SOLUTION BRIEF

FortiGate and OPSWAT Security Protection

Broad, Integrated, and Automated Solution for Unmatched File Scanning and Sanitization to Protect Against Zero-day Attacks and Malware

Executive Summary

Fortinet and OPSWAT have partnered to deliver an industry-leading security solution by integrating FortiGate Next-Generation Firewall and MetaDefender Core Platform to provide enterprises with full visibility into uploaded files and advanced protection from malicious threats.

Challenge

An organization's website is a custom portal leading to critical assets inside the network. The success of any organization depends on the seamless sharing and transfer of productivity files. Legitimate users of an organization should be able to share documents and media files without impeding their performance, making it critical to ensure that asset uploads by users don't become a conduit for malware injection into the network.

OPSWAT and Fortinet have established a technology partnership to provide organizations an extra layer of security from malware and potential zero-day attacks. The partnership ensures safeguarding websites from file-borne threats that are capable of compromising databases, penetrating networks, or distributing malicious malware.

Joint Solution Description

Bringing the Fortinet FortiGate and OPSWAT MetaDefender Core products together in an integrated solution delivers advanced data threat protection to organizations.

OPSWAT MetaDefender Core protects organizational data from cybersecurity threats originated from any source, including web, email, portable media, and endpoints. The MetaDefender ICAP Server is the ICAP interface between MetaDefender Core and ICAP clients. As a result, all content routed through the ICAP interface is scanned with the same anti-malware engines and policies as files scanned through other MetaDefender Core interfaces.

Solution Components

- Fortinet FortiGate Next-Generation Firewall
- OPSWAT MetaDefender® Platform

Joint Solution Benefits

- Sanitization of suspicious files using Deep CDR and without compromising usability
- High detection rates and advanced file analysis through FortiGate at the perimeter
- Easy-to-use MetaDefender interface for investigating threats and designing custom workflows, and traffic reports

Fabric-Ready

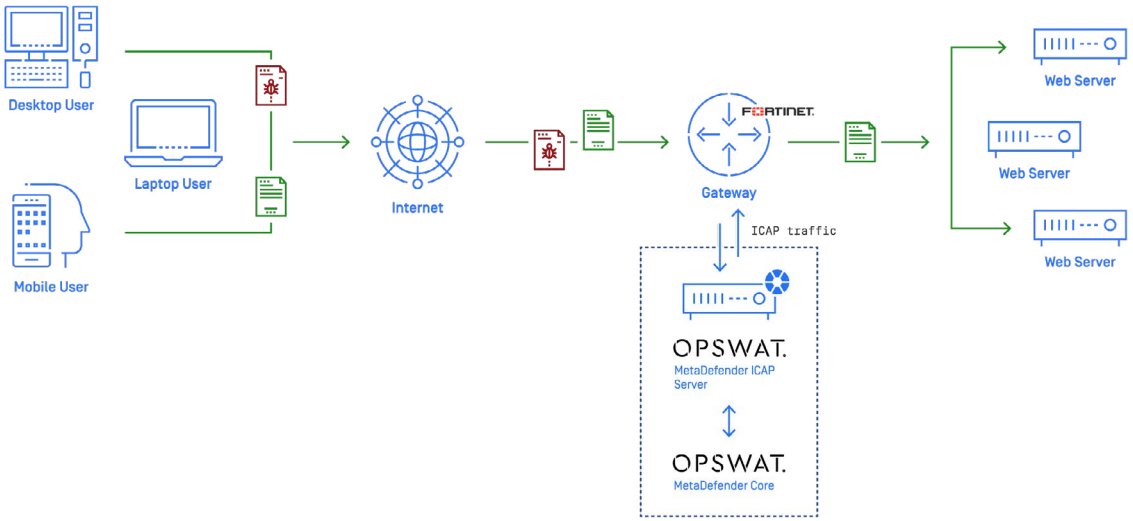

Figure 1: OPSWAT MetaDefender inline integration with the Fortinet FortiGate via ICAP to cleanse malware-infected files.

FortiGate next-generation firewalls (NGFWs) enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. FortiGate firewalls scan and filter network traffic to protect an organization from external threats. The inspections occur at an unparalleled speed, scale, and performance without degrading user experience or creating costly downtime.

MetaDefender Core integrates with an ICAP compatible client via the MetaDefender ICAP Server. Organizations benefit from file scanning from industry-prevalent anti-malware engines, in addition to OPSWAT's Deep Content Disarm and Reconstruction (Deep CDR), and File-Based Vulnerability Assessment for advanced protection. In tandem, Fortinet NGFWs provide the superior ability to inspect traffic and identify attacks, malware, and other threats, which are stopped in their tracks as soon as they are detected.

Joint Solution Components

OPSWAT MetaDefender ICAP Server

MetaDefender ICAP Server protects the network as an add-on security feature to any gateway that speaks ICAP. MetaDefender ICAP Server relays files from the gateway to the MetaDefender Core Security Platform, serving as a portal to MetaDefender Core technologies.

Fortinet FortiGate

FortiGate NGFWs utilize purpose-built security processors and threat-intelligence security services from artificial intelligence (AI)-powered FortiGuard labs to deliver top-rated protection and high-performance inspection of clear-texted and encrypted traffic. NGFWs reduce cost and complexity with full visibility into applications, users, and networks and provide best-of-breed security. Other products that complement FortiGate's security profile include FortiGate Secure Web Gateway and the FortiWeb.

Joint Use Case

Fortinet FortiGate integration with the MetaDefender Core Platform via the MetaDefender ICAP Server allows the FortiGate firewall to offload traffic to a separate server set up for the specialized processing (deep content disarm and reconstruction, and malware and file-based vulnerability scanning) of the incoming traffic. This reduces the resource strain on the firewall.

About OPSWAT

OPSWAT protects critical infrastructure. Our goal is to eliminate malware and zero-day attacks. We believe that every file and every device can pose a threat. Threats must be addressed at all locations at all times—at entry, at exit, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access. The result is productive systems that minimize risk of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.
Learn more at https://www.opswat.com/.

April 22, 2020 1:12 AM

645531-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\OPSWAT\sb-FA-fortigate-and-opswat-security-protection-4172020\sb-FA-fortigate-and-opswat-security-protection-4172020