OPSWAT.

DATASHEET

MetaAccess OT™

Industrial-grade secure remote access for OT assets

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

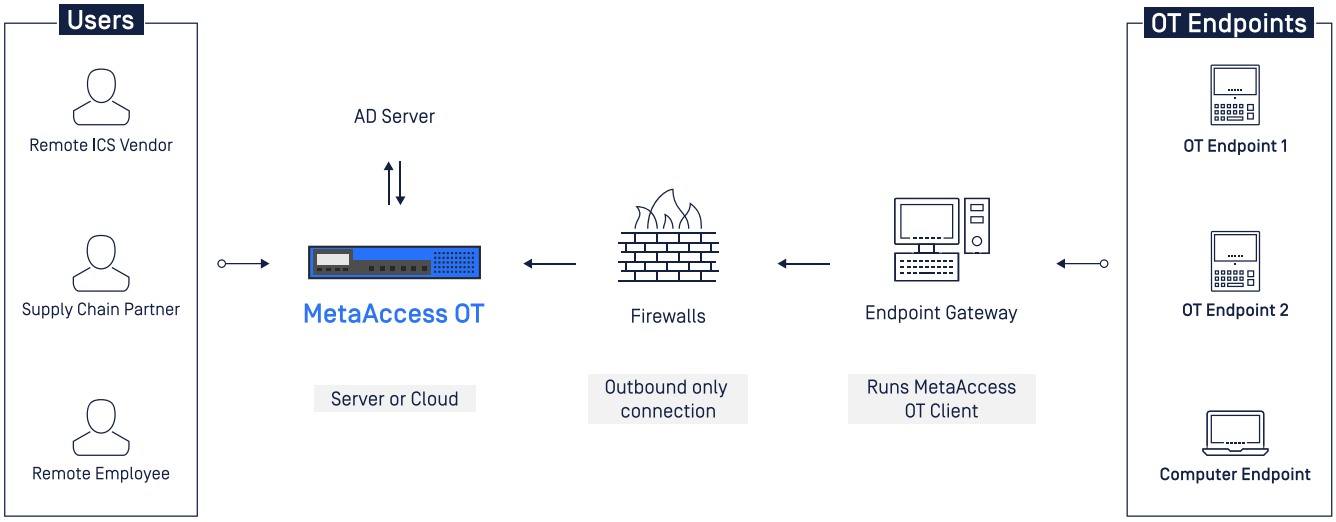
VPNs are typically the go-to solution for IT to provide remote access, but they're not designed for OT environments. With VPNs, it is all or nothing. Once a user gains access, they can see and inspect any asset on the OT network without supervision, and there is no way to terminate the session should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

OPSWAT MetaAccess OT 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. MetaAccess OT 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.



OPSWAT.

MetaAccess OT™

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.

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.

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.

Deep packet inspection

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

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 (RDP).

Private cloud or on-prem deployment options

Go with a customer-dedicated AWS instance for maximum reliability, uptime, and performance. Or a standard 1U server (or VM) on-premises with separate management and administration interfaces.

Pay-as-you-go flexibility

Lower TCO with a flexible pricing model that scales with your business based on the number of concurrent users and endpoint servers.

Solution comparison

Feature	MetaAccess OT	Software-defined networking tools	VPNs
Native OT protocol support	Yes, including deep packet inspection	Port-level only	None
Session origination	Outbound only via TLS from customer to policy engine	Inbound or outbound, depending on product and vendor	Inbound through to perimeter firewalls
Session types	Highly granular single-user-to-single-service permissions	User-to-network permission defaults	Network-to-network permission defaults
Local use or AD users/groups	Yes	Yes	Yes

Native policy controls

	FINS	Modbus	OPCUA	S7	SLMP	RDP	Ethernet IP	VNC	HTTP HTTPS	sftp	ssh	telnet
Read-only	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓
Read-write	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓
No SQL injection	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
No XSS	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓

OPSWAT.

Protecting the World's Critical Infrastructure