OPSWAT.

METADEFENDER OT SECURITY

An AI-powered, Enterprise Cybersecurity Tool to Protect OT Networks

SOLUTION BRIEF

MARCH 2024

CONTENTS

THE OT ENVIRONMENT

Operational Technology (OT) is the combination of hardware and software that monitors and controls industrial processes. Industrial and critical infrastructure organizations use OT and ICS to safely produce and ensure delivery of goods and services which are essential to the daily life of billions of people around the world.

OT CYBERSECURITY CHALLENGES

Shortage of A Skillful Workforce and Effective Security Solutions
We face a significant shortage of cybersecurity workforce as well as effective cybersecurity solutions for OT businesses. Many cybersecurity products were built primarily for IT professionals and are too complex or costly to implement and maintain in an OT environment. This combined shortage makes cybersecurity programs in an OT organization even more challenged.

Increasing Threats from IT/OT Convergence
While IT/OT convergence brings many benefits to OT business, it also increases the risks as OT environments are now exposed to cyberthreats of the IT world. Recent attack campaigns like BlackEnergy, Triton, Colonial Pipeline, and JBS Foods, show that conventional defenses are no longer sufficient to protect OT networks from today's sophisticated attacks.

Lack of Visibility into Assets and Network Activity
You can't protect what you don't see. OT environments are inherently heterogenous and often consist of decades-old devices from a variety of vendors, spread across locations. The ability to have full visibility into the assets and a thorough understanding of what is happening on the network is the key to any effective OT cybersecurity programs.

Complex Regulatory Compliance Requirements
Adhering to OT security compliance requirements is often a manual and inefficient process. Critical infrastructure organizations heavily invest in people, process, and technology to comply with regulatory programs required to meet audit and compliance requirements across global, regional, and industry standards.

Facts & Figures

Cybersecurity labor crunch to hit 3.5 million unfilled jobs

The 2023 WEF's Global Risks Report listed cyberattacks on critical infrastructure as a top concern

The number of industrial control systems connected to the Internet is 100,000+ and continues to grow

Ensuring the reliability and availability of control systems is the number #1 concern for OT/ ICS security for organizations

One of the top 5 concerns for OT/ ICS security businesses is meeting regulatory compliance

METADEFENDER OT SECURITY: A NEW APPROACH

MetaDefender OT Security Employs a New Approach to Address the Challenges in OT Cybersecurity

MetaDefender OT Security addresses risks to OT systems from both traditional IT and specific ICS threats. It provides unparalleled visibility into converged IT/OT operations and delivers deep situational awareness of cyberthreats throughout the network. It helps maximize your visibility, security, and control across your entire operations, protecting critical assets effectively, and stay compliant with regulatory requirements.
MetaDefender OT Security's benefits are from its advanced AI technologies, knowledge of the unique attributes and requirements of OT environments, and deep understanding of OT usage preferences.

Designed to easily deploy at an enterprise level, MetaDefender OT Security is easy to use with an OT-native UI, and can be operated without expert skillset or training.

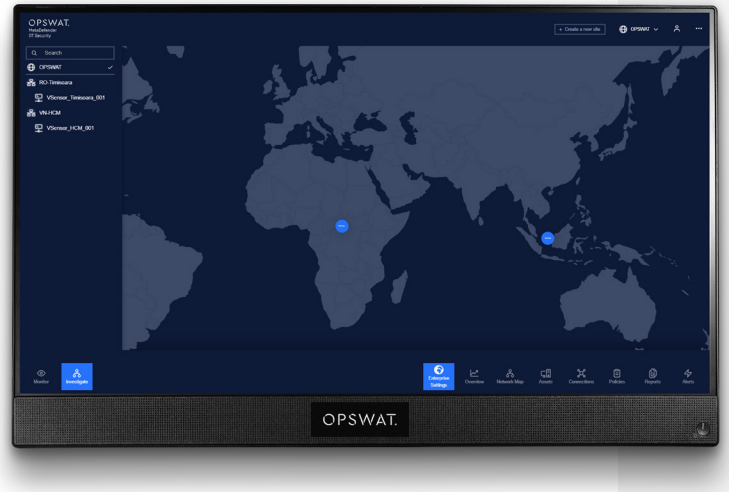
A Powerful Tool to Protect OT Networks

- Purpose-built OT and IT View Mode help OT Personnel and Security professionals address cybersecurity issues with different views and preferences.
- Centralized, scalable, enterprise solution to discover and manage assets across distributed networks. Employs advanced discovery techniques for complete assets inventory without impact on OT networks and devices.
- Predefined policies incorporate requirements in regulatory standards.
- AI algorithms for auto defining comprehensive security policies and proactively identifying of a variety of vulnerabilities and threats.
- Continuous and real-time monitoring of asset and network connectivity, immediate alert on any violation of security policies or anomalies.
- Seamless integration with MetaDefender Industrial Firewall & IPS for complete intrusion detection and prevention capabilities.

BENEFITS

- Built as an easy-to-use, simple-to-deploy solution to maximize OT personnel's usage and performance
- Address both IT and specific ICS threats to OT systems
- Enterprise Management Console for complete asset visibility and centralized security management for geographically dispersed networks
- Timely and accurately informed of any threats or anomalies on the network
- Support regulatory requirements with wide and objective risk assessments
- Unified view of Operation, Security and Compliance, in a single pane of glass

METADEFENDER OT SECURITY PLATFORM ARCHITECTURE



Plug & Play Visibility and Protection

- OT Friendly
- Simple to Deploy
- Easy to Use & Maintain
- No expert skillset or training required

Capabilities and Use Cases

- Centralized Asset Inventory and Vulnerability Assessment
- Network Visualization and Monitoring
- Threat Detection and Response
- Exposure Assessment and Alert Workflow
- Dashboard & Reporting
- Remote Patch Management

OT- IT View mode

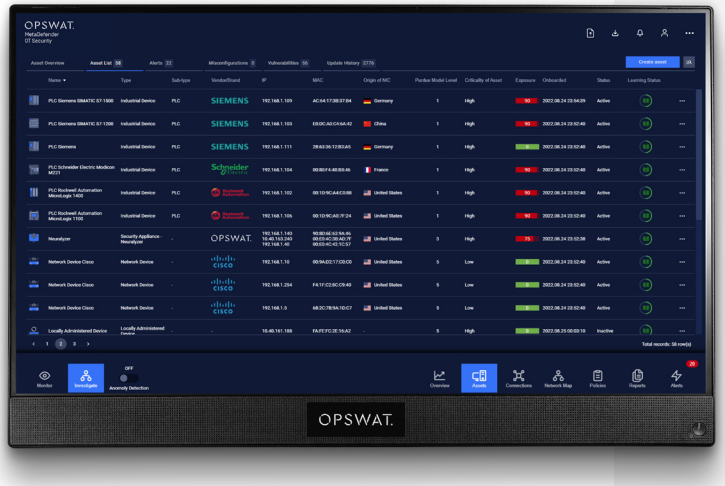
Realtime, AI-Based Analytics Engine

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

Deep Network Analysis and Device Fingerprinting

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

METADEFENDER OT SECURITY: EFFECTIVE, SMART, & SIMPLE



Rapidly Discover Devices and Build Asset Inventory

As soon as MetaDefender OT Security is deployed, it starts looking for the devices across your networks. Using the combined non-intrusive passive monitoring and selective probing specific to each vendor and device type, MetaDefender OT Security can safely uncover devices on your networks. Its capabilities are not limited to single networks, but across large, distributed networks. The result is a full, detailed and ready to use asset inventory list.

Any device on the network becomes fully visible on MetaDefender OT Security

Asset Inventory & Details

Provides an overview of all assets on your network and features customizable filtering to quickly see what you need.

Insights about device's properties, connectivity, security posture (vulnerability, open port/ service), update history, and alerts. These details are necessary for Asset Management and help provide useful data for meeting regulatory requirements.

Scalable and Flexible

MetaDefender OT Security can scale with your business, across thousands of networks without compromising on performance.

It provides customizable data collection through hierarchical aggregations, enabling users to tailor their security view.

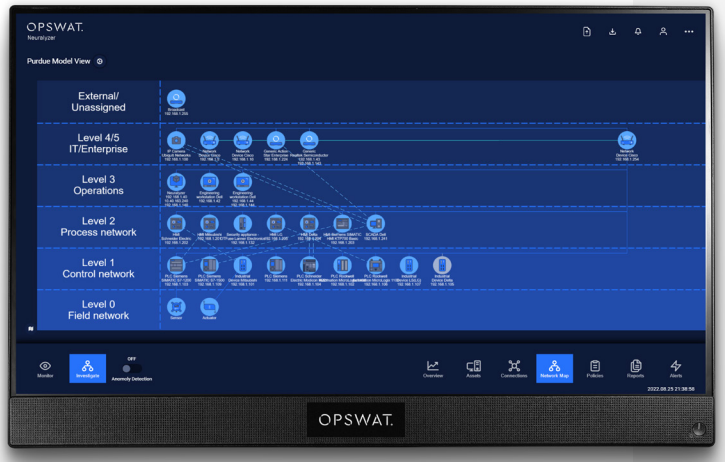
Supports multi-tenancy for effective, centralized management across diverse units.

The interactive network map provides a clear view of connectivity between devices

Immediately Explore Connectivity and Visualize Network Map

MetaDefender OT Security 's Enterprise Management Console captures and analyzes the network traffic, displays connectivity, security posture, renders the topology, and visualizes a real-time, interactive network map.
All communication (protocol, port, time, and data length), whether between devices on the network or between an internal device and a remote host, is clearly shown in great detail.

Allows smart asset profiling with active and passive monitoring capabilities



Realtime Purdue model network map helps immediately spot abnormal/ unauthorized connection

Customizable Filter and Navigation

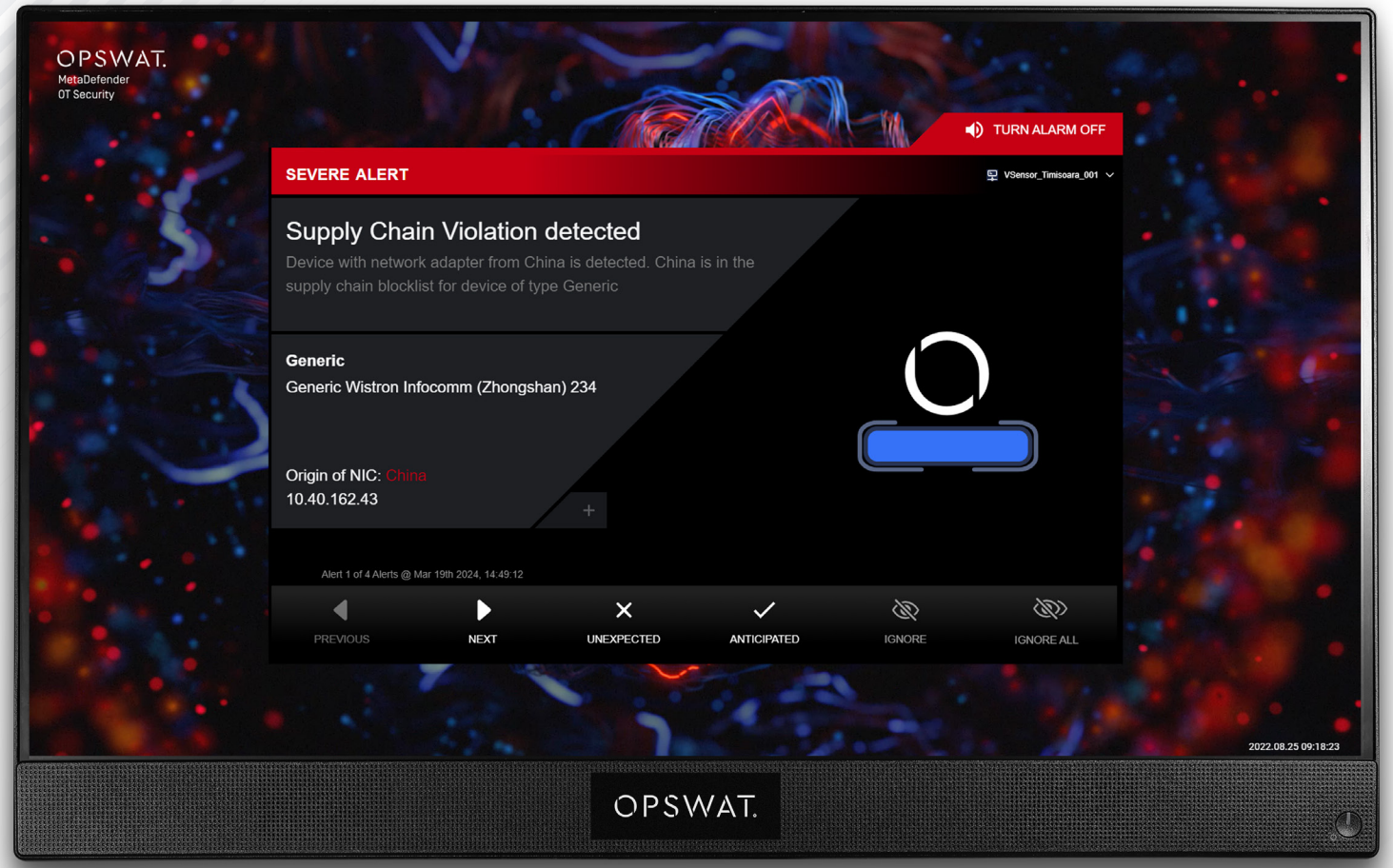
The customizable layout allows for both a macro view of the overall network as well as a detailed look into any single connection.

Granular, role-based access control, ensuring only authorized users have access to specific functions and data.

Different Views to facilitate different focuses

“Cluster” view focuses on connections around a device.

“Purdue model” view provides insight on connectivity through network levels.



Alerts like this supply-chain violation will display with clear action options

CONTINUOUSLY MONITOR NETWORKS TO DETECT THREATS AND ANOMALIES

MetaDefender OT Security continuously monitors ICS networks and triggers alerts on detection of potential threats, vulnerabilities, supply chain violations or non-compliance issues of device and network connectivity. Security policies are either inherited from predefined configurations, self-learning, or manually created, altogether creating a comprehensive detection mechanism for potential threats or operational mistakes.

MetaDefender OT Security helps security professionals and control engineers stay ahead of cyberattacks through prompt, concise, and contextual alert notifications when any security policy violation or network anomaly is detected.

Device's CVEs are detected by MetaDefender OT Security

CONSTANTLY AND OBJECTIVELY ADDRESS OT VULNERABILITIES AND RISKS

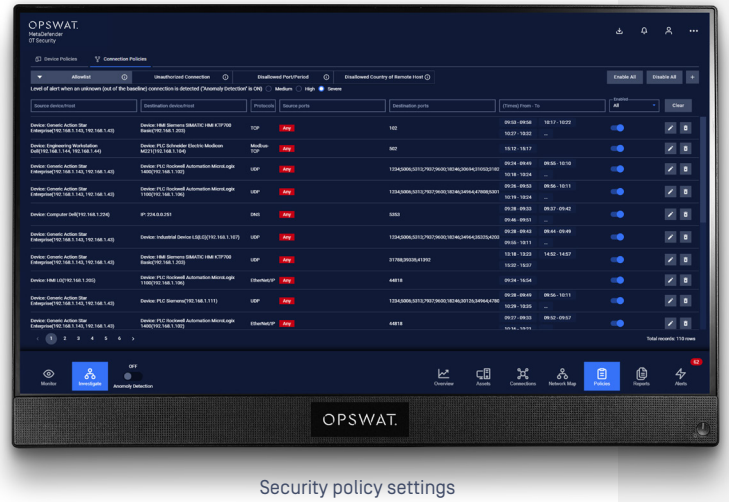
MetaDefender OT Security leverages our team's extensive research in industrial cybersecurity and specific vendor device specifications for finding supply chain risk and vulnerabilities (unpatched CVEs) associated with ICS assets. MetaDefender OT Security also routinely discovers possible misconfigurations such as when a port or service is open but not in use, and improper network segmentation through network connectivity.

Vulnerabilities, supply-chain violations, misconfiguration, threats, or anomalies are employed in MetaDefender OT Security through a proprietary smart algorithm to create a comprehensive Exposure Score. This score is used to measure the exposure (risk) aspect of each asset accurately & objectively on the network.

The exposure score, along with the asset's classified criticality, enables authorized personnel to quickly identify the highest risk for priority remediation before attackers exploit vulnerabilities and cause disruption to operations or even worse damage to the ICS system.

Any change to the asset, either automatically updated by MetaDefender OT Security or manually edited by user/ operator, is recorded with all details. This will help with the audit or regulatory requirements.

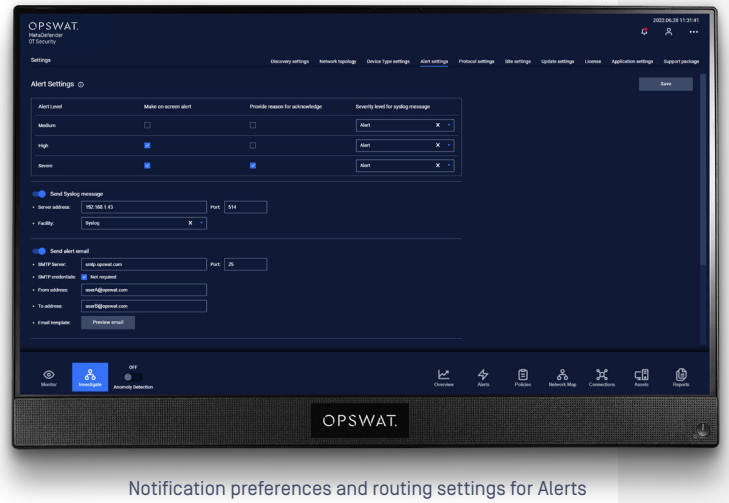
STRUCTURED AND STREAMLINED RISK ALERT WORKFLOW



Security policy settings

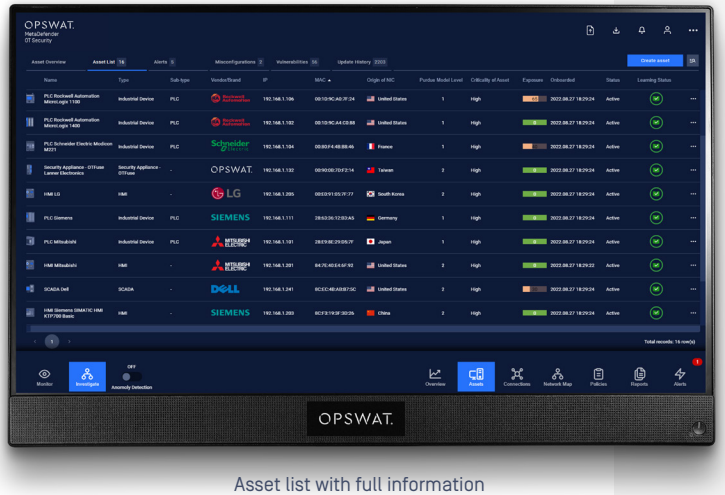
Accurate and timely notifications on cybersecurity incidents or threats are crucial to any OT cybersecurity solution. Equally important are the processes to monitor, collect, classify, and route alerts, for dual (and usually contradictory) purposes. This ensures personnel will not miss a critical incident or report a trivial event.

MetaDefender OT Security enables users to hook alerts to different events, including device types, protocol, device connectivity etc. Predefined policies or allowlists (which MetaDefender OT Security automatically learns) are among the places where alert/ risk is defined.



Notification preferences and routing settings for Alerts

MetaDefender OT Security provides flexibility for all users to monitor and control their organization's cybersecurity. Notifications can be tailored to the appropriate channels so all alerts of all levels can be shown on screen, through syslog, or via emails.



Asset list with full information

Global, Regional and Industry Regulatory Compliance Reporting

MetaDefender OT Security supports global, regional, and industry regulatory requirements for OT cybersecurity such as NERC CIP, NIST, NIS2, NIS Directive, NEI 8-09, ISA/IEC 62443. These compliance and reporting standards help organizations assess and improve their cybersecurity status to meet regulatory requirements.

Customizable dashboards provide overall and quick view of what matters most with regards to OT security

Comprehensive and Customizable Dashboard

MetaDefender OT Security allows for comprehensive visibility into the entire ICS network with quick, summary views on its intuitive dashboard. This unified view eliminates the need for juggling various tools and simplifies network monitoring.

The consolidated threat and anomaly detection resulting from distributed sites empowers centralized analysis and quicker response.

The platform also enables real-time queries on any aspect of the network status which facilitates proactive incident identification and mitigation, reducing downtime.

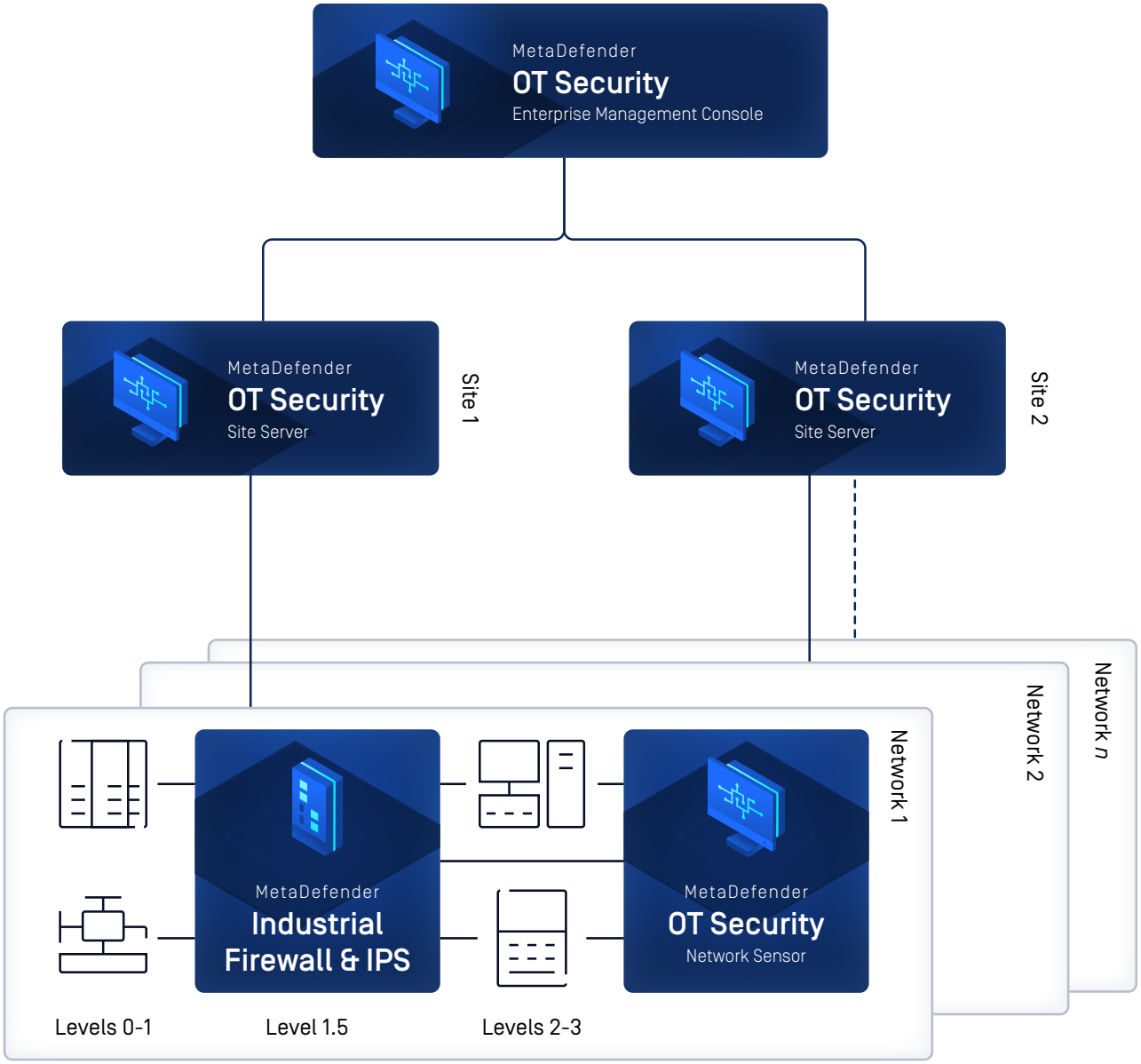
SIMPLE DEPLOYMENT, OT-FRIENDLY AND EASY TO USE

MetaDefender OT Security is built with simplicity and OT-friendliness in mind. The unique dual OT-IT View Mode feature enables the users, either Control Engineers, ICS Operators, or Security Specialists to comfortably work with the system in the most convenient and effective way.

MetaDefender OT Security is super easy to deploy. It takes just five minutes to set up MetaDefender OT Security and gain immediate visibility into your OT environment.

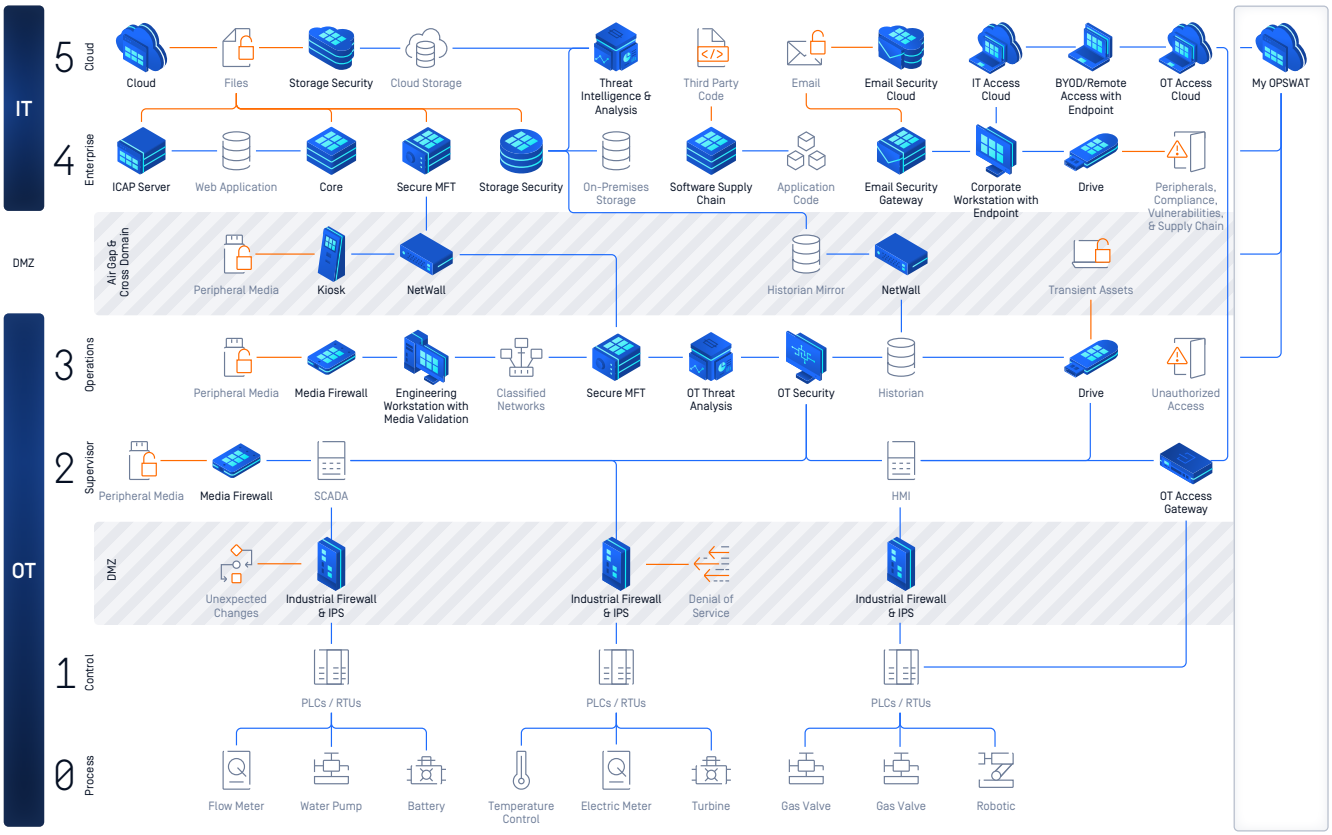
DEPLOYMENT

MetaDefender OT Security can be deployed at the Purdue model level 3 or level 2 of the network. The best deployment scenario is to connect one of its ethernet interfaces to the span (mirror) port of the switch for passive monitoring and connect the other ethernet interface to a normal port for selective smart active probing.



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.



SUPPORTED PROTOCOLS

Our current supported protocols are located below and new protocols are continually added. Connect with OPSWAT for the latest list.

STANDARD OT PROTOCOLS
BACNet
CC-LINK IE Field
CIP
COTP
DNP3
EtherCAT
EtherNet/IP
Genisys
HART IP
IEC 60870-5-104
IEC 61850 (MMS, GOOGSE, SMV)
Modbus TCP
MQTT
OPC UA
Profinet DCP
Profinet IO
Synchrophasor
VNET/IP

IT PROTOCOLS		
ARP	NTP	TDS
CIFS	OpenVPN	TFTP
DCE/ RPC	OSPF	WireGuard
DHCP	POP3	XMPP
DNS	RADIUS	Various tunnel protocols (e.g., GTP, GRE, Teredo, AYIYA, IP-in-IP, etc.)
FTP	RSH/ Rlogin	
GQUIC	RDP	
HTTP	RFB	
ICMP/PING	SIP	
IMAP	SMB	
IPsec	SMTP	
IRC	SNMP	
Kerberos	SOCKS	
LLDP	SSDP	
MQTT	SSH	
MySQL	SSL/ TLS	
NetBIOS	STUN	
NTLM	Syslog	

PROPRIETARY OT PROTOCOLS
BSAP IP
FINS
S7
S7 Plus

OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats. Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,500 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations. Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.

opswat.com/contact