OPSWAT.

A Day in the Life of a File

– Aktive Abwehr im IT-/OT-Datenfluss

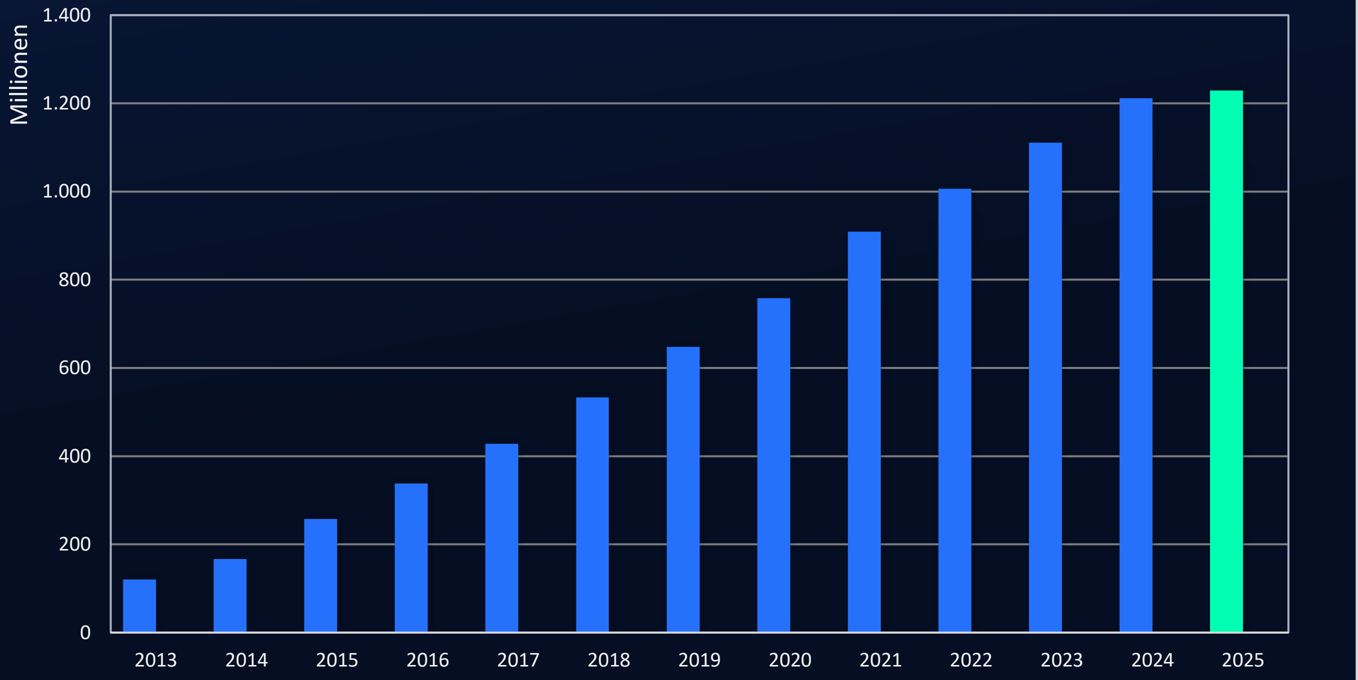
Petar Duic, Regional Sales Manager, Opswat

München, 3. März 2026

SECURITY & BUSINESS CHALLENGES

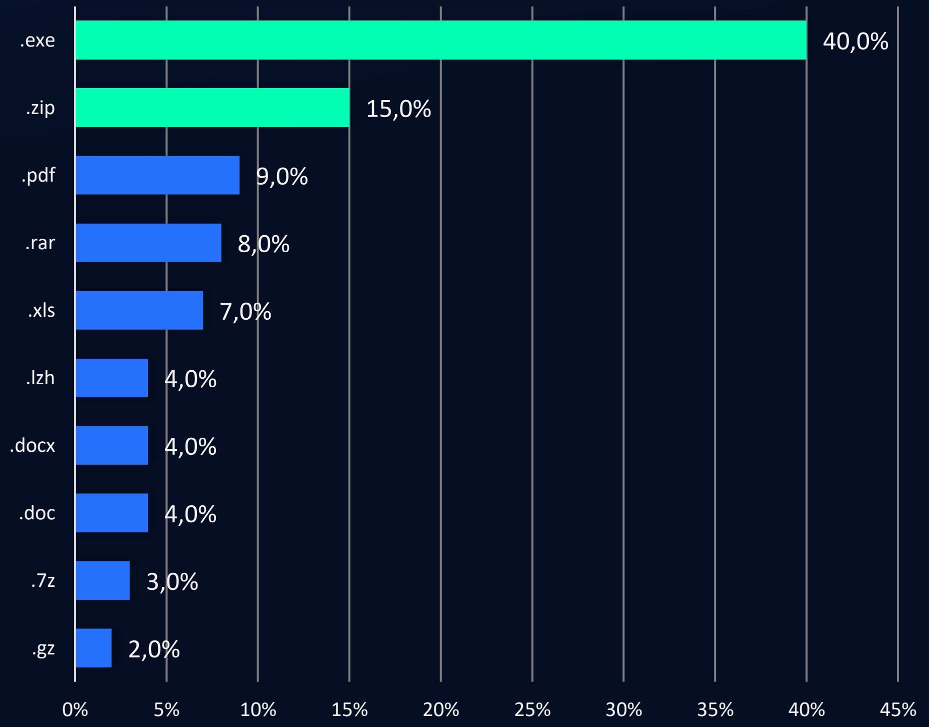
The Rise of File-Borne Malware

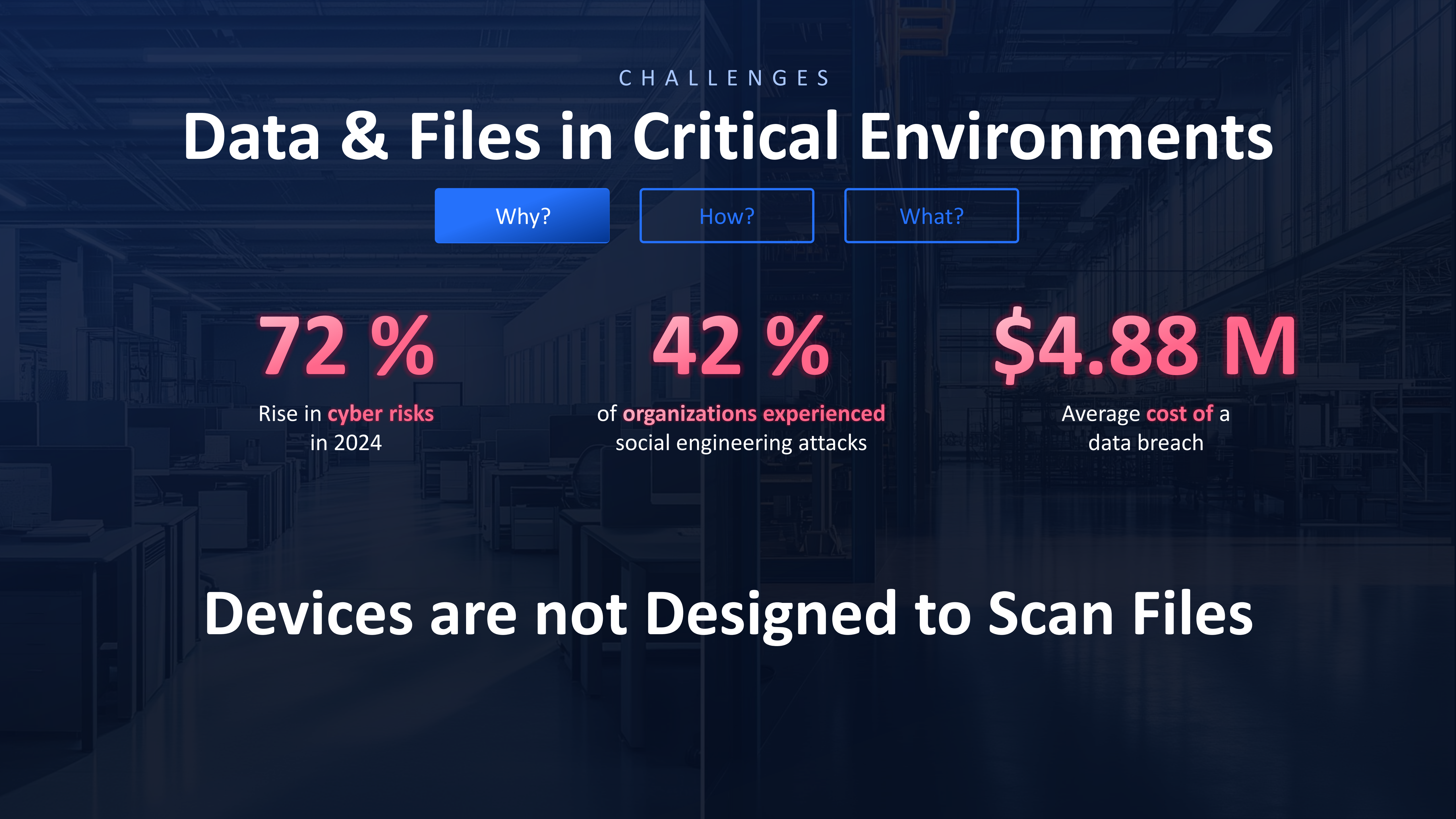
Total malware in 2025



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

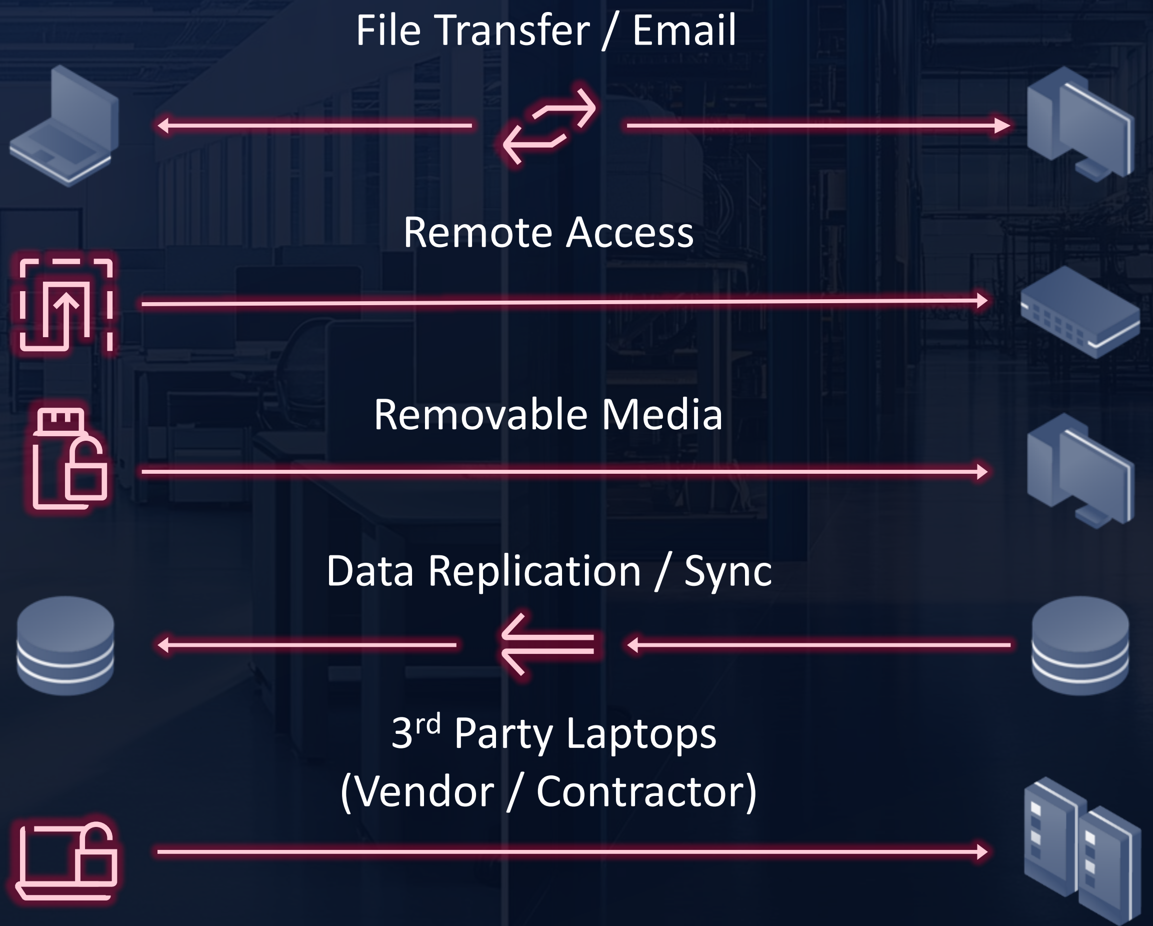
Average **cost of** a
data breach

Devices are not Designed to Scan Files

CHALLENGES

Data & Files in Critical Environments

Why? | **How?** | What?



File Transfer / Email

Remote Access

Removable Media

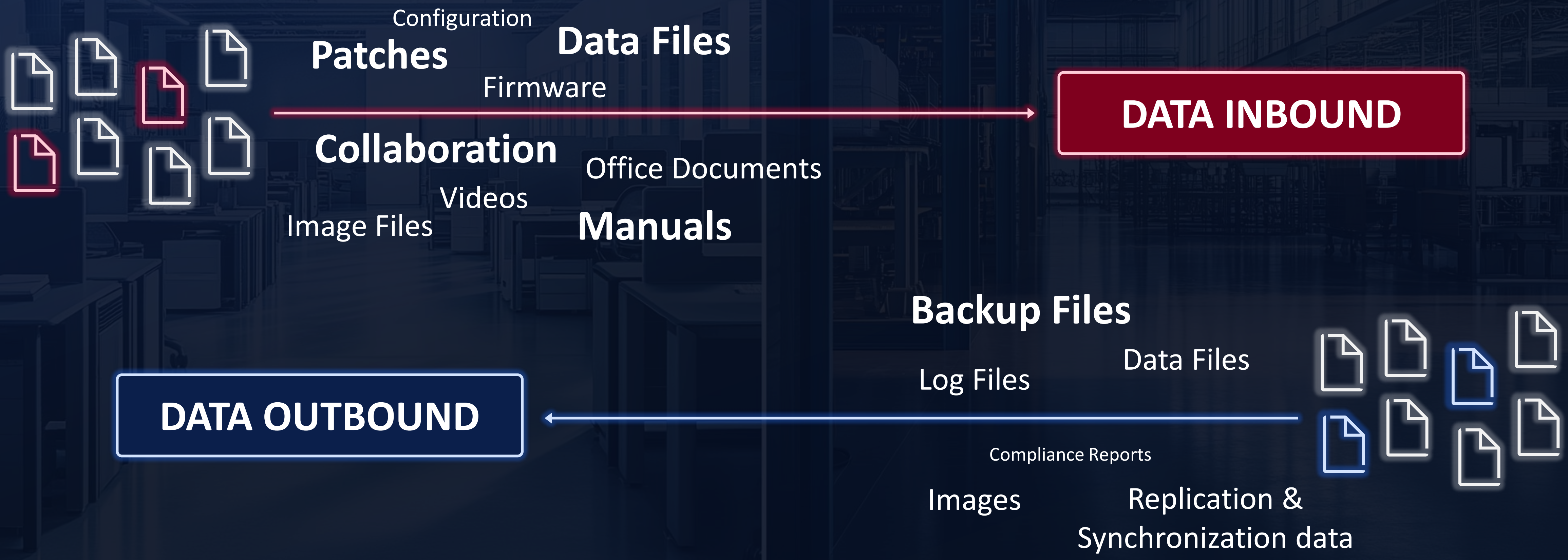
Data Replication / Sync

3rd Party Laptops
(Vendor / Contractor)

CHALLENGES

Data & Files in Critical Environments

Why? How? What?



Configuration

Patches

Data Files

Firmware

Collaboration

Office Documents

Videos

Image Files

Manuals

DATA INBOUND

Backup Files

Data Files

Log Files

Compliance Reports

Images

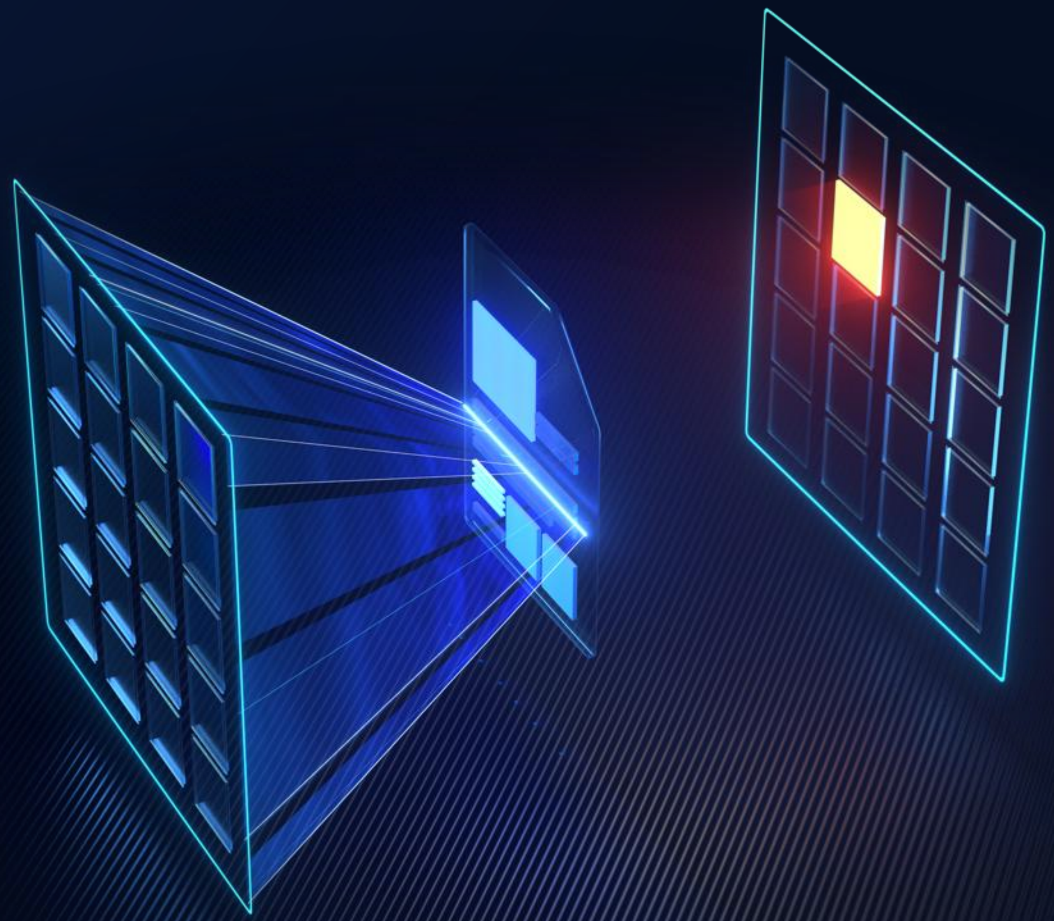
Replication & Synchronization data

DATA OUTBOUND

OPSWAT.

Multiscanning

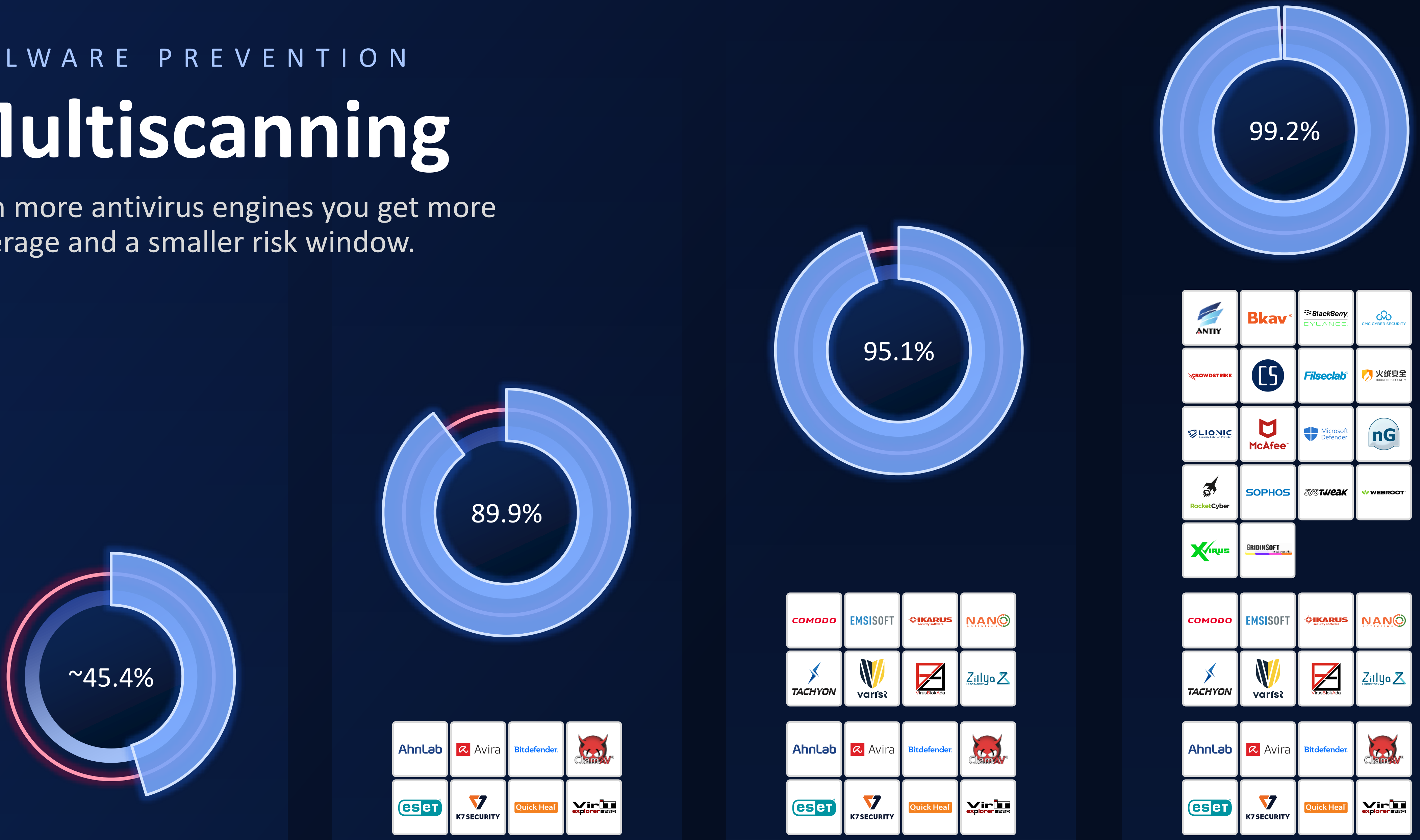
Detect nearly 100% of threats using 30+ antivirus engines simultaneously.



MALWARE PREVENTION

Multiscanning

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



Single Engine

8 Engines

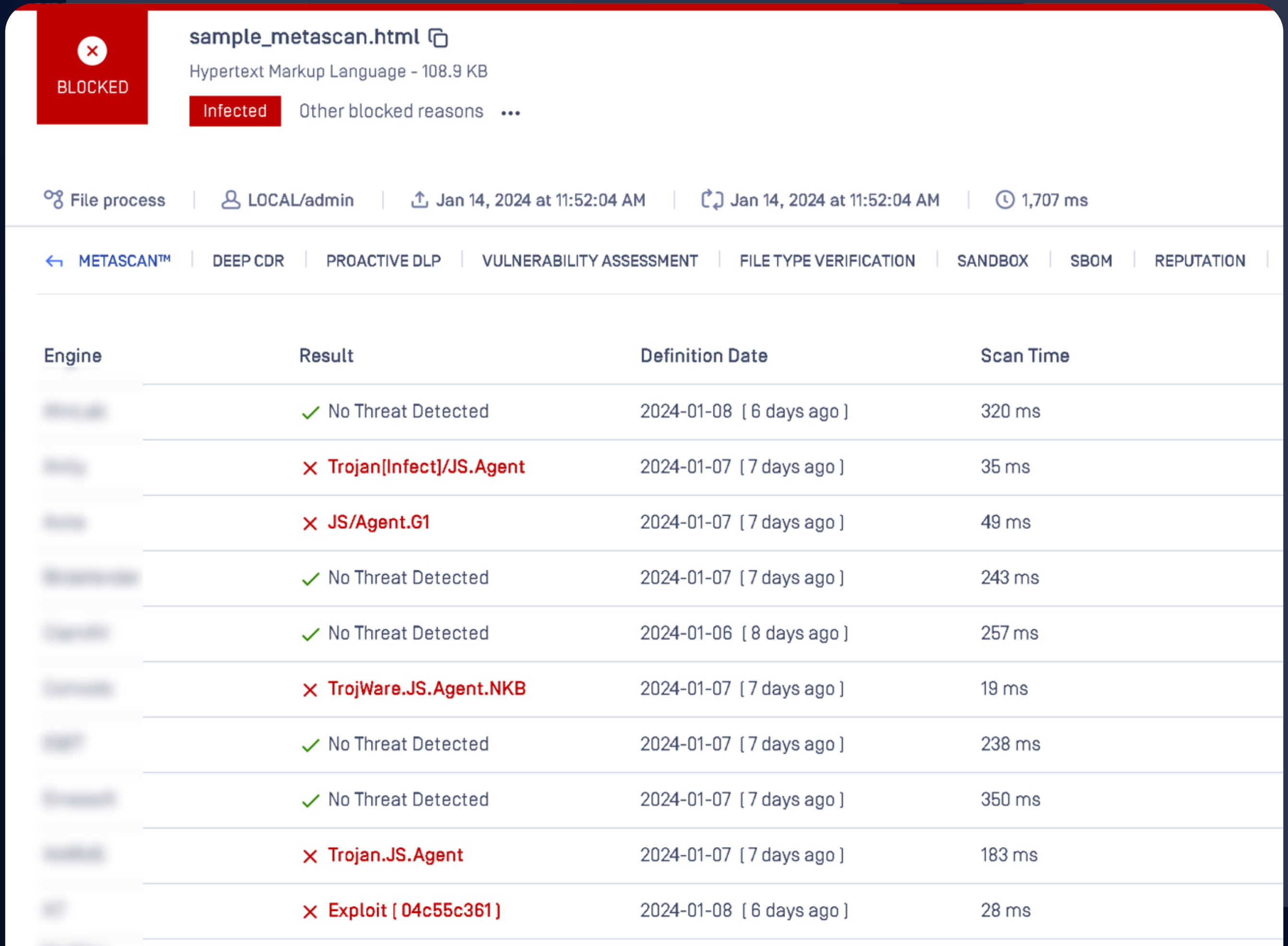
16 Engines

Max Engines

METASCAN™

Why Multiscanning

- Different AV vendors will be the first to discover new malware (polymorphic & non-polymorphic)
- Some AV vendors may take days, weeks, months, or even years to add detection
- AV Vendors use proprietary heuristic algorithms
- Different algorithms have their own strengths and weaknesses
- Proactive defense



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

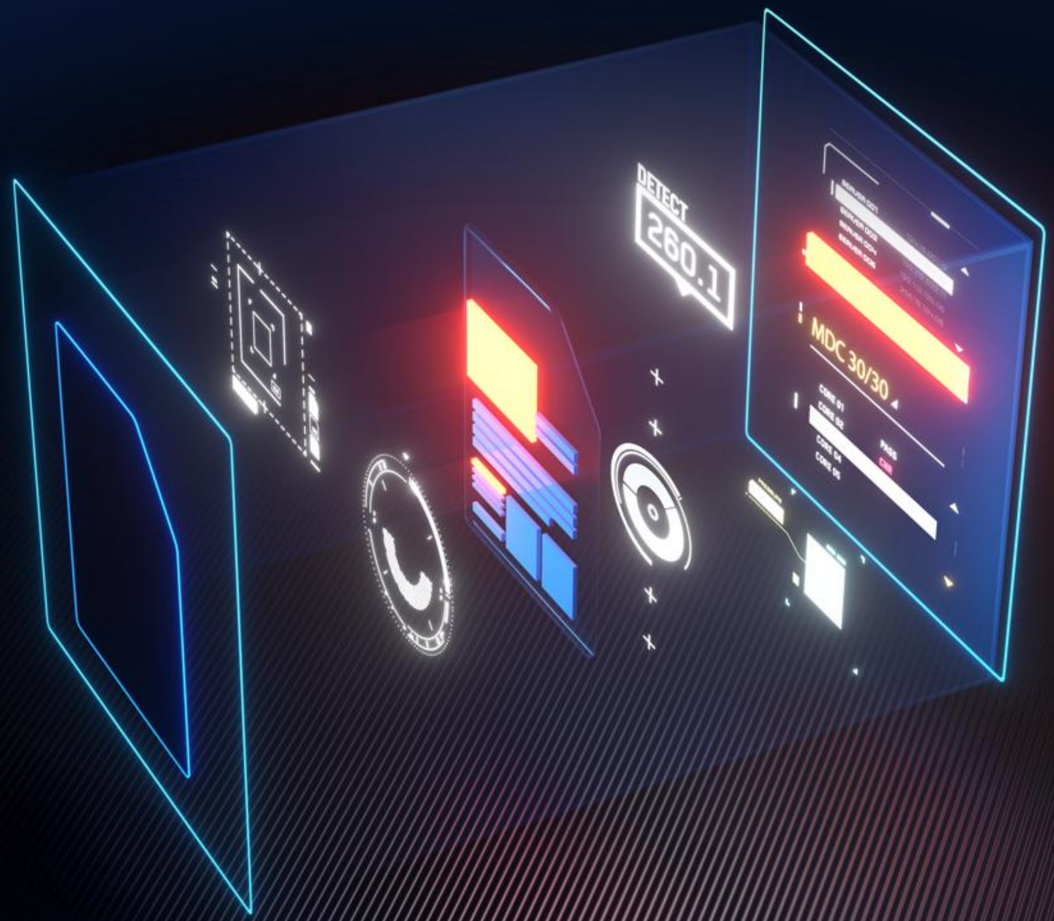
METASCAN™ | DEEP CDR | PROACTIVE DLP | VULNERABILITY ASSESSMENT | FILE TYPE VERIFICATION | SANDBOX | SBOM | REPUTATION

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

OPSWAT.

Adaptive Sandbox

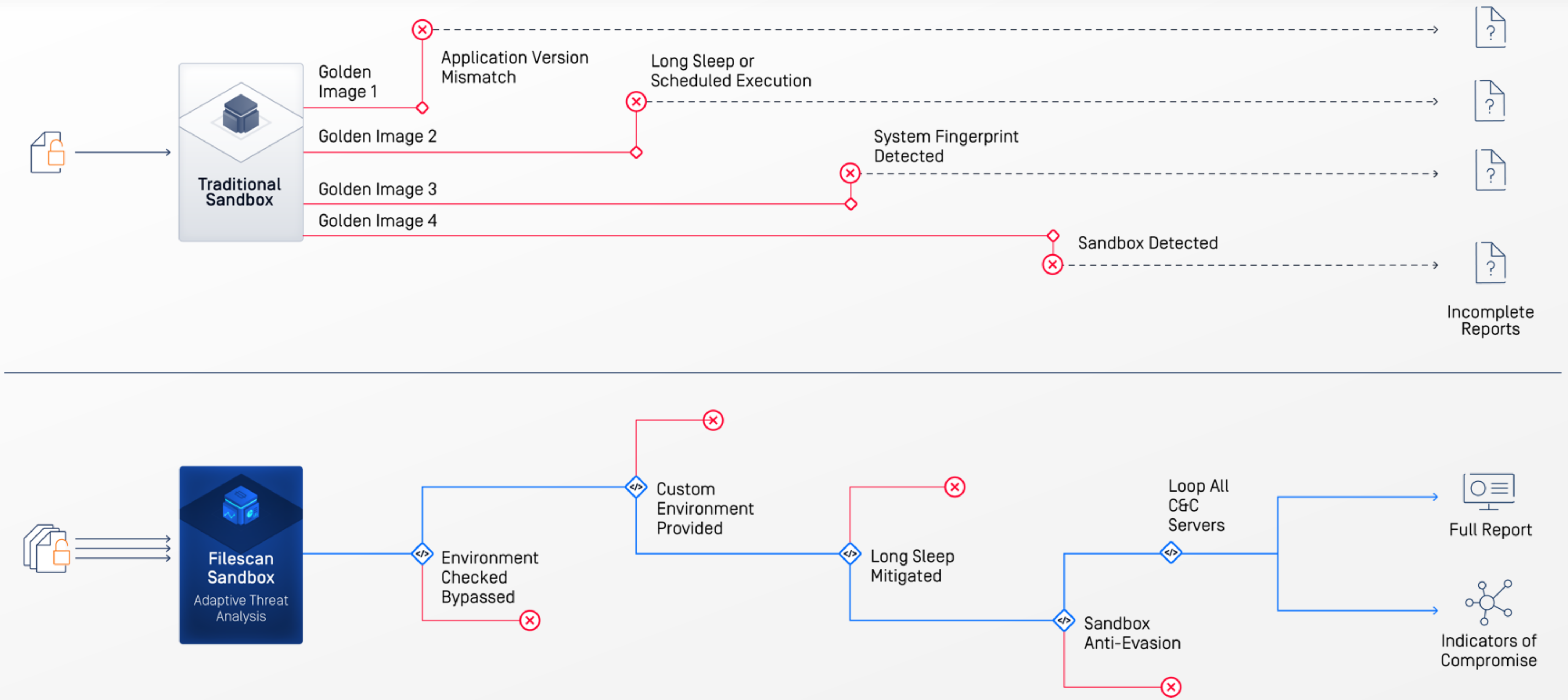
Adaptive threat analysis technology enables zero-day malware detection and extracts more indicators of comprise.



MALWARE PREVENTION

Adaptive Sandbox

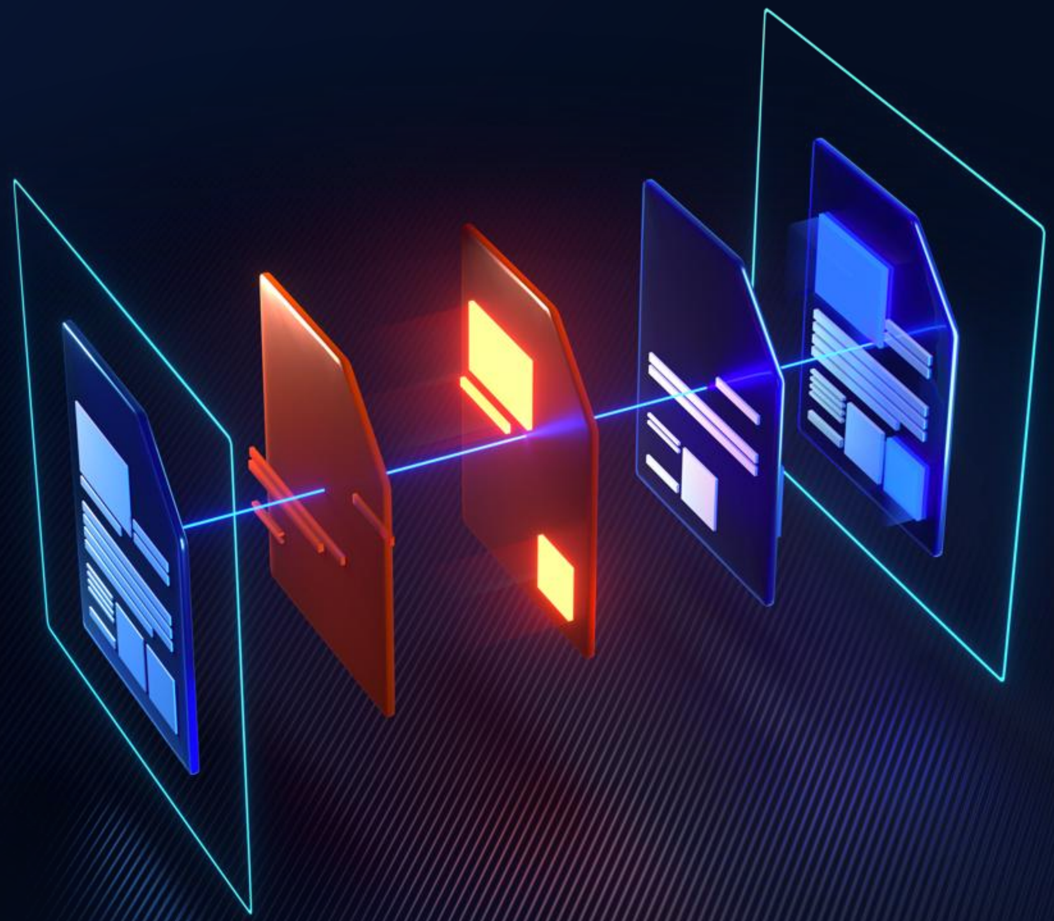
How our emulation-based sandbox works.



OPSWAT.

Deep CDR

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



DEEP CDR

What Deep CDR Does

✓ Identify & Scan

Verify file type and identify all active embedded content in file

✓ Regenerate & Convert

Disarm all the potentially malicious content and reconstruct the file with safe components

✓ Rebuild & Use

Generate a threat-free file with full functionality and quarantine the original file

Productivity Files,
Archives, HTMLs

Links, Media, Objects

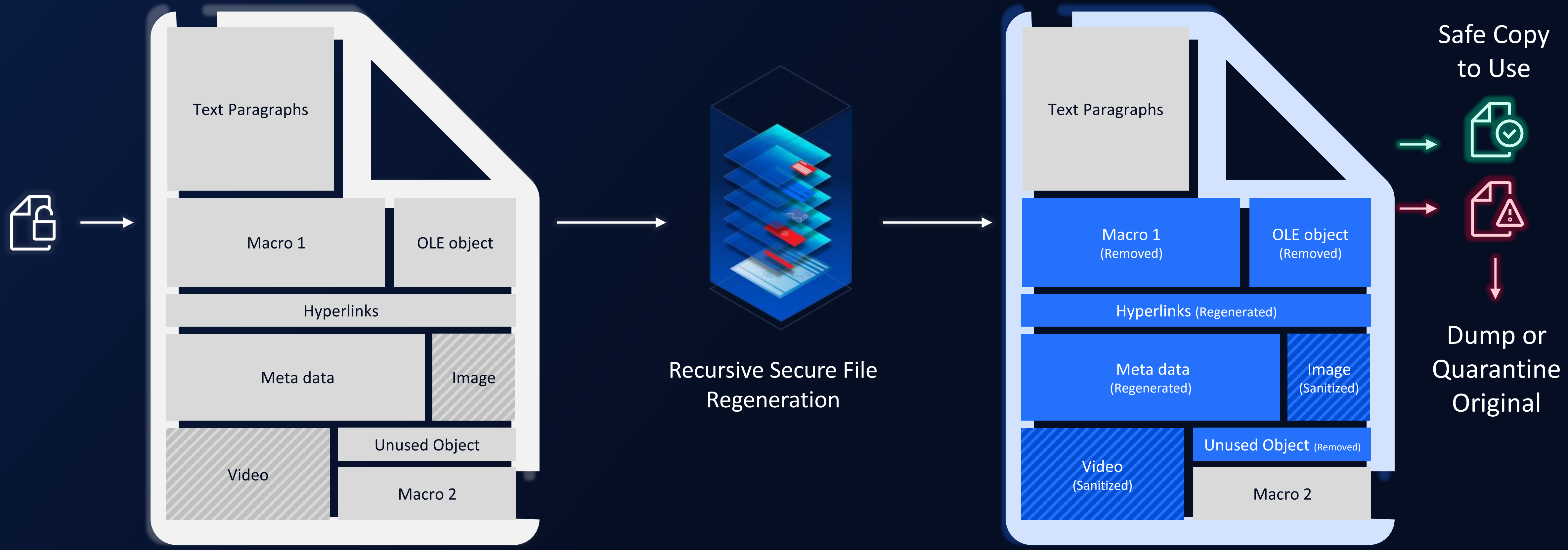
Clean Files
Usable Elements

OPSWAT.

MALWARE PREVENTION

Deep CDR

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



OPSWAT.

OPSWAT TECHNOLOGIES

File-Based Vulnerability Assessment

Detect Application Vulnerabilities Before They Are Installed

- Check certain types of software for known vulnerabilities before installation
- Scan systems for known vulnerabilities when devices are at rest
- Quickly examine running applications and their loaded libraries for vulnerabilities

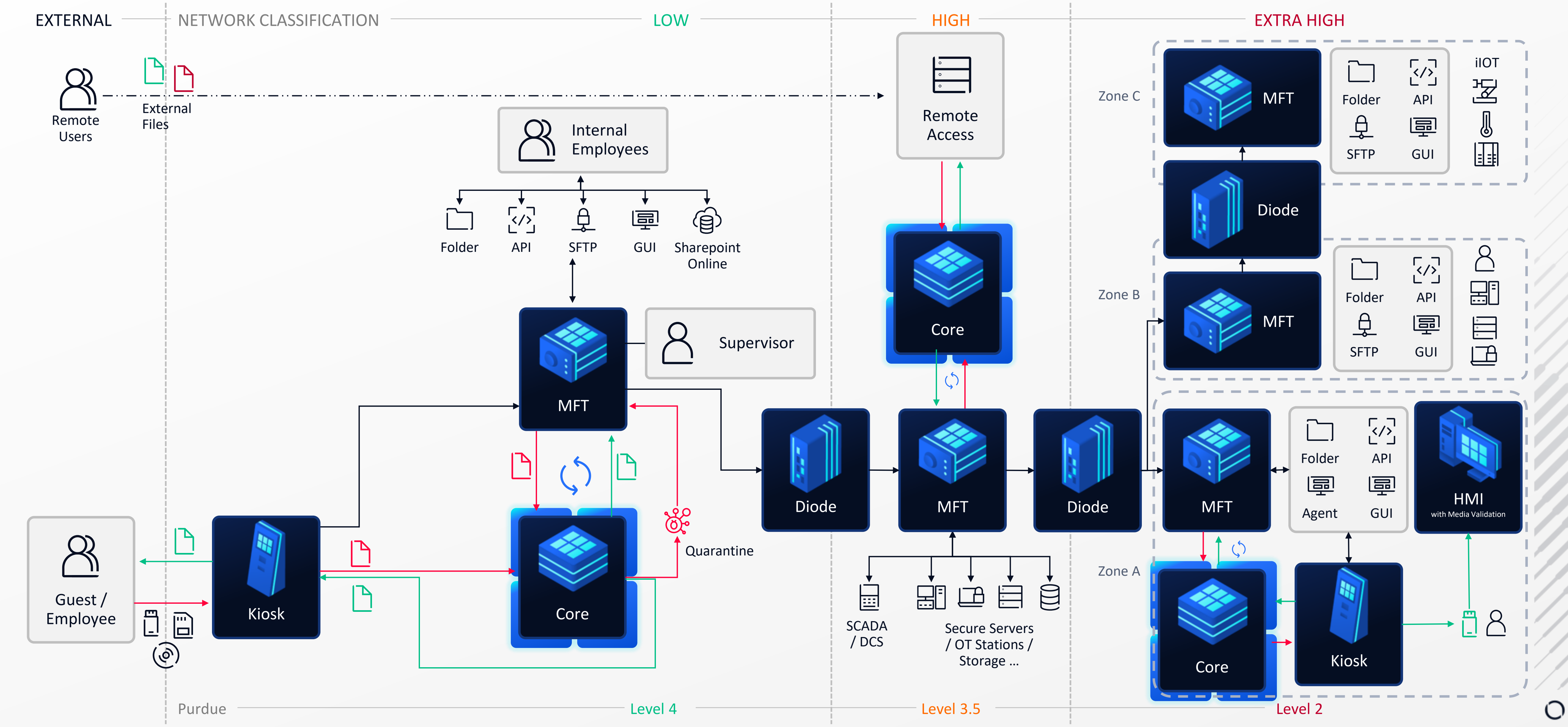
2.5k
Supported Vendors

30k+
Associated CVEs With Severity Information

3M
Identified Active Vulnerable Hashes

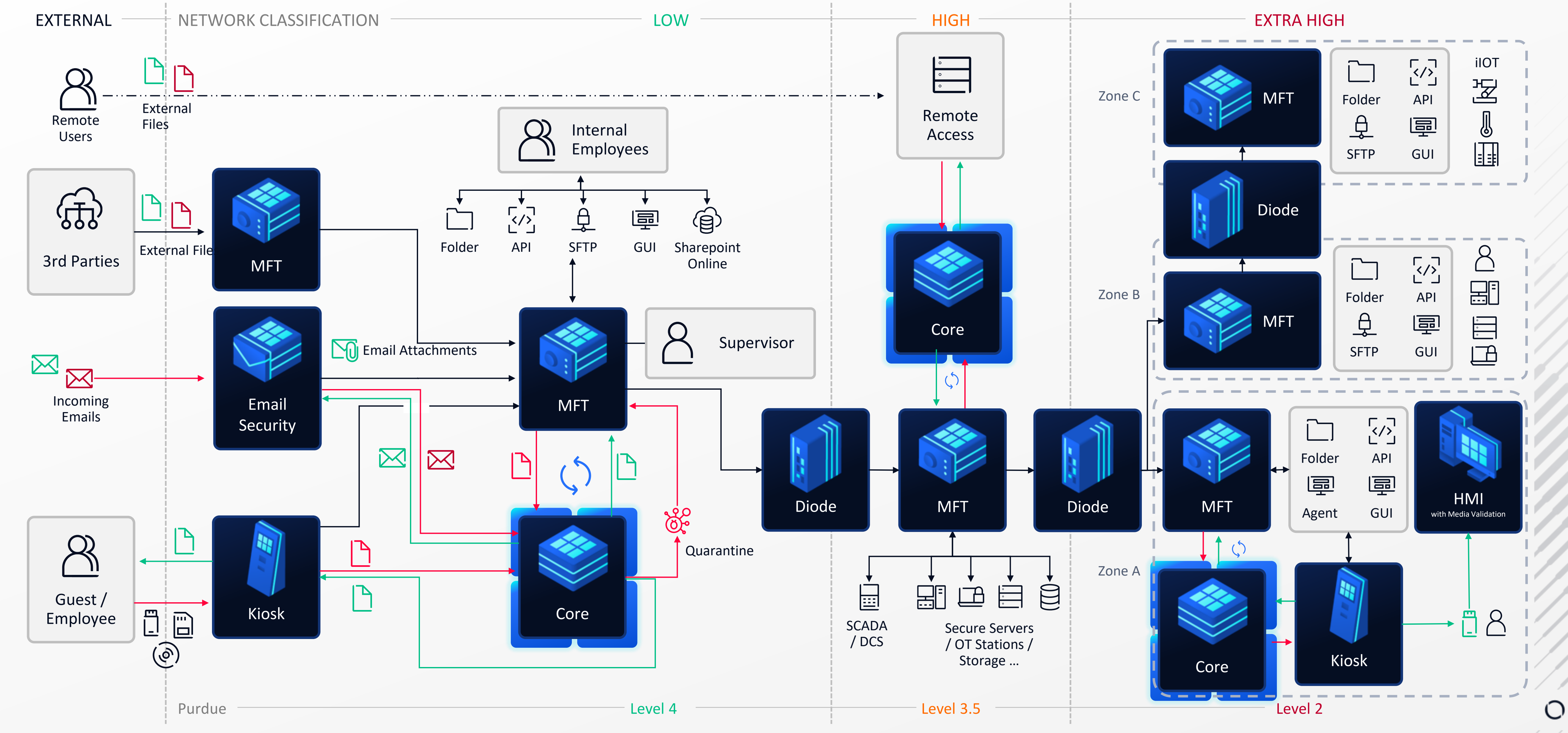
SECURING THE FLOW OF DATA

A Day in the Life of a Data File



SECURING THE FLOW OF DATA

A Day in the Life of a Data File



IT-Security
Roadshow 2026

controlware

Danke für Ihre Aufmerksamkeit.