that fall into the gray area between clean and malicious. It surfaces a short description of the risk associated with a particular email. And it conveys the level of risk with different colors, which is easy to consume by your users. They can report suspicious email directly from the warning tag, even when they access email via mobile devices. This feature helps reduce the risk of potential compromise by making your users more cautious of uncertain email.

Email Protection also allows email admins to give users the ability to manage encrypted messages and low-priority emails like bulk mail, review quarantined messages and take actions directly in the Outlook task pane. User feedback is then transmitted to Proofpoint, helping us improve the global accuracy of bulk mail classification.

Centrally Manage across Email Encryption and DLP

You can easily extend your protection by adding Proofpoint Targeted Attack Protection, Email Fraud Defense, Email Encryption or Email Data Loss Prevention (DLP). While Email Protection provides you with basic email encryption and DLP capabilities, you can get more robust email encryption and DLP solutions through the same management console. This tight integration helps you manage sensitive data sent through email. It also prevents data leakage or data loss via email. And it satisfies several compliance requirements.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.