OPSWAT.
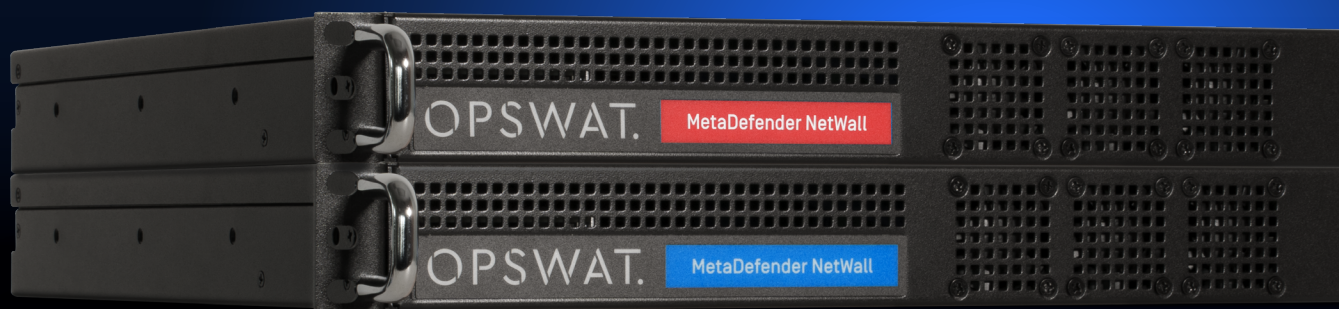
NetWall™ Series

FOR ASPENTECH IP.21

MetaDefender Bilateral Security Gateway shown

Secure Replication of AspenTech IP.21

AspenTech, a world leader in industrial historians with its widely adopted Aspen InfoPlus.21® (IP.21), enables organizations across critical infrastructure to capture and leverage sensor-based data for improved efficiency. IP.21 enables organizations to collect, store, and retrieve time-series data and make it accessible for analysis and reporting.

MetaDefender Bilateral Security Gateway takes a proactive stance against cyberthreats, securing critical systems while ensuring IP.21 data is accurately replicated and available to key stakeholders for reporting and analysis. By seamlessly integrating with existing infrastructure, Bilateral Security Gateway preserves the security of operational data while facilitating collaboration between IT and OT domains, keeping critical systems impervious to malicious attacks, malware, and unauthorized access attempts.

By leveraging cutting-edge technologies and industry-leading best practices, MetaDefender Bilateral Security Gateway sets a new standard for secure data transfer. Replication of IP.21 Historian data across Bilateral Security Gateway ensures uninterrupted operations and uncompromising security.

OPSWAT.

Comprehensive Integration

- IP.21 database replication is used to publish schema, historical backfill, and current values from an AspenTech IP.21 server source to an AspenTech IP.21 destination
- Unidirectional transfer of IP.21 records
- No additional 3rd party software connectors
- Supports multiple IP.21 replication methods: Aspen Connect or MSMQ (Microsoft Message Queue)

MetaDefender Bilateral Security Gateway supports real-time replication and transfer of IP.21 historians without compromising the security and integrity of critical production systems and strictly enforces one-way data flows. It also employs a proprietary bilateral mechanism to handle data replies needed by industrial historians hosted in OT environments, which is completely transparent and requires no change to application configurations or work procedures.
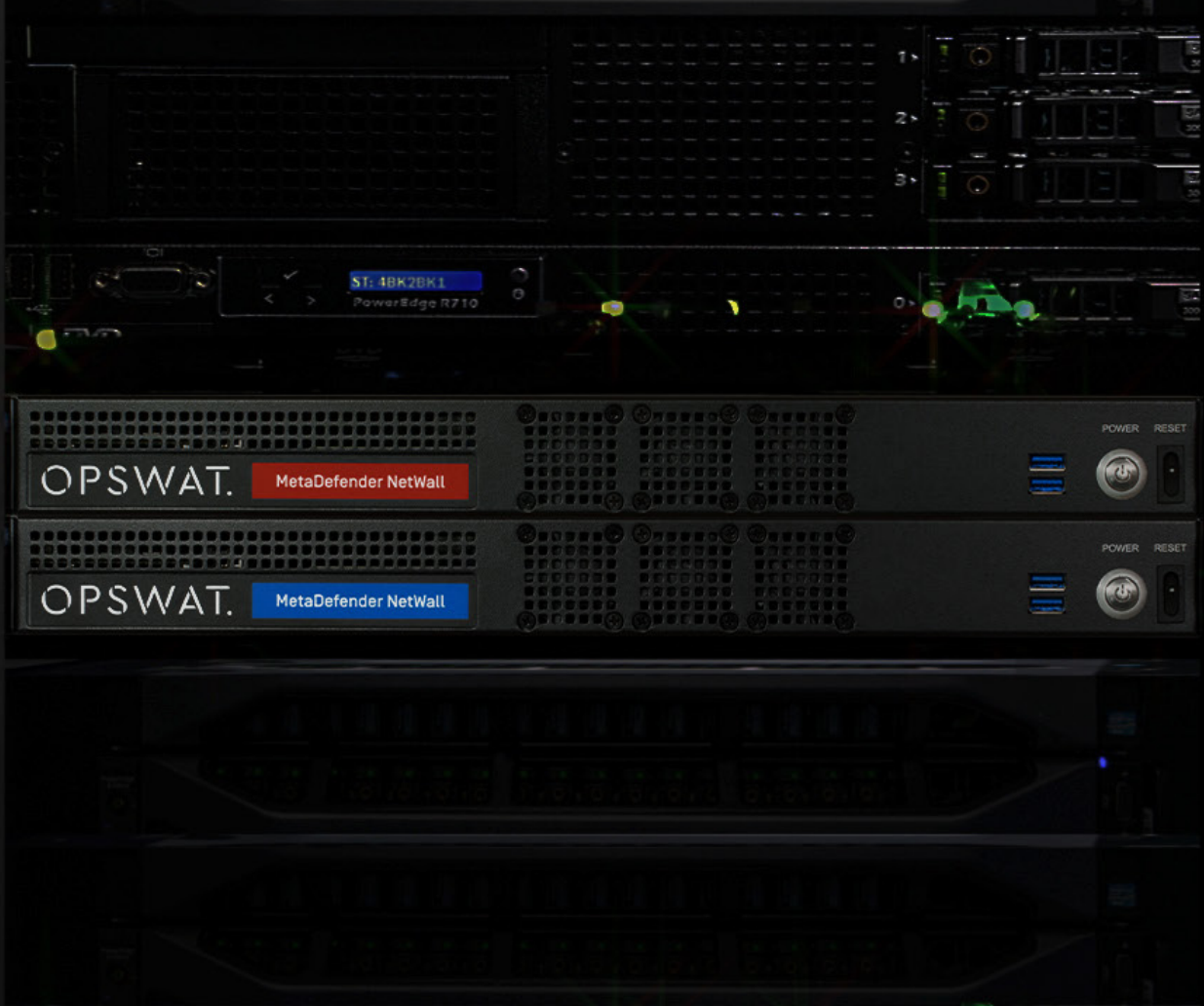
Better Together
AspenTech IP.21 and MetaDefender NetWall

No Return Path	One-way data flows are enforced by a non-networked serial connection between the BSG server pair.
Segmentation	Isolates OT/ICS assets against cyberattacks.
Zero Loss	Guaranteed payload delivery with absolutely no data loss.
Bilateral Support	A unique mechanism permits data replies while enforcing full protocol break and physical isolation.
Easy to Deploy	The preconfigured platform deploys quickly and seamlessly.
Reliability	IP.21 database replication with no database synchronization issues.

Native IP.21 Support

MetaDefender Bilateral Security Gateway for Aspentech IP.21 supports the Aspen Connect product as well as standard IP.21 database replication. Aspen Connect is used to publish data from an Aspentech IP.21 server source to an Aspentech IP.21 destination. IP.21 database replication is used to publish schema, historical backfill, and current values from an Aspentech IP.21 server source to an Aspentech IP.21 destination. The MetaDefender Bilateral Security Gateway is placed between the source and destination IP.21 databases and provides all the security features inherent in the MetaDefender Bilateral Security Gateway. MetaDefender Bilateral Security Gateway is transparent to the Aspentech software applications and does not require customized software.

IP.21 PC Publishers — Air Gap — MetaDefender **Bilateral Security Gateway** — MetaDefender **Bilateral Security Gateway** — IP.21 Enterprise Subscriber

Are you ready for MetaDefender NetWall series to protect your AspenTech IP.21?

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure

For the last 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 1,700 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.