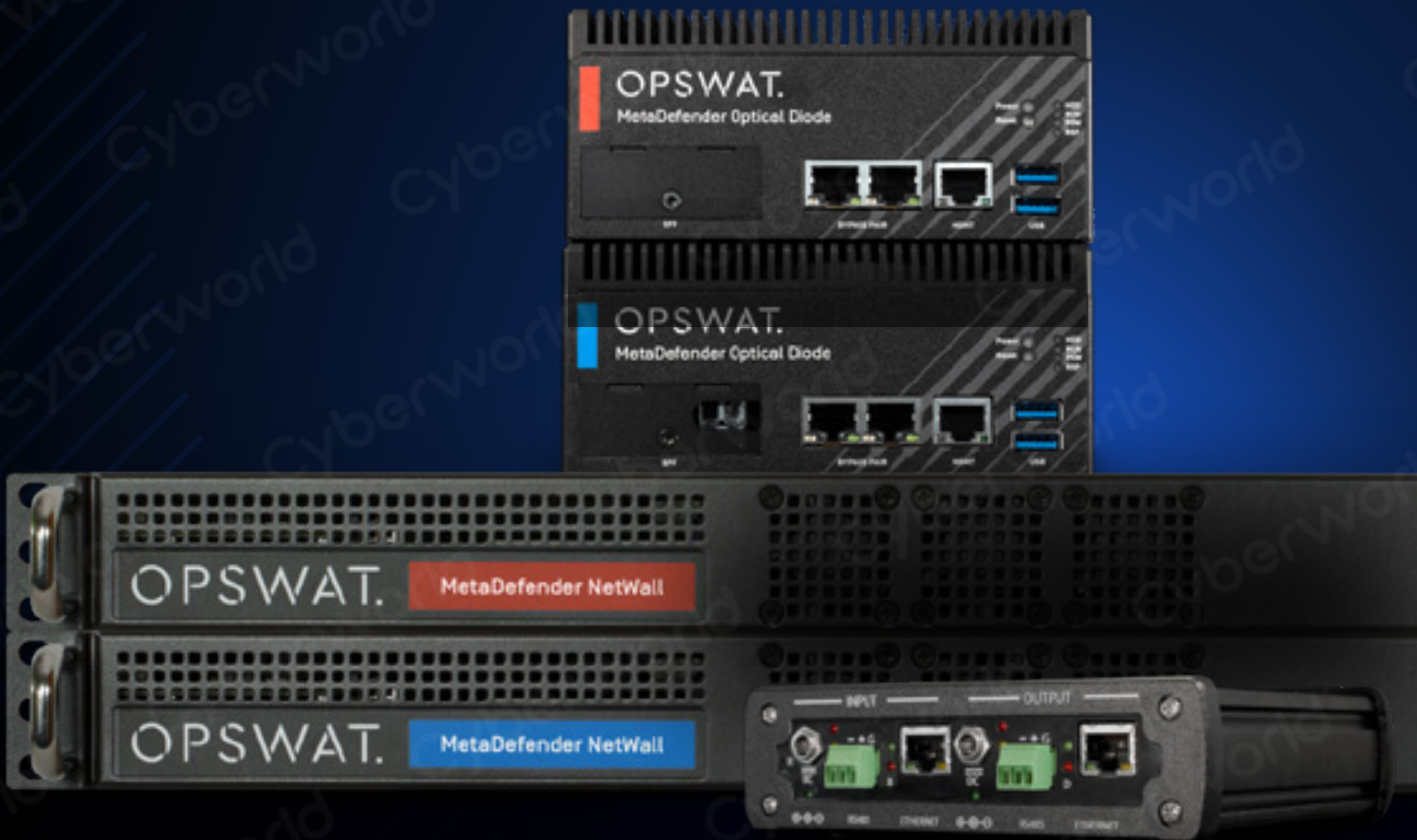


METADEFENDER

NetWall™ 系列

新一代 Data Diode (数据隔离装置) 与 Security Gateway (安全网关) 解决方案
保障 IT-OT 零风险通信





挑战

在 IT 与 OT 融合的世界中 保护您的关键网络

IT 与 OT 的系统、流程和人员之间曾经清晰的界限正在逐渐消失。

由于企业对工业环境中的连接和数据分析需求不断增加,传统的 OT 与 IT 网络分段之间的物理隔离 (air gap) 已被侵蚀。

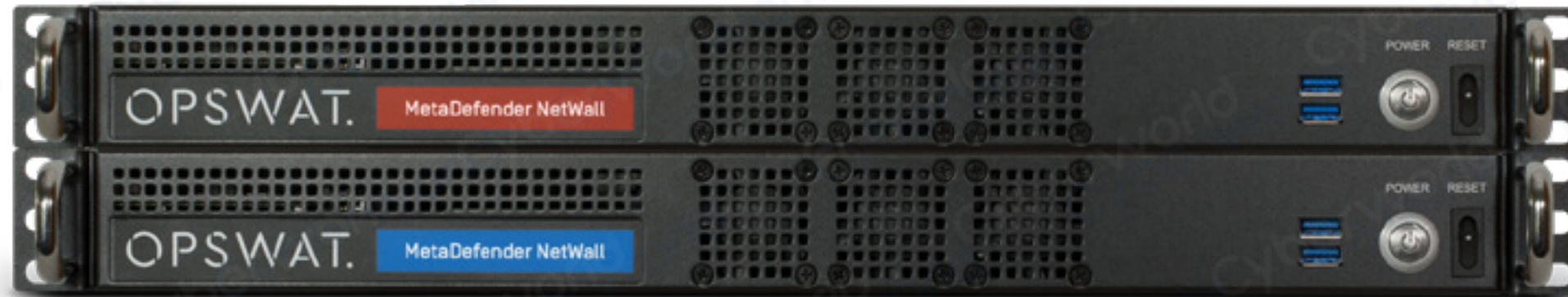
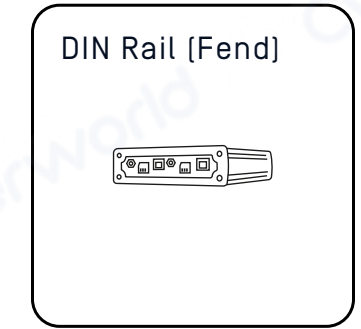
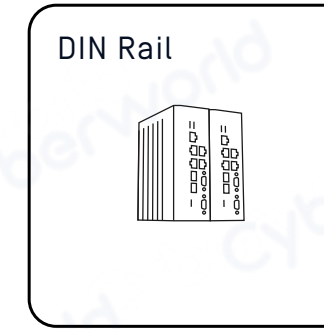
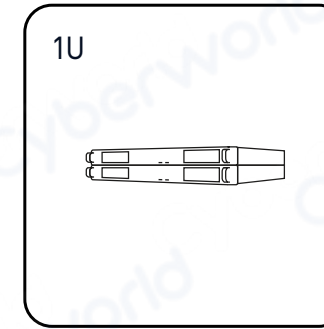
这种连接需求的增加,让工业资产暴露在针对性网络攻击之下,因为防火墙和下一代防火墙本质上是双向的。它们依赖基于软件的策略,容易出现配置错误,从而被攻击者利用。

MetaDefender Optical Diode™ (单向光闸) (Fend) 与 Security Gateways (安全网关) 可提供对实时 OT 数据的访问,实现向 OT 环境的安全数据传输,不会损害关键生产系统的安全性与完整性。

METADefENDER

NetWall 系列

可用的机型规格



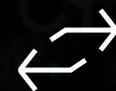
功能特性



实时传输 OT 数据至业务用户，不干扰其工作流程。



无风险，网络威胁无法进入受保护的 OT 网络。



支持文件传输及数据库、服务器复制，无需依赖特定厂商的专有硬件与软件。



高保障的负载传输，支持并发传输多种数据类型。[†]



无需复杂的防火墙审计、策略配置，也不会 OT 网络中产生高风险的后门通道。



广泛兼容 OPC (DA、AgE、UA)、IEC 104、AVEVA PI、Modbus/TCP 等工业协议，支持文件传输及 TCP/UDP sockets (套接字)。



符合 NERC CIP、NIST CSF/800-82/800-53/ICS、IEC 62443、NRC 5.71、CFATS、ISO 27001/27032/27103、ANSSI、IIC SF 等标准。防御 MITRE ATT&CK for ICS 框架所列出的工业攻击技术。



OPSWAT 提供 100Mbps 基础平台，可现场升级至 1Gbps。另有企业级服务器上交付的 10Gbps 选项。10Mbps DIN Rail 型号可现场升级至 50Mbps。

[†] 仅适用于 USG 型号

METADEFENDER™

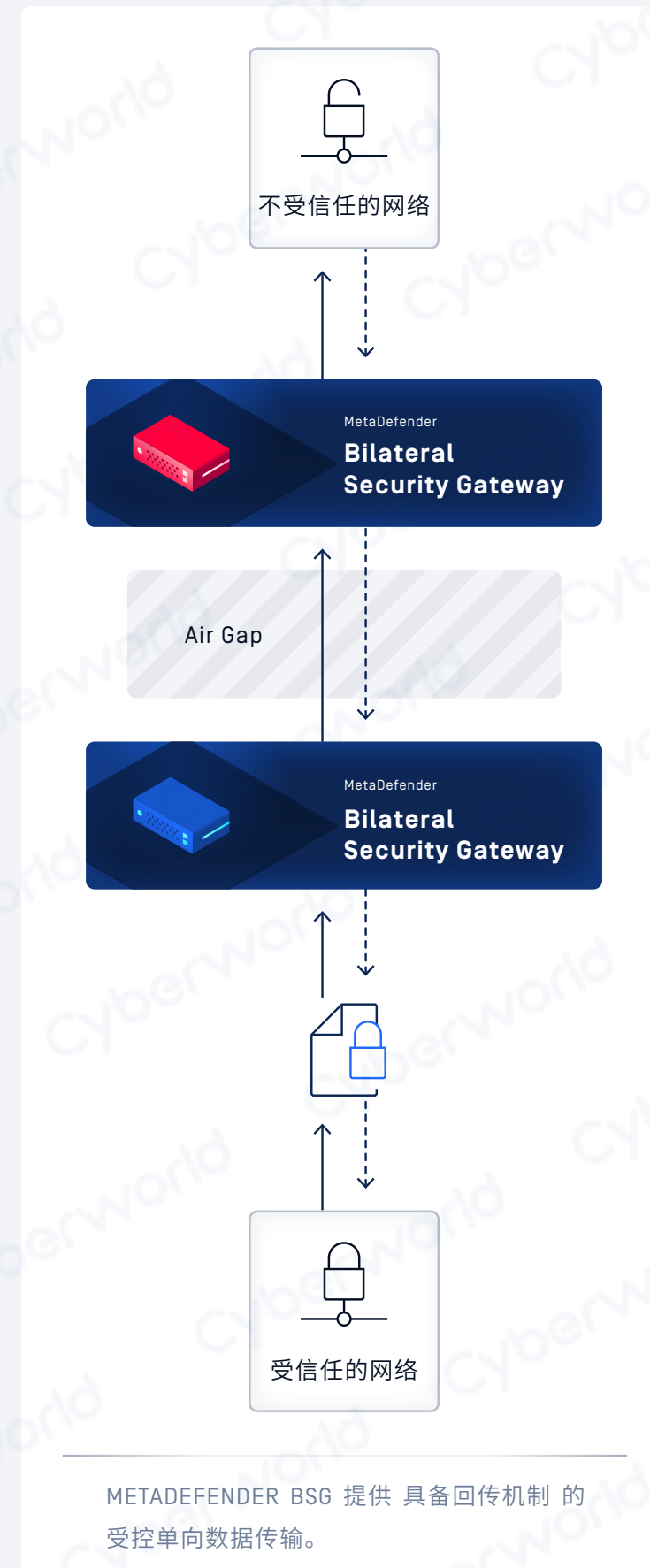
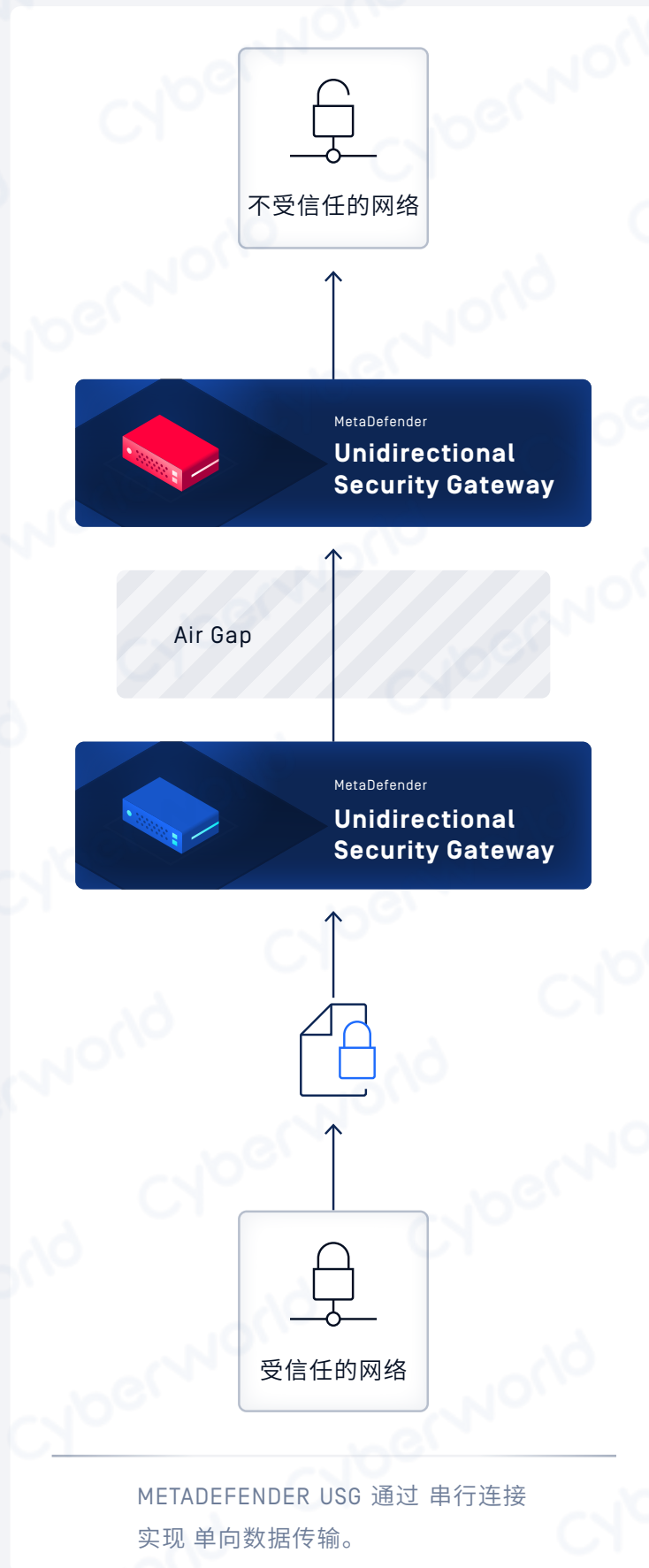
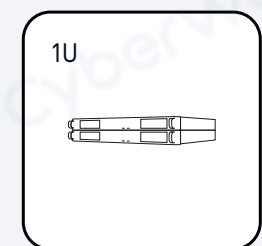
Unidirectional Security Gateway [USG]

单向安全网关

MetaDefender Unidirectional Security Gateway (USG, 单向安全网关) 提供对实时 OT 数据的访问, 支持安全的 IT-OT 数据传输, 具备高速、低延迟、功能齐全的全部优势, 确保可靠性, 无数据丢失。

由于不存在返回路径网络, MetaDefender USG 能够保证实时运行的数据可以安全地传送到企业网络用户, 而不会给受保护的 OT 网络带来安全威胁。

可用的机型规格



METADEFENDER™

Bilateral Security Gateway [BSG]

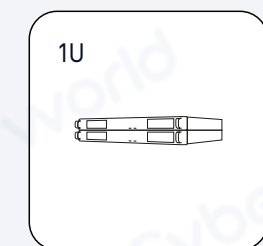
双向安全网关

MetaDefender Bilateral Security Gateway (BSG, 双向安全网关) 在具备 MetaDefender USG 全部功能的基础上, 还支持需要数据响应才能运行的应用程序, 例如 Historian (历史数据库) 和 SQL 数据库服务器。

MetaDefender BSG 可执行实时数据复制, 无数据丢失, 并通过双向机制处理数据响应, 同时不损害 OT 网络的安全性与完整性。

当受信任的网络向不受信任的网络的目标发起连接时, MetaDefender BSG 会执行完整的协议阻断, 允许目标端的特定应用通过不可路由的连接, 安全地向源应用返回数据响应。MetaDefender BSG 不允许不受信任的网络主动发起连接, 从而确保通信通道不会被利用。

可用的机型规格



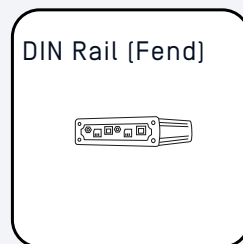
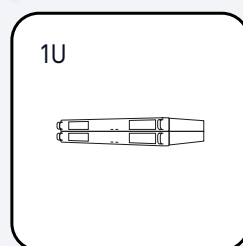
METADefENDER™

Optical Diode 单向光闸

MetaDefender Optical Diode (单向光闸) (Fend) 提供硬件强制 (hardware-enforced) 的单向实时 OT 数据传输, 并通过可靠、高速、低延迟的光链路实现安全的 IT-OT 数据传输。由于不存在返回路径网络, MetaDefender Optical Diode (单向光闸) (Fend) 在传输实时运行数据的同时, 符合行业对确定性单向传输设备的监管要求。MetaDefender Optical Diode (单向光闸) (Fend) 还执行负载完整性检查, 支持冗余光链路, 实现无与伦比的可靠性与数据传输保障。

MetaDefender Optical Diode (单向光闸) (Fend) 可部署在企业级服务器或工业级 DIN rail 服务器 (多机箱与单机箱结构), 适用于严苛的工业环境。

可用的机型规格



*不适用于 Fend diodes (隔离装置)



METADefENDER™

Super Diode Cross Domain 进阶型隔离装置 跨域传输

原名: MetaDefender Transfer Guard

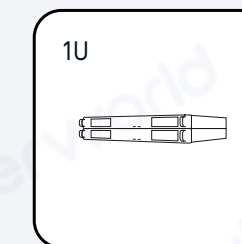
具备 File Sanitization (文件净化) 功能

MetaDefender Super Diode Cross Domain 集成了 OPSWAT 屡获殊荣的 MetaDefender Core™ file sanitization (文件净化) 引擎。

文件通过 Super Diode Cross Domain 跨越网络安全边界安全传输至目标端之前, MetaDefender Core 会对文件进行彻底的扫描与净化。

该功能可部署在 MetaDefender Optical Diode (单向光闸) 平台上。

可用的机型规格



聚焦最高的 安全性与可靠性

MetaDefender NetWall 与 防火墙 对比

传统防火墙、路由规则、VLAN可以限制或划分流量，但它们仍然依赖双向的、可路由的连接，这让 OT 网络暴露在网络风险之中。

Optical diodes (单向光闸) 强制执行真正的单向安全，物理上阻止外部连接进入受保护的 OT 域。这让它们在本质上比防火墙更安全，仍能实现受控的数据外传。

网关：
类似隔离装置
但具备可靠传输保障

不同于传统 data diodes (数据隔离装置) 仅强制单向通信而不确认接收情况，Security Gateways (安全网关) 把单向数据传输与负载传输保障相结合，避免数据丢失、重复传输。这确保了数据完整性，防止数据丢失，消除了重传需求，为企业提供了 data diodes (数据隔离装置) 级别的安全性，同时保证每一个关键数据包都能完整到达目标端。

MetaDefender Optical Diode (单向光闸) 与其它 Data Diodes (数据隔离装置) 对比

不同于其他 data diodes (数据隔离装置)，MetaDefender Optical Diode (单向光闸) 提供更高的传输保障、更强的可扩展性、更简便的配置与部署。

功能特性	NetWall	网络解决方案
路由配置	✓	✓
协议阻断 (Protocol break) 完全脱离 TCP/IP 连接	✓	✗
满足 data diodes (数据隔离装置) 的功能需求 (NetWall USG)	✓	✗
确保数据不仅能成功送达 而且传输行为可以被验证、无法否认	✓	✗
无需繁琐的规则构建	✓	✗
保证阻止恶意软件传播	✓	✗
无 ARP、BGP、TCP/IP 握手过程	✓	✗

功能特性	Optical Diode (单向光闸)	其他 Data Diode
单向数据流	✓	✓
彻底的协议阻断 (Protocol break)	✓	✓
冗余光学连接 确保数据传输的高度可靠性	✓	✗
吞吐量范围: 5Mbps - 10Gbps	✓	✗
管理员访问专用的硬件加密狗 (dongle)	✓	✗
快速且易于部署	✓	✗
高性价比 可选 订阅 或 永久许可	✓	✗

应用案例

高效监控 电力变电站 同时符合 NERC CIP 合规要求

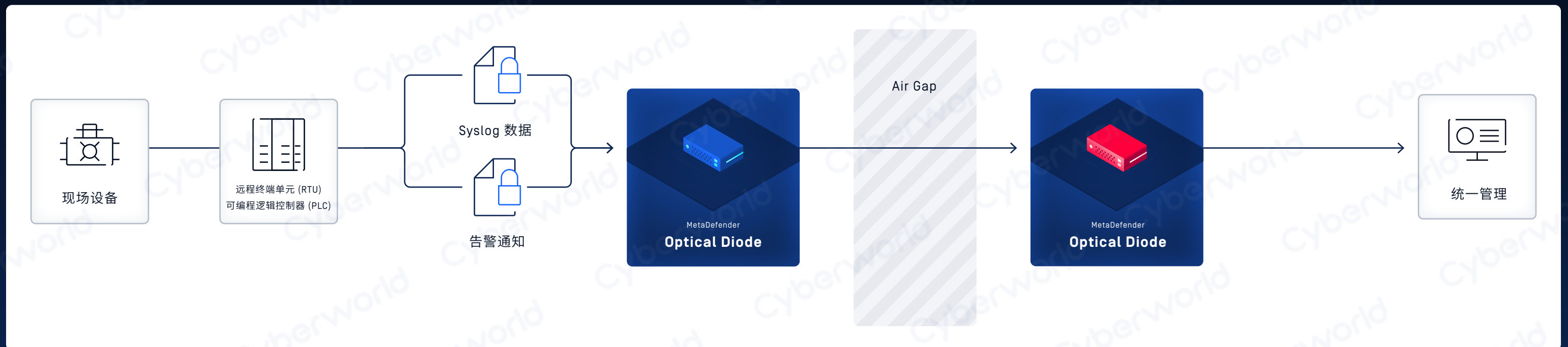
挑战

遵循 NERC CIP 合规要求, 保护 data substations (数据变电站) 免受外部威胁, 同时建立一种运营高效的变电站监控方法。

解决方案

MetaDefender Unidirectional Security Gateway (USG, 单向安全网关) 能够复制日志文件, 并支持把 syslog 传输到一个或多个 SIEM 系统。

MetaDefender USG 的可靠数据传输架构 可实现实时数据传递, 支持高效的系统监控与告警管理。



应用案例

在三座电厂与企业级历史数据库之间进行 AVEVA PI 数据复制

挑战

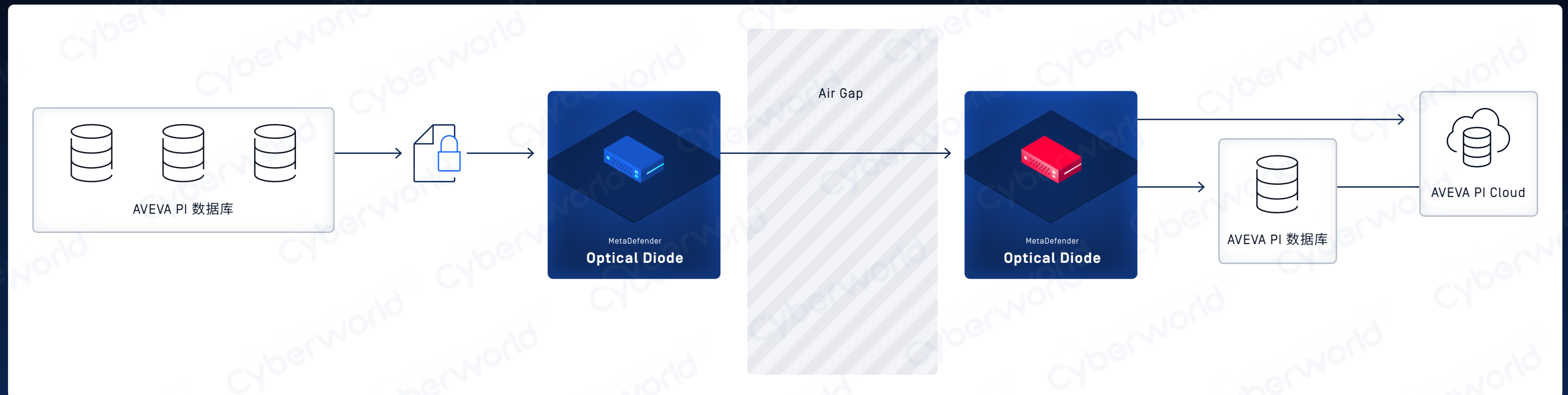
三座电力涡轮发电厂的历史数据已采集至 AVEVA PI historians (历史数据库)。

在电厂资产周围建立安全边界后, 需要一种安全机制把 OT 历史数据共享至 IT 业务网络。

解决方案

MetaDefender Optical Diode (单向光闸) 通过 MetaDefender AVEVA Pi Connector (连接器) 可靠地复制 AVEVA Pi historian (历史数据库) 数据。

数据经不可路由的协议阻断进行传输, 提升源网络的安全性与机密性。



应用案例

能源供应商 要求 对 HMI 屏幕进行安全复制

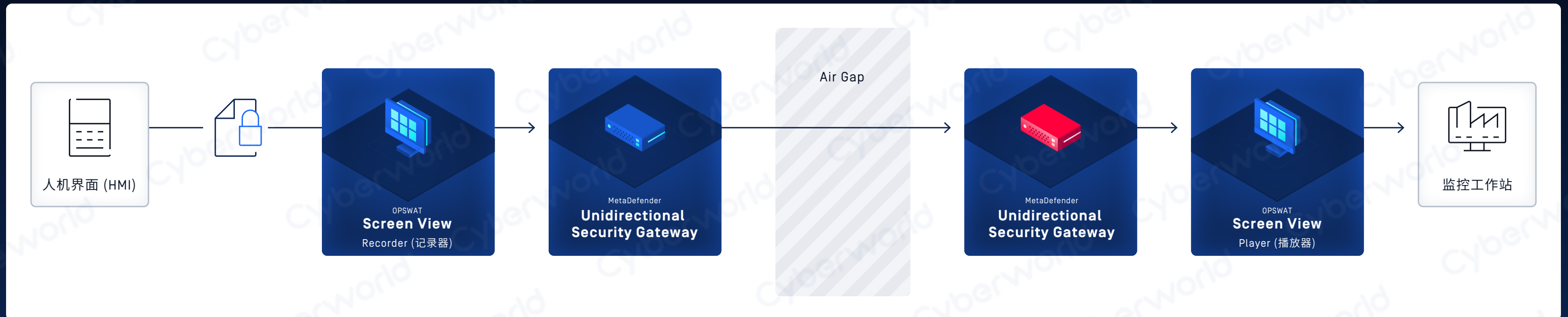
挑战

在不影响 OT 基础设施安全的前提下, 把 OT HMI 屏幕 复制 到 中央监控设施。

解决方案

MetaDefender Unidirectional Security Gateway (USG, 单向安全网关) 在工厂内部 实时捕获 HMI 屏幕图像, 并将其 复制 到 IT 网络上的远程监控位置。

MetaDefender Screen View connector (连接器) 通过 强制单向传输 和 不可路由的协议阻断, 复制 HMI 屏幕图像。



应用案例

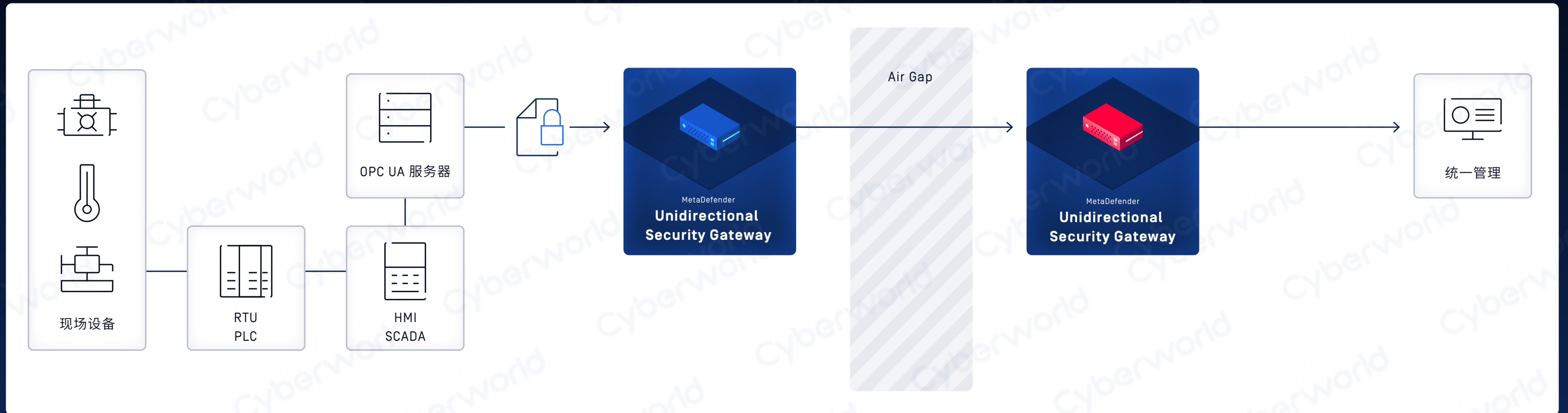
水厂要求 实时复制 OPC 数据

挑战

在水处理和污水处理设施中, 确保 OT 基础设施安全的前提下, 把 实时运行数据 从 OT 安全传输至 IT 。

解决方案

MetaDefender Unidirectional Security Gateway (USG, 单向安全网关) 原生支持 Open Platform Communications Unified Architecture (OPC UA, 开放平台通信统一架构), 可与 OT 域中的 OPC UA 服务器集成, 并通过 不可路由的协议 实现 强制单向传输, 把实时数值传输至 IT 。



应用案例

国家级医疗服务提供商 要求 安全传输数据中心告警与监控数据

挑战

在不影响 OT 基础设施安全的前提下,复制数据中心告警和监控数据。

解决方案

MetaDefender Optical Diode (单向光闸) 可以把告警与监控数据 安全传输至 中央监控位置。

MetaDefender 的 Modbus、SFTP 与 SMTP (电子邮件) 连接器通过不可路由的协议阻断, 实现强制单向传输。



应用案例

把合规报告文件 从 OT 传输到 IT

石油和天然气供应商 要求 散装工厂(Bulk Plant) OT 网络中的文件 安全传输至 企业 IT 网络。

挑战

工厂的合规报告在 OT 网络中以文件形式生成, 并传输到 IT 网络。

当在散装工厂周围建立安全边界时, 需要一种安全的方式, 把 合规报告 安全共享到 外部业务网络。

解决方案

MetaDefender Unidirectional Security Gateway (USG, 单向安全网关) 通过 安全文件传输 (SFTP) 可靠地传输 合规报告。

文件经 不可路由的协议阻断, 实现单向安全传输, 且无法回流至 OT 网络。



应用案例

液化天然气生产商 要求 对 OPC DA/AE 数据 进行安全的实时复制

挑战

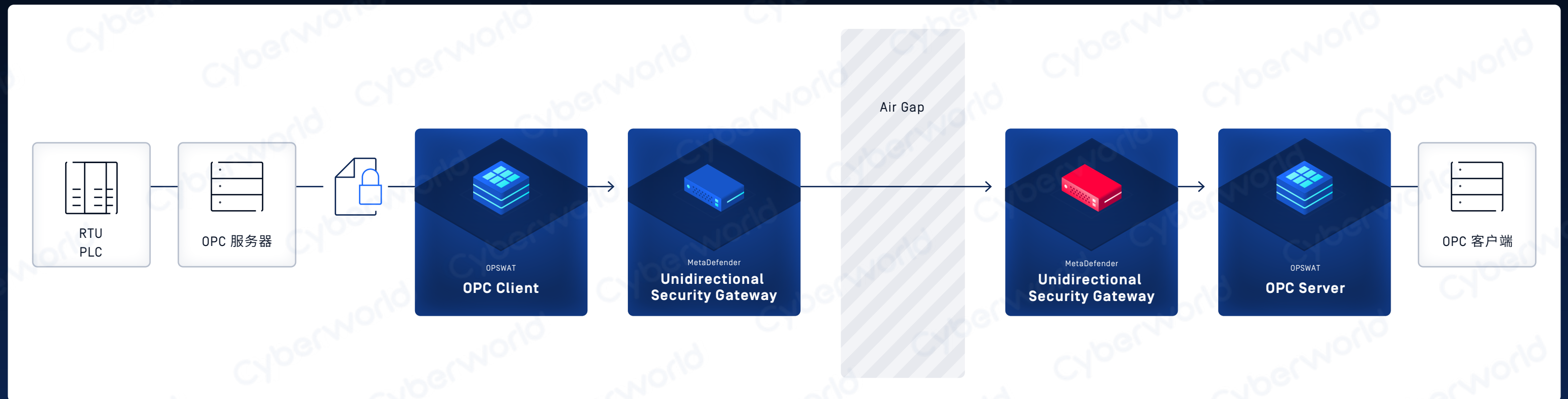
在不影响 OT 基础设施安全的前提下,把实时 OPC DA/AE 数据 从 OT 传输到 IT 。

解决方案

MetaDefender Unidirectional Security Gateway (USG, 单向安全网关) 原生支持 OPC DA/AE 。

MetaDefender OPC Connector (连接器) 在 OT 网络中充当 OPC Client (客户端), 在 IT 网络中充当 OPC Server (服务器)。

MetaDefender通过不可路由的协议阻断,实现强制单向传输,把实时 OPC 数值与 告警、事件 安全传输至 IT。



应用案例

从 MetaDefender Kiosk 安全传输文件至 Managed File Transfer (MFT)

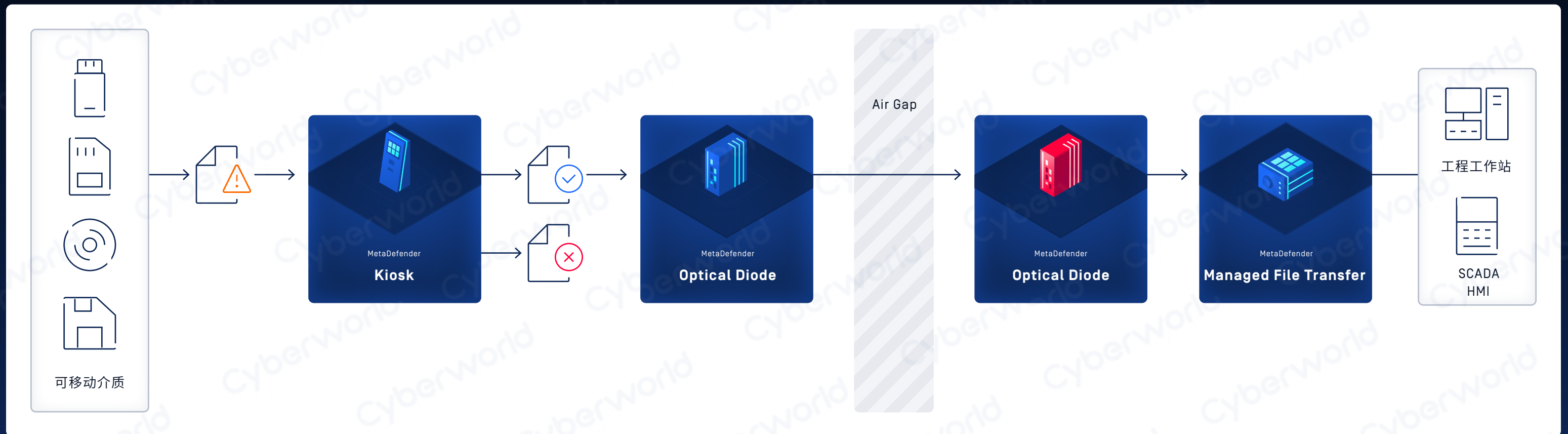
挑战

通过安全文件传输机制, 实现 便携式介质 上的 软件更新、补丁、文件 传输, 并在 IT 网络中进行安全清理, 以防止恶意软件传播至 OT 网络。

解决方案

MetaDefender Kiosk 通过 Multiscanning AV engines (多引擎杀毒扫描) 和 file sanitization (文件净化), 仅让 已知的安全文件 跨越 网络边界 传输。

MetaDefender Unidirectional Security Gateway (USG, 单向安全网关) 提供物理隔离的网络分离, 并把文件安全传输到 MetaDefender MFT。



应用案例

在发电厂的灾难救援设施中 创建安全备份

挑战

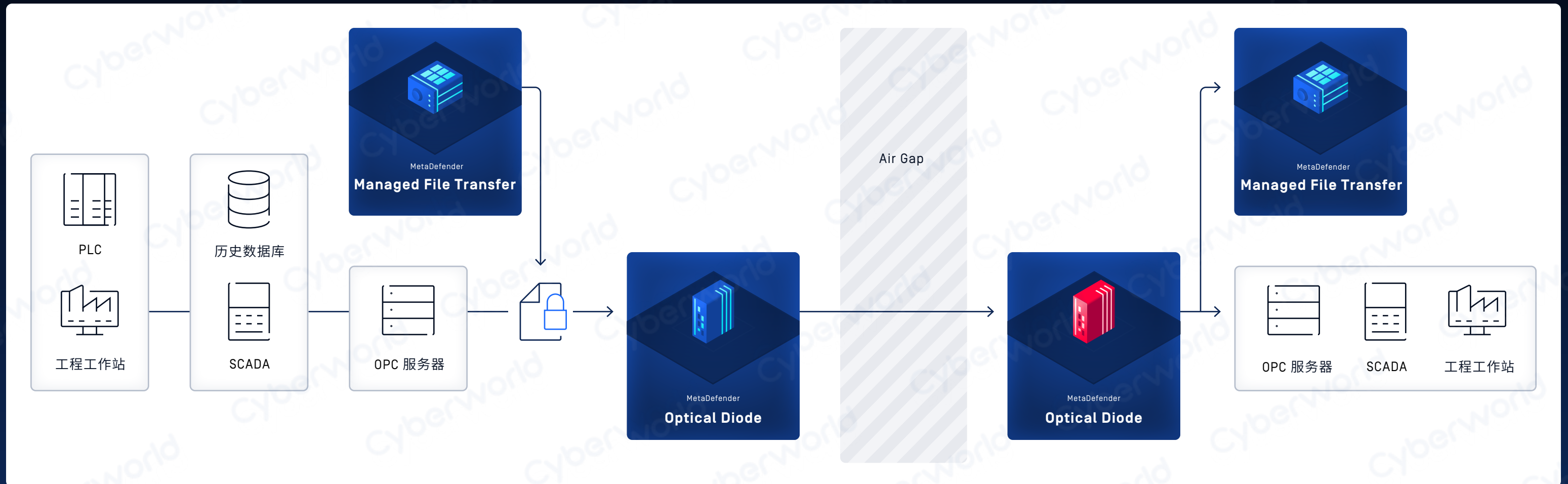
在发生物理或网络问题导致正常运行受损时，需要一个安全的备份站点来恢复运营。

该站点必须隔离，以防止恶意软件传播到灾难恢复设施。

解决方案

MetaDefender Optical Diode (单向光闸) 可把实时 SCADA 数据复制至灾难恢复备份站点，并与受损环境隔离。

MetaDefender Managed File Transfer (MFT) 到 MFT 的复制功能，可把设备软件的最新版本存储在备份设施中。



应用案例

食品加工厂 要求 把 MQTT 消息 安全复制到 云端代理 (Broker)

挑战

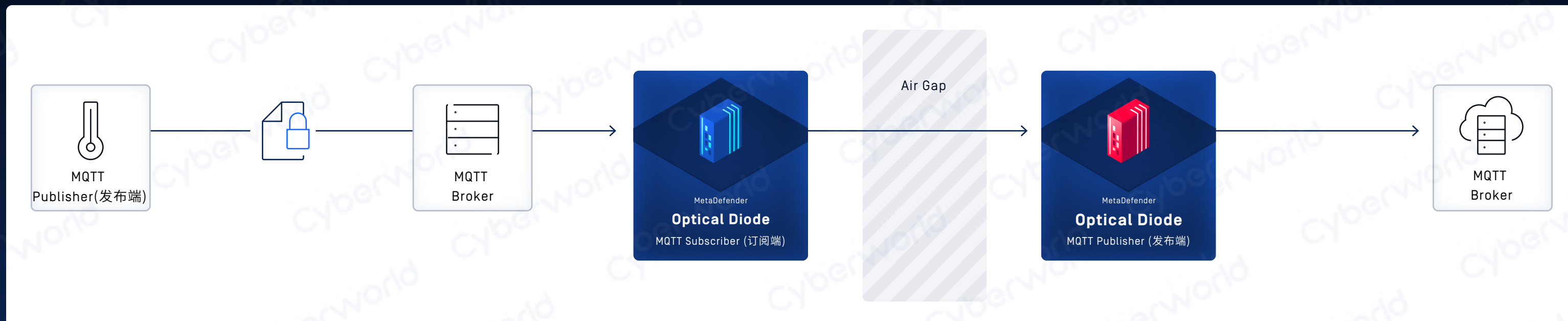
在不影响 OT 基础设施安全的前提下,把 MQTT 消息安全复制并传输到云端部署的 MQTT Broker。

解决方案

MetaDefender Optical Diode (单向光闸) Din Rail 原生支持 MQTT。

MQTT connector (连接器) 在 OT 网络中充当 MQTT Subscriber (订阅端), 在 IT 网络中充当 MQTT Publisher (发布端)。

Optical Diode (单向光闸) 通过 TLS 连接, 在不可路由的协议阻断下, 实现强制单向传输, 把 MQTT 消息安全传输至云端 Broker。



应用案例

在 DeltaV 控制网络周围 建立安全边界

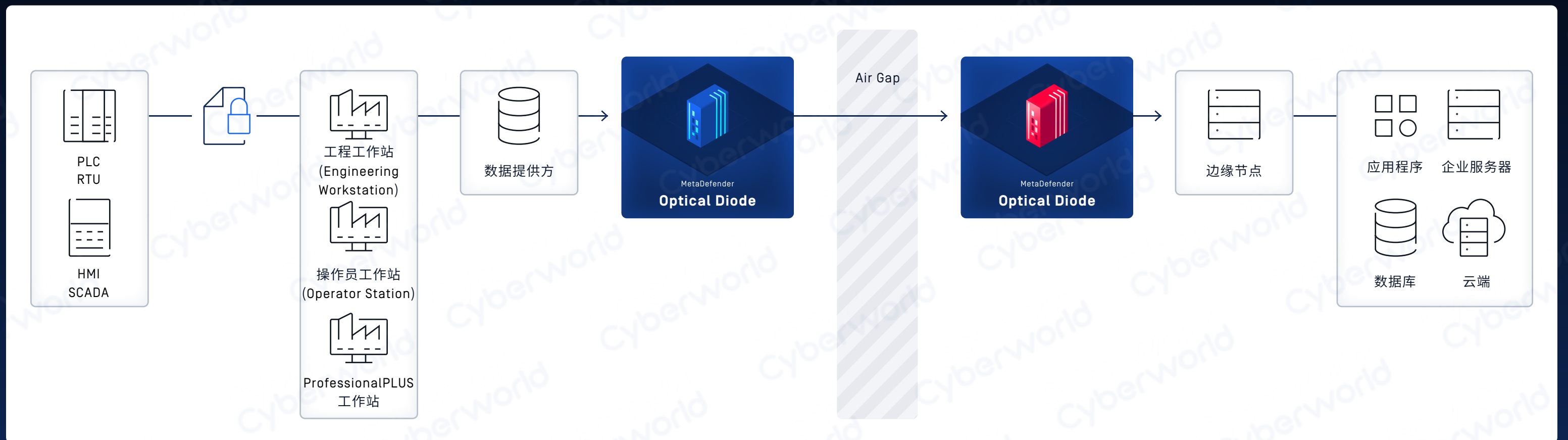
挑战

把数据从 数据提供方 安全传输至 边缘节点,同时防止外部入侵或数据被回写至 DeltaV。

解决方案

MetaDefender Optical Diode (单向光闸) 可直接连接 数据提供方 与 边缘节点。

MetaDefender HTTPS connector (连接器) 通过不可路由的协议阻断,实现强制单向传输,确保不存在 外部入侵 或数据被回写至 DeltaV 的可能性。



应用案例

使用 Fend Diodes (隔离装置) 传输工业 Modbus 数据 实现 远程监控

挑战

水务公司依赖于遍布处理厂和配水系统的数千个工业传感器和控制器。这些系统通常运行 Modbus TCP 或 Modbus RTU。操作员和工程师需要及时获取运行数据，以监控工厂性能并确保水质。

然而，为了提供对 Modbus controllers (控制器) 和 PLC 的访问而开放网络通道，会让关键设备面临网络风险，包括勒索软件攻击和远程利用。

解决方案

MetaDefender Optical Diode(单向光闸)(Fend)内置支持 Modbus TCP 与 Modbus RTU, 可实现从 处理厂网络 到 监控中心远程服务器的 传感器与控制器数据的安全单向传输。

MetaDefender Optical Diode(单向光闸)(Fend) 还可以在设备端进行协议转换, 例如: 把传统的 Modbus RTU 转换为 Modbus TCP 或 JSON 格式。操作员无需建立回传通道, 即可获得对生产过程性能的可视化, 从而在保持物理隔离的控制环境下, 确保持续监控、合规性、运营效率。



应用案例

使用 Fend Diodes (隔离装置) 实现安全数据传输 并在云端进行分析

挑战

制造工厂正逐步采用基于云的分析, 以实现预测性维护、能源优化、生产效率洞察。

然而, 把生产环境直接连接至云端存在风险, 可能引入恶意软件或命令通道, 干扰生产运行。

解决方案

MetaDefender Optical Diode(单向光闸)(Fend) 可安全地从生产环境中提取数据, 经本地以太网或 LTE 传输至 Fend Cloud。在云端, 数据被收集, 并通过 API 安全传递至第三方或内部分析平台。

此方法确保数据机密性与完整性, 同时阻止任何进入关键制造资产的连接。



应用案例

在石油和天然气生产网络实现工业控制数据从 OT 向 IT 传输的单向防护

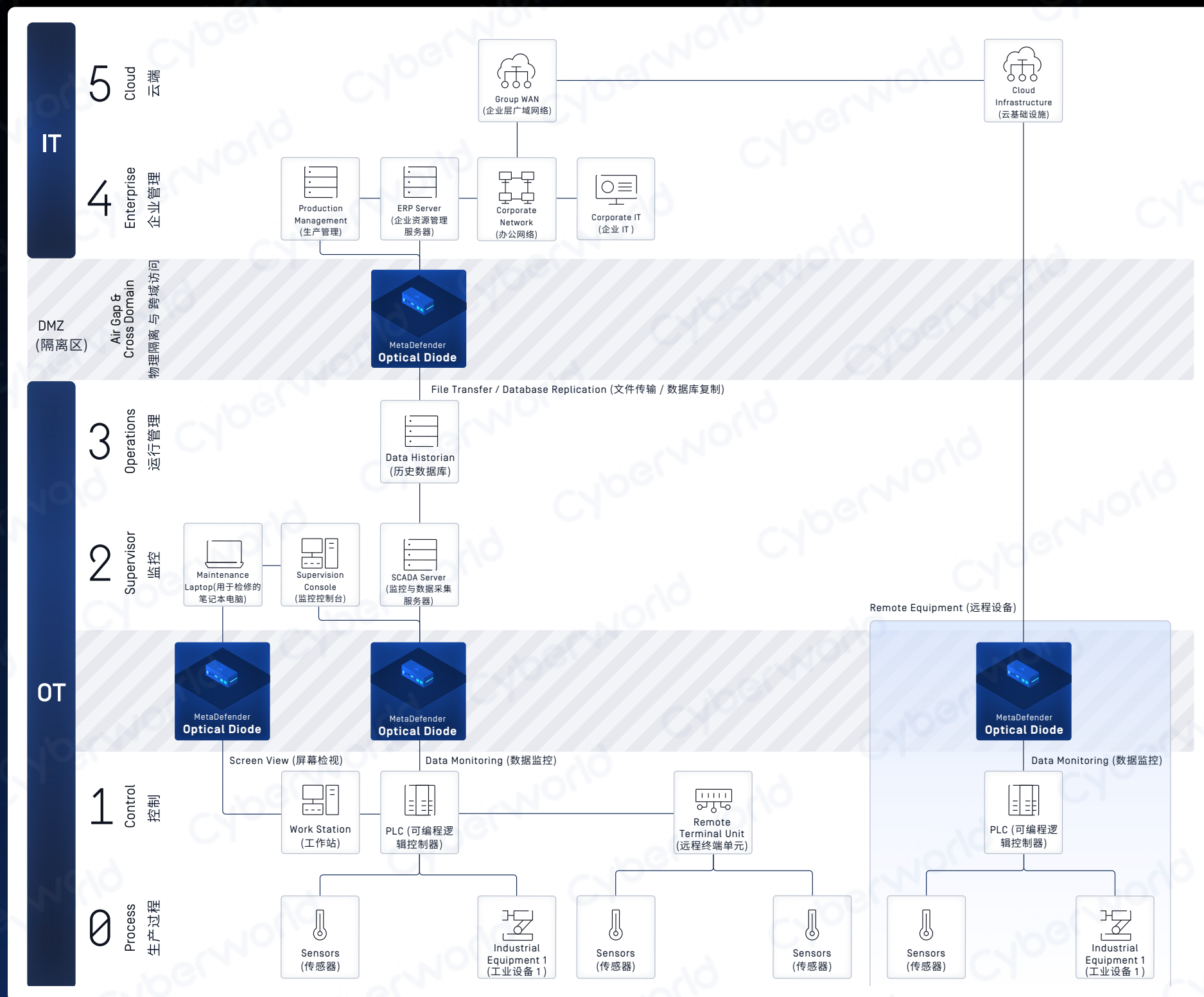
挑战

石油和天然气网络承载着关键资产，例如：运行钻井、压缩、炼制的 PLC、SCADA 服务器、RTU。企业 IT 部门和监管团队需要持续访问日志、合规报告、性能指标，这些一般通过 UDP/TCP 传输。然而，开放这些通道会让生产网络暴露于网络风险、配置错误、攻击之中，可能导致运营或安全受到干扰。

解决方案

MetaDefender Optical Diode (单向光闸) (Fend) 为 UDP、TCP、Syslog 提供硬件强制 (hardware enforced) 的单向通信，实现从生产环境到 IT 的安全传输。

数据、告警、日志可安全输出，而所有入站流量均被阻止。此隔离方式在不暴露 PLC 或设备的情况下，提供实时可视化 和 合规保障，帮助操作员减少停机时间，并提升安全性。



应用案例

SQL Server 复制

挑战

使用原生复制工具, 实现大型 Microsoft SQL 数据库的实时安全复制, 确保同步无误。

解决方案

MetaDefender Bilateral Security Gateway (BSG, 双向安全网关) 采用 微软标准的事务复制服务, 无需复杂脚本、自定义安装 或 修改 SQL 环境。SQL Server复制对用户没有影响。当连接暂时中断时, 标准缓冲机制会自动接管。MetaDefender 保持 微软复制约束, 不增加额外要求。



应用案例

AspenTech IP.21 数据复制 实现工厂与企业级历史数据库 之间的同步

挑战

工厂历史数据被采集,并存储在称为“历史数据库 (historians)”的专用数据库中。

当在工厂资产周围建立安全边界时,需要一种安全机制,把历史数据库数据共享至外部业务网络。

解决方案

MetaDefender Bilateral Security Gateway (BSG, 双向安全网关) 使用原生 AspenTech IP.21 复制功能,可靠地复制历史数据库数据。数据通过不可路由的协议阻断,进行传输,从而提升源网络的安全性与机密性。



立即启用

您是否准备好 把 MetaDefender NetWall 置于网络安全战略的前线？

OPSWAT.

保护全球关键基础设施

在过去 20 多年里，OPSWAT 作为 IT、OT 和 ICS 关键基础设施网络安全的全球领导者，不断发展端到端解决方案平台，为涵盖金融服务、国防、制造、能源、航空航天、交通系统的公共部门组织及私营企业，提供保护其复杂网络免受威胁所需的关键优势。

OPSWAT 秉持“信任零文件，信任零设备™ (Trust no file. Trust no device.™)”的理念，通过零信任解决方案和专利技术，解决客户在硬件扫描、数据与文件传输以及设备访问安全方面的挑战，覆盖其基础设施的各个层级。全球1,900+家关键基础设施相关的企业、政府和机构信任OPSWAT，借助其技术保护设备、文件、网络免受已知与未知威胁、零日攻击和恶意软件的侵害，确保符合行业和政府制定的政策与法规。

Cyberworld
科明大同

中国区
总代理

公司网站 www.cyberworld.com.cn
业务联系 info@cyberworldchina.com
售后支持 support@cyberworldchina.com



关注公众号