OTORIO

Product Portfolio

Protect Everything You Operate

Ensuring Operational Resilience

OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations by leveraging a technology-enabled ecosystem.

OTORIO enables you to achieve an integrated, holistic security strategy for industrial control systems (ICS) and cyber physical systems (CPS). Our innovative platform supports you in scaling as your processes mature, ensuring that you always stay one step ahead. No matter where you are in your operational security journey, OTORIO is here to help you take the next step and achieve a robust and secure environment.

Our operational security platform provides you with a unified, actionable framework and consolidated visibility of your entire network. This empowers operational security practitioners with the tools needed to take control of security posture and proactively identify the most critical vulnerabilities. OTORIO provides prescriptive mitigation playbooks and expert-defined remediation guidance, tailored for your specific operational environment. Our platform uses best practices so you can harden security configurations and network interfaces, delivering immediate business value across your organization.

OTORIO helps you establish a unified, enterprise-wide security strategy that protects your organization from financial losses and downtime. Automated asset and site-level assessments help you easily meet Industry specific security standards and demonstrate compliance governance, ensuring a secure and profitable future for your organization.

OTORIO's OT Cyber Risk Management platform includes:

RAM² ™
Continuous OT cyber risk management

spOT ™
On demand OT cyber risk assessment

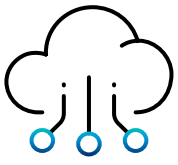
remOT ™
Secure remote access module

Why choose OTORIO

- Comprehensive visibility of your entire operational network, orchestrates data from cross domain sources.
- Risk assessment based on operational context, focuses on risks that matter most to your business.
- Prescriptive mitigation playbooks, and expert-defined remediation guidance, ensures operational continuity and safety.
- A unified, actionable framework for operational security practitioners, promotes IT-OT team collaboration to mitigate cyber risks.
- Out-of-the-box asset and site-level compliance, enables you to enforce and govern industry required regulations.
- Immediate business value across your organization, maximizes ROI from your operational security controls and processes.

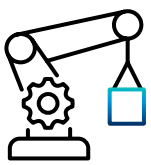
Energy, Utilities & Mining

- Electrical Generation, Transmission & Distribution
- Oil & Gas (Upstream, Midstream & Downstream)
- Mining



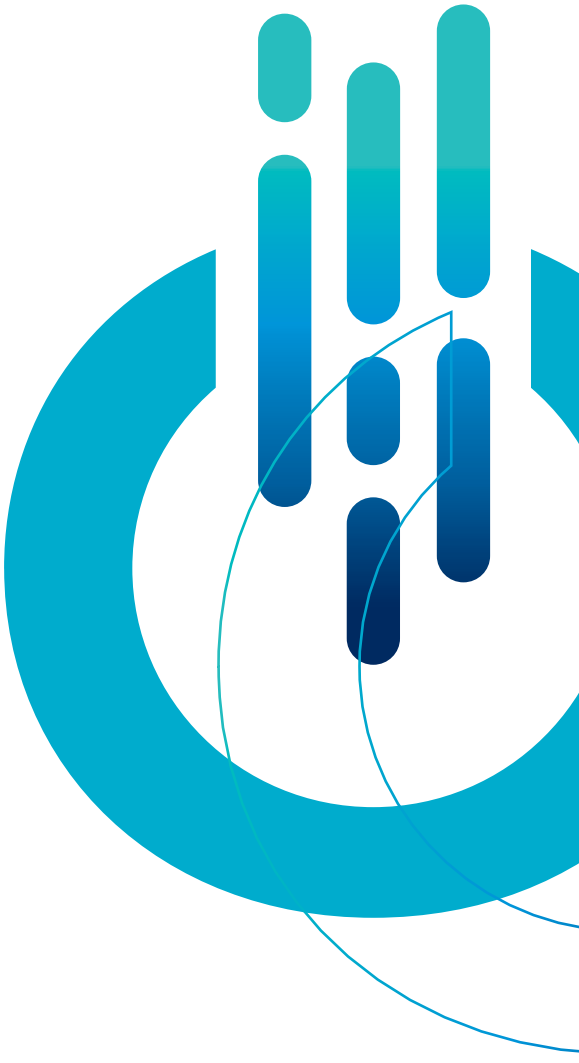
Smart Infrastructure

- Government
- Smart Transportation & Logistics
- Smart Buildings & Cities
- Airports
- Maritime



Manufacturing

- Pharmaceuticals
- Automotive
- Food & Beverage
- Chemical
- Pulp & Paper



RAM²

Continuous OT cyber risk management

Prescriptive protection for operational networks

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.

RAM² provides you with **unparalleled consolidated visibility** of your entire operational network by orchestrating data from cross-domain sources. This includes IDS, Firewall, EDR, PLC, DCS, SCADA, Historians, Engineering systems, and more. All devices, networks, and systems in the OT environment can be seen and monitored in real-time, so practitioners can efficiently address potential risks with a proactive approach.

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

RAM² promotes collective governance with a **unified framework for operational security.** Easy-to-navigate, customizable dashboards empower IT and OT security practitioners with the tools needed to bridge skill gaps, accelerate decision making and significantly improve your mean time to detect (MTTD) and resolve (MTTR).

RAM² supports practitioners with **expert remediation and prescriptive 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 overlays with a variety of third-party tools and technologies to deliver deeper contextual analysis, preventing downtime and financial losses.

RAM² can be used as an overlay or a standalone OT security solution for industrial control systems (ICS) and cyber physical systems (CPS).

Key Benefits

- RAM² enhances operational resilience against cyber security risks.
- Scalable third-party integrations with your other security and operational systems for a holistic view of your OT-IT-IIoT environments.
- Complete, accurate visibility into asset inventories combined with operational insights, including the asset's role and impact on the environment.
- Pioneering exposure based prioritization leveraging a Cyber-Digital-Twin technology for non-intrusive attack vectors analysis.
- Reduce noise and alert fatigue by prioritizing risk alerts enriched with operational context, show only legitimate, relevant alerts of highly impacted assets.
- Orchestrated, efficient operational cyber risk mitigation processes to streamline process and resource management.
- Contextualized risk prioritization helps focus on the most important, highest-priority mitigation actions first, to ensure the safety and efficiency of your operational processes.
- Clear, practical 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 overviews and compliance governance.
- Improve ROI of existing security tools when seamlessly overlaying RAM².

How does it work?

01 Collect Data

Online / offline network Monitoring data

Passive, active and integration-based data collection

02 Enrich and Analyze

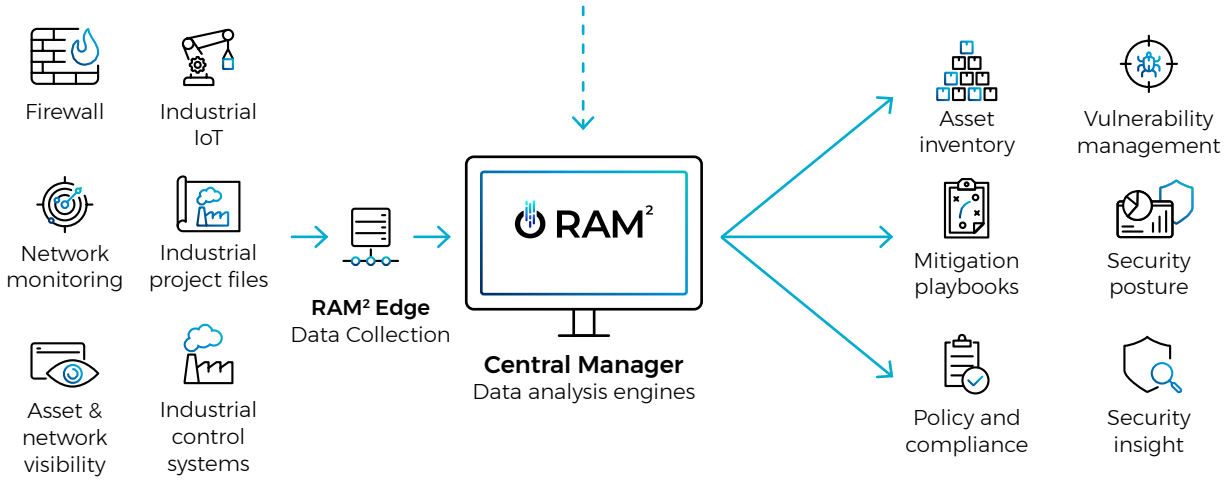
Market-leading vulnerabilities database

Based on OTORIO's research and professional services

03 Deliverables

Dashboards and reports

A unified organizational view of digital risk



spOT

On demand OT cyber risk assessment

Evidence based risk and compliance assessment

spOT by OTORIO provides organizations with fast, on-demand technical risk assessments of operational networks. spOT is easy to set up and execute, either on-site or remotely. It also saves practitioners valuable time and resources by leveraging the existing install base to expedite audits of assets, sites, or an entire organization's security posture across multiple sites. spOT automatically builds an advanced OT-IT-IIoT asset inventory and performs contextual analysis to identify vulnerabilities and gaps in security posture. Critical risks are then prioritized by business impact and their potential effect on other operational processes.

Many industries and critical infrastructure sectors are subject to strict regulations and standards for OT security. spOT provides automated, out-of-the-box compliance assessments at the asset and site level, helping organizations demonstrate compliance, and avoid penalties and fines.

spOT provides a rich, granular security posture overview and compliance governance report with clear, practical recommendations, tailored specifically for OT environments. Expert-defined remediation guidance is provided for each identified vulnerability, security gap, exposure, and compliance deviation as well as best practices for hardening security configurations and network interfaces. The ROI of spOT increases over time with its ability to reassess the same environment, track historical comparisons, and receive ongoing alerts as a service.

spOT simplifies and automates digital machine security. It significantly reduces the time and cost of cyber security FAT (Factory Acceptance Test) and SAT (Site Acceptance Test) processes with accurate asset inventory, out-of- the-box compliance, automated OT security gap identification, and documentation.

Key Benefits

- A technical assessment report of OT security controls with best practices to harden security configurations and network interfaces.
- Expedites the OT technical assessment and audit process by reducing time and effort.
- Conduct a safe operational security posture assessment without disturbing ongoing operations.
- Rich, granular reports for comprehensive security posture overviews and compliance governance.
- Risk assessment report that prioritizes vulnerabilities according to their OT environment impact, highlighting the most critical risks.
- Contextualized mitigation steps for each risk presented in a clear, practical way that is suitable for operational environments.
- Out-of-the-box asset and site-level compliance (IEC 62443, NERC CIP, NIST) and governance of organizational policies.
- High-fidelity asset inventory with a deeper and richer understanding of its role, impact, vulnerabilities, and organizational structure.
- Improve ROI for existing security tools.
- Reduce cybersecurity FAT/SAT costs and enhance service offerings with automated machine cyber security.

How does it work?

01 Collect Data

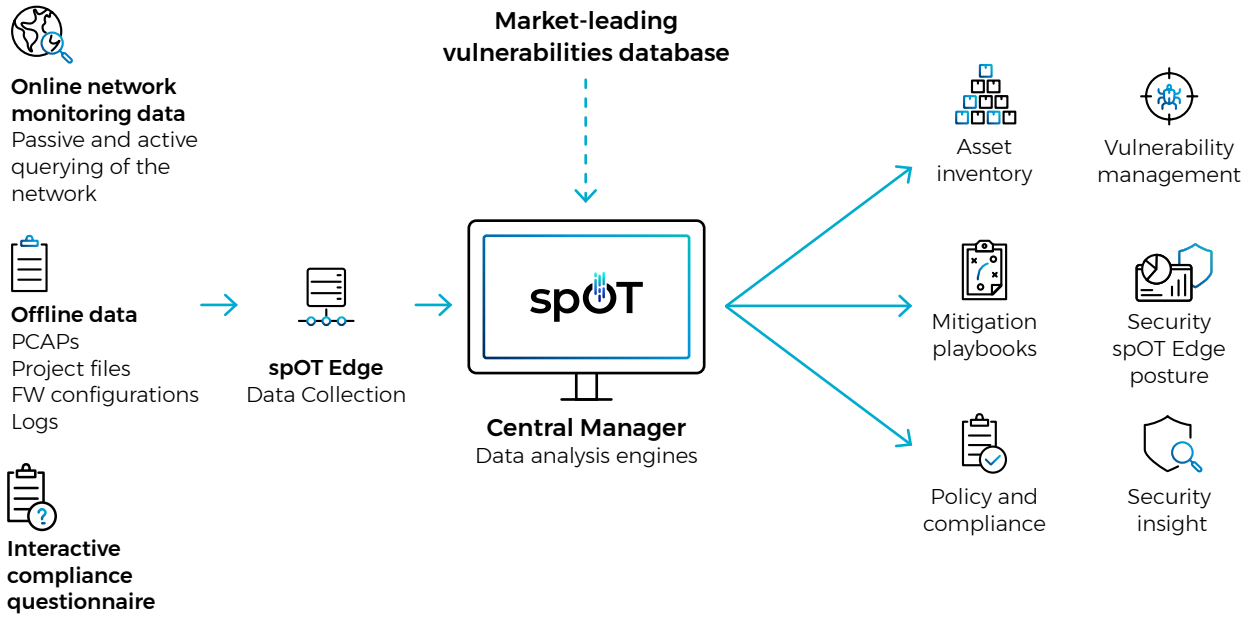
Integrates with security controls of critical assets and operations systems

02 Enrich and Analyze

Based on OTORIO's research and professional services

03 Assessment Reports

Comprehensive digital security assessment report



remOT

Secure remote access module

Operational zero-trust remote access

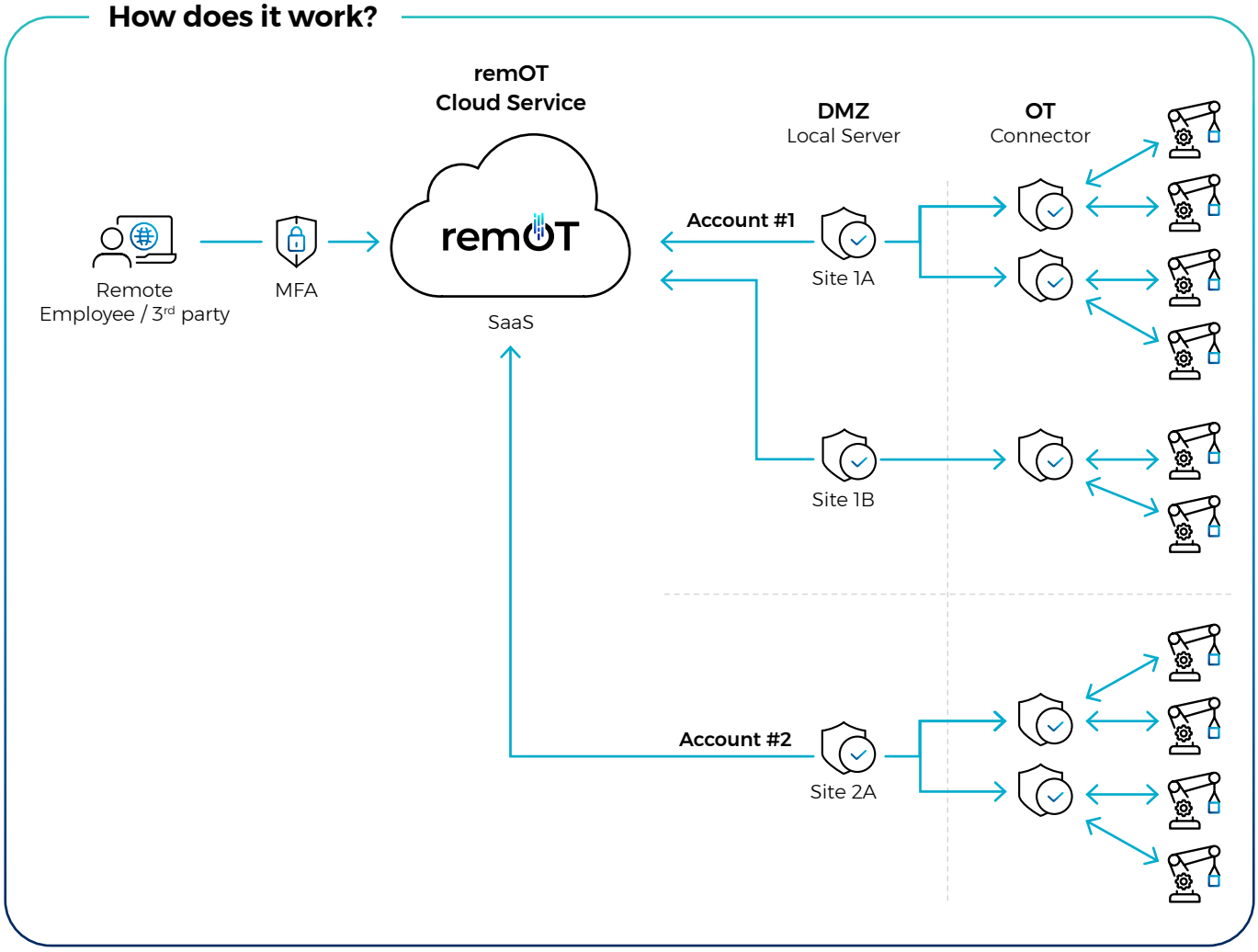
remOT by OTORIO delivers a secure by design, simple, and fully governed remote access to the operational environment. As a clientless solution with no agents, no VPN, and no Jump Server, remOT simplifies connectivity to assets for third-party vendors, service providers, and internal users, without compromising on safety. It scales seamlessly to the needs of your organization while maintaining OT network segmentation between sites, with a low total cost of ownership (TCO).

With remOT, access is governed and controlled using separated, multi-tenant cloud account management. By leveraging remOT zero-trust approach, access is given only to authorized employees, and authorized third-parties to specific assets, according to the needs of industrial networks. remOT delivers full visibility of any secure, remote connection.

Key Benefits

- Zero trust architecture providing secure access for internal and third party users.
- Seamless remote access to specific assets in target sites from the web browser with no agents, no VPN, and no jump server.
- Single-sign-on controlled access.
- Audit of every user and admin action.
- Secure-by-design with full TLS communication, credentials and asset protection, protocol and session isolation.
- Separated multi-tenant cloud account management.
- Secure and easy to use file transfer.
- Full governance and monitoring of any secure, remote connection.
- Scales easily with low TCO.

How does it work?



RAM²™

Continuous OT cyber risk management

spOT

On demand OT cyber risk assessment

Key Features

- 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
- Vulnerability assessment
- Segmentation assessment
- Context-aware security posture and attack surface assessment
- Security gaps and exposure identification
- Non-intrusive attack vector analysis powered by OTORIO's Cyber Digital Twin technology
- Prioritized alerts based on operational context
- Correlated insights for detection of potential attacks and noise reduction
- Continuous OT security monitoring and risk management
- Out-of-the-box compliance audit from the single asset level to the site and entire network level
- Practical, clear and feasible playbooks for risk mitigation, tailored for the operational environment
- Case management mechanism enabling IT-OT team collaboration for cyber risk mitigation
- Customizable dashboards to support efficient decision making
- Rich, granular reports for comprehensive security posture overviews and compliance governance

- Support for on-demand data collection in a mobile and portable way
- Complete and accurate asset inventory
- Passive network monitoring and Safe active querying asset discovery
- Vulnerability assessment
- Segmentation assessment
- Security gaps and exposures identification
- Non-intrusive attack vector analysis powered by OTORIO's Cyber Digital Twin technology
- Out-of-the-box asset and site-level compliance
- Detailed risk mitigation playbooks and hardening of site-specific OT network risks and vulnerabilities
- Rich, granular reports for comprehensive security posture overviews and compliance governance
- Prescriptive mitigation steps for each risk presented in a clear, practical way that is suitable for operational environments, and guidance for cyber security hardening of the network

Use Cases

Advanced OT-IT-IIoT asset visibility

Vulnerability assessment

Segmentation assessment

Continuous identification of security gaps and exposures

Real-time incident detection

OT contextualized risk assessment

Security compliance & governance

Risk assessment of a production line, a site or an entire OT organization

OT technical assessment

Expedite OT security audit process

Cyber security and compliance audit during Factory and Site acceptance tests

remOT

Secure remote access module

- Cloud management user access
- Seamless remote access to specific assets in target sites from the web browser with no Agent, no VPN, and no Jump Server
- Single-sign-on controlled access
- Management of assets exposure from the local site
- Audit of every user and admin action
- Security-by-design with full TLS communication, credentials & asset protection, protocol, and session isolation
- Separated multi-tenant cloud accounts management
- Secure file transfer

Providing secure remote service by a vendor or a service provider to multiple end-customers and environments

Managing secure remote access to an OT environment by multiple third parties

Controlled access of authorized only internal employees to assets in the network

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.

otorio.com

CN 020523

OTORIO