OTORIO

Simplifying Cybersecurity to Protect Water Treatment Facilities

Safe and clean water is essential for public health, environmental protection, and economic growth. To ensure the reliability of water purification facilities, it is critical to address the unique security constraints of Information Technology (IT), Operational Technology (OT), and distributed Internet of Things (IoT) devices.

OTORIO's Risk Assessment, Monitoring & Management platform (RAM²) is a next-generation industrial cybersecurity and digital risk management platform that is uniquely designed for converged industrial IT/OT/IoT environments comprising hundreds of multi-protocol and multi-vendor devices from different generations.

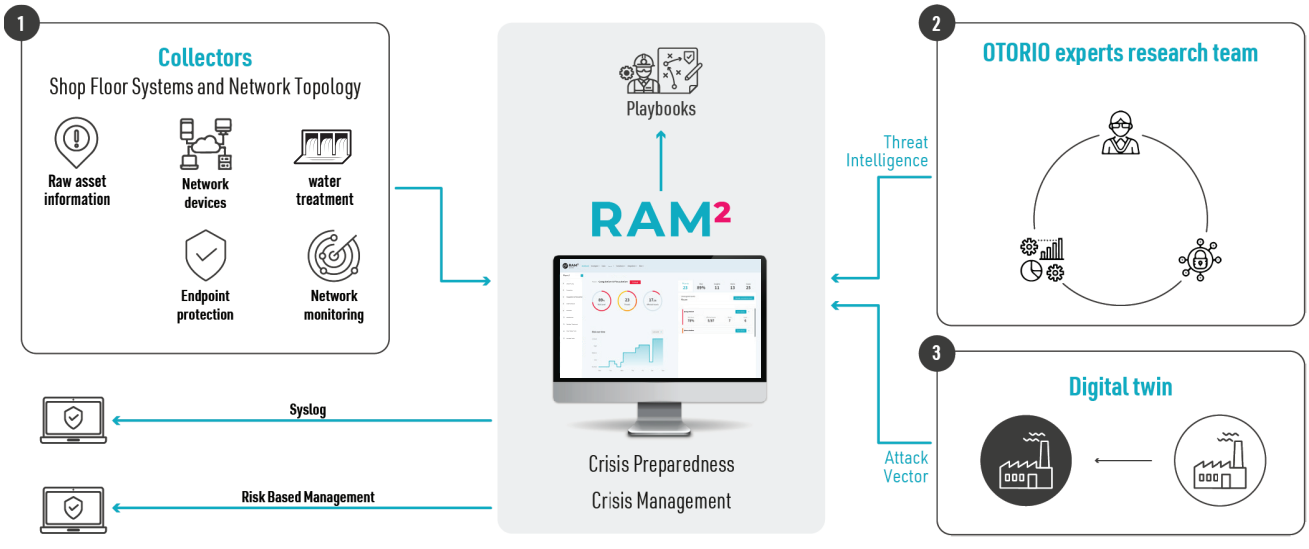
The vendor-agnostic RAM² platform collects data directly from multiple IT/OT/IoT devices, delivering a detailed asset inventory. Alerts and events from all operational and cybersecurity devices are correlated into meaningful, contextualized insights. These insights are displayed using intuitive dashboards and prioritized according to their impact on operational continuity.

Using the data it collects, RAM² creates a digital twin of the operational environment. Then, applying a non-intrusive breach and attack simulation engine, the platform allows operational and security teams to identify and proactively mitigate vulnerabilities before they become breaches. When cyber incidents require SOC intervention, RAM² facilitates seamless collaboration between operational and cyber teams, providing analysts with a tailored workbench for in-depth forensic investigation.

Benefits

- Simplifies cybersecurity processes to ensure uninterrupted operations
- Proactively identifies vulnerabilities before they become breaches
- Unique, non-intrusive breach and attack simulation
- Unmatched view of asset inventory based on location, process and impact on continuity
- Automatically-generated mitigation playbooks for multiple attack scenarios
- Simplifies compliance and auditing processes
- Tailored to environments with hundreds of multi-vendor/ multi-protocol devices
- Maximizes investments in existing IT/OT/IoT security systems
- Continuous OT security and OT compliance monitoring

OTORIO RAM² Architecture



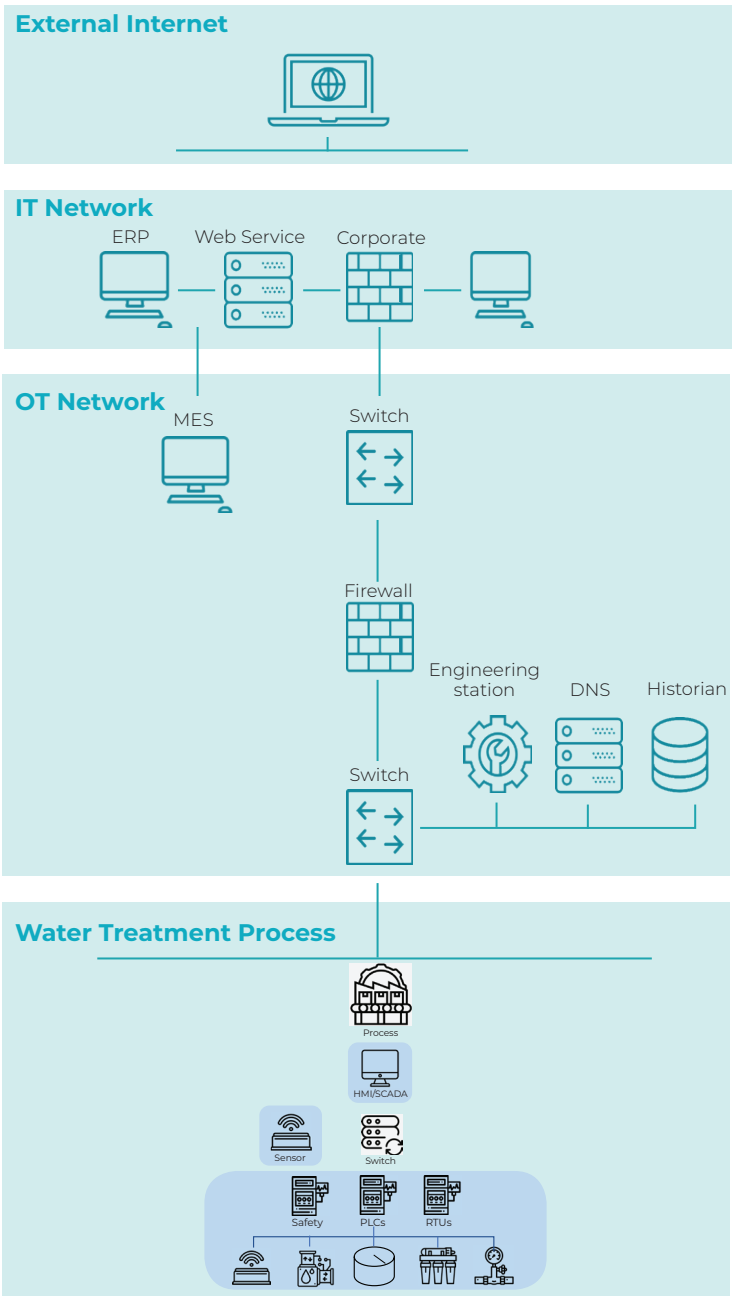
HIGH EXPOSURE

Intel collection, reconnaissance & initial access to network

Propagation and enumeration, gaining high privileges in the IT level

Usage of gathered credentials and footholds to reach and communicate with **PLCs on the operational environment**

Attackers can influence water treatment processes in any way they wish – **impacting operational continuity and potentially causing health hazards**



SOLUTION & SERVICES

PREVENTION
- Threat Intelligence
- Security Assessment
- Non-intrusive breach & Attack Simulation

DETECTION
- Asset Inventory
- Detailed Insights
- Prioritized Alerts
- Analyst-in-a-box
- Compliance Gaps

CONTAINMENT
- Automated Mitigation Playbooks
- Threat Hunting
- Incident Response

OTORIO – Your Partner for Secure Digital Production

OTORIO, the leading OT security and digital risk management solutions provider, delivers a suite of products and services that guarantee plant safety and reliability from the network level down to the individual device.

With the OTORIO offering, every machine and connected device is monitored and controlled, ensuring that each meets the highest standards of digital safety and cybersecurity, while ensuring continuous, uninterrupted, and resilient operations that maximize digitization efficiencies.

RAM² Key Features

Asset Inventory and Change Management
Discovers, analyzes and monitors all assets (IT/OT/IoT) within the environment based on production process, physical location, business impact, state, and other factors for full visibility.

Digital Twin / BAS Engine
Creates a digital twin of the IT/OT/IoT environment to conduct breach and attack simulations with zero disruption to the production environment.

Cyber Risk Insights
Correlates alerts, asset data, and industrial context from multiple security and industrial sources to identify gaps in the security posture and early detection of attack patterns.

Actionable Playbooks
Creates step-by-step remediation guidelines to help operational teams manage and mitigate threats efficiently.

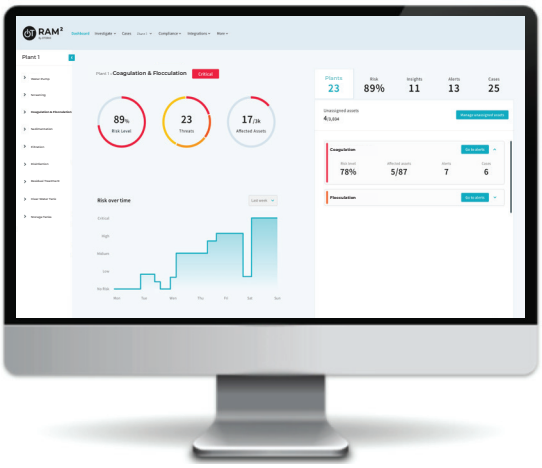
Case Management Tracking
Collaborates within teams, tracks progress, and communicates with external stakeholders to reduce mean time to resolution. Provides a common language for operational teams and cyber analysts, with the necessary granularity for each.

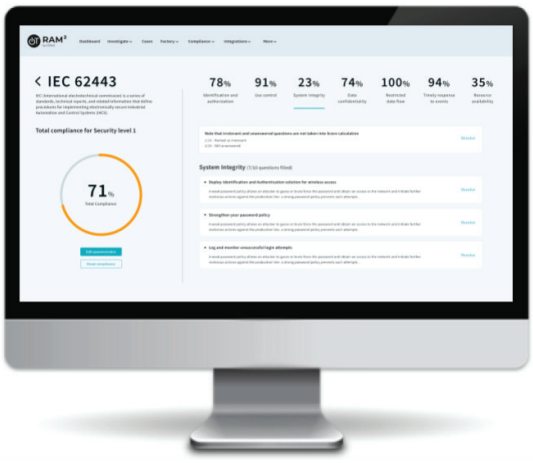
Detailed Dashboards
Overall risk assessment
- Risk details for each operational level and process
- Risk over time
- Risk per threat category
- Prioritized insights and alerts
- Open cases
- Drill down from risk assessments to assets and alerts
- Compliance score

Reports
Generates and shares risk assessment, compliance, and asset inventory reports with stakeholders for transparency and cooperation.

Integrations
Easy sync of RAM² data with other internal security systems for a comprehensive IT/OT/IoT cybersecurity assessment. Enables collection of assets and events, and export of OTORIO insights to operations and control center for collaboration with different stakeholders.

Compliance Tracking
Ensures that any industrial organization meets common cybersecurity best practices and standards.





RAM²

About OTORIO

OTORIO designs and markets the next generation of OT security and digital risk management solutions. The company combines the experience of top nation-state cybersecurity experts with cutting-edge digital risk management technologies to provide the highest level of protection for the manufacturing industry. Visit our website at https://www.otorio.com/