

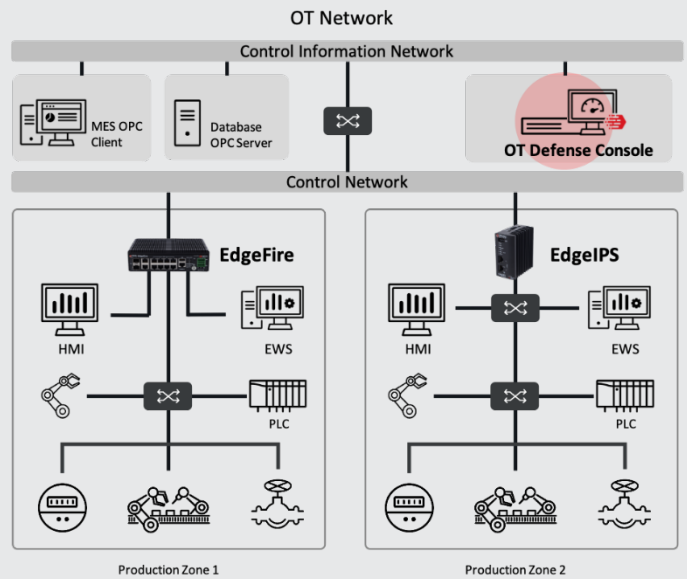
OT Defense Console™ Industrial Central Management Console

DATASHEET

Centralized Continuous Monitoring of OT Cyber Threats with a Secure, Distributed Industrial Network for Uninterrupted Production Line Operation

Attacks on manufacturers and critical infrastructure sites have become serious cybersecurity issues in recent years. Typically two types of malicious actors are responsible for these incidents: state-sponsored and cybercriminal. Proper security management requires both visibility and control of security policies, while OT security protection requires even higher-grade security management for proper defense and effective response.

TXOne Networks offer both security policy control and security management to protect OT environments. Edge Series product enable network segmentation and segregation to divide the network into different zones of control down to the cell level. OT Defense Console (ODC™) provides central visibility and defense line management to manage and deploy different security policies to Edge Series nodes with an at-a-glance dashboard giving a clear overview of current security status.



Benefits

Built for industrial-grade resilience, security, and flexibility

- Tailored for OT environments and industrial design.
- ODC supports cross-plant management and can be easily integrated with SOC/SIEM.
- Intercepts the spread of worms from deployed EdgeIPS, EdgeIPS Pro and EdgeFire nodes.
- ODC is a virtual versions, and it works well in your choice of server.

Broad visibility for large-scale OT networks

- Use the dashboard to easily monitor cases, receive notifications, and analyze activity in the OT environment.
- Maintain an overview of system cyber risk status, threat vulnerability, and ability to resist attack.
- Customizable dashboard allows you to add or arrange widgets to monitor network activities and system status.
- Scalable to hundreds or even thousands of assets at multiple sites with EdgeIPS, EdgeIPS Pro and EdgeFire.
- Gain visibility into your shadow OT environment.

Increase convenience and interconnectivity

- Reduce your maintenance costs across facilities with easy, efficient management system.
- Convenient management policies as well as up-to-date security signature updates and provisioning.
- Manual firmware and pattern provision to EdgeIPS, EdgeIPS Pro and EdgeFire by node group.
- ODC logs activity at each EdgeIPS, EdgeIPS Pro and EdgeFire node, including cybersecurity, policy enforcement, protocol filtering, system logs, audits, and asset detection.

Flexible policy deployment and advanced reporting

- Maintain consistent, standardized policy with dual-track parallelization of centralized and decentralized policies.
- Gives users ease of access to comprehensive threat reporting that can be generated both on-demand and by schedule.

Key Features

- Organize Your Info with the ODC Dashboard**
 The dashboard of OT Defense Console gives you a comprehensive, consolidated overview. This is organized into alerts, assets, and incident events, allowing you to directly monitor the security of your enterprise's industrial control system.
- Gain an Overhead View of Your Cyber Situation**
 Clear visibility is crucial for strong ICS security, so ODC gives clear visibility of all installed ICS assets in the OT environment and how they're connected, as well as giving users vision of the shadow OT environment.
- Easily Manage Vast Amount of Network Nodes**
 ODC allows large-scale and remote management of all Edge Series devices in your different facilities.
- IPS and Policy Enforcement by Group**
 ODC uses the powerful, signature-based "Virtual Patch" threat prevention solution, organized by node group, to protect the OT network from known threats.
- Effort-Saving Update Functionality**
 Update Edge Series products with the latest patterns and firmware by node group, centralizing and improving the efficiency of administrative and on-site support tasks.
- Flexible Policy Management for Network Nodes**
 ODC provides administrators with the ability to edit the OT protocol Allowlist to enable interactive interoperability between key production machine assets, as well as to deeply analyze L3-L7 networks by node group.
- Virtual ODC is Ready for Your Hardware**
 Virtual ODC manages a maximum number of nodes depending on system resources, which it checks when a node license is activated.
- User-Friendly Log Viewing with Adaptive Queries**
 ODC's user-friendly GUI allows users to generate reports from log files according to different business intentions using variant queries for any Edge series node operating on the network. ODC keeps track of every necessary record including cybersecurity, policy enforcement, protocol filter, node group, system, audit, and asset detection logs.
- Comprehensive Advanced Reporting**
 ODC provides flexible report templates for easy access to threat information. Generated reports give users a better understanding of complex threat scenarios, informing plans for containment and mitigation.

OT Defense Console™ Specifications

	OT Defense Console - Virtual Appliance						
Target Max Managed Node	1000	500	300	200	150	100	50
vCore	32	16	12	8	6	4	4
Memory	128GB	96 GB	64 GB	32 GB	32 GB	16 GB	16 GB
Disk Storage (Recommend)	SSD or HD 10TB Storage capacity or above	SSD or HD 5TB Storage capacity or above	SSD or HD 2TB Storage capacity or above	SSD or HD 2TB Storage capacity or above	SSD or HD 1TB Storage capacity or above	SSD or HD 1TB Storage capacity or above	SSD or HD 1TB Storage capacity or above
	RAID System is better						
Supported Hypervisors	VMWare ESX 6.X or above / VM Workstation V14 or above / KVM 2.x or above / Hyper-V 10.x or above						