

**CASE STUDY**

Strengthening the Pharmaceutical Defense Line – Phlow Leverages Claroty Technologies for Unparalleled Cyber-Physical System Protection

Introduction

Phlow Corp. is a pharmaceutical contract development and manufacturing organization working to reimagine the manufacture and science behind life-changing medicines. Phlow supports its customers through tech-enabled process excellence, innovation, and advanced manufacturing with a commitment to providing high-quality, life-saving, and life-enhancing treatments. Phlow's Virginia-based operations consist of research and development labs, a Kilo-Scale cGMP facility, a Metric-Ton scale cGMP manufacturing facility, and a highly automated warehouse.

Phlow is now manufacturing critical essential medicines through modern approaches to medicine manufacturing that challenge the scientific and manufacturing status quo.

At the heart of these complex operations lie advanced Cyber-Physical Systems (CPS). These systems drive Phlow's sophisticated technological stack, overseeing an array of operations in research labs, stringent quality control in manufacturing lines, and efficient inventory management in warehouses.



Phlow is a U.S.-based, Certified B Corporation™ leveraging advanced manufacturing processes to reimagine the domestic production of key starting materials, active pharmaceutical ingredients (API), and finished drug products that are critical to U.S. healthcare. Utilizing its advanced R&D labs and best-in-class, tech-enabled cGMP facilities ranging from kilo to metric ton scales, Phlow provides customized contract development and manufacturing services for small molecule APIs. Phlow measures its success by driving down costs and waste, improving quality and yield, and offering a more environmentally friendly approach to manufacturing medicines that lead to healthy and resilient communities.

With the fast-paced progress in connected industrial control systems and cyber threats unfolding with equal aggression from state-sponsored hackers and corporate spies alike, it was crucial for Phlow to ensure their vital CPS was securely protected. This necessity marked Phlow's pursuit of a comprehensive CPS solution that could holistically secure their operational assets.

Identifying the Problem

The leadership at Phlow realized that to compete with the low cost of labor available in other drug-producing countries, they needed to rely on the convergence of Information Technology (IT) and CPS to provide opportunities for enhanced operation efficiencies. Phlow operates in a highly critical industry where even the slightest business disruption can lead to significant challenges. Phlow relies on its CPS for drug discovery, research, production, and distribution. Additionally, even if handled correctly, the use of CPS can pose threats in and of itself due to greater interconnectivity and potential for breach points. Without top-of-the-line security measures, these sophisticated, interlinked systems are vulnerable to attacks, which could lead to data theft, manufacturing interruption, or even harm to public health.

“We cannot afford to allow potential threats to escalate, placing our critical infrastructures at risk of unwarranted attacks. With the growing sophistication of cyber threats, it is imperative to adopt a comprehensive security solution that specializes in addressing the unique vulnerabilities inherent in converged IT and CPS systems.”

– JUAN PIACQUADIO, CIO AND VP, IT/IS

Phlow sought a solution that demonstrated mastery of CPS security complexities. The solution could defend intricate networks amidst these dynamic threats while sustaining operational efficiency in the converged environment.

Why Claroty?

Before working with Claroty, Phlow ran a comprehensive search and evaluation process, considering several top providers in the CPS security marketplace. Each solution evaluated had unique strengths, but none offered comprehensive coverage, unparalleled visibility, in-depth industry understanding, and proactive risk-mitigation tactics to the same extent as Claroty.

“Our research revealed that Claroty is a market leader with an impressive track record and a strong financial position. Claroty demonstrated a forward-thinking approach to thought leadership, aligning with our goal of partnering with an organization that is truly driving innovation in the field.”

- JUAN PIACQUADIO, CIO AND VP, IT/IS

Known for its continuous threat detection, Claroty has a unique approach to tackling CPS security challenges. Several reasons accounted for Claroty's selection:

- **Comprehensive Coverage:** Claroty's extensive portfolio breadth provides end-to-end protection across the entire CPS stack.
- **Unparalleled Visibility:** It delivers unparalleled visibility into CPS networks, aiding in continuous threat monitoring and system vulnerability management.
- **In-depth Industry Understanding:** Claroty's extensive experience with industrial networks, devices, and protocols, along with their deep understanding of pharmaceutical manufacturing processes gained from having some of the biggest pharma customers in the Fortune 500, made them a fitting choice.
- **Unrivaled Network Insight:** Claroty provides the industry's first out-of-the-box zone and communication policy recommendations for various CPS based on in-depth insight into the operational context and best practices, driving network segmentation and anomaly detection.
- **Proactive & Risk-mitigation Tactics:** Claroty's ability to predict, detect, and neutralize threats before they cause serious damage was a critical aspect that resonated with Phlow.

Implementation And Results

In partnership with Claroty, Phlow implemented a tailored CPS security infrastructure using Claroty xDome. Phlow now has a robust security layout, providing rigorous network visibility, real-time monitoring, and instantaneous threat detection.

Asset management is at the heart of Phlow's implementation. Their highly specialized assets required tailored security strategies. With Phlow working as a part of a network of services with partners that also manufacture for them, it was critical to have tight controls.

With Claroty xDome's proactive approach, Phlow gained comprehensive visibility to its entire CPS asset portfolio, allowing technicians to maintain a detailed and updated inventory. This plays a pivotal role in identifying and rectifying system vulnerabilities before they can be exploited.

Micro-segmentation proved to be an equally significant security aspect. By dividing the OT network into smaller, isolated sections, Claroty could limit lateral movement within the network, thus containing any potential threats within a localized area and preventing its spread to the larger network.

Phlow was in the process of switching and standardizing networks and firewalls, and Claroty's integrations with both its prior and new vendors helped it through the transition effectively and quickly, providing better micro-segmentation and greater risk control.

Conclusion

Leveraging Claroty xDome has been transformative in redefining Phlow's CPS security matrix, taking it from a point of vulnerability to one of strength. Their collaboration has widened the lens through which Phlow perceives its entire operational continuum—from precision-dependent research labs to process-intensive manufacturing facilities and automation-driven warehouses. The tactical mixture of asset management and micro-segmentation provided a robust, tailored defense against potential cyber intrusions.

The work with Claroty has helped Phlow sustain its commitment to modernizing medicine manufacturing, ensuring that its infrastructure and operations remain fortified against cyber threats. Because Claroty xDome is built on the AWS platform, it leverages AWS's inherent scalability and security features, such as encrypted connections between on-premise networks and AWS, immediate access to new features and threat definitions, and automated updates. These features ensure a comprehensive and adaptive cybersecurity posture that aligns with modern demands for flexibility and scalability in security solutions.

In sum, beyond the substantial CPS security benefits, leveraging Claroty's technologies has amplified Phlow's operational resilience, safeguarded its reputation for trust and reliability, and ultimately, protected the end-consumers. Through this transformative journey, Phlow has set an industry standard on cybersecurity, demonstrating that robust CPS defense is not just feasible but critically essential in today's hyperconnected manufacturing environment.

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 organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations 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.