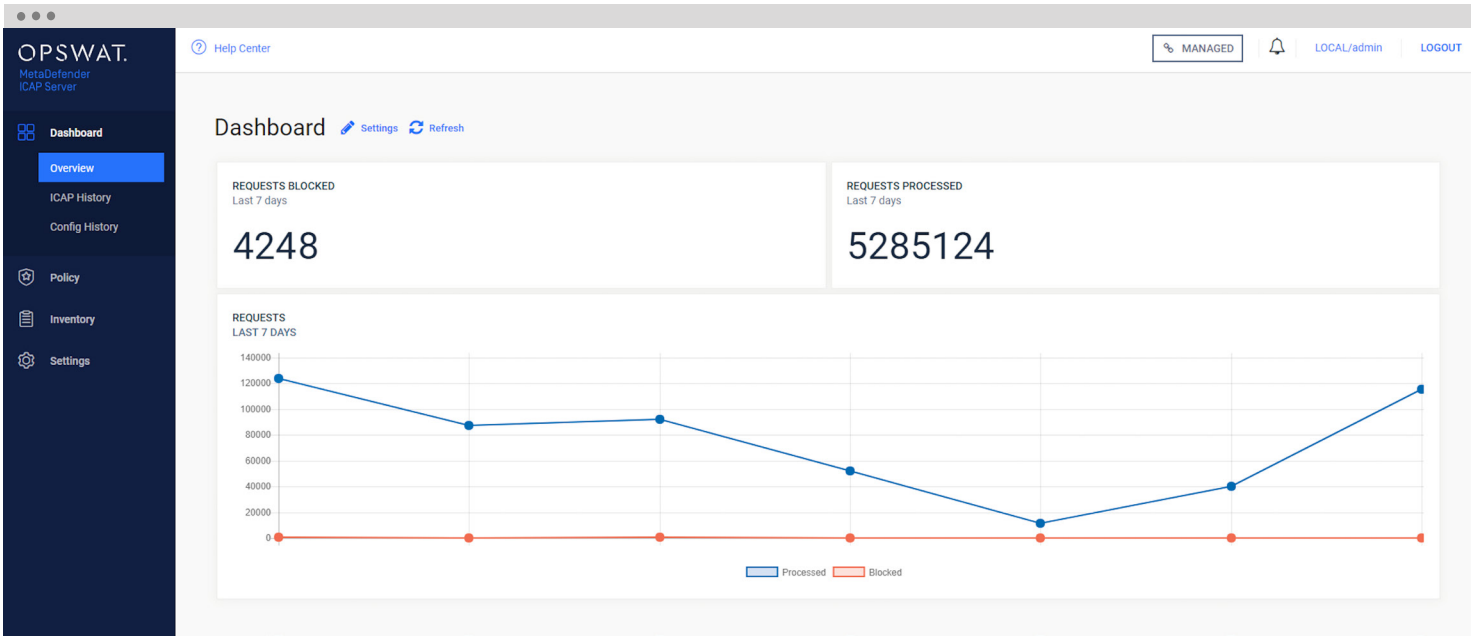
OPSWAT.

MetaDefender® ICAP Server

Advanced Threat Prevention for Network Traffic and Storage Devices

MetaDefender ICAP Server uses the Internet Content Adaptation Protocol (ICAP) to integrate with network appliances to protect against advanced threats in network traffic and storage devices, using industry-leading multi-scanning, vulnerability scanning, and data sanitization, also known as content disarm & reconstruction (CDR) technology. 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%.



Benefits

Protect Uploads - Add enhanced security by integrating MetaDefender ICAP Server with reverse proxies such as load balancers, network application firewalls and application delivery controllers.

Protect Downloads - Prevent the entry of document based malware and exploits coming from the network in forward proxy mode, and gain visibility into the vulnerability levels of installers and executable software applications your users are downloading.

Protect Data on Storage Devices - Prevent malware on storage devices by detecting and preventing known and unknown threats.

Enhance Security Appliance Effectiveness - Add advanced threat protection to Intrusion Prevention Systems and Next Generation Firewalls that support ICAP, such as Check Point, Cisco and others.

Easy Deployment - Integrate MetaDefender with any ICAP-enabled device without the need for coding or developer time.

MetaDefender ICAP Server Features

Data Sanitization (CDR) - Disarm over 30 common file types, and reconstruct each file ensuring full usability with safe content.

Multi-Scanning - Choose from over 30 anti-malware engines in flexible package options.

Vulnerability Scanning - Detect vulnerabilities in over 15,000 software applications using over 1 billion hashes.

Caching - Significantly improve the performance of your network appliance by using MetaDefender's scan results caching.

High Performance - Scalable for any traffic volume with built-in high-performance architecture.

Granular Policies - Configure security rules based on host, client or any HTTP header attributes.

Role Based Configuration - Active Directory and LDAP group-based administrative roles.

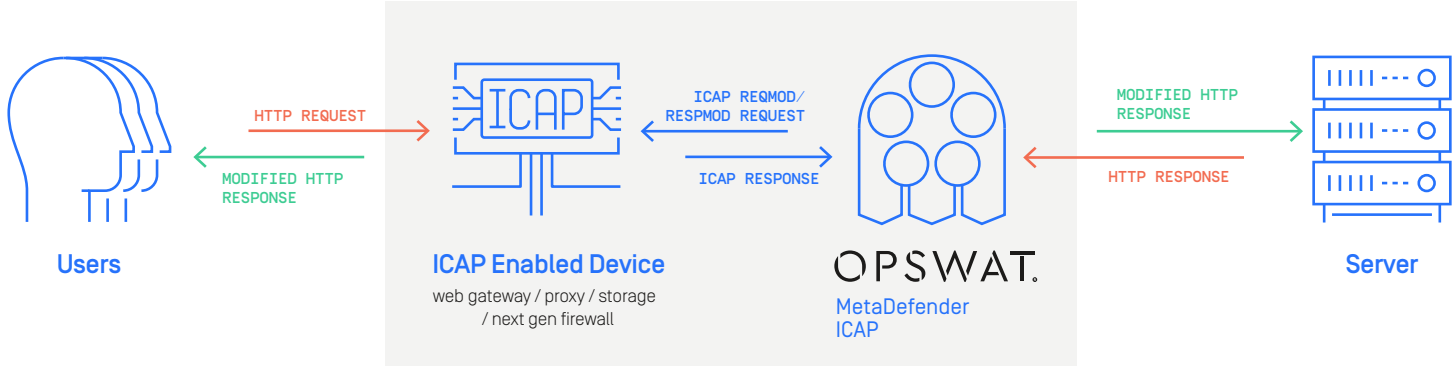
"We've used OPSWAT technology for several years, in multiple integrations and in various products, [and] their reputation in the industry has just been stellar over [that] time. I've worked in the industry for 30 years, and OPSWAT [is] a company I've always trusted and worked well with."

Joe Peck
Senior Director of Product Management, F5®

Deploy with any ICAP Device

MetaDefender ICAP Server can be used with any ICAP-enabled network appliance, including application delivery controllers, network gateways, forward and reverse proxies, attached storage devices, and next-generation firewalls.

System Requirements - 64-bit platform, 2 GB RAM (min), 2 GB free hard disk space + 500MB * [number of scan engines], CentOS 6.6+/7.0+, Red Hat Enterprise Linux 6.6+/7.0+, Debian 7.0+/8.0+, Ubuntu 14.04/16.04, Windows 7+ (64 bit), Microsoft Windows Server 2008 R2 or newer (64 bit).



OPSWAT.
Trust no file. Trust no device.

www.opswat.com