OPSWAT.

PROTECTING THE WORLD'S
CRITICAL INFRASTRUCTURE

Perimeter Security

Securely Exchanging Data with Third Parties

2025 - EVENT

OPSWAT.

Protect your files wherever they are.

Stefan Liversidge

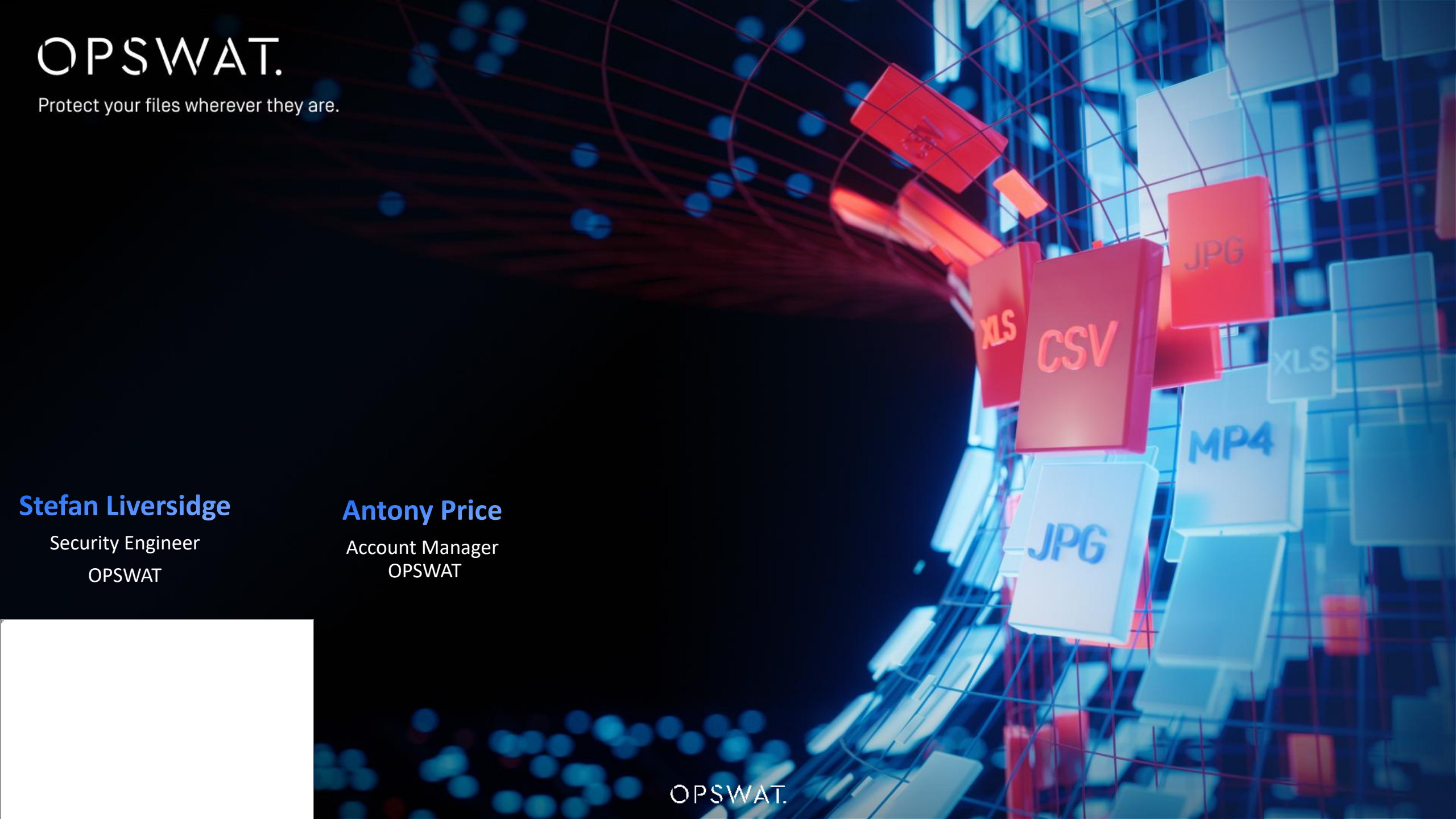
Security Engineer

OPSWAT

Antony Price

Account Manager

OPSWAT

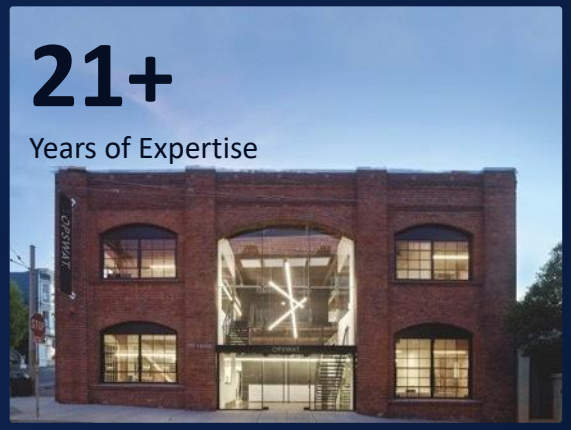



OPSWAT.
Protecting the World’s Critical Infrastructure

Our Key Customer Focus Areas:

Who is OPSWAT?

Over 20 Years of Innovation



2024 SE Labs
100% Protection Score

2024 Global InfoSec Awards (RSA 2024)
Winner

2024 Cybersecurity Excellence Awards
Gold – IDP/IPS
Gold – OT Security
Gold – Supply Chain Security

2024 Globee Awards
Winner – Critical Infrastructure Protection

Cybersecurity Breakthrough Awards 4 Years Running
2024 Supply Chain Cybersecurity Solution of the year
2023 Overall Enterprise Email Security Solution
2022 Professional Certification Program
2021 Overall Infrastructure Security Solution Provider

2024 The Channel Co.
CRN Partner Program Guide

ISO/IEC 27001:2022 Certification.

OPSWAT MetaDefender Core achieved EAL2+
(ALC_FLR. 1) Met all Common Criteria Evaluation Assurance Level

TRUST NO FILE

Supply Chain Cyber Risk

Your Supply Chain

Products, Systems, Services

- Contractors / Integrators
- Service Providers (MSP / CSP)
- Software Vendor
- Hardware Manufacturer

Are You the Target?

Direct

Indirect

Risk Management

Internal Assessments

Security Profiles

External Audits

DATA Security

File Scanning

Threat Detection

Content Inspection

File Protection

TRUST NO FILE

ImpEx of Data & Files

What? | How? | Why?

KYC files

Patches

Data Files

Dissertations

PDFs

Firmware

Request document

DATA IN

Configuration

Office Documents

C2B Data

Videos

Proof of ID

Photos

Manuals

DATA OUT

Backup Files

Data Files

Log Files

B2B Data

Images

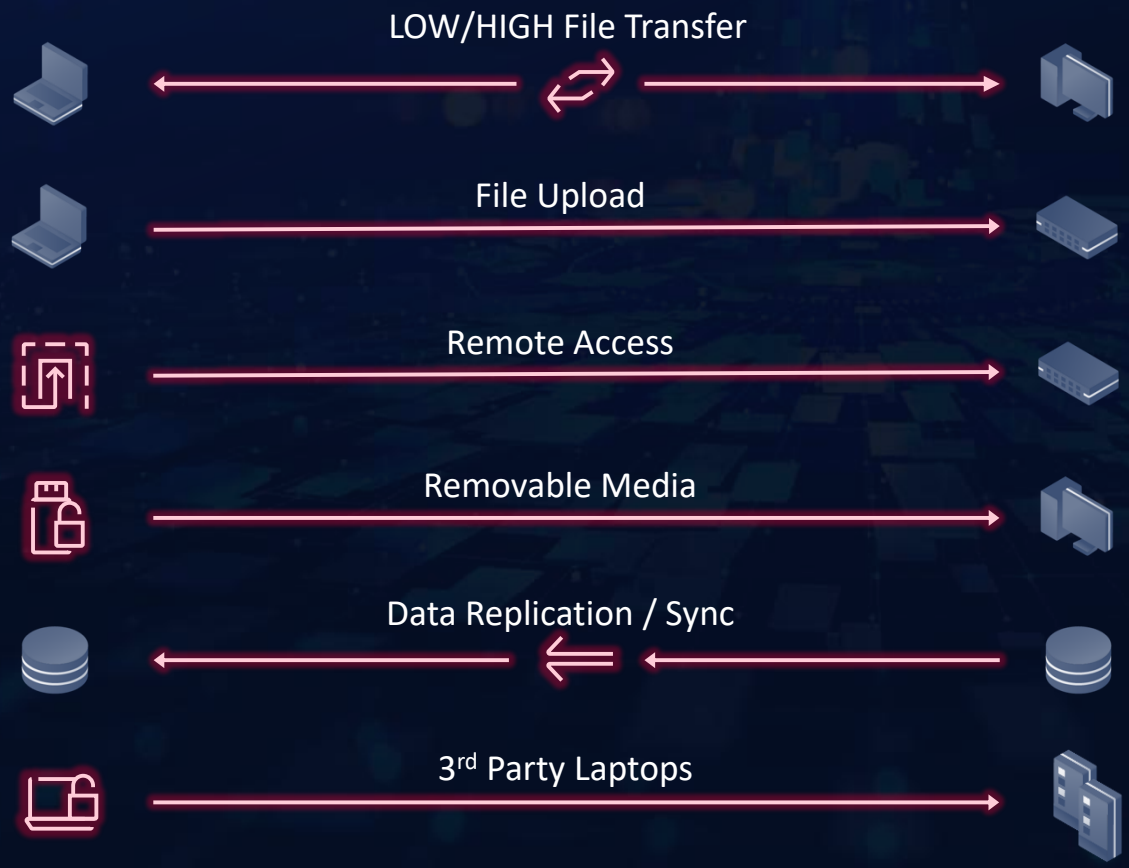
Compliance Reports

Replication & Synchronisation data

TRUST NO FILE

ImpEx of Data & Files

What? | How? | Why?



TRUST NO FILE

ImpEx of Data & Files

What? | How? | Why?

99% are attacks from **removeable media***

2% of threats are ever **discovered***

94% ransom attacks are fully **successful***

*According to my Mother

What's the

IMPACT

of the:

Data **Loss / Leakage?**
Data **Corruption?**
Data **Modification?**
Environment **Damage?**
Environment **Outage?**

ico. Information Commissioner's Office | IEC | NIS2 DIRECTIVE | ISO | National Cyber Security Centre | NIST | NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

TRUST NO FILE

How are Threat Actors Weaponising Data?

Embedded
MACROs
(& other objects)

Embedded
Archiving

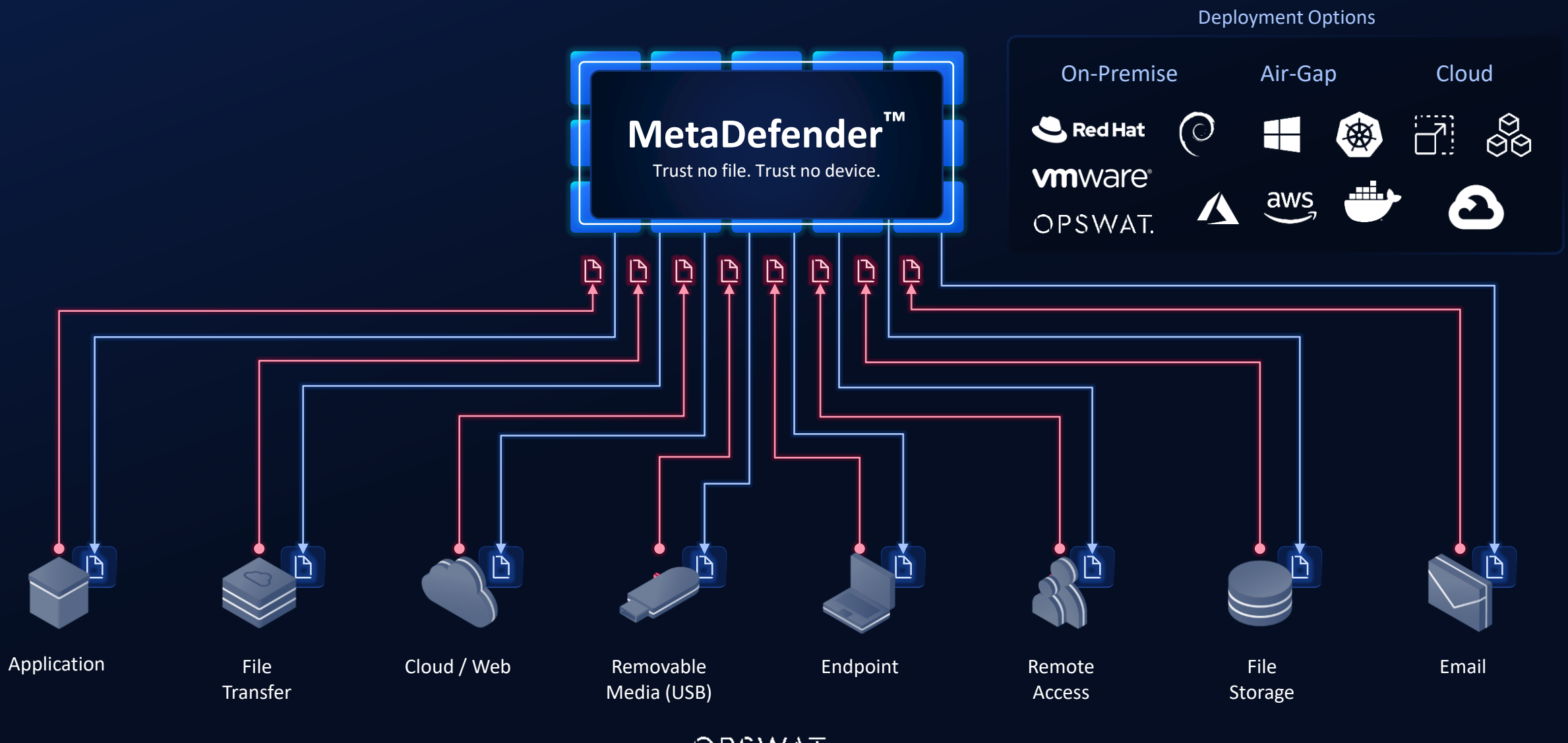
Image
Stenography

Alternate Data
Streams

Evasion Frameworks

TRUST NO FILE

MetaDefender Core



OPSWAT.

MetaDefender CORE

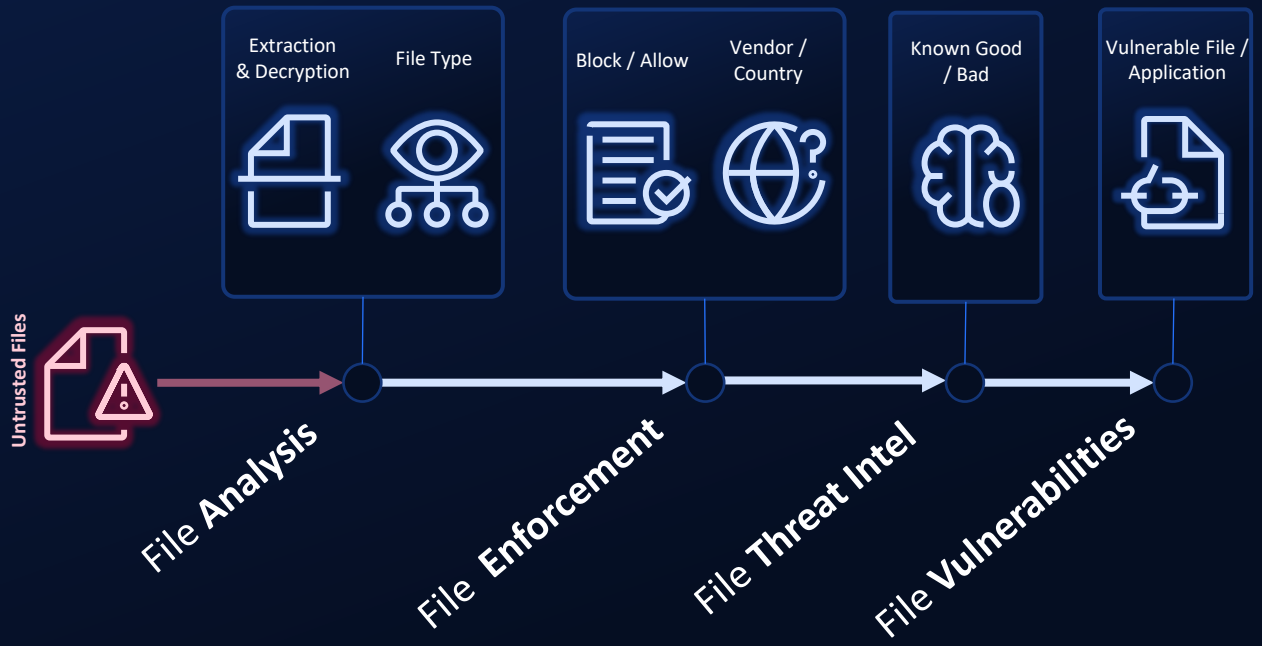
METADEFENDER CORE

Layered File Protection

METADEFENDER CORE

Layered File Protection

MetaDefender CORE



Untrusted Files

BLOCKED

sample_metascan.html

Hypertext Markup Language - 108.9 KB

Infected | Other blocked reasons ...

File process | LOCAL/admin | Jan 14, 2024 at 11:52:04 AM | Jan 14, 2024 at 11:52:04 AM | 1,707 ms

METASCAN™ | DEEP CDR | PROACTIVE DLP | VULNERABILITY ASSESSMENT | FILE TYPE VERIFICATION | SANDBOX | SBOM | REPUTATION

Engine	Result	Definition Date	Scan Time
[redacted]	✓ No Threat Detected	2024-01-08 [6 days ago]	320 ms
[redacted]	✗ Trojan[Infect]/JS.Agent	2024-01-07 [7 days ago]	35 ms
[redacted]	✗ JS/Agent.G1	2024-01-07 [7 days ago]	49 ms
[redacted]	✓ No Threat Detected	2024-01-07 [7 days ago]	243 ms
[redacted]	✓ No Threat Detected	2024-01-06 [8 days ago]	257 ms
[redacted]	✗ TrojWare.JS.Agent.NKB	2024-01-07 [7 days ago]	19 ms
[redacted]	✓ No Threat Detected	2024-01-07 [7 days ago]	238 ms
[redacted]	✓ No Threat Detected	2024-01-07 [7 days ago]	350 ms
[redacted]	✗ Trojan.JS.Agent	2024-01-07 [7 days ago]	183 ms
[redacted]	✗ Exploit [04c55c361]	2024-01-08 [6 days ago]	28 ms

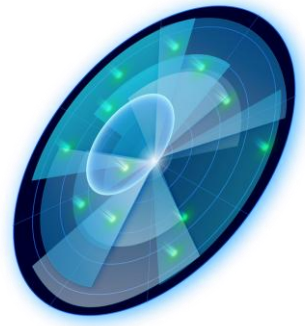
Malware detection rate by AVs

1 Engine	8 Engines	12 Engines	16 Engines	20 Engines	Max Engines
6% - 76%*	89.90%	92.30%	95.10%	96.40%	99.20%

Data updated: July 18, 2023

*34 AV Vendor Scans on the Most Frequent 10,000 Malware Samples

Utilise **30+** engines for close to 100% detection

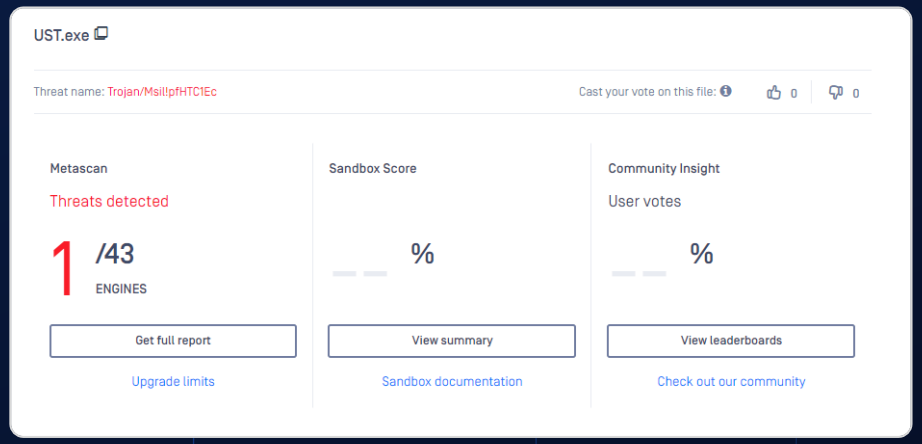


MetaDefender CORE

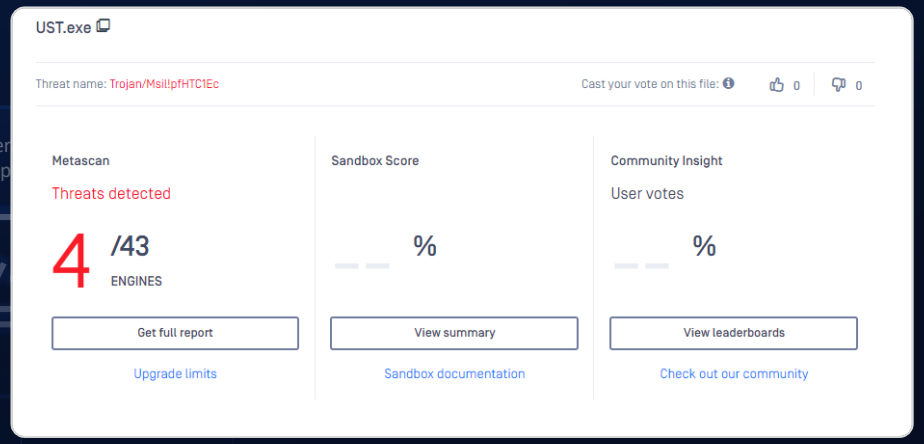
C O R E t o o u r s o l u t i o n s

Layered File Protection

November 2015
Only 1 AV scanner found the threat (Filseclab)

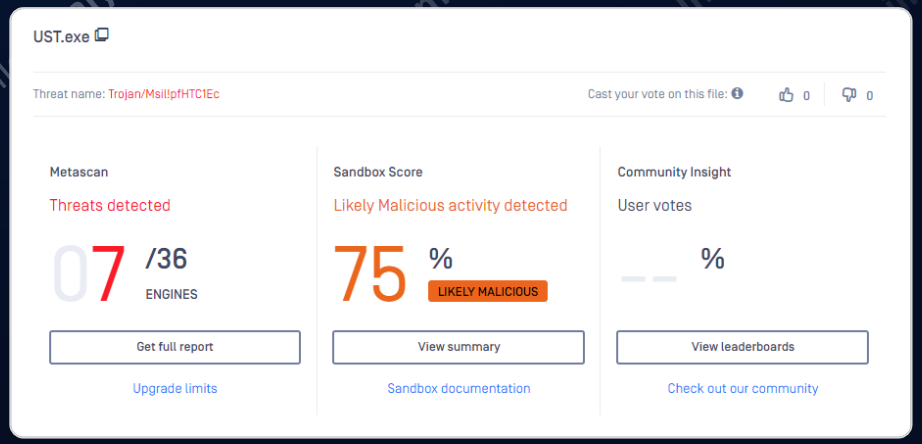


February 2016
Only 4 AV scanners found the threat (Antiy, AegisLab, Filseclab, and Zillya)

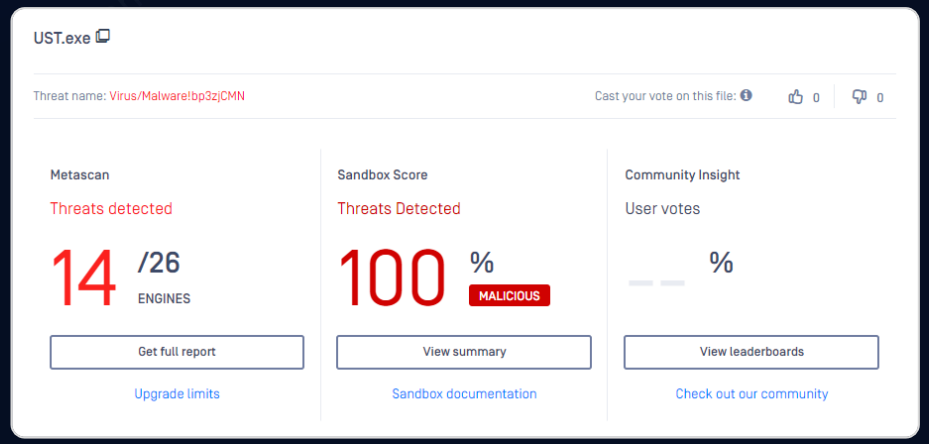


Untrusted Files

May 2018
Only 07 AV scanners found the threat,



Until July 2024
Only 14 scanners found the threat, Many of the best-known AVs still do not detect this malware



BLOCKED

sample_metascan.html

Hypertext Markup Language - 108.9 KB

Infected | Other blocked reasons ...

File process | LOCAL/admin | Jan 14, 2024 at 11:52:04 AM | Jan 14, 2024 at 11:52:04 AM | 1,707 ms

METASCAN™ | DEEP CDR | PROACTIVE DLP | VULNERABILITY ASSESSMENT | FILE TYPE VERIFICATION | SANDBOX | SBOM | REPUTATION

Engine	Result	Definition Date	Scan Time
[redacted]	✓ No Threat Detected	2024-01-08 [6 days ago]	320 ms
[redacted]	✗ Trojan[Infect]/JS.Agent	2024-01-07 [7 days ago]	35 ms
[redacted]	✗ JS/Agent.G1	2024-01-07 [7 days ago]	49 ms
[redacted]	✓ No Threat Detected	2024-01-07 [7 days ago]	243 ms
[redacted]	✓ No Threat Detected	2024-01-06 [8 days ago]	257 ms
[redacted]	✗ TrojWare.JS.Agent.NKB	2024-01-07 [7 days ago]	19 ms
[redacted]	✓ No Threat Detected	2024-01-07 [7 days ago]	238 ms
[redacted]	✓ No Threat Detected	2024-01-07 [7 days ago]	350 ms
[redacted]	✗ Trojan.JS.Agent	2024-01-07 [7 days ago]	183 ms
[redacted]	✗ Exploit [04c55c361]	2024-01-08 [6 days ago]	28 ms

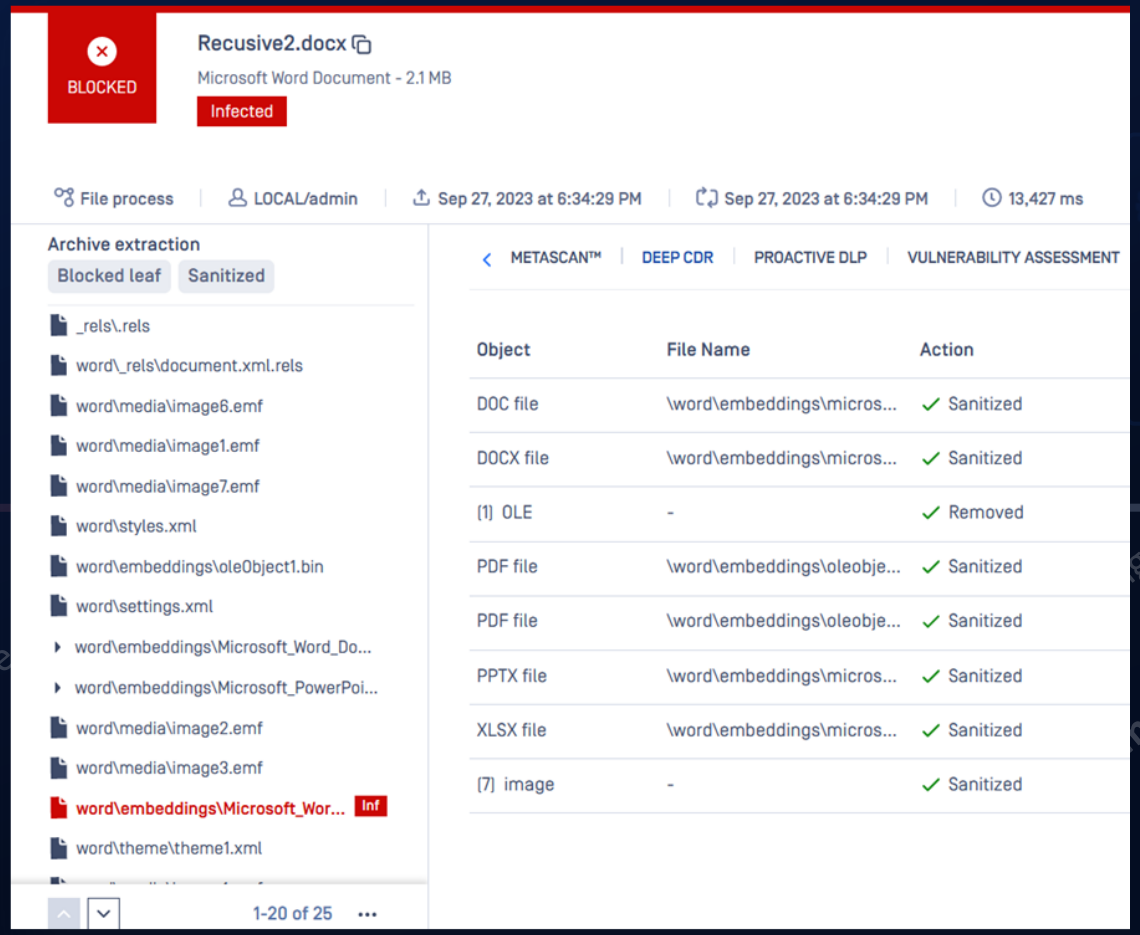
Untrusted Files

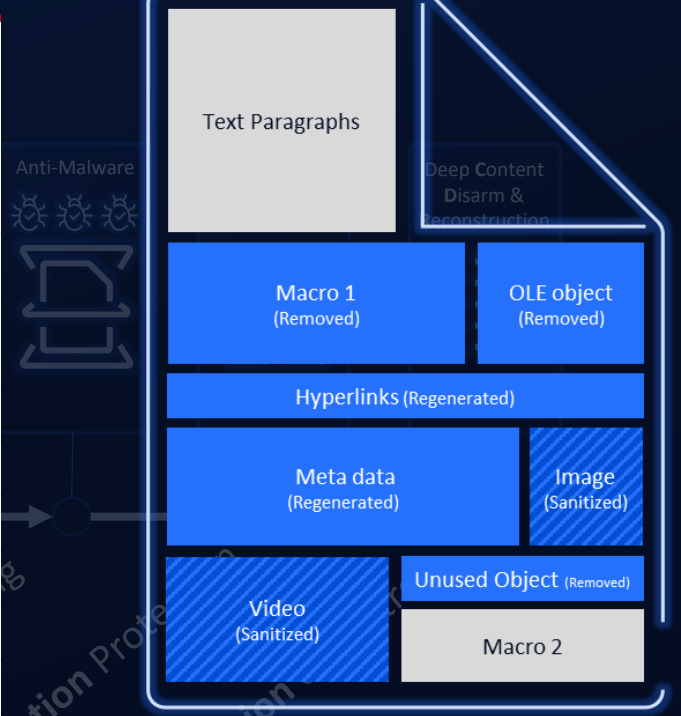
DLP

METADEFENDER CORE

Layered File Protection

MetaDefender CORE

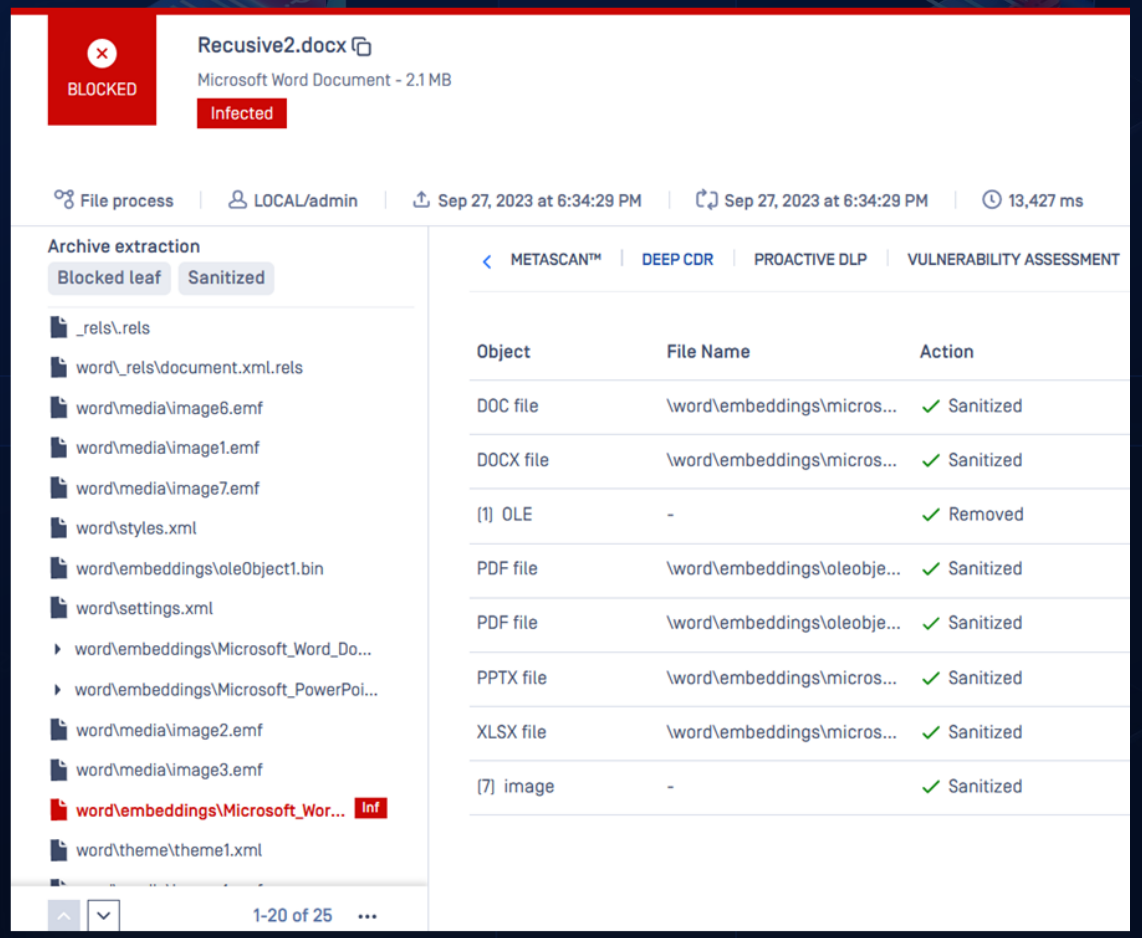


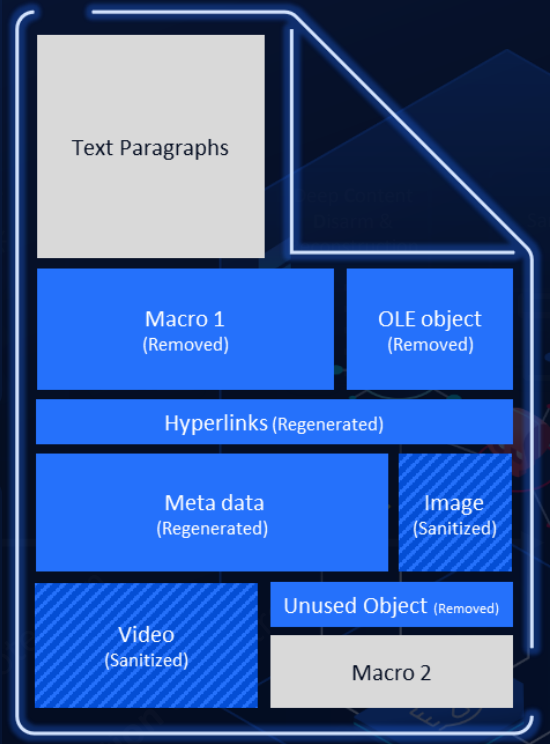


175+
supported file types

200+
file conversion options

100%
protection score
from SE Labs





175+
supported file types

200+
file conversion options

SE Labs AAA October 2023 Content Disarm and Reconstruction CDR Protection
OPSWAT Deep CDR

100%
protection score
from SE Labs

METADEFENDER CORE

Layered File Protection

MetaDefender CORE

Fast, Efficient & Inline Analysis

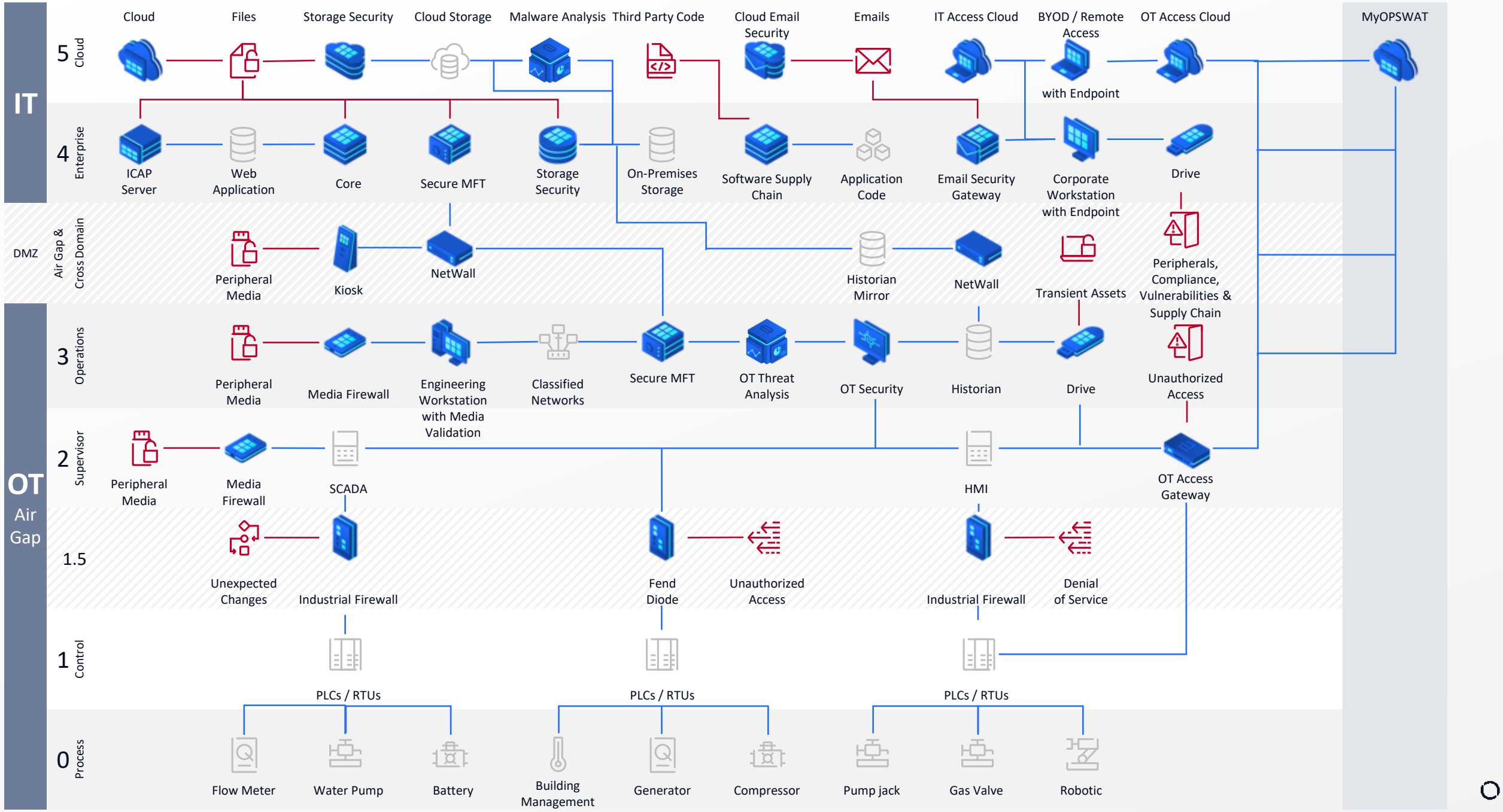
Deep Structural Analysis

Adaptive Threat Analysis

Next-Gen Threat Detection

How does this protection fit into your environment?

OPSWAT.

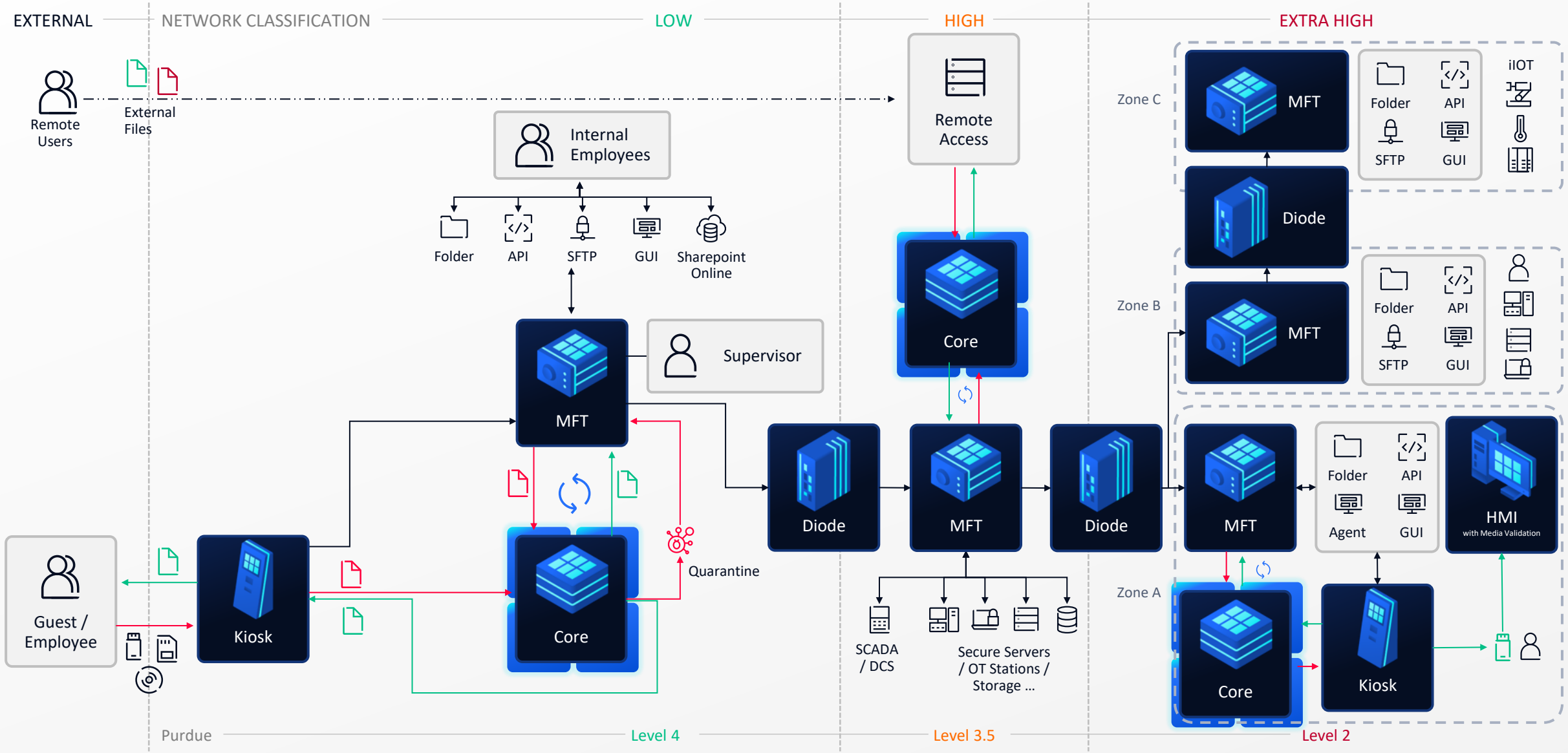

IT
OT
Air Gap
5 Cloud
4 Enterprise
DMZ
Air Gap & Cross Domain
3 Operations
2 Supervisor
1.5
1 Control
0 Process
Cloud
Files
Storage Security
Cloud Storage
Malware Analysis
Third Party Code
Cloud Email Security
Emails
IT Access Cloud
BYOD / Remote Access
with Endpoint
OT Access Cloud
MyOPSWAT
ICAP Server
Web Application
Core
Secure MFT
Storage Security
On-Premises Storage
Software Supply Chain
Application Code
Email Security Gateway
Corporate Workstation with Endpoint
Drive
Peripheral Media
Kiosk
NetWall
Historian Mirror
NetWall
Transient Assets
Peripherals, Compliance, Vulnerabilities & Supply Chain
Peripheral Media
Media Firewall
Engineering Workstation with Media Validation
Classified Networks
Secure MFT
OT Threat Analysis
OT Security
Historian
Drive
Unauthorized Access
Peripheral Media
Media Firewall
SCADA
HMI
OT Access Gateway
Unexpected Changes
Industrial Firewall
Fend Diode
Unauthorized Access
Industrial Firewall
Denial of Service
PLCs / RTUs
PLCs / RTUs
PLCs / RTUs
Flow Meter
Water Pump
Battery
Building Management
Generator
Compressor
Pump jack
Gas Valve
Robotic

How does this all come together?

OPSWAT.

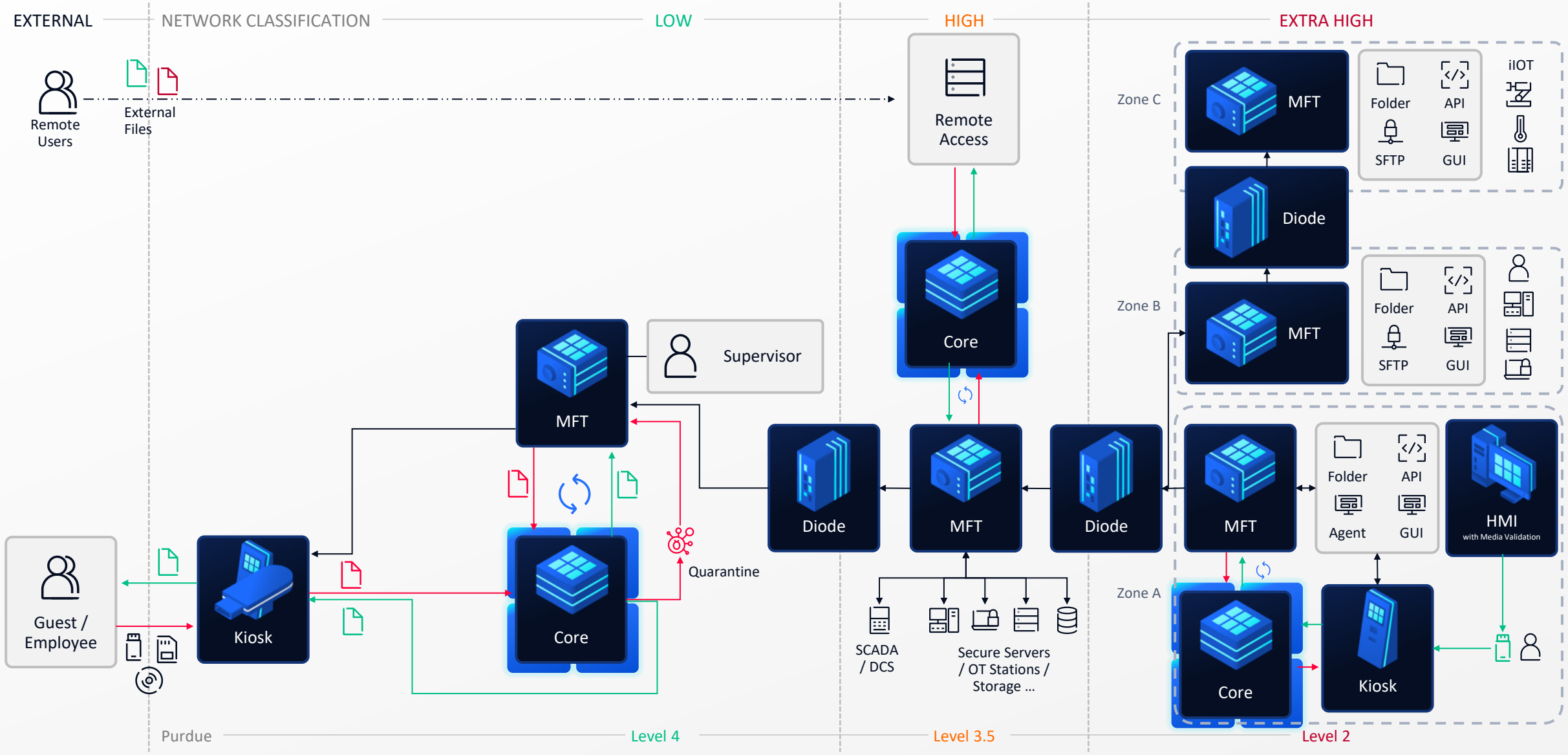
SECURING THE FLOW OF DATA

A Day in the Life of a Data File



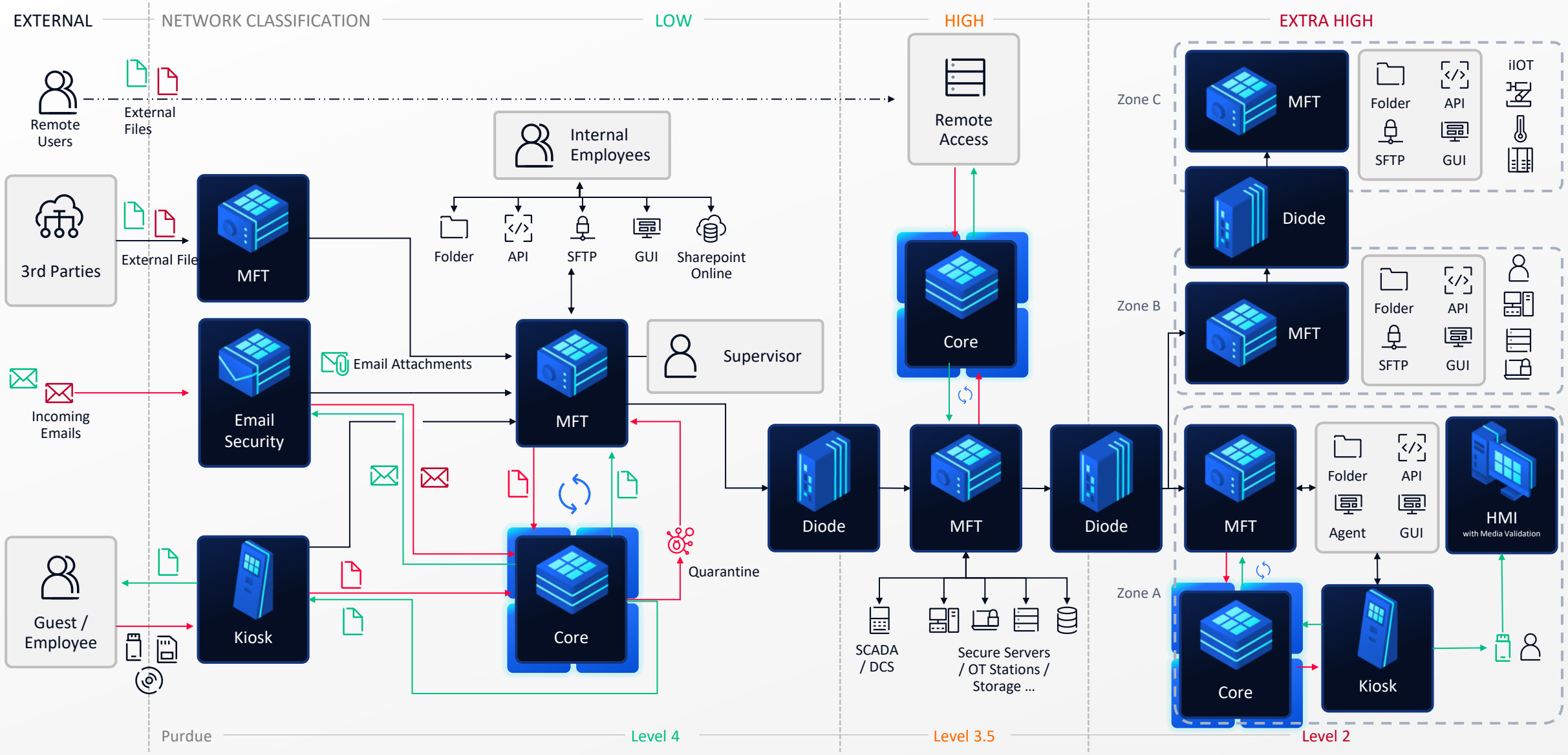
SECURING THE FLOW OF DATA

A Day in the Life of a Data File



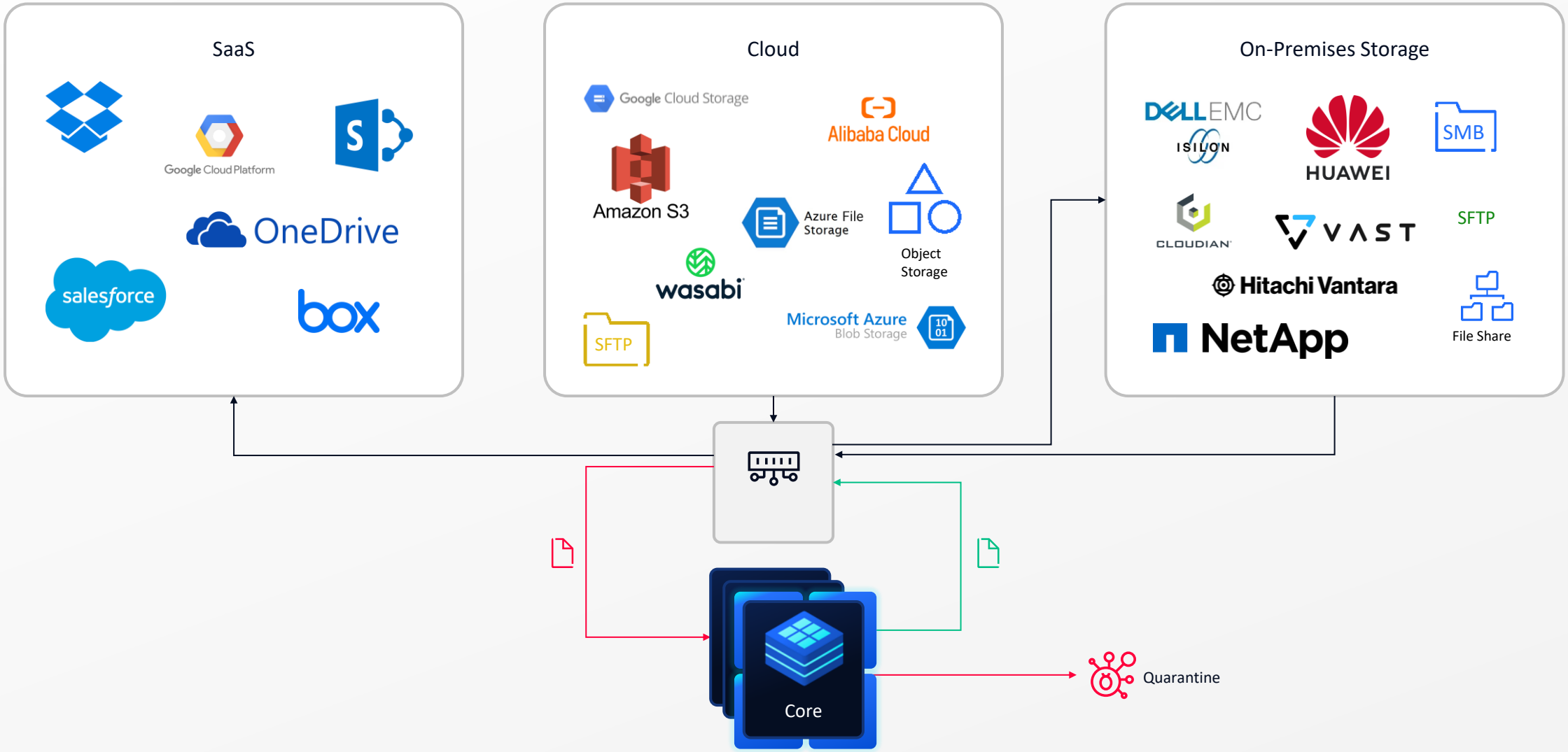
SECURING THE FLOW OF DATA

A Day in the Life of a Data File



SECURING THE FLOW OF DATA

Centralized File Security Data Flow



The OPSWAT Approach

Security Pedigree

#1 Market Leader in Multiscanning and Deep CDR

20+ Years expertise

30% Annual Turnover on **R&D**

Trusted by Many

9 out of 10 largest Global Defence
6 of the top 10 Pharmaceutical

20 Ministry of Defence in EMEA

4 of the largest Auto Manufacturers Globally

98% US Nuclear Sites

Customer Testimonial


OPSWAT.
Protecting the World's
Critical Infrastructure
Questions?

Thankyou

OPSWAT.