txOne networks | Keep the Operation Running

Datasheet

EdgeFire 1012

Industrial Next Generation Firewall Series

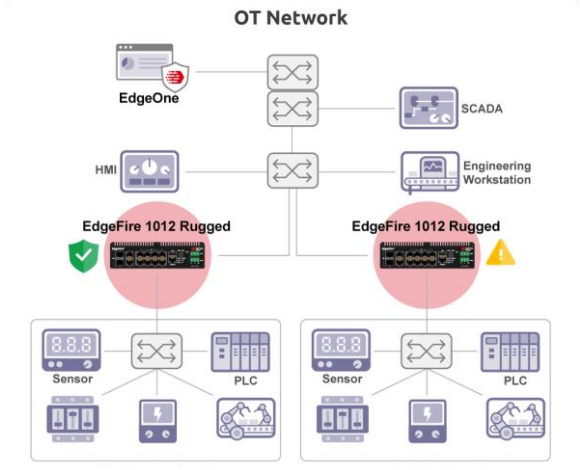
Safeguarding the Future of Industry: OT Network Security Solutions for Uninterrupted Operation

As we enter the era of Industry 4.0, the integration of Operational Technology (OT) into manufacturing and industrial production is revolutionizing the industry. However, this advancement also brings an increase in sophisticated cyber threats such as ransomware, supply chain attacks, and critical infrastructure targeting. To combat these threats, TXOne has developed a comprehensive suite of OT security solutions, meticulously designed in respond to the complex needs of today's production environments.

Selecting the right security solution is essential to any effective cybersecurity strategy. TXOne offers a diverse range of Edge security solutions, tailored to the specific requirements and operational contexts of each industrial vertical. This ensures that every industry can deploy an optimal solution for its unique environment.

In OT security, protecting operations without disrupting production is critical. TXOne's Edge devices provide robust protection while ensuring uninterrupted business continuity. These devices integrate seamlessly into existing networks, eliminating the need for downtime, and in the rare event of hardware failure, they are equipped with multiple bypass mechanisms to maintain smooth production network traffic.

Comprehensive protection is the cornerstone for security, and TXOne leads the industry with advanced features designed to defend against evolving threats. TXOne CPSDR technology strengthens network defenses, preventing unauthorized access and suspicious activities. Additionally, by integrating SageOne, our Cyber-Physical Systems protection platform, OT security operators can correlate network security intelligence with data from other sources, gaining enhanced visibility into their overall security posture. This empowers them to respond more efficiently and effectively to cyber incidents and potential security risks.



Solution Overview

Building a reliable OT network with ease involves three key elements. First, ensuring a strong feature-environment fit is crucial for seamless hardware **adoption**. Second, all security features are designed with a primary focus on **operational** efficiency and continuity. Lastly, OT-specific insights play a pivotal role in enhancing **prevention** capabilities, addressing gaps often overlooked by general IT security products.

You can find your Edge for all sorts of environments —whether harsh or temperate, centralized or distributed. Our flexible connection types and available port density options ensure that your specific needs are met. The pioneering fail-safe mechanisms and AI-driven deployment strategies reduce the configure-to-service time, ensuring a seamless, uninterrupted end-to-end flow. Combined with our OT-centric, proactive prevention technologies, TXOne makes resilient networking both practical and effective. With rising cybersecurity threats, robust OT security is crucial. TXOne Edge products offer innovative Network-wide Security Situational Awareness, providing real-time threat detection and response across the entire OT environment.

Core Capabilities

Adoption

Fulfilling Technical and Operational Demands with a Swift Onboarding Flow

- Rugged design for diverse environments.
- Compact size for space-constrained production sites.
- Easy on-site installation for rapid deployment.
- Batch setup supported with TXOne Deployment Assistant.

Operation

Activating Protection Painlessly with No Operational Disruption

- Ensures uninterrupted production by supporting high-availability mechanisms during hardware failures.
- Supports failover with dual WAN interfaces, enabling multiple connections for external network access.
- Automatically creates and deploys security policies based on AI-curated traffic behaviors.
- Integrates seamlessly into existing networks without disrupting operations.

Prevention

Crafting a Resilient Network with Operational Insights

- Identifies and predicts anomalous network behaviors with CPSDR Networking technology.
- Secures OT network communication and prevents insider threats across ICS protocols.
- Enhances network segmentation to contain cyber infections and limit lateral movement.
- Protects unpatched production assets with signature-based virtual patching.
- Extends IT to OT network protection by importing suspicious objects from third parties.

Key Features

Cyber-Physical System Detection and Response

EdgeFire 1012 is built with TXOne's pioneering CPSDR (Cyber-Physical System Detection and Response) technology, designed to identify and predict anomalous network behaviors at an early stage. With the CPSDR, your OT network can proactively stay a step ahead of cyber risks, blocking potential threats before they materialize.

Asset-Centric Auto Rule Learning Technology

EdgeFire 1012 features Asset-Centric Auto Rule Learning Technology, an AI-driven solution tailored to the ICS network environment. This advanced technology analyzes traffic for each asset, generating baseline allowlists that can be reviewed individually, streamlining administration and boosting security management.

Mastering Industrial Protocols

EdgeFire 1012 supports a variety of OT protocols, including Modbus, SECS/GEMS, CIP, and more, to allow OT and IT security administrators to collaborate for seamless operation within the existing network architecture.

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.

Signature-Based Virtual Patching

With the cutting-edge research of the Zero Day Initiative (ZDI) vulnerability rewards program, EdgeFire 1012 offers you superior control of the patching process for legacy systems to protect them against known threats through virtual patching.

Unrivaled Threat Intelligence

Leveraging the Zero Day Initiative (ZDI) vulnerability rewards program, EdgeFire 1012 provides your systems with unparalleled protection against undisclosed and zero-day threats.

Shadow OT Visibility Enhancement

EdgeFire 1012 is designed to seamlessly integrate and coordinate you IT and OT networks, while also providing visibility into your shadow OT environment.

Flexible Segmentation and Isolation

EdgeFire 1012 is the ideal solution for segmenting your network into efficiently managed and secure zones, enhancing overall network security and performance.

Multi-Segmenting with Integrated Security

EdgeFire 1012, specifically designed for levels 1-3, can be deployed in front of mission-critical assets or at the OT network edge. Its transparency and high performance enable it to safeguard network traffic and production assets without disrupting operations.

Secure Remote Connectivity with VPN Solutions

EdgeFire 1012 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 1012 for remote OT operation.

Configurable Operation Modes

EdgeFire 1012 can flexibly switch between 'Monitor' and 'Prevention' modes. Keep in 'Monitor' mode until the detection results are verified by the IT or OT team, then switch to 'Prevention' mode to block malicious traffic.

Holistic CPS Protection Platform Integration

By integrating TXOne SageOne with Edge security solutions, you can orchestrate cybersecurity information across all Edge Series devices. This integration goes beyond visibility, offering comprehensive protection and threat detection across all CPS facilities in your organization. It offers actionable recommendations ready for implementation by OT security management teams.

Centralized Management with Convenient, Consolidated Overview

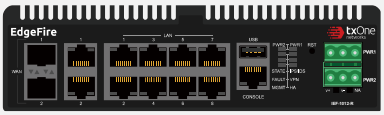
Pattern updates and firmware management can all be centralized on a large scale. For facilities with extensive EdgeFire 1012 nodes, EdgeOne facilitates group administration and management, thereby reducing costs and enhancing efficiency on a large scale.

EdgeFire 1012 Hardware

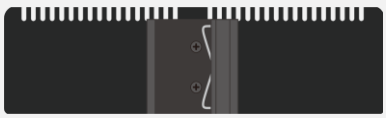
EdgeFire 1012 Rugged

180 mm x 120 mm x 50 mm (7.09 in x 4.72 in x 1.97 in)

Front Panel



Rear Panel



EdgeFire 1012 Specifications

Feature	EdgeFire 1012 Rugged
Threat Prevention Throughput / Firewall Throughput*	200 Mbps+ (IMIX) / 600 Mbps+ (UDP 1518 bytes)
Latency*	<500 microseconds on average under mixed traffic condition
Concurrent Connection (TCP)	100,000
Intrusion Prevention / CPSDR-Networking	Yes / Yes
Supported ICS Protocols	Modbus / EtherNet IP / CIP / FINS / S7Comm / S7Comm+ / SECS / GEM / IEC61850-MMS / IEC-104, with more being added regularly
Policy Enforcement Rules	512 device rules / 512 EdgeOne rules (in gateway and bridge modes)
L2 Policy Enforcement Rules	256 device rules (in bridge mode)
ICS Protocol Filter Profiles	64 profiles
Maximum Concurrent VPN Tunnels	50 site-to-site / client-to-site VPN tunnels
Supported VPN Protocols	IPSec (IKEv1, IKEv2), L2TP over IPSec
IPSec VPN Throughput	50 Mbps
Form Factor	DIN-rail mounting, server rack mount and wall mounting (with optional kit)
Weight (Standalone Device)	1.381 kg (3.044 lb)
Dimensions (W x D x H)	180 mm x 120 mm x 50 mm (7.09 in x 4.72 in x 1.97 in)
Network Interface Type	8 x auto-sensing 10Mbps/100Mbps/1Gbps BASE-TX (RJ-45) ports / 2 x 100Mbps/1Gbps SFP ports and 2 x auto-sensing 10Mbps/100Mbps/1Gbps BASE-TX (RJ-45) ports (Combo)
USB Interface	1x USB 2.0 interface (Type-A)
Management Interface (Web Console)	LAN interface
Management Console Interface	RJ-45 console
Power Supply	Dual power input, 6x pin terminal block
Power Input	9/12/24/48 VDC, dual redundant inputs (2 x 3 pin terminal block, shall locate in front panel); reverse polarity protection supported. (*12V VDC recommended)
Input Current (A)	1.8/1.35/0.68/0.35A
Operating Temperature	-40 to 75 ˚C (-40 to 167 ˚F) (wide temperature)
Ambient Relative Humidity	5 to 95% (non-condensing)
Storage Temperature	-40 to 85 ˚C (-40 to 185 ˚F)
Mean Time Between Failure (MTBF)	700,000 hours (under 25°C)
Safety Certification	CE, UL, UL60950-1
Electromagnetic Compatibility	EMI: CISPR 32, FCC Part 15B Class A / EMC: EN 55032/35, VCCI Class A
Green Product	RoHS, RoHS2, CRoHS, WEEE
Centralized Management Console	Supports EdgeOne

* Note: Performance and latency are measured in a laboratory; these values may vary according to test conditions and system configuration.
* Each EdgeFire is entitled to 2 years of hardware warranty. Upon renewal of the software license and hardware warranty extension, the hardware warranty WILL NOT be extended for the same renewal period, subject to a maximum warranty period of 7 years.