OTORIO

RAM²

Continuous OT cyber risk management

Prescriptive protection for operational networks

Digital transformation in operational environments continues to accelerate risk. Using different vendors, manual processes, and multi-generation technology makes OT security complex. The unwavering need to prioritize safety, productivity, and uptime means that operational resiliency cannot be compromised. All these factors significantly increases risks, making it challenging to map and understand security posture and protect industrial operations.

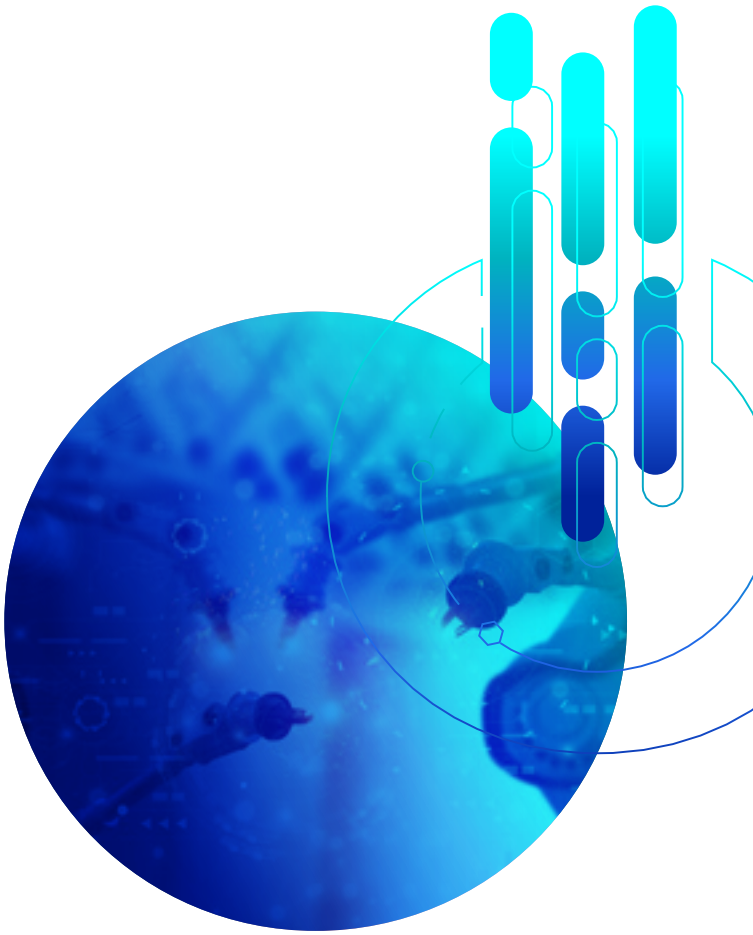
OTORIO's RAM² is an OT security solution with a unified framework built to help you proactively manage cyber security risks, build resilient operations, and future-proof operational environments. It provides you with **unparalleled consolidated visibility** of your Firewall, EDR, IDS, PLC, SCADA, DCS, Historians, Engineering systems, and more. All devices, networks, and systems in the operational environment can be seen and monitored in real-time, so practitioners can efficiently address potential risks with a proactive approach.

RAM² enables you to **take control of your security posture** by leveraging enriched asset attribution with operational context, vulnerabilities, and exposures. It delivers rich, granular reports that proactively identify the most critical vulnerabilities and provide alerts prioritized by operational context and business impact.

RAM² provides a **unified framework for operational security** to help your team establish an enterprise-wide security strategy to triage and address security threats faster and more reliably. It enables full governance and bridges skill gaps. RAM² accelerates decision-making and significantly improves your mean-time-to-detection (MTTD) and mean-time-to-response (MTTR).

RAM² supports practitioners with **prescriptive expert-defined risk mitigation guidance**. Best practice and tailored practical playbooks provide step-by-step instructions to help teams mitigate vulnerabilities, demonstrate compliance and ensure operational resilience.

RAM² integrates as an overlay to **maximize ROI from your existing operational security stack**. The platform seamlessly integrates with a variety of third-party tools and technologies to deliver deeper contextual analysis, preventing downtime and financial losses.



KeyBenefits

- Enhance operational resilience against cyber security risks.
- Scalable third-party integrations with cross domain security and operational data sources for a consolidated visibility into OT-IT-IIoT operational environments.
- Complete and accurate visibility into asset inventories including asset role and impact on the environment.
- Pioneering exposure-based prioritization leveraging a non-intrusive Cyber-Digital-Twin technology for analysis of attack vectors.
- Reduce alert fatigue by decreasing noise from irrelevant events and assets.
- Automatic analysis and identification of critical risks using correlated insights.
- Context-aware impact-driven prioritization of most critical risks.
- Clear, practical step-by-step risk-mitigation playbooks tailored for operational environments.
- Out-of-the-box asset and site-level compliance assessment (IEC 62443, NERC CIP, NIST).
- Rich, granular dashboard and reports for comprehensive security posture assessment and governance.
- Enhance the ROI of your technology, people, and processes by seamlessly overlaying RAM² on top of your existing security controls.

How does it work?

01
Collect Data

Online / offline network Monitoring data

Passive, active and integration-based data collection

02
Enrich and Analyze

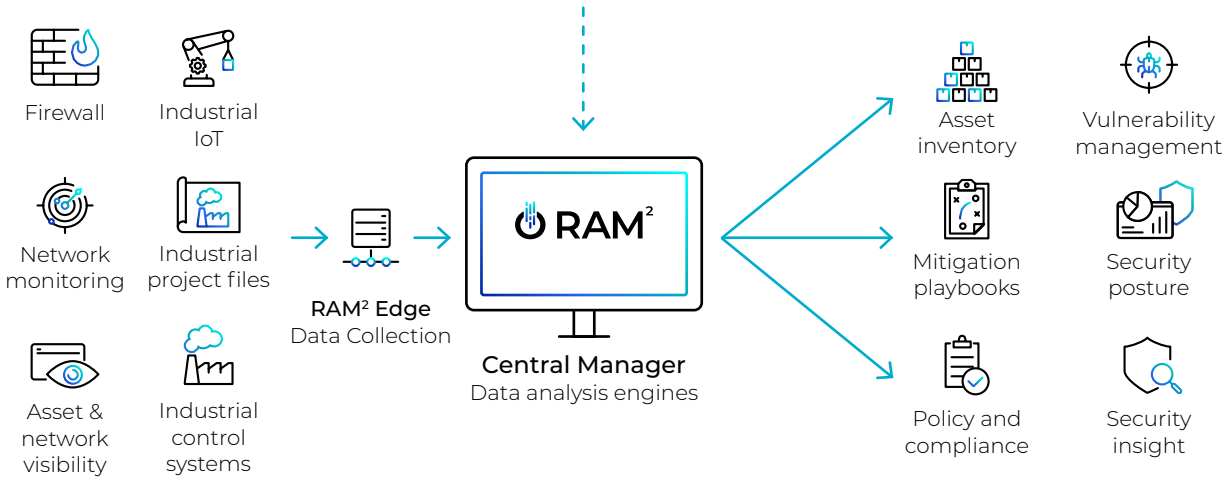
Market-leading vulnerabilities database

Based on OTORIO's research and professional services

03
Deliverables

Dashboards and reports

A unified organizational view of digital risk



Use cases & Key Features

Advanced OT-IT-IIoT asset visibility

- Complete, accurate visibility covering OT, IT and IIoT assets.
- Scalable integration with cross-domain data sources.
- Passive network monitoring and Safe active querying asset discovery
  - Simplified, non-intrusive data collection.
  - Maps assets to operational processes
  - Monitors changes in asset inventory.
  - Level 0 assets are made visible.
- Integrations with:
  - Endpoint Detection and Response (EDR)
  - Firewalls
  - IDS/IPS
  - Secured Remote Access
  - IT SIEM/SOAR
  - APM/CMMS
  - Identity and access management
  - Industrial Systems (OPC, DCS, Historian, MES and more).

Continuous security posture monitoring and assessment

- Identifying security misconfigurations of assets, industrial systems and security controls.
- Automatic identification of gaps in the security configurations of the assets and the network, including the use of default credentials, misconfigured security parameters of industrial systems and of the security controls themselves, end-of-life assets, use of unsecure communication protocols, and more.
- Attack graph analysis provides accurate recommendations for proactive hardening of specific assets to prevent exposure of high-risk assets and processes, based on business-impact prioritization.
- Non-intrusive attack vector analysis powered by OTORIO's Cyber Digital Twin technology.
- Customizable dashboards to support efficient decision making.

Vulnerability assessment

- Market-leading vulnerabilities database based on OTORIO's research.
- Accurate identification and mapping of publicly known vulnerabilities (CVEs).
- Prioritized alerts based on operational context.
- Practical, clear and feasible playbooks for risk mitigation, with alternatives to patching.

Segmentation assessment

- Identifies firewall misconfigurations and segmentation gaps.
- Optimization of firewall rules.
- Delivers intuitive and prioritized risk mitigation steps.
- Reduces the attack surface.

Real-time incident detection

- Correlated insights based on events from multiple data sources to detect suspicious patterns and reduce noise from benign events.
- Leveraging proprietary capabilities such as passive network monitoring, SNMP traps and more to improve the detection of threats.
- Risk-based alerting according to the potential impact on the related operational processes and business consequences.
- Automated email notifications to relevant personnel according to operational process and severity.

Security compliance & governance

- Out-of-the-box compliance audit from the single asset level to the site and entire network level.
- Rich, granular reports for comprehensive security posture overviews and compliance governance.
- Dynamic and granular compliance score.
- Multiple standards like NIST 800-82, IEC-62443, NERC CIP and organizational policies.
- Compliance governance dashboard.

Use cases & Key Features

Case Management

- Case management mechanism enabling IT-OT team collaboration for efficient resolution and risk mitigation.
- Manage all the relevant information for investigation and mitigation in one place.
- Assign tasks to different stakeholders and track progress.

OT contextualized risk assessment

- Context-aware security posture and attack surface assessment
- Correlated insights for detection of potential attacks and noise reduction.
- Identify host, network and IAM gaps and exposures.
- Prioritized gaps based on risk calculation including impact analysis and various threat levels.
- Comprehensive granular dashboard overview of security posture from asset to business unit to enterprise level.
- Rich and granular reports - customizable for different needs.
- OTORIO's proprietary prioritized cyber risk insights algorithms.
- Practical, clear and feasible playbooks for risk mitigation, tailored for the operational environment.
- ICS ATT&CK MITRE based insights.

Risk Mitigation

- Prescriptive mitigation and expert remediation guidance.
- Best practices for hardening security configurations and network interfaces.
- Segmentation assessment with recommended steps to reduce risk levelOTORIO's proprietary prioritized cyber risk insights algorithms.
- Practical, clear and feasible playbooks for risk mitigation, tailored for the operational environment.
- ICS ATT&CK MITRE based insights.

Summary

OTORIO's RAM² operational security management solution offers a comprehensive and actionable framework that consolidates visibility of your entire operational environment, empowers you to take control of your security posture, identify critical vulnerabilities, and proactively reduce cyber risk. RAM² expert-defined remediation guidance and prescriptive mitigation playbooks are tailored to your specific operational environment, so you can implement industry best practices and strengthen your security configurations and network interfaces. With RAM², you can ensure safe, reliable, and efficient operations that deliver immediate business value for your entire organization.

About OTORIO

OTORIO has pioneered an industrial-native OT security platform that enables its customers to achieve an integrated, holistic security strategy for industrial control systems (ICS) and cyber-physical systems (CPS).

Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. The company's platform provides automated and consolidated visibility of the entire operational network, enabling companies to take control of their security posture, eliminate critical risks, and deliver immediate business value across the organization.

OTORIO's global team combines the extensive mission-critical experience of top nation-state cyber security experts with deep operational and industrial domain expertise.

www.otorio.com

CN 040523