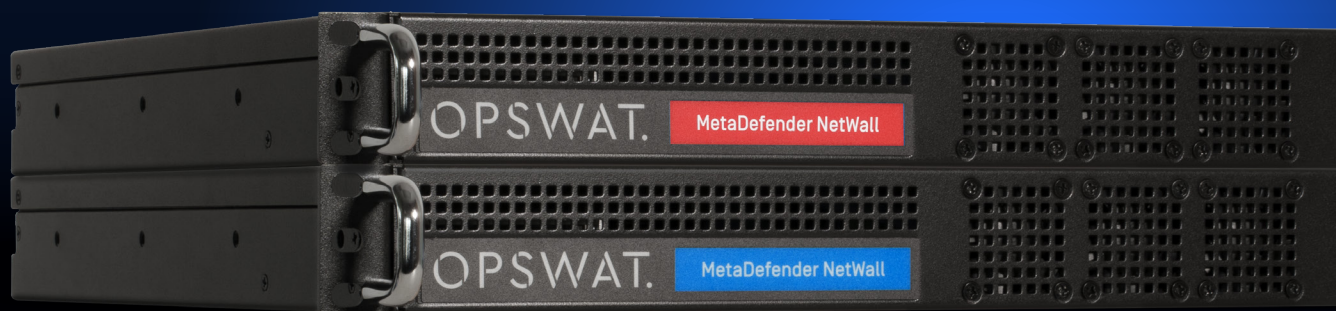


OPSWAT.

METADEFENDER™

# NetWall™ Series

FOR AVEVA PI



MetaDefender Unidirectional Security Gateway shown

## Secure Replication of AVEVA PI Historian

AVEVA, a world leader in historians with its widely adopted PI System, enables organizations across critical infrastructure to capture and leverage sensor-based data for improved efficiency.

MetaDefender Optical Diode and MetaDefender Unidirectional Security Gateway [USG] take a proactive stance against cyberthreats, securing critical systems while ensuring AVEVA PI Historian data is accurately replicated and available to key stakeholders for reporting and analysis. By seamlessly integrating with existing infrastructure,

MetaDefender security gateways preserve 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 NetWall series sets a new standard for secure data transfer. Replication of AVEVA PI Historian data across NetWall ensures uninterrupted operations and uncompromising security.

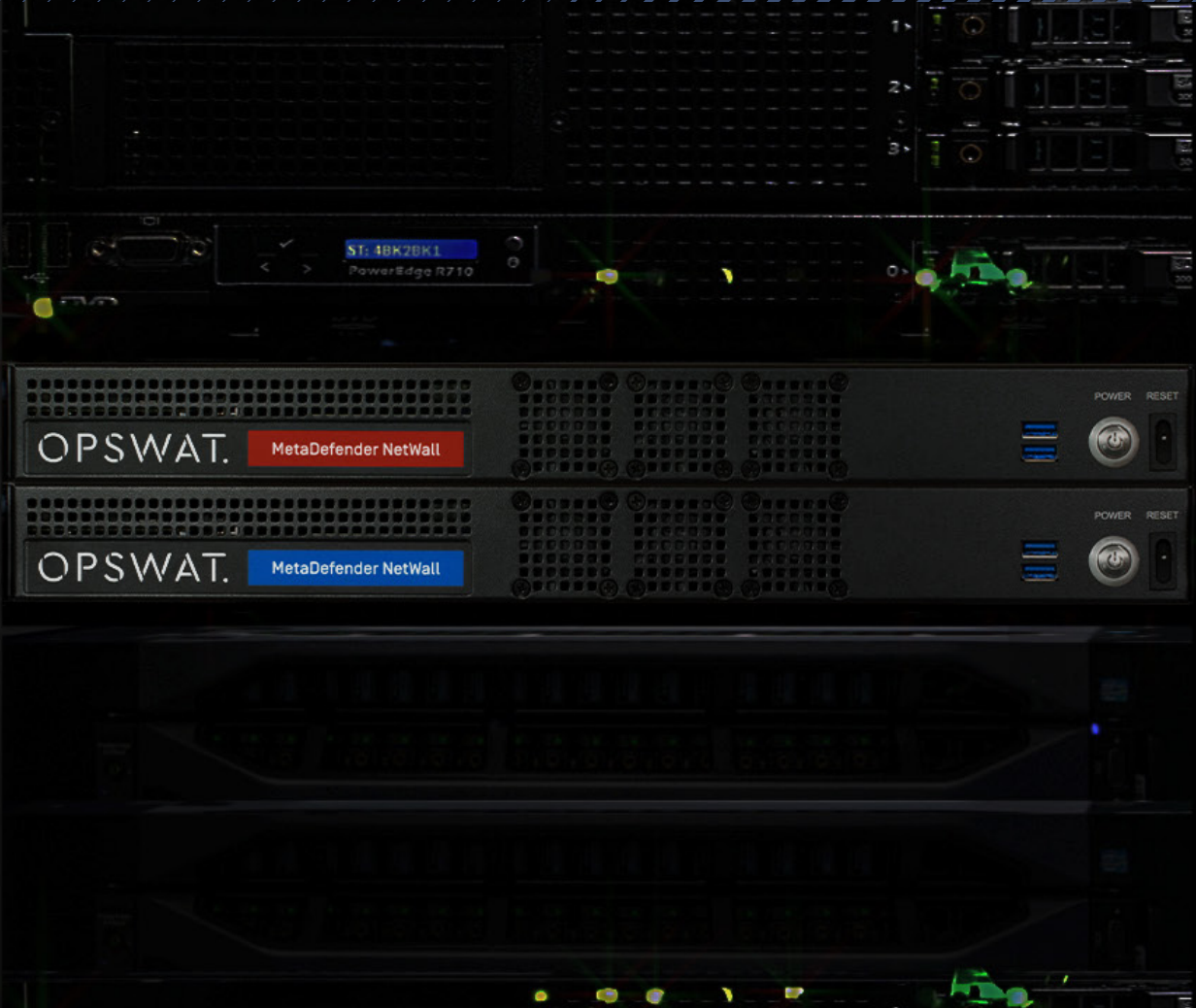
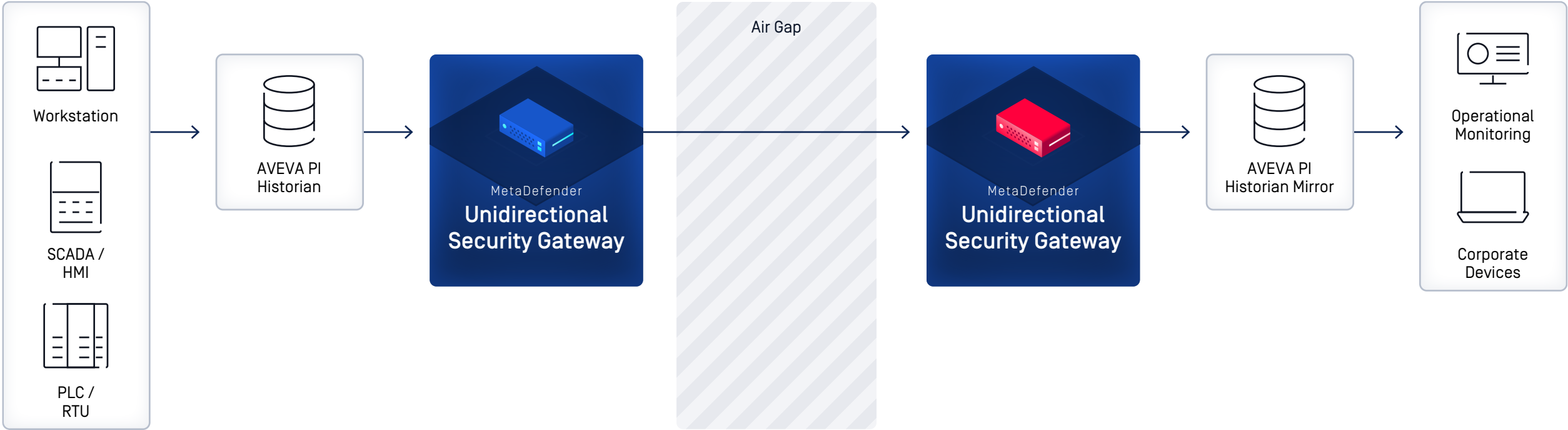
Comprehensive Integration

- Unidirectional transfer of PI records and schema definition with configurable historical backfill operation
- Securely replicate changes to tags (Add/Modify) to replicate PI historian
- Supports PI-to-PI or PI Database Replication and PI Collective Redundancy

With the implementation of MetaDefender USG or MetaDefender Optical Diode for the AVEVA PI System, organizations can better prevent remote cyberattacks from infiltrating their industrial control systems. MetaDefender NetWall series enforces a secure environment while facilitating effortless access to critical operational data across the enterprise and cloud.

Native PI Support

MetaDefender NetWall series for AVEVA PI is a native replication without need for third-party protocol converters running on PI Servers or other systems. MetaDefender NetWall series for AVEVA PI supports many-to-one architectures, Backfill, PI Collectives, events, tags, tag data, and tag attribute replication and synchronization, with options for native High Availability. Additionally, MetaDefender Unidirectional Security Gateway supports the replication of PI Archive.



Better Together

AVEVA PI and MetaDefender NetWall

- |                  |                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Replicate</b> | Secure replication for AVEVA PI Data Archive, PI Backfill, and PI Schema Definitions                                                                                 |
| <b>Protect</b>   | Mitigation of remote-control cyberattacks and online malware propagation                                                                                             |
| <b>Alert</b>     | Simultaneously transfer real-time alarms and diagnostics via Syslog, Windows logs, email, SNMP traps, and log files, for comprehensive monitoring of critical assets |
| <b>Deploy</b>    | The PI connector is easy to deploy with a simple web user interface                                                                                                  |
| <b>Support</b>   | Native protocol support for all PI data types, including numeric, digital, string, and timestamp                                                                     |

GET STARTED

# Are you ready for MetaDefender NetWall series to protect your AVEVA PI Historian?

**Talk to one of our experts today.**

Scan the QR code or visit us at:

[opswat.com/get-started](https://opswat.com/get-started)

[sales@opswat.com](mailto: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](https://www.opswat.com).