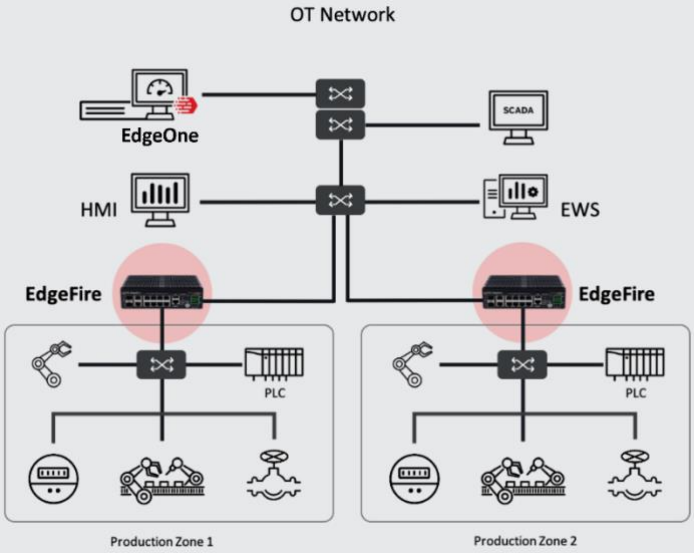
EdgeFire™
Industrial Next Generation Firewall Series

DATASHEET

Inline Threat Defense for Continuous Production Line Operation, Key Asset Protection, and Incident Response

Modernization and interconnection are the keys to this connected world. This revolution bridges the gap between Information Technology (IT) and Operational Technology (OT). Usually, IT and OT technologies operate separately, each with its own respective network, maintenance task force, goals, and needs. Furthermore, the typical OT network connects with a massive number of assets that were not designed for the modern corporate network, and as a result it is extremely difficult to conduct timely updates and patching to maintain protection of critical assets.

EdgeFire, the Next Generation Firewall, enables network segmentation and segregation to divide the network into different zones of control, even down to the cell level. Featuring network access control and network attack prevention for critical assets, the EdgeFire is designed for in-depth cyber defense to streamline OT daily operations.



Benefits

Robust, Resilient Firewall Provides Security, Stability and Convenience

- Segments networks and isolates connectivity both to and between facilities as well as production zones.
- Works excellently as a standalone and synergizes well with our centralized management system “EdgeOne™”.
- Certified industrial-grade hardware with compact size, dual power input, a wide thermal operation range, and durability tailored for industrial cabinet design and OT environments.
- Ruggedized to work well in harsh environments.

Detect and Intercept Threats with Hardware Specially Created to Prevent Worms from Spreading

- Provides immediate and continuous threat protection through flexible deployment options for easy installation and management via the centralized management interface.
- Protects vulnerable unpatched devices and legacy systems.
- Shields your assets against OT exploits with signature-based virtual patching.
- Uses segmentation to create production zones for reducing the damage of mis-operation or cyberattack.

Enable Full Visibility of Your Shadow OT Network

- Operates with a high level of asset visibility using passive asset identification and IT/OT traffic communication within OT networks.
- Minimizes downtime for patching or maintenance.
- Increases Shadow OT visibility.
- Purifies OT network communication.
- Smooth event and traffic monitoring with event log tracing.
- View and query event logs with the built-in log viewer.

Streamline Administration and Policy Deployment with Operational Network Learning

- Streamline network access control, establish security policies, and define your baseline with OT-native machine learning for network behavior.
- Guides users with appropriate settings, inspects ICS protocols in depth, and generates OT network-specific trust lists based on popular protocols.

Key Features

- **OT-Aware Operational Intelligence**

  Our core technology for EdgeFire, TXOne One-Pass DPI for Industry (TXODI™), gives you the ability to create and edit allowlists, enabling interoperability between key nodes and deep analysis of L2-L7 network traffic.

- **Improve Shadow OT Visibility by Integrating IT and OT Networks**

  EdgeFire comes equipped to make your IT and OT networks as integrated and coordinated with each other as possible, and to grant visibility of your shadow OT environment.

- **Signature-Based Virtual Patching**

  Through virtual patching, your network has a powerful, up-to-date first line of defense against known threats. Users have superior control of the patching process, which creates a preemptive defense during incidents, and provides additional protection for legacy systems.

- **Flexible Operation Modes, 'Monitor' & 'Protection'**

  EdgeFire can flexibly switch between 'Monitor' and 'Protection' modes, preserving your productivity while maximizing security.

- **Policy Rule Auto Learning**

  EdgeFire automatically learns network connections based on daily OT operations and generates allowlists, reducing deployment time.

- **Wide Range of Industrial Protocols**

  EdgeFire supports OT protocols including Modbus, Ethernet/IP, CIP, and more, allowing OT and IT security system administrators to collaborate for seamless coordination with existing network architecture.

- **Top Threat Intelligence and Analytics**

  EdgeFire provides advanced protection against unknown threats with its up-to-date threat information. With the cutting-edge research of the Zero Day Initiative (ZDI) vulnerability reward program, EdgeFire offers your systems exclusive protection from undisclosed and zero-day threats.

- **Flexible Segmentation and Isolation**

  EdgeFire is the ideal solution for segmenting your network into easily managed security zones.

- **Secure Remote Connectivity with VPN Solutions**

  EdgeFire can set up IPSec VPN tunnels for the remote OT site to connect back to the operating center for remote management. L2TP/IPSec VPN clients can also connect to EdgeFire for remote OT operation.

- **Centralized Management**

  Pattern updates and firmware management can all be centralized on a large scale. For facilities with massive EdgeFire nodes, the EdgeOne™ helps administer and manage them by group, reducing costs and increasing large-scale efficiency.

EdgeFire™ Specifications

Feature	EdgeFire 1012
Supported IPS Throughput	200Mbps at least (IMIX) / 600Mbps (UDP 1518 bytes)
Latency	<500 microseconds
Concurrent Connection (TCP)	100,000
Supported ICS Protocol	Modbus / EtherNet IP / CIP / FINS / S7Comm/ S7comm+/ TOYOPUC, with more being added regularly
Policy Enforcement Rules	512 Rules (L3 Policy Enforcement Rules in gateway/bridge mode) 256 Rules (L2 Policy Enforcement Rules in bridge mode)
ICS Protocol Filter Profiles	64 Profiles
VPN	Max. concurrent IPSec VPN tunnels: 50 VPN Tunnels Site-to-Site VPN / Client-to-Site VPN Protocol: IPSec (IKEv1, IKEv2), L2TP over IPSec VPN Throughput: 50 Mbps
Form Factor	DIN-rail mounting and wall mounting (with optional kit)
Weight (Standalone Device)	1381g (3.044 lb)
Dimensions (W x D x H)	180mm x 120mm x 50mm (7.09 x 4.72 x 1.97 in)
Network Interface Type	8 x Auto-sensing 10/100/1000 Mbps ports (RJ45 connector) 2 x 100/1000 fiber optic ports and 2 x Auto-sensing 10/100/1000 Mbps Copper ports (Combo)
USB Interface	1 x USB v2.0 Type-A
Management Interface (Web Console)	LAN Interface
Management Console Interface	RJ-45 Console
Power Input	9/12/24/48 VDC, Dual Redundant Inputs (2 x 3 Pin Terminal Block, located in front panel); Reverse Polarity Protection Supported. (* 12V VDC Recommended)
Input Current (A)	1.8/1.35/0.68/0.35A
Power Supply	Dual Power input, total 6 pin terminal block
Operating Temperature	-40 to 75 ˚C (-40 to 167˚F)(Wide Temperature)
Ambient Relative Humidity	5 to 95% non-condensing
Non-operating / Storage Temp.	-40 to 85 ˚C (-40 to 185 ˚F)
Non-operating / Storage Relative Humidity	5 to 95% non-condensing
Vibration	IEC 60068-2-6, IEC 60068-2-27, IEC 60068-2-64 (without any USB devices attached)
Mean Time Between Failure (MTBF)	700,000 hours +
Safety Certification	CE, UL, UL 60950-1
Electromagnetic Compatibility	EMI: CISPR 32, FCC Part 15B Class A EMC: EN 55032/35, VCCI Class A
Green Product	RoHS, RoHS2, CRoHS, WEEE

* Note: Performance is measured in a laboratory, performance values may vary according to test conditions and system configuration.
- Each EdgeFire is entitled to 5 years of hardware warranty. Upon renewal of the software license, the hardware warranty WILL NOT be extended for the same renewal period, subject to a maximum warranty period of 5 years for the hardware.
- VPN throughput measured based on RFC 2544 (1,424-byte UDP packets).