Proofpoint Email Protection

Detect and Block Both Known and Unknown Email Threats

KEY BENEFITS

- See more threats, detect faster, and protect better
- Improve productivity with fast email tracing and email hygiene
- Scale for large enterprises with complete flexibility
- Provide operational efficiencies via automation of security operation and threat response
- Extend protection with integrated 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

Email is the number one threat vector—more than 90% of cyber attacks start with email.[1] In addition to common email threats like phishing and malware, emerging business email compromise (BEC) has posed a new threat to organizations. Proofpoint 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 malwareless threats, such as impostor email. With Email Protection, you can stop a vast majority of threats before they arrive in your user's inbox.

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 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. And it's 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.

1 Data Breach Investigations Report, Verizon, 2019.

CATCH EMERGING THREATS THAT OTHERS MISS

Detect Phishing and Impostor Email

Proofpoint Email Protection detects emerging threats before they can get to your user's inbox. Our unique Stateful Composite Scoring Service (SCSS), an advanced machine-learning technology, accurately classifies various types of email and detects threats that don't involve malware. This includes credential phishing and impostor email—also known as business email compromise (BEC). It assesses the reputation of the sender by analyzing multiple message attributes, including headers and content, across billions of messages. Along with this information, it develops a baseline by learning your organization's normal flow and aggregating other Proofpoint deployments. Having this baseline allows us to quickly spot and block email that falls outside of the norm, boosting its overall effectiveness. Rather than relying on updates, SCSS learns in real time to better classify good and bad emails and reacts to changes in the attack tactics.

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 divides your incoming email into separate quarantines 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. And you can download and export your search results by up to one 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

Unlike other solutions, 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 END-USER SECURITY AWARENESS

The email warning tag feature enables your end users to make more informed decisions on the emails that fall into the gray area between clean and suspicious. 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 end users. As a result, this feature helps reduce the risk of potential compromise by making your end users more cautious of uncertain email.

Email Protection also allows email admins to give end users the ability to manage low-priority emails like bulk mail, review quarantined messages, and take actions accordingly. Your user feedback is then transmitted to Proofpoint, and this helps 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 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 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**.

Proofpoint Targeted Attack Protection

Gain Advanced Threat Protection and Visibility

KEY BENEFITS

- Detect, analyze and block advanced threats before they reach your inbox
- Gain unique insights to identify your Very Attacked People and overall security risk
- Leverage Proofpoint Threat Intelligence to protect against threats and receive detailed forensics on attacks
- Provide adaptive security controls through URL isolation and security awareness training

More than 90% of attacks start with email[1]—and these threats are always evolving. Proofpoint Targeted Attack Protection (TAP) provides an innovative approach to detect, analyze and block advanced threats targeting your people. It also offers unique visibility into these threats so you can optimize your response.

TAP stops both known and never-before-seen email attacks. It detects and blocks polymorphic malware, weaponized documents, credential phishing and other advanced threats. It monitors cloud app activity to identify suspicious logins, broad file sharing, risky third-party applications and more. And it gives you the insight you need to identify and protect your most targeted people.

DEFEND AGAINST URL-, ATTACHMENT- AND CLOUD-BASED THREATS

TAP uses both static and dynamic techniques to continually detect and adapt to new attack patterns. We analyze potential threats using multiple approaches that examine behavior, code and protocol. This helps detect threats early in the attack chain, potentially before they do damage.

We use sandboxing to study a wide variety of attacks. Attacks include the use of malicious attachments and URLs to install malware or trick users into sharing sensitive information. We also leverage analyst-assisted execution to maximize detection and intelligence extraction.

To help you better understand cloud attacks, TAP detects threats and risks in cloud apps and connects them to credential theft and other email attacks. Our technology doesn't just detect threats, it also applies machine learning to observe the patterns, behaviors and techniques used in each attack. Armed with that insight, TAP learns and adapts so it can catch future attacks more quickly.

1 Verizon, "Cost of a Data Breach Investigations Report." July 2019.

URL Defense

TAP URL Defense provides protection against URL-based email threats including malware and credential phishing. It provides unique predictive analysis that identifies and sandboxes suspicious URLs based on email traffic patterns.

All URLs that reach inboxes are transparently rewritten. This protects users on any device or network. Real-time sandboxing is also performed every time a URL is clicked.

Attachment Defense

TAP Attachment Defense delivers protection against known and unknown threats that are delivered via attachments. It protects against threats hidden in a large range of file types, password-protected documents, attachments with embedded URLs and Zip files.

SaaS Defense

TAP SaaS Defense, compatible with Microsoft 365 (Office 365) or Google G Suite, brings to light suspicious login activity. This includes unusual login locations and excessive login attempts and failures. It also flags when there are too many connections to known malicious IP addresses. You also get visibility into internal and external high-exposure file sharing events. This lets you see when sensitive data could have been leaked during the previous 30 days. Finally, TAP SaaS Defense detects critical and high-severity third-party applications being used by your organization.

GAIN DEEP INSIGHT AND VISIBILITY INTO THREATS AND TARGETS

Proofpoint provides threat intelligence that spans email, cloud, network, mobile and social media. Our threat graph, derived from community-based intelligence, encompasses more than a trillion data points. It correlates attack campaigns across diverse industries and geographies. You can easily see this and gather other important insights with the TAP Threat Insight Dashboard. This dashboard provides detailed information on threats and campaigns in real time. You can understand both widespread and targeted attacks with this data. Details about the threat, including impacted users, attack screenshots and in-depth forensics are available.

Very Attacked People (VAPs)

Your security teams need to know who the top targets are in your organization in order to protect them. The Proofpoint Attack Index helps identify your VAPs™. This index is a weighted composite score of all threats sent to an individual in your organization. It scores threats on a scale of 0-1000 based on four factors: threat actor sophistication, spread and focus of attack targeting, type of attack, overall attack volume. With a better understanding of your VAPs, you can prioritize the most effective ways to stop threats.

Company-level Attack Index

The Attack Index can also be applied at the company level and compared to other industries to give you an overall company-risk comparison. This report helps your CISO and security team understand how attacks on your company compare to attacks on peers across industries. It covers frequency of attacks and types of threats. With this insight, you can prioritize security controls based on your unique attack landscape.

LEARN MORE

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