txOne networks | Keep the Operation Running

Datasheet

EdgeIPS 103/103F

Next-Generation Intelligent Protection System

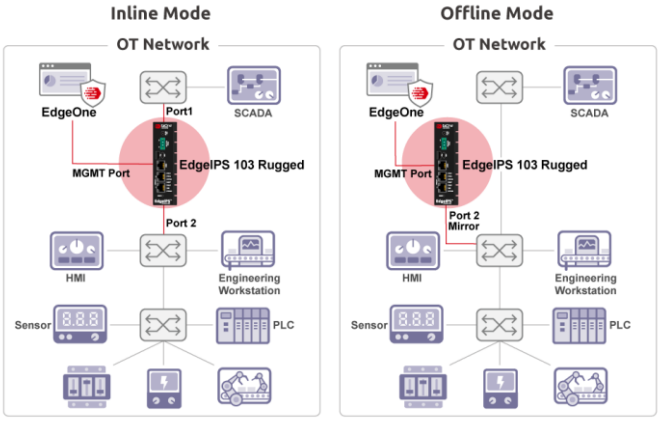
Safeguarding the Future of Industry: OT Network Security Solutions for Uninterrupted Operation

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 Ovreview

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

- ❖ Offers copper and fiber interfaces for varied connectivity.
- ❖ Rugged design for diverse environments.
- ❖ Compact size for space-constrained production sites.
- ❖ Easy on-site installation for rapid deployment.
- ❖ Batch setup supported with Deployment Assistant.

Operation

Activating Protection Painlessly with No Operational Disruption

- ❖ Ensures uninterrupted production by supporting fail-safe mechanisms during hardware failures.
- ❖ 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

EdgeIPS 103/103F 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.

Hybrid Approach to OT Protocol Filtering

EdgeIPS 103/103F delivers granular inspection of a wide range of OT protocols—such as Modbus, SECS/GEM, CIP, TSAA, and CODESYS—without requiring a firmware upgrade. This hybrid approach ensures up-to-date protocol filtering capabilities while maintaining uninterrupted operations.

Signature-Based Virtual Patching

With the cutting-edge research of the Zero Day Initiative (ZDI) vulnerability rewards program, EdgeIPS 103/103F offers you superior control of the patching process for legacy systems to protect them against known threats through virtual patching.

Asset-Centric Auto Rule Learning Technology

EdgeIPS 103/103F 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.

OT-Aware Operational Intelligence

Our core technology for EdgeIPS 103/103F, 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.

Transparent Network Traffic Control

EdgeIPS 103/103F, 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.

Flexible Operation Modes

EdgeIPS 103/103F 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.

Shadow OT Visibility Enhancement

EdgeIPS 103/103F is designed to seamlessly integrate and coordinate your IT and OT networks while providing visibility into your shadow OT environment with detailed insights into asset communication, leaving no blind spots and no room for compromise.

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

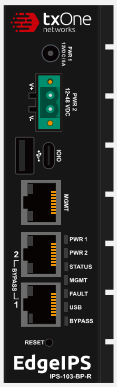
Pattern updates and firmware management can all be centralized on a large scale. For facilities with extensive EdgeIPS 103/103F nodes, EdgeOne facilitates group administration and management, thereby reducing costs and enhancing efficiency on a large scale.

EdgeIPS 103/103F Hardware

EdgeIPS 103

140.1 mm x 109.8 mm x 40.2 mm (5.515 in x 4.322 in x 1.582 in)

Front Panel



Rear Panel

EdgeIPS 103F

195 mm x 110 mm x 34 mm (7.677 in x 4.33 in x 1.338 in)

Front Panel

Rear Panel

EdgeIPS 103/103F Specifications

Feature	EdgeIPS 103	EdgeIPS 103F
Model	IPS-103-BP-R-TX	IPS-103F-BP-R-TX
Threat Prevention Throughput*	850Mbps at least (IMIX) / 1.2Gbps+ (UDP 1518 bytes)	
Latency*	<500 microseconds on average under mixed traffic condition	
Concurrent Connection (TCP)	30,000	
Intrusion Prevention / CPSDR-Networking	Yes / Yes	
Supported ICS Protocol	Modbus, EtherNet IP, CIP, FINS, S7Comm, S7Comm+, SECS, GEM, IEC61850-MMS, IEC-104, TSAA, CODESYS, and more — all supported without requiring a firmware update	
Policy Enforcement Rules	512 device rules / 512 EdgeOne rules	
L2 Policy Enforcement Rules	256 device rules	
ICS Protocol Filter Profiles	64 profiles	
Form Factor	DIN-rail mounting and wall mounting (with optional kit)	
Weight (Standalone Device)	933 g (2.0569 lb)	1.155 kg (2.5463 lb)
Dimensions (W x D x H)	140.1 mm x 109.8 mm x 40.2 mm (5.515 in x 4.322 in x 1.582 in)	195 mm x 110 mm x 34 mm (7.677 in x 4.33 in x 1.338 in)
Network Interface Type	2 x auto-sensing 10/100/1000 Mbps ports (RJ45 connector)	2 x 1Gbps 1000BASE-SX fiber ports (LC connector type – multi-mode)
USB Interface	1 x USB v2.0 Type-A	
Management Interface	Out-of-band interface, 1 x auto-sensing 10/100/1000 Mbps ports (RJ45 connector)	
Hardware Failover	Configurable hardware bypass (copper)	Configurable hardware bypass (fiber)
Management Console Interface	USB Type-C console	
Input Voltage	12/24/48 VDC terminal block / DC-IN 12V	
Input Current	0.483/0.241/0.127 A	
Power Supply	Dual-type input (4-pin terminal block, V+, V-) / DC-IN 12V standard 12V DC power adapter	
Operating Temperature	-40 to 75˚C (-40 to 167 ˚F) (wide temperature)	0 to 40˚C (32 to 104 ˚F)
Ambient Relative Humidity	5 to 95% non-condensing	
Non-Operating / Storage Temperature	-40 to 85 ˚C (-40 to 185 ˚F)	
Non-Operating / Storage Relative Humidity	5 to 95% non-condensing	
Vibration	IEC60068-2-6 (without any USB devices attached)	
Mean Time Between Failure (MTBF)	680,000 hours (under 25 ˚C)	
Certification	CE, FCC (Part 15B Class A), VCCI (Class B) UL (UL 62368-1, UL 60950-1) CISPR 32, EN 55032/35	
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 EdgeIPS is entitled to 2 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 7 years for the hardware.