OPSWAT.

Content Inspection in Network Traffic Security

The key to efficient and automated threat prevention for enterprise networks

Network security appliances such as load balancers, proxies, ADCs, or WAFs provide flexibility, visibility, and control to protect organizations from network-based threats. However, they offer little to no capability to inspect the content, data, and files moving through the traffic. Environments handling sensitive data need a comprehensive solution to protect their web applications and cloud storage from malicious file uploads.

Extend Your Network Security with Zero-Trust Content Inspection

MetaDefender ICAP Server seamlessly integrates with any network appliance that supports the Internet Content Adaptation Protocol (ICAP), allowing organizations to quickly assess, analyze, and sanitize any files passing through the system before these files reach the web applications and end-users.

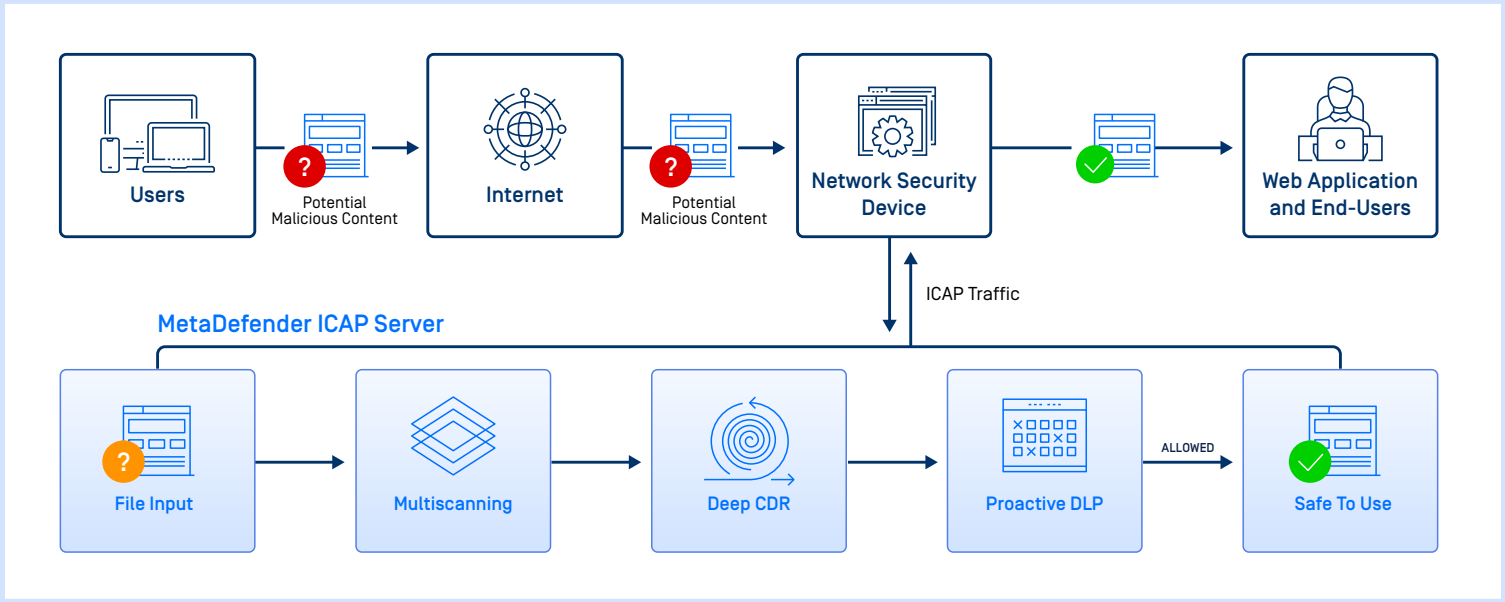
The result: Comprehensive threat detection and prevention that protects organizations from file-borne malware, zero-day attacks, and data loss.

Network Appliances that can be Connected via ICAP

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

OPSWAT.

MetaDefender ICAP Server



The Challenge	The OPSWAT Solution
Network security appliances lack threat prevention features	Zero-trust content inspection through proprietary technologies: multiscanning, data sanitization, and data loss prevention
Complex integration, high implementation costs	▪ Lightweight, frees up resources on the security device ▪ Plug-and-Play solution allows for flexible implementation and deployment with any ICAP-enabled network appliance ▪ Minimized configuration and Total Costs of Services (TCS) ▪ Minimal impact on network performance

MetaDefender ICAP Server Use Cases

Ensure Safe File Uploads

Cybercriminals can upload malicious files or overwrite existing files to distribute malware, demand ransom, or steal sensitive data.

MetaDefender ICAP Server protects web applications from malicious file uploads without negatively impacting the scalability of their services.

Protect Enterprise File Transfer and Storage

Mass transfer of business documents between internal departments, partners, and customers can create opportunities for attackers to move laterally across organizations.

Implement MetaDefender ICAP Server at the central file transfer gateway or repository to add a protection layer to your network.

Secure Web Traffic

Users can be susceptible to social engineering while browsing the web and may visit reputable websites that have been compromised.

MetaDefender ICAP Server screens web traffic before it reaches your organization's network to prevent malicious files from being downloaded by your users.

OPSWAT.

Protecting the World's Critical Infrastructure

For more information
visit opswat.com/products/metadefender/icap

©2021 OPSWAT, Inc. All rights reserved. OPSWAT, MetaDefender, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT, Inc. Revised 2022-Jul-08

OPSWAT.com/contact