

Benefits of RAM² with FortiGate

Overview

Traditionally, Operational Technology (OT) and IT networks were separated by an air gap. Rapid digitalization processes promote a growing connectivity which is essential for efficiency and competitiveness, but at the same time, increases the digital attack surface of OT environments. OTORIO's RAM² OT security solution and FortiGate now integrate with one another to protect converged OT-IT-IIoT environments against cyber security attacks, and enable safe, reliable, and efficient industrial operations.

The Challenges

Securing Industrial Control Systems (ICS) against cyber threats challenges and continues to dominate the everyday to-do lists of OT teams. Reasons for this include:

- OT security complexity is overwhelming (e.g., multi-vendor, multi-generation, distributed operations, alert fatigue)
- Lack of visibility in the converged environment (IT/OT/IIoT)
- Lack of business context for risk prioritization
- Achieving and maintaining an effective air gap is increasingly difficult, if not impossible
- Expanded attack surface of the operational network
- Insufficient regulation of component manufacturers and the industrial supply chain, introducing the possibility of equipment compromise, even prior to installation.
- Poor network segmentation between IT and OT and operational processes
- OT limited access and permission control
- Skill gap - Many security experts lack an understanding of industrial processes, and OT personnel lack cyber security knowledge

Highlights











- These complementary solutions secure IT/OT convergence by integrating OTORIO's contextual OT cyber risk solution with FortiGate for secure access control
- Improves operational continuity with ongoing OT risk assessment and reduction
- Bridges the OT security skills gap via automated mitigation steps and a corresponding playbook
- Operational Environment Segmentation Assessment - Segmenting the network to limit the impact of any intrusion
- Control access by users and devices, and enforce identity-based policies with continuous trust assessment
- OT Operational Context - Scalable and flexible log collection and These complementary solutions secure provides OT contextual insights with noise reduction

Benefits of RAM² with FortiGate

The Solution

OTORIO's RAM² and Fortinet Security Fabric provide a joint, comprehensive solution to protect the digitalization of ICS environments. OTORIO's RAM² is an OT cyber security solution for risk assessment, monitoring and management. RAM² identifies gaps in an industrial network's security posture and enables organizations to mitigate risk against potential attacks in cooperation with Fortinet's extensive network security expertise via FortiGate. The combined OTORIO-Fortinet solution enables automated and continuous monitoring, detection, and management of risks, whether a network outage, an unreliable connection, or a cyber attack. By proactively reducing risk, the complementary tools ensure that all elements operate together safely, and quickly initiate timely responses and mitigation measures.

Together, OTORIO's RAM² and FortiGate provide:

-  **Extensive Network Visibility Asset** inventory of the firewalls themselves and the assets behind them.
-  **Out-of-the-Box Compliance** for industrial security standards and regulations such as NERC CIP, IEC 62443 and NIST.
-  **Network Activities Monitoring** on the converged operational networks across hundreds of facilities from a single console, including OT-specific capabilities for detection of suspicious behavior, and correlation with other events.
-  **Noise Reduction** focused on relevant insights based on automatic analysis.
-  **Effective Network Segmentation** between IT and OT and between operational processes. Such segmentation is based on continuous assessment and optimization of firewall configurations and virtual patching of known vulnerabilities.
-  **A Single Source of Truth (SSoT)** for all OT related risks.
-  **Contextualized risk - based prioritization** of alerts and mitigation actions.
-  **Contextualized Mitigation Steps** for each risk, presented in a simple, actionable way, suitable for the operational environment constraints.
-  **Controlled Access Authentication**
-  **Proactive Pre-Breach and Post-Breach Protection**, rather than only reactive detection of potential attacks.

How it works

OTORIO's RAM² is an OT cyber security risk management platform that enables operations security leaders to proactively protect critical operational processes, and reduce the time to assess, manage, and mitigate risks. RAM² ingests data from the entire Fortinet Ecosystem in addition to a variety of security and industrial sources (e.g., PLC, DCS, SCADA, Historians, Engineering systems) within the OT environment.

RAM² provides a complete and accurate industrial asset inventory. It identifies IOCs (indications of compromise) as well as vulnerabilities and IOEs (indications of exposure), and automatically correlates these indicators to identify suspicious patterns and risk scenarios that may affect the safety, efficiency, and reliability of industrial processes. RAM² provides contextualized prioritization based on OTORIO's unique risk calculation engine, taking into account the potential impact on production operations and business goals. RAM² also provides out-of-the-box compliance audits according to common industrial security standards (e.g., IEC 62443, NERC CIP and NIST) leveraging the results of deep asset inspection, SCADA systems, and the entire ICS network.

By processing offline data such as industrial project files, industrial firewall configurations, PCAPs, RAM² provides extended visibility into operational networks, including areas which are not accessible to continuous monitoring. The platform filters irrelevant events that are generated by multiple siloed sources in industrial networks, and provides correlated insights that are enriched by enhanced and robust threat intelligence of OTORIO's security experts. By distributing RAM²'s alerts and insights to FortiSIEM, we reduce the noise and assist in efficient and scalable protection of integrated OT/IT security teams.

Benefits of RAM² with FortiGate

Use Case



Proactive segmentation planning and assessment

Ensuring operational continuity and preventing unauthorized access to critical assets begins by clarifying the scope of each operational process and its relations with other parts of the OT network. With RAM², industrial organizations can create a logical representation of their operations, gain maximum visibility of the assets involved in each process, and the connections among them. This enables for effective segmentation control planning from a business and operational perspective.

Fortinet's FortiGate Firewall controls the communication between IT and OT networks, and the FortiGate Rugged Firewall can be positioned to ensure that only mandatory communication is generated between operational processes. RAM² monitors potential breaches between operational processes to provide "Virtual Segmentation" to complement FortiGate firewalls when they are not available. OTORIO's RAM² also identifies unsecure protocols and helps operations security teams mitigate unnecessary risks.

But even the best security controls will not provide proper protection if they are not configured properly. OTORIO's RAM² analyzes Firewall rulesets and alerts for misconfigurations that create gaps in segmentation (such as Inbound Internet Management Communication, Permissive Rules, Rule Logging Not Enabled, Shadowed Rule, and Unused rules), so IT and Operations teams can maximize the ROI on their security controls..



Continuous Risk Management

FortiGate is capable of monitoring and controlling high volumes of traffic. Logging these transactions is imperative for audit, threat detection and forensics. Without context, however, it is difficult to know what's relevant and what's not, and what warrants high priority investigation. The challenge becomes more acute for IT and security teams who have neither sufficient visibility into the OT environment nor a good understanding of operational processes and business objectives. RAM² ingests FortiGate event logs, classifies them, identifies the IOC (indicators of compromise) and analyzes those events and their relation to additional information gathered from a variety of security and industrial sources within the network. Seemingly benign events (e.g., login attempts using IT protocols to a SCADA system) are correlated with information about suspicious events (e.g., a breach between processes using unsecure processes, discovery of a rogue device in the network or detection of malware on an asset which can impact a critical process). RAM² turns the suspicious pattern that was detected into an insight with a high risk

score which can automatically be distributed to FortiSIEM in the integrated SOC.

About OTORIO

OTORIO's industrial-native OT security platform enables industrial organizations to achieve an integrated, holistic security strategy. Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. OTORIO's global team brings the extensive mission-critical experience of top nation-state cyber security experts combined with deep operational and industrial domain expertise.