OTORIO

Advanced Asset Visibility

Make it easier for OT security practitioners to manage operational risk more effectively.

The Importance of Advanced Asset Visibility

Advanced asset visibility is increasingly critical to OT security.

Protecting industrial control systems (ICS) and cyber-physical systems (CPS) is a complex challenge faced by companies across all industries. OT networks are increasingly connected to IT and IoT networks, creating a larger attack surface that needs to be accurately mapped, monitored and secured. Gartner reports emphasize that achieving comprehensive asset visibility in the OT environment should be a key priority for organizations and makes the following eye-opening 2025 predictions:

of OT security incidents will be caused by inadequate visibility into OT assets, up from 10% in 2015. [1]

of OT security solutions will include asset discovery and management capabilities, up from less than 10% in 2020.[2]

As an industrial-native security company, OTORIO understands the unique challenge of protecting operational technology. To protect everything they operate, industrial organizations need to deploy an integrative, holistic security strategy founded upon the concept of advanced asset visibility.

This eBook discusses the role and impact of advanced asset visibility in ensuring resilient operations.

1 Gartner. (2021). How to Develop an Operational Technology Cybersecurity Strategy.

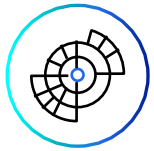
2 Gartner. (2021). Hype Cycle for Cyber and IT Risk Management.

Unique Challenges of OT/ICS Security in 2023

The OT threat landscape has become more complex and dynamic, creating unique challenges that complicate end-to-end operational security.

Outdated and legacy technologies are susceptible to security threats

As companies race to digitize, new potential attack vectors are created that make ICS and CPS more easily exploitable to attacks. Security practitioners must have a complete and accurate view of all the assets, including all hardware and software systems, network devices, and other connected components, to successfully protect operational environments.



Vast inter-connected IT and OT networks make accurate mapping complex

Operational technology is increasingly connected to IT and IoT networks. The compromise of one part of the network or digital asset can cascade into OT and affect operations. Security practitioners must comprehensively map entire IT-OT-IIoT networks with operational context to better understand network connections and impact on business.

Security control alert fatigue detracts focus from what's essential

Utilizing multiple security processes and technologies, like Firewalls and EDRs, creates a lot of unstructured alerts. It's impossible to triage everything at once or prioritize risk mitigation actions without understanding the role and impact of each risk. Reducing noise enables security practitioners to highlight and mitigate the most critical risks first.

Industrial organizations face a shortage of skilled OT security professionals

Security governance requires cross-department collaboration and mitigation. Basic recommendations provided by most security systems leave IT and OT security practitioners ill-equipped to eliminate security threats. Providing teams with a comprehensive mitigation framework with clear and practical instructions enables a faster and more efficient response.

You Can't Protect What You Can't See

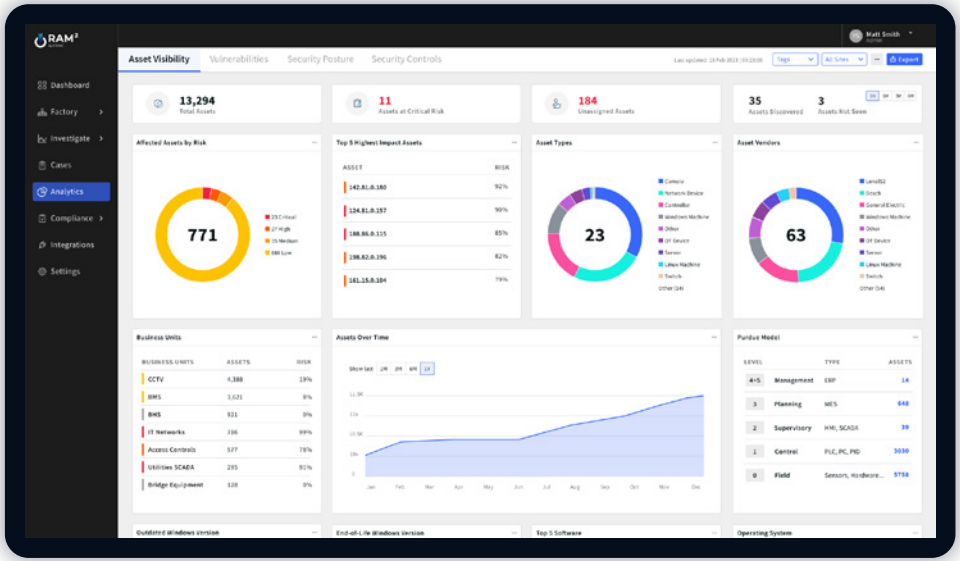
Advanced asset visibility enables organizations to improve MTTD (mean time to detect) and MTTR (mean time to response), increase visibility into OT devices and systems, improve asset management, and meet compliance requirements better. It is about more than mapping networks, assets, sites and processes, it is foundational to building an enterprise-wide OT security strategy with the following best practice:

- **Define people, processes and workflows to establish an enterprise-wide, holistic OT security strategy.**
- **Proactively manage risk by continuously monitoring the entire OT network to identify vulnerabilities in advance.**
- **Enrich attack vector analysis with operational context, so risk alerts are prioritized according to business impact.**
- **Facilitate better IT-OT security team collaboration by providing a unified framework with case management capabilities.**
- **Provide security practitioners with detailed mitigation guidance that enables fast and effective responses.**

Solution to Advanced Asset Visibility

See and monitor all devices, networks, and operational/industrial systems in the OT environment in real-time, using OTORIO's continuous OT cyber risk management solution.

Built upon the concept of advanced asset visibility, The OTORIO Titan platform enables organizations to discover vulnerabilities, proactively respond to security risk, and implement best practices suitable for the operational environment; all of which are critical for ensuring the safety and security of industrial control systems.



OTORIO Titan consolidates the visibility of the entire operational network, going deeper and richer to remove blind spots and noise from the operational environment by orchestrating the following:

- Complete, accurate visibility into asset inventories combined with operational insights, including the asset's role and impact on the environment.
- Scalable third-party integrations with other security and operational systems for a holistic view of the OT-IT-IIoT environments.
- Prioritized alerts based on operational context, highlighting the most critical risks, helping reduce the noise, and clear blind spots based on risk.
- Prescriptive risk-mitigation playbooks with clear, practical guidance that bridges skill gaps and significantly improves the MTTD and MTTR.

Case Study:

How an International Airport Manages Digital Risk with OTORIO in a Diverse OT-IT-IIoT Environment

The busy airport had limited security governance, initial asset documentation, and a partial work process to identify and reduce security risks. OTORIO worked directly with the security and operations teams to deploy the platform, provide them with advanced asset visibility, and implement a reliable enterprise-wide security strategy. OTORIO's expert OT security team even developed a unique plug-in for the CCTV management system that was able to discover assets that the airport's digital security team was unaware of.

OTORIO initially mapped 5,693 assets and identified 137 CVEs, 32 of which were critical. These numbers continue to grow by more than 10k+, which demonstrates the scalability, improved performance, and ROI of deploying OTORIO Titan.

Read the case study to see how OTORIO Titan was deployed and provided a busy International airport with advanced asset visibility and a unified risk management framework.

Assets by Type

Camera	3770
Controller	1351
Windows machine	282
OT device	269
Firewall	8
Linux machine	5
Software	5
Network device	3

CVEs affecting assets by severity

High	69
Medium	33
Critical	32
Low	3

Key takeaway

The OT devices detected were vastly outnumbered by thousands of cameras and controllers, leaving them with a significant potential attack surface. Many of these would not have been identified without OTORIO's advanced asset visibility and dedication to developing scalable integrations.

Summary

Advanced asset visibility is a critical component of operational network security and forms the foundations of an asset-centric security strategy.

Real-time advanced asset visibility enables security practitioners to detect and respond to potential security threats quickly, ensure compliance with regulations and standards, streamline security operations, and improve network performance.

The OTORIO Titan platform empowers industrial organizations to leverage a proactive risk-based approach orchestrated by advanced asset visibility.

The platform's flexible, plugin-based architecture is scalable and adaptable, and can be tailored to the unique characteristics of each vertical or specific operational environment. The ability to overlay the platform over various siloed systems enables OTORIO's platform to go beyond standard visibility, thereby improving the return on investment of existing security controls in the environment.

Learn More

3 Gartner Innovation Insight for Cyber-Physical Systems Protection Platforms Published 2 August 2022 - ID G00753275

About Us

OTORIO is a leader in OT security solutions, dedicated to safeguarding enterprise IoT and OT environments for enhanced safety, productivity, compliance and resilience. Its flagship platform, OTORIO Titan, provides an all-encompassing suite of applications that brokers IIoT, OT, and CPS security controls into IT workflows, ensuring proactive protection and efficient risk management.

Visit OTORIO.com

OTORIO