




OPSWAT.

NetWall

OT Cybersecurity That No  
Firewall Can Match



# Security Gateway Solutions Powering Risk-Free IT-OT Communications

The once clear distinction between information technology (IT) and operational technology (OT) systems, processes, and people is becoming blurred. Conventional airgaps between OT and IT network segments have eroded due to increased corporate demand for connectivity and data analytics from industrial environments.

This increased demand for connectivity exposes industrial assets to targeted cyberattacks because firewalls and next-generation firewalls are inherently bi-directional. They rely on software-based policies and are prone to misconfiguration that threat actors can exploit.

OPSWAT NetWall Security Gateways provide access to real-time OT data and enable secure data transfer to the OT environment without compromising the security and integrity of your critical production systems.

# NetWall USG

## [Unidirectional Security Gateway]

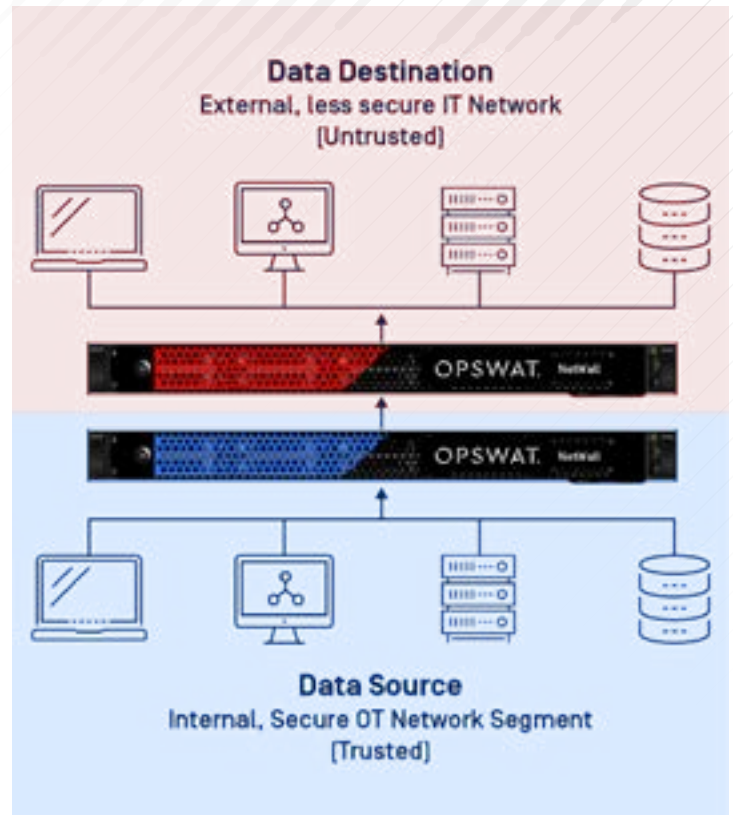
OPSWAT NetWall USG provides access to real-time OT data and enables secure IT-OT data transfers—with the full benefit of speed, low latency, and functionality—and with complete reliability and no data loss. Since no return-path networking is possible, OPSWAT NetWall USG assures real-time operations data can be sent to the corporate network users without the risk of introducing security threats to protected OT networks.

# NetWall BSG

## [Bilateral Security Gateway]

In addition to all the capabilities of NetWall USG, NetWall BSG supports applications such as Historians and SQL database servers that require a data response in order to operate. OPSWAT BSG performs real-time replication of the data [with no data loss] and uses a patented bilateral mechanism to handle “ack” responses without compromising the security and integrity of the OT network.

When a TCP connection is initiated from the trusted network to a destination in the untrusted network, OPSWAT NetWall BSG performs a full protocol break. The protocol break allows select applications from the destination to return a data response to the OPSWAT BSG appliance, however, no connection may be initiated from the untrusted network, ensuring the communication channel cannot be exploited.



OPSWAT NetWall USG comprises a pair of pre-configured appliances with a non-networked serial cable between them that permits unidirectional data flows from OT assets and applications to stakeholders in external IT network.

## Compelling Benefits

- Bring real-time OT data to business users without disrupting their work procedures
- Eliminate the risk of cyber threats entering your protected OT network
- Transport files, database/server replications without proprietary vendor HW and SW
- Guarantee payload delivery with no data loss and no need for data retransmission
- Eliminate complicated firewall audit/configuration projects and risky backdoor channels to the OT network
- Easy to deploy. Scale as needed with field-upgrade software license keys

# Focus on Maximum Security and Reliability

## OPSWAT NetWall versus Firewall, Router rules, VLANs

Unlike firewalls, routers and VLANs, OPSWAT Network Security Gateways enforce true unidirectional communications, with no possibility of routable connections to the protected OT network domain.

Feature	OPSWAT NetWall	Networking Solutions
Routing configuration	✓	✓
Protocol break, completely removed from TCP/IP connection	✓	✗
Meets functional requirements of data diodes (NetWall USG)	✓	✗
Guaranteed delivery with non-repudiable data movement	✓	✗
No complex rule-building	✓	✗
Guaranteed prevention of malware propagation	✓	✗
No ARP, BGP, TCP/IP handshake	✓	✗

## OPSWAT NetWall versus Hardware Data Diodes

Unlike data diodes, OPSWAT Network Security Gateways guarantee reliable data replication and guaranteed data delivery with no data loss, no overruns, and no sync issues.

Feature	NetWall	Data Diodes
Unidirectional Gateway (NetWall USG)	✓	✓
Complete protocol break	✓	✓
Supports all industrial protocols without vendor HW and SW	✓	✓
Guaranteed data delivery	✓	✗
Efficient data synchronization and replication	✓	✗
Improved throughput (reduced repeat transmissions)	✓	✗
Same hardware scales from 50 Mbit/sec to 1Gbit/sec (in BSG); and to 10 Gbit/sec (in USG)	✓	✗
Hardware dongle for admin access	✓	✗
Fast and easy to deploy	✓	✗
Cost effective with competitive subscription options	✓	✗

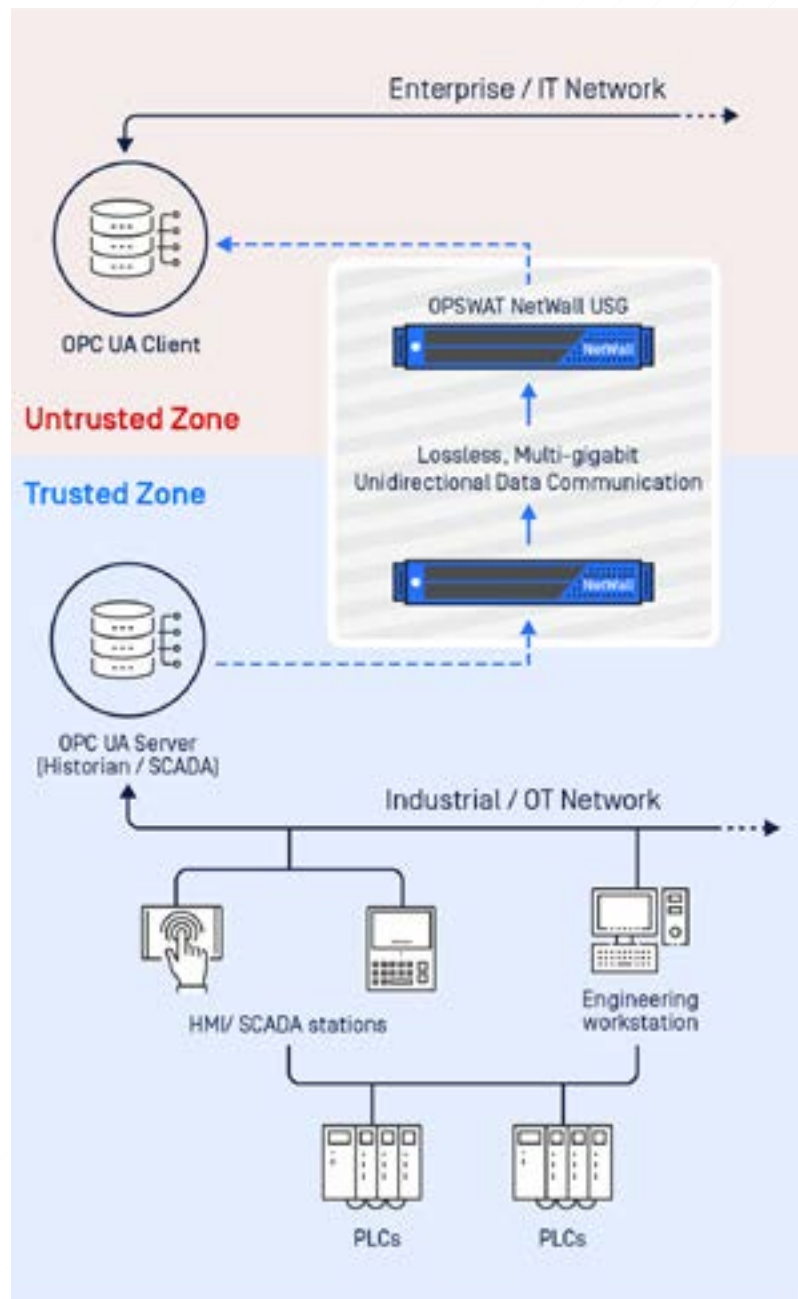


# OT Cybersecurity That No Firewall Can Match

Deployed as a pair of preconfigured appliances, OPSWAT NetWall Security Gateways enable secure communication from protected OT domains to external corporate users. The transmitting appliance is connected exclusively to the protected OT network, while the receiving appliance is connected exclusively to the external IT network. A non-networked serial cable between the two permits unidirectional data flows from OT assets and applications to stakeholders in the external IT network. Return path data flows to the protected network are impossible. OPSWAT NetWall is an ideal solution for a number of OT cybersecurity use cases:

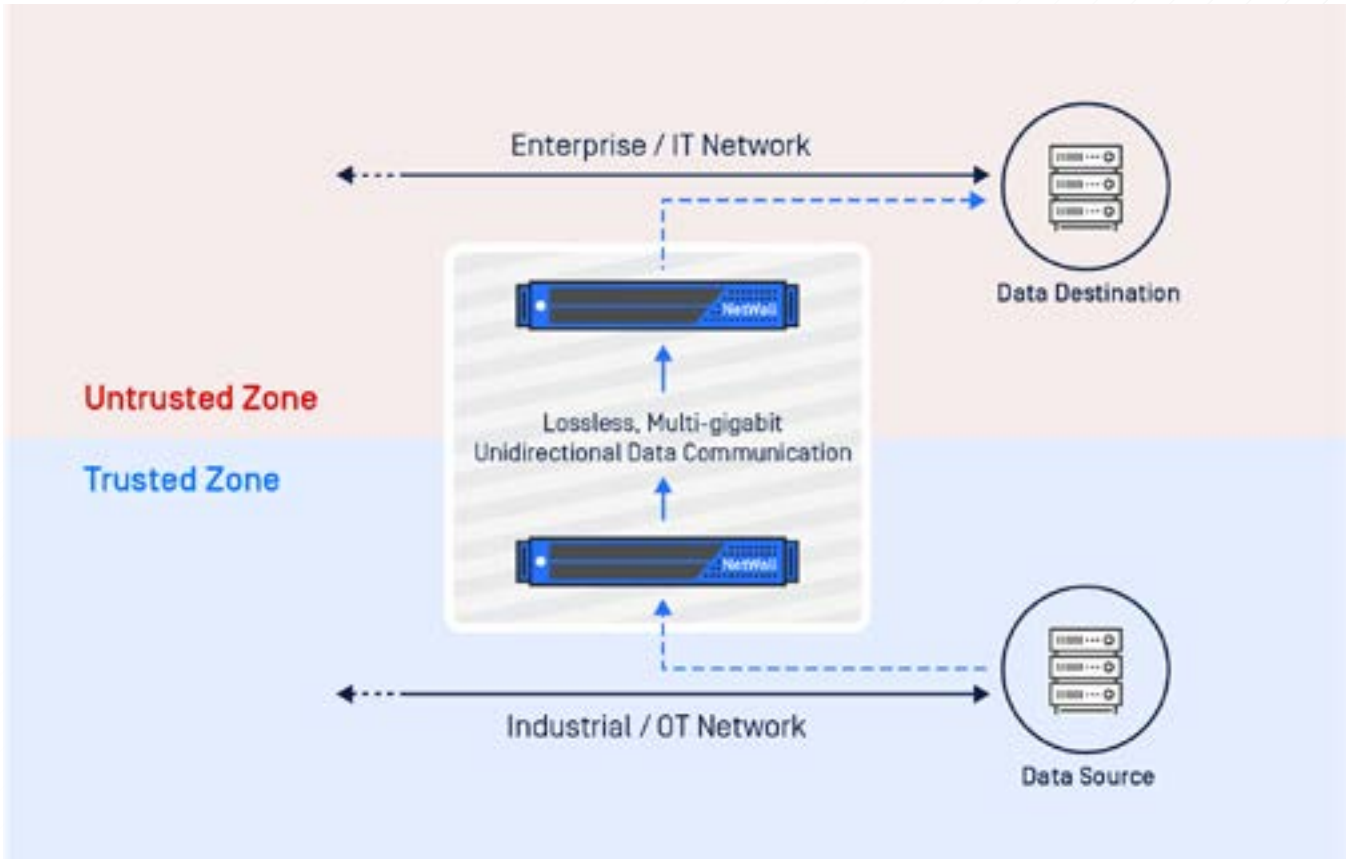
## Use Case: OPC UA Server Replication

In the protected network domain, the OPSWAT NetWall transmitting server listens via filtered ports on its local network interface for incoming data from the OPC UA server. As activity is received, it is disassembled, the payload and connection metadata are delivered to the receiving OPSWAT NetWall OPC UA server in the corporate network domain. The OPSWAT NetWall OPC UA server assimilates the data and makes it available to customer OPC UA clients in the corporate network domain. The replication process is transparent both to external users and to the OPC UA server. Corporate users access the replica just as they would the OT native server. No need to learn new processes or procedures.



## Use Case: Fast and Secure File Transfer

One-way file transfer assures file delivery quickly and guarantees file integrity. OPSWAT NetWall supports FTP, Windows File Share and most file transfer tools as well as Active/Passive transfer modes, ASCII/Binary transfer types and selective file/folder replication. Use OPSWAT NetWall USG to replicate OT data and to enforce one-way communication in real-time. Any attempt at two-way sessions or back-channel access are stopped at the industrial network perimeter.

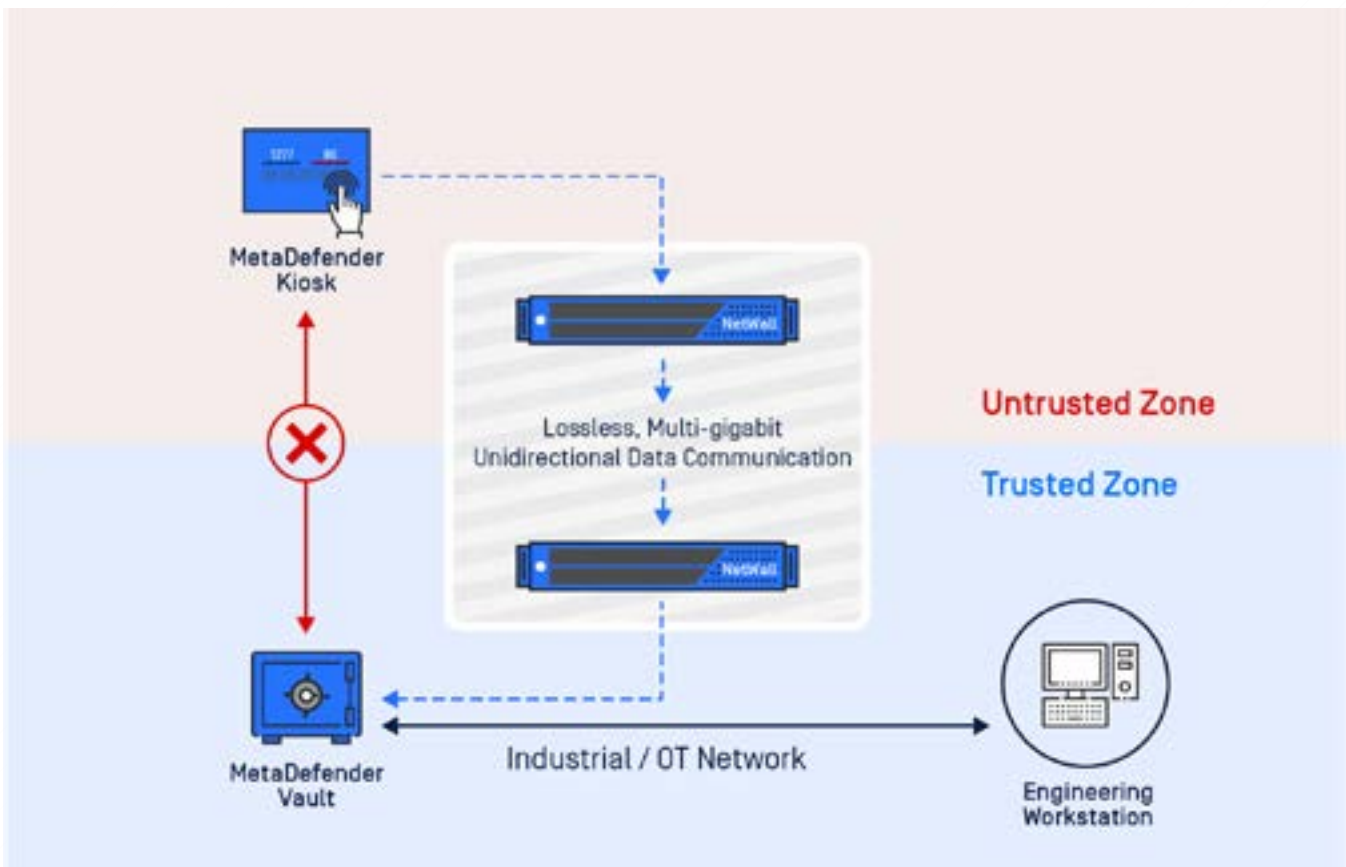


## Use Case: No-Risk Transfer from Kiosk to Vault

The convenience of portable and removable media have made them popular methods for transferring files into and out of a networked environment. Since this practice is fraught with risk, it has given rise to digital security guards – or kiosks – that inspect portable media for malware, vulnerabilities, and sensitive data, before allowing them into the OT environment. Kiosks typically employ a “vault” or secure file storage and retrieval solution that provides a multi-tiered approval process and detailed audit log for data transfers within the organization.

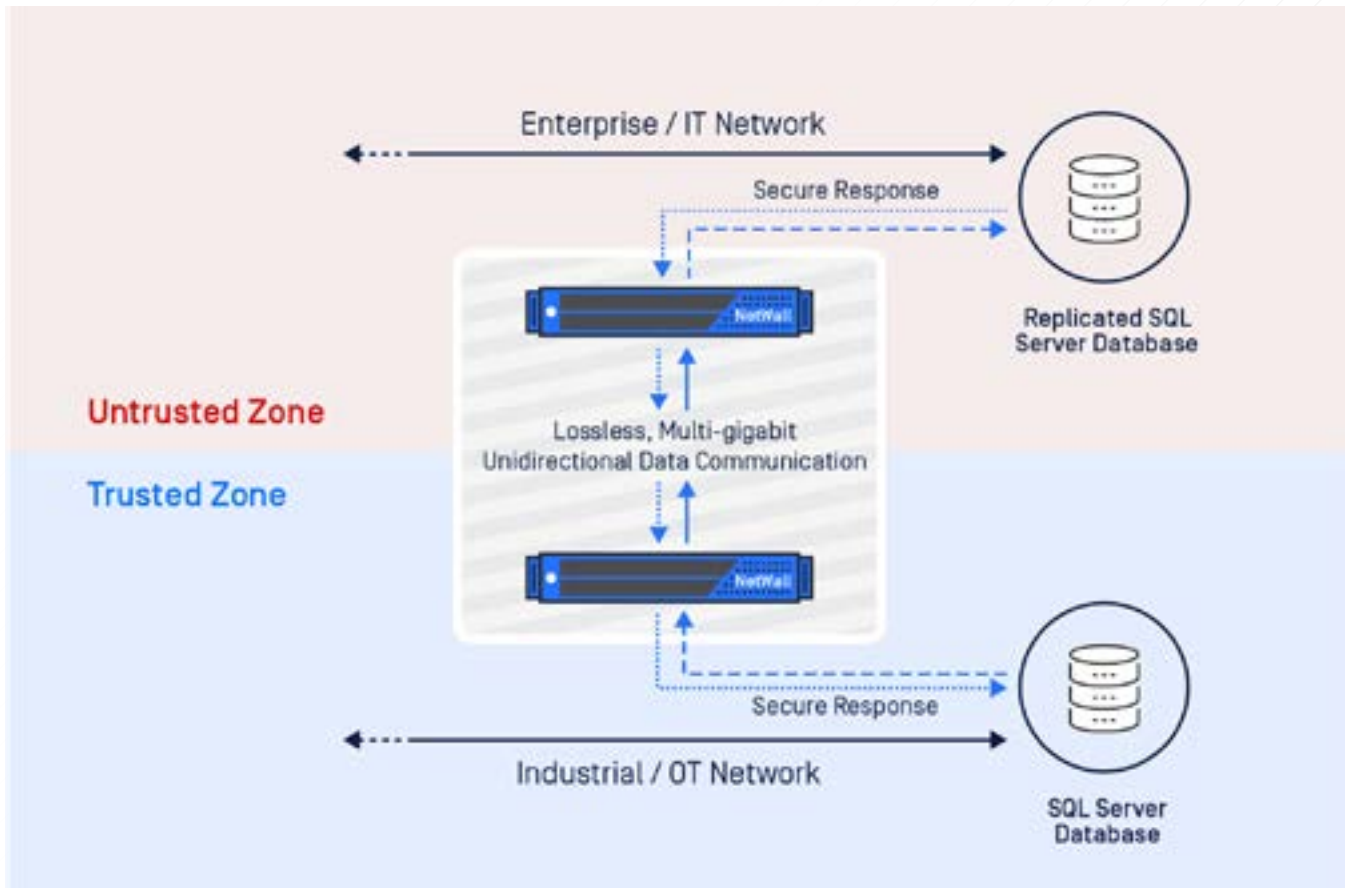
In this case, use OPSWAT NetWall USG to enforce one-way file delivery from kiosk to vault, assuring secure transfer of files and data into your production environment. Working together with Kiosk and Vault solutions to eliminate risk, OPSWAT NetWall USG enables quick and secure delivery of patches, signatures and other product updates to the OT assets that need them.

OPSWAT NetWall Security Gateways are seamlessly integrated with OPSWAT Metadefender Kiosk and Metadefender Vault solutions, providing end-to-end security for IT-OT convergence.



## Use Case: SQL Server Replication

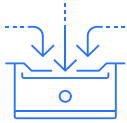
When access to SQL databases is required, OPSWAT NetWall Bilateral Security Gateway employs Microsoft's standard transactional replication services, so there is no need for complicated scripting, custom installation, or modification of the SQL environment. Standard buffering takes over if the connection is temporarily lost. OPSWAT maintains Microsoft replication constraints and does not introduce any additional requirements. SQL server replication is transparent to users so there is no need to change the way they work. It doesn't get much easier than this.



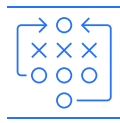
Transfer from Source to Destination is configured in the NetWall USG, using console software and USB dongle.



# Key Features



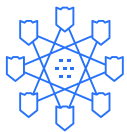
**Guaranteed Payload Delivery**  
with absolutely no data loss.



**Anti-Overrun**  
control eliminates data overflow, retransmissions, and sync issues.



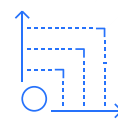
**No Return Path**  
one-way data flows are enforced by a non-networked serial connection between the NetWall server pair. The bilateral support mechanism in NetWall BSG permits data replies ("acks") while enforcing full protocol break and physical isolation.



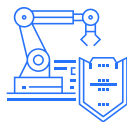
**Easy deployment**  
Preconfigured platform deploys quickly, seamlessly.



**Simple setup**  
Ready for use in minutes after one-time initial setup. No firewall audit or configuration needed.



**Simple scalability**  
Choose 50Mbit/sec, 100Mbit/sec, 1Gbit/sec or 10Gbit/sec throughput - all software selectable.



**Full support for industrial protocols**  
including OPC DA, A&E, and UA, plus Modbus/TCP, file transfers, and TCP/UDP sockets



**Transparent to users**  
Fast and high-fidelity data replication means there is no need to alter work procedures of corporate users.



**Fulfills regulatory compliance**  
for many requirements of Industrial Cyber Security standards, including NERC CIP, NIST CSF, NIST 800-82, NIST 800-53, NIST ICS, IEC 62443, NRC 5.71, CFATS, ISO 27001/ 27032 / 27103, ANSSI, IIC SF, and more. Protects against Industrial attack techniques outlined by MITRE ATT&CK for ICS.

## Don't Compromise on Security for OT-IT Communications

Contact us at [sales-inquiry@opswat.com](mailto:sales-inquiry@opswat.com) to set up a personal demo and let us show you how OPSWAT NetWall Security Gateways can power secure and reliable IT/OT communications in your industrial enterprise.

Trusted by over 1,500 enterprises and government organizations worldwide. OPSWAT protects critical infrastructure. Our goal is to eliminate malware and zero-day attacks. We believe that every file and every device pose a threat. Threats must be addressed at all locations at all times—at entries, at exits, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access. The result is productive systems that minimize risks of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.

©2022 OPSWAT, Inc. All rights reserved.

OPSWAT, MetaDefender, the OPSWAT Logo, the O Logo, Trust no file, Trust no device. are trademarks of OPSWAT, Inc. Revised 2022-Jan-10

**OPSWAT.**

Trust no file. Trust no device.

[OPSWAT.com](https://www.opswat.com)