proofpoint

Proofpoint Targeted Attack Protection

Proofpoint Targeted Attack Protection™ is the industry's first comprehensive solution for combatting targeted threats using a full lifecycle approach, monitoring suspicious messages containing malicious URLs or malicious attachments, and observing user clicks as they attempt to reach out. Proofpoint Targeted Attack Protection uses Big Data analysis techniques with Cloud Architecture to add additional layers of security that cannot be matched by traditional security solutions and gateways.

Why Proofpoint Targeted Attack Protection?

Advanced targeted attacks represent one of the most dangerous advanced threats facing enterprises today. Many of these threats, begin with a spear-phishing attack: a single, carefully crafted email that tricks a recipient into clicking a link to download malware or open a malicious attachments. Proofpoint Targeted Attack Protection provides real time threat prevention against these kind of targeted attacks and defends against these threats with a full lifecycle strategy that includes:

Next Generation Detection

Proofpoint Targeted Attack Protection uses sophisticated techniques to evaluate advanced threats that are traditionally missed by signature-based and reputation-based solutions. These techniques include:

- Malicious List Check – Check for emerging campaigns and known new malicious websites
- Code Analysis Check – Check for suspicious behavior, obfuscated scripts, malicious code snippets, and redirects to other malicious sites
- Dynamic Analysis – Sandbox a destination or sandbox a suspicious attachment to simulate a real user to a machine to observe changes made to a system

Predictive Defense

Proofpoint Targeted Attack Protection uses Big Data techniques and machine learning heuristics to predictively determine what 'could likely' be malicious, and take preemptive steps before any user clicks on it. It is achieved by:

- Modeling every user's email patterns and building behavioral history of that specific user to determine which email is suspicious and anomalous.

Highlights

- Advanced Protection against targeted email attacks like spear-phishing attacks, zero-day exploits, advanced persistent threats (APTs)
- Advanced Protection against malicious attachments. Support for most commonly used file formats
- Extends visibility into full threat lifecycle
- Use of techniques like Dynamic Malware Analysis and Cloud-based Sandboxing
- Protection across the corporate network, public network, and mobile devices
- Leverage Big Data techniques to build statistical models to provide predictive analysis
- Cloud-based solution that can be rapidly deployed without up-front capital expenditures

- Building Cloud based statistical model using history, Alexa ranking, IP block reputation, velocity of email sent from an originating IP, and a set of other criteria. Predicting malicious URLs, and proactively sandboxing with the help of real time scoring against this statistical model.

Follow-Me Protection

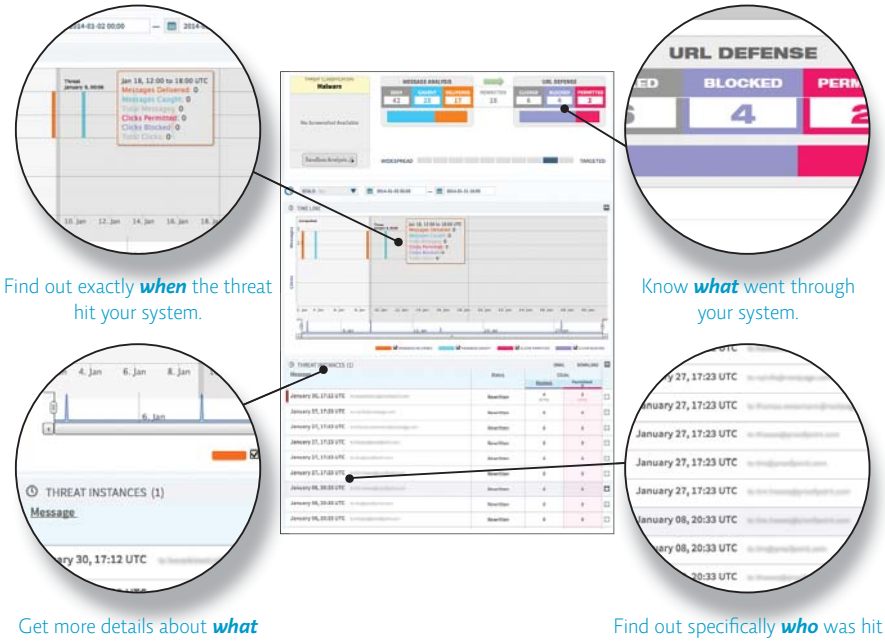
Proofpoint Targeted Attack Protection enables the solution to provide protection on any device, at any time, from any location, by following the email and checking for the URL destination's safety in real-time. A frequent technique used by hackers has been to drive recipients to click on a link directing them to a website which is initially harmless but turns malicious after a period of time. With Proofpoint Targeted Attack Protection, users are still protected: whether they access the message from the corporate network, home network, mobile device, or a public network.

- Protects users and organizations on and off the corporate VPN across all devices including Mobile, Tablet and Laptops.
- Architected to help comply with existing corporate security controls and acceptable use policies by redirecting the user's browser to safe destinations rather than acting like a proxy service.

End-to-End Insights

Proofpoint Threat Insight Service provides increased visibility and a real-time view to administrators and security professionals, to see how many and what types of threats are currently being received. It includes a web-based graphical threat analysis dashboard that provides data at an organizational-level, threat-level, and user-level helping to take immediate action, if required. Proofpoint's Threat Insight Service dashboard enables organizations to know critical information like:

- Is our organization under attack?
- Who is being targeted and what threats have been received?
- What is the status of each threat? Have we blocked it? Or, have they been neutralized? Or, are they still valid threats?



Find out exactly ***when*** the threat hit your system.

Know ***what*** went through your system.

Get more details about ***what*** made it through.

Find out specifically ***who*** was hit by the threat.

Proofpoint Provides Complete Protection

- Provides complete protection against advanced threats with URL Defense Service and Attachment Defense Service.
- Works together with Proofpoint Enterprise Protection to provide complete protection against all email threats.
- Protect sensitive and confidential data with Proofpoint Enterprise Privacy to accurately detect both structured and unstructured data to be secured with an integrated email encryption solution.

proofpoint™

Proofpoint, Inc.
892 Ross Drive, Sunnyvale, CA 94089
Tel: +1 408 517 4710
www.proofpoint.com