

NEXT-GENERATION EMAIL SECURITY

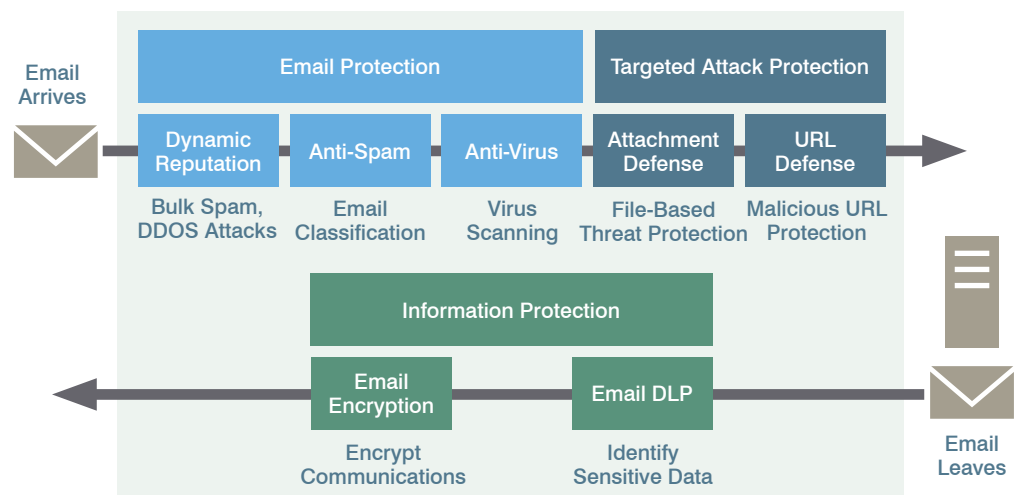
KEY FEATURES:

- Accurately detect and quarantine spam, phishing, bulk, adult and malware
- Customised end-user control over unwanted email
- Static and dynamic analysis of URLs and attachments
- Actionable forensic detail of all threats identified
- Transparent policy-based DLP and encryption

It is clear that the threat landscape has shifted. We have moved from a world where mass spam email was the main problem, to one where highly targeted, advanced threats are now affecting organisations large and small across the globe.

There is no doubt that traditional solutions using legacy techniques, such as reputation and signatures, are no longer sufficient to identify and stop spam and malicious email. Malware techniques have rapidly evolved and, in order to keep pace, so must the technology used to protect against these threats. This increase in threat is compounded by the growth of impostor email attacks that attempt to trick targeted victims into sending money without the use of any malicious content at all.

Proofpoint offers a next-generation email security platform that protects against attacks and secures sensitive data leaving the organisation. Our solutions are built on a single, extensible platform that offers clear visibility into all email communication, with search and reporting capabilities to help you to identify and prioritise security incidents.



PROOFPOINT EMAIL PROTECTION

Proofpoint delivers the industry's most effective spam detection by using a combination of machine learning technology and composite reputation analysis. Organisations can feel more secure knowing that over 99% of spam and unwanted email will not make it to an employee inbox—guaranteed. This control extends to impostor email detection, to prevent this rapidly emerging threat from causing your business to lose money. Added to this, end users have personalised control over bulk or unwanted mail by easily defining which emails they wish to receive and block.

Granular reports and real-time alerts give you complete visibility into the state of your enterprise messaging system. Our advanced message-tracing features use a high-performance search engine to pinpoint hard-to-find log data based on dozens of search criteria. More than 60 real-time graphical reports give you the information you need to proactively address issues and trends.

Proofpoint Email Protection is built using the Sendmail MTA and can be deployed as a cloud service, virtual appliance, or hardware appliance to support even the most complex routing requirements.

PROOFPOINT TARGETED ATTACK PROTECTION

Proofpoint Targeted Attack Protection (TAP) helps detect, mitigate, and resolve advanced threats that target people through email. We detect known threats and new, never-before-seen attacks that use malicious attachments and URLs. TAP is unmatched in stopping targeted attacks that use polymorphic malware, weaponised documents, and credential-stealing phishing techniques to access sensitive information.

TAP analyses threats in several stages using multiple approaches to examine behaviour, code, and protocols. Our technologies are built not just to detect threats but also learn from them. We observe patterns, behaviours, and tools of each attack—making the next one easier to catch.

Malware campaign intelligence and forensic reports can be accessed on the TAP dashboard. From there, you can easily distinguish campaigns from targeted attacks, prioritise alerts, and identify affected users to know how to best respond and resolve potential security incidents.

Proofpoint is the only cybersecurity company with threat intelligence spanning email, network, mobile apps, and social media. Our threat graph of community-based intelligence contains more than 300 billion data points to correlate attack campaigns across diverse industries and geographies.

PROOFPOINT INFORMATION PROTECTION

Proofpoint builds outbound information protection in a simple, yet granular way. Our solutions integrate key elements of data loss prevention (DLP) and encryption to create transparent policy enforcement.

With Proofpoint, using a combination of smart identifiers and managed dictionaries, you can construct policies to comply with data protection regulations—whether PCI, HIPAA or other requirements based on industry or geography. You can define the types of sensitive data—such as credit card, social security, or driving license details—that are relevant to your company. If sensitive data is identified in outgoing email, you can set policies to automatically block or encrypt the communication in order to keep the data secure.

Our integrated reports provide prioritised visibility into all potential policy violations—enabling your cybersecurity teams to focus their efforts on the people and incidents that have the highest impact to your business.

BACKED BY WORLD CLASS SUPPORT

All Proofpoint solutions are backed by our award-winning global support organisation, who are always there to make sure our customers have the support they need, when they need it.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.