

OTORIO for the Pharmaceutical Sector

Data theft and process manipulation are not a mere matter of inconvenience in the pharmaceutical industry. They can pose a serious risk to operational reliability, employee safety, health, and business continuity.

OTORIO works with you to protect the integrity and availability of your products, so you can keep your employees and your consumers safe.

OTORIO – Your Partner for Secure Digital Production

Digital transformation makes the pharmaceutical industry more connected and productive – but also more exposed. Especially today, digital and cybersecurity risk avoidance becomes imperative to the success of automation development processes.

OTORIO delivers a suite of products and services that guarantee the safety and reliability of the plant from the network level down to the individual device. The OTORIO offering enables every machine and connected device to be monitored and controlled, meeting the highest standards of digital safety and cybersecurity. This ensures the continuous, uninterrupted operations that maximize digitization efficiencies.

Understanding the Unique Challenges of the Pharmaceutical Market

The OTORIO team is an integral part of safe industrial automation solutions. With decades of experience, the team is intimately familiar with the industry's particular challenges. Bringing best-practices and unique methodologies gained in multiple successful deployments in multi-vendor, multi-generational OT environments, OTORIO is ready to bring ROI and security value from day one.

A Unique Combination of Advanced Technology and Cyber Expert Services

Pharmaceutical companies can now benefit from a unique combination of OTORIO's OTORIO Titan solution, a next-generation OT security and digital risk-management platform, and OTORIO's broad portfolio of OT-centric, cyber-expert services.

Proactive Digital and Cyber Risk Reduction

Prevent

- **Threat Intelligence:** Receive a complete OT focused risk analysis that covers your digital footprint, third-party interfaces, production plant inventory, and potential attack scenarios.
- **Penetration Testing:** OTORIO's elite cybersecurity experts imitate advanced persistent attack patterns to uncover hidden attack surfaces and potential vectors.
- **Attack Simulation:** OTORIO creates a Digital Twin of your OT network, allowing you to run multiple attack simulations and obtain valuable insights with zero impact to production integrity.
- **Actionable Security Analysis:** Receive clear guidelines for improving your digital production's safety, integrity, and resilience.
- **Secure Remote Operations:** With OTORIO's remOT™ solution, operational teams, partners, and vendors can utilize secure remote access connectivity to OT environments.

Detect

- **Detailed view of asset inventory:** Integrating information from diverse operational and security data sources to discover, analyze, and monitor all OT, IT, and IIOT assets within the operational environment
- **Prioritized insights:** Based on the collected data, OTORIO Titan delivers clear alerts and insights that are prioritized based on their business impact.

Contain and resolve

- **Mitigation playbooks:** Easy to follow mitigation playbooks are built-in to OTORIO Titan to allow operational teams to successfully mitigate complex industrial cyber-risks before any damage can be done.
- **Collaboration with IT SOC:** OTORIO Titan gives SOC analysts access to logs and raw data and enables them to perform in-depth forensic investigations of the information leading up to, and following, the event.
- **Threat Hunting and Incident Response:** OTORIO's cybersecurity experts will assist you to triage, investigate, and mitigate threats as early as possible, to minimize risk and losses and maximize production integrity.



HIGH EXPOSURE



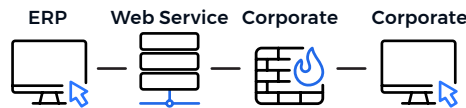
SERVICES & PRODUCTS

Intel collection,
reconnaissance & initial
access to the network

EXTERNAL INTERNET



IT NETWORK

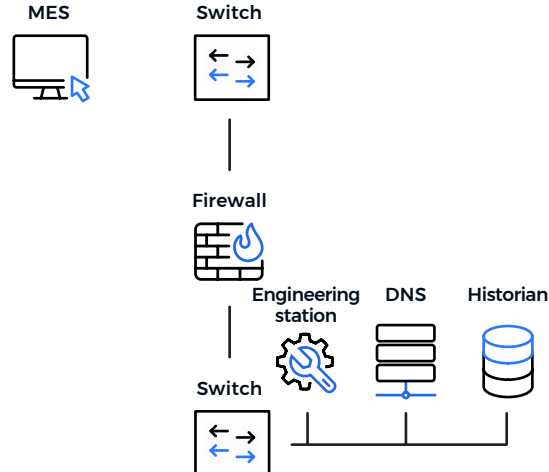


PREVENTION

- Threat Intel
- Security Assessment
- Attack Simulation

Usage of gathered
credentials and
footholds to reach and
communicate with **PLCs**
on the production floor

OT NETWORK



DETECTION

- Asset inventory
- Detailed insights
- Prioritised alerts
- Analyst-in-a-Box

Attackers can influence
production in any way
they wish – **damaging
operations or stealing
data**



Production Machinery A



Production Machinery B



Production Machinery C



CONTAINMENT

- Mitigation Playbooks
- Threat Hunting
- Incident Response

DEEP EFFECT

About OTORIO

OTORIO is a leader in OT security solutions, dedicated to safeguarding enterprise IIoT 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.