Proofpoint Enterprise Protection

Guard against advanced phish, malware, spam, and other email-borne threats

Protect your business from email threats, including phising, malware, spam, and other forms of objectionable or dangerous content. The Proofpoint Enterprise Protection™ Suite delivers best-in-class inbound and outbound email security and management in one cost-effective, easy-to-use, cloud-based solution.
Proofpoint Enterprise Protection Benefits

» Delivers industry-leading inbound and outbound email security – phishing protection, anti-spam, anti-virus, email policy enforcement, message tracing and TLS encryption – as a cost-effective, on-demand service.

» Offers total control and flexibility for email security preferences, policies, enabled services, end-user controls, alerts and reporting.

» Enterprise-class availability and scalability ensure continuous service and complete security of data.

Proofpoint Enterprise Protection Features

» Proofpoint MLX deep content analysis for accurate threat classification of phish, spam, and other malware

» Multi-layered virus protection with signature-based anti-virus and behavioral based zero-hour protection

» Dynamic reputation service leverages Global IP and URL reputation

» Granular policy management

Additional Capabilities

Add privacy protection, data loss prevention and email encryption features with the Proofpoint Enterprise Privacy Suite:

» Advanced detection of private or confidential info in unstructured and structured data

» Pre-configured data protection policies

» Integrated, policy-based email encryption

» Robust DLP incident management, reporting and more

Advanced Threat Protection

Proofpoint has been a leader in effective blocking of email-borne threats for over a decade. Use Proofpoint Enterprise Protection to block known and unknown vectors including:

» Polymorphic and zero-day malware

» Weaponized attachments

» Malicious embedded URLs

» Other advanced exploits

...as well as spam, viruses, phish, bulk mail, and more.

To detect such known and emerging inbound advanced threats effectively and quickly, Proofpoint employs a variety of technologies based on Big Data analysis techniques, including both reactive and predictive approaches, as follow:

» Real-time IP reputation: assesses a sending address’ likely threat level based on content

» Real-time URL reputation: assesses embedded URLs’ likely threat level based on content

» Content & attachment signatures: match inbound content against known bad signatures

» Predictive URL sandboxing: pre-emptively runs binary downloads in virtual environments long before end-users click to download them.

» Credential Phishing detection: identifies credential-seeking attacks, even without malicious binaries

» IP-velocity and volume tracking: assesses inbound vectors based on rapidity and volume relative to threat level associated with senders and recipients.

» Zero-hour attachment blocking: proactively evaluates attachments against heuristics and virtual environment results

» Automated campaign identification: associates classes of content with threats

» Predictive content analysis: pre-emptively assesses threat levels based on content

Collectively, these technologies have made Proofpoint the leader in the Gartner Magic Quadrant.

Threat Classification and Real-Time Analysis

Some vectors contain multiple threats, which should be handled differently.

For example, an inbound email might appear to be simple advertising, based on content – but also link to dangerous advanced malware. Fine-grained classification is essential, to prevent such an email being placed into user-releasable spam quarantine vs. preserved in a safe environment for IT analysis of the malware risk.

Proofpoint applies multiple automated analyses to inbound and outbound traffic, to understand the precise nature and threat level of the traffic, including:
Multiple content filters:

» Structural tests
» Single-byte and double-byte language content inspection
» Pornography detection
» Malicious URL detection

...as well as any custom filter policies your administrators have defined

Multiple anti-virus filters, from your choice of multiple leading A/V engines

Advanced Threat Detection, as described in the previous section.

Collectively, these technologies enable administrators to specify appropriate routing of threats, risks, and prioritized communications, for better security and better end-user productivity & satisfaction.

Unmatched Control
Proofpoint’s solution provides a rich set of policy options, to enable fine-tuning of routing, handling and security rules.

From administrator-level customization of policies based on users, groups, or domains to end-user self-service to adjust receiving preferences, Proofpoint enables security and flexibility – and Proofpoint’s SmartSearch technology enables rapid message tracing and tracking for remediation.

Control functionality includes:

Administrator Filter Customization
All filter policies can be customized at a global, group, or user level—with full integration to LDAP or Active Directory to simplify on-going administration.

End-User Control of Preferences
Reducing the load on IT, end-users can exert simple, “self-service” control over their personal preferences within the limits set by IT, including:

» Personalized filter quarantines and quarantine digest reports within the communication stream they receive after filtering
» Personalized filter safelists and blocklists. (Global filter lists override end user lists.)
» Web-based, filter quarantine and profile administration.
» Ability to opt in and out of different filter policies (as permitted by IT administrator-configurable settings).

Collectively, these technologies enable administrators to balance control and end-user satisfaction, while reducing the load on IT and ensuring better security and message delivery.

<table>
<thead>
<tr>
<th>Proofpoint Enterprise Protection</th>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify Malicious Phishing Attacks</td>
<td>Isolate malicious phish messages from nuisance spam to prevent end users from mistakenly compromising the security of your organization</td>
<td></td>
</tr>
<tr>
<td>Identify Malicious Phishing Attacks</td>
<td>Shed locally or in the cloud with global reputation from Proofpoint Dynamic Reputation</td>
<td></td>
</tr>
<tr>
<td>Remove Spam and Virus</td>
<td>99%+ anti-spam accuracy with Proofpoint MLX</td>
<td></td>
</tr>
<tr>
<td>Remove Spam and Virus</td>
<td>Multi-layered virus protection, including Proofpoint Zero-Hour Anti-Virus™</td>
<td></td>
</tr>
<tr>
<td>Powerful End User</td>
<td>Controls Self-service to the end user</td>
<td></td>
</tr>
<tr>
<td>SaaS without Compromise</td>
<td>Full control, just like an on-premises solution</td>
<td></td>
</tr>
<tr>
<td>SaaS without Compromise</td>
<td>Isolated instances</td>
<td></td>
</tr>
</tbody>
</table>
Robust Delivery and Administration
Proofpoint offers flexible deployment options from on-premise to cloud, powerful and scalable performance based on Sendmail, and flexible, multilingual global administration capabilities.

Specific details of form-factors, routing, business continuity and administration include:

» Support for multiple form-factors (Cloud, Appliances, Virtual Machines, Hybrid) for flexible deployment, and scalable performance. Proofpoint has proven ability to scale from thousands to hundreds of thousands of users in 72 hours in customer deployments.

» Powerful routing: Proofpoint’s solution is built on top of the commercial version of Sendmail, the world’s most widely used MTA.

» Business Continuity: ensures uninterrupted secure email access in the event of a disaster or security breach.

» Flexible, global administration: Proofpoint’s solution provides granular and delegated administration for complex global organizations, including the ability to assign administration to globally separated teams. Proofpoint also has multilingual support interfaces for message digests and web-based spam quarantines in Chinese, Dutch, English, German, Finnish, French, Italian, Japanese, Portuguese, Russian, Spanish, and Swedish.

Collectively, this functionality ensures administrators can easily use and rely on Proofpoint to provide a robust security solution that can evolve with their organizations’ needs.

SaaS without Compromise
Proofpoint Enterprise Protection provides organizations the benefits of SaaS without compromising on control, flexibility or security. Built on modern virtualization and cloud-computing technologies, Proofpoint’s next-generation Security-as-a-Service architecture provides each organization with a logically isolated instance of Proofpoint. This ensures complete security of all customer data and processing capabilities, while leveraging the total cost-of-ownership and efficiency benefits of cloud computing.

Powerful End-User Tools
Proofpoint Enterprise Protection gives email users easy, self-service control over their individual email preferences with personalized quarantines and digest reports, personalized safelists and blocklists and web-based access to quarantines and profile administration. If desired, administrators can easily let users opt in and out of different spam policies.

Proofpoint Enterprise Protection is fully configurable, easy to brand and supports numerous languages (which can be configured for specific regions) for end users. Administrators have complete control over the look and feel of all end user components with point-and-click control over colors, logos, terms, help content, and more.

Subscribe to the Threat Insight blog at www.proofpoint.com/threat-insight, or follow us on Twitter @threatinsight.

Industry Leading SLAs
When deployed as SaaS, Proofpoint’s best-in-class service level agreements guarantee:

» 99.999% service availability
» 99% spam effectiveness
» 100% anti-virus protection
» < 1 minute email latency

About Proofpoint
Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint’s expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

©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.