DATASHEET

Mission Secure

Protect Your OT Networks with the Mission Secure Platform.

The first integrated cyber-protection platform for complete visibility, segmentation, protection, and patented signal-integrity monitoring.

Visibility

Identify all connected devices & communications on your OT network.

Segmentation

Segment your OT environment without rearchitecting the network.

Protection

Prevent, alert on, and investigate unauthorized traffic in your OT environment.

Signal-Integrity

Monitor and validate physical process signals to prevent system damage.

How much risk can you afford?

What does a day of downtime and lost production cost you? Isn't it time to stop cyber threats and minimize operational risks?

See how the Mission Secure Platform is different.

$1M - $2B

MISSION SECURE PLATFORM

Visibility

Full visibility means you see every device connected to your OT network and can monitor all traffic. Visibility with a purpose — protection.

- Inventory and manage all OT connected assets
- Monitor OT communications and protocols
- Map your OT environment (both devices and communications)

LEARN MORE

Visibility enablement to lock down your OT environment.

Visibility is only a means to an end. For our clients, that end is minimizing operational risks by stopping OT cyber threats.

Inventory and map connected assets and communications

See and understand what's on your OT network and what specific communications are taking place.

Data and tools for complete OT network control

Gain the insights you need to ensure your OT network is protected against cyber threats.

Proactive monitoring of communications and protocols

Restrict all communications except what is absolutely necessary and authorized.

A solid foundation for cybersecurity protection

Leverage unmatched visibility—the first step to complete OT network control.

MISSION SECURE PLATFORM

Segmentation

Logically segment your OT environment without re-architecting the network, reducing the risk of any material operational cyber event.

- Create security zones throughout the OT network
- Fine-grained controls to lock down unauthorized communications
- Manage or restrict third-party vendor access

LEARN MORE

Limit material impact and exposure in your OT environment.

Logically segment your OT environment without the need to re-architect your network — and control all touchpoints inside and out.

No costly, time-consuming restructuring of the existing network.

Deploy Mission Secure's platform as an overlay to your existing OT network.

Limit your exposure by creating security zones for robust protection.

Segment your network to diminish the risks to critical assets.

Control and restrict third-party vendor access to your network.

Leverage individual zones to control and restrict user access.

Limit the possibility of material impact due to a cyber incident.

Create an OT network environment that's resilient to cyber-attacks.

MISSION SECURE PLATFORM

Protection

Stop cyber threats, reduce the risk of downtime, and minimize alerts by immediately preventing unauthorized activity, keeping your OT environment safe at all times.

- ✓ Protect SCADA, controllers, PLCs, safety systems, and other OT/IoT devices
- ✓ Monitor OT traffic, restrict unauthorized access, and block unknown activity
- ✓ Manage all external communication and prevent unwanted traffic

LEARN MORE

OT security begins with protection.

Stop cyber threats in their tracks before they become an operational issue you have to deal with. Avoid the idea of hiring a “bank monitor” to tell you “the bank is being robbed.”

Safeguard operations and your OT network

Trust that your operations are locked down and will remain reliable against cyber threats.

Stop cyber incidents BEFORE they happen.

Restrict unauthorized access and block unknown, unwanted activity on your OT network. Don’t wait to figure it out later.

Proven fail-safe designs for OT environments.

Even in protect mode, the Mission Secure Platform prioritizes OT network uptime and continues to pass OT traffic under any failure scenario.

Prevention is the best defense against cyber threats.

Stop OT cyber threats, minimize the resource impact to your teams, and protect unpatched older systems now instead of waiting until they can be upgraded.

MISSION SECURE PLATFORM

Signal-Integrity

Patented monitoring of critical Level 0 assets to detect threats before property, plant, or equipment damage can occur.

- ✓ Micro-segment key Level 0 assets and processes creating zero trust zones
- ✓ Tamper-proof, third-party monitoring of critical physical process electrical signals
- ✓ Validate signal integrity from process to controller to HMI

LEARN MORE

Tamper-proof, “last line of defense” cybersecurity for the most critical assets in your operation.

Patented cyber protection to prevent operational, property, and equipment damage when all other cybersecurity measures fail.

Assurance that your process is running the way it’s reading.

Eliminate the possibility your operational data is wrong, or worse yet, spoofed. Restore operator confidence and trust with Mission Secure.

Third-party validation that your controllers are relaying accurate information.

The days of manually checking sensor and process readings are gone. Mission Secure monitors and validates process readings to remove all doubt.

Create micro-security zones around critical processes.

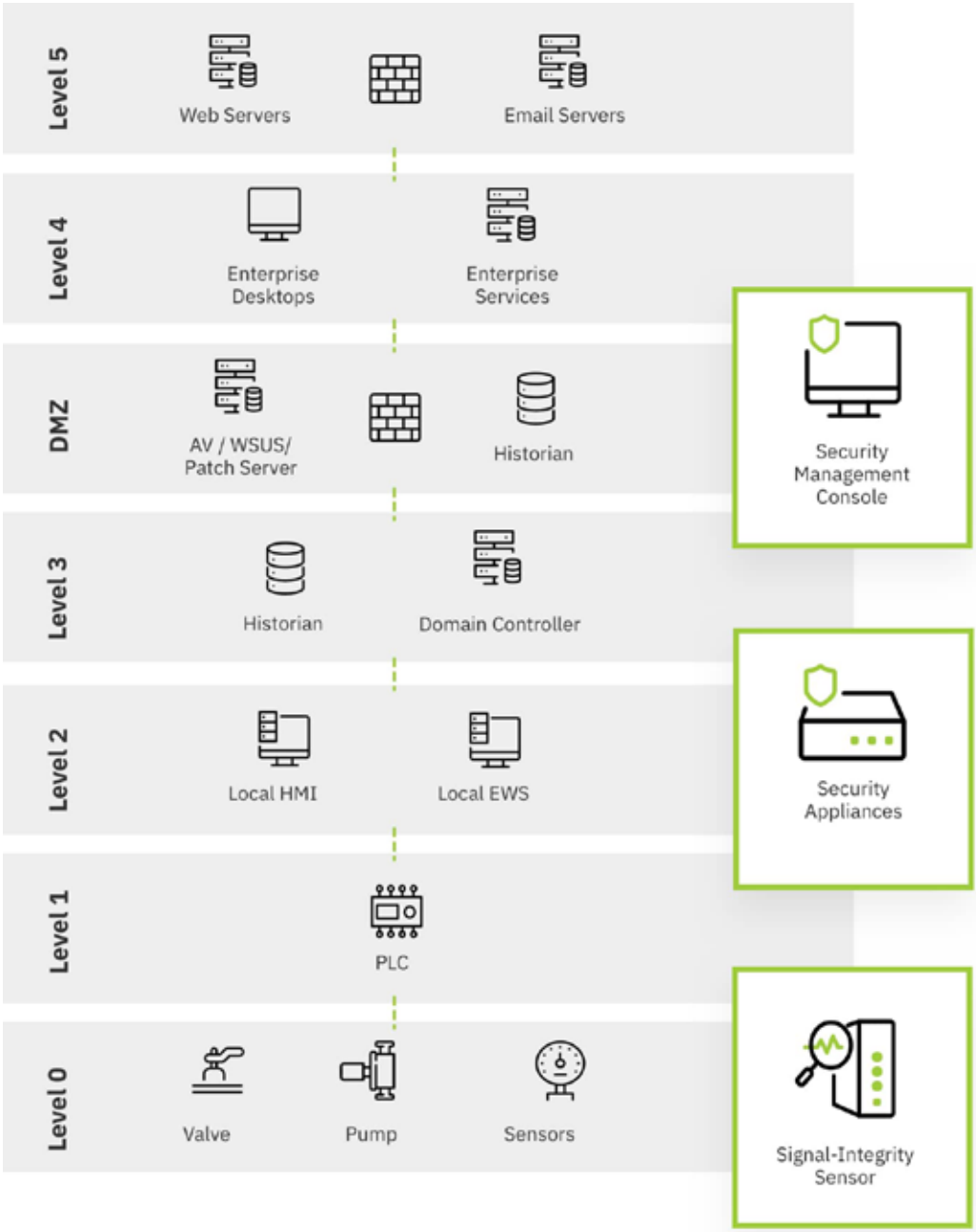
Virtually segment individual processes and implement a zero-trust security model where it matters most in your operations.

True OT security for your OT network.

Directly monitor raw electrical OT asset signals from critical processes with our military-strength, industrial-grade security platform.

Purdue Model Deployment Example

The Mission Secure Platform easily deploys in a wide range of operational technology (OT)/ ICS network environments, providing control system visibility, segmentation, and protection at Purdue Model Levels 0, 1, 2 and 3 with a combination of Security Appliances and Signal-Integrity Sensors and local management using the Security Management Console.



Security Management Console

Central Management

Rack-mounted appliance for centralized management of multi-tier, distributed deployments. Primary user interface for visibility, and used to manage segmentations, protections, and signal-integrity monitoring.

Front

Rear

TECHNICAL SPECIFICATIONS

Max. Managed Appliances	75
Max. Throughput	1 Gbps
Management Ports	2 x 1GbE
Expansion Slots	Up to 4 x 3.5 hot-plug SATA
Storage	1 TB
Form Factor	1 rack unit
Max. Power Consumption	350W
Power Supply	Dual, hot-plug, redundant power supply 100-240V AC autoranging - 50/60 Hz
Temperature Range	Storage: –40°C to 65°C (–40°F to 149°F) Continuous operation: 10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment.
Chassis Dimensions	Width: 434.00mm (17.08 in) Depth: 595.63mm (23.45 in) Height: 42.8mm (1.69 in)
Chassis Weight	13.6 kg (29.98 lb.)

Security Appliance

Visibility, Segmentation and Protection

DIN rail or flat surface mounted. Deploys on a SPAN port, network Tap or inline. Passively monitors OT traffic on the IP network, and provides network segmentation and protection of OT assets.

TECHNICAL SPECIFICATIONS

Enclosure Material	Black powder coated formed steel
Install Options	DIN rail or flat surface
Physical Ports	1xMSTB 2 Power connector 2xGigabit RJ45 1x100MB Management Port
Indicator Lights	Power/FailSafe status Ethernet port status
Power Requirements	12-24 V DC 0.5A
Operating Temperature	-20C to +75C
Marks and Certifications	DEMKO 20 ATEX 2389X II 3 G EX ec nC IIC T4 Gc IND CONT EQ FOR HAZ LOC CL I, Div. 2, Grp A, B, C, D E514376 UL LISTED CE
Dimensions	32.2mm H x 150.0mm W x 106.3mm D
Weight	550.0g (19.3 oz.)
Security	Hardened OS with kernel module signing, multiple security controls and tested using 3rd party security audits

Signal-Integrity Sensor

Continuous Signal-Integrity Monitoring

DIN rail or flat surface mounted. Deploys on an analog signal splitter or digital IO contacts. Passively monitors electric signals at the physical level (Level 0) to detect changes that may indicate possible compromise or failure.

TECHNICAL SPECIFICATIONS	
Enclosure Material	Polyamide plastic
Install Options	DIN rail or flat surface
Physical Ports	1xMSTB 2 Power connector 1xGigabit RJ45 2xAnalog Inputs (V1 & V2) 0-10V 2xAnalog Inputs (A1 & A2) 4-20mA 2xDigital Inputs (D1 & D2) 0-51V
Indicator Lights	Power, I/O, network status/activity
Power Requirements	12-24 V DC 0.5A
Operating Temperature	-20C to +75C
Marks and Certifications	pending
Dimensions	122.5mm H x 114.4mm W x 25.0mm D
Weight	170.0g (6 oz.)
Security	Hardened OS with kernel module signing, multiple security controls and tested using 3rd party security audits

Mission Secure

Mission Secure

Stop OT Cyber Threats Head-On

Mission Secure is setting a new standard in OT cyber-protection stopping OT cyber threats head-on. The Mission Secure Platform backed by 24/7 Managed Services is the first to seamlessly integrate OT visibility, segmentation, protection, threat hunting, and incident response, delivering military strength, industrial grade OT protection. With Mission Secure, defense, critical infrastructure, and process industry customers keep critical operations up and running and safe from harm.