OPSWAT.

DATASHEET

METADEFENDER™

OT Access

Industrial Secure Remote Access

Establish Granular Visibility and Control Down to the Asset, Protocol, and User

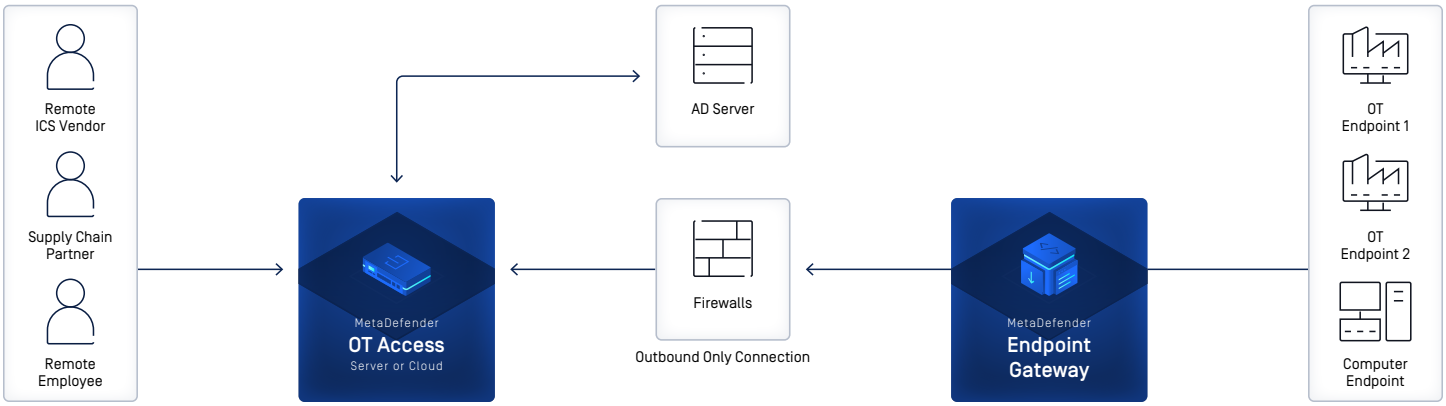
VPNs are typically the go-to solution for IT to provide remote access, but they're not designed for OT environments. With VPNs, it is all or nothing. Once a user gains access, they can see and inspect any asset on the OT network without supervision, and there is no way to terminate the session should something go wrong. OPSWAT's MetaDefender IT-OT Access solution eliminates this risk.

It enforces a logical line-of-sight protection model where users can only access what they are authorized to see across their connection and nothing else.

One Platform to Secure All Remote Access to Industrial Assets

Say goodbye to managing multiple remote access platforms, and lengthy user onboarding processes. MetaDefender IT-OT Access delivers secure remote access to all third parties, OEM, and remote users through one centralized platform, without the gaps that traditionally come with VPN solutions. More importantly, it significantly reduces the attack surface of your operational network—and risks posed by remote users.

There's no simpler way to establish a single, supervised, and secure line-of-sight entry point for remote users that require access to your OT assets.



Key Features

One Secure Solution for All
Simplify remote access with one software solution for all third party, OEM, and remote user access. No hardware required.

Easy Deployment
Set up in less than a day, with far fewer complications compared to standard VPNs.

Flexible Deployment Options
Use our multi-tenant instance for the absolute fastest onboarding experience, or go with a dedicated AWS instance for maximum isolation, reliability, and performance.

Run our software on a VM platform of your choice, or we can send you a 1U rack-mountable appliance with the software pre-installed.

Seamless Integration
Natively integrate with Microsoft Active Directory for seamless authentication of users and groups, including employees, third-party suppliers, contractors, and industrial equipment manufacturers.

Deep Packet Inspection
Monitor session duration, provide read/write/program level policies, and instantly block any user or session that violates a policy.

Granular Access
Customize access of every session down to the protocol, user activity, and role to ensure OT assets and network are not remotely manipulated outside the line of sight.

Best-in-Class Device Posture Checks
Ensure that any device granted remote access to your OT environment complies with your organization's security policies using OPSWAT's industry leading OESIS framework.

Secure Password Sharing
Keep passwords hidden from users without restricting access with 2-factor authentication.

No Firewall Compromises
Connect through a fully-encrypted, outbound-only TLS service registration tunnel without any firewall reconfiguration. No risk of pre-auth attacks, which are common for VPNs recently.

Continuous Monitoring
Supervise, enforce (policies), or terminate any session instantly.

Session Recording
Every session is thoroughly logged for compliance (syslog) and auditability (syslog and RDP session recordings).

Feature	METADEFENDER OT Access	VPNs
Native OT protocol controls	✓ Including deep packet inspections	✗
Connection origination	Outbound only via TLS from site to server	Inbound through perimeter firewall
Permission type	Granular single-user to single-user	Course Single-user to whole-network

Native Policy Controls	Read-Only	Read-Write	No SQL Inject	No XSS
FINS	✓	✓	✗	✗
Modbus	✓	✓	✗	✗
OPCUA	✓	✓	✗	✗
S7	✓	✓	✗	✗
SLMP	✓	✓	✗	✗
RDP	✗	✗	✗	✗
Ethernet IP	✗	✗	✗	✗
VNC	✗	✗	✗	✗
HTTP(S)	✗	✗	✓	✓
ssh	✗	✗	✗	✗
telnet	✗	✗	✗	✗

OPSWAT.
Protecting the World's Critical Infrastructure