MetaDefender® ICAP Server

Plug-and-Play Malware Prevention Solution for F5 BIG-IP and F5 Distributed Cloud (XC) platforms

Cloud transformation is driving the adoption of web applications that accept file uploads for a wide array of use cases: B2B file transfers, client personal data handling, and other functions essential to maintaining business continuity.

However, this functionality also opens a new threat vector for ransomware and other malicious content to invade your organizations.

OPSWAT and F5 have partnered to deliver powerful anti-malware defense capabilities for critical infrastructure environments. Analyze, detect and block malicious files before they reach web applications, enabling organizations to reduce web application attacks and secure network. Together, F5 and OPSWAT help customers to fulfill their portion of the shared responsibilities in cybersecurity.

The Problem

- The needs for securing files entering network against malware, zero-day attacks, file-based vulnerabilities, and data loss.
- Network security appliances effectively safeguard the environment against network-based attacks. However, they do not inspect the file contents moving through the network traffic.
- Environments handling sensitive data need a comprehensive solution to protect their web applications and cloud storage from malicious file uploads.
- Complex integrations, high implementation costs.
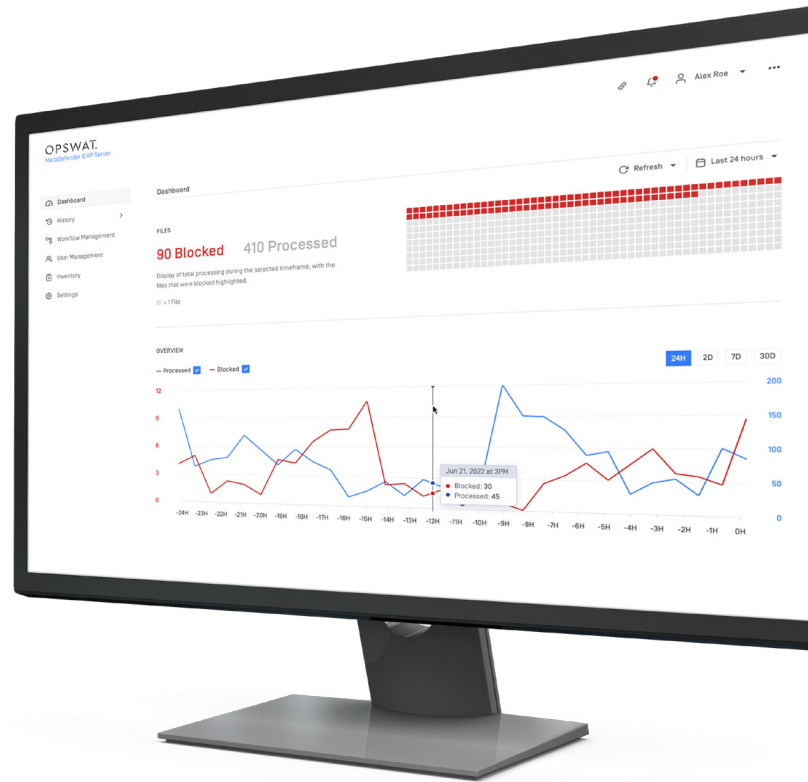
The OPSWAT Solution

Analyze all file upload traffic before it enters your network

- **Multiscanning:** Increase threat detection rate to nearly 100% with 30+ antivirus engines.
- **Deep CDR (Content Disarm and Reconstruction):** Prevent zero-day and advanced targeted attacks.
- **Proactive DLP (Data Loss Prevention):** Prevent data breaches and maintain regulatory compliances.
- **Sandbox:** Adaptive threat analysis technology enables zero-day malware detection and extracts indicators of compromise (IOCs).
- **SBOM (Software Bill of Materials):** Identify known vulnerabilities, validate licenses, and generate component inventory for open-source software (OSS), third-party dependencies, and containers.
- **Vulnerability Assessment:** Detect application and file-based vulnerabilities before they are installed.
- **Plug and Play:** Integrating into your existing infrastructure via ICAP takes less than five minutes, with no architecture changes.
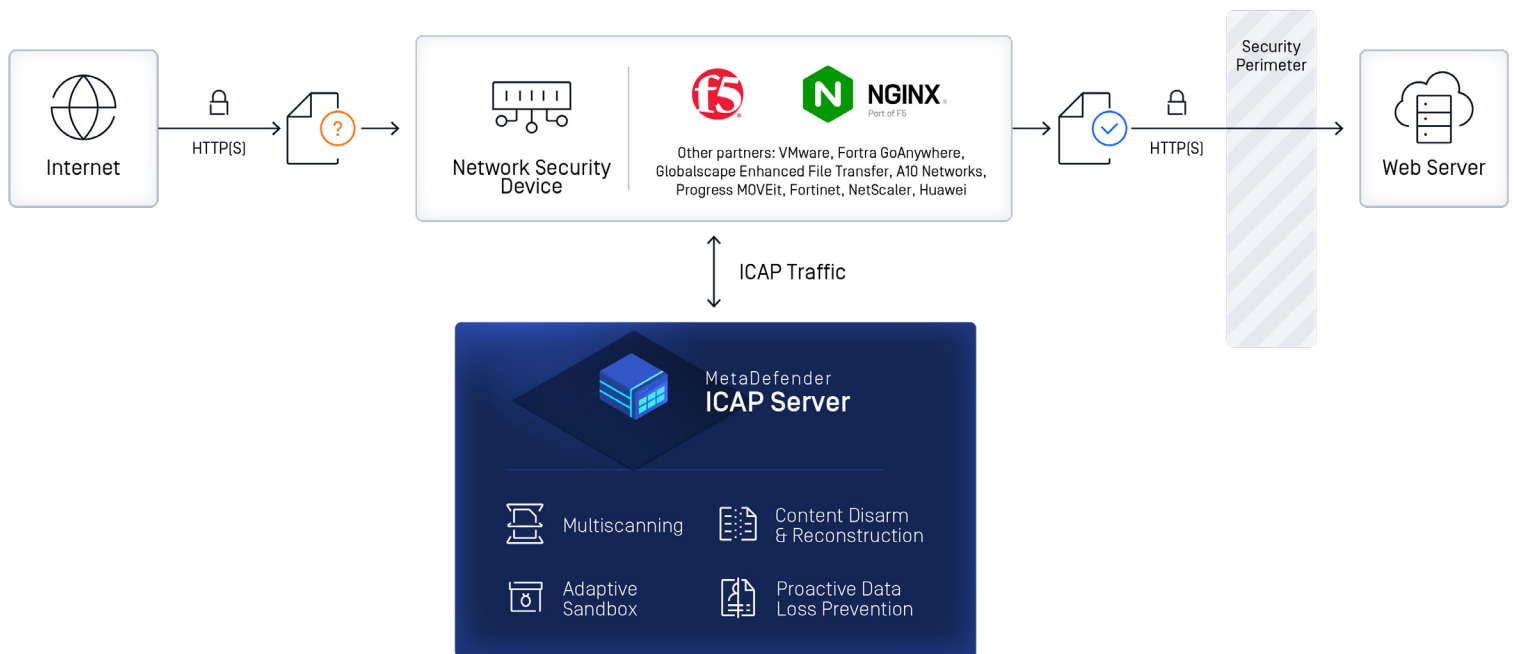
Supported Network Devices

Seamless integration into your existing infrastructure

Reverse and Forward Proxies	Web Application Firewall (WAF)	Next-Gen Firewall (NGFW)
Load Balancer	Secure Web Gateway (SWG)	Application Delivery Controller (ADC)
Managed File Transfer (MFT)	Ingress Controller	

"We've used OPSWAT technology for several years, in multiple integrations and in various products, [and] their reputation in the industry has just been stellar over [that] time. I've worked in the industry for 30 years, and OPSWAT [is] a company I've always trusted and worked well with."

Joe Peck
Senior Director of Product Management at F5®