



# OTORIO for the Pulp and Paper Industry



Paper mills have improved the quality and quantity of their goods since they adopted more Industry 4.0 practices and automation. Along with business improvement came cyber risks.

OTORIO's Risk Assessment, Monitoring & Management platform (RAM<sup>2</sup>) is a next generation Security Orchestration, Automation and Response (SOAR) and SIEM platform. RAM<sup>2</sup> was uniquely designed to provide cybersecurity and digital risk management capabilities in converged IT/OT/IOT environments comprising hundreds of multi-protocol devices.

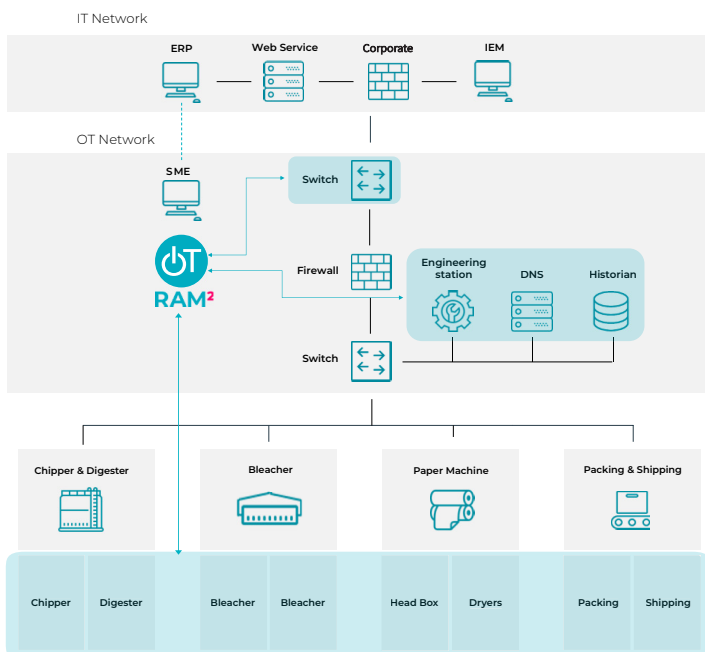
The vendor-agnostic RAM<sup>2</sup> collects data directly from multiple IT/OT/IOT devices, to deliver a detailed view of all the network assets based on their location, process and the operational risk. Alerts and events from all operational and cybersecurity devices are correlated into meaningful, contextualized insights by RAM<sup>2</sup>. The insights are displayed in intuitive dashboards and are then prioritized according to their impact on operational continuity.

RAM<sup>2</sup> creates a digital twin of the OT network for breach and attack simulations of various attack vectors. This provides operational and security teams with powerful tools to preempt and proactively remove risks before they can cause any damage. When cyber incidents require SOC intervention, RAM<sup>2</sup> facilitates seamless collaboration between operational and cyber teams, providing analysts with a tailored workbench for in-depth forensic investigation.

## Benefits

- Maximize investments on existing IT/OT/IOT security systems
- Proactive and preventive cybersecurity and digital risk management
- Tailored to environments with hundreds of multi-vendor/multi-protocol devices
- Detailed view of asset inventory based on location, process and impact on continuity
- Correlated and contextual events and insights reduce alert fatigue
- Provides cyber-expert-in-a-box capabilities
- Generates simplified mitigation playbooks for multiple attack scenarios
- Continuous management, qualification and remediation of IT/OT/IOT digital and cyber risks

## OTORIO Pulp and Paper Industry Architecture



### Orchestration

<b>Firewall</b> M-Guard, Cisco, Checkpoint, Fortinet, Palo Alto	<b>Raw asset information</b> MSB, Querying devices
<b>Endpoint protection</b> Sophos, McAfee, Symantec, Trend Micro	<b>Network devices</b> Netflow, Routing tables
<b>Network monitoring</b> IDS, IPS	<b>Industrial solutions</b> OPC, DCS, Historian



## RAM<sup>2</sup> Key Features

### Asset Inventory and Change Management

Discovers, analyzes, and monitors all assets (IT/OT/IOT) within the network based on their production process, physical location, business impact, state, and other factors for full visibility.

### Digital Twin / BAS Engine

Create a digital twin of the IT/OT network 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

Step-by-step remediation guidelines to help operational teams manage and mitigate threats efficiently.

### Case Management Tracking

Collaborate within teams, track progress, and communicate with external stakeholders to reduce mean time to resolution. Provide a common language to the operational team and the cyber analyst, with the needed granularity for each of the teams.

### 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
- Drills down from risk assessments to assets and alerts
- Compliance score

### Reports

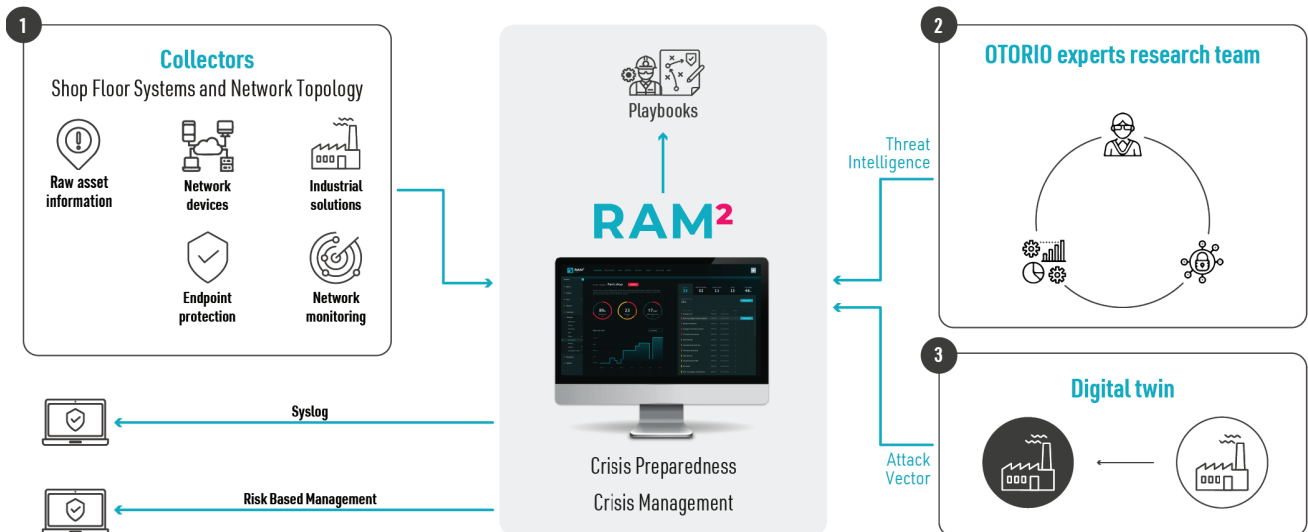
Generate and share risk assessment, compliance, and asset inventory reports with stakeholders for transparency and cooperation.

### Integrations

Easily sync RAM<sup>2</sup> data with other internal security systems for a comprehensive IT/OT/IOT cybersecurity assessment view. Collect assets and events, and export OTORIO's insights to the operations and control center for collaboration with different stakeholders.

### Compliance Tracking

Ensure that your industrial organization meets common cybersecurity best practices and standards.



### About OTORIO

OTORIO delivers next-generation OT security and digital risk management solutions that ensure reliable, safe and efficient industrial digitalization. The company combines the professional experience of top nation-state industrial cybersecurity experts with cutting edge digital risk management technology to provide the highest level of protection to the manufacturing industry.