proofpoint

Proofpoint Essentials

Attachment Defense

Highlights

- Proofpoint Essentials leverages Proofpoint's Targeted Attack Protection Technology to provide protection against all malicious attachments
- Cloud Architecture: Billions of messages traverse the Proofpoint cloud every day, providing global visibility and early protection for emerging threats
- 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

Advanced Protection with Proofpoint's Targeted Attack Protection

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 Attachment Defense to effectively detect malicious attachments targeting this market.

Why do Small and Medium Enterprises need Attachment Defense?

Cybercriminals are profit-driven businesses that focus their resources on techniques and tools that deliver the greatest return on investment. Small to medium enterprises are often seen as easier targets because they are generally protected by less sophisticated software or in some cases not protected at all. Unfortunately attackers have worked this out and now realize that targeting a smaller enterprise can actually mean an easier path to reward in the end. Proofpoint research shows that attachment-based campaigns can actually cost cyber criminals 50% less than URL-based attacks, making their return on investment even greater. Phishing campaigns that utilized document attachments increased by 1,500% over 2014 to 2015 to exploit of this financial advantage.

Proofpoint Essentials takes a unique approach to threat detection and email security for SMEs, by taking advantage of our enterprise-class Targeted Attack Protection analysis techniques and a cloud based architecture to identify and block suspicious messages. This helps small and medium enterprises further protect their end users by adding additional layers of security scrutiny that cannot be matched by traditional email security solutions and gateways.

Advanced Malware Detection

Attachment Defense uses the visibility and intelligence gathered from analyzing the email of many of the largest companies in the world and applies this to smaller enterprises. This enables SMEs to take advantage of the scale and security capabilities of Proofpoint, without having to dedicate resources to managing the system.

The Attachment Defense capability within Proofpoint Essentials leverages dynamic sandbox technology that powers the Proofpoint Targeted Attack Protection solution. Intelligence gathered by the dynamic malware analysis is used to identify and block malicious attachments that are designed to evade traditional security solutions. These attachments, such as Microsoft Office documents, are often used in spear-phishing attacks, to deliver banking Trojans, ransomware, or other malware.

Proofpoint ensures all aspects of Attachment Defense meets the security, availability, and resiliency needs of the smaller enterprise.

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