proofpoint

Proofpoint Essentials URL Defense

Advanced Protection with Proofpoint's Targeted Attack Protection

Highlights

- Proofpoint Essentials leverages Proofpoint's Targeted Attack Protection Technology to provide complete protection against all email threats.
- Cloud Architecture: Billions of messages traverse the Proofpoint cloud every week, providing global visibility and early protection for emerging threats
- Advanced Protection against targeted email attacks like spear-phishing attacks, zero-day exploits, advanced persistent threats (APTs)
- Use of techniques like Dynamic Malware Analysis
- Protection across the corporate network, public network, and mobile devices
- Leverage Big Data techniques to build statistical models to provide predictive analysis

.

Proofpoint Essentials leverages the advanced power of Targeted Attack Protection, Proofpoint's Industry Leading email analysis solution, to provide small to mid-sized enterprises with URL Defense, the only service that effectively detects, catches and analyses malicious URLs targeting this market.

Targeted email attacks containing malicious links represent one of the most dangerous IT threats facing enterprises today. Proofpoint Targeted Attack Protection™ is the industry's first comprehensive email analysis 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.

The Proofpoint Essentials URL Defense feature takes a more advanced approach to identifying suspicious email messages containing malicious URLs. This helps small to mid-sized enterprises to add additional layers of security scrutiny that cannot be matched by traditional security solutions and gateways.

Why do small and medium enterprises need URL Defense?

Small to mid-sized enterprises are easier targets for cyber criminals because they are generally protected by less sophisticated software or they are not protected at all. Unfortunately email attackers have worked this out and now realise that targeting a smaller enterprise can actually mean a bigger reward in the end.

What is worse is that no matter the training provided to staff at any enterprise, users are still falling for these targeted email attacks as they get more sophisticated. Proofpoint research has found that on average, 1 in 10 users that receive email messages with malicious URLs will click on these URLs. Frequently, Proofpoint has observed that malware used in these attacks remain undetected by less than 10% of traditional AV and reputation solutions, even hours after the attack.

Predictive Analysis

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

- Modeling user's email patterns and building behavioral history of that specific user to determine which email is suspicious and anomalous.
- 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 with the help of real time scoring against this statistical model.

Key Benefit: Proactively identifies threats and minimizes clean-up for incident response teams by catching malicious URLs before users click and get infected.

Advanced Malware Detection

Proofpoint 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

Key Benefit: Cloud scale and elasticity for malware analysis with global and immediate benefit to all organizations for emerging campaigns, with proprietary technology to defeat malware through counter-evasion techniques.

Real-time Dynamic Analysis

Proofpoint 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 this feature, 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.

Key Benefit: Enables security controls to persist, even if users are off the corporate network and bypassing on-premise security controls.