OPSWAT.

METADEFENDER ICAP SERVER™

ICAP Server File Security Integrations

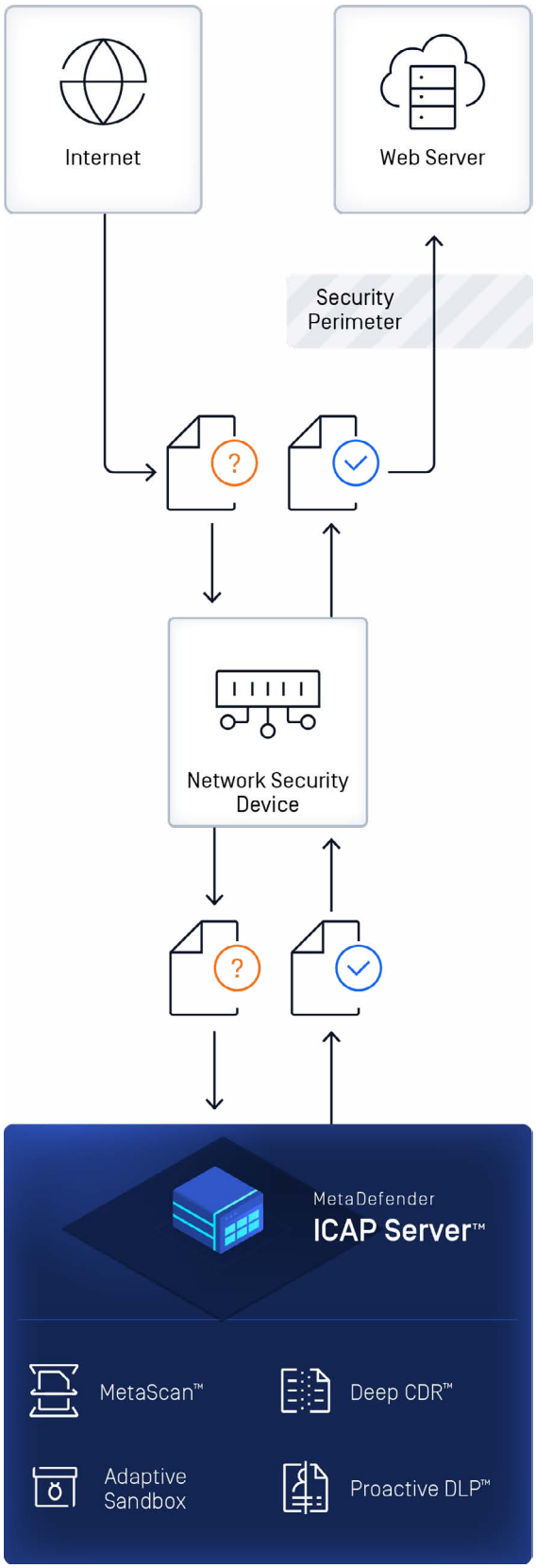
Maximize Network Traffic Security with Content Inspection

Network security appliances – such as load balancers, WAFs (web application firewalls), proxies, or ingress controllers – provide visibility and protection from network-based threats but lack the capability to inspect malicious file content moving through the traffic. Organizations need a robust, defense-in-depth strategy that protects them from these threats.

Extend Your Network Security with Zero-Trust Content Inspection

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

The result: comprehensive threat detection and prevention added on top of your existing IT solutions. Protect against file-borne malware, zero-day attacks, and sensitive data breaches, with no additional development needed.



METADEFENDER ICAP SERVER™

Integrate with any ICAP-enabled device

- Reverse Proxy
- Forward Proxy
- Load Balancer
- SWG (Secure Web Gateway)
- ADC (Application Delivery Controller)
- SSL (Secure Sockets Layer) Inspector
- Storage Solution
- MFT (Managed File Transfer)
- Ingress Controller
- NGFW (Next-Gen Firewall)
- IPS (Intrusion Prevention System)
- WAF (Web Application Firewall)

Defense in Depth for your Organization

Plug and Play

Simple integration that takes approximately 5 minutes. Eliminate the hassle of developing and maintaining API integration.

MetaScan™ Multiscanning

Leverages 30+ leading anti-malware engines to proactively detect over 99% of malware threats.

Deep CDR™

Preventative technology that removes potentially malicious content and regenerates safe-to-use files, eliminating APTs and zero-day attacks, and obfuscating malware before delivery.

Proactive DLP™

Prevents sensitive and confidential information from leaving or entering the company's systems by content-checking files before they are transferred.

Adaptive Sandbox

Features threat agnostic analysis of files and URLs, identifying valuable IOCs (indicators of compromise) for incident response.

File Uploads

F5, NGINX, Trellix, Squid, IBM, Symantec by Broadcom, netscaler, FORTINET, vmware by Broadcom, A10

File Transfers

IBM, axway, netscaler, FORTRA GoAnywhere, SEEBURGER Business Integration, globalscape securely connected, Progress MOVEit, NUTANIX, AIRLOCK Secure Access Hub, Cyolo

File Sharing

DELL EMC ISILON, FILECLOUD, HUAWEI

OPSWAT.

Protecting the World's Critical Infrastructure

For more information on MetaDefender ICAP Server, visit opswat.com/products/metadefender/icap

Schedule a demo with a cybersecurity expert at opswat.com/contact