OPSWAT.

SOLUTION BRIEF

MetaDefender® ICAP Server and F5 NGINX

Protect Modern Applications Against Malicious File Uploads

MetaDefender ICAP Server seamlessly integrates with NGINX via a certified dynamic module. The joint solution protects enterprise networks from malware by inspecting all incoming files uploaded to the web for potential threats.

Risks and Challenges

Modern cloud-native and hybrid-cloud environments enable organizations to deploy highly performant, feature-rich applications at scale. The benefits of these technologies are undeniable, but so are the increased security risks organizations face.

Containerized, cloud-based systems that allow file transfers are susceptible to malicious document uploads, ransomware, data breaches, and supply chain attacks causing reputational damage and lost revenue.

- Modern applications deployed in containerized environments can be vulnerable to cyberattacks such as malware, DDoS, or data leaks
- File upload vulnerabilities are a common attack vector targeting web applications
- Without data sanitization, malicious files can slip past an organization's network perimeter into their environments
- Sensitive and confidential data can be stolen or inadvertently transferred outside of organizations, resulting in data breaches and compliance violations

Strengthen Cybersecurity Posture with Shared Responsibilities

Organizations using NGINX Plus or NGINX Open Source can implement MetaDefender ICAP Server to add an additional threat prevention layer on top of their existing infrastructure.

F5 NGINX provides a cloud-native reverse proxy, load balancer, web server and API gateway platform for fast application delivery.

OPSWAT MetaDefender ICAP Server easily integrates with NGINX to protect containerized applications against file-borne malware, known and unknown threats, sensitive data leaks, and application file vulnerabilities.

OPSWAT.

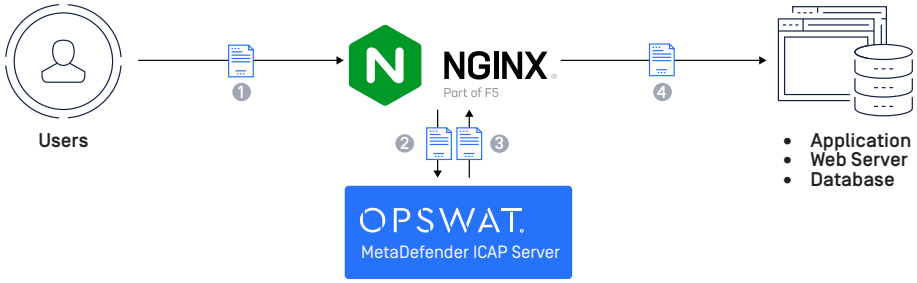
SOLUTION BRIEF

Key Benefits

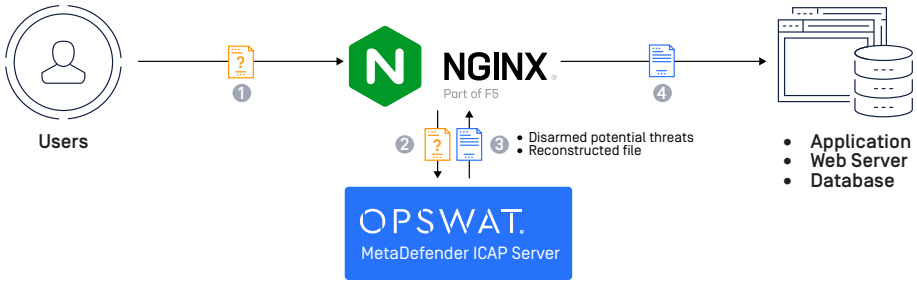
- All-in-one reverse proxy, load balancer, API gateway, web server, and content cache
- Detect malware to nearly 99% rate using simultaneous analysis with 30+ antivirus engines
- Remove zero-day threats by disarming all potentially malicious content in nested archives and other complex files
- Manage compliance and keep sensitive data private
- NGINX-certified dynamic module easily integrates to your existing deployment stack

Workflows

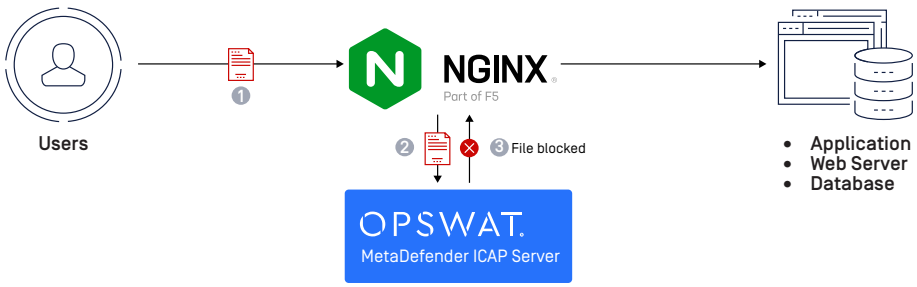
Allow clean files



Sanitize file content



Block malicious files



About MetaDefender ICAP Server

OPSWAT MetaDefender ICAP Server provides a plug-and-play, multi-layered, and robust solution to protect enterprise networks from malicious file uploads.

The solution can be seamlessly integrated into any network appliances supporting an ICAP client:

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

** Native integration