

The background is a dark blue space filled with abstract digital elements. On the right side, a large, dense cluster of blue and white rectangular blocks, resembling data or code, extends from the top right towards the center. A network of thin, glowing blue lines connects various points across the image. In the lower right, a series of red rectangular blocks and lines form a curved, funnel-like shape, suggesting a flow or a specific data path. The overall effect is one of high-tech, digital connectivity and data processing.

OPSWAT.

File Upload Security

Detect, analyze and eliminate threats and zero-day attacks from malicious file uploads



Business and Technical Challenges

With malicious file uploads, attackers can compromise your servers or your entire system. This can result in leaked sensitive data or high ransom payouts to cybercriminals.

Since limiting file transfers from internal or external parties is not an option, organizations need to take protective measures before accepting incoming files. When traditional signature-based and behavior-based detection mechanisms are insufficient to prevent advanced threats and zero-day attacks, many organizations attempt to protect their systems with an in-house set of security tools. However, these can be costly, time-consuming, and add a lot of overhead for maintenance and upgrades.

Table of Contents

- 01 OPSWAT MetaDefender Platform Solutions
- 02 Six Best Practices to Prevent File Upload Vulnerabilities
- 03 Key Differentiators
- 04 How We Can Help
- 05 Integration and Deployment
- 06 Internet Content Adaptation Protocol (ICAP)
- 07 MetaDefender Core Container

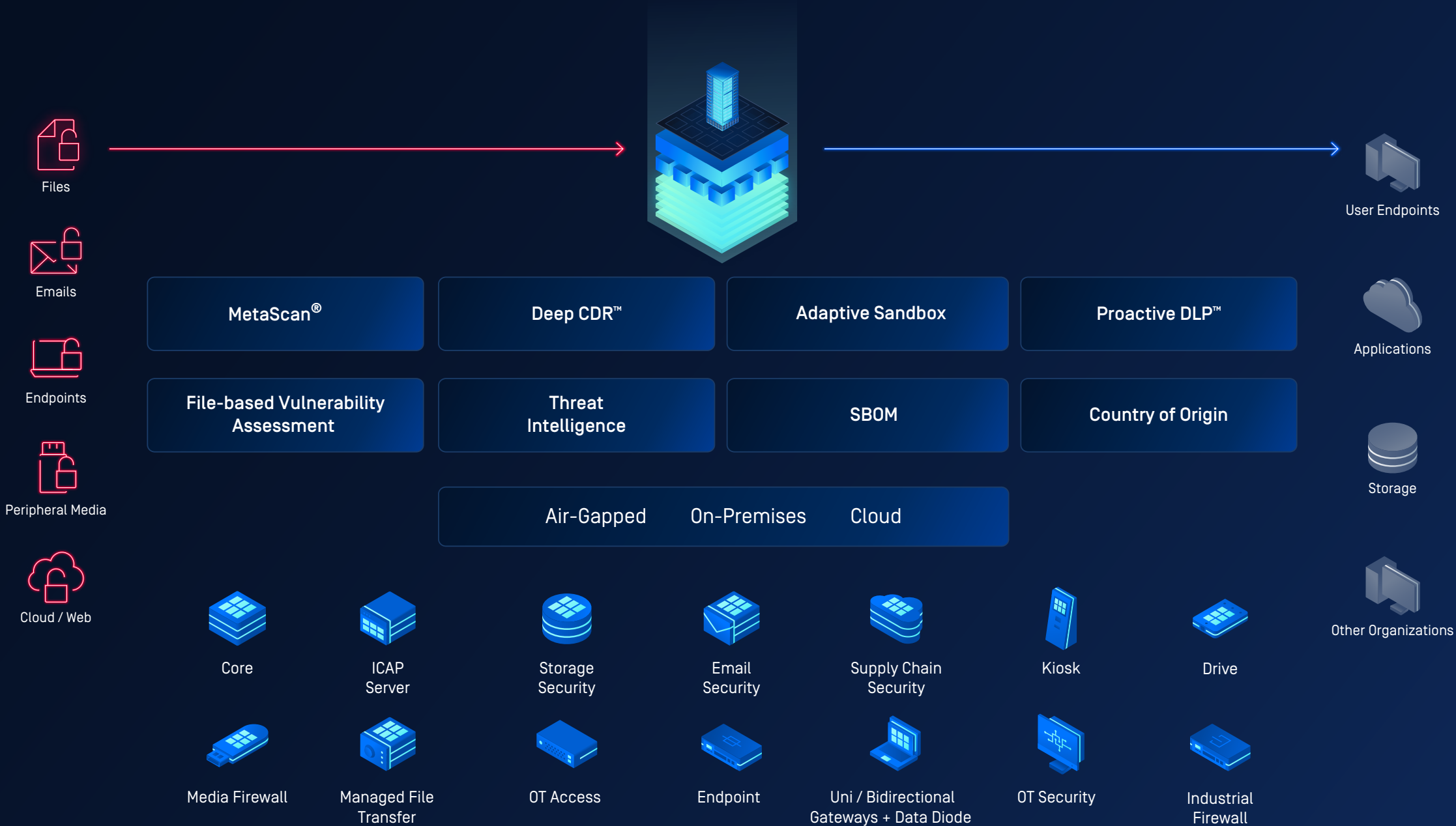
01

OPSWAT MetaDefender™ Solutions

Comprehensive and Multilayered File Upload Security

OPSWAT is committed to preventing malware and zero-day attacks to secure data transfer across your network, applications, and customer operations. With more than two decades of experience in securing critical infrastructure systems, OPSWAT integrates advanced malware protection and detection technologies into your IT infrastructure.


MetaDefender Core—our advanced threat prevention platform for file uploads—has been used by organizations that require the highest level of security, including critical infrastructure, government agencies, and financial institutions.




02

Six Best Practices


Preventing File Upload Vulnerabilities




Remove potential threats embedded in files




Verify file types to prevent spoofing




Scan files with multiple anti-malware engines



Restrict specific file extensions




Check for vulnerabilities in files




Authenticate users

03


Key Differentiators




Advanced Threat Detection and Prevention Technologies
MetaDefender Core is a comprehensive cybersecurity solution powered by technologies like MetaScan and Deep CDR, which detect and prevent both known and unknown threats.



High Performance and Scalability
Fast scanning and regeneration of files in milliseconds without affecting performance. Scalability to any volume with our built-in high-performance architecture and load balancing features.



Simple and Flexible Deployment
Use RESTful API or ICAP (Internet Content Adaptation Protocol) for flexible and secure deployment on-premises and in the cloud.



Customizable Policies
Configurable workflows and analysis rules based on user, file source, and file type.

04

How We Can Help

Detect Nearly 100% of Malware

MetaScan simultaneously scans files with 30+ anti-malware engines* and provides the earliest protection against malware outbreaks with a near-100% detection rate.

*Maximum engine package.

Protect Sensitive and Important Information

Proactive DLP secures your data by examining uploaded files for sensitive information, including personally identifiable information (PII), personal healthcare information (PHI), and DICOM images. Suspicious content can be blocked or removed before it reaches its destination or leaves your environment.

Maximize Vulnerability Detection

Numerous organizations are exposed to attacks leveraging file vulnerabilities. Uploaded files can trigger vulnerabilities in libraries or applications. OPSWAT File-Based Vulnerability Assessment technology detects vulnerabilities in installers and binary files at the gateway of your network, before they enter your organization.

Prevent Zero-Day Attacks

Deep CDR technology, rated 100% effective by SE Labs for protection and accuracy, prevents potentially undetected file-borne attacks by sanitizing and regenerating new, safe-to-use files, ensuring that any possible embedded threats are neutralized while maintaining full usability with safe content.

Meet Compliance Requirements

Adherence to strict regulations like GDPR, PCI DSS, and HIPAA is crucial for preventing data breaches. Meeting these compliance standards can be challenging and costly. OPSWAT provides technologies to streamline compliance processes, offer complete visibility, and generate detailed reports to meet industry benchmarks, including OWASP guidelines.

Threat Analysis with Adaptive Sandbox

Adaptive Sandbox provides fast, accurate malware analysis and actionable threat intelligence. It utilizes adaptive threat analysis to detect and analyze the most evasive, targeted malware. It also uses machine learning-powered similarity search, enabling security teams to investigate and detect new and evolving threats and proactively search for indicators of compromise (IOCs) and potential vulnerabilities.

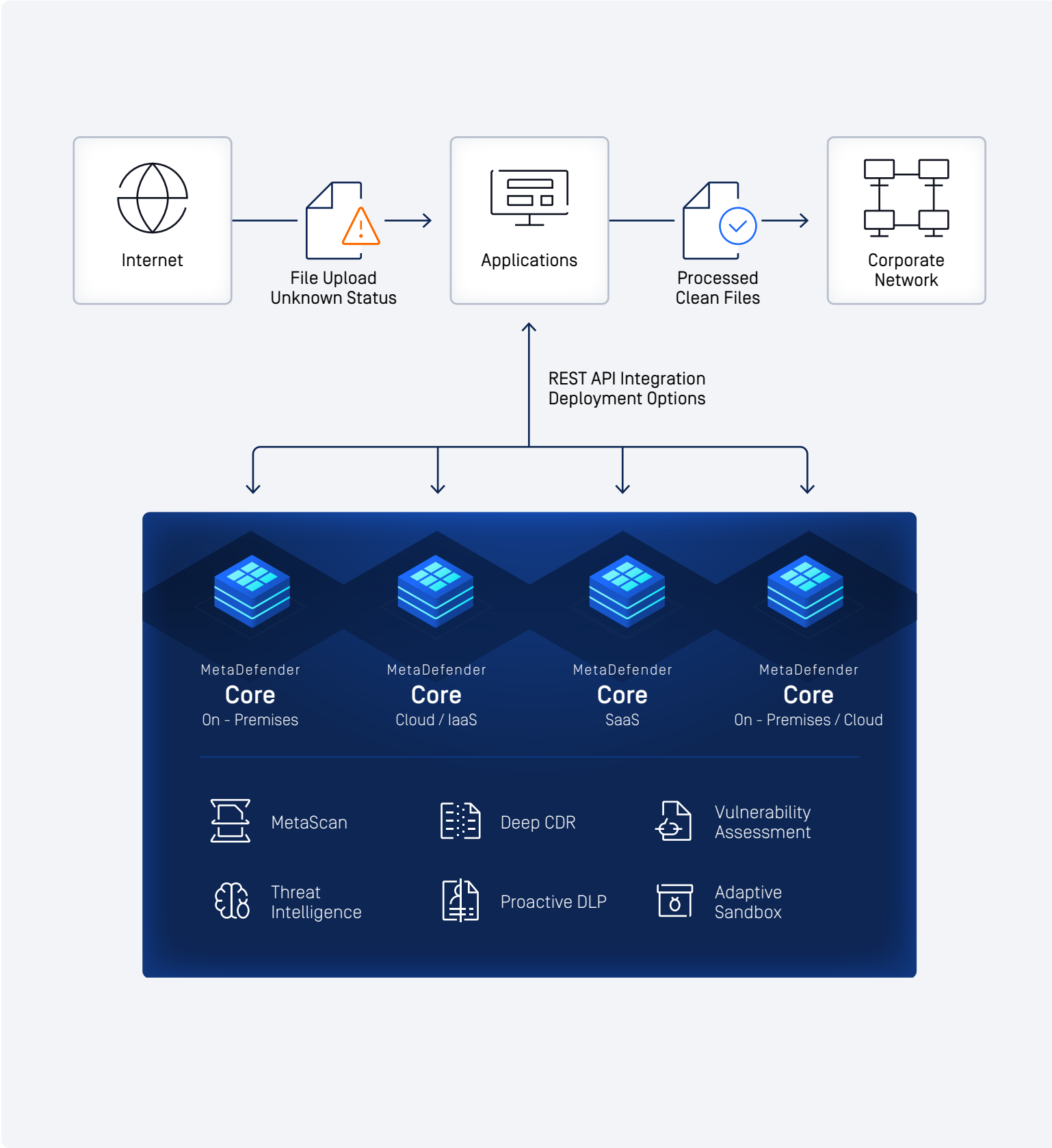
Integration and Deployment

OPSWAT MetaDefender Core can be deployed on-premises, within your cloud infrastructure or by integration with MetaDefender Cloud. Depending on where the data lives, we offer native connectors or the ability to integrate via REST API that supports a variety of deployment scenarios.

- **On-Premises** :For on-premises deployments with strict constraints, MetaDefender Core is often the best solution.
- **SaaS**: If you need MetaDefender Core to integrate with SaaS products, consider MetaDefender Cloud for easy scalability, 24/7 availability, and minimal overhead.
- **Cloud/IaaS**: If you'd like to deploy in an IaaS environment, still consider MetaDefender Cloud, but if you're sending files outside your organization, MetaDefender Core can be deployed in a cloud environment. For AWS deployments, consider MetaDefender AMI for seamless scalability that is easy to implement.

Benefits

- Comprehensive Protection**
Mitigating risks on your critical systems and preventing threats that may have bypassed defenses.
- Custom Security Policies and Workflows**
Enabling administrators to create multiple workflows to handle different security policies based on user, file source, and file type.
- Continuous Visibility and Control**
A centralized UI with a real-time visual security status dashboard, providing complete visibility to your assets and immediately alerting you of potential threats
- Low Total Cost of Ownership (TCO)**
Flexible offerings to provide beneficial TCO. Powerful control over cybersecurity through a single platform that results in a higher ROI, higher adoption, lower overhead, and fewer trained professionals need to oversee complex systems.



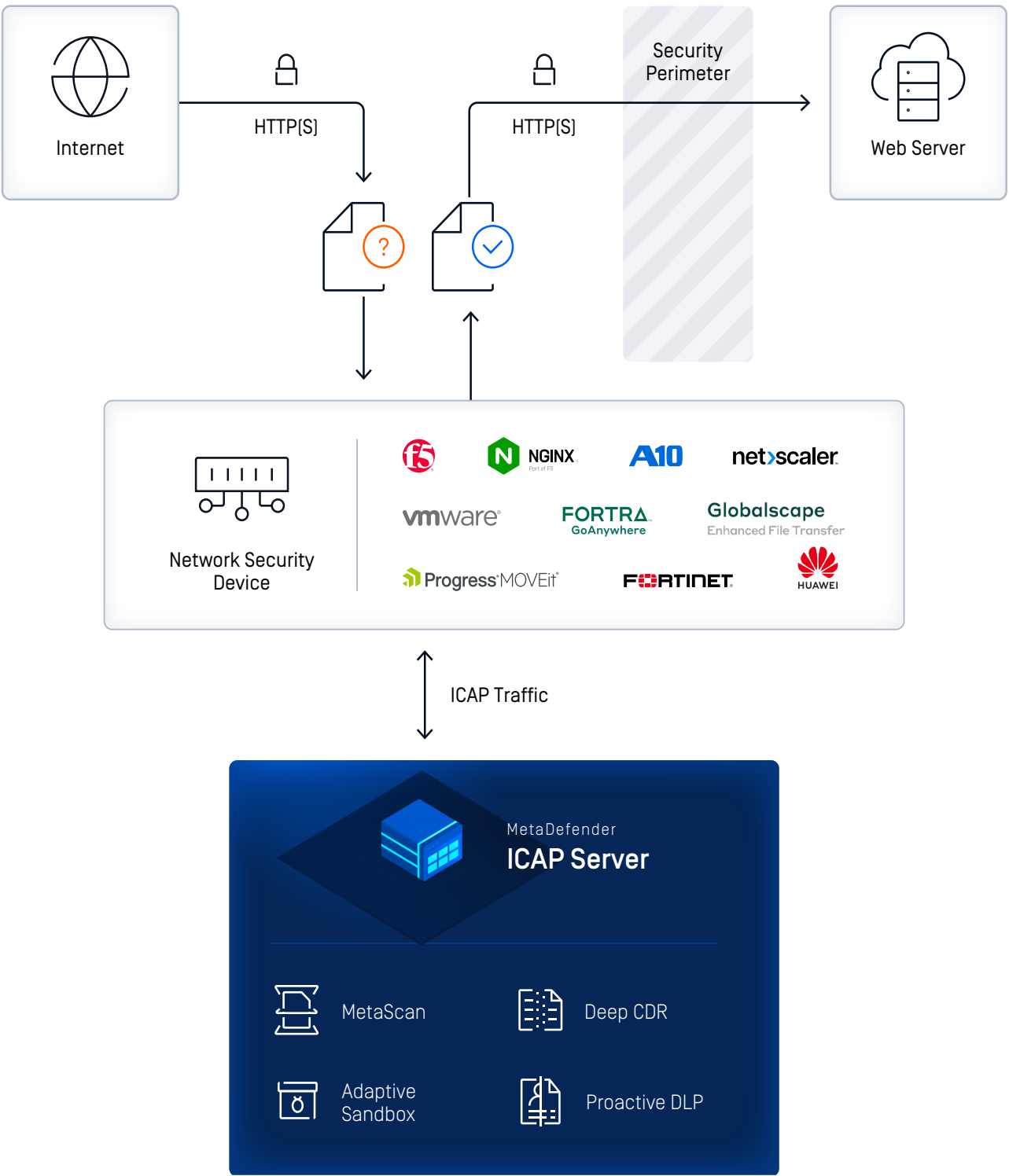
06

ICAP [Internet Content Adaptation Protocol]

For IT environments using network security appliances, MetaDefender ICAP Server offers seamless, native integration to enhance file security at the network perimeter. This plug-and-play solution supports any ICAP-enabled devices, including web application firewalls (WAFs), load balancers, managed file transfers (MFTs), ingress controllers, reverse and forward proxies, intrusion prevention systems, and more.

ICAP-Enabled Devices

- F5 BIG-IP: Advanced WAF ASM, LTM, SSL Orchestrator, NGINX Plus, NGINX Open Source
 - A10 Networks Thunder SSLi
 - Fortra: GoAnywhere MFT, GlobalScape MFT
- Progress MOVEit MFT
 - NetScaler ADC
 - VMware Avi Vantage
 - Nutanix Files
- Fortinet Fortigate
 - and more

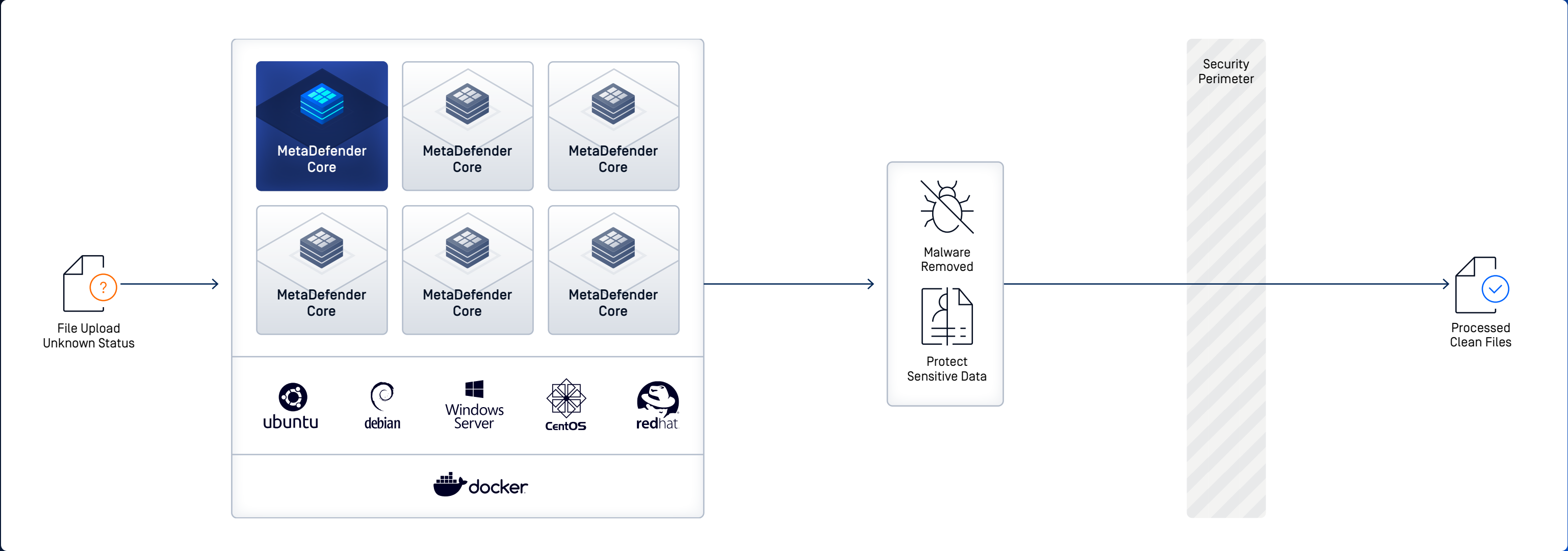


MetaDefender Core Container

To meet the need for scalability, our solution enables the deployment of MetaDefender Core in a containerized ecosystem. With MetaDefender Core Container, organizations can scale the advanced multilayered cybersecurity platform across different environments and operating systems, while ensuring application uniformity, removing any environment-specific dependencies, lowering resource consumption, and focusing on preventing malware attacks.

Benefits

- Automated deployment and operability simplify integration and maintenance
- Significantly lower total cost of ownership (TCO)
- Easy and flexible horizontal scaling
- Remove the complexity and ambiguity caused by the external factors such as conflict application dependencies
- Respond to load spikes by scaling only the required services



GET STARTED

Are you ready to put MetaDefender on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

Scan the QR code or visit us at:

opswat.com/get-started

sales@opswat.com



OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and

device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.