

Datasheet

Virtual EdgeIPS Pro



Intent-Based Industrial Intelligent Protection System

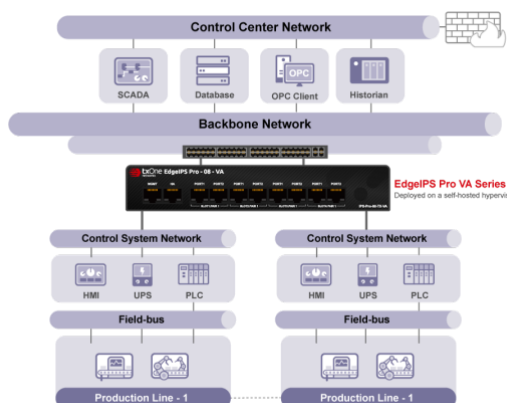
Safeguarding the Future of Industry: OT Network Security
Solutions for Uninterrupted Operation

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 increasingly sophisticated cyber threats, including ransomware, supply chain attacks, and attacks targeting critical infrastructure. To address these challenges, TXOne has developed a comprehensive suite of OT security solutions, purpose-built to meet the complex security and operational requirements of today's production environments.

Selecting the right security solution is essential to an effective cybersecurity strategy. TXOne Virtual EdgeIPS Pro extends OT-native network security into virtualized environments, providing flexible and scalable protection tailored to diverse industrial architectures and operational requirements. It enables organizations to deploy consistent OT security across physical and virtual environments while adapting to evolving infrastructure needs.

In OT security, protecting operations without disrupting production is critical. Virtual EdgeIPS Pro leverages AI-powered security intelligence to provide robust and precise protection while supporting operational continuity. Designed for seamless integration with existing virtualized and network environments, it enables security capabilities to be deployed without requiring changes to the underlying production infrastructure, helping organizations strengthen OT protection with minimal operational impact.

Comprehensive protection is the cornerstone of effective OT security. Virtual EdgeIPS Pro combines advanced CPSDR technology with AI-powered security intelligence to strengthen network defenses against unauthorized access, anomalous behavior, and evolving cyber threats. Its enhanced OT visibility provides deeper insight into assets, communications, risks, and threats, enabling security teams to make faster, more informed decisions and respond more effectively to 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 virtualized deployment. Second, all security features are designed with a primary focus on operational efficiency and continuity. Lastly, OT-specific insights and AI-powered intelligence play a pivotal role in enhancing prevention capabilities, addressing gaps often overlooked by general IT security products.

Virtual EdgeIPS Pro adapts to diverse virtualized OT environments, whether centralized or distributed, providing flexible deployment options to meet specific infrastructure requirements. Its AI-driven deployment and security intelligence streamline configuration and policy deployment, reducing configure-to-service time while supporting seamless, uninterrupted operations. Combined with OT-centric, proactive prevention technologies, TXOne makes resilient OT security practical and scalable across virtualized environments.

With rising cybersecurity threats, robust OT security is crucial. Virtual EdgeIPS Pro provides enhanced visibility into OT assets, communications, risks, and threats, enabling real-time threat detection and response across the OT environment.

Core Capabilities



Adoption

Fulfilling Technical and Operational Demands with a Swift Onboarding Flow

- ❖ Flexible interface configuration with multiple virtualization platforms for versatile environments.
- ❖ Protect your entire shop floor with a single, Multiple Virtual EdgeIPS Pro Appliance.
- ❖ 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.
- ❖ AI-Powered OT asset identification automatically discovers and profiles OT assets.



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 and antivirus.
- ❖ Extends IT to OT network protection by importing suspicious objects from third parties.

Key Features



Cyber-Physical System Detection and Response

Virtual EdgeIPS Pro 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.



AI-Powered Asset-Centric Auto Rule Learning

Virtual EdgeIPS Pro uses AI-driven traffic analysis to automatically learn each asset's communication behavior and generate asset-specific allowlist rules. Security teams can quickly review and optimize policies with greater accuracy, reducing manual effort while strengthening OT operational protection and resilience.



Hybrid Approach to OT Protocol Filtering

Virtual EdgeIPS Pro 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.



OT-Aware Operational Intelligence

Our core technology for Virtual EdgeIPS Pro, 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 and Antivirus

Virtual patching shelters endpoint and network vulnerabilities while signature-based antivirus provides an extra layer of protection under Virtual EdgeIPS Pro. Research-supported, up-to-date signatures protect your production assets against the latest threats, and the frequency of flexible updates is fully under the administrator's control.



Unrivaled Threat Intelligence

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



Multi-Segmenting with Integrated Security

Virtual EdgeIPS Pro, 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.



Shadow OT Visibility

Virtual EdgeIPS Pro leverages AI-Powered Asset Intelligence to autonomously discover unknown OT assets, legacy systems, vulnerabilities, and communication paths across IT/OT networks with zero manual intervention. Eliminate Shadow OT blind spots and gain reliable asset intelligence from day one.



Centralized Management with Convenient, Consolidated Overview

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



Holistic CPS Protection Platform Integration

By integrating TXOne EdgeOne 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.



Flexible Deployment

Virtual EdgeIPS Pro flexibly switches between 'Monitor' and 'Prevention' modes and supports up to 4 segments to preserve your productivity while maximizing security.

Virtual EdgeIPS Pro

Virtual EdgeIPS Pro	vEdgeIPS Pro-02-VA	vEdgeIPS Pro-04-VA	vEdgeIPS Pro-08-VA
vCPU Core	2	4	8
Security Performance	500Mbps	1.5Gbps	2.5Gbps
Firewall Throughput	800Mbps	1.8Gbps	2.8Gbps
Concurrent Connection	30,000+	100,000	200,000
Connection Rate	Rely on Hardware capacity	Rely on Hardware capacity	Rely on Hardware capacity
Network Segmentation (Network isolation)	Up to 1 Segments (2+1 NICs)	Up to 2 Segments (4+1 NICs)	Up to 4 Segments (8+1 NICs)
Policy Enforcement	Up to 64 template rule sets / 2048 rule per template rule set	Up to 64 template rule sets / 2048 rule per template rule set	Up to 64 template rule sets / 2048 rule per template rule set
Max number of registered client	1024 Clients/Assets	2048 Clients/Assets	4096 Clients/Assets
Memory requirement (Min/ Max)	8GB / unlimited	8GB / unlimited	16GB / unlimited
Storage Requirement (Min/Max)	70GB / 2TB (RAID System Recommended)	70GB / 2TB (RAID System Recommended)	70GB / 2TB (RAID System Recommended)
Supported CMS	EdgeOne (2.7.x or above)	EdgeOne (2.7.x or above)	EdgeOne (2.7.x or above)
Supported Hypervisors	VMWare ESX 6.5 or above KVM 2.x or above		

* **Note:** Performance and latency are measured in a laboratory; these values may vary according to test conditions and system configuration.

* **Note:** All performance values are "up to" and vary depending on system configuration.

* **Note:** The maximum number of network interfaces supported by a virtual EdgeIPS Pro instance. The actual limit varies by hypervisor platform and instance type.