OPSWAT.

A Day in the life of a file

Aktive Abwehr im IT-/OT-Datenfluss

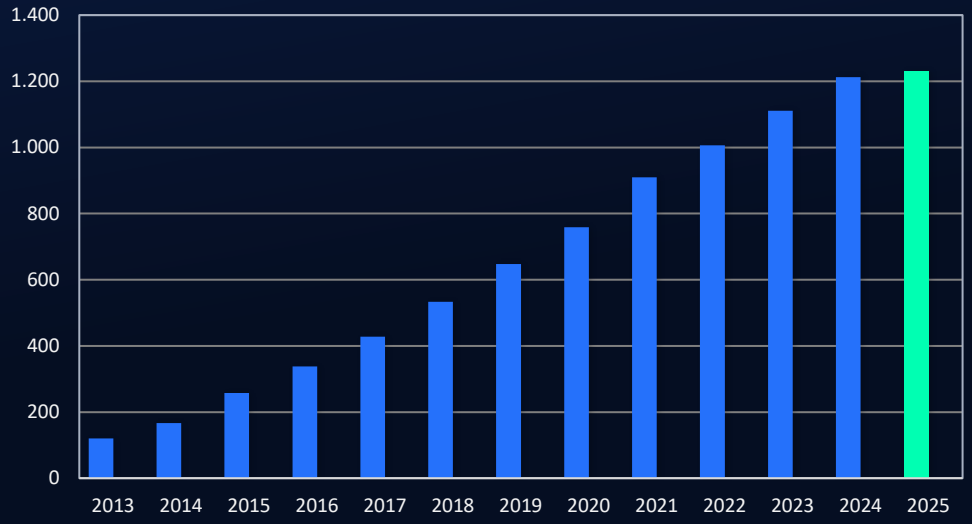
Martin Lüning, Senior Solution Engineer, OPSWAT
Kolja Oswald, Regional Sales Manager, OPSWAT

September 2025, Congress Park Hanau

SECURITY & BUSINESS CHALLENGES

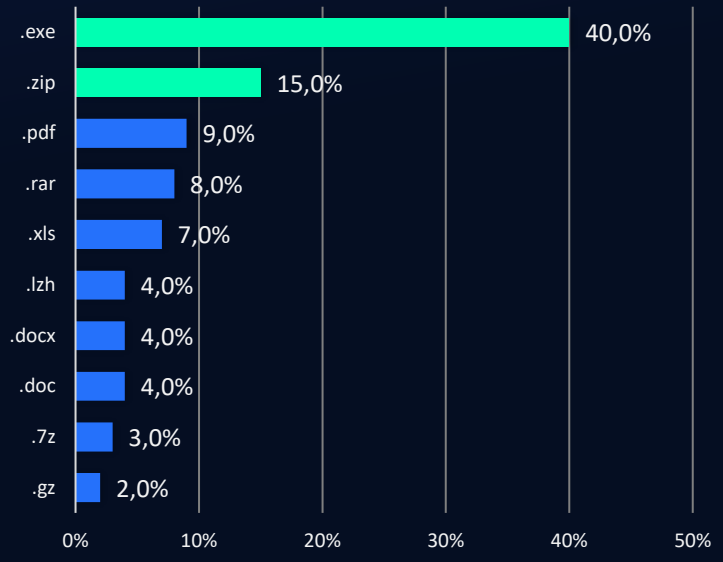
The Rise of File-Borne Malware

Total malware in 2025



Last updated: Feb 2025.
Source: AV-Test Institute & HP Wolf Security

Malicious artifacts by file types 2025



CHALLENGES

Data & Files in Critical Environments

Why? | How? | What?

72 %

Rise in **cyber risks** in 2024

42 %

of **organizations experienced** social engineering attacks

$4.88 M

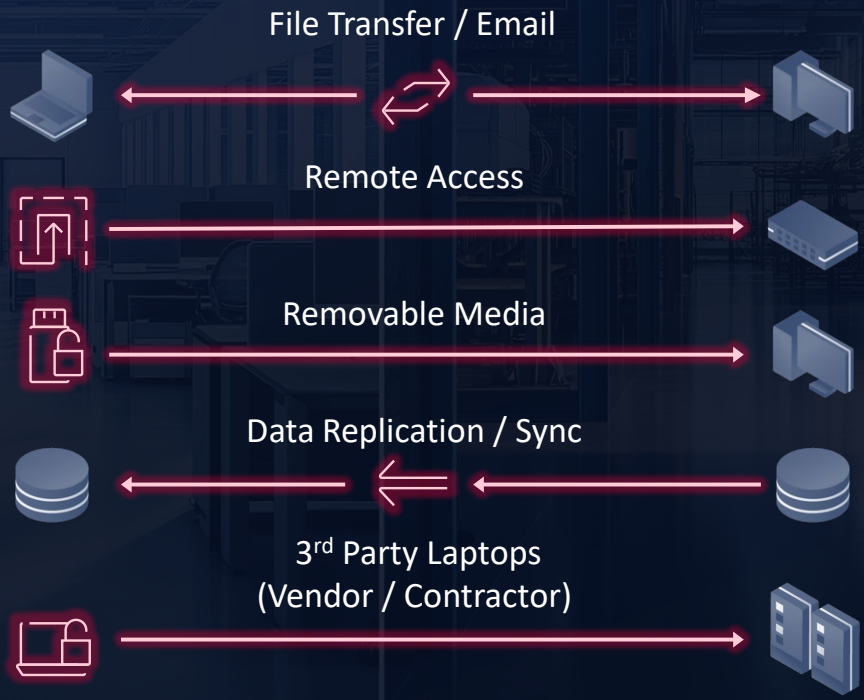
Average **cost of** a data breach

Devices are not Designed to Scan Files

CHALLENGES

Data & Files in Critical Environments

Why? | How? | What?



CHALLENGES

Data & Files in Critical Environments

Why? | How? | What?

Configuration

Patches

Data Files

Firmware

DATA INBOUND

Collaboration

Office Documents

Videos

Image Files

Manuals

Backup Files

Log Files

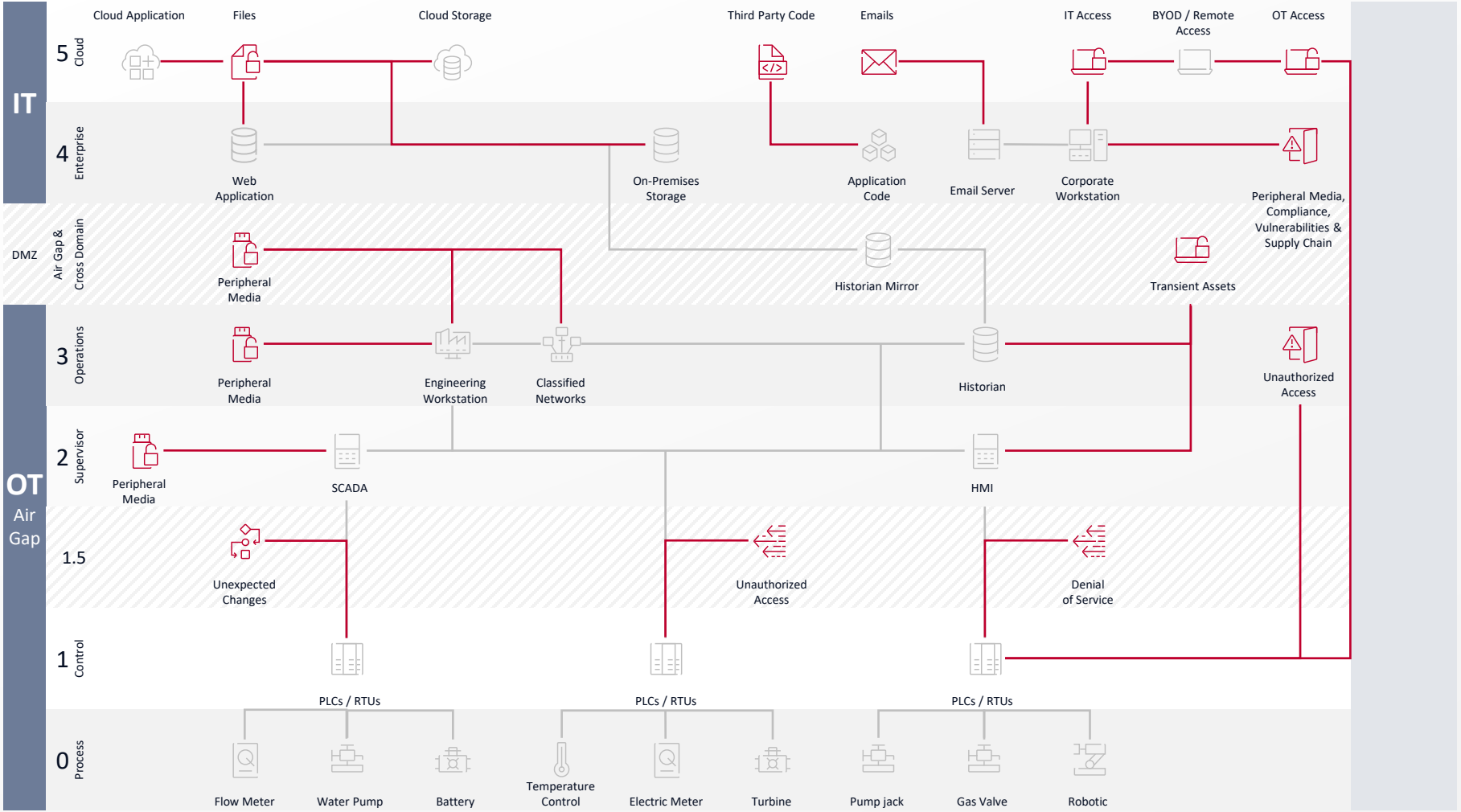
Data Files

DATA OUTBOUND

Compliance Reports

Images

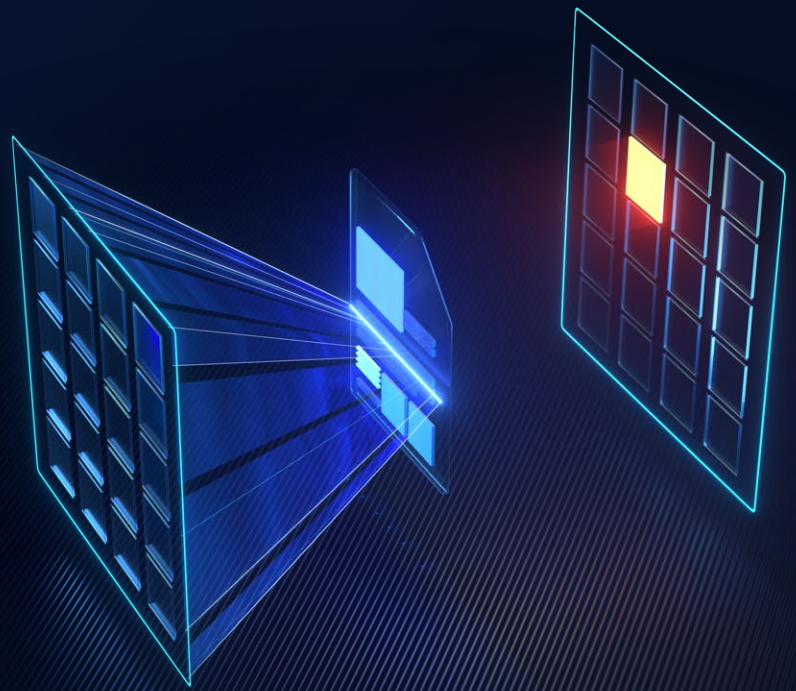
Replication & Synchronization data


IT
OT
Air Gap
DMZ
Air Gap & Cross Domain
5 Cloud
4 Enterprise
3 Operations
2 Supervisor
1.5
1 Control
0 Process
Cloud Application
Files
Cloud Storage
Third Party Code
Emails
IT Access
BYOD / Remote Access
OT Access
Web Application
On-Premises Storage
Application Code
Email Server
Corporate Workstation
Peripheral Media, Compliance, Vulnerabilities & Supply Chain
Peripheral Media
Historian Mirror
Transient Assets
Peripheral Media
Engineering Workstation
Classified Networks
Historian
Unauthorized Access
Peripheral Media
SCADA
HMI
Unexpected Changes
Unauthorized Access
Denial of Service
PLCs / RTUs
PLCs / RTUs
PLCs / RTUs
Flow Meter
Water Pump
Battery
Temperature Control
Electric Meter
Turbine
Pump jack
Gas Valve
Robotic

OPSWAT.

Multiscanning

Detect nearly 100% of threats using 30+ antivirus engines simultaneously.

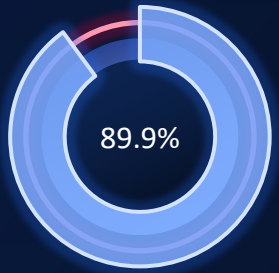


MALWARE PREVENTION

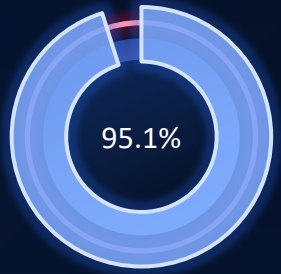
Multiscanning

With more antivirus engines you get more coverage and a smaller risk window.

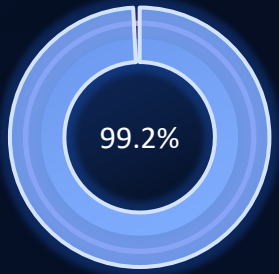
Single Engine



8 Engines



16 Engines

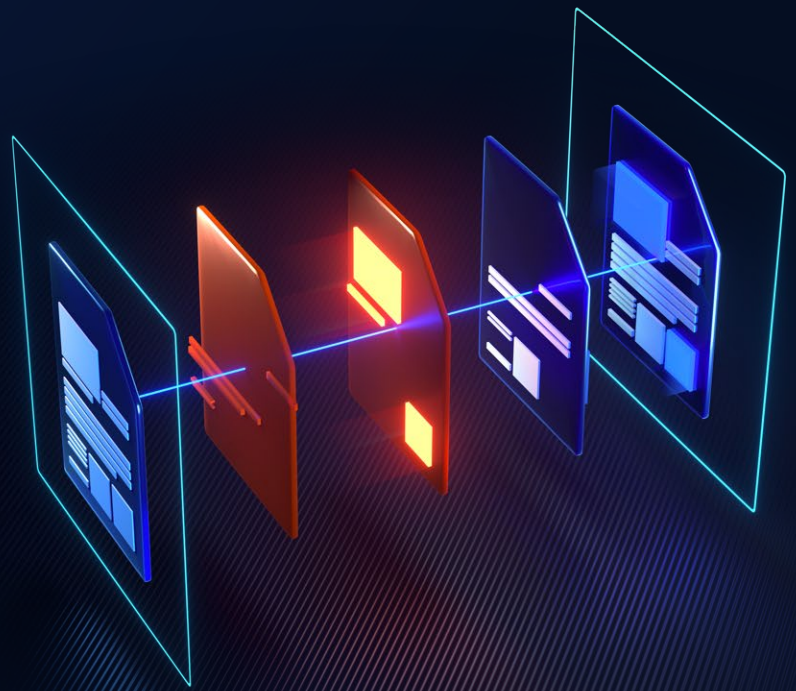


Max Engines

OPSWAT.

Deep CDR

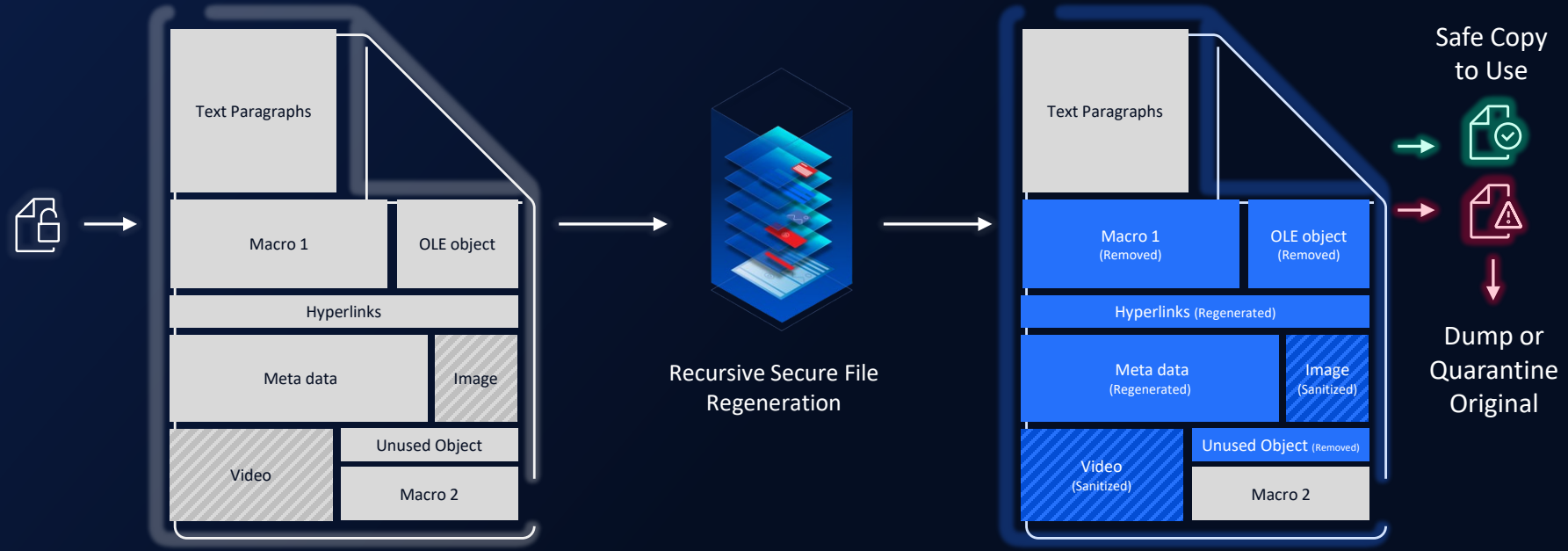
Sanitize files to prevent known and unknown malware and zero-day attacks.



MALWARE PREVENTION

Deep CDR

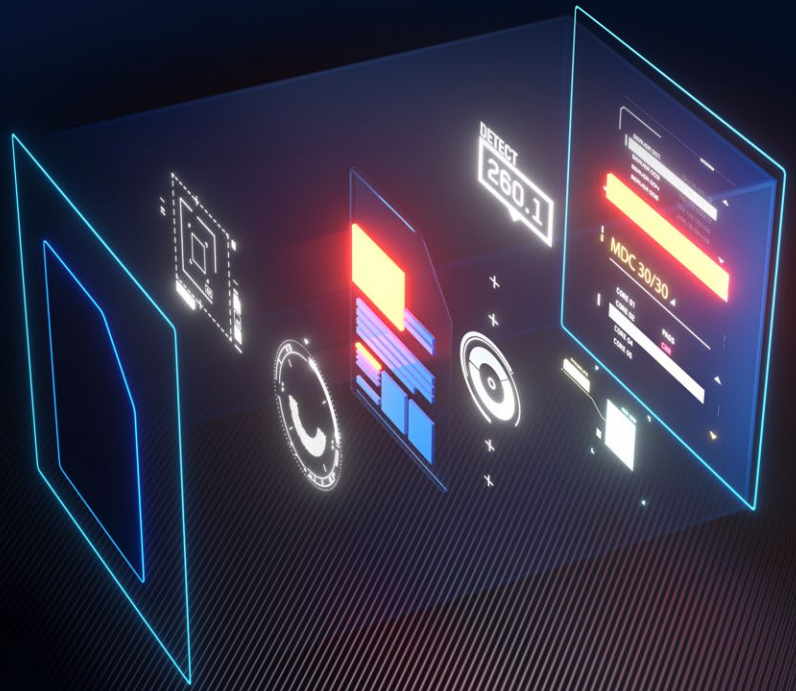
Sanitize, block and remove file objects and regenerate a safe copy.



OPSWAT.

Adaptive Sandbox

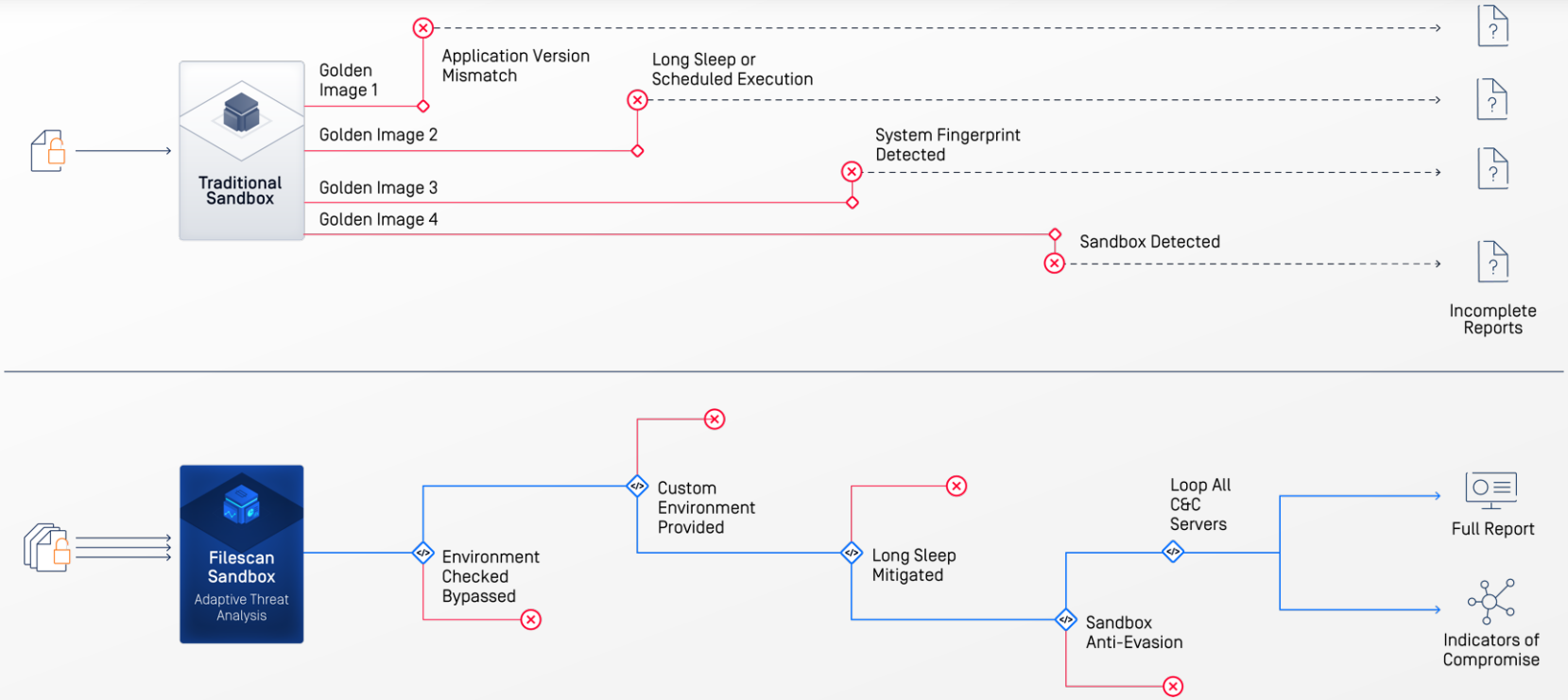
Adaptive threat analysis technology enables zero-day malware detection and extracts more indicators of comprise.



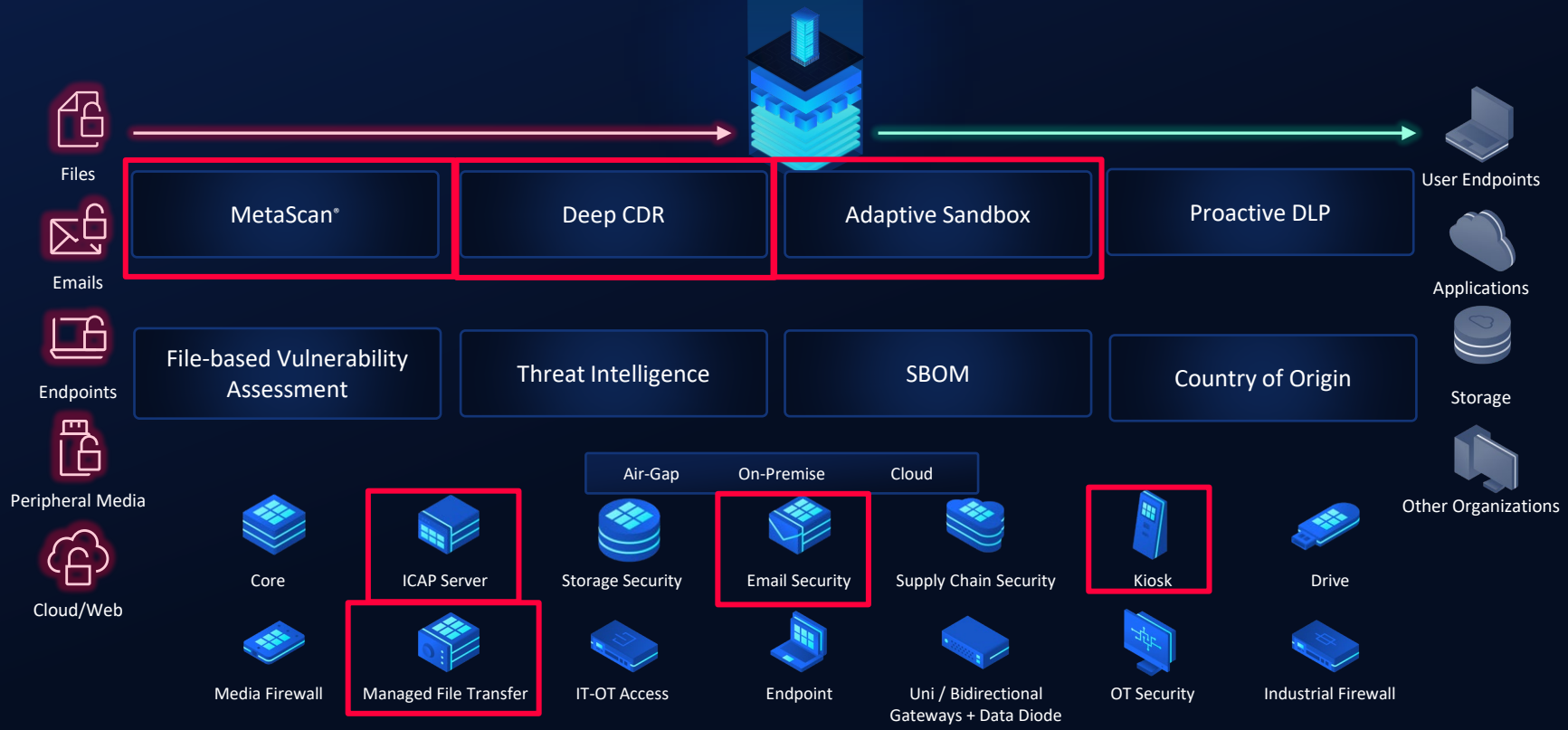
MALWARE PREVENTION

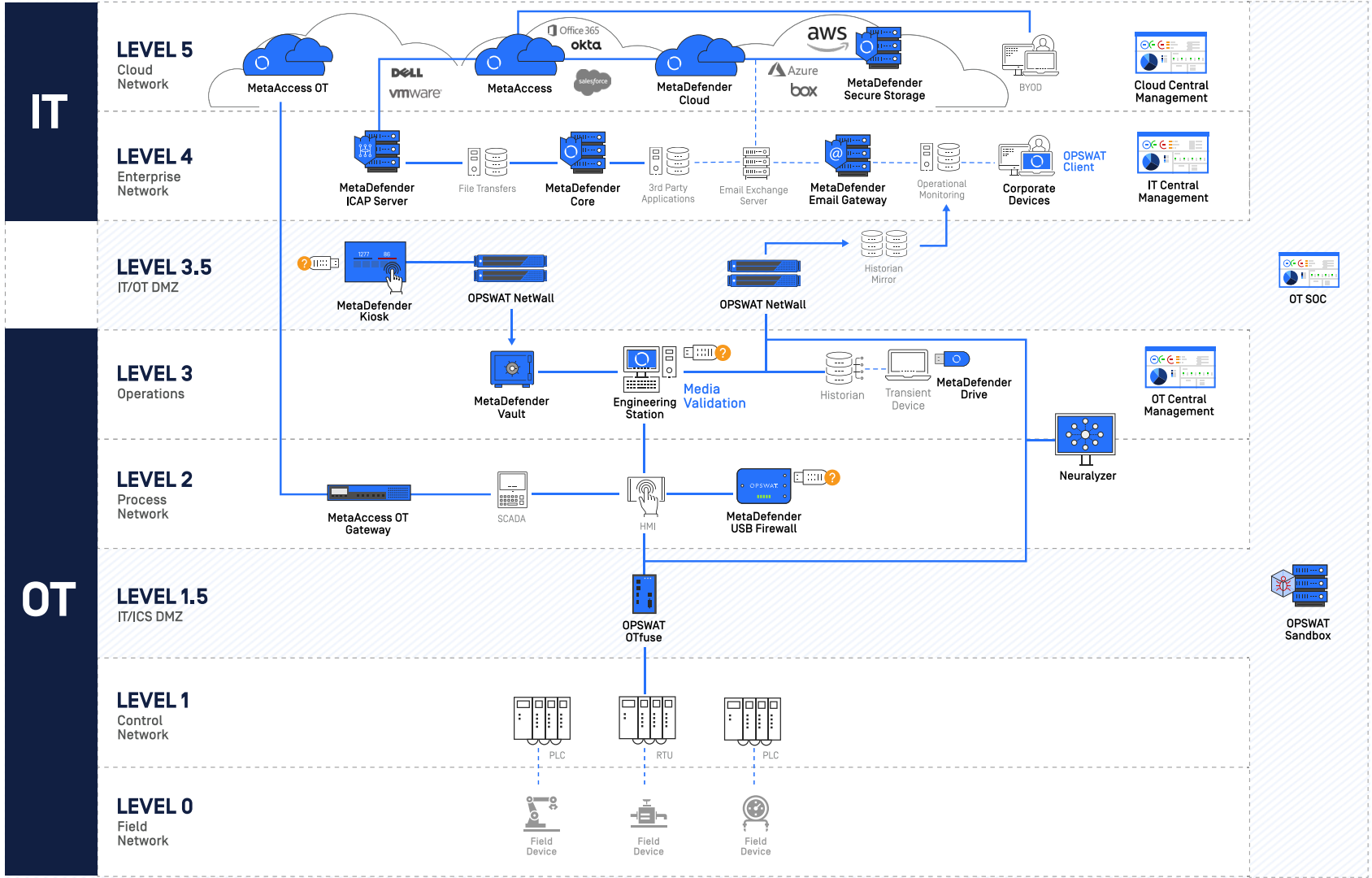
Adaptive Sandbox

How our emulation-based sandbox works.



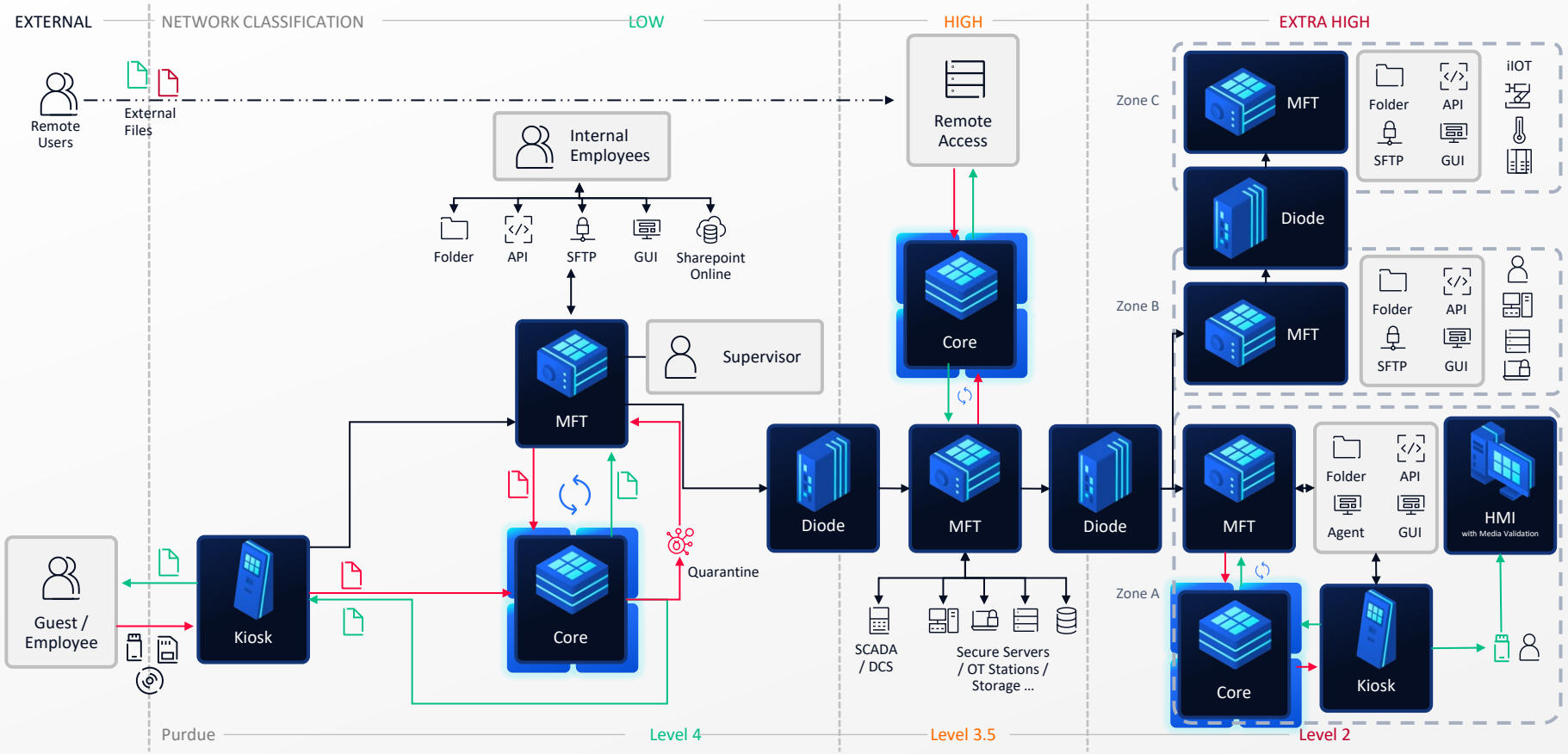
MetaDefender Platform





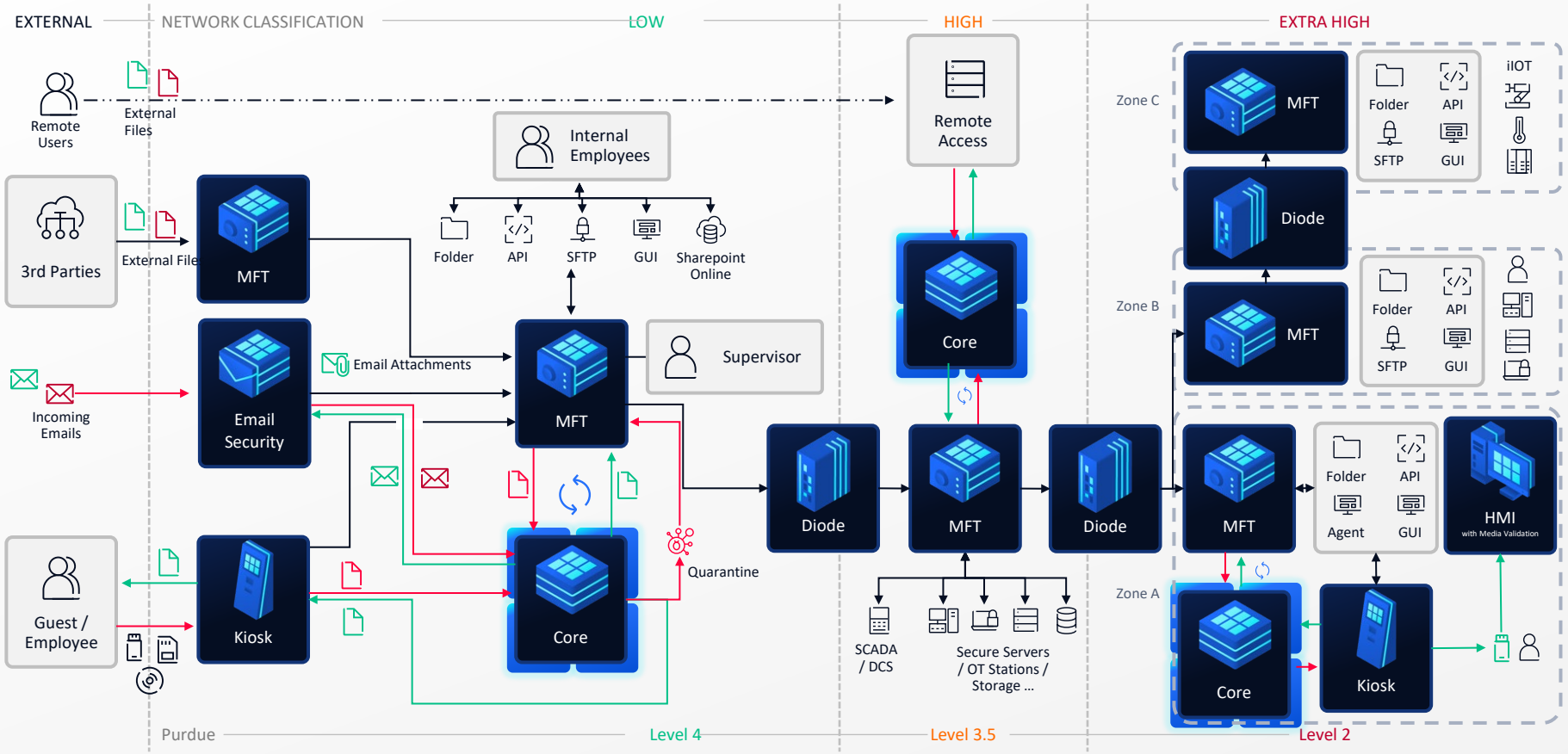
SECURING THE FLOW OF DATA

A Day in the Life of a Data File



SECURING THE FLOW OF DATA

A Day in the Life of a Data File



OPSWAT. | Swiss Re

Swiss Reinsurance Company Ltd

One of the world's leading providers of reinsurance, insurance and other forms of insurance-based risk transfer.

Profile

Company: Swiss Reinsurance Company Ltd

Industry: Insurance

Products Used: MetaDefender ICAP

""The majority of documents we handle contain client personal data. These must all be scanned before reaching the internal network to protect our web applications from malicious file uploads. OPSWAT provides a high quality, easy-to-use, effective solution to secure this traffic."

Raymond Bucher
Director/Cloud Architect

Explore the Full Story at OPSWAT.com

Challenge

- Risk of infected files entering secure network via web applications
- Compatible with microservices architecture: deployable in Azure/Kubernetes and has native support for NGINX
- Meet regulatory requirements, cost-effective and rapidly scalable

Solution

MetaDefender ICAP Server on top of their Azure Container Instances (ACI), integrated with an API Gateway

Outcomes

- Scalable web application security
- Enterprise-class performance
- Superior service

OPSWAT.

Your team, how can we help?

Kolja Oswald
Regional Sales Manager

Martin Lüning
Senior Solution Engineer

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.