OPSWAT.

Cross Domain Security

Eliminating Cyber Threats to Safeguard your IT & OT Network

Prepared for: ITSA ´23

Prepared by: Christian Reuling, Sales Engineer

Wednesday, October the 11th

Introduction

OPSWAT.

We Protect the World’s Critical Infrastructure

Today’s Agenda

Who is OPSWAT?

OPSWAT Cross Domain Solution

Who is OPSWAT?

Twenty Years of Innovation

60+

Countries

600+

Employees

1500+

Customers

100M+

End Points Protected

20+

Years of Expertise

90K+

Professionals Certified

2023 Cybersecurity Excellence Awards
Gold – ICS/SCADA Security
Gold – Web Application Security
Gold – CS Solution

2023 Globee Awards
Bronze – Cybersecurity

2022 CyberSecurity Breakthrough Awards
Prof Certification Program of the Year

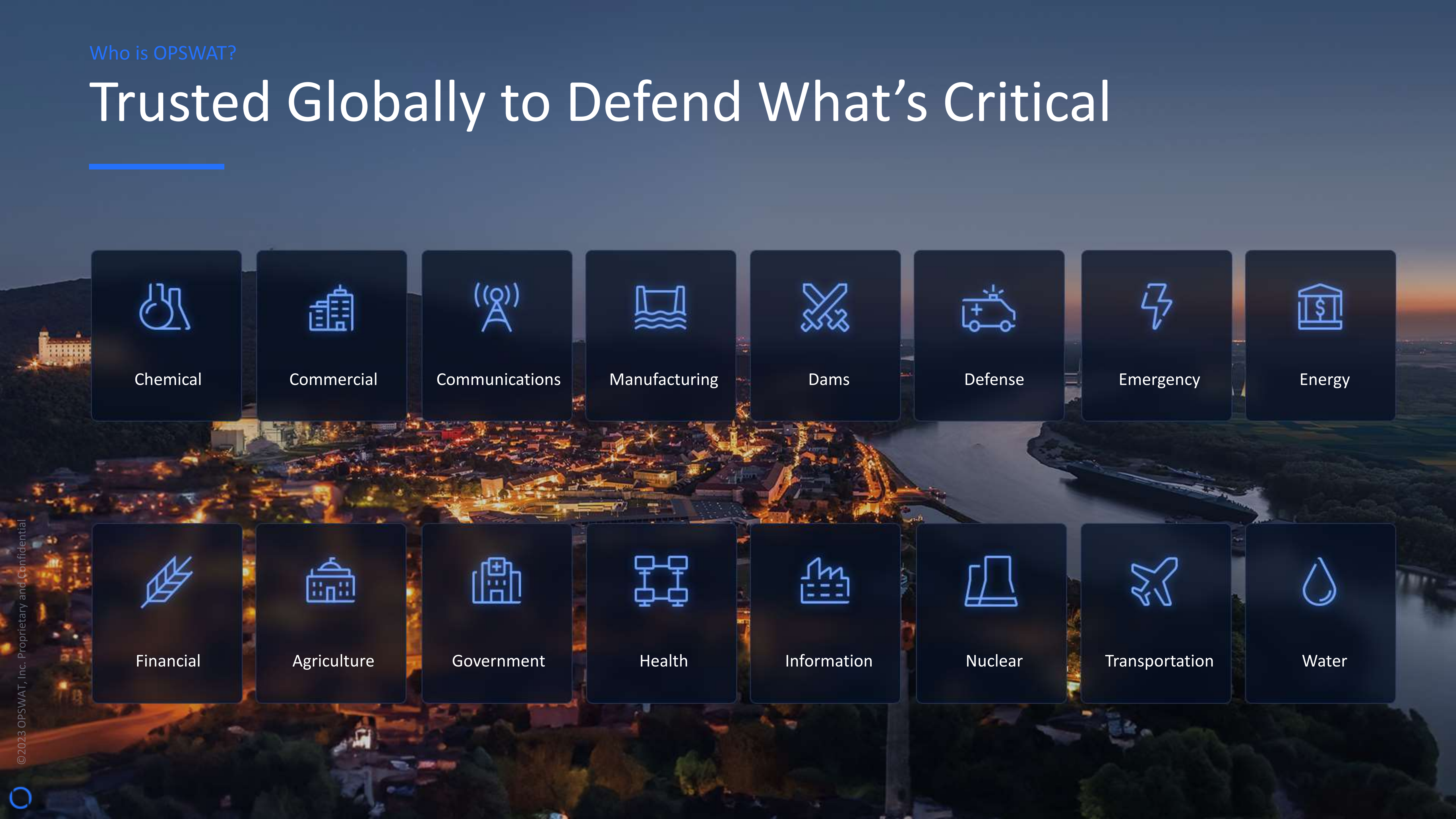
2022 CIOCoverage
Top 10 Leading VMware Partner

2023 The Channel Co.
CRN Partner Program Guide

2022 Cybersecurity Excellence Awards
Gold – Cybersecurity Education Provider
Gold – Content Disarm & Reconstruction
Gold – Critical Infrastructure Security

Who is OPSWAT?

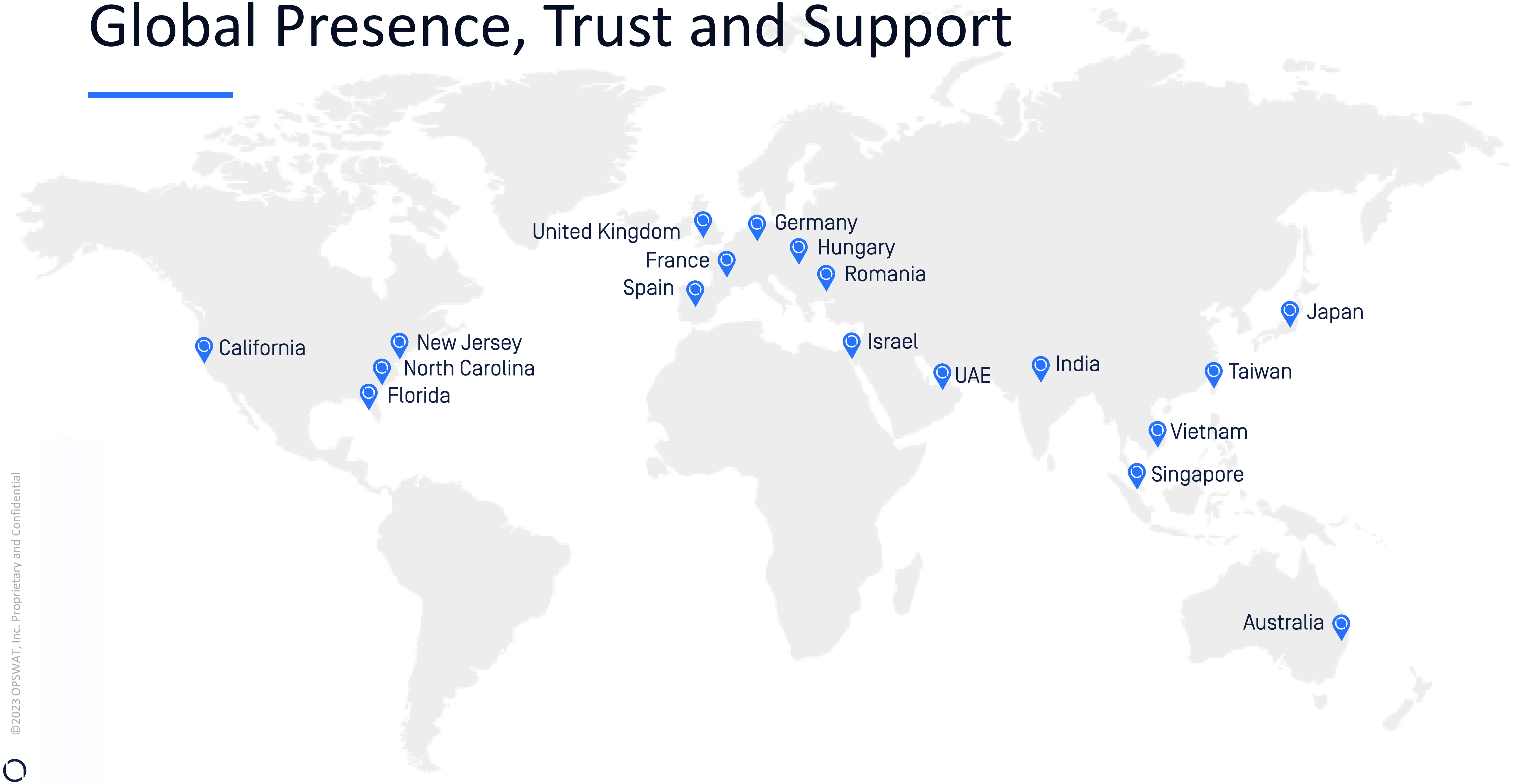
Trusted Globally to Defend What’s Critical



- Chemical
- Commercial
- Communications
- Manufacturing
- Dams
- Defense
- Emergency
- Energy
- Financial
- Agriculture
- Government
- Health
- Information
- Nuclear
- Transportation
- Water

Who is OPSWAT?

Global Presence, Trust and Support



Today’s Agenda

Who is OPSWAT?

OPSWAT Cross Domain Solution

Why OPSWAT?

Your Files.
Your Weakness.

“In 2022, malware saw a rapid resurgence from its seven-year low in 2021 – climbing to an astonishing **1.2 billion attacks**.”

“PDF, Word and .EXE files serve as the payload mechanism for over **62% of malware**.”

https://parachute.cloud/cyber-attack-statistics-data-and-trends/
https://www.comparitech.com/antivirus/malware-statistics-facts/

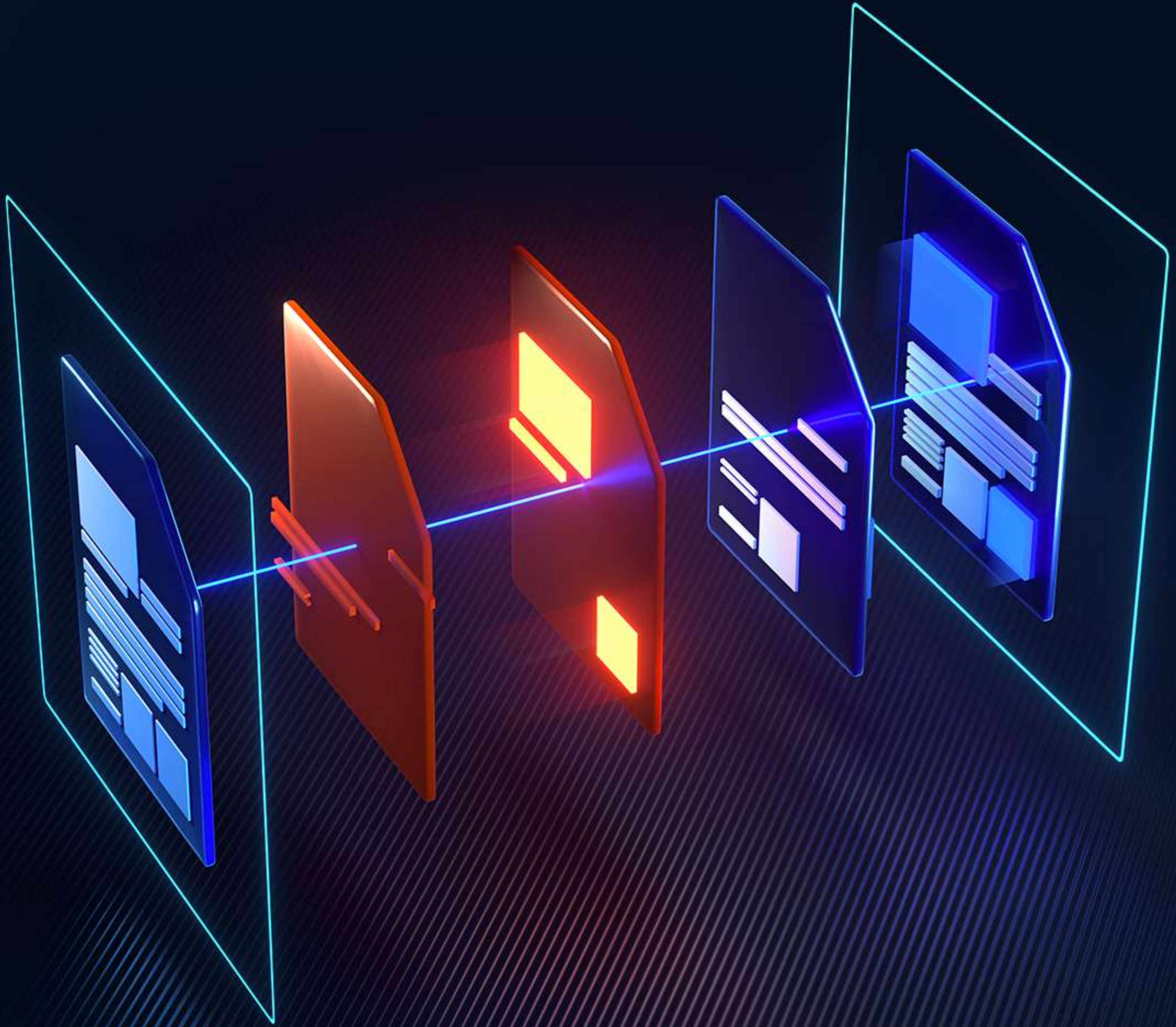
Why OPSWAT?

Trust no file.
Trust no device.

Our philosophy drives our products and defines our mission. We believe that all files and devices are malicious until they are confirmed otherwise.

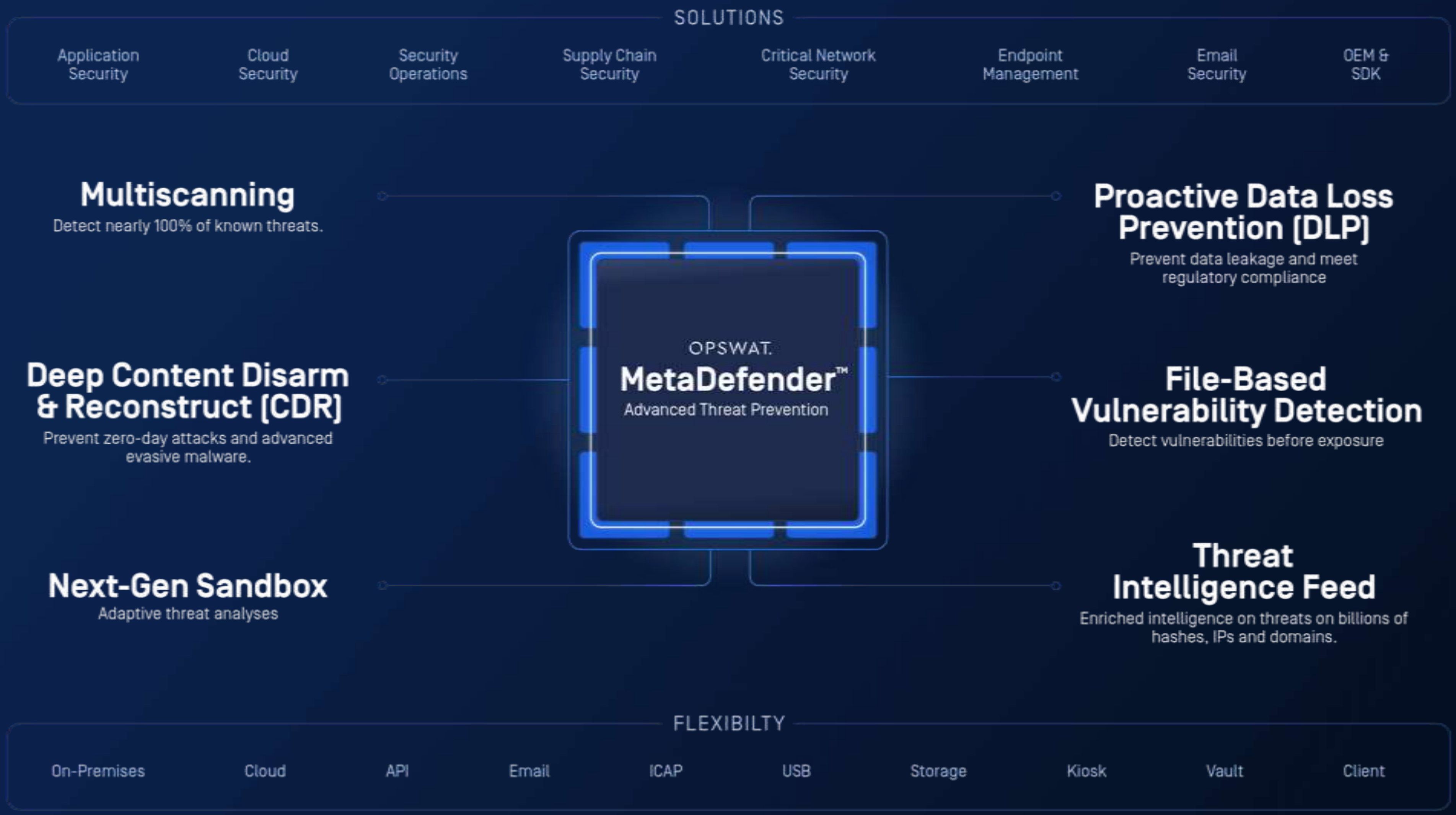
Assume All Files Are Malicious

Treat every file, whether it is from a known or unknown source, as potentially harmful until proven otherwise. This approach encourages the use of robust security measures, such as multi-scanning, content disarm and reconstruction (CDR), and data sanitization, to verify and neutralize threats.



Why OPSWAT?

MetaDefender Core Technology Engine



SOLUTIONS

Application Security | Cloud Security | Security Operations | Supply Chain Security | Critical Network Security | Endpoint Management | Email Security | OEM & SDK

Multiscanning
Detect nearly 100% of known threats.

Deep Content Disarm & Reconstruct (CDR)
Prevent zero-day attacks and advanced evasive malware.

Next-Gen Sandbox
Adaptive threat analyses

OPSWAT.
MetaDefender™
Advanced Threat Prevention

Proactive Data Loss Prevention (DLP)
Prevent data leakage and meet regulatory compliance

File-Based Vulnerability Detection
Detect vulnerabilities before exposure

Threat Intelligence Feed
Enriched intelligence on threats on billions of hashes, IPs and domains.

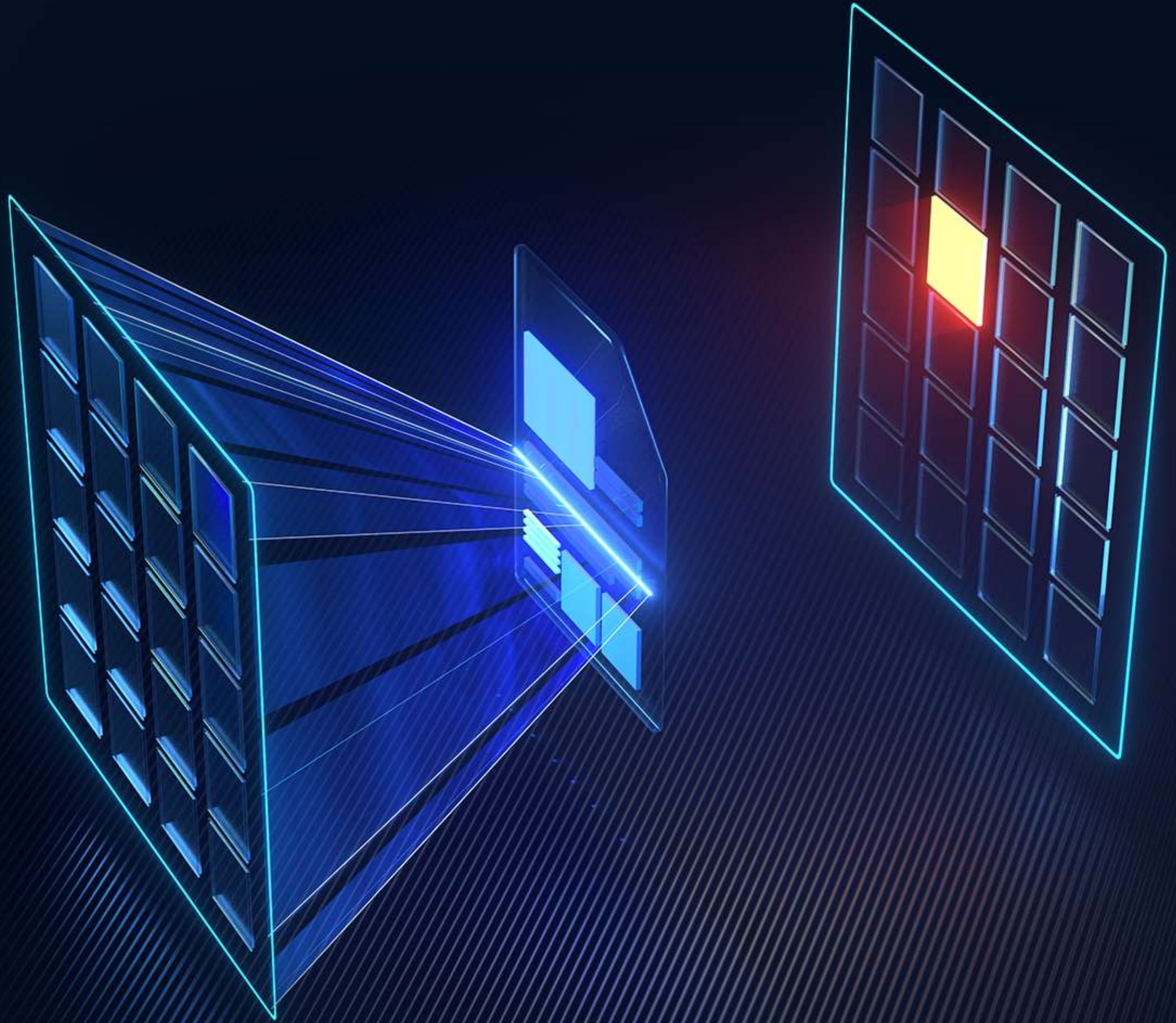
FLEXIBILTY

On-Premises | Cloud | API | Email | ICAP | USB | Storage | Kiosk | Vault | Client

Why OPSWAT?

Multiscanning

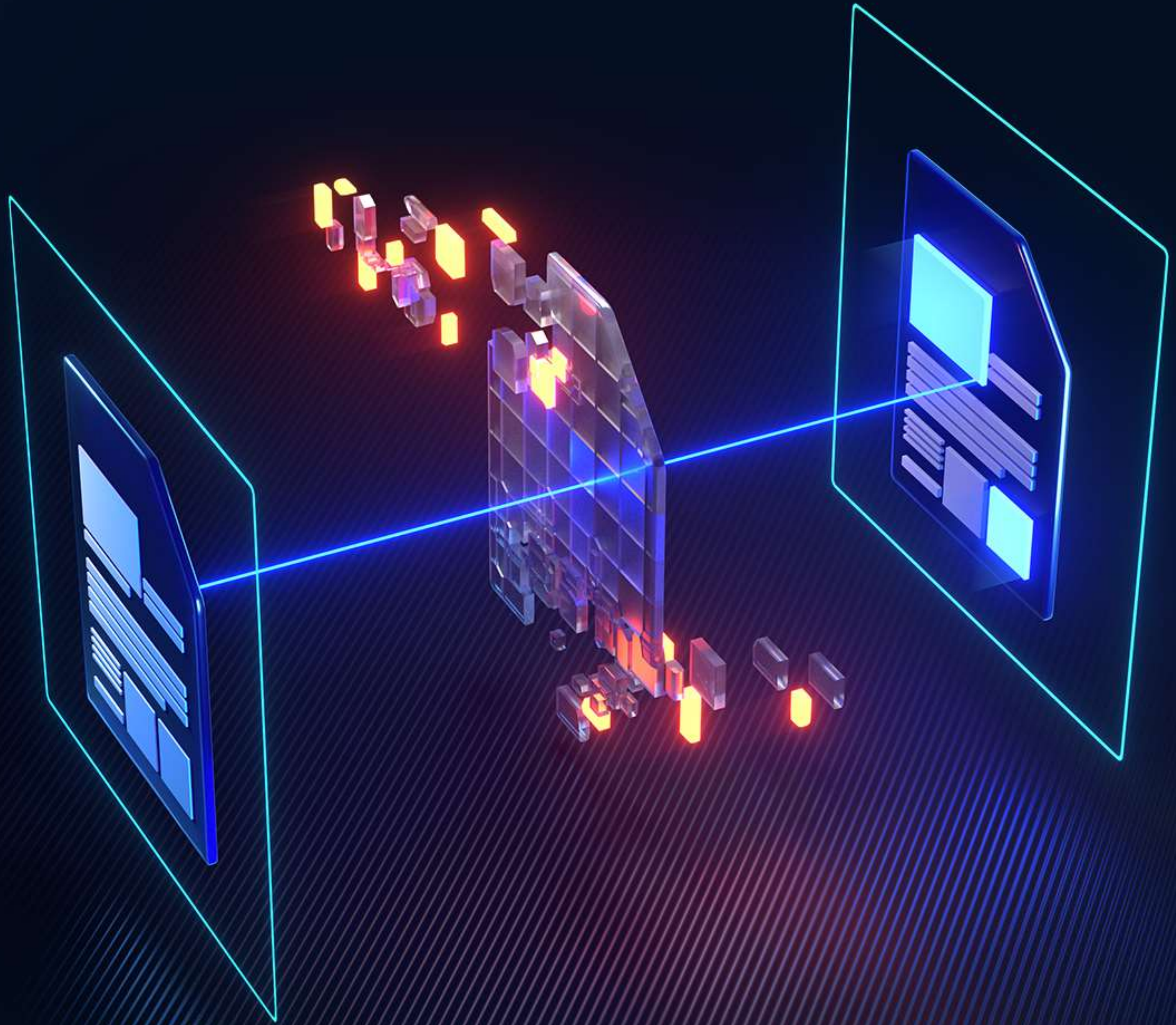
- 30+ commercial anti-malware engines in one solution
- Combine analysis based on signatures, heuristics, AI/ML, algorithms, emulation, NGAV accelerates detection of new and evolving malware
- Near 100% malware detection rate
- Faster outbreak detection- proactive defense-in-depth dramatically reduces Mean Time to Detect (MTTD)
- Lower false positives



Why OPSWAT?

Deep CDR

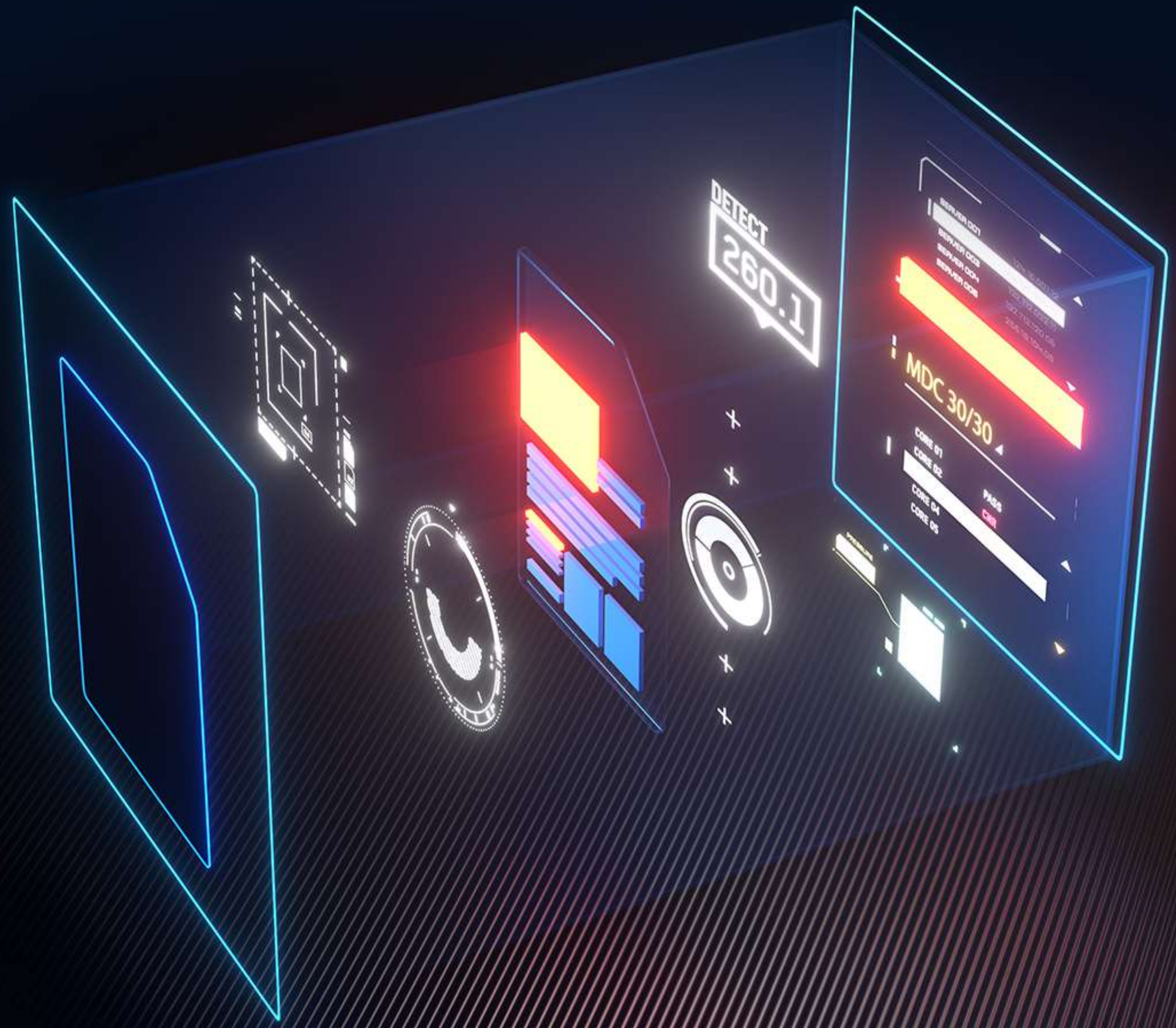
- Recursive sanitization within milliseconds even for nested archives
- Remove all embedded active content
- 100+ file types
- 200+ sanitization/conversion options
- 100s of file type verification
- Deep Image Sanitization
- Steganography
- Metadata/Headers
- Hyperlinks



Why OPSWAT?

Next Gen Sandbox

- Advanced emulation technology
- Patented technology to execute every code branch -> efficient in detecting targeted attacks and extracting IOCs
- Not using virtual machines like traditional sandboxes
- 10x faster and 10x less resource intensive

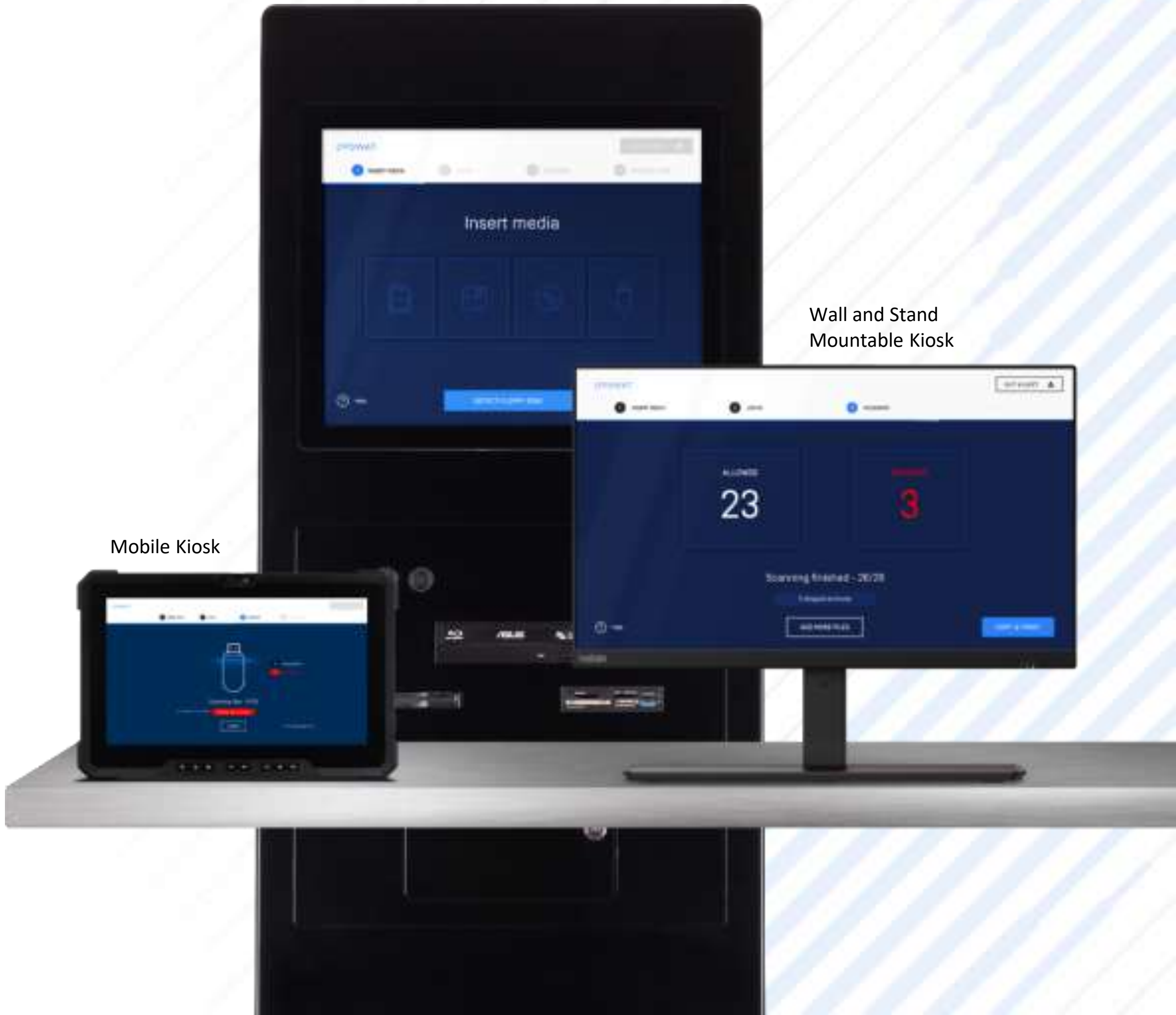


MetaDefender Kiosk™

- Industry leading enforceable end-to-end removable media security solutions
- Improve control of inbound and outbound content across critical networks
- Simplify compliance and reporting
- Turnkey set-up, intuitive configuration and management
- Modular deployment configurations easily tailored to fit any critical environment

Features:

- Over 30 different AV engines
- Deep Content Disarm & Reconstruction (CDR)
- Embedded next-gen sandbox
- Scan 20+ Media Types
- Enforce Scanning Policies
- Country of Origin Check
- File Vulnerability Assessment
- Windows or Linux OS
- 9 Languages Supported



Freestanding Kiosk

Wall and Stand Mountable Kiosk

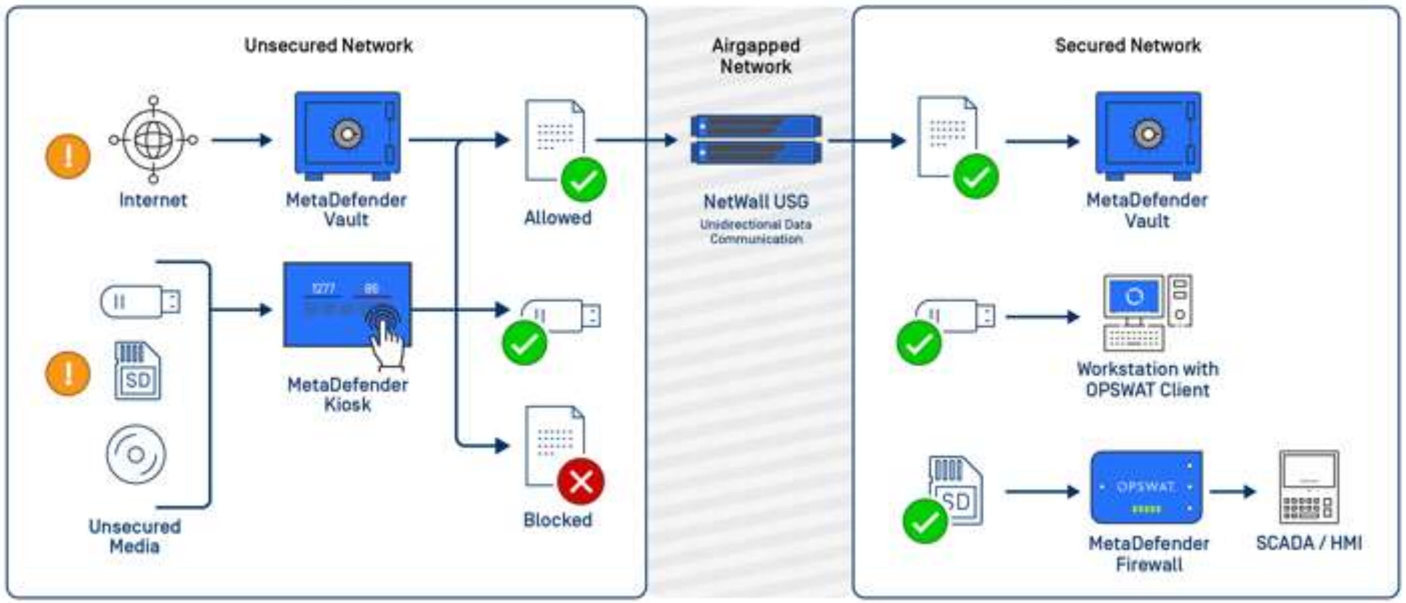
Mobile Kiosk

MetaDefender Vault

Secure data transfers for supply chain and IT/OT segment transfers

Features:

- Secure data transfer and storage
- End to End armored pipe for safe data transfer using TLS 1.3
- Reliable connection SHA256 when hashing files per FIPS 140-2
- Enables remote uploads, and secure transfers across network segments
- Multiscan and send sanitized files securely over a LAN or a WAN network



OPSWAT NetWall™ USG, BSG & Optical Diode

Security Gateway for IT & OT Convergence

NetWall USG – Unidirectional Security Gateway
NetWall BSG – Bilateral Security Gateway
NetWall OPT – Optical Diode

- ✓ Airtight protection for OT/ICS-to-IT communication
- ✓ Secure, segmented, unidirectional data paths
- ✓ True protocol break, non routable connection
- ✓ Easy deployment and operation

Features

Unidirectional flow – A non-networked connection between the NetWall server pairs enforces one-way data flows

No data loss – Delivery assurance mechanism in **USG** and **BSG** assures reliable operation, eliminates data overflow and conserves valuable bandwidth

Deterministic One-Way – NetWall Optical Diode is physical layer enforce one-way transfer solution

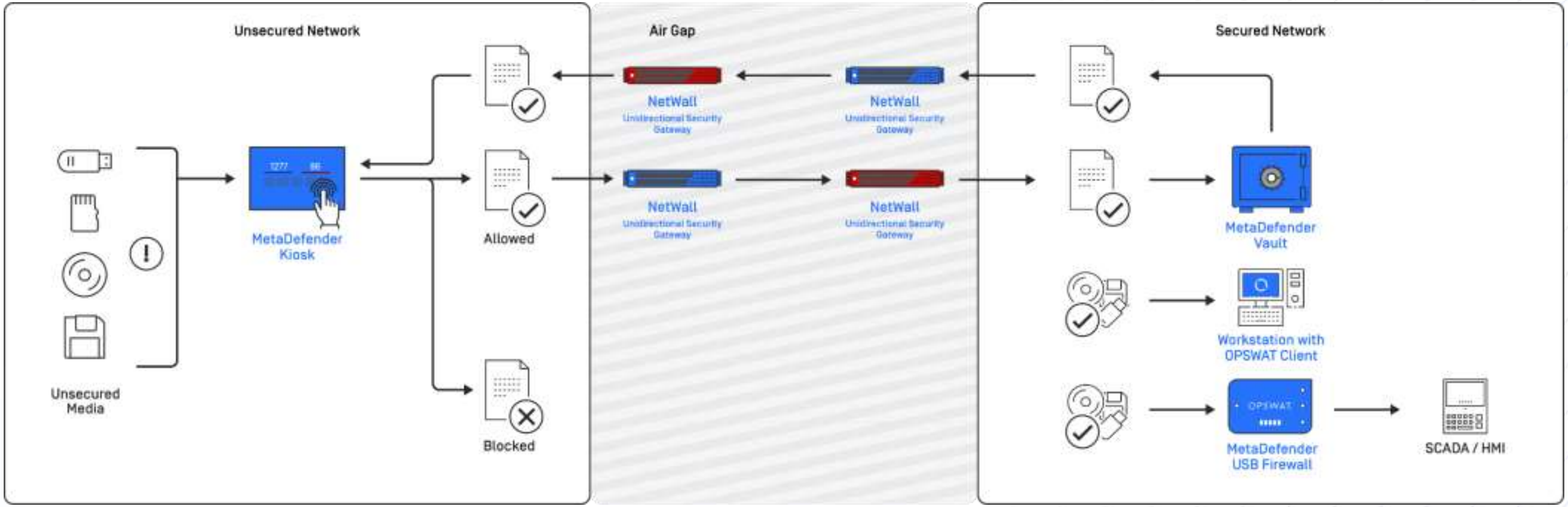
Full Industrial Support – Modbus, OPC DA, A&E, UA, UDP, TCP, File Transfers, Historian and DB Replication, IEC 104, DNP3 and other protocols

Easily Scalable – License upgradable bandwidth to address current and future requirements. NetWall 1U scalable from 100Mbps to 10Gbps. NetWall Din Rail scalable from 10Mbps to 50Mbps

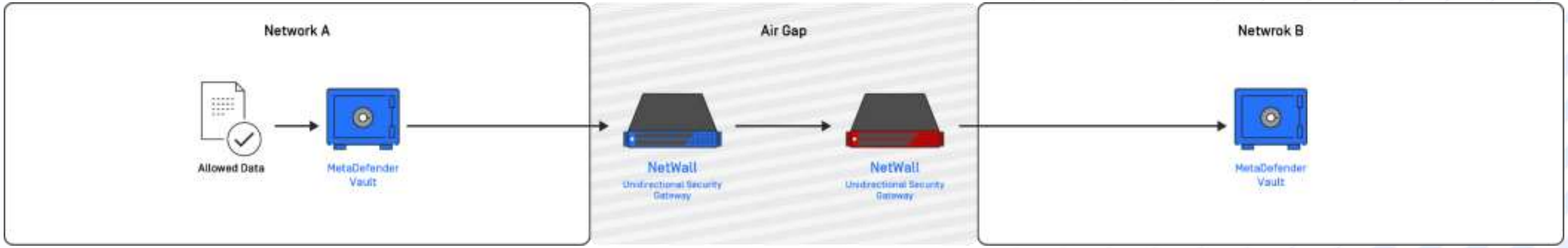
Bilateral Applications – NetWall BSG includes a unique mechanism to support data replies, while enforcing full protocol break and network isolation

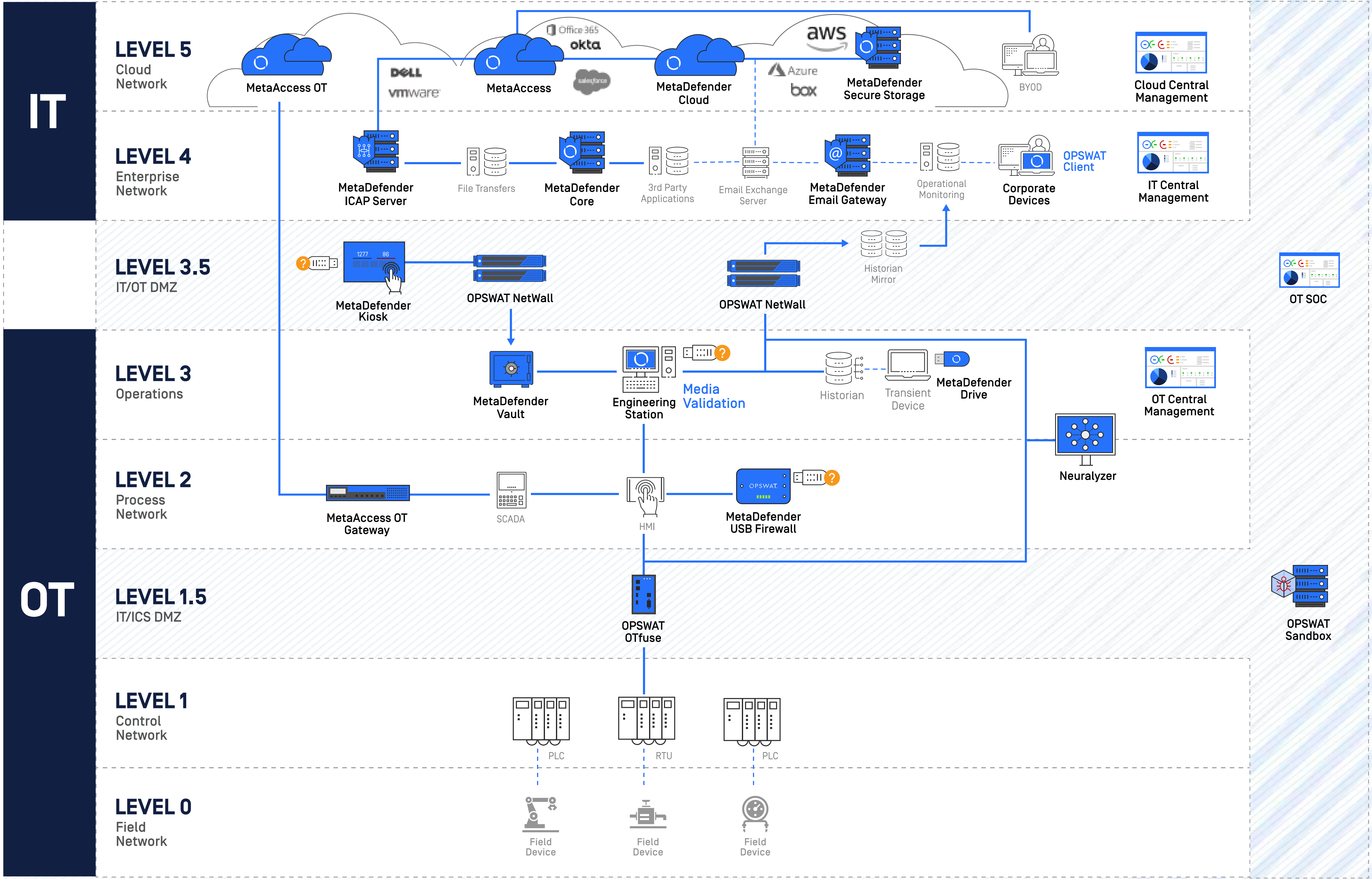
OT Security Deployment Case Study

Secure data transfer



Unsecured Network
Air Gap
Secured Network
Unsecured Media
MetaDefender Kiosk
1277
86
Allowed
Blocked
NetWall
Unidirectional Security Gateway
NetWall
Unidirectional Security Gateway
NetWall
Unidirectional Security Gateway
NetWall
Unidirectional Security Gateway
MetaDefender Vault
Workstation with OPSWAT Client
OPSWAT
MetaDefender USB Firewall
SCADA / HMI





IT

LEVEL 5
Cloud Network

MetaAccess OT

DELL
vmware

Office 365
okta

MetaAccess

salesforce

MetaDefender Cloud

aws

Azure

box

MetaDefender Secure Storage

BYOD

Cloud Central Management

LEVEL 4
Enterprise Network

MetaDefender ICAP Server

File Transfers

MetaDefender Core

3rd Party Applications

Email Exchange Server

MetaDefender Email Gateway

Operational Monitoring

Corporate Devices

OPSWAT Client

IT Central Management

LEVEL 3.5
IT/OT DMZ

MetaDefender Kiosk

OPSWAT NetWall

OPSWAT NetWall

Historian Mirror

OT SOC

OT

LEVEL 3
Operations

MetaDefender Vault

Engineering Station

Media Validation

Historian

Transient Device

MetaDefender Drive

OT Central Management

Neuralyzer

LEVEL 2
Process Network

MetaAccess OT Gateway

SCADA

HMI

MetaDefender USB Firewall

LEVEL 1.5
IT/ICS DMZ

OPSWAT OTfuse

OPSWAT Sandbox

LEVEL 1
Control Network

PLC

RTU

PLC

LEVEL 0
Field Network

Field Device

Field Device

Field Device

OPSWAT.

Hall 6 – booth #144

Visit OPSWAT @ ITSA 23

©2023 OPSWAT, Inc. Proprietary and Confidential

Thank you