OPSWAT in der Praxis

IT- und OT-Sicherheit integriert –

KRITIS-Anforderungen effizient umsetzen

Sven Tichy

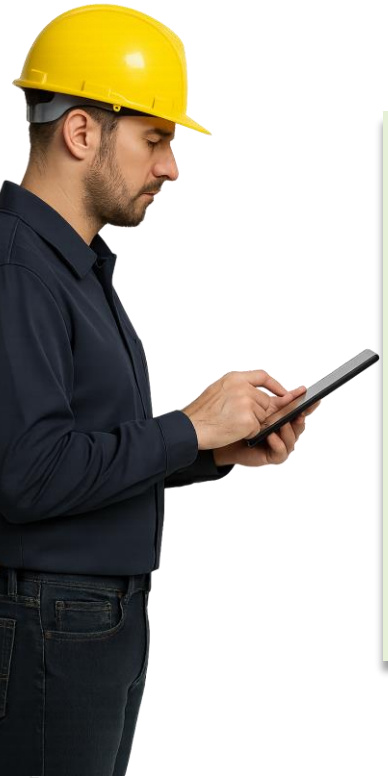
Peter Hoods

Dietzenbach, 02.07.2025

www.controlware.de

Agenda

1. Vorstellung und Einleitung
2. Herausforderungen
3. Bericht aus der Praxis
4. Lösungen mit OPSWAT
5. Fazit und Q&A



Sven Tichy

Senior Information Security Architekt
CC Security Design & Engineering

Peter Hoods

Lead System Architect
CC Operational Technology /
Industrial Control Systems

Herausforderungen (Konvergenz)
IT schützt Daten – OT schützt Prozesse

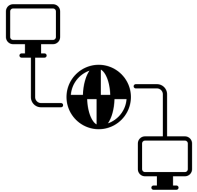
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Zugriffsmodelle in der Regel Maschinen- und oder Prozessorientiert.

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Zugriffsmodelle in der Regel Nutzerzentriert.

Bericht aus der Praxis

Albtraum des (Security) Consultants

Die (vermutlich) 3 besten Möglichkeiten einer OT-Umgebung durch Datenaustausch Schaden zuzufügen.



Bericht aus der Praxis

- Stuxnet
- Conficker
- Ransomware
- Keylogger
- Spionage-Tools
- BADUSB
- Rubber Ducky
- Manipulation von Konfigurationsdateien
- Umgebung von Air-Gap usw.

Bericht aus der Praxis

Albtraum des (Security) Consultants

Hallo zusammen,

- Phishing
- Spear-Phishing-Mail
- Manipulation von Konfigurationsdateien
- Exfiltration von sensiblen Daten
- Umgehung von Air-Gap usw.

Bericht aus der Praxis

Albtraum des (Security) Consultants

Umgehung sämtlicher Sicherheitsfunktionen!

Bericht aus der Praxis

Albtraum des (Security) Consultants

Durch die Nutzung von USB, Mail und Remote Access Lösungen geht ein großes Risiko einher, das im Worst-Case-Szenario, sämtliche Sicherheitszonen unbemerkt überwinden kann.
Die möglichen Auswirkungen sollten im besten Fall per Risiko Analyse sichtbar gemacht werden.

Agenda

1. Vorstellung und Einleitung
2. Herausforderungen
3. Bericht aus der Praxis
4. **Lösungen mit OPSWAT**
5. Fazit und Q&A

OPSWAT

1. **MetaDefender Platform**
2. Dioden & Security Gateway
3. Managed File Transfer
4. Kiosk & Media Firewall

MetaDefender Platform

File Security →
- MetaDefender Core →
- MetaDefender ICAP Server →

Storage Security →
- MetaDefender Storage Security →

Cloud Security →
- MetaDefender Cloud →
- ICAP Cloud →
- Storage Cloud →
- Salesforce Cloud →

Supply Chain Security →
- Hardware Supply Chain →
- Software Supply Chain →

Threat Intelligence →
- MetaDefender InSights C2 →
- MetaDefender InSights TI →
- MetaDefender InSights OSINT →

Network Detection & Response →
- MetaDefender NDR →

Peripheral & Removable Media Protection →
- MetaDefender Kiosk →
- MetaDefender Media Firewall →
- MetaDefender Endpoint →

Secure Access →
- My OPSWAT Central Management →
- MetaDefender Network Access Control →

Malware Analysis →
- MetaDefender Sandbox →
- Adaptive Sandbox for MetaDefender Core →
- Adaptive Sandbox for MetaDefender Cloud →

Email Security →
- MetaDefender for Email Exchange Server →
- MetaDefender for Microsoft 365 →

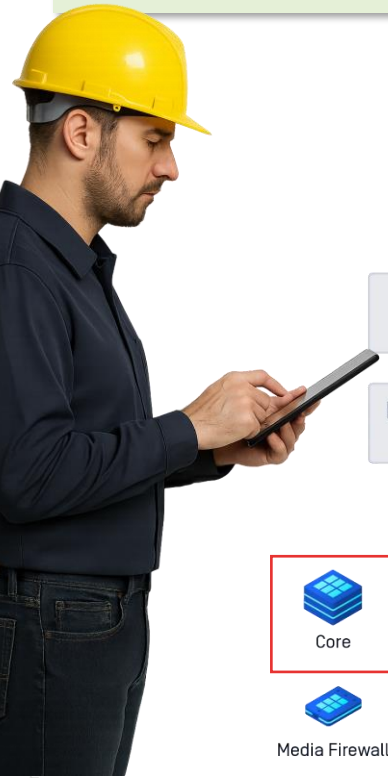
Managed File Transfer →
- MetaDefender Managed File Transfer →

OT and Cyber-Physical Systems →
- MetaDefender OT Security →
- MetaDefender OT Access →
- MetaDefender Industrial Firewall →
- MetaDefender Drive →

Data Diodes & Security Gateways →
- MetaDefender Optical Diode →
- MetaDefender Unidirectional Security Gateway →
- MetaDefender Bilateral Security Gateway →
- MetaDefender Transfer Guard →

OEM Solutions →
- MetaDefender Endpoint Security SDK →

MetaDefender Plattform

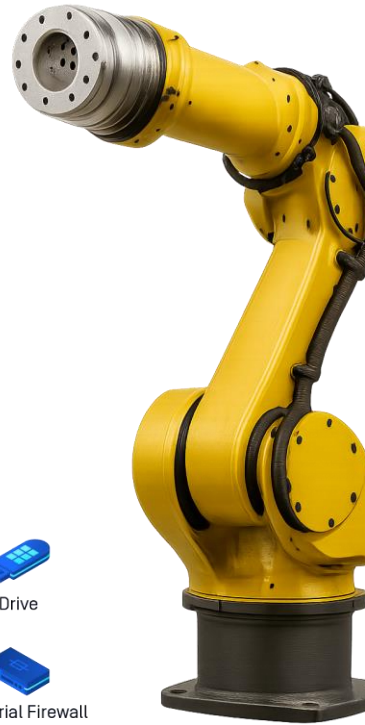


MetaDefender™
Trust No File. Trust No Device.

MetaScan®	Deep CDR	Adaptive Sandbox	Proactive DLP
File-based Vulnerability Assessment	InSights Threat Intelligence	SBOM	Country of Origin

Air-Gapped | On-Premises | Cloud

Core
ICAP Server
Storage Security
Email Security
Supply Chain Security
Kiosk
Drive
Media Firewall
Managed File Transfer
OT Access
Endpoint
Uni / Bidirectional Gateways + Data Diode
OT Security
Industrial Firewall



Core

Erfüllt KRITIS-Anforderungen:

- ✓ Schwachstellen- & Malware-Schutz
- ✓ Schutz vor unbekannten Bedrohungen (Zero-Day durch CDR)
- ✓ Integration in automatisierte Workflows (z.B. mit DLP, SIEM, Gateways)

OPSWAT

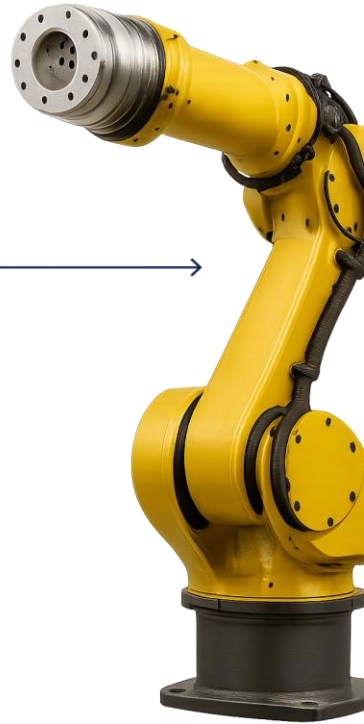
1. MetaDefender Platform
2. **Dioden & Security Gateway**
3. Managed File Transfer
4. Kiosk & Media Firewall

Optische Dioden

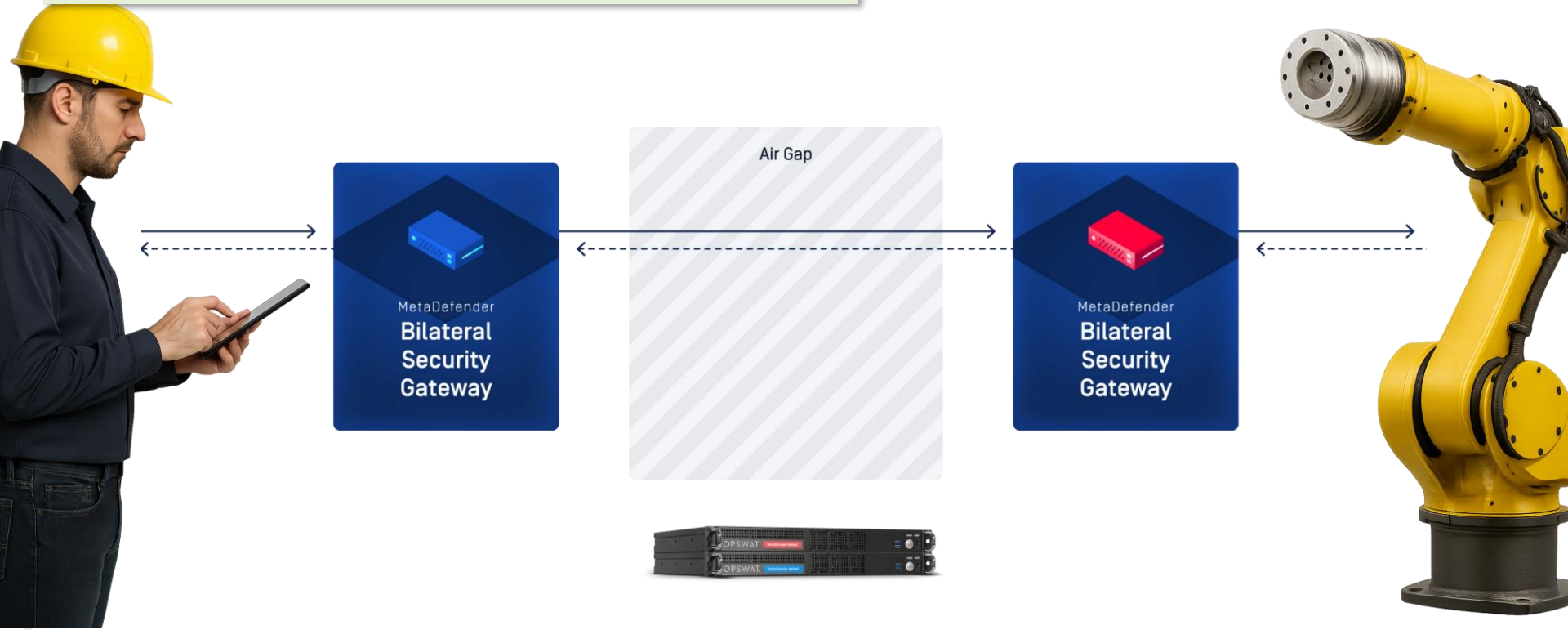
MetaDefender
Optical
Diode

Air Gap

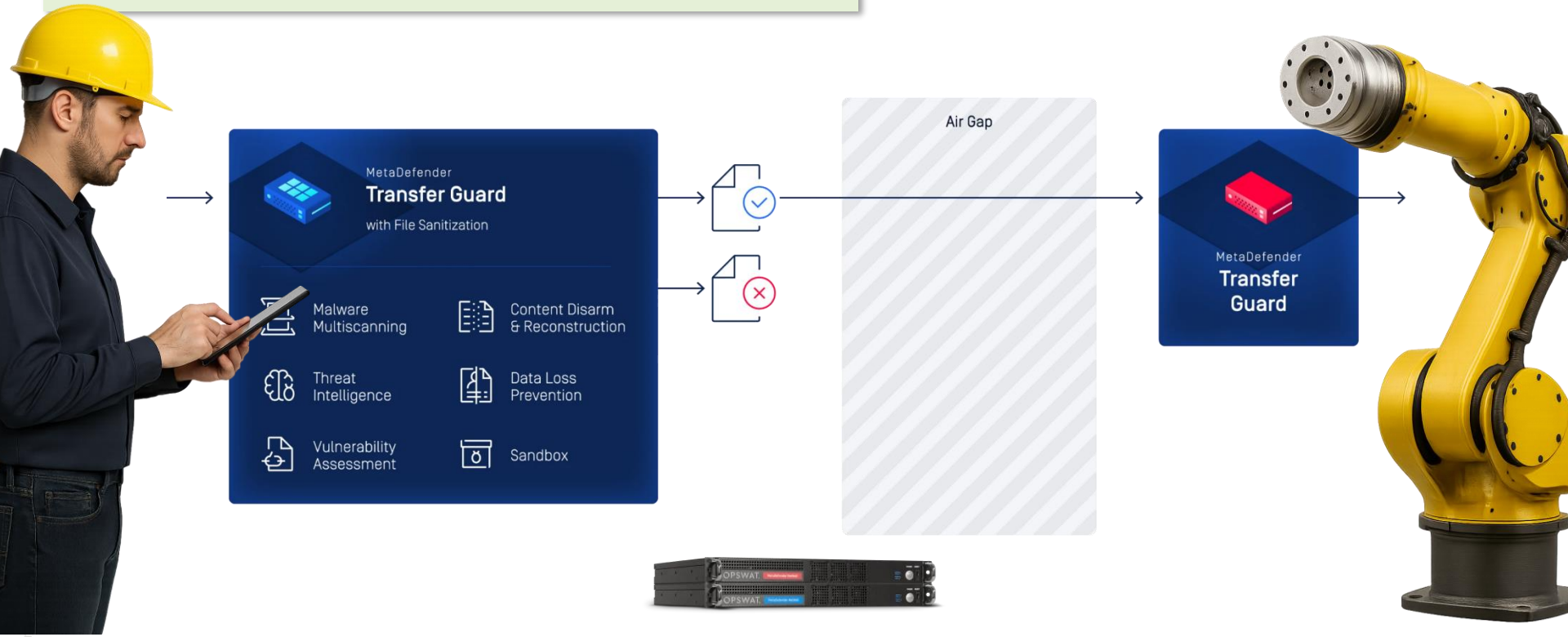
MetaDefender
Optical
Diode



Bilateral Security Gateways



Transfer Guard



NetWall

Erfüllt KRITIS-Anforderungen:

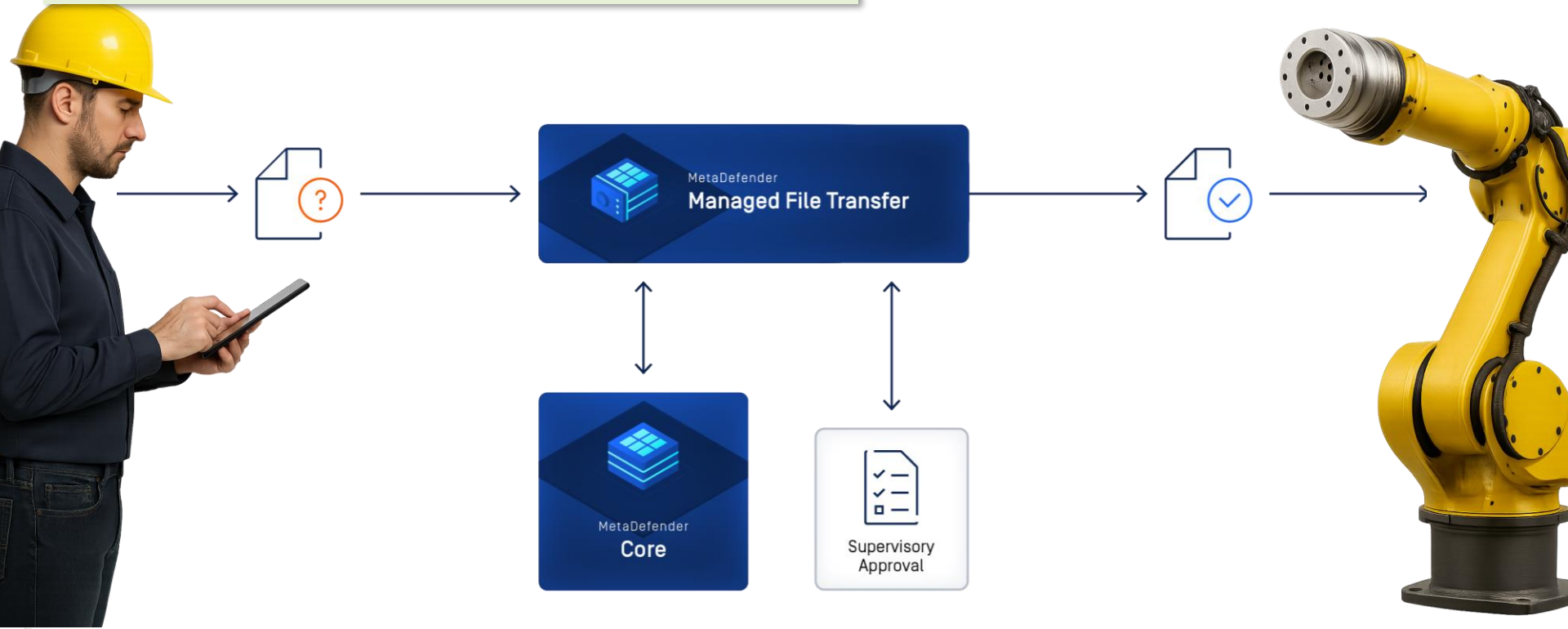
- ✓ Trennung von IT-/OT-Netzen (Micro-Segmentierung)
- ✓ Sichere, kontrollierte Datenweiterleitung (z.B. Prozessdaten, Logs, Diagnostik)
- ✓ Kein Rückkanal möglich – Air-Gap-ähnlich

OPSWAT

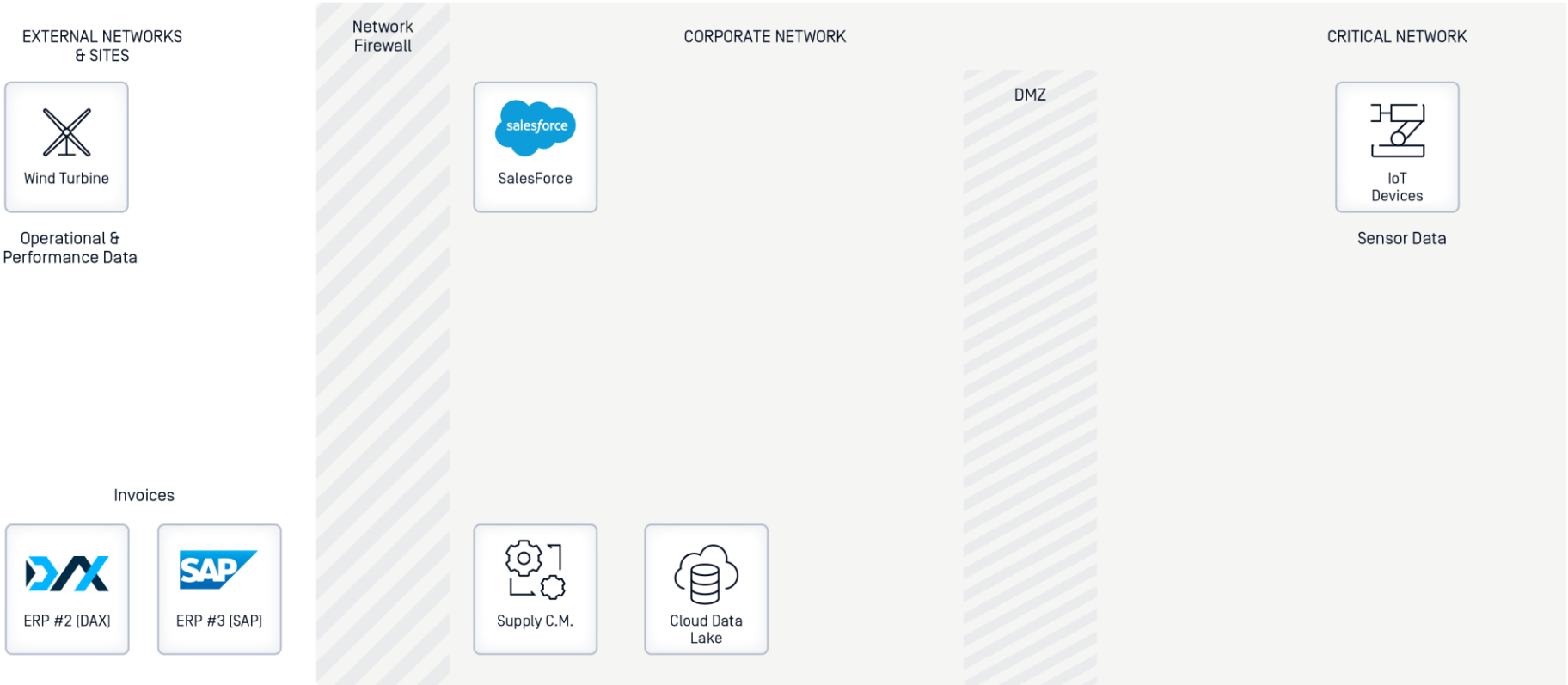
1. MetaDefender Platform
2. Dioden & Security Gateway
3. **Managed File Transfer**
4. Kiosk & Media Firewall

Managed File Transfer

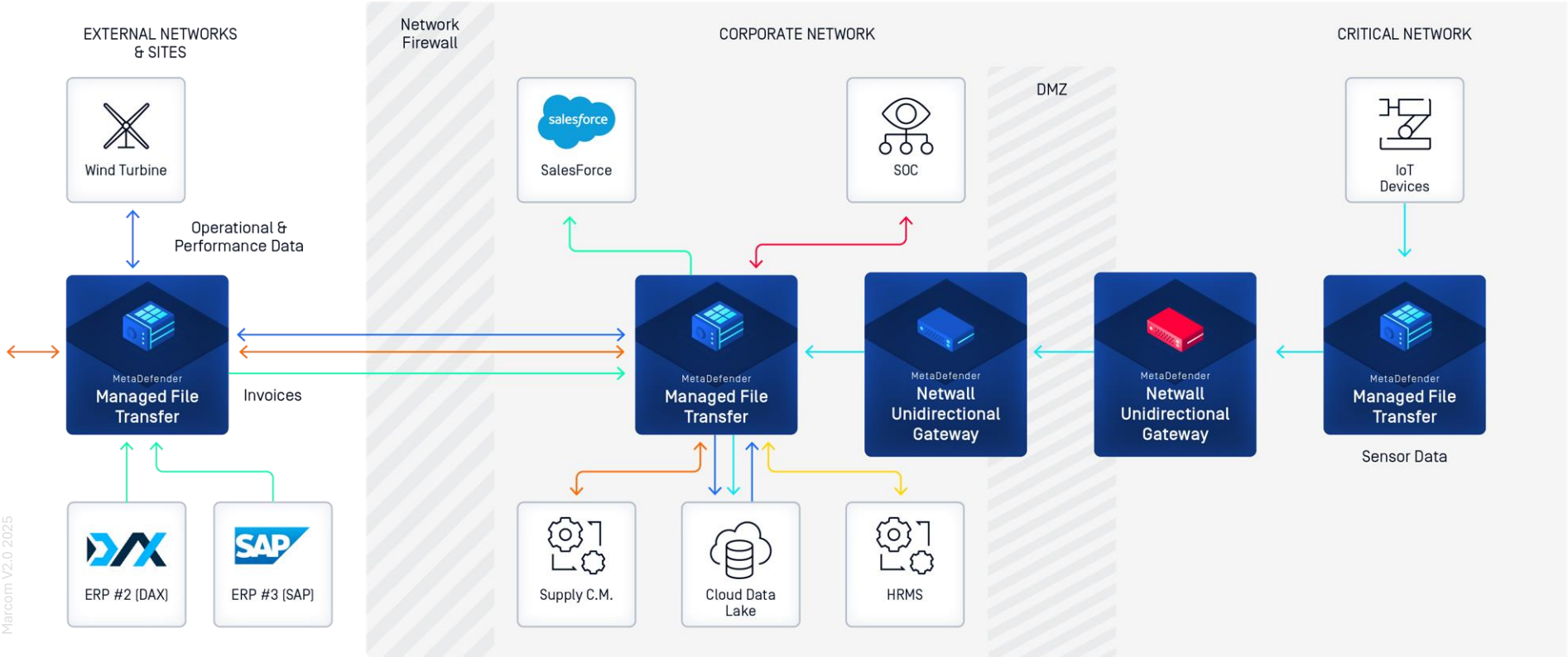
Managed File Transfer



Managed File Transfer



Managed File Transfer



Marcom V2.0 2025

Managed File Transfer

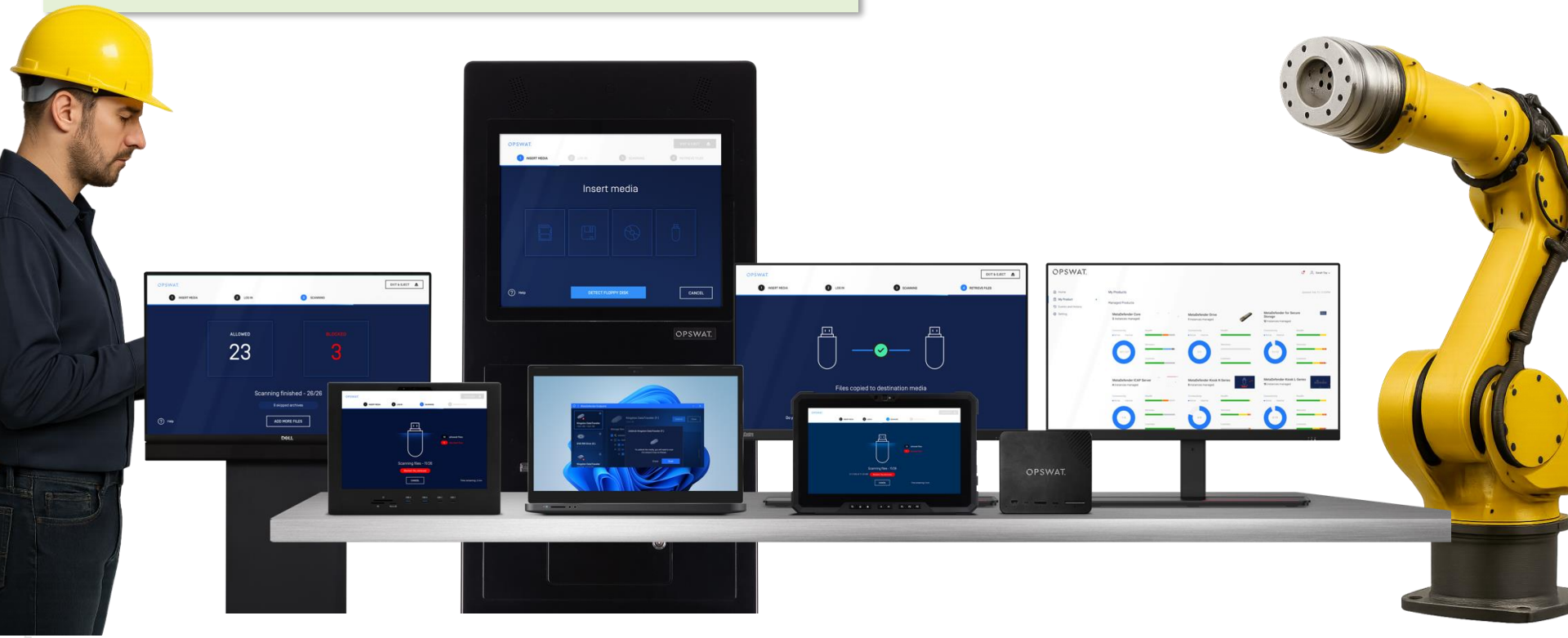
Erfüllt KRITIS-Anforderungen:

- ✓ Sichere Dateiübertragung mit Protokollierung
- ✓ Zugriffsschutz & Autorisierung (z.B. Rollen, Policies)
- ✓ Trusted Path zwischen: IT ↔ OT / Cloud ↔ On-Prem
- ✓ Integrität & Authentizität von Dateien

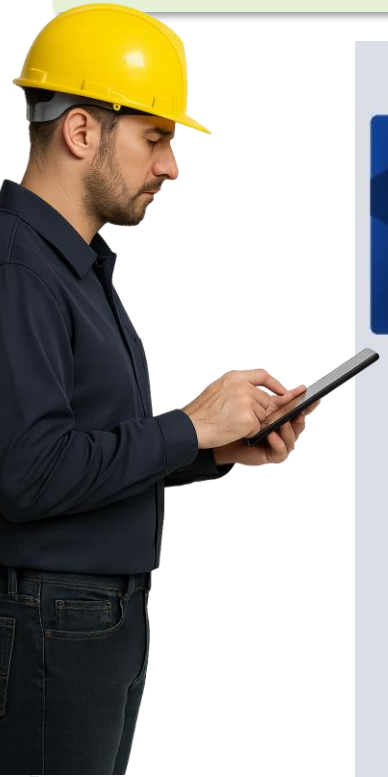
OPSWAT

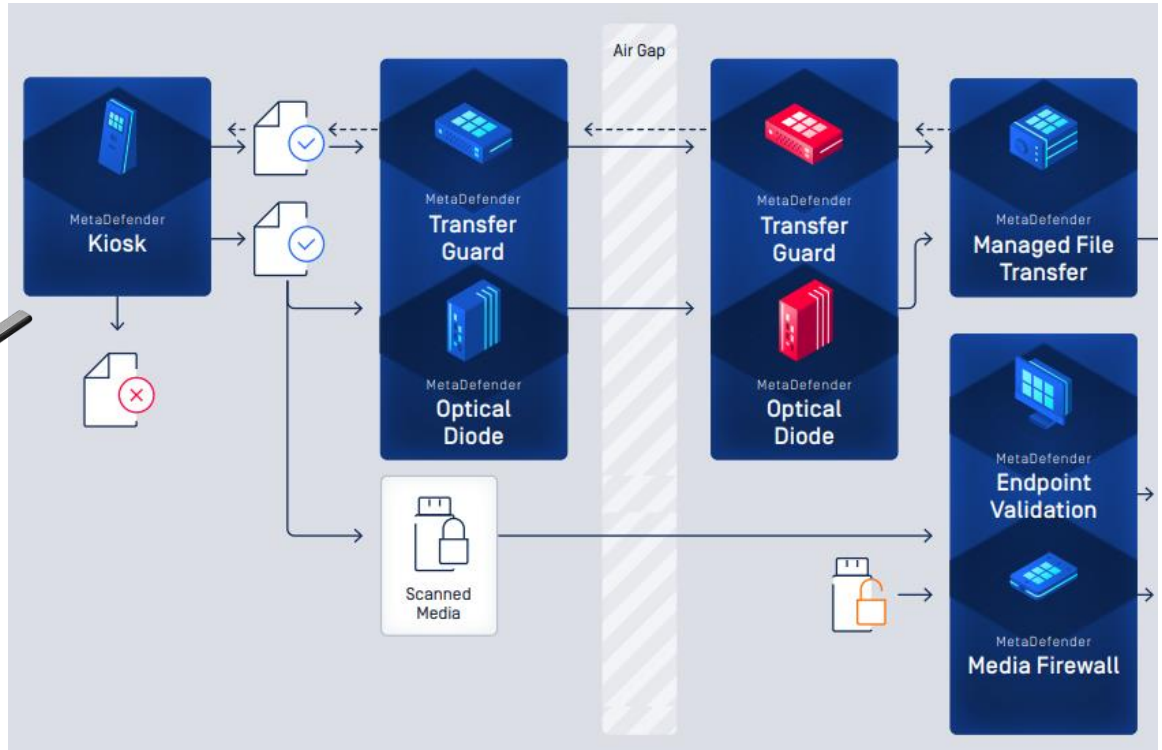
1. MetaDefender Platform
2. Dioden & Security Gateway
3. Managed File Transfer
4. **Kiosk & Media Firewall**

Kiosk (Übersicht)



Kiosk (Integration)





Media Firewall

Kiosk

Erfüllt KRITIS-Anforderungen:

- ✓ Segmentierung & Air-Gap-Überbrückung
- ✓ Sichere Bring-Your-Own-Medium-Checks
- ✓ Schutz vor verseuchten Dateien an Zugangspunkten
- ✓ Logging, Audit und Richtliniendurchsetzung

Agenda

1. Vorstellung und Einleitung
2. Herausforderungen
3. Bericht aus der Praxis
4. Lösungen mit OPSWAT
5. **Fazit und Q&A**

controlware

Vielen Dank für Ihre Aufmerksamkeit!
Thank you very much for your attention!