



Diodo de Dados em Ambientes NERC CIP



Salvaguarda contra Falhas de Firewall

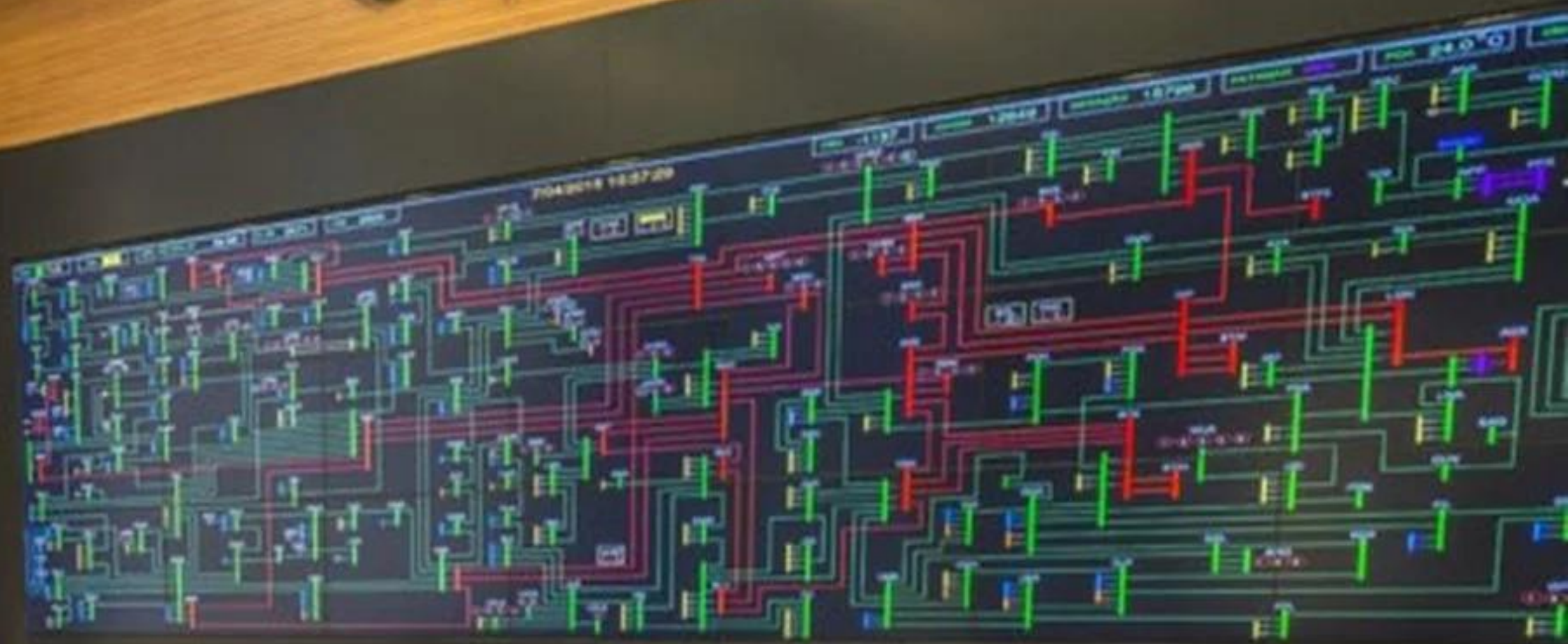
VINICIUS MOYANO

OPSWAT.

O DESAFIO Protegendo redes críticas em um cenário de convergência entre TI e TO

A separação que tradicionalmente existia entre os ambientes de TI e TO está diminuindo rapidamente. A necessidade crescente de conectividade, integração com sistemas corporativos e uso de analytics em ambientes industriais vem reduzindo o isolamento natural entre esses domínios. Isso vem trazendo riscos aos ambientes operacionais, que contam ainda com tecnologias básicas bidirecionais.

ONS Operador Nacional
do Sistema Elétrico



O problema: precisamos retirar dados da OT

COMPARTILHAR INFORMAÇÃO NÃO É CONCEDER ACESSO

Transferir dados $\neq$ abrir acesso

DADOS QUE PRECISAM SAIR

-  Logs e eventos
-  Historiadores
-  COMTRADE e oscilografias
-  Alarmes e telemetria



ACESSOS QUE NÃO SÃO NECESSÁRIOS

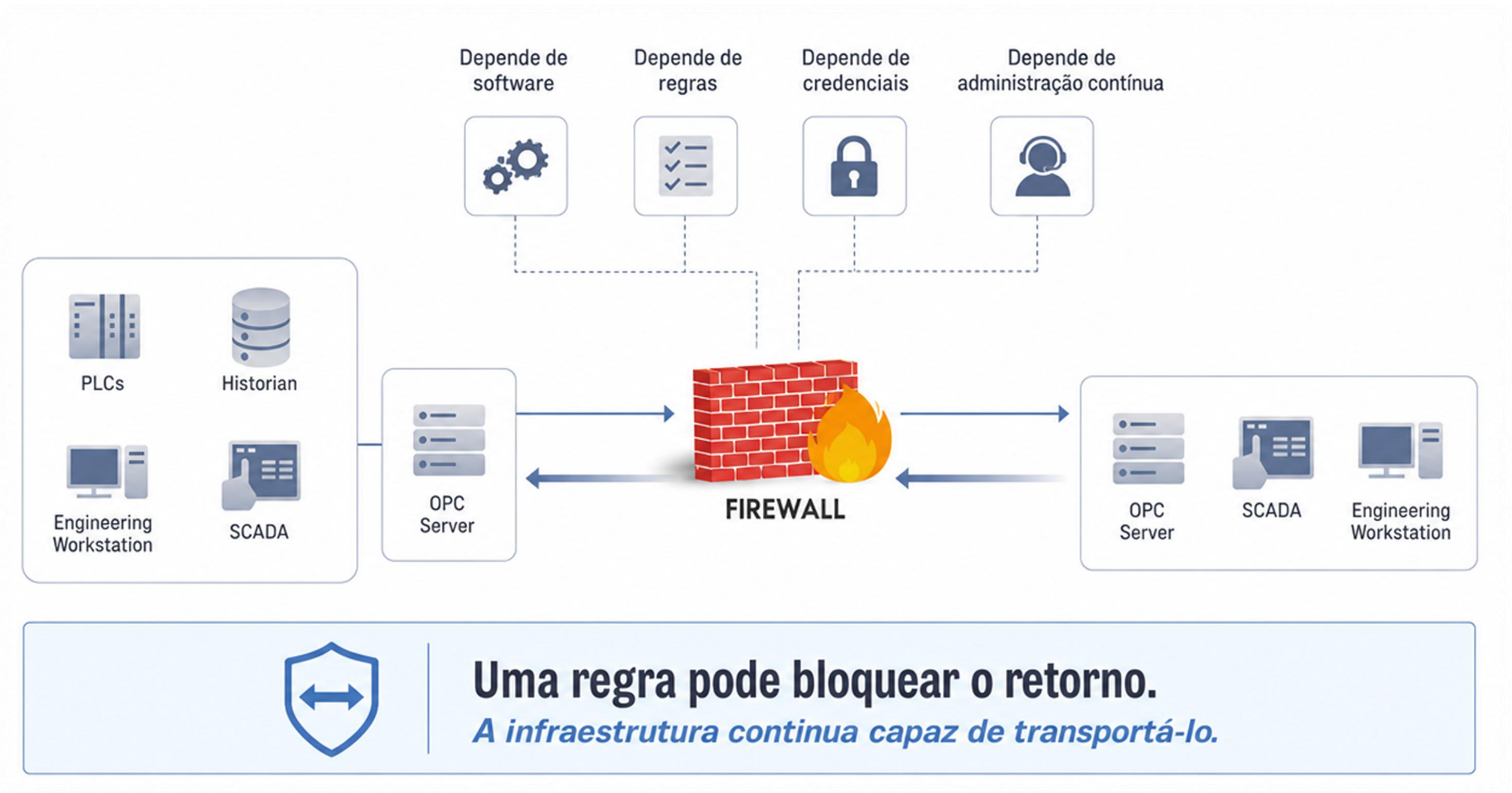
-  Sessões iniciadas pela TI
-  Comandos remotos
-  Roteamento de retorno
-  Movimento lateral



Compartilhar dados, não conceder acesso.

Firewall: essencial, porem com o mesmo caminho

O FIREWALL CONTROLA O CAMINHO, MAS NÃO ELIMINA O CAMINHO



O caminho de ataque

COM FIREWALL, O CAMINHO DE ATAQUE CONTINUA EXISTINDO

Cenário ilustrativo

① Comprometimento da TI



② Exploração de regra, credencial ou vulnerabilidade



③ Travessia da fronteira TI/OT



④ Acesso a SCADA, HMI ou PLC



Sem caminho para ataque

COM O DIODO, NÃO EXISTE UM CANAL FÍSICO DE RETORNO

Cenário ilustrativo

① A TI é comprometida



② O atacante tenta alcançar a OT



③ Não existe receptor na direção proibida



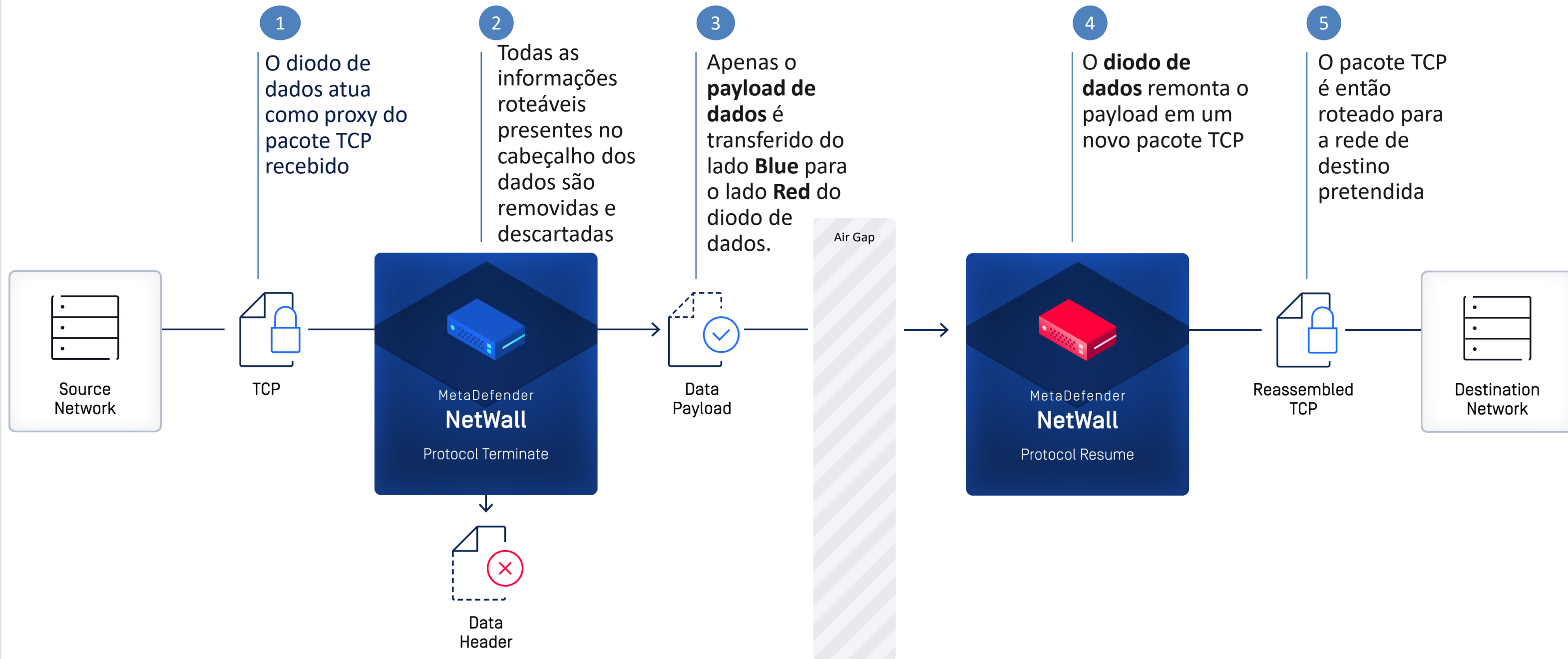
④ A operação permanece isolada por esse enlace



O software não pode ativar um componente físico que **não existe**.

Diodo de Dados

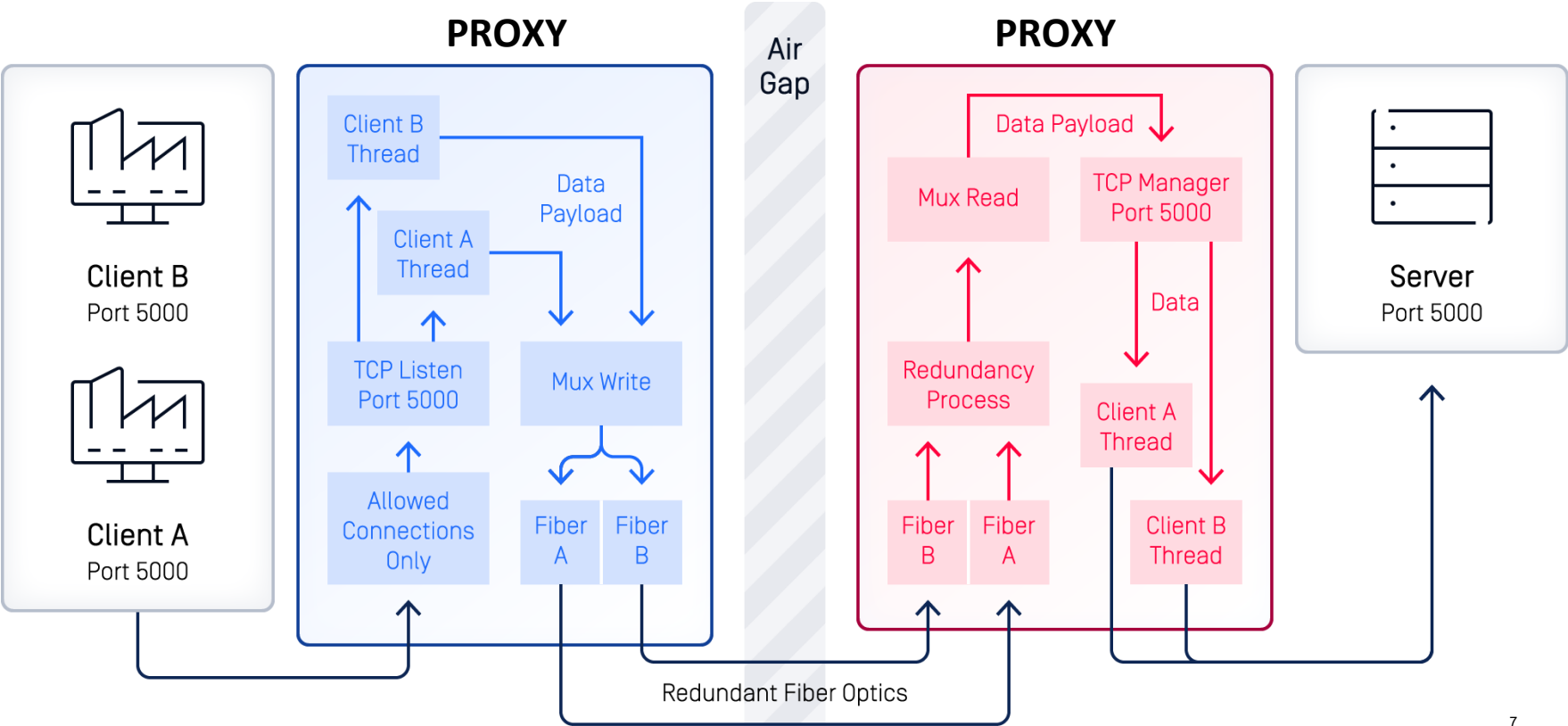
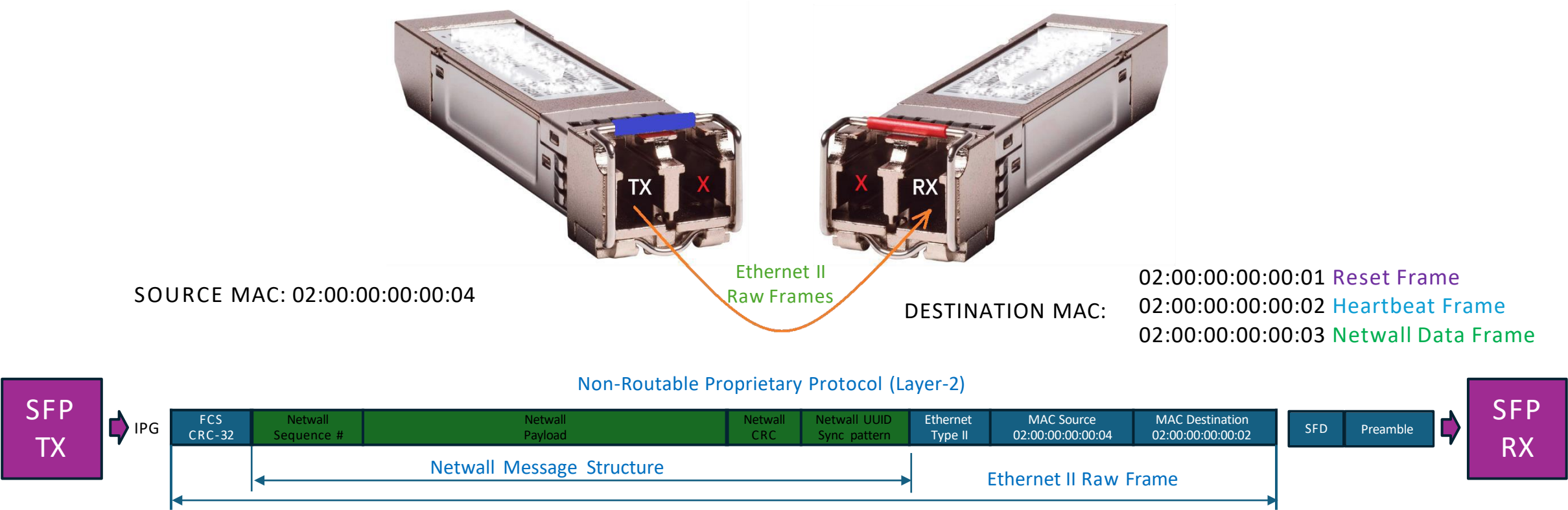
Tecnologia de Quebra de Protocolo Não Roteável



Como funciona Tecnicamente?



TCP e aplicações bidirecionais precisam de proxies ou replicação; o fluxo físico continua em uma direção.



Firewall × Gateway Unidirecional × Air Gap

Três modelos diferentes de controle de comunicação entre zonas.



Firewall

- Comunicação bidirecional possível
- Política baseada em regras
- Flexível para integrações
- Exige governança contínua



Unidirectional Gateway

- Fluxo reverso fisicamente bloqueado
- Permite saída automática de dados
- Reduz superfície de ataque
- Exige desenho por protocolo



Air Gap

- Sem conectividade de rede
- Máxima separação lógica
- Dificulta automação de dados
- Pode gerar processos manuais



Unidirectional Gateway = conectividade para dados, sem conectividade reversa pelo canal protegido.

Conformidade exige controle demonstrável

CONFORMIDADE VALORIZA CONTROLE DEMONSTRÁVEL DO FLUXO



01

RECONHECIMENTO EXPLÍCITO

- NERC CIP
- NIST

Reconhecimento explícito em normas de alto impacto e referência internacional de segurança cibernética.

REQUISITO REGULATÓRIO

Exigência direta.
Não é opcional.



02

BASE ARQUITETURAL

- ISA/IEC 62443
- Zonas, conduítes e fluxo restrito

Fundamentação técnica e arquitetural que orienta a construção de soluções seguras por design.

BOAS PRÁTICAS RECONHECIDAS

Referência consolidada para projetar com segurança.



03

NECESSIDADE OPERACIONAL BRASILEIRA

- ONS
- Monitoramento, registros e redes de proteção

Exigências operacionais do contexto brasileiro para assegurar continuidade, confiabilidade e proteção da operação.

REQUISITO OPERACIONAL

Necessidade do sistema elétrico.
Essencial para operar.

COMPLIANCE NÃO COMPRA O PRODUTO — TORNA A ARQUITETURA MAIS JUSTIFICÁVEL

A força da solução não está em cumprir uma norma isolada, mas em sustentar evidências em todos os níveis.

NERC CIP

O NERC CIP RECONHECE GATEWAYS UNIDIRECIONAIS

CIP reconhece gateways unidirecionais como evidência concreta de controle.



CIP-003-9

Obrigatório desde
1º de abril de 2026



Attachment 2

“implementing unidirectional gateways”
como exemplo de evidência



CIP-005-7

Permissões de entrada e saída
justificadas; demais acessos negados.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-003-9 – Cyber Security — Security Management Controls Attachment 2 – Examples of Evidence

The following are examples of evidence that may be used to demonstrate compliance with Requirement R1.

- implementing unidirectional gateways
- implementing data diodes
- configuring access lists
- implementing comprehensive logging and log retention
- performing periodic access reviews

Fonte: NERC CIP-003-9 – Cyber Security — Security Management Controls, Attachment 2 – Examples of Evidence, Requirement R1.



INTERPRETAÇÃO PARA O NEGÓCIO

“O diodo não substitui o programa NERC CIP.
Ele pode materializar fisicamente
uma permissão exclusivamente de saída.”



Conformidade comprovada. Risco reduzido. Controle fortalecido.

Fontes: NERC CIP-003-9 Attachment 2;
NERC CIP-005-7 Requirement R1.



NIST E IEC 62443

NIST E IEC 62443 REFORÇAM FLUXO RESTRITO E SEGMENTAÇÃO

Padrões internacionais convergem: fluxo unidirecional, segmentação e proteção de fronteira



NIST



Data diode

Dispositivo que permite dados em apenas uma direção



SP 800-82 Rev. 3

Proteção de ambientes OT



AC-4

Mecanismos de fluxo unidirecional



Zonas e conduítes

Estrutura de segmentação e proteção de fronteira



FR 5

Restricted Data Flow
Fluxo de dados restrito



Escolha baseada em risco

Decisão arquitetural baseada em risco;
não em produto obrigatório



ISA/IEC 62443



Ambos reforçam o controle de fronteiras e o fluxo restrito.
A decisão deve ser baseada em risco, não em produto obrigatório.

ONS - Brasil

OS DADOS PRECISAM SAIR, A REDE DE PROTEÇÃO NÃO PRECISA SE EXPOR



DESAFIO

Ambientes de proteção e automação precisam enviar dados de **monitoramento, eventos, oscilografia, Syslog e historiadores** para DMZ, SOC, NOC e IT sem abrir uma rota de retorno para a rede crítica.



ENCAIXE TÉCNICO

O **Diodo de Dados** cria comunicação unidirecional imposta por hardware, permitindo que dados saiam da OT enquanto bloqueia fisicamente comunicação inbound para a rede protegida.



Dados saem. A ameaça não volta.

NÍVEL
DE SEGURANÇA

5

4

3

2

1

IT

OT



REFERÊNCIAS ONS E POSICIONAMENTO

O argumento correto: o ONS define requisitos; o diodo é uma arquitetura possível para atendê-los.



2.11

Redes utilizadas para proteção

Mecanismos de segurança cibernética nos segmentos locais e externos usados pela proteção.



7.1.x

Monitoramento independente da rede

Dados de monitoramento podem ser exportados para DMZ/SOC/NOC sem abrir retorno para OT.



5.3.1

Registros de perturbação

Oscilografias, COMTRADE e eventos podem sair da subestação por fluxo unidirecional.



5.13

RO-CB.BR.01 — Zonas de segurança

Reforça segregação entre Supervisão, DMZ Operativa e Zona Corporativa.



MENSAGEM-CHAVE

Não posicionar como “tecnologia exigida por nome”. Posicionar como controle defensável para segmentação, controle de acesso e exportação segura OT → IT.

Casos de uso prático no setor elétrico

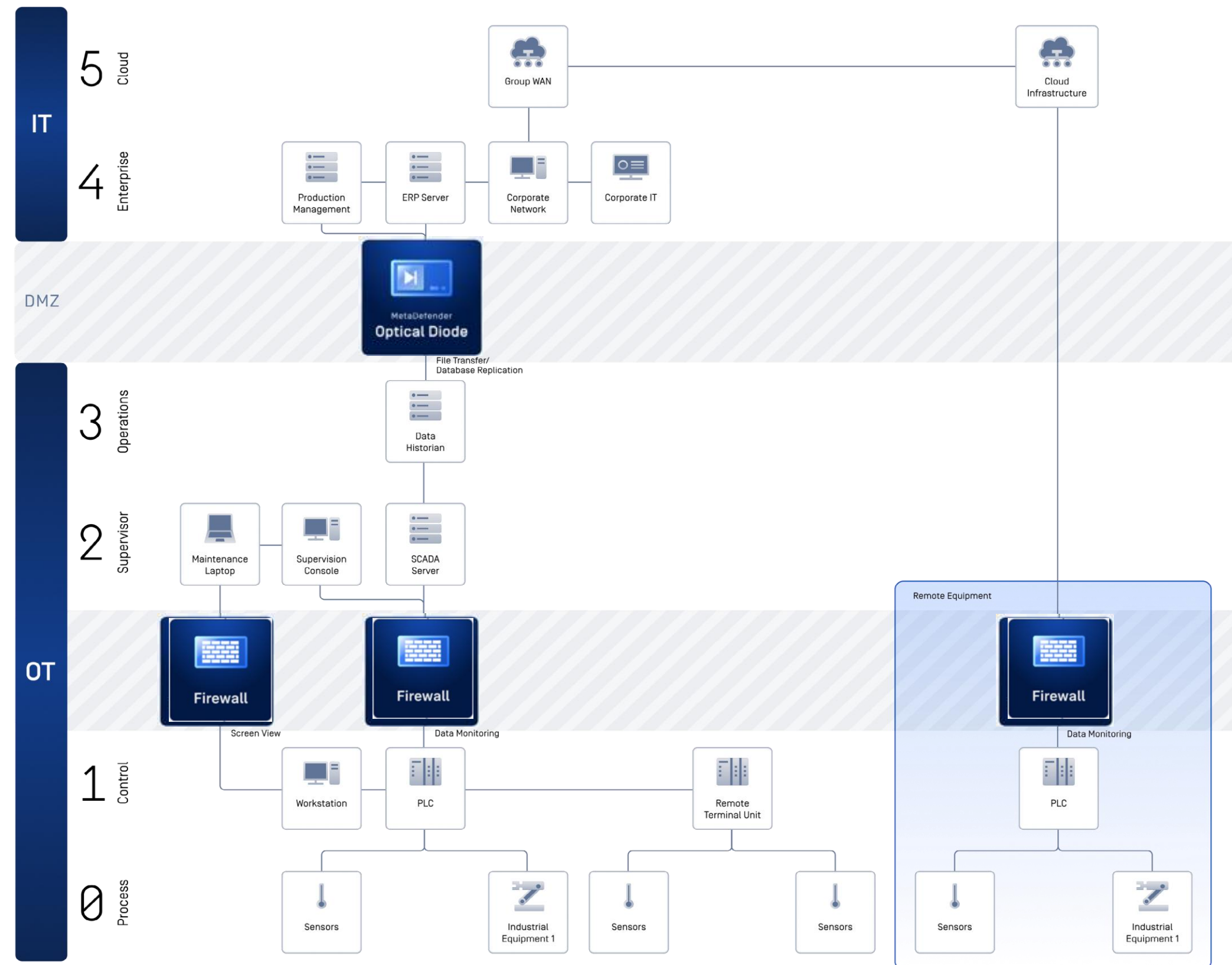
ONDE O DIODO GERA VALOR NO SETOR ELÉTRICO

Desafio

Ambientes de energia possuem ativos críticos como **SCADA, IEDs, PLCs, RTUs e relés de proteção**. Equipes de TI e segurança precisam acessar dados operacionais, alarmes, logs e telemetria sem criar novos riscos para a rede OT.

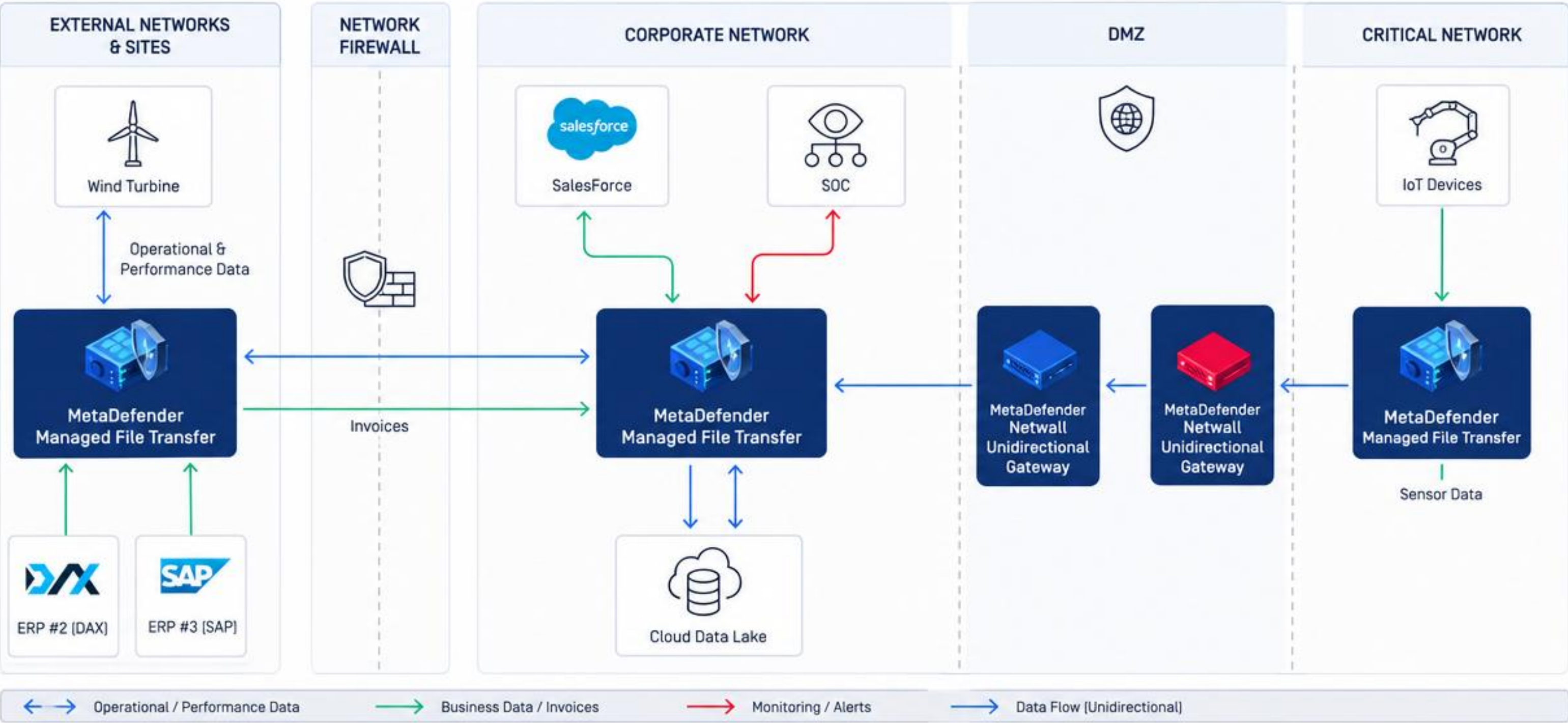
Solução

O **Diodo de Dados** permite a transferência unidirecional de informações da **OT para a IT**, bloqueando fisicamente qualquer comunicação de retorno. Isso garante **visibilidade, monitoramento e integração segura de dados**, reduzindo a superfície de ataque e protegendo subestações, centros de controle e demais infraestruturas críticas.



Arquitetura prática OT → IT/SOC/Cloud

Camadas típicas para permitir visibilidade sem expor o controle operacional.



- Malware Scanning
- Data Validation
- Content Disarm & Reconstruction
- Comprehensive Logging & Auditing



MetaDefender NetWall

Data Diode and Security Gateway Solutions



1 METADEFENDER™ Optical Diode

Provides a hardware-enforced unidirectional transfer of real-time OT data over a reliable, high-speed, low latency optical link.



One way data transfer using an optical link

2 METADEFENDER™ Unidirectional Security Gateway

Provides real-time OT data access with full benefits of speed, low latency, functionality, and reliability—no return path.



One way data transfer over a serial connection

3 METADEFENDER™ Bilateral Security Gateway

Enables secure bidirectional communication with full protocol break—allowing only approved responses.



One way data transfer with data response

4 METADEFENDER™ Diode X

Previously MetaDefender Transfer Guard

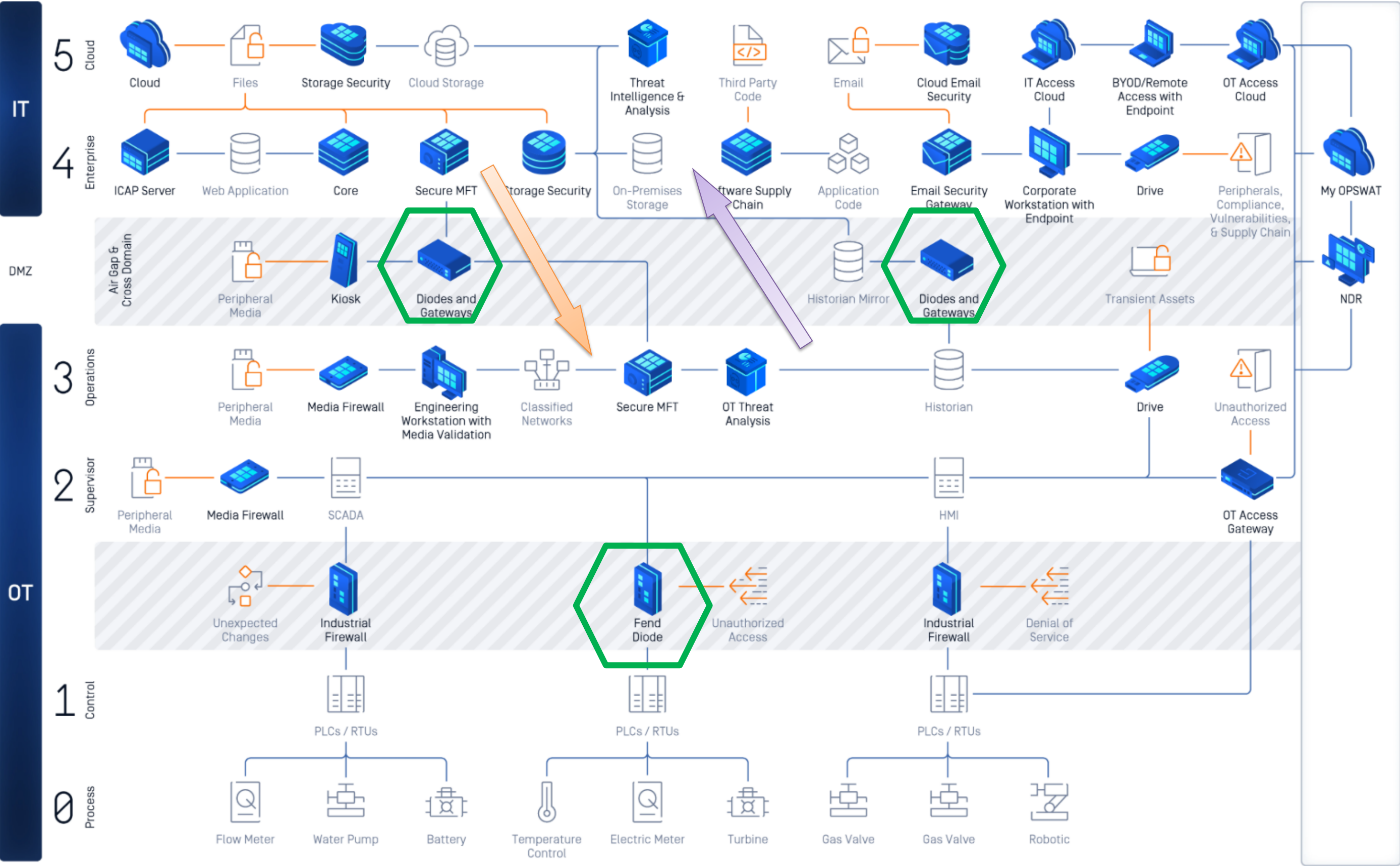
with File Sanitization

One way data transfer with file sanitization by MetaDefender Core before crossing the boundary.



One way data transfer with additional file sanitization by MetaDefender Core

Outros controles, fecham outros vetores



The MetaDefender™ Platform



Objecções com os Diodos de Dados

O DIODO NÃO BLOQUEIA O NEGÓCIO; ELE EXIGE CLAREZA SOBRE O FLUXO



**VOU PERDER
ACESSO À OT?**



Não.

O diodo é aplicado somente onde o retorno não é necessário.



**ELE SUBSTITUI
TODOS OS FIREWALLS?**



Não.

Atua em fronteiras específicas e pode operar em conjunto com firewalls.



**APLICAÇÕES TCP
DEIXAM DE FUNCIONAR?**



Não.

As sessões são terminadas e recriadas pelos gateways.



**COMO ENVIO PATCHES
OU ARQUIVOS PARA A OT?**



Por um fluxo separado,
autorizado, inspecionado e
orientado na direção correta.



**É UMA SOLUÇÃO APENAS
PARA DEFESA?**



Não.

Energia, saneamento, indústria e outras infraestruturas utilizam fluxos naturalmente unidirecionais.

Três respostas “sim” justificam uma avaliação

SE TRÊS DESTAS RESPOSTAS FOREM “SIM”, EXISTE UM FORTE CASO PARA AVALIAÇÃO

☐

A OT envia logs, históricos, COMTRADE ou telemetria para outra rede?

☐

O firewall é hoje a única barreira entre TI e OT?

☐

Existe integração planejada com SOC, SIEM, cloud ou data lake?

☐

Há subestações, plantas ou sites remotos com arquitetura repetível?

☐

O destino não precisa iniciar conexões de volta?

☐

A indisponibilidade da operação teria impacto elevado?

☐

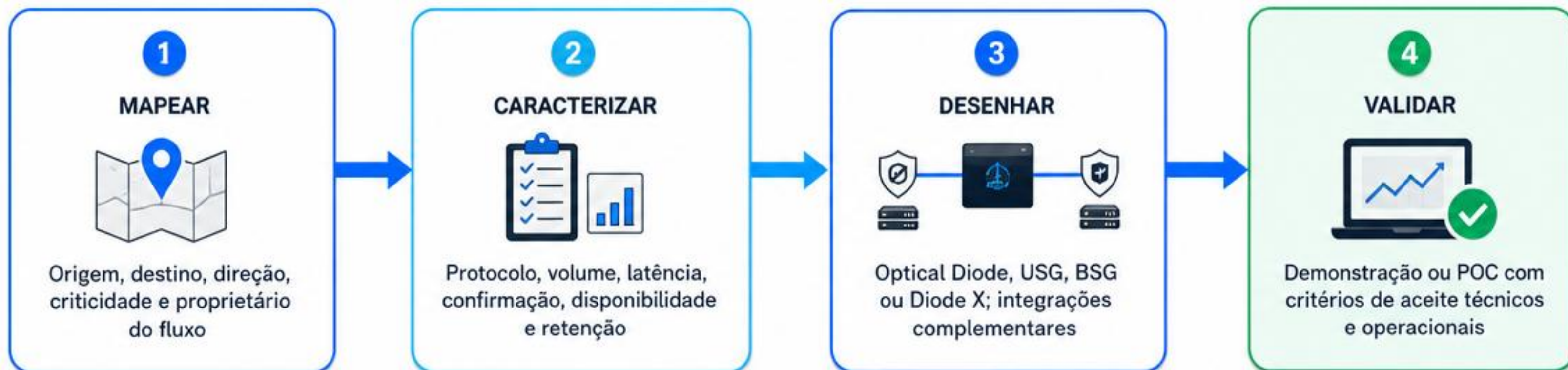
Auditoria ou gestão de risco exige evidência mais forte de segmentação?



Quanto mais “sim”, mais forte o caso para eliminar o caminho reverso

Proposta: avaliação técnica de um fluxo crítico

AVALIAÇÃO TÉCNICA DE UM FLUXO DE DADOS CRÍTICO



EXEMPLO DE FLUXO



Entregável proposto:

**“Arquitetura recomendada +
matriz de aderência +
plano de validação”**

MetaDefender™

OT Access

Acesso remoto seguro para ambientes industriais (SRA)

VPNs tradicionais frequentemente concedem acesso amplo e irrestrito, deixando sistemas OT críticos vulneráveis. O MetaDefender OT Access redefine o acesso remoto seguro com um modelo de line-of-sight, permitindo que os usuários interajam exclusivamente com ativos, protocolos e atividades autorizadas.

Essa abordagem minimiza a superfície de ataque e aumenta a proteção da rede. Com controle centralizado, simplifica o acesso remoto para terceiros, OEMs e contratados, eliminando a necessidade de múltiplas ferramentas.



Principais Benefícios



Proteger sistemas críticos contra alterações não autorizadas



Melhorar conformidade com logs rastreáveis de acesso



Reduzir o risco de erro humano em operações sensíveis



Gravação de sessões e visibilidade em tempo real para auditoria



Transferência segura de arquivos e processo de permissão para proteger redes

Opções de implantação

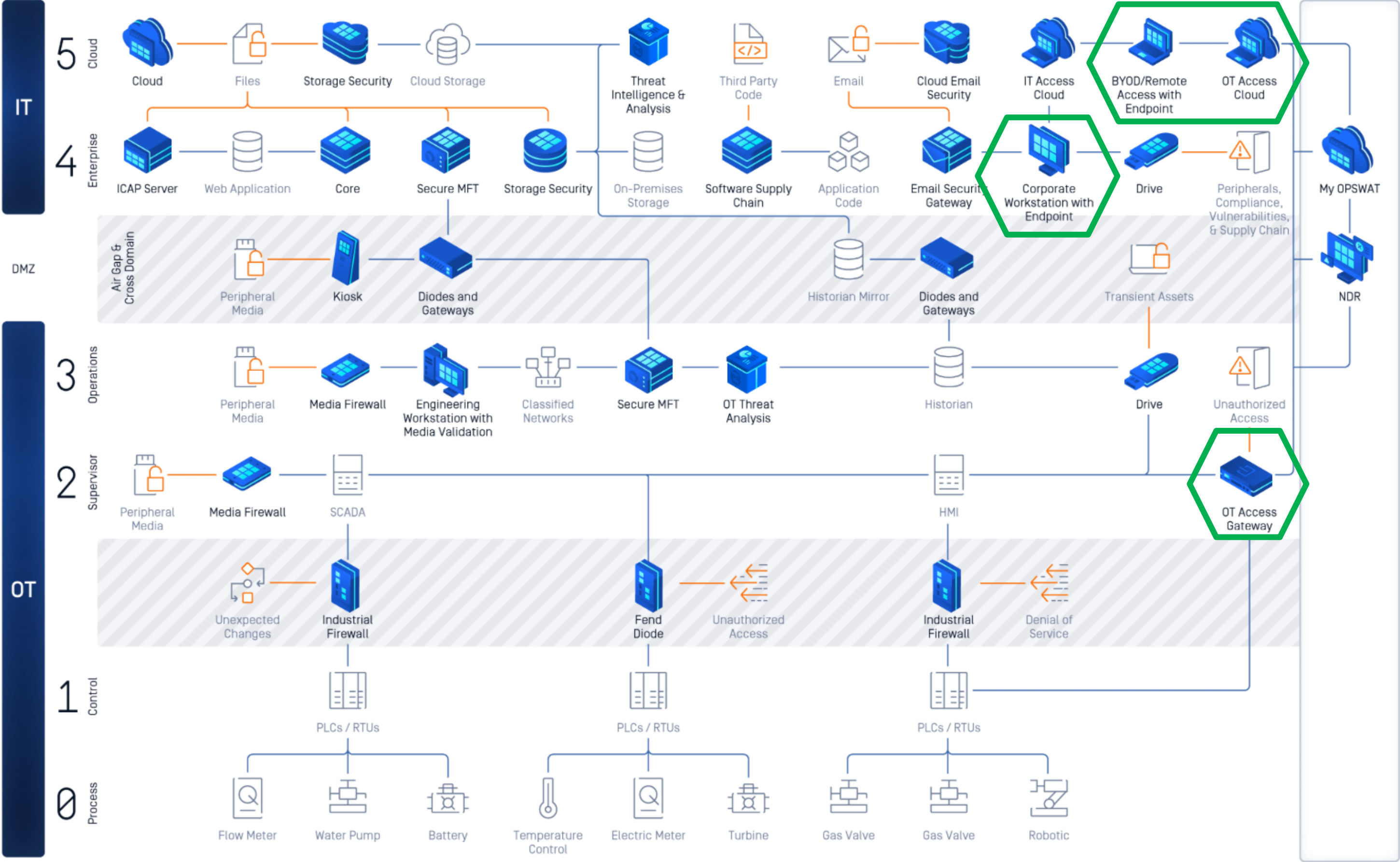
On-Premises



Cloud



The MetaDefender™ Platform



MetaDefender™

Kiosk™ series

Escaneie mais de 20 tipos de dispositivos, de USB-C a disquetes

Proteger PLCs, HMIs e estações de trabalho.

Proteger contra vulnerabilidades, ataques zero-day, malware e outras ameaças.

Aplicar políticas para garantir que todos os dispositivos sejam escaneados antes do uso.

Relatórios simples.

Conformidade com requisitos NIST, NEI, NERC CIP, ISO/IEC e ISA/IEC.

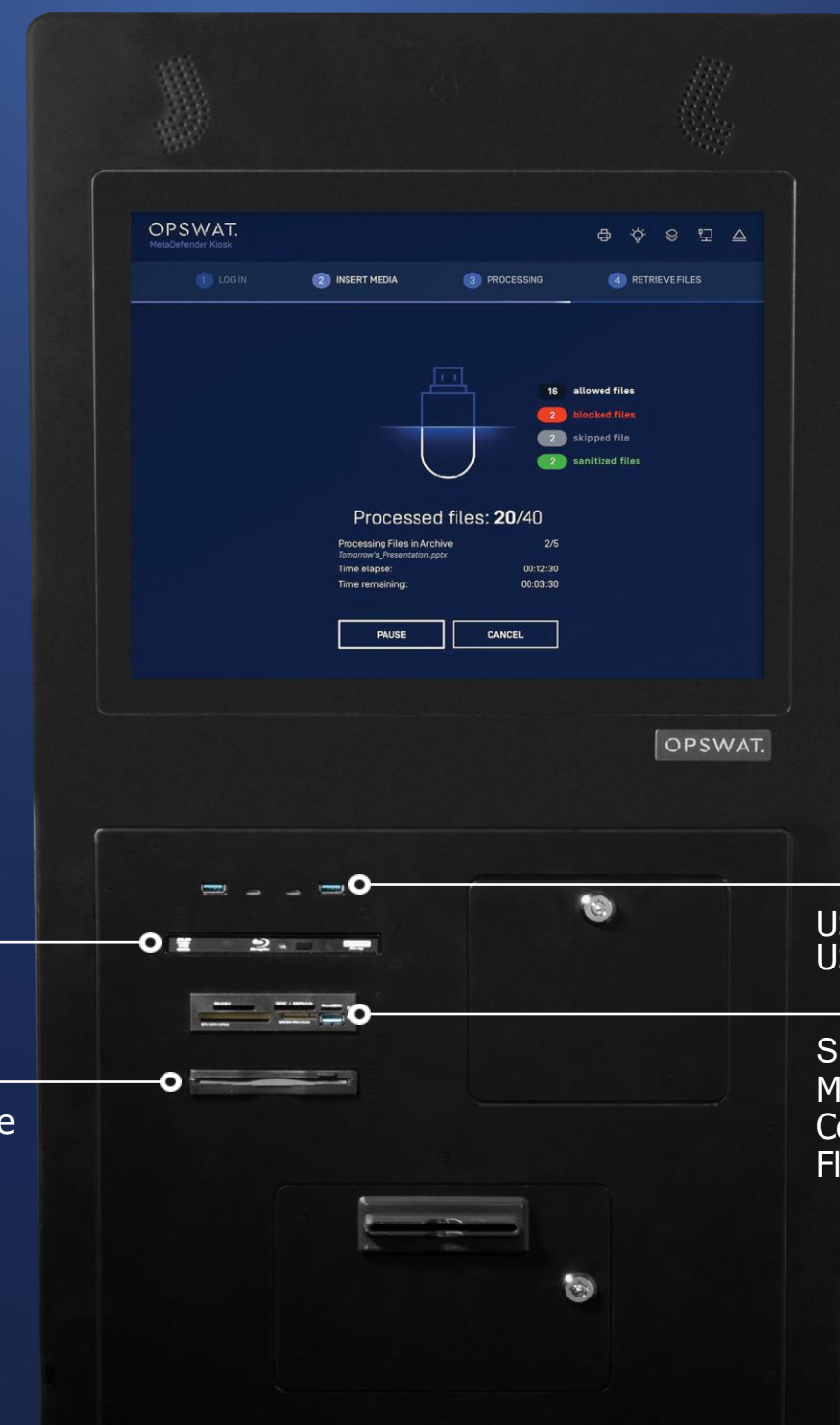


CD
DVD
Blu-Ray

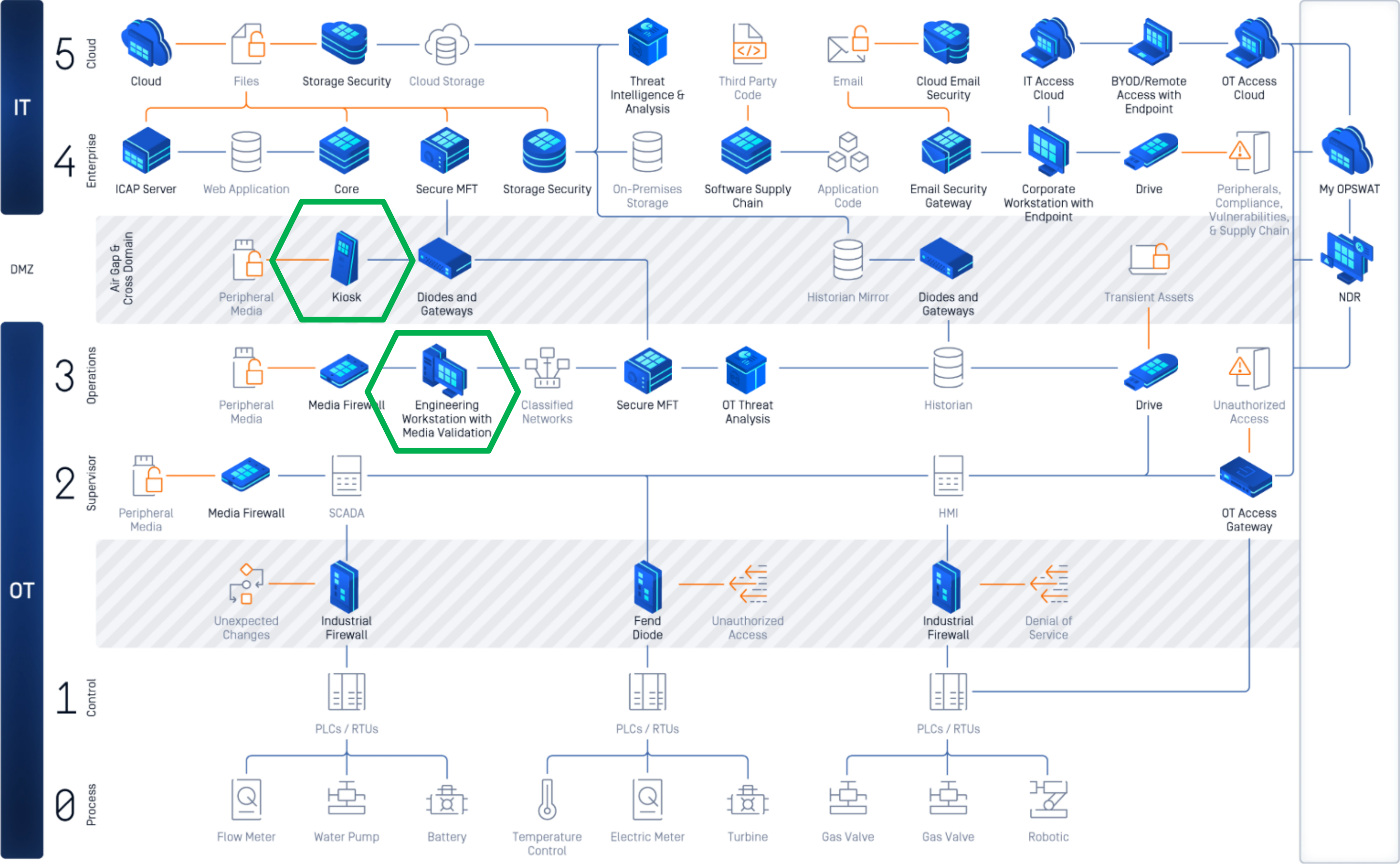
3.5" Diskette

USB-A
USB-C

SD
Micro SD
Compact
Flash



The MetaDefender™ Platform



Secure MFT: Efficient. Secure. Compliant.



Single MFT

File Sharing, System-To-System & User-based

Gain secure file sharing and automated file transfers between internal/external users & collaboration platforms such as SFTP, SMB, and SharePoint Online.



MFT to MFT

IT Network to OT Network

Ensure managed secure file transfer between low- and high-security environments. Supports various configurations [Low to High, Low to Low, High to High, High to Low].



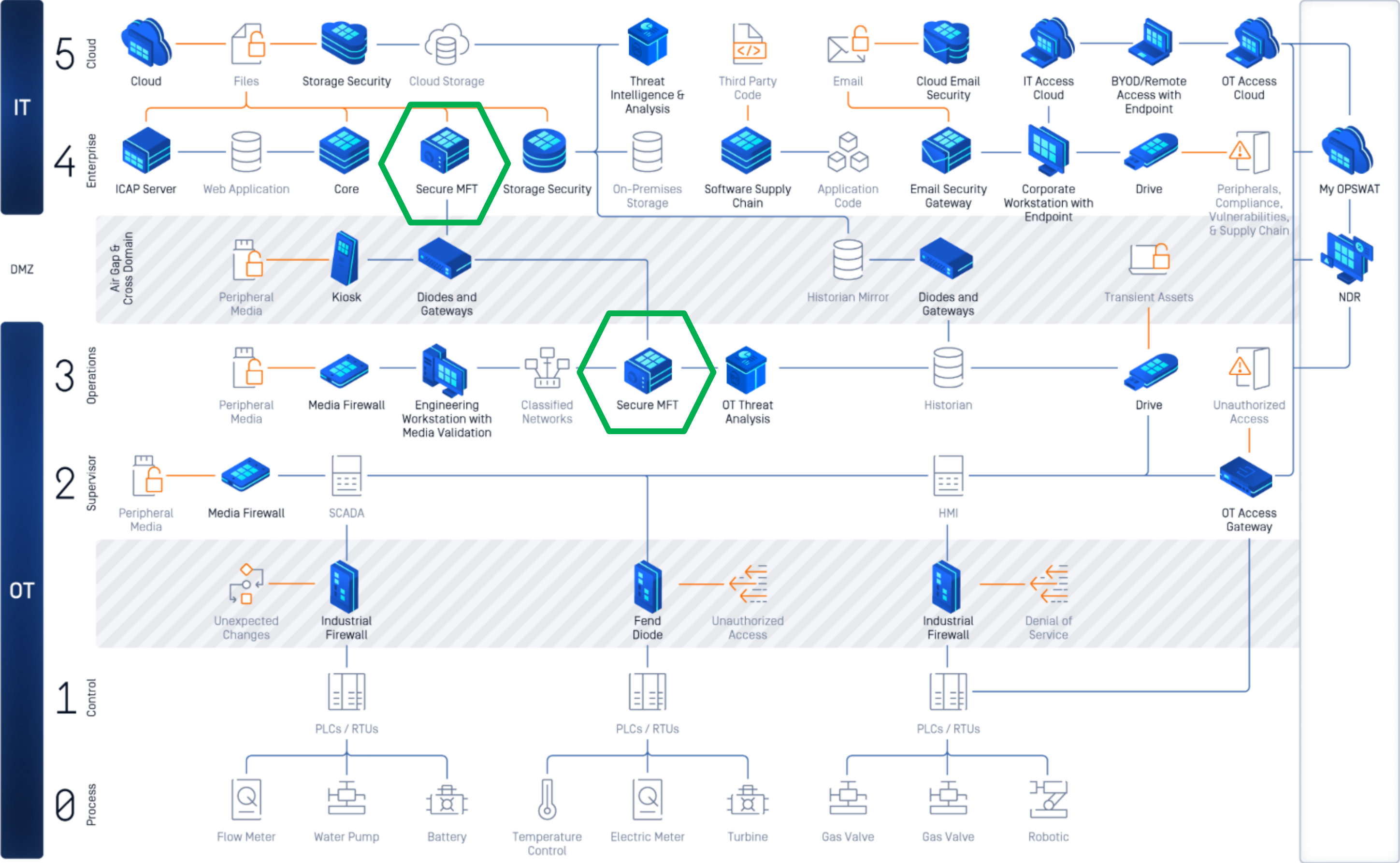
One MFT To Many Transfers

Efficient Multi-Directional Transfer

Centralized file management with one-to-many MFT configurations, enabling automated, secure data transfers to multiple locations.



The MetaDefender™ Platform



MetaDefender™

Industrial Firewall

Proteção de última milha para sistemas OT críticos e sistemas ciberfísicos

Protegendo infraestrutura crítica com segurança de rede orientada por IA, o MetaDefender Industrial Firewall é apresentado como a última linha de defesa contra erros de configuração acidentais, uso malicioso, ameaças zero-day, ataques DoS/D-DoS e anomalias potencialmente prejudiciais. Essa solução usa IA avançada para simplificar o desenvolvimento de políticas e proteger redes operacionais e de controle de processos. Seu hardware reforçado permite implantação em ambientes industriais severos, com suporte a mais de 100 protocolos de rede para proteção abrangente.

O MetaDefender Industrial Firewall integra-se ao MetaDefender OT Security, reunindo detecção ativa de ameaças e gerenciamento de ativos em uma única interface.



DPI (Deep Packet Inspection): previne acesso não autorizado ou uso indevido intencional por meio de monitoramento e filtragem de tráfego com base em protocolos industriais como Modbus, DNP3 e IEC 61850, incluindo protocolos proprietários da GE.

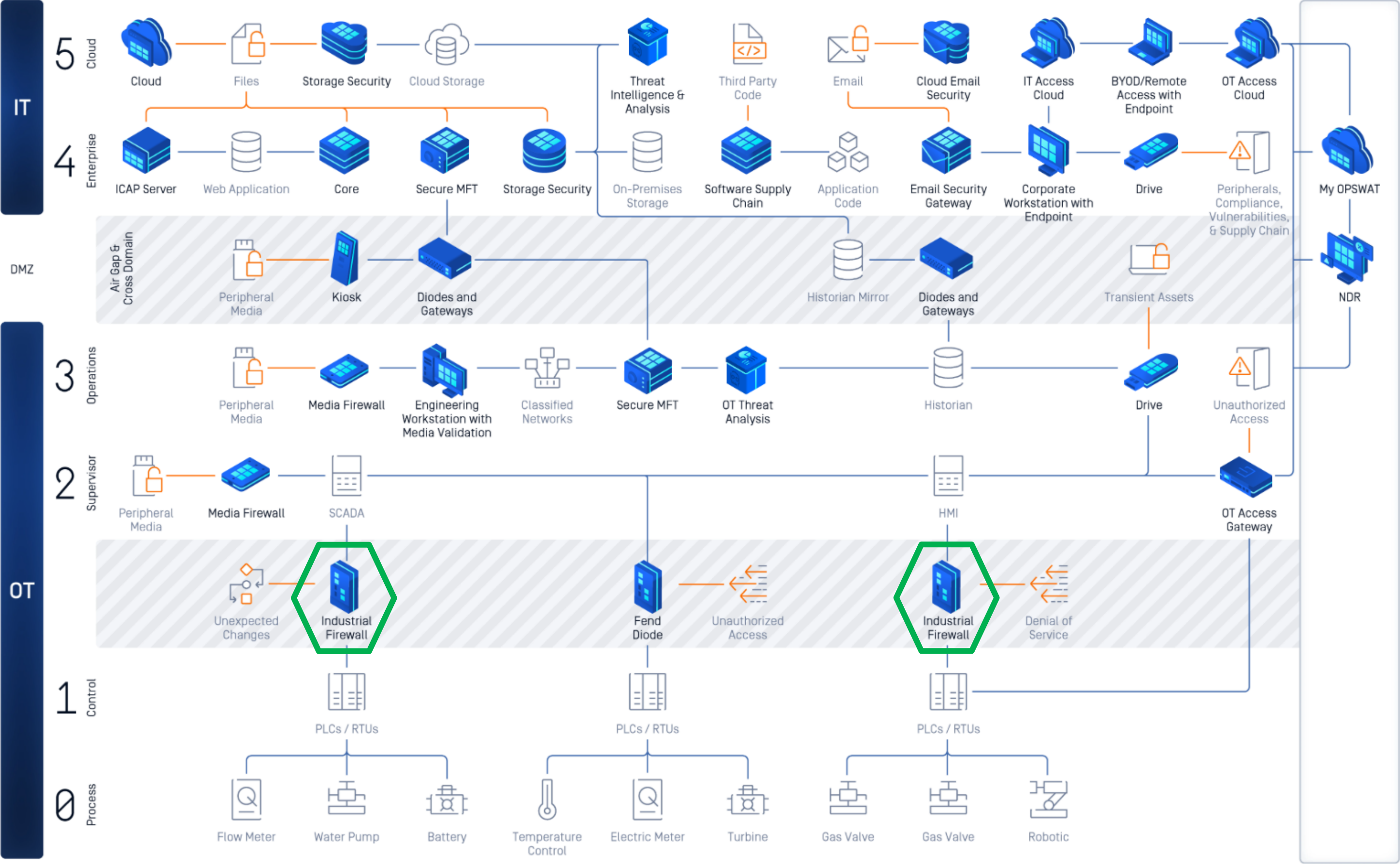


Segmentação de rede: fortalece a postura de segurança ao reduzir a superfície de ataque e isolar sistemas OT sensíveis de ameaças externas.



Conformidade com IEC 62443: ajuda a conter violações protegendo contra movimento lateral sem interromper fluxos de dados necessários.

The MetaDefender™ Platform



MetaDefender Drive

Transient Device Threat Scanner



Multiscanning

Scans with up to 7 anti-malware engines using signatures, heuristics, and machine learning to proactively detect known and unknown threats.



Scan Without a Screen

Available on the MetaDefender Drive with Digital Display, scan servers or machines with no monitor and view results on the built-in digital display.



Flexible Workflow

Full system or custom scan for specific file path. Supports scanning while target system is online or offline



Tamper Proof

Device firmware is protected by a digital signature. The ruggedized housing is waterproof and tamper proof.



Encrypted Disk Support

Detects encrypted volumes and prompts for a password, confirming that encrypted files are scanned. Supports LUKS-based encryption, macOS FileVault, and Microsoft BitLocker.



Inoperable OS Recovery

Recover inoperable operating systems by first booting from MetaDefender Drive's built-in one.



File-Based Vulnerability Assessment

Detects known vulnerabilities in more than 20,000 software applications with a patented file-based approach.



Self-Protection Against Unauthorized Files

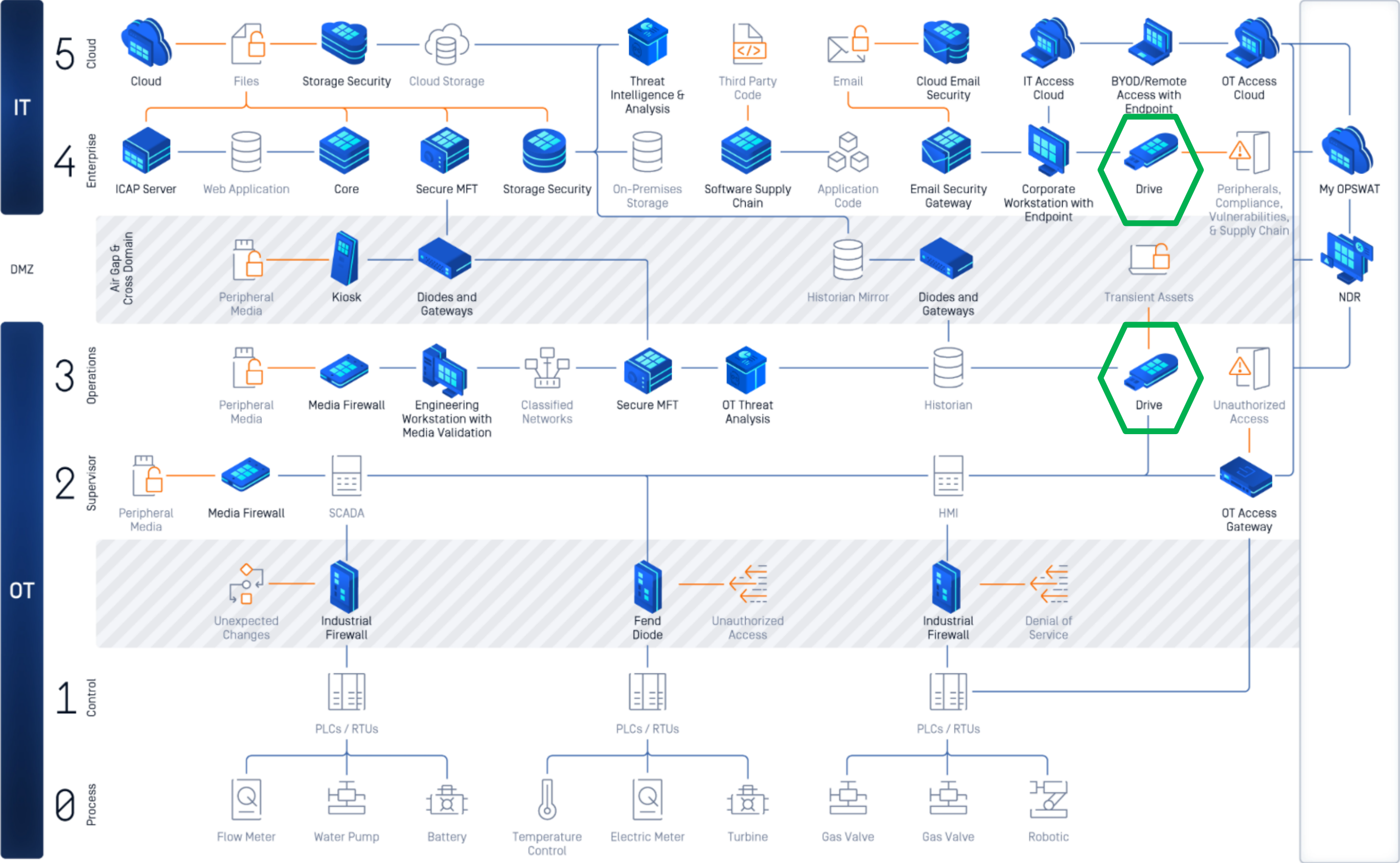
Automatically detects and removes unauthorized files during boot and when connected to MetaDefender Drive Toolkit to maintain integrity and security.



Multilingual Support

MetaDefender Drive comes with localization support, covering key interface elements in the following 12 languages: English, Dutch, German, Vietnamese, Korean, Chinese, French, Italian, Japanese, Arabic, Hebrew, and Polish.

The MetaDefender™ Platform



Comece agora com
Proteção Avançada

Fale hoje com um de nossos especialistas.

Escaneie o QR Code ou visite:

internationalit.com/opswat

vendas@internationalit.com



internationalIT

Com uma atuação orientada à excelência técnica, à proximidade com o cliente e à execução consultiva, a International IT ajuda empresas a enfrentar desafios relacionados ao monitoramento de redes, gerenciamento de infraestrutura, conectividade segura, defesa cibernética e continuidade operacional.

Seu portfólio combina serviços especializados, tecnologias líderes de mercado e capacidade de implementação ponta a ponta, permitindo que organizações reduzam riscos, melhorem desempenho e avancem com segurança em suas jornadas de transformação digital. A empresa atua desde a avaliação de cenário e definição de arquitetura até a implantação, suporte e otimização contínua dos ambientes.

Com experiência em projetos corporativos e ambientes de missão crítica, a International IT entrega valor por meio da combinação entre conhecimento técnico aprofundado, visão estratégica e execução prática. Dessa forma, capacita seus clientes a proteger redes, sistemas e dados contra ameaças conhecidas e desconhecidas, ao mesmo tempo em que apoia requisitos de conformidade, governança e disponibilidade dos negócios.

OPSWAT.

Os últimos 25 anos, a OPSWAT, líder global em cibersegurança de infraestrutura crítica para TI, OT e ICS, tem evoluído continuamente uma plataforma de soluções ponta a ponta que oferece a organizações públicas e privadas, bem como empresas dos setores de serviços financeiros, defesa, manufatura, energia, aeroespacial e transportes, a vantagem necessária para proteger suas redes complexas contra ameaças cibernéticas.

Baseada na filosofia “Não confie em nenhum arquivo. Não confie em nenhum dispositivo.”, a OPSWAT resolve desafios dos clientes, como varredura em hardware para proteger a transferência de dados, arquivos e acesso de dispositivos, utilizando soluções de zero trust e tecnologias patenteadas em todos os níveis da infraestrutura.

A OPSWAT é confiada globalmente por mais de 2500 organizações, governos e instituições de infraestrutura crítica para ajudar a proteger dispositivos, arquivos e redes contra ameaças conhecidas e desconhecidas, ataques zero-day e malware, ao mesmo tempo em que apoia conformidade com políticas e regulamentações do setor e do governo.

NetWall Series (Data Diodes) – H.A.

High Availability Solution

Comprehensive Features

- Active/Standby Architecture
- Easy to Deploy
- Automated Failover
- Wide Data Type Support
- Streamlined Updates/Maintenance
- Pre-Enabled Feature

The MetaDefender NetWall High Availability Solution uses two sets of appliances of the same type (MetaDefender Optical Diode, USG, BSG, and Transfer Guard) and an

appropriate appliance configuration. High Availability utilizes active/standby components, whereby one NetWall will be in an active state at a given time while the other NetWall will be in standby, ready to take over in the event of a failure in the active NetWall. The solution requires two network switches (blue/red), that support multicast switching, which the NetWall appliances are connected to.

The Benefits of High Availability

Maximized Uptime/ Minimized Data Loss:
Hardware redundancy with automated failover, maximizes uptime and minimizes data loss in the event of a hardware failure, power loss, or network connectivity issue

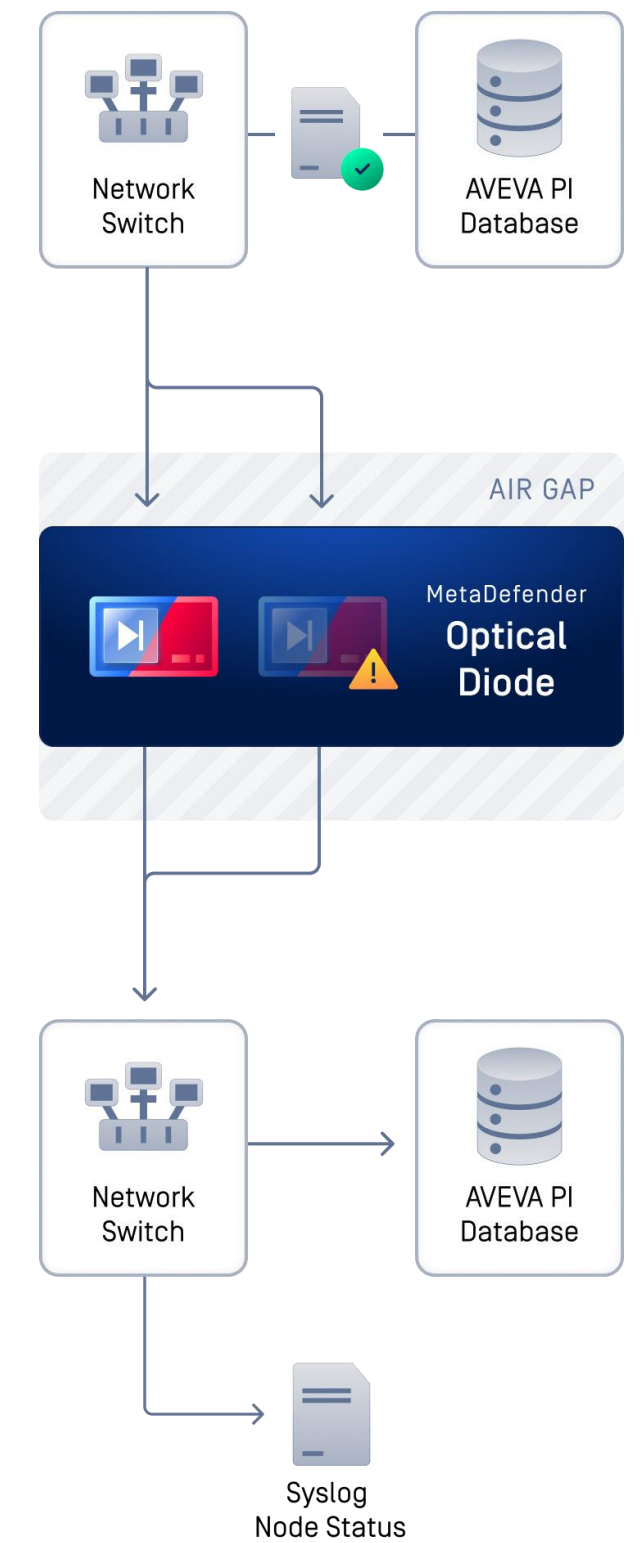
Customer Value:
Every MetaDefender NetWall product comes High Availability enabled

Future Proof Tech:
Field upgradeable—now or at a later date

First-of-its-Kind Diode Technology:
Redundant optical connections enable MetaDefender Optical Diode to overcome historical limitations associated with High Availability using data diodes



High Availability data flow with
MetaDefender USG and BSG



High Availability data flow with
MetaDefender Optical Diode

NetWall Protocol Support

All connectors included in MetaDefender NetWall products. One exception: AVEVA PI replication requires additional license purchase and supported on server based NetWall diode solutions only.

	MetaDefender USG	MetaDefender BSG	MetaDefender Optical Diode		MetaDefender USG	MetaDefender BSG	MetaDefender Optical Diode
TCP unicast multicast	✓	✓	✓	Backup of System Configuration Files	✓	✓	✓
TCP Back-to-Back Diode (Requires 2 NetWall pairs to allow TCP application responses) No support for ports 443, 80.			✓ w/ 2 NetWalls	Modbus	✓	✓	✓
UDP unicast multicast	✓	✓	✓	OPC DA / A&E (Windows OS)	✓	✓	✓
FTP, SFTP, FTPS, FTPES	✓	✓	✓	OPC UA	✓	✓	✓
SMB	✓	✓	✓	AVEVA PI (server platforms only, requires additional license fee) (Windows OS)	✓ add on Lic.	✓ add on Lic.	✓ add on Lic.
Windows FS	✓	✓	✓	Historian	✓	✓	✓
CIFS	✓	✓	✓	DNP3	✓	✓	✓
Mix & Match FT Protocols	✓	✓	✓	IEC-104	✓	✓	✓
Distributed File (DFS)	✓	✓	✓	MQTT	✓	✓	✓
OPSWAT MFT to MFT push	✓	✓	✓	ICCP	✓	✗✗	✓
OPSWAT MFT to MFT pull		✓	Back-to-Back	Ethernet/IP CIP	✓	✗✗	✓
OPSWAT Kiosk to MFT push	✓	✓	✓	SPLUNK	✓	✓	✓
HTTPS	✓	✓	✓	Goose	✓	✓	✓
Email (SMTP)	✓	✓	✓	Microsoft SQL	✗	✓	✓ w/ 2 NetWalls
Ethernet Packet (SPAN)	✓	✓	✓	Oracle	✓	✓	✓
HMI Screen View	✓	✓	✓	Database Replication	✗	✓	✓ w/ 2 NetWalls
Syslog (UDP and TCP)	✓	✓	✓				

AVEVA is a registered trademark of AVEVA Group Limited. Microsoft and Windows are registered trademark of Microsoft Corporation. Oracle is a registered trademark of Oracle Corporation. NOTE Back to Back has no support for using ports 443, 80.

Fend Protocol Support

All connectors included within Fend products, only one data flow can be enabled per device at one time.

	Fend Optic Diode XE/SE/CE 5 Mbps	Fend Optic Diode XE/SE/CE 15 Mbps	Fend Optic Diode XE/SE/CE 50 Mbps		Fend Optic Diode XE/SE/CE 5 Mbps	Fend Optic Diode XE/SE/CE 15 Mbps	Fend Optic Diode XE/SE/CE 50 Mbps
TCP	✓	✓	✓	Modbus TCP	✓	✓	✓
TLS	✓	✓	✓	Modbus RTU (in only on XE, CE)	✓	✓	✓
TCP Syslog	✓	✓	✓	BACnet (in only)	✓	✓	✓
UDP	✓	✓	✓	LON-IP (in)	✓	✓	✓
UDP Syslog	✓	✓	✓	Historian (File Transfer)	✓	✓	✓
FTP	✓	✓	✓	OPSWAT OPC DA, A&E	✓	✓	✓
SFTP	✓	✓	✓				
FTPS	✓	✓	✓				
OPSWAT Screen View	✓	✓	✓				
HTTPS w/custom response			✓				
OPSWAT MFT to MFT HTTPS			✓				
OPSWAT Kiosk to MFT HTTPS			✓				
				Syslog Diode output, all output on the output side of the diode.			✓

Fend Protocol Support and Conversions

Input	UDP Server	Ethernet
	TCP Server	
	TCP Server (w/ TLS)	
	Syslog (over UDP or TCP)	
	SFTP Server	
	FTPS Server	
	FTP Server	
	OPSWAT Screen View	
	Modbus TCP Master / Client	
	Modbus TCP (Listen)	RS485
	BACnet IP (Listen)	
	LON IP (Listen)	
	Modbus RTU Master / Client	
	Modbus RTU (Listen)	
	BACnet MSTP (Listen)	

All Models

Output												
UDP Client	TCP Client	TCP Client (w/ TLS)	Syslog (over UDP or TCP)	SFTP Client	FTPS Client	FTP Client	OPSWAT Screen View	Modbus TCP Slave / Server	TCP Client (JSON Conversion)	MQTT (Fend Cloud)	Modbus RTU Slave / Server	MQTT (Fend Cloud)
Ethernet											RS485	Cellular
All Models											SE Only	CE Only
Y	Y											
Y	Y											
Y	Y	Y										
			Y									
				Y	Y	Y						
				B	Y	Y						
				B	B	Y						
							Y					
								Y	Y	Y	Y	Y
								Y	Y	Y	Y	Y
									Y	Y		Y
									Y	Y		Y
									Y	Y	Y	Y
								Y	Y	Y	Y	Y
									Y	Y		Y

Y = Fully Supported
B = Supported in Buffered Mode Only

NetWall Series (Data Diodes)

Use cases



ONE WAY OUT OF OT

- ✓ Historian Replication
- ✓ Reporting Files, file structures replication
- ✓ Syslog data, systems performance
- ✓ Security Information Event Management (SIEM)
- ✓ Raw machine data, OPC, Modbus, others
- ✓ Alarms and events, OEM systems data
- ✓ Vibration Monitoring
- ✓ OEM System performance
- ✓ Digital Twin data
- ✓ Power condition monitoring
- ✓ Performance/use data to suppliers
- ✓ Subnet cell/area zone data to DCS/SCADA
- ✓ SCADA data collection and output
- ✓ OT asset protection
- ✓ Safety Information Sys to Digital Control Sys



ONE WAY INTO OT

- ✓ Patch update systems
- ✓ Patch updates with file scanning
- ✓ 3rd party onsite delivery of software
- ✓ Quantum Encryption Key Delivery
- ✓ Secure supply chain
- ✓ IT to OT Application Data
- ✓ Weather data for operations
- ✓ Operations planning
- ✓ Transient System Scanning
- ✓ Subnet cell/area zone updates



BIDIRECTIONAL

- ✓ Secure Remote Access (RSA)
- ✓ Remote Desktop Protocol (RDP)
- ✓ Guaranteed Data Delivery
- ✓ SQL synchronization
- ✓ 3rd party applications that can not be supported one-way