SOLUTION BRIEF

Fortinet and Industrial Defender Operational Technology (OT) Visibility and Protection

Security, Change Detection, and Compliance for (OT) Environments

Executive Summary

By monitoring Fortinet devices with the Industrial Defender ASM management platform, users get real-time visibility into firewall rule changes, mission-critical network settings, and reports on compliance posture within a single platform. Industrial organizations can significantly enhance ISA-62243, National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), or American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) implementations with audit-friendly reporting of configuration changes and events for all your OT assets, including all components of the Fortinet Security Fabric.

Joint Solution Components

- Industrial Defender ASM solution
- Fortinet Security Fabric
- FortiOS Devices
- FortiSIEM

Joint Solution Benefits

- Monitor and manage configuration changes
- Quickly detect and remediate cybersecurity events
- Mitigate risk from hardware and software-based vulnerabilities

FORTINET Fabric-Ready

The Challenge

OT infrastructure has never been more vulnerable to cybersecurity incidents than they are today, either from directed attacks or just casualties of bigger malware campaigns. These networks are often not supervised by the core IT network and security teams, but often support the most critical aspects of a company's business. To make matters worse, the number of OT devices are vastly increasing and networks often lack defense in depth against these attacks and are ever more reliant on network protections to defend themselves. It is critical to implement proper microsegmentation and constantly monitor for anomalous activity. Additionally, the ability to report on configurations across the entire spectrum of often disparate networks is critical to prioritizing remediation against the newest daily threat.

The Joint Solution: Fortinet and Industrial Defender

To address these challenges, Industrial Defender and Fortinet are partnering to deliver critical security and visibility capabilities for OT environments. These application programming interface (API) integrations will combine advanced network protection and enforcement from Fortinet with OT security and asset and configuration management from Industrial Defender. The integration of the Industrial Defender ASM product and Fortinet Security Fabric devices is enabled through proprietary security event monitoring, configuration data collection, and change detection for critical settings and data points within the OT environment. Additionally, all critical security data for the entire OT environment can be shared with a FortiSIEM, enabling companies to achieve visibility into critical OT operations in the SOC.

Joint Solution Components

1. Industrial Defender ASM solution
2. Fortinet Security Fabric
3. FortiOS Devices
4. FortiSIEM

How It Works

Industrial Defender ASM periodically collects configuration data about firmware, software, ports, services, firewall rules, and users from Fortinet Security Fabric devices and monitors them for changes. In addition to configuration data, ASM can monitor security events generated by Fortinet Security Fabric devices and correlate them with configuration changes to give real-time visibility into how network infrastructure is changing, who changed it, and why.

Joint Use Cases

Change Detection for FortiGate, FortiSwitch, and FortiManager Devices

Monitoring for configuration changes, security events, vulnerability detection, and compliance reporting of Fortinet devices with Industrial Defender ASM gives visibility into changes being made to the firewalls in the environment. With the ASM you get centralized visibility into all the firewall rules being used in your environment and alerts for if and when they change.

- Track which users have access to these devices, as well as when they logged in and the configuration changes they may have made.
- Monitor the software and firmware installed in the firewall to know exactly when it changes and who changed it.
- Inspect the firewall for software and firmware-based vulnerabilities using the ASM vulnerability monitoring service.
- See network changes like a new interface on a FortiSwitch or changes like a virtual local-area network (VLAN) configuration in real time.
- Correlate changes being made by FortiManager on the devices it is managing.

In addition to real-time monitoring, ASM provides forensic reports of the changes for security teams' analysis and compliance-based reports for evidence during audits.

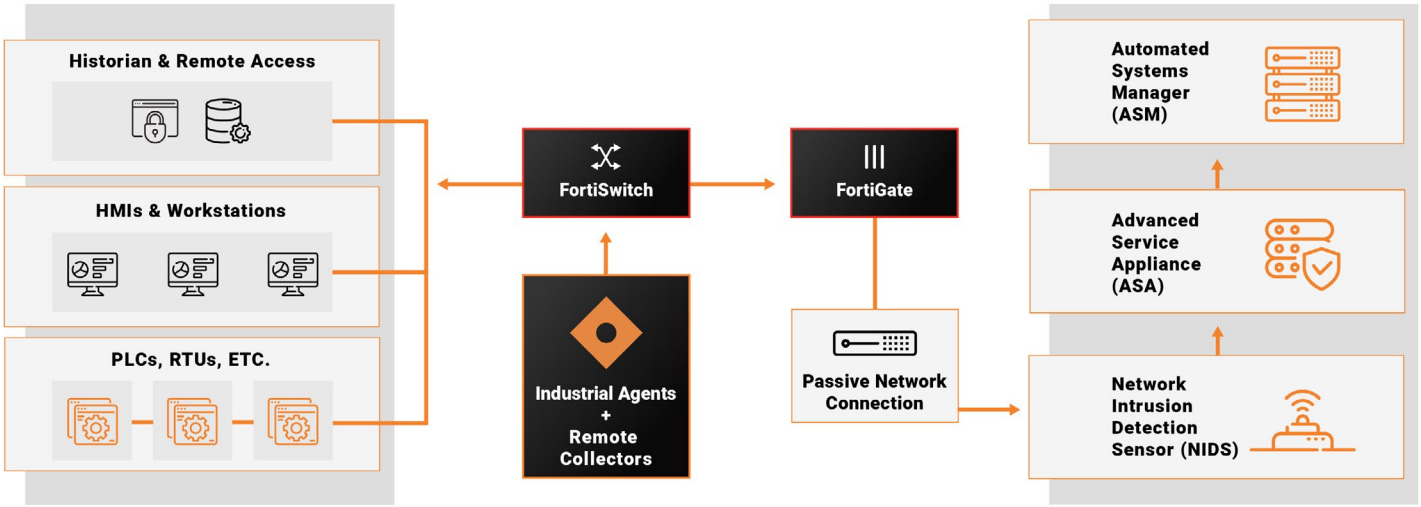

Figure 1: Securing and monitoring an OT environment with Fortinet and Industrial Defender.

Integrating ASM Security Data Into FortiSIEM for IT/OT Collaboration

SOC teams struggle to get valuable, actionable intelligence from OT networks and devices. Industrial Defender has over a decade of experience in collecting data from hard-to-reach, sensitive OT devices, as well as the nonstandard protocols used in OT. ASM employs a vendor-agnostic hybrid monitoring approach using industrial agents, remote collectors, and deep packet inspection to give unprecedented visibility into 200+ unique devices that are found in OT networks. Visibility into these devices, their security events, configuration changes, and vulnerabilities is passed along to FortiSIEM to provide SOC analysts with insight into OT operations to reduce the mean time to remediation (MTTR) of security investigations.

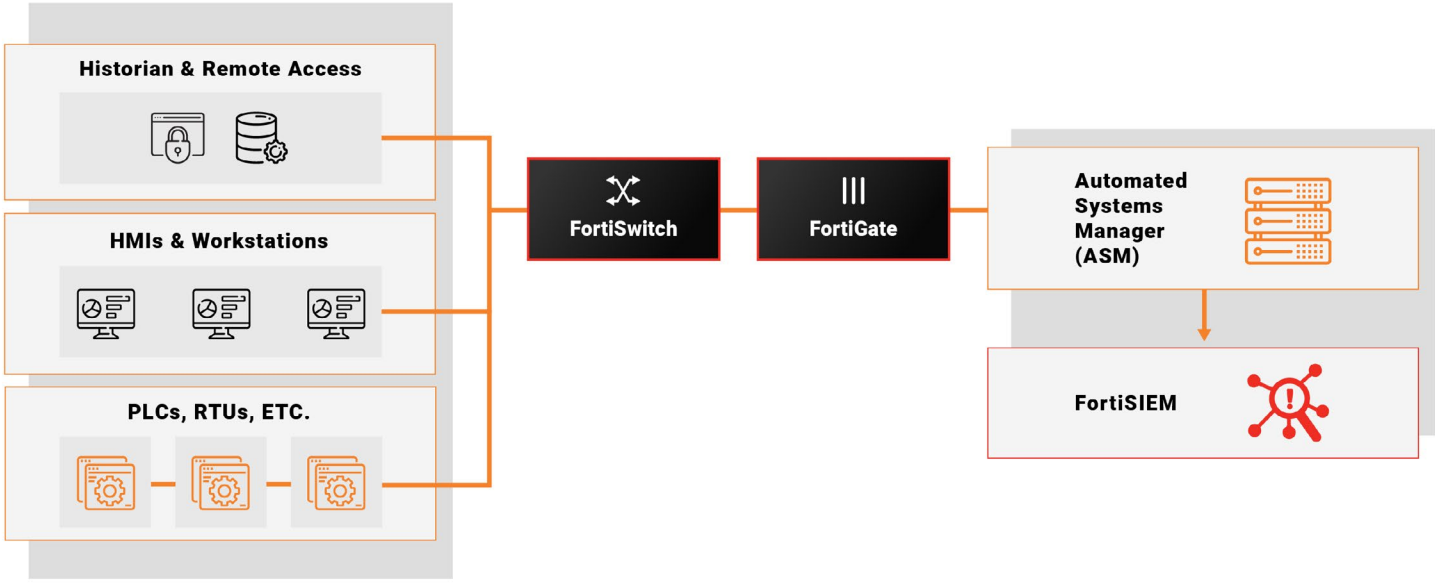

Figure 2: SOC enablement for IT/OT convergence.

About Industrial Defender

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. Learn more at www.industrialdefender.com.

February 11, 2021 8:10 AM

123456-0-0-EN

D:\Fortinet\2020 Old templates\Solution Brief\Grey Solution Brief\Industrial Defender\sb-fortinet-and-industrial-defender-operational-technology-V1-2112021\sb-fortinet-and-industrial-defender-operational-technology-V1-2112021