SOLUTION BRIEF

Fortinet and OTORIO Security Solution

Secure Industrial IT/OT Convergence Through Automated Security Orchestration and Response

Executive Summary

As industrial internet technology (IT) and operational technology (OT) systems converge, creating an ever-connected, modernized production floor, organizations are facing expanded attack surfaces. The more digitally advanced an organization becomes, the more susceptible it is to cyberattacks, making secure digital operations a top challenge facing the industry today.

Fortinet and OTORIO have established a technology partnership to address this challenge and enable secure industrial growth with the Fortinet FortiGate next-generation firewall (NGFW) and FortiSIEM with RAM², the OTORIO Industrial security orchestration, automation, and response (SOAR) platform. Customers benefit from advanced cyber risk management capabilities from OTORIO, while leveraging the best validated security protection in the industry from Fortinet.

The Fortinet and OTORIO Joint Solution

The OTORIO RAM² platform automates security orchestration and response by integrating with leading security systems. Together, RAM² and FortiGate provide continuous cyber risk assessment of the OT network using Fortinet Security Fabric application programming interfaces (APIs). The OTORIO security engine correlates events from FortiGate with data and events from multiple security and industrial systems to generate insights about how to prevent risk and alert about security incidents that may otherwise be missed. The OTORIO RAM² platform empowers the security operations team to immediately and intelligently mitigate threats, while the generated alerts enrich FortiSIEM and secure converging OT and IT environments.

OTORIO Product Name and Description

OTORIO RAM² is a centralized, simplified, and automated industrial cyber risk management solution. It is an unparalleled SOAR platform, drawing from industrial and security data sources to automate and coordinate converged IT/OT security tasks for rapid remediation and response. The RAM² platform easily integrates with a variety of production floor data:

- **Nonintrusive**, meaning it does not interfere with production by utilizing existing solutions
- **Industrial native design specifically for operations**, considers the business impact while simplifying security tasks
- **Risk impact assessment** of operational and business impact for operations and management
- **Improved collaboration** between operational and cybersecurity teams
- **Unified tool for the operational team** centralizes OT security systems in one place

Joint Solution Components

- Fortinet Next-generation Firewall (NGFW), FortiSIEM
- OTORIO RAM²

Joint Solution Benefits

- Secures IT/OT convergence by integrating OTORIO OT alerts with FortiSIEM
- Provides firewall segmentation assessments based on contextual attack graph simulation
- Improves operational continuity with ongoing OT risk assessment and risk reduction
- Bridges the OT security skills gap through automated mitigation steps
- Offers practical remediation actions that minimize production interference (e.g., patching on the production floor)

FORTINET FABRIC-READY

- **Full visibility** into production floor status
- **Prioritized, actionable, smart mitigation** that suggests remediation playbooks to help prevent potential attacks and reduce manual processes
- **Continuous, integrated threat intelligence** based on unique industrial control systems vulnerabilities

Diagram of Joint Solution

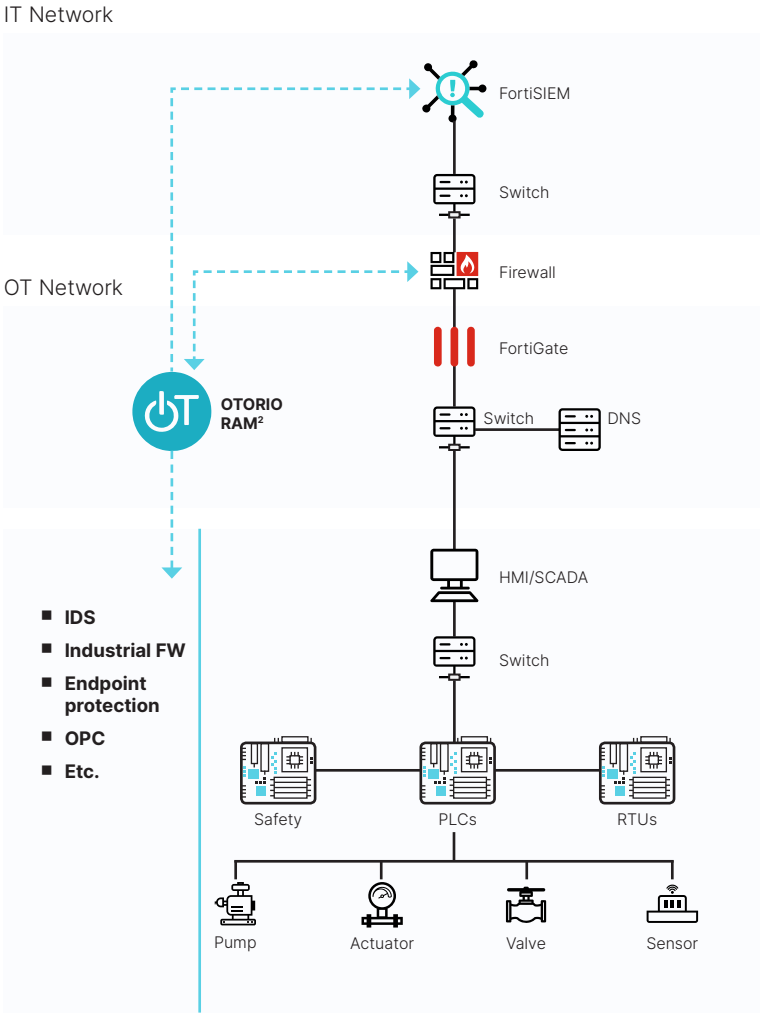

Figure 1: Comprehensive IT/OT protection from Fortinet and OTORIO.

Use Cases

Continuous assessment of the attack surface

OTORIO RAM² includes an advanced threat-intelligence database with vulnerabilities unique to industrial systems in the OT network. RAM² integrates with FortiGate to collect firewall events and configuration rules that are used in the creation of the OT network's digital twin. RAM² simulates an attack graph based on the network topology, considers the operational and business impact of the affected assets and operational processes, and determines the asset vulnerabilities.
It identifies the highest risks to operational continuity and suggests the most impactful configuration changes in segmentation and firewall rules for virtual patching. The joint Fortinet and OTORIO solution enables an alternative method for mitigation, which is critical for operational continuity.

Converged OT/IT SOC

OTORIO RAM^2 enhances FortiSIEM as an industrial IT solution by providing a single point for all security alerts from the OT network. RAM^2 orchestrates industrial systems and protocols to collect data and correlate it for the generation of OT-specific alerts. Security teams can manage a unified priority queue of the alerts with FortiSIEM. The RAM^2 feeds FortiSIEM with alerts in a unified format that complements IT data with additional insights regarding industrial assets within operational processes. Together, these solutions add important industrial context that reflects potential impacts on operational continuity, hence bridging the gap between the operational team and the cyber analysts.

About OTORIO

OTORIO is leading in safe industrial transformation. It delivers an industrial-native SOAR, providing centralized and simplified security automation and cyber risk reduction. The company is led by former Israel Defense Forces cybersecurity experts with decades of experience defending mission-critical infrastructures.

The OTORIO comprehensive offering of products and professional services address the different stages an industrial company faces when embarking on digital transformation. Its mission is to provide industries the security they need to utilize digital technologies, improve productivity, and grow their business. Learn more at www.otorio.com.

July 9, 2021 5:32 AM
558759-A-0-EN