INDUSTRIAL DEFENDER®

SOLUTION BRIEF

Safely Collect, Monitor & Manage OT Asset Data at Scale

THE CHALLENGE

Effective Cybersecurity Management for Industrial Control Systems

Multiple vendor systems, geographically dispersed plants and hard-to-reach endpoints make it difficult to effectively monitor, manage and protect control networks. Traditional IT security tools don't work inside these environments, yet IT teams still need to understand what is going on with OT assets to effectively protect them from cyber threats. Because of this, building an effective and sustainable ICS cybersecurity program can feel like an overwhelming task.

INDUSTRIALDEFENDER.COM ➤

THE SOLUTION? INDUSTRIAL DEFENDER ASM

Our solution is made specifically for complex industrial control system environments to protect the availability and safety of these systems, while also simplifying compliance requirements. Easy integrations into the broader security and enterprise ecosystem also empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks.

KEY BENEFITS

- Create a solid foundation to apply effective OT security controls using an asset-centric methodology for endpoint data collection and normalization.
- Mitigate cyber threats quickly with actionable security data from passive, on-demand vulnerability monitoring.
- Enhanced IT and OT collaboration with integrations that deliver enterprise-level visibility, access and situational awareness into critical ICS environments.
- Automate standards and regulatory compliance with built-in policy and reporting templates for standards like NERC CIP, NIST and the NIS Directive.

Industrial Defender ASM Use Cases

Asset Management

Knowing what you have in your environment is the first step to securing it. The ASM provides a single view into your OT asset base. The Endpoint Risk Analytics Suite provides a graphical representation of your assets with the ability to drill down into individual asset health and provides a detailed risk score for each.

Security Event Management

Our event management engine delivers an unprecedented level of visibility and actionable security data to provide the foundation for a sustainable security program. By collecting, normalizing, and analyzing the vast amount of information provided by your control systems in one place, you can easily keep track of the security events that really matter.

Features & Capabilities

- Unified view of control systems cybersecurity, operations, and compliance management
- Quantification of cyber risk with the Endpoint Risk Analytics Suite
- Vulnerability monitoring and notifications
- Real-time monitoring of changes across asset base, systems health and performance, and network traffic
- Scalable architecture, virtual machines to dedicated appliances
- Interoperability with 3rd party security technologies
- Default policies and reporting templates for NERC CIP, NIST, NIS Directive, and NEI 8-09
- Event logging, correlation and archiving

Configuration Management

Automatically collects, normalizes, and reports changes affecting your control systems environment, regardless of vendor or location. You can easily create asset baseline configurations that our change detection engine compares with actual asset configuration data including ports and services, users, software, and patches and firewall rules.

Policy Management

Provides you with an easy way to create, deploy, and audit compliance with policies across your control systems environment. As a vendor-agnostic solution, policies can be written and applied to multiple assets, saving time and effort. We even include standard policies for NERC CIP, Nuclear Energy Institute (NEI) 08-09 and the NIST standards.

Compliance Reporting

With a suite of built-in standard reports, including NERC CIP, NIS Directive and NIST CSF reporting packages, the ASM eliminates the manual task of data collection and report generation. The reporting application lets you configure report subscriptions for non-privileged users and send them via email, server share, and SharePoint, to ensure the delivery of real-time information to those who need it the most.

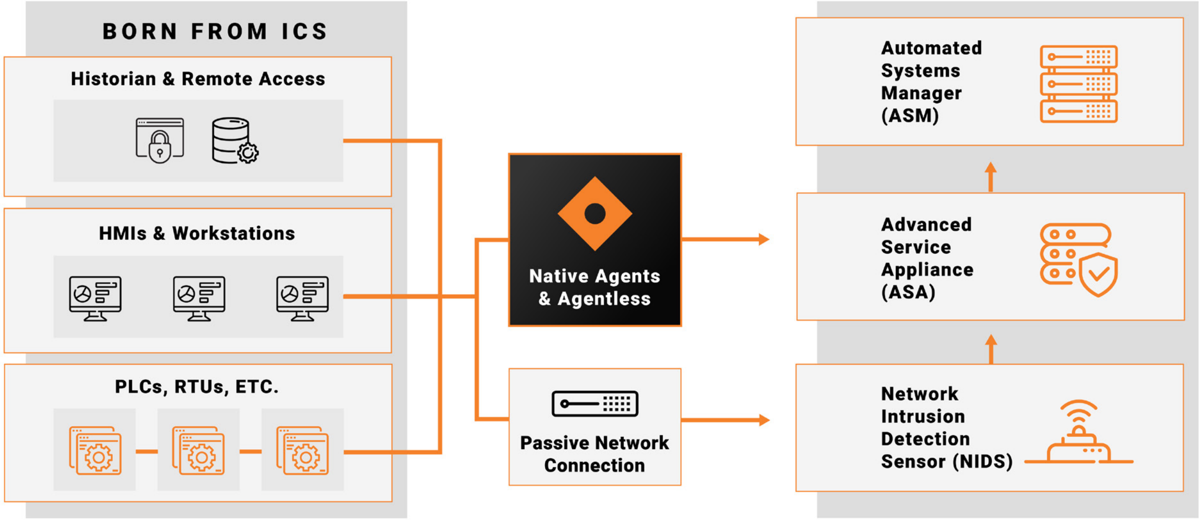
Workflow Automation

This optional application suite integrates document management and reporting as part of a structured workflow. You can improve operational efficiency by initiating, tracking, approving, documenting, and reporting on changes made to control systems assets automatically and store all documents related to a change, like emails, test approvals, and configuration files, in one place.

Vulnerability Monitoring

Our vulnerability monitoring combines the power of asset management with the accuracy and completeness of NIST's vulnerability database. This feature reports a current list of the potential Common Vulnerabilities and Exposures (CVEs) associated with your asset inventory and provides information on patches available for these vulnerabilities.

Industrial Defender ASM Architecture


BORN FROM ICS
Historian & Remote Access
HMIs & Workstations
PLCs, RTUs, ETC.
Native Agents & Agentless
Passive Network Connection
Automated Systems Manager (ASM)
Advanced Service Appliance (ASA)
Network Intrusion Detection Sensor (NIDS)

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.

SCHEDULE A DEMO

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com
225 Foxborough Blvd, Foxborough, MA 02035
industrialdefender.com