Industrial Defender Automation Systems Manager (ASM)

Ensuring security, compliance and change management

Make the most of your energy℠

Schneider Electric™

Industrial Defender Automation Systems Manager (ASM)

Operational system complexity, interconnectivity, exponential increases in intelligent field devices, and ever-tightening regulatory requirements have put intense pressure on Industrial Control Systems (ICS) professionals tasked with keeping production assets and systems up and running.

Cyber attacks targeting critical infrastructure and control systems have increased dramatically — over 400 percent in the past year alone, according to the Department of Homeland Security's ICS-CERT Incident Response Summary Report. At the same time, these organizations have a growing number of endpoints connected to the corporate network and the Internet, presenting both security and change management challenges, while simultaneously facing increased regulatory oversight. To help clients meet these challenges, Schneider Electric has partnered with Industrial Defender to offer a best in class solution, Automation Systems Manager (ASM), which holistically addresses security, compliance and change management activities.

ASM

With an exclusive focus on operational technology, ASM includes a suite of software and hardware solutions that help ICS professionals to ensure the reliability of their automation systems and key industrial processes. ASM provides these capabilities by correlating data throughout processes and technologies, and then leveraging it across security, compliance and change management activities.

One view

ASM is fully interoperable with Schneider Electric SCADA and DMS solutions. It provides a single, unified view into heterogeneous automation systems, including legacy systems, to enhance operational efficiency. Industrial Defender solutions are built from the ground up to protect automation system environments from internal and external threats. They also automate the process of documenting compliance with external regulations and internal performance requirements. With them, companies have effective and unified ways to meet their rapidly-growing change management requirements.

> Our best in class solution, ASM , which holistically addresses security, compliance and change management activities.

ASM applications

With this powerful tool, operators can maximize availability, reliability and safety levels. It includes applications for:

- Asset management: offers a single, unified view of all assets within the automation system's environment. It enables on-boarding and decommissioning of assets, while reporting device status, information access and state information. It also provides a snapshot of the control network and automatically detects when new devices connect to the network, alerting operators.

- Event management: provides event log data for additional control system and network visibility. It also receives and consolidates events from multiple security sources, centralizes operations and reduces costs for monitoring multiple systems.

- Configuration change management: enables operators to track and audit device settings, applications, firewall rules and user accounts. Operators can view and baseline system configurations, ports, services and software.

- Policy management: allows operators to communicate new policies, track acceptance and manage conformance.

- Reporting: meets regulatory requirements, including NERC CIP, and simplifies adherence to internal policies. Users can define, generate and automate standard, configurable reports, as needed.

Integrated solutions

ASM is available in two fully-integrated solutions, including software, hardware, and complementary services.

- **Monitor** collects event data from industrial endpoints and provides centralized event logging capabilities, while consolidating log data for analysis and forensics.

- **Manage** builds on Monitor and offers unmatched capabilities for data capture from automation systems. It automatically collects configuration data from heterogeneous industrial endpoints, tracks changes to configurations, software, patches and user accounts, while providing automated policy management and exception identification.

A strong partner

Schneider Electric's partner, Industrial Defender, is the global leader in security, compliance and change management solutions for industrial control systems. The company has more than a decade of experience dedicated to ICS cybersecurity, and has completed more than 10,000 global technology deployments to secure critical infrastructure systems in 25 countries. Its clients include many Fortune 100 companies.

ASM Capabilities

	Monitor	Manage
Event logging, correlation, and archiving	●	●
Asset management	●	●
Single, unified view across disparate endpoint base	●	●
Customizable user interface dashboards	●	●
Scalable architecture	●	●
Configuration change management		●
File integrity		●
Network traffic monitoring		●
Report subscriptions		●
Critical process and service monitoring		●
User account change identification		●
Device configuration file archiving		●
Understand network and system health and performance		●
Maintain central configuration policy		●
Collect and report on settings, accounts, and configurations		●
Analyze changes across asset base and environment		●
Manage hardened electronic security perimeter		●

July 2013