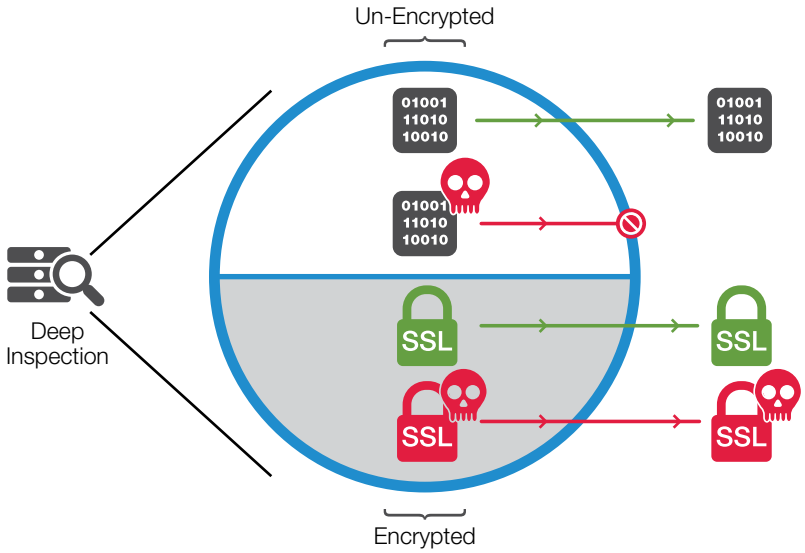
Advanced Threat Protection with F5 and FireEye

Uptime, Scale, and SSL Visibility

Discover how F5 and FireEye deliver scalable advanced threat protection to identify and stop malicious activity targeting enterprise applications.

As Defenses Evolve, Attackers Adapt and Innovate

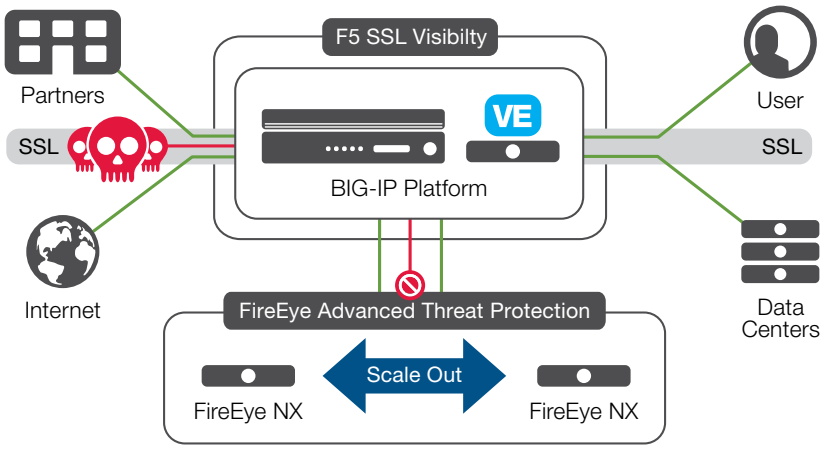
Cyber criminals are growing more sophisticated and evasive in their attacks. As SSL becomes the de-facto standard for all Internet traffic, hidden threats such as malware pose a risk to uninspected SSL traffic. Attackers use novel techniques to deploy and hide web-based malware. Because traditional network architectures are built for little or no encryption, attackers plant SSL-encrypted malware on compromised servers to evade network monitoring. Without security tools to inspect SSL traffic, attacker actions can go undetected.



SSL is the new, rapidly growing threat vector that attackers are leveraging to encapsulate attacks and avoid detection.

F5 and FireEye Joint Security Solutions

Accelerate your business growth without increasing the risk of cyber breaches. Comprehensive perimeter security solutions from F5 and FireEye provide threat protection, application delivery, and best-of-class products integration. These joint solutions offer the highest service availability and performance with the most effective technology, intelligence, and expertise to identify and stop malicious activity.



FireEye and F5 provide advanced threat protection.

F5 and FireEye joint solutions allow you to find hidden threats with SSL visibility, deliver advanced threat protection with greater scalability, and improve operation efficiency with enhanced architecture.

Other key benefits include:

- Increasing threat protection and performance with SSL hardware acceleration.
- Eliminating single points of failure while having control to scale your environment.
- Blocking malicious files and communications to prevent data theft and cyber attacks.
- Combining traditional rule and policy engines with heuristic detection to identify and stop sophisticated attacks.

FireEye Network Threat Prevention Platform

The FireEye Network Threat Prevention Platform identifies and blocks zero-day web exploits, droppers (binaries), and multi-protocol callbacks to help organizations scale their advanced threat defenses. FireEye Network with Intrusion Prevention System (IPS) technology further optimizes spend, substantially reduces false positives, and enables compliance while driving security across known and unknown threats.

Cyber criminals use the web as a primary threat vector to deliver zero-day exploits and malicious URLs in email and exfiltrate data. The FireEye Network is designed to stop drive-by downloads and blended web and email attacks.

Learn More

For more information about F5 and FireEye, visit f5.com/fireeye.

Web Pages

F5 SSL Everywhere Reference Architecture

FireEye Network Security

Recommended Practices

Advanced Threat Protection with FireEye and F5

Deployment Guide

F5 iApp: Air Gap Inspection with SSL Intercept

Building a Scalable Architecture to Stop Attacks

F5 helps provide effective, comprehensive, and resilient network security solutions for the FireEye Network. More than any other alternative, F5 and FireEye joint solutions offer the fastest, most effective, and always-on protection against all types of cyber attacks.

Finding hidden threats with SSL visibility

Leveraging the URL filtering and SSL inspection capabilities of the F5® BIG-IP® platform, select traffic can be decrypted, inspected by FireEye NX appliances, and then re-encrypted. This delivers enhanced visibility to potential threats traversing the network.

Performance, scale, and high availability in heavy network traffic environments

Enterprises with substantial traffic loads can optimize FireEye deployments by using the health monitoring, load-balancing, and SSL offload capabilities of the BIG-IP platform. This enables FireEye to scale and protect against Advanced Persistent Threats (APTs) in the most demanding application environments.

Enhanced security architecture

The F5 SSL inspection, URL filtering, and FireEye NX integration provide a foundation for enhanced security. For example, the SSL visibility and control, performance, and scale benefits can be extended to other offerings, including F5's on-premises web application firewall, BIG-IP® Application Security Manager™ (ASM)—and FireEye's intrusion prevention system, FireEye Multi-Vector Virtual Execution (MVX).

To find out how F5 and FireEye joint solutions can help your business, visit f5.com/fireeye.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas info@f5.com
Asia-Pacific apacinfo@f5.com
Europe/Middle East/Africa emeainfo@f5.com
Japan f5j-info@f5.com

Solutions for an application world.