OPSWAT.

USE CASE GUIDE

Integrated File Security: From Perimeter to Storage

Powered by MetaDefender ICAP Server and MetaDefender Storage Security

Protecting the World's Critical Infrastructure

OPSWAT.

Files are essential to business workflows, and a common attack vector if not properly secured. As they move between network zones and reside in diverse storage environments, they can inadvertently introduce risk and expand the organization's attack surface. Despite ongoing investment in cybersecurity, many enterprises still rely on siloed tools that offer only partial coverage. This fragmented approach leaves gaps where advanced, file-based threats can persist undetected.

MetaDefender ICAP Server and MetaDefender Storage Security work together to deliver consistent file security across complex infrastructures. By protecting files in transit at the network perimeter and at rest within storage systems, these solutions adapt to each organization's architecture. The result: scalable and comprehensive protection wherever your data lives.

Table of Contents

OPSWAT.

01

The Challenges

Expanding Attack Surface

Modern enterprises manage billions of files across on-premises, hybrid, and multi-cloud environments. Every file can become a potential risk, which widens the attack surface beyond what traditional point solutions can protect.

Evolving Threat Tactics

Sophisticated malware uses polymorphism, zero-day exploits, and embedded payloads to bypass conventional detection. Single-engine scanners often fail to detect these threats across the full file lifecycle.

Regulatory Compliance

Regulatory frameworks increasingly mandate comprehensive protection for sensitive data, requiring organizations to implement and document security controls throughout the data lifecycle.

Resource Limitations Amid Growing Demands

Security teams are under increasing pressure to protect expanding digital environments with limited resources. As data volumes grow and infrastructure becomes more complex, teams are expected to do more with less.

Rising Threat Sophistication and Operational Fatigue

Security operations struggle to keep up with advanced, persistent, and evasive threats, often stuck in a reactive posture, overwhelmed by high alert volumes and the constant risk of missing critical threats.

Why Partial Protection Falls Short

A siloed approach, where perimeter security and storage security are treated separately, cannot keep pace with the threats targeting modern enterprises. Tackling these challenges requires a more comprehensive, integrated approach to file security, protecting files throughout their complete lifecycle while minimizing operational impact and optimizing security resources.

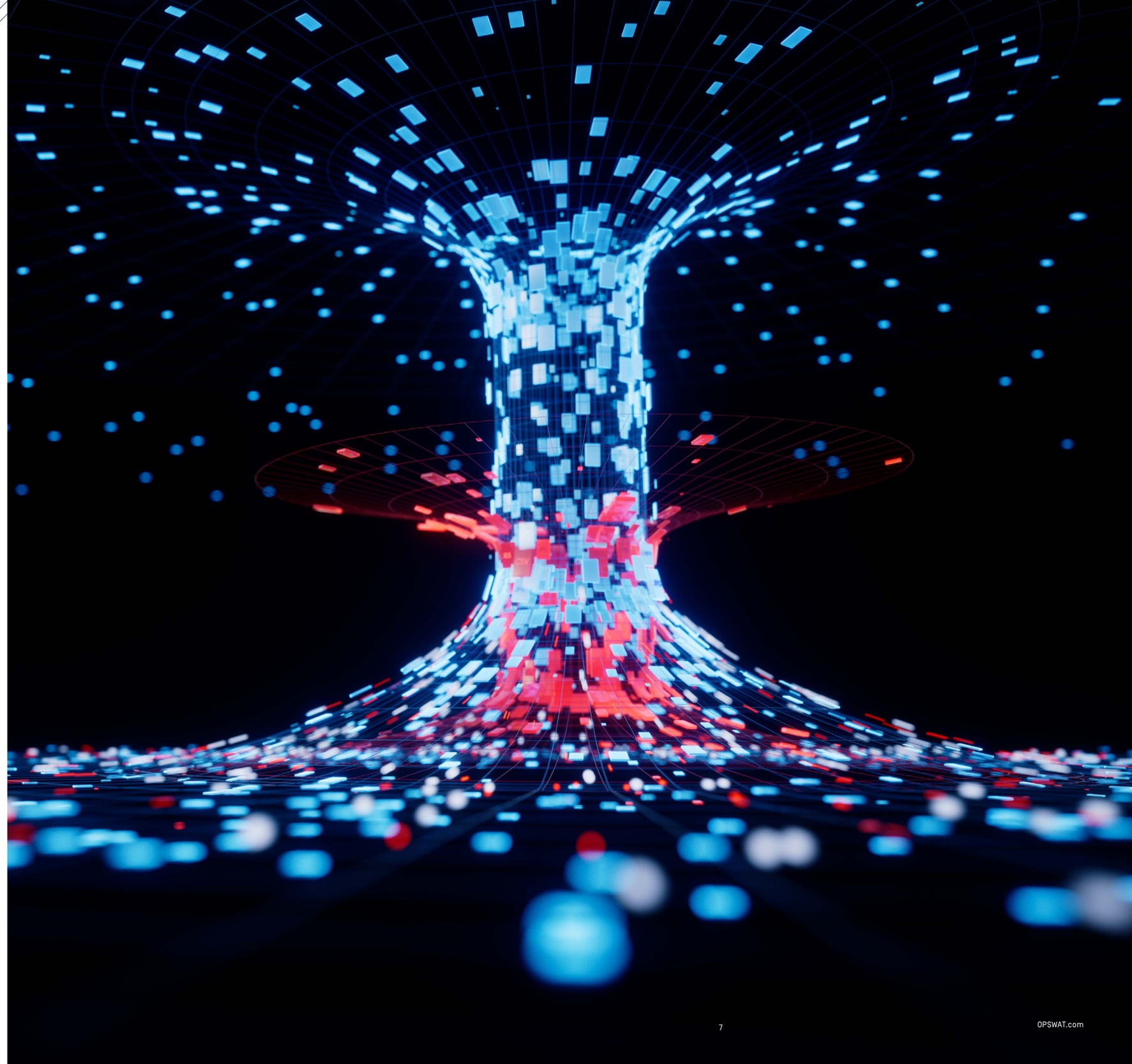
A unified file security framework should address the file lifecycle from initial receipt through ongoing storage and utilization:

- **Covers the complete file lifecycle**, from intake to long-term storage
- **Minimizes operational friction** through seamless integration into existing infrastructure
- **Optimizes detection and prevention** through advanced multi-layered techniques for evolving threat tactics

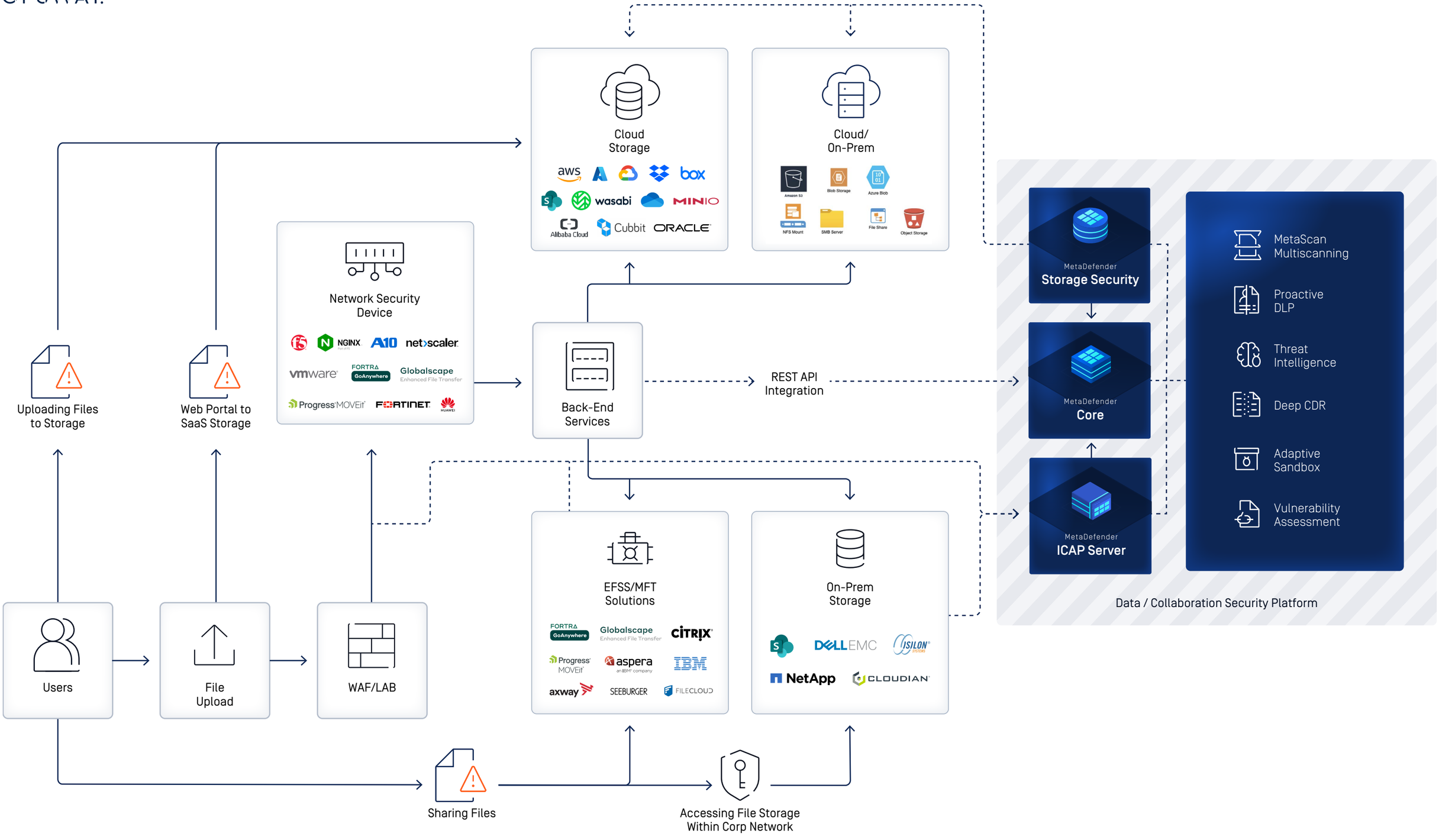
02

The OPSWAT Integrated Framework for Your File Security Strategy

OPSWAT provides a comprehensive security framework that protects files throughout their entire lifecycle. By combining MetaDefender ICAP Server and MetaDefender Storage Security, enterprises can create a comprehensive security ecosystem that protects data throughout its lifecycle, both in transit and at rest.



OPSWAT.


Cloud Storage
aws
box
wasabi
MINIO
Alibaba Cloud
Cubbit
ORACLE
Cloud/ On-Prem
Amazon S3
Blob Storage
Azure Blob
NFS Mount
SMB Server
File Share
Object Storage
Network Security Device
NGINX
A10
netscaler
vmware
FORTRA GoAnywhere
Globalscape Enhanced File Transfer
Progress MOVEit
FORTINET
HUAWEI
Back-End Services
REST API Integration
MetaDefender Storage Security
MetaDefender Core
MetaDefender ICAP Server
MetaScan Multiscanning
Proactive DLP
Threat Intelligence
Deep CDR
Adaptive Sandbox
Vulnerability Assessment
Data / Collaboration Security Platform
Uploading Files to Storage
Web Portal to SaaS Storage
Users
File Upload
WAF/LAB
EFSS/MFT Solutions
FORTRA GoAnywhere
Globalscape Enhanced File Transfer
CITRIX
Progress MOVEit
aspera an IBM company
IBM
axway
SEEBURGER
FILECLOUD
On-Prem Storage
DELL EMC
ISILON
NetApp
CLOUDIAN
Sharing Files
Accessing File Storage Within Corp Network

MetaDefender ICAP Server™

MetaDefender ICAP Server delivers a powerful file security layer at the network perimeter by integrating with your existing infrastructure. Powered by multi-layered threat prevention engines in the MetaDefender Platform, it scans all file traffic for malware, zero-day exploits, and sensitive data before it reaches your environment.

With plug-and-play deployment, MetaDefender ICAP Server works with any ICAP-compatible device, including load balancers, web application firewalls (WAFs), application delivery controllers, ingress controllers, managed file transfer systems, proxies, storage gateways, and more.

As the most broadly compatible ICAP server for file security, MetaDefender ICAP Server adapts to your architecture: scaling with your security needs and ensuring files are secure at the point of entry.

MetaDefender Storage Security™

MetaDefender Storage Security provides comprehensive, multi-layered protection for your data at rest, across on-premises, hybrid, and cloud-native storage environments.

From local servers to cloud platforms like Amazon S3, Microsoft Azure Blob Storage, NetApp, Cloudian, Dell EMC ECS, SharePoint, Box, and any S3 or SMB/NFS/SFTP-compatible storage, MetaDefender Storage Security safeguards enterprise data and files against breaches, downtime, and compliance violations.

	MetaDefender ICAP Server Secure Files at the Network Perimeter	MetaDefender Storage Security Secure Your Data at Rest
Integrations	F5, NGINX, Kemp, IBM, A10, Fortinet, Trellix, netscaler, Symantec, vmware, Fortra GoAnywhere, Progress MOVEit, axway, Globalscape Enhanced File Transfer, Nutanix, SEEBURGER, AIRLOCK, Cyolo, DELL EMC, ISILON SYSTEMS, FILECLOUD, HUAWEI	aws, CLOUDIAN, Google Cloud, NetApp, wasabi, Cubbit, Alibaba Cloud, OPSWAT. MetaDefender Managed File Transfer, ISILON SYSTEMS, OneDrive, ORACLE, box, SharePoint, Microsoft Azure, S3-compatible storages, SMB/NFS/SFTP-compatible-storages
Deployments	On-premises, Cloud, Hybrid	
Key Technologies	▪ **MetaScan Multiscanning**: 30+ Anti-Malware Engines ▪ **Deep CDR**: Content Disarm and Reconstruction ▪ **Proactive DLP**: Block Private and Personal Identifiable Information ▪ **Adaptive Sandbox**: Real-Time, Emulation-Based Sandbox ▪ **Vulnerability Assessment**: Detect Application Vulnerabilities Before Installation	
Benefits	▪ **Cross-Environment Protection**: Scan files in transit and at rest for comprehensive and consistent security ▪ **Prevent File-Borne Malware and Data Breaches**: Detect threats before they enter storage and continuously monitor files during their lifecycle ▪ **Compliance Adherence**: Help meet regulatory requirements (GDPR, HIPAA, NIST, SOX, ISO 27001, PCI-DSS, etc.) by ensuring all files are scanned and processed for malware, sensitive data, and policy violations ▪ **Integration with Existing Infrastructure**: Both solutions work wherever your data is stored (network devices, cloud storage, on-premises storage) ▪ **Proactive Security Posture**: Apply tailored security policies and workflows, scanning configurations, remediation actions, and false detection mechanisms across active file transfers and stored data ▪ **High Availability Mechanism**: Support back-up protection and self-healing with Kubernetes deployments	

OPSWAT.

03

Integrated File Security Use Cases

End-to-End File Protection from Upload to Storage

MetaDefender ICAP Server secures files in transit at the network perimeter, while MetaDefender Storage Security extends that protection to files at rest within storage systems.

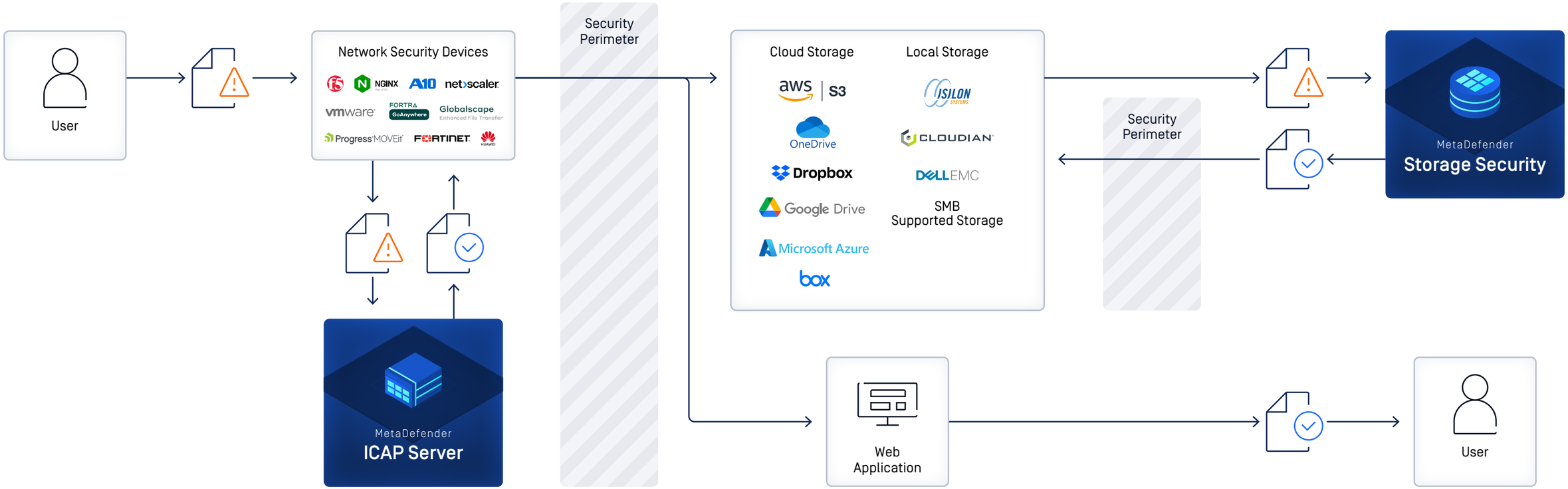
A company allows employees and customers to upload files via web applications, which are then stored in cloud or on-premises storage. The organization needs to secure files both at the perimeter and after they have been transferred and stored in their environment.

A company enables employees, partners, or customers to upload files through public-facing web applications (such as portals, forms, or ticketing systems). These files may include documents, images, or other business-critical content, which are then stored in either cloud-based or on-premises repositories. While these uploads support collaboration and process automation, they also introduce potential risk: malicious files can enter the network, and sensitive data may be mishandled or stored in non-compliant ways. The organization must secure file transfers both at the point of entry and throughout their lifecycle in storage.

- **MetaDefender ICAP Server** secures data in transit. The solution integrates with network security devices (web proxy, load balancer, web application firewall, ingress controller, etc.) to inspect the content of all uploaded files for malware, exploits, and sensitive data before they enter the organization's environment. Files that pass inspection are then stored in a regulated repository, either on-premises or in the cloud.
- **MetaDefender Storage Security** secures data at rest. It provides continuous protection by performing real-time or periodic scans of stored files to detect previously undetected threats, file-based vulnerabilities, and sensitive data. Unallowed or non-compliant files can be blocked or moved to separate storage.

Benefits

- Comprehensive protection against file-borne threats, both in transit and at rest, through multi-layered threat prevention
- Supports regulatory compliance and data governance across the file lifecycle
- Continuous security defense against known and unknown malware, zero-day exploits, sensitive data loss, and insider risks



Consistent File Security from On-Premises to Cloud

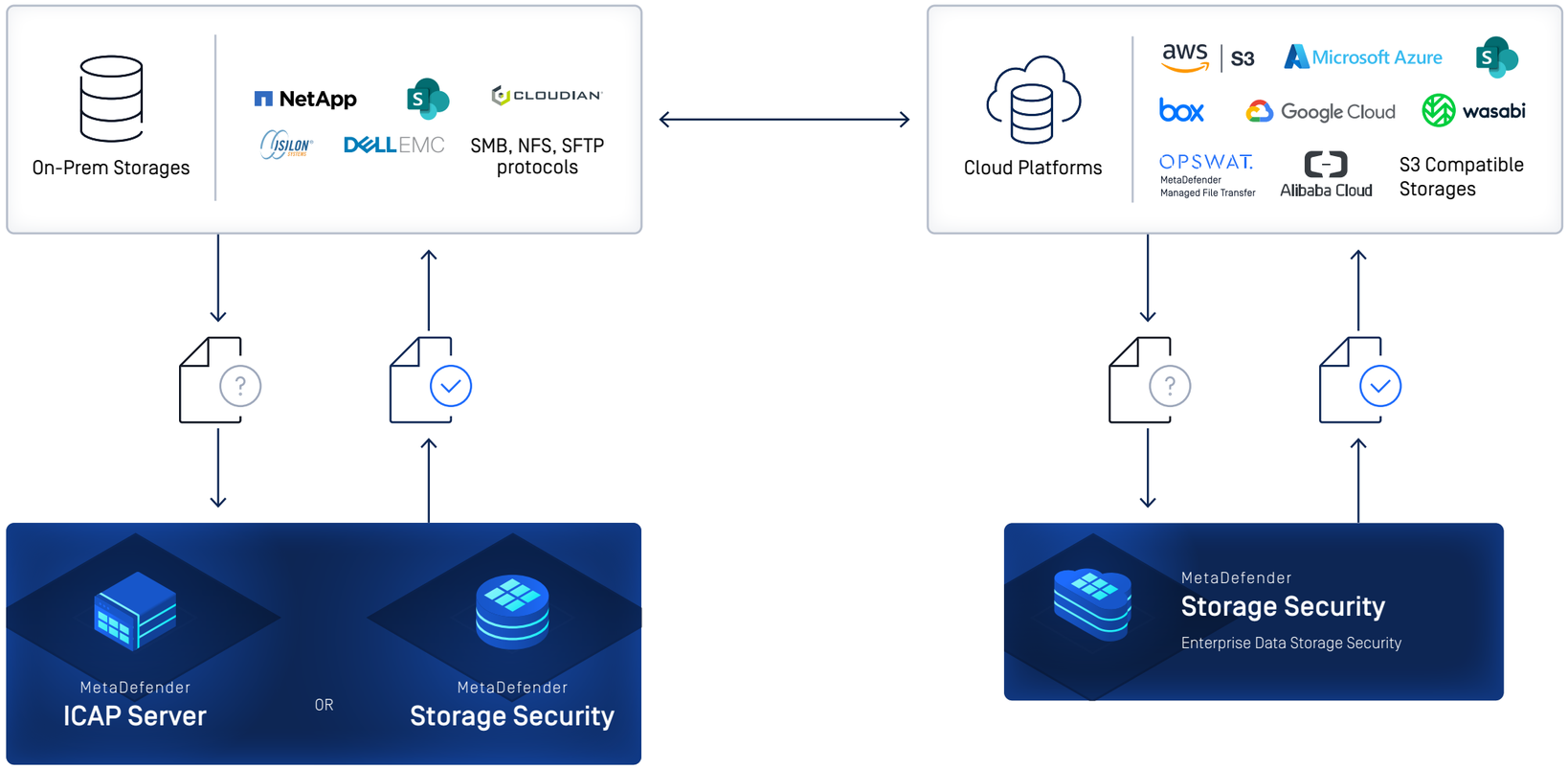
MetaDefender solutions support both on-premises and cloud storage environments, ensuring consistent and adaptive file security measures that follow your data where it resides.

An enterprise currently relies on on-premises storage systems (such as Dell EMC) protected by MetaDefender ICAP Server. They are transitioning from on-premises storage systems to cloud-based storage (like Amazon S3 or Azure Blob). During this migration, maintaining the integrity and security of files is critical to avoid transferring existing threats or compliance risks into the cloud.

- On-premises, both MetaDefender ICAP Server and MetaDefender Storage Security provide multi-layered scanning and continuous monitoring of stored files for threats, zero-day vulnerabilities, and sensitive data.
- Post-migration, MetaDefender Storage Security integrates natively with cloud storage platforms such as Amazon S3, Azure Blob, Google Cloud, Wasabi, SharePoint, Box, etc., to provide ongoing protection, mirroring the same security measures previously enforced on-premises.

Benefits

- Prevents the transfer of malicious or non-compliant files into cloud environments
- Maintains a unified file security posture throughout the migration journey
- Provides consistent protection across hybrid environments



OPSWAT.

Secure Remote Access from Low to High Security Zones

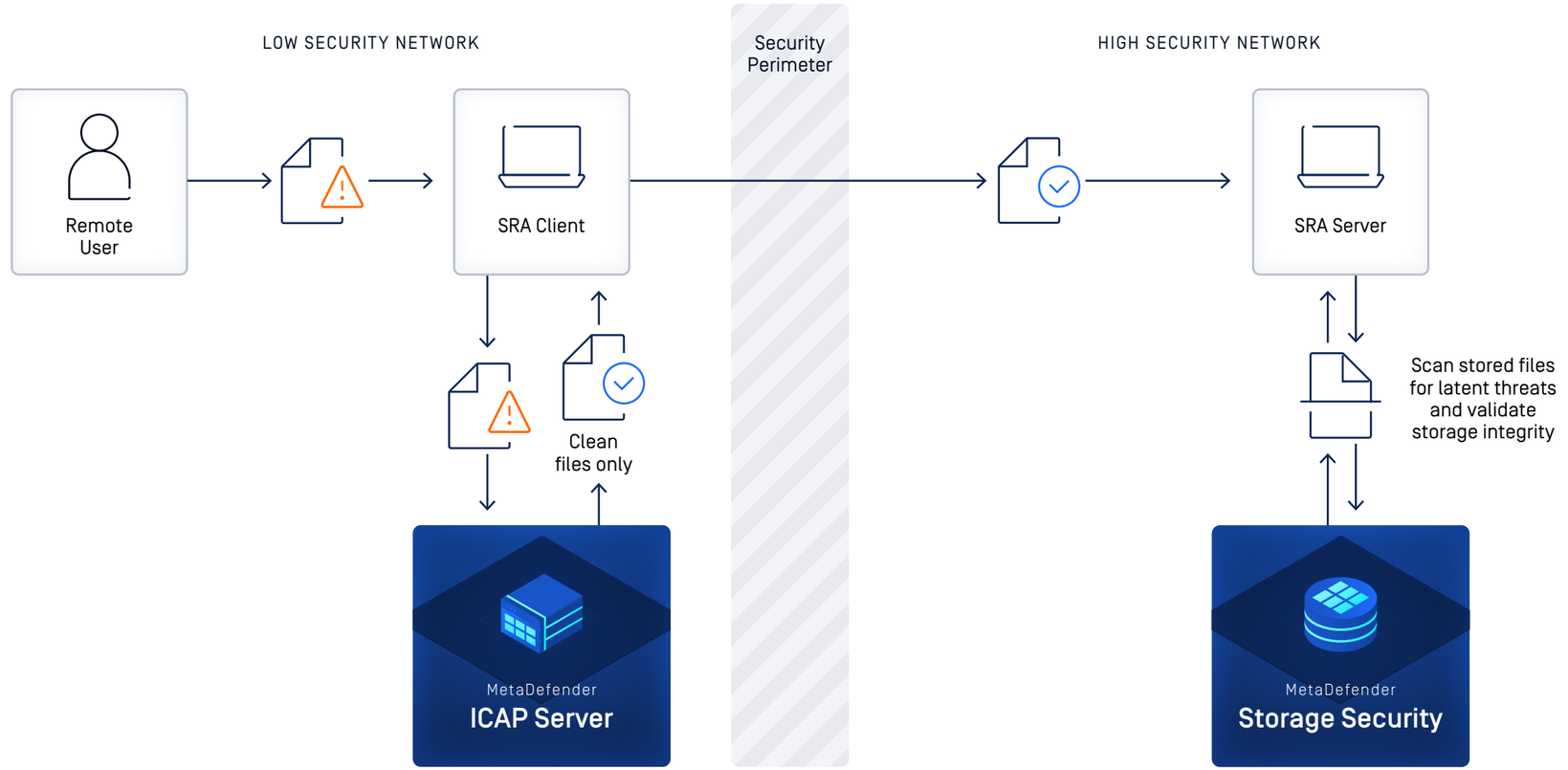
MetaDefender ICAP Server and MetaDefender Storage Security work together to secure file transfers during remote sessions between low and high security zones.

An industrial organization uses an SRA (Secure Remote Access) solution to allow administrators and users to remotely access systems in isolated or high-security network zones. These remote sessions frequently involve files being transferred between the SRA client and SRA server, creating a risk vector for malicious files to move laterally within the network environment.

- MetaDefender ICAP Server integrates with SRA infrastructure to inspect and sanitize files transferred during remote desktop sessions. Files moving from the lower-security environment (remote client) to the higher-security zone (target server) are intercepted and scanned for malware, exploits, and sensitive data.
- Once files arrive in the higher-security zone, MetaDefender Storage Security provides ongoing protection for data at rest by continuously scanning stored files (e.g., patches, security updates, installer files). This second phase validates the storage repository and prevents latent threats, eliminating the need for manual checks and supports compliance with internal security policies.

Benefits

- Prevents file-borne threats from entering critical systems during remote access sessions
- Enables secure and policy-compliant file transfers between network zones
- Centralizes and secures validated files for future use, reducing manual verification and operational overhead



04

CUSTOMER SUCCESS STORY

Leading Financial Institution (Asia)

Use Case

- Securing sensitive data within AWS S3 storage with continuous, near real-time scanning and sanitization
- Implementing a Zero-Trust security model for file uploads and object storage
- Deep file inspection and sanitization (Deep CDR) within S3

Challenge

- Securing file upload and S3 storage processes against malware without disrupting workflows
- Achieving effective malware removal while preserving data integrity through deep sanitization
- Seamless integration with existing on-premises AWS S3 infrastructure

Solution

- Deployed MetaDefender Storage Security integrated directly with the customer's on-premises AWS S3 storage
- Utilized MetaDefender ICAP Server deployment to enforce a Zero-Trust approach for file handling
- Leveraged Deep CDR technology for thorough document sanitization, ensuring data integrity and compliance
- Implemented automated quarantine for risky files and secure routing for safe files

Outcome

- Significantly reduced malware infiltration risk through Zero-Trust and comprehensive scanning
- Ensured business continuity via seamless integration with existing AWS S3 setup
- Met regulatory compliance obligations through data integrity preservation and thorough sanitization
- Transformed AWS S3 into a secure and compliant data repository

Get Started Today

Contact our security experts to schedule a demonstration and see how OPSWAT's solutions can strengthen your organization's security posture while supporting operational efficiency and compliance requirements.

Contact Us

Scan the QR code or visit:

opswat.com/contact

Learn More about Our Solutions

MetaDefender Storage Security

opswat.com/solutions/storage-security

MetaDefender ICAP Server

opswat.com/products/metadefender/icap

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 1,800 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