OPSWAT.

DATASHEET

METADEFENDER™

OT Security

Rethink OT Cybersecurity

Visibility into OT environments continues to be a major challenge and risk vector for organizations. OT environments are inherently heterogeneous and quite often consist of decades-old devices from multiple vendors. The ability to have full visibility into assets and what is happening on the network is key to any effective OT cybersecurity program.

What We Offer

MetaDefender OT Security addresses risks to OT systems from both traditional IT and specific ICS threats. It is extremely simple to deploy and easy to use with OT-native UIs. MetaDefender OT Security can be operated without an expert skillset or training.

Designed for enterprise-level deployments, MetaDefender OT Security provides unparalleled visibility into converged IT/OT operations. It also delivers deep situational awareness of threats throughout the network.

It helps to protect your critical assets by maximizing your visibility, security, and control across your entire operations while staying compliant with regulatory requirements.

MetaDefender OT Security leverages AI technologies to gain knowledge of the unique attributes and requirements of OT environments.

Benefits

- Complete asset visibility and centralized security management for geographically dispersed networks
- Streamlines incident response and expedites remediation
- Easy to use and deploy. Built for OT personnel
- Timely and accurately informs you of any threats or anomalies on the network
- Supports regulatory requirements with wide and objective risk assessments
- Scalable across OT environments at an Enterprise level
- Provides a unified view of operation, security, and compliance in a single pane of glass
- Seamless integration with MetaDefender Industrial Firewall & IPS

OPSWAT.

MetaDefender OT Security

DATASHEET

Capabilities

- Rapidly Discover Devices and Build Asset Inventory
- Smart Asset Profiling
- Active and Passive Threat Monitoring
- Continuously Monitor Network to detect Threats and Anomalies
- Constantly & Objectively Address OT Vulnerabilities and Risks
- Structured and Streamlined Risk Alert Workflow
- Centralized Patch Management
- Global, regional & Industry Regulatory Compliance Reporting
- Comprehensive & Customizable Dashboard
- Granular Access and Controlled User Permissions

Use Cases

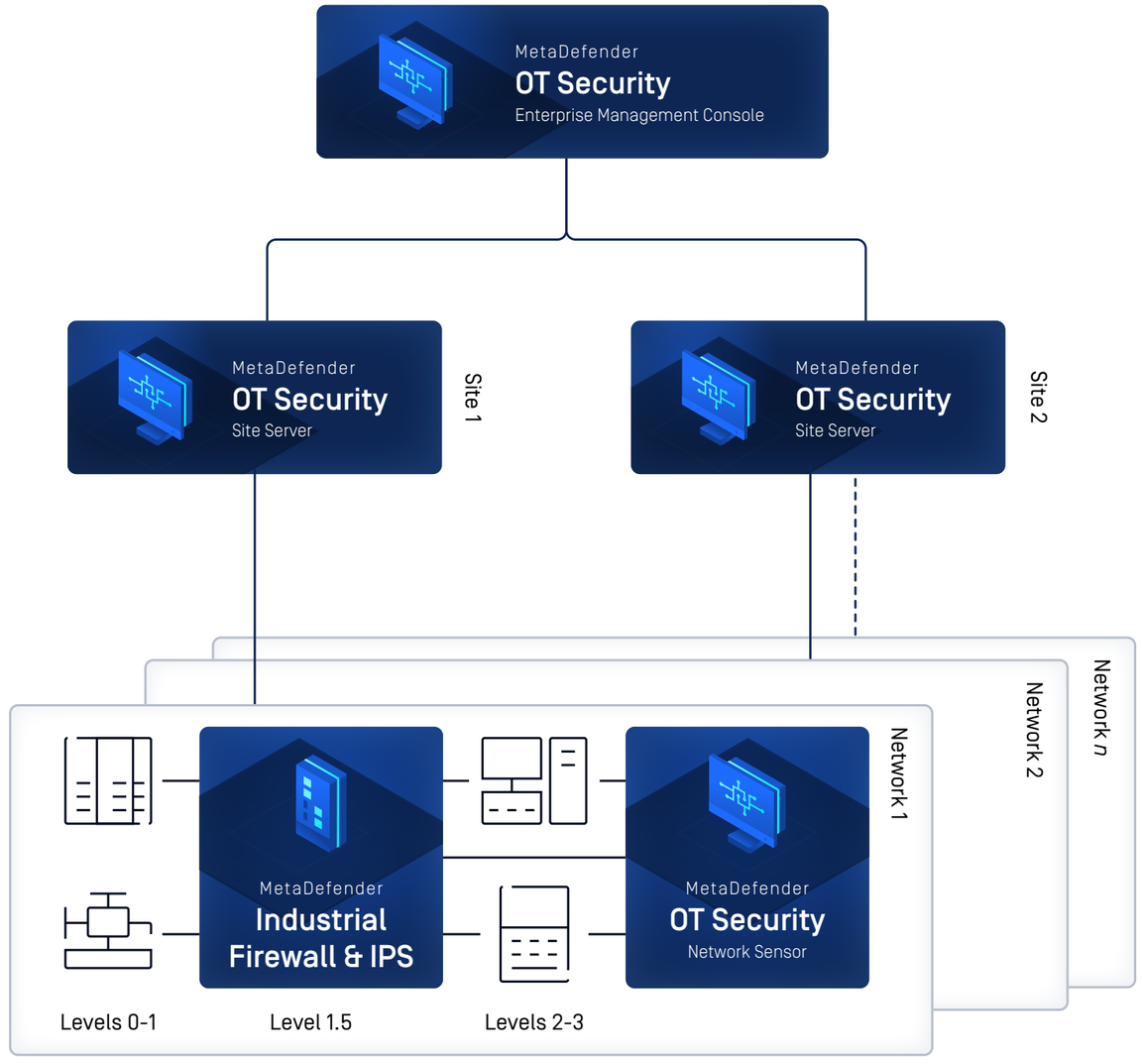
- Asset Inventory & Vulnerability Assessment
- Network Visualization & Monitoring
- Threat Detection & Response
- Exposure Assessment & Alert workflow

Realtime, AI-based analytics Engine

- Behavioral Anomaly Detection
- Asset's Changes Detection
- Unusual Communication Detection
- Violation of Security Policies Detection

Deep Network Analysis & Device Fingerprinting

- Deep Network Traffic Dissection
- Knowledge of OT Devices & Protocols
- Proprietary ICS Fingerprinting & Vulnerability



Deployments Guideline for MetaDefender OT Security

Component Criteria	MetaDefender OT Security Network Sensor	MetaDefender OT Security Site Server	MetaDefender OT Security Enterprise Management Server
Installation Options	Virtual Appliance or Bundled Software	Virtual Appliance or Bundled Software	Virtual Appliance or Bundled Software
Typical Number of Assets	100 - 200 Assets per Sensor (DIN Rail Industrial PC) 250 - 500 Assets per Sensor (Rack server)	5,000 Assets per Site Server	Multiple Sites Supported
Max. Network Throughput	200Mbps (DIN Rail Industrial PC) 400Mbps (Rack server)		
Typical HW Specs.	• CPU Cores: 4 - 8 • RAM: 8GB - 16GB • Storage: 250GB - 500GB	• CPU Cores: 16 - 32 • RAM: 32GB - 64GB • Storage: 4TB - 8TB	• CPU Cores: 16 - 32 • RAM: 32GB - 64GB • Storage: 5TB - 10TB
Networking	3 x GB Ethernet Interfaces 1. Gbps Ethernet port: Connects to the **SPAN port** on the switch of the OT network, for passive monitoring/ discovery. 2. Gbps Ethernet port: Connects to the OT network, for active discovery. 3. Gbps Ethernet port (Northbound interface): for connection to MD OT Security Site Manager. The same physical interface can be used for #2 and #3 if there are appropriate network segmentation and/ or routing configurations. Using interface #1 (which connects to the SPAN port of switch) with other purposes is NOT recommended as there is heavy network traffic at the SPAN port; and issues on inter-network connection (routing) observed at the interface connected to the SPAN port for some types of switch.	2 x GB Ethernet Interfaces 1. Gbps Ethernet port (Southbound interface): For connecting with the sensors. 2. Gbps Ethernet port (Northbound interface): For connection to MetaDefender OT Security Enterprise Manager.	2 (or 3) x GB Ethernet Interfaces 1. Gbps Ethernet port (Southbound interface): For connecting with the Site Managers. 2. Gbps Ethernet port: Exposes the Enterprise Management Console users accessing the IP of this interface for interacting with the Enterprise Management Console. 3. Gbps Ethernet port (optional): For Enterprise Manager connecting to the Internet for (online) license activation and auto update/ upgrade of MD OT Security product. The same physical interface can be used for #2 and #3 if there are appropriate routing configurations.