

# Safeguard electric power systems from evolving cyber threats with OTORIO's solutions

## The impacts of expanding electrification to grid operational technology reliability

In today's rapidly evolving digital landscape, as electrification expands to meet growing demand, electric utilities digitize the operation systems and increase the interconnectivity across transmission, distribution and distributed energy resources (DER) to improve service availability, reliability, and sustainability while enhancing control and safety. Along with the positive side of digital transformation, the industry faces a significant cyber security challenges due to their complex, interconnected multi-vendor, multi-generation of devices and systems in the power generation, transmission and distribution processes. The industry's complex nature, combined with its high-risk environment, critical components of national security and economic stability, has made it a prime target for cyber attacks.

With interconnected systems, electric utilities' security practitioners' main concern is addressing cyber risk in their operational technology (OT) environment and aligning security with business objectives. To effectively align and be compliant with regulations, electric utilities companies need to consider adopting operational technology security programs, and take into account operational context with business impact to manage, and mitigate risk effectively, while including stakeholders in the overall security process of the business.

## Proactively Protecting Electric Utility OT Environment

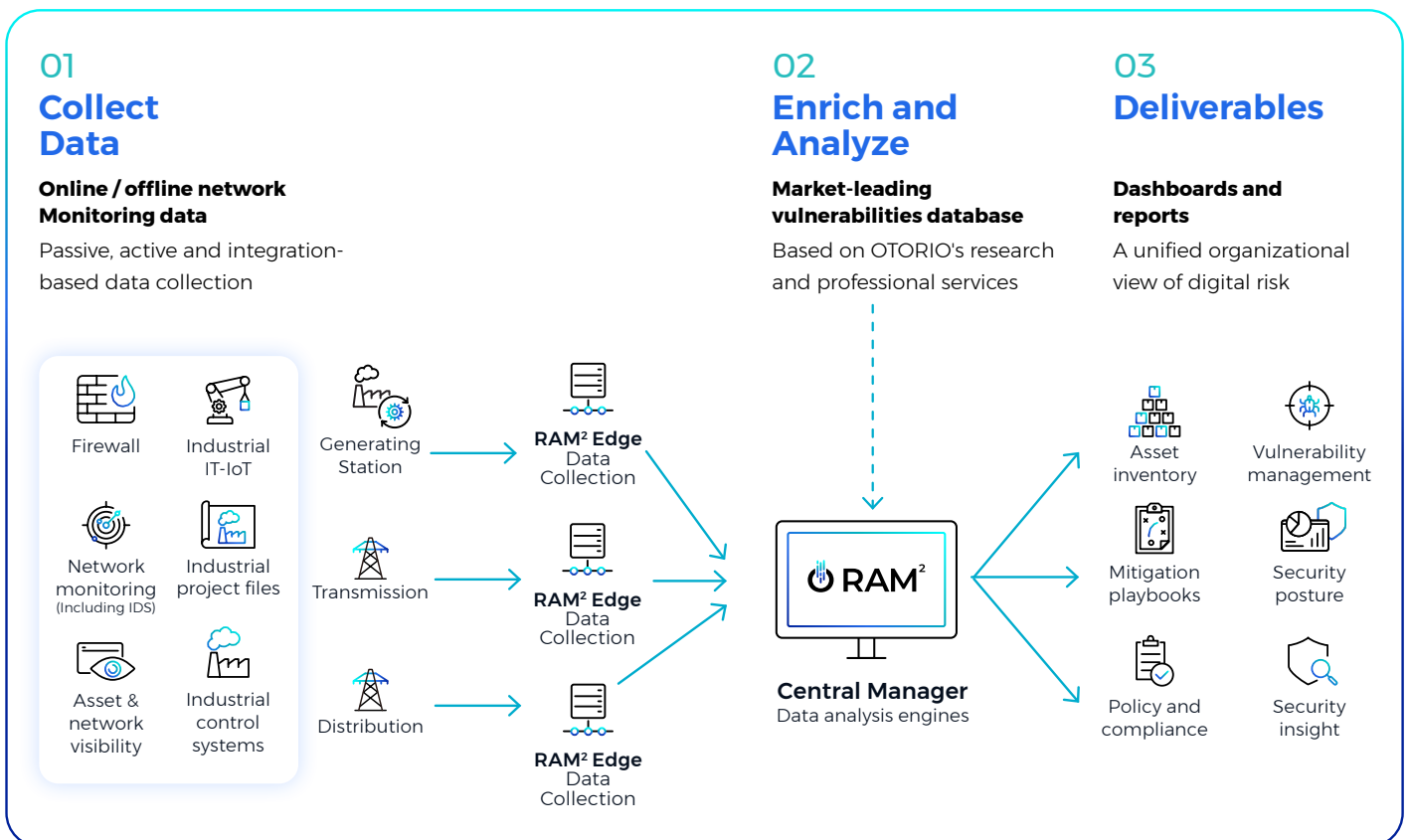
OTORIO's industrial-native OT cyber risk management platform is tailored to meet the unique needs of the electric utilities sector, providing consolidated visibility of all operational assets, business impact-driven risk prioritization, and prescriptive mitigation steps. Our solution bridges the gap between different domains and functions, enabling electric utility companies to confidently digitize processes without compromising safety, reliability, or efficiency.

With OTORIO's solution, security and operation engineer can work together to gain:

- Continuous security posture visibility and improvement
- Mitigate cyber and digital risks before they become breaches
- Detection of ongoing attacks and fast response
- Continuous compliance fulfillment

## Holistic, Scalable OT Risk Management Solution

RAM<sup>2</sup> automatically discovers OT, IT, and IIoT assets in electrical grids and maps them to operational processes while identifying the critical assets – power generation plants, substations, transmission lines, and more – as well as sub-processes and assets like control gates, transformers, grids, etc. RAM<sup>2</sup> proactively identifies exposures and risks before they become breaches. Upon detection of security gaps and vulnerabilities, RAM<sup>2</sup> delivers industry-native context-based prioritized risk with realistic mitigation playbooks. It also facilitates compliance governance, enabling security practitioners to easily enforce policies, industrial standards and more. The solution significantly improves the OT cybersecurity compliance governance's efficiency and accuracy by shortening the time and reducing the required resources.



## Comprehensive visibility of transmission and substations for enhanced security

Transmission asset owners face many issues—among them aging infrastructure, stringent operating requirements, financial constraints, and retiring expertise—that make maintaining and managing assets challenging. They seek safe, reliable, resilient, and cost-effective operations from their transmission lines and substations.

With OTORIO's RAM<sup>2</sup>, you gain complete and accurate visibility into your entire OT/ICS environment. From the site level down to level 0 assets, the platform provides automated asset inventory and vulnerability assessments, ensuring accurate vulnerability management. This comprehensive visibility allows you to identify security gaps and prioritize mitigation efforts effectively.

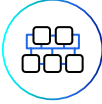







## Safeguarding the grid reliability and resiliency

The evolving landscape of customer expectations, regulatory and policy initiatives, extreme weather, and the imperative to incorporate distributed energy resources (DER) and advanced technologies are fueling transformations in the planning and operational approaches of distribution utilities for the grid. In response, utilities are investing in people, processes, and technology to modernize the grid and meet the utility's and its customers' future needs. OTORIO's RAM<sup>2</sup> enables impact-driven prioritization of the most critical risks in the smart grid environment, providing actionable prescriptive mitigation guidance tailored to electric utility's operational environments. By creating a common language between stakeholders, OTORIO's platform facilitates collaborative risk mitigation efforts and enhances operational resilience.

## Expedited Compliance assessment process for all transmission lines and substations

RAM<sup>2</sup> empowers security practitioners to conduct efficient security posture and compliance assessments, whether for a single asset or an entire operational network. OTORIO's platform provides out-of-the-box compliance assessment capabilities, supporting adherence to industry security standards such as NERC CIP, NIST 800-82, IEC 62443, NIS2, and more. With RAM<sup>2</sup>, you can obtain overall compliance scores, detailed deviation information, and remediation instructions, significantly reducing the time and effort required to generate assessment documentation.

### OTORIO's Benefits to Electric Utilities:

-  Automated, accurate asset inventory and vulnerabilities management, down to level 0 assets
-  Automated evidence collection and risk assessment
-  Simplify audit and Governance with out-of-the-box compliance
-  Extended coverage from a single asset to site level
-  Compliance score tracking and visibility for continuous improvement
-  Business-driven prioritization of mitigation actions
-  Actionable recommendations tailored to your operational environment
-  Ransomware-readiness assessments: host configuration gaps, FW rules and segmentation optimization, Security gaps identification

## 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.