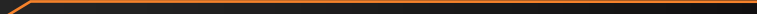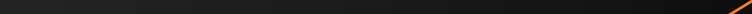# Industrial Defender Platform

Industrial Defender safely collects, monitors and manages ICS asset data at scale, providing the essential foundation to apply ICS security controls effectively.

INDUSTRIAL DEFENDER®

Industrial Defender Platform

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY MANAGEMENT

Multiple vendor systems, geographically dispersed plants and hard-to-reach endpoints make it difficult to effectively monitor, manage and protect process control networks. Traditional IT enterprise solutions can be demanding of already limited computing resources and often fail to fully address the cybersecurity needs of operational environments. Industrial Defender is an industry leading solution for security, compliance and operations of control systems environments.

By combining multiple applications on a single platform, it provides a consolidated real-time view to secure and manage your control systems environment. From ultra-low bandwidth requirements to proprietary protocols Industrial Defender was designed and built from the ground up to ensure security, safety and reliability of your control systems. Certified to maintain performance standards by multiple control systems vendors, Industrial Defender is the only platform to offer applications specifically engineered to address the overlapping requirements of cybersecurity, compliance, and change management.

Industrial Defender can be deployed either as a dedicated appliance or optionally as a Virtual Machine (VM) providing aggregation, analysis, visualization, alerting and reporting to security teams.

Product Overview

- Product and service solutions for ICS cybersecurity

- Centralized asset repository with automated notification of changes to assets

- Automated data collection for compliance with internal requirements, industry standards, and external regulations

- Consolidated change approvals, documentation and reports within defined project work packages

- Customizable dashboards support different user profiles

- Deployed with no disruption to operations via appliances or software on VM's
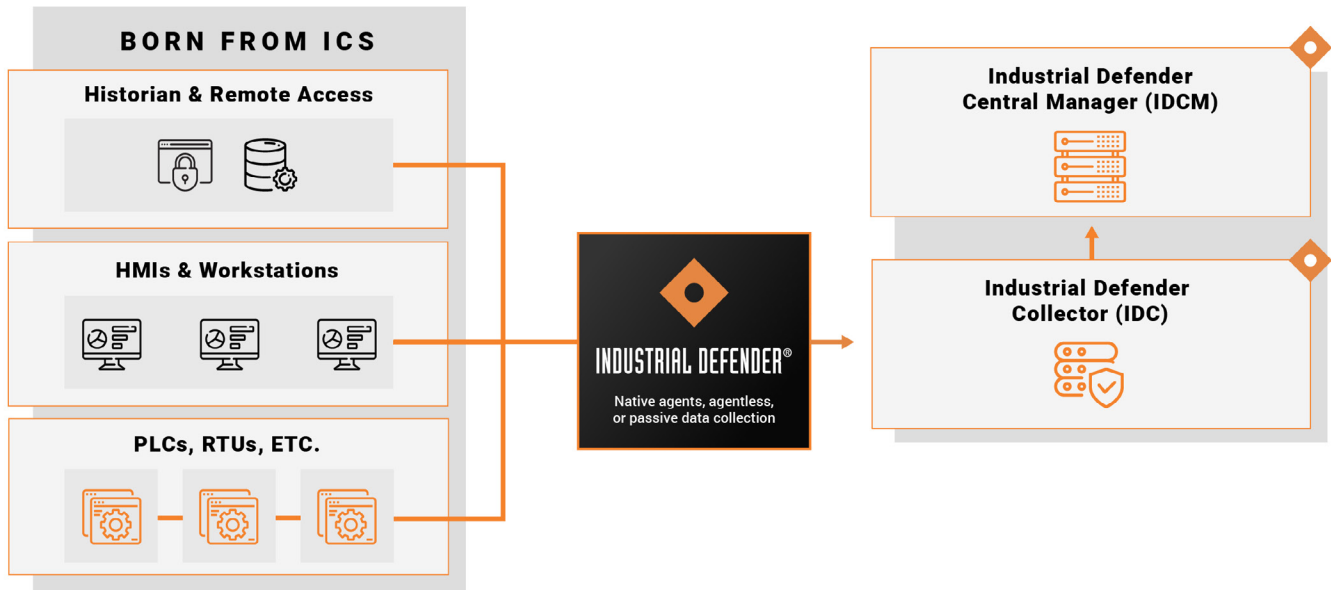
INDUSTRIAL DEFENDER®

💎 Key Benefits

- Visualize control system assets and network communications with our asset topology map

- Drill down into individual asset health to monitor trends, manage events and investigate anomalies

- Quantify risk for individual assets with The Endpoint Risk Analytics Suite, which offers a transparent scoring methodology and scores for four different threat vectors

- Automate asset configuration collection and on-demand vulnerability management

- Monitor systems performance, including application and process failures, registry and file changes

- Detect security events across your asset base and at your perimeter to take decisive action when vulnerabilities and threats are identified

- Ease user, patching and policy management

- Reduce total cost of ownership (TCO) with multiple applications on a single platform

- Improve accuracy and efficiency of compliance reporting with automated data collection and archival of artifacts relevant to regulatory requirements

- Leverage ready-to-go NERC CIP, NIST and NEI 08-09 policy libraries along with the Work Automation Suite to automate the collection, storage and reporting of compliance artifacts for audit requirements.
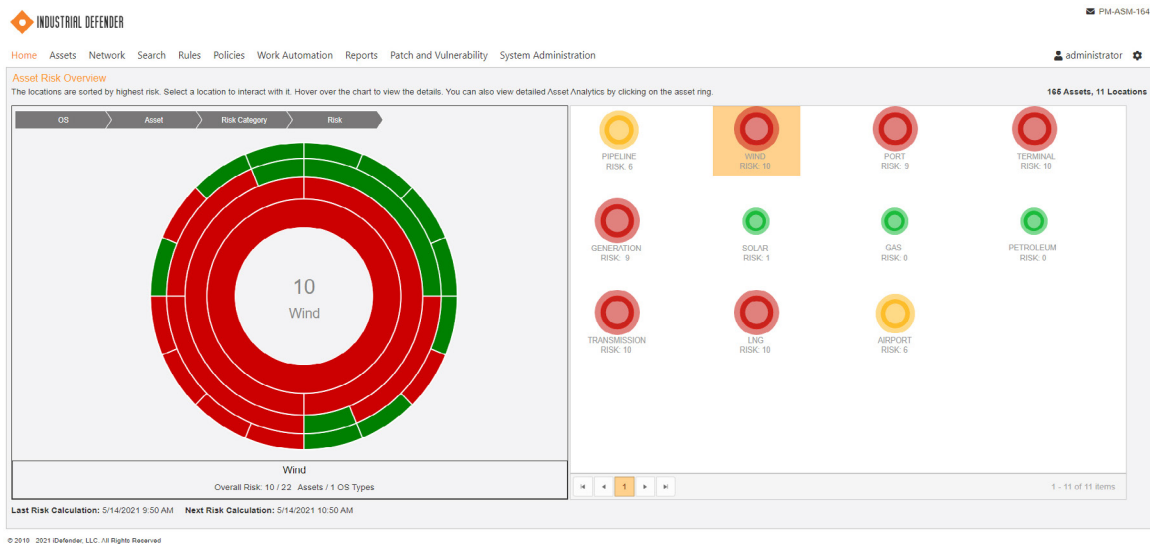
The Endpoint Risk Analytics Suite

INDUSTRIAL DEFENDER®

Industrial Defender Architecture

Industrial Defender Components

The Industrial Defender infrastructure consists of two interrelated components:

- **Industrial Defender Central Manager (IDCM)**

- **Industrial Defender Collector (IDC)**

This infrastructure can be deployed at your locations with no disruption to operations and no reboot required. The vendor-agnostic solution is tuned to collect data from over 100+ industrial endpoints – including those hard to reach RTUs, IEDs, and PLCs – and report on baseline deviations, alert on priority security events and flag policy violations. With up-to-date information operators can confidently manage users, compliance reporting, patches, security events and incident response from a single, unified view.

INDUSTRIAL DEFENDER®

Industrial Defender Central Manager (IDCM)

The IDCM can be deployed either as a dedicated appliance or optionally as a Virtual Machine (VM) providing aggregation, analysis, visualization, alerting and reporting to security teams. Once the appliance is turned on, users can immediately start receiving data out-of-the-box without complicated set up or third party integrations, like a well-tuned control system.

IDCM Appliance Specifications

Platform Feature	Normal Throughput	Extreme Throughput
Rack Configuration	2U Server	2U Server
Processor	2 x Intel® Xeon®; 8 core; 1.7 Ghz	2 x Intel® Xeon® E5 v3; 8 core; 2.6 Ghz
Memory	48GB DDR4-2666	384GB DDR4-2666
Network	4 x 100/1000/10GBase-T	4 x 100/1000/10GBase-T
Network Adapter	RJ-45 Copper	RJ-45 Copper
Storage	14 x 960GB SSD SATA drives	14 x 1.9TB SSD SATA
Data Storage Method	RAID-1 and RAID-6	RAID-10
USB	4 x USB, 1 x Serial	4 x USB, 1 x Serial
Drive Insertion Strategy	Hot Swap	Hot Swap
Video	Integrated VGA	Integrated VGA
Power Supplies	Dual, Hot-Swappable	Dual, Hot-Swappable
Power Input	100—240 VAC; 50-60Hz	100—240 VAC; 50-60Hz
Power Output	920 Watts	920 Watts
BTU Output	3137 BTU/Hour	3137 BTU/Hour
Mechanical Cooling	Fan cooled; redundant fans	Fan cooled; redundant fans
Dimensions (H X W X D)	3.5 x 17.2 x 24.8 in.; 89 x 437 x 630 mm	3.5 x 17.2 x 24.8 in.; 89 x 437 x 630 mm
Weight	61 lbs; 27.7 Kg	61 lbs; 27.7 Kg

INDUSTRIAL DEFENDER®

Industrial Defender Collector (IDC)

The Industrial Defender Collector (IDC) monitor all network traffic within the control network security perimeter, enabling detection of internally generated attacks, as well as any attacks that may have circumvented perimeter defenses. The IDC includes the ability to monitor industry standard protocols used by process control systems such as Modbus TCP, DNP3, Profibus, ODVA Ethernet/IP, and ICCP, and generate alarms that are sent to the IDCM for logging and diagnosis.

IDC Appliance Specifications

Platform Feature	Normal Throughput	Extreme Throughput
Rack Configuration	1U Appliance	1U Appliance
Processor	Intel® Xeon® Silver; 8 cores; 1.8 Ghz	Intel® Xeon® Scalable Bronze; 6 cores; 1.7 Ghz
Memory	48GB DDR4-2666	96GB DDR4-2400
Network	2 x 100/1000/10GBase-T; 4 x 10/100/1000Base-T	8 x 100/1000/10GBase-T
Network Ports	RJ-45 Copper	RJ-45 Copper
Storage	1 x 960GB SATA SSD	2 x 960GB SATA SSD; RAID-1
USB	4 x USB; 1 x Serial	2 x USB; 1 x Serial
Drive Insertion Strategy	Fixed	Hot Swap
Video	Integrated VGA	Integrated VGA
Power Supplies	Single, auto-sensing	Redundant pair, auto-sensing; Hot swappable
Power Input	100—240 VAC; 50-60Hz	100—240 VAC; 50-60Hz
Power Output	350 Watts	750 Watts
BTU Output	1200 BTU/Hour	2,560 BTU/Hour
Mechanical Cooling	Air Cooled, 2 x fans	Air Cooled, 8 x heavy duty fans
Dimensions (H X W X D)	1.7 x 17.2 x 14.5 inches; 43 x 437 x 368 mm	1.7 x 17.2 x 28.5 inches; 43 x 437 x 724 mm
Weight	14 lbs; 6.35 Kg	26 lbs; 11.8 Kg

INDUSTRIAL DEFENDER®

THE INDUSTRIAL DEFENDER DIFFERENCE

Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while providing cross-functional teams with a unified view of security. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. They secure some of the largest critical control system deployments with vendors such as GE, Honeywell, ABB, Siemens, Schneider Electric, Yokogawa and others to protect the availability and safety of these systems, simplify standards and regulatory requirements, and unite OT and IT teams.

Planning an OT Security Project?

SCHEDULE A DEMO

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com

225 Foxborough Blvd, Foxborough, MA 02035

industrialdefender.com

INDUSTRIAL DEFENDER®