Protect Against Malicious Network Traffic

Discover how F5 and OPSWAT deliver scalable advanced threat prevention by detecting and preventing malicious files on enterprise applications.

Overview

F5 and OPSWAT have teamed up to offer a complete solution for securing web traffic and keeping networks secure. The F5® BIG-IP® product line offers the superior application intelligence that network managers need to ensure applications are fast, secure, and available. Combined with the OPSWAT MetaDefender advanced threat prevention platform, the joint solution ensures that any files passing through BIG-IP products are free of threats.

F5 and OPSWAT Joint Security Solution

MetaDefender ICAP Server uses the Internet Content Adaptation Protocol (ICAP) to integrate with F5 BIG-IP Local Traffic Manager™ (LTM) and F5 Advanced Web Application Firewall™. Together, they provide advanced threat prevention using industry-leading multi-scanning, vulnerability assessment, and content disarm and reconstruction (CDR) technology.

MetaDefender protects web applications that use BIG-IP products for traffic management by preventing advanced threats such as ransomware, macro-enabled productivity documents, and malicious hyperlinks that lead to web drive-by downloads of Trojans and other malware.

MetaDefender prevents unknown threats and zero-day attacks by removing any possible malicious content from files and detecting vulnerabilities in software applications. In addition, by leveraging over 30 anti-malware engines, MetaDefender increases detection rates of known threats to nearly 100%.

KEY BENEFITS:

• Detect and prevent malicious file upload attacks on web applications using BIG-IP products for scale and availability.

• Remove embedded threats not detected by anti-malware engines, including zero-day targeted attacks, using CDR technology.

• Deploy over 30 anti-malware engines for the highest malware detection rate and shortest window of exposure to malware outbreaks.

• Detect vulnerabilities in files passing through BIG-IP products for more than 20,000 software applications using over one billion hashes.
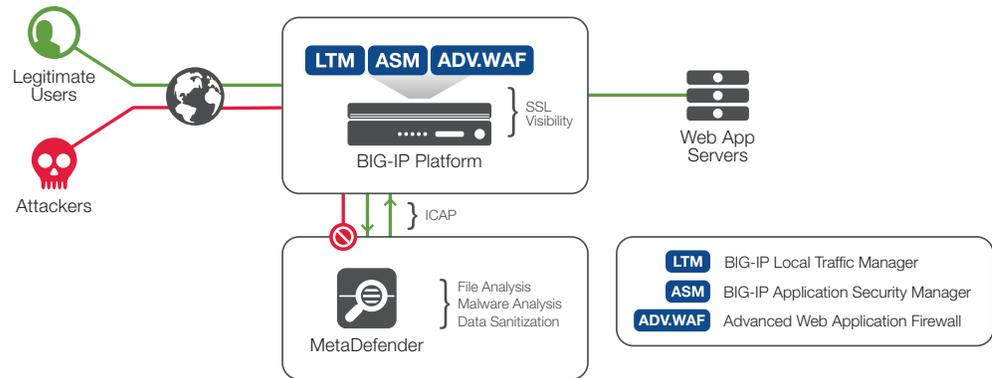
• Deploy fast via ICAP, no development time required.

Figure 1: F5 and OPSWAT Advanced Threat Prevention

Building a Scalable Architecture to Stop Attacks

Enterprises with substantial traffic loads can optimize OPSWAT deployments by using the health monitoring and load-balancing capabilities of the BIG-IP platform. Along with MetaDefender's high-performance architecture, the joint solution can protect against advanced persistent threats (APTs) in the most demanding application environments.

Enhanced Security Architecture

The integration of F5's SSL inspection and URL filtering with OPSWAT's product provides a foundation for enhanced security. For example, the SSL visibility and control, performance, and scale benefits can be extended to other offerings, including F5 Advanced WAF and F5 SSL Orchestrator™.

To find out how F5 and OPSWAT joint solutions can help your business, visit f5.com/solutions/technology-alliances or opswat.com/partners/f5.