CASE STUDY

A Prescription for Protection

An Italian multinational in the pharmaceutical sector secures its critical plans and maintains regulatory compliance without interrupting production.

Overview

Fidia Farmaceutici recognised that protecting an industrial environment requires more than simply building a perimeter. As the convergence of IT and cyber-physical systems (CPS) infrastructure management practices increased, alongside greater digitalisation and remote access, the boundary between networks became highly porous. Faced with assets that possess long life cycles and severely limited downtime windows, Fidia required a model capable of detecting potential issues before they escalated into incidents. The organisation needed to generate clear evidence to support governance without requiring invasive interventions on delicate machine control systems.

Challenges

Before partnering with Claroty, Fidia Farmaceutici faced a complex landscape where traditional security mitigation strategies were incompatible with operational realities.

- **Expanding attack surface alongside legacy constraints:** Fidia's production environment housed a complex mix of control systems, automation components, and legacy applications layered over time. Frequent updates were unviable because any configuration change required exhaustive testing to ensure continued compliance with stringent pharmaceutical industry regulations, including the emerging requirements of NIS2 and the GAMP® 5 - 2nd Edition guidelines.

About Fidia Farmaceutici

Fidia Farmaceutici is an Italian multinational established in 1946, dedicated to creating healthcare solutions to improve quality of life. Known for harnessing the regenerating potential of Hyaluronic Acid, Fidia is a fully integrated company that controls its entire supply chain from research to marketing. The organisation employs 1,700 people and generated 510.1 million Euros in revenue in 2024. With a presence in over 120 countries, Fidia drives continuous innovation, supported by more than 310 clinical studies and 1,400 patents.

- **Heterogeneous systems and strict regulatory compliance:** Fidia's production environment housed a complex mix of control systems, automation components, and legacy applications layered over time. Frequent updates were unviable because any configuration change required exhaustive testing and revalidation to ensure continued compliance with stringent pharmaceutical industry regulations.
- **High operational risks of system revamping:** Faced with massive complexity, large scale revamping of control systems was practically impossible to execute safely in the short term. Gilberto Rossi, Corporate OT & Industrial Process Automation Manager at Fidia Farmaceutici, noted that unpredictable machine downtime and strict compliance activities made such projects too risky for operational continuity.
- **Blind spots in dynamic asset visibility:** The heterogeneity of the plant made it incredibly difficult to rely on a static snapshot of the asset landscape. Because an asset that is unconnected today might become connected tomorrow, this limited visibility represented a security risk that continuously grew over time.

> **"Claroty has enabled the continuous and automatic updating of the system inventory and risk analysis, thanks to the constant updating of the vulnerability index of field devices, providing real time reporting on assets and any changes introduced."**
>
> **Gilberto Rossi,** Corporate OT & Industrial Process Automation Manager at Fidia Farmaceutici

Solution

To address these compounding risks, Fidia selected a top-down, 'Cybersecurity by Design' approach supported by Claroty and ServiTecno, a leading provider of platforms and services in the pharmaceutical sector. This strategic partnership allowed Fidia to complete part of their remediation work ahead of schedule, creating the conditions to plan interventions over time in a highly controlled manner.

- **Passive monitoring via Deep Packet Inspection:** Fidia deployed Claroty xDome to observe the environment without interfering with delicate pharmaceutical processes. The platform analyses network traffic passively at interconnection points, interpreting industrial protocols and distinguishing commands from standard readings without requiring agents on sensitive control systems.
- **Establishing structural domain segregation:** The organisation prioritised a top down approach by establishing structural domain segregation. By defining specific zones, permitted relationships, and interconnection points, Claroty helped Fidia govern access and maintenance activities, fundamentally limiting the propagation of unwanted events across the network.
- **Behavioural baselining and event detection:** Because CPS environments rely on deterministic and repetitive communications, the Claroty platform established a reliable baseline of normal operations. By leveraging machine learning models alongside DPI, the system precisely identifies anomalous patterns and deviations, drastically reducing false positives while highlighting configuration errors or untracked maintenance activities.

- **Zero Trust remote access management:** To further secure their perimeter, Fidia implemented the Claroty Secure Access. This allowed for the controlled management of remote access according to Zero Trust principles, ensuring full traceability and auditability of all remote activities within the production environment.
- **Implementing an integrated CMDB model:** With support from ServiTecno during the OT dedicated Network Design Phase, Fidia built an Integrated Configuration Management Data Base (CMDB) Model. Within this model, Claroty serves as the main pillar for Inventory, Surveillance, and Prevention, acting as the ultimate weapon to respond to NIS2 remediation requests over the next three crucial years.

Benefits

Since deploying Claroty xDome, Fidia Farmaceutici has transformed its operational resilience, turning complex CPS security into a streamlined enabler of governance.

- **Automated and continuous asset inventory:** By powering the Integrated CMDB Model, Fidia transitioned from static guesswork to a dynamically updated, real-time inventory. The continuous monitoring provided by Claroty xDome automatically identifies new assets and changes in communication patterns, serving as a powerful tool for NIS2 compliance by providing a continuously updated vulnerability index and a dynamic view of risk exposure.
- **Significant resource optimisation:** The implementation of Claroty xDome delivered tangible operational benefits by drastically increasing the level of control across the plant. Crucially, this heightened security posture was achieved while simultaneously reducing the manual resources previously required for continuous network monitoring.
- **Enhanced traceability for regulatory audits:** In the highly regulated pharmaceutical sector, the ability to produce evidence is just as vital as preventing incidents. The newly gained visibility into network flows and configuration traceability allows Fidia to rapidly reconstruct events and decisions, significantly strengthening controls and enabling faster responses to both internal and external compliance audits.
- **Alignment with emerging regulations:** Fidia's technological partnership established clear governance and structural control over their new OT infrastructure. By taking a proactive approach with their CMDB design, Fidia is now positioned ahead of the curve to satisfy stringent pharmaceutical guidelines, including GAMP® 5 - 2nd Edition and the emerging NIS2 regulation.
- **Accelerated diagnosis without production halts:** By correlating CPS events with IT activities, such as remote access or supplier interventions, Fidia can quickly assess the true impact of an anomaly on the production process. This clear visibility accelerates diagnosis, prevents impulsive reactions, and allows the organisation to adopt proportionate countermeasures, successfully protecting their infrastructure without stopping the factory.

> **"In the pharmaceutical sector, CPS cybersecurity must coexist with complex plants, long lifecycle systems, and stringent regulatory requirements. Anomaly detection is a key element, but it delivers real value only when embedded within a broader model of visibility, dynamic asset inventory, and continuous risk assessment.**
>
> **Fabrizio Alviti,** Sales Director Mediterranean Region at Claroty

Conclusion

Fidia Farmaceutici has successfully transitioned from an environment constrained by legacy technology and limited visibility to a resilient, data driven operational model. By leveraging Claroty xDome alongside the expert support of ServiTecno, Fidia built an Integrated CMDB Model and established a continuous control layer that provides deep network visibility and precise anomaly detection without disrupting critical pharmaceutical production. This strategic 'Cybersecurity by Design' investment ensures that Fidia can proactively manage the risks associated with IT and CPS convergence, confidently tackle NIS2 regulation requirements and GAMP® 5 guideline suggestions, preserve process quality, and secure their vital infrastructure for the future.

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organisations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organisations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.