METADEFENDER

# OT Access

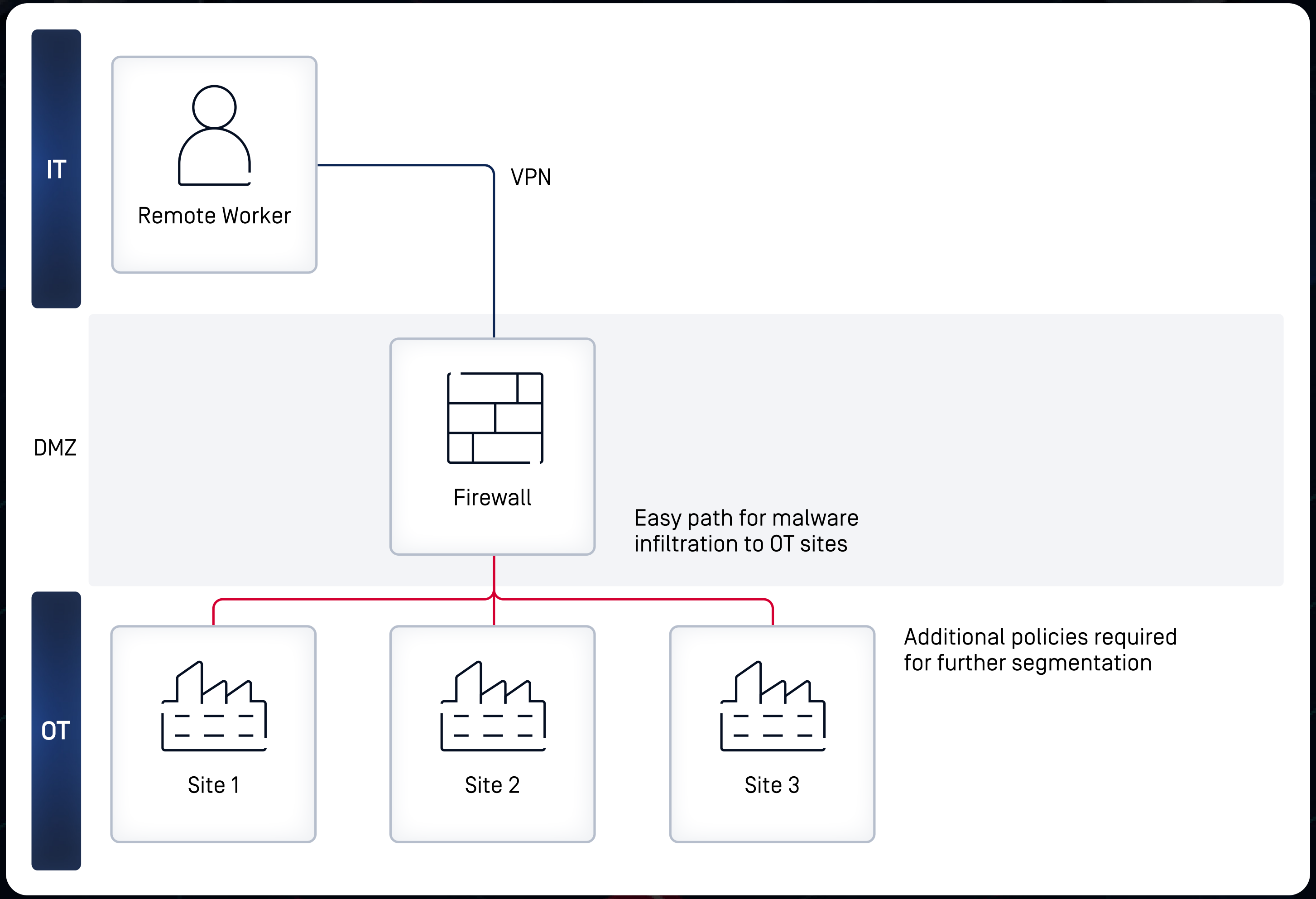
## Granular & Secure Remote Access for OT & CPS Environments

Protect your secure environments with zero-trust, line-of-sight remote access that eliminates lateral movement risks and enables safe collaboration.

Protecting the World's Critical Infrastructure

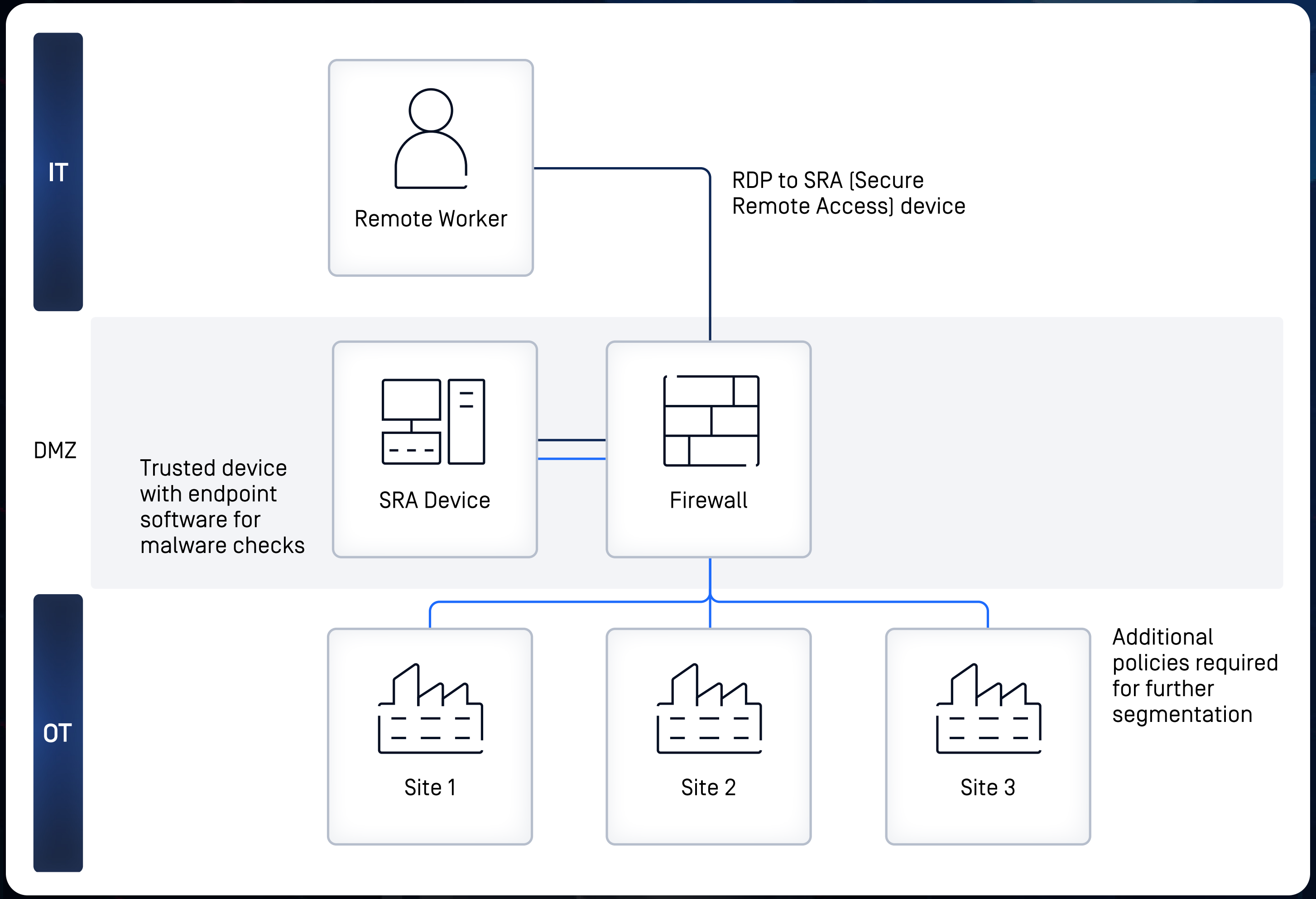
# The Challenge

Traditional VPNs and jump servers provide broad network access, exposing OT (operational technology) to cyber risks and compliance gaps. Vendors, contractors, and engineers often gain more visibility than needed, leaving industrial systems vulnerable.


IT
Remote Worker
VPN
DMZ
Firewall
Easy path for malware infiltration to OT sites
OT
Site 1
Site 2
Site 3
Additional policies required for further segmentation

# The Solution

MetaDefender OT Access delivers a purpose-built secure remote access solution for OT & CPS (cyber-physical systems) critical infrastructure. With granular, protocol-specific control and outbound-only tunnels, MetaDefender OT Access ensures engineers, vendors, and administrators access only what they need, and nothing more.


IT
Remote Worker
RDP to SRA (Secure Remote Access) device
DMZ
Trusted device with endpoint software for malware checks
SRA Device
Firewall
OT
Site 1
Site 2
Site 3
Additional policies required for further segmentation

# Key Features

### Line-of-Sight Access

Users connect only to assigned OT assets, without seeing or scanning the broader network.

### Granular Access Control

Define access by protocol, user, seat, endpoint, or activity.

### Outbound-Only TLS Tunnels

Secure, mutually authenticated connections—no inbound firewall changes required.

### Secure File Transfer

Integrated with MetaDefender Managed File Transfer, MetaDefender Core, and MetaDefender Cloud for file scanning and policy enforcement.

### Live Session Monitoring & Recording

Real-time visibility, termination, and compliance reporting.

### Rapid Deployment

Pre-configured appliance installs in under a day; no additional agents or jump servers needed.

### Scalability at Enterprise Level

Proven deployment at 70+ sites, supporting 900+ users with unified access management.

# Benefits

### Eliminate Lateral Movement

Prevent unauthorized traversal across OT networks.

### Zero-Trust Enforcement

Provide *least privilege* access by design.

### Operational Continuity

Allow secure maintenance, patching, and troubleshooting without disrupting production.

### Faster Vendor Collaboration

Give external vendors controlled, auditable access without opening the network.

### Compliance Ready

Align with IEC 62443, NERC CIP, and industry cybersecurity standards.

### Visibility & Auditability

Centralized logs, Splunk/syslog integration, and session forensics.

USE CASE

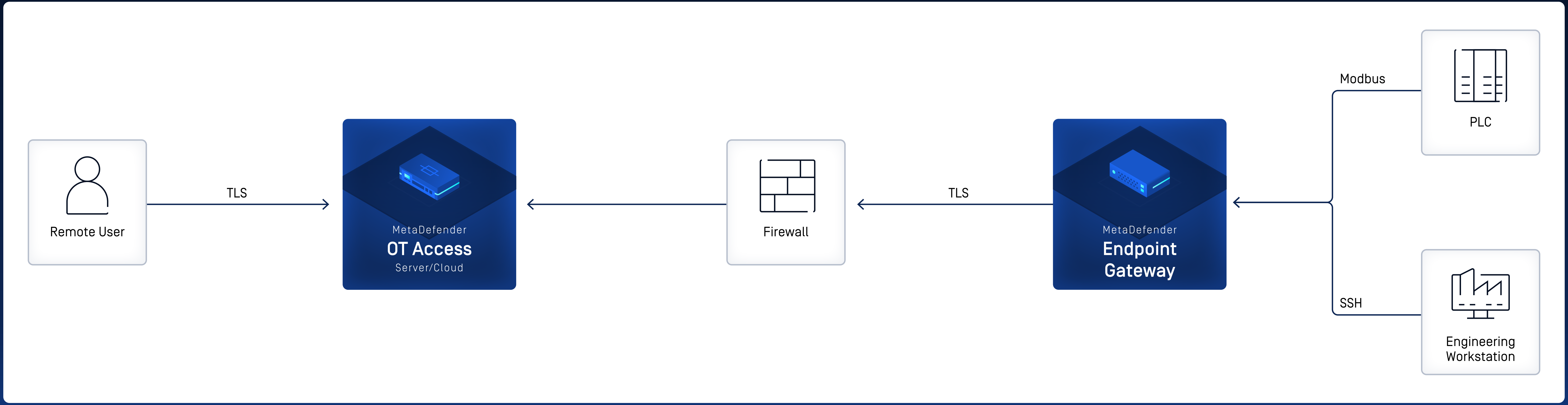
# Read-Only Native Secure Remote Access to a Modbus PLC Placed in the OT Facility

## Challenge

A water treatment plant needs to remotely monitor pH values, which are managed by a Modbus PLC within the facility. To enable this, secure remote access must be provided to the responsible personnel, while ensuring that any modifications—whether accidental or malicious—to the PLC values are prevented, as they could have extremely dangerous consequences.

## Solution

MetaDefender OT Access provides secure remote access to the responsible personnel. They can remotely access the Modbus PLC using the native Modbus protocol. To ensure security, a policy is configured that allows the remote user to read PLC registers only, with no ability to write or modify them under any circumstance.



OPSWAT.

USE CASE

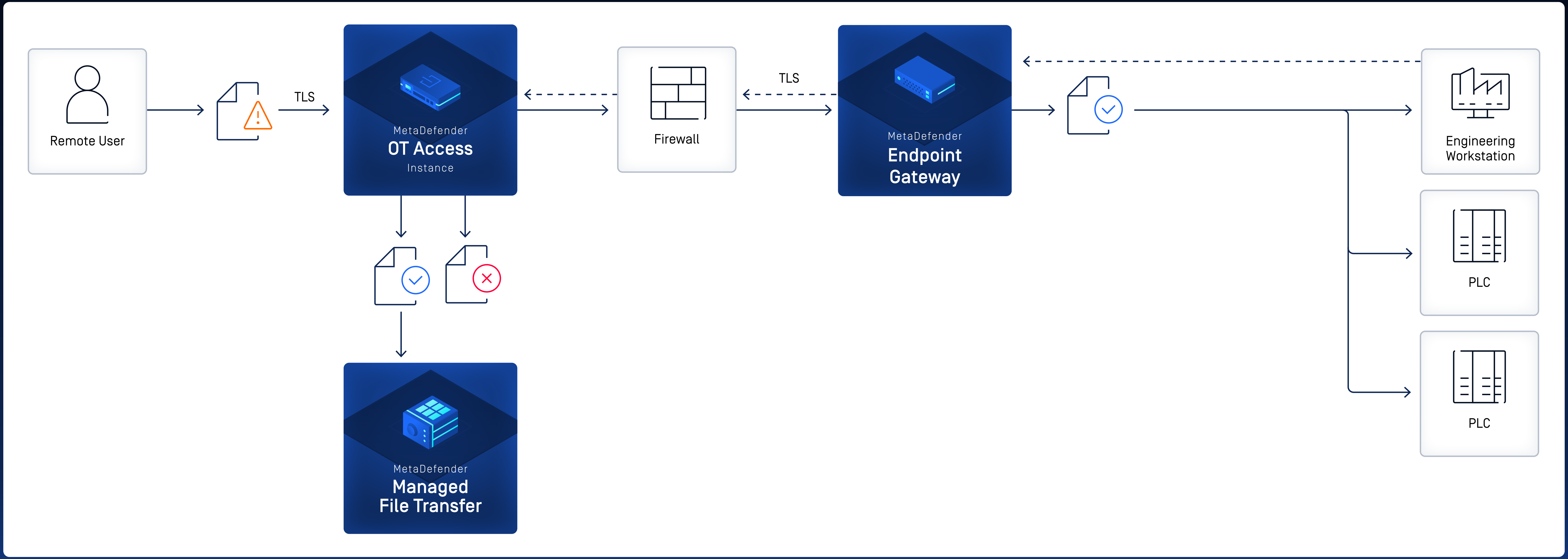
# Secure File Transfer for OT Networks

## Challenge

Remote workers and vendors often need to upload configuration files, firmware, or reports into OT networks. Standard transfer methods bypass scanning, exposing OT environments to malware and corrupted files.

## Solution

MetaDefender OT Access integrates seamlessly with MetaDefender Managed File Transfer, enforcing secure file transfers directly into OT. All files are scanned, sanitized, and policy-checked before delivery, ensuring safe transfer across IT/OT boundaries.



USE CASE

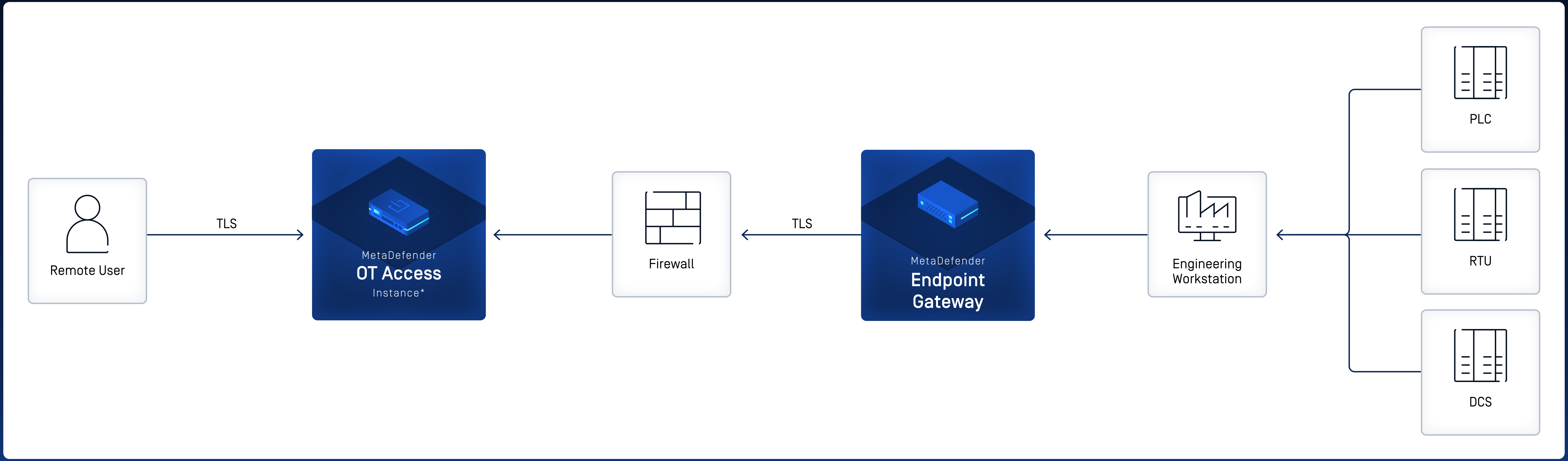
# Emergency Patching & Secure Update in Oil Refinery

## Challenge

An Oil & Gas company needs to remotely access an engineering workstation on an oil rig for emergency patching and secure updates. This access must be robust and adhere to Zero Trust security principles, incorporating MFA and real-time session monitoring.

## Solution

MetaDefender OT Access can be deployed to provide secure remote access to the engineering workstation via the RDP protocol. All sessions require MFA, and MetaDefender Endpoint ensures that the accessing device complies with company security policies. During access, the oil rig supervisor can monitor the RDP session live to prevent any restricted actions and can terminate the session if necessary.



USE CASE

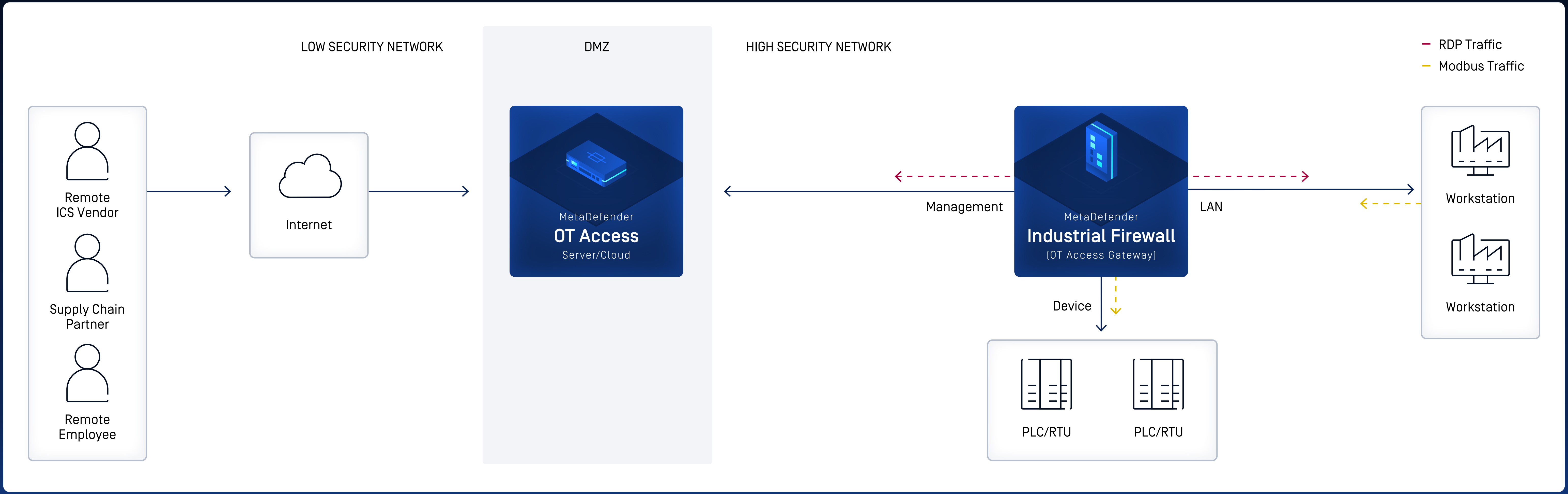
# Secure Remote Access Through Industrial Firewall to Have a Last Line of Defense for Critical Systems

## Challenge

A manufacturing company needs to provide some of their internal users with remote access to two different facilities and one of these Is particularly sensitive to malicious attacks and/or misuse of the OT systems, so it needs an extra layer of security.

## Solution

MetaDefender Industrial Firewall integration with MetaDefender OT Access enables Secure Remote Access while acting as a last line of defense against misconfigurations, malicious misuse, zero-day threats and DoS and DDoS attacks.



# Customer Story

A global consumer goods leader deployed MetaDefender OT Access across 70+ facilities, managing over 900 users. The deployment was completed in less than a day per site, without changes to firewalls. As a result, they gained full visibility and control over third-party vendors while eliminating lateral movement risks.

> “We now have complete visibility into who’s accessing what, when, why, and how—all while supporting our teams and OEM partners with the secure access they need to keep our production lines running smoothly.

**Chief Information Security Officer**

# Purpose-Built for Your Environment

Discover how MetaDefender OT Access can mature your cybersecurity posture.

Scan the QR code to connect with an expert today.

opswat.com/get-started
sales@opswat.com

OPSWAT.

Protecting the World's Critical Infrastructure

For over 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,900 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.