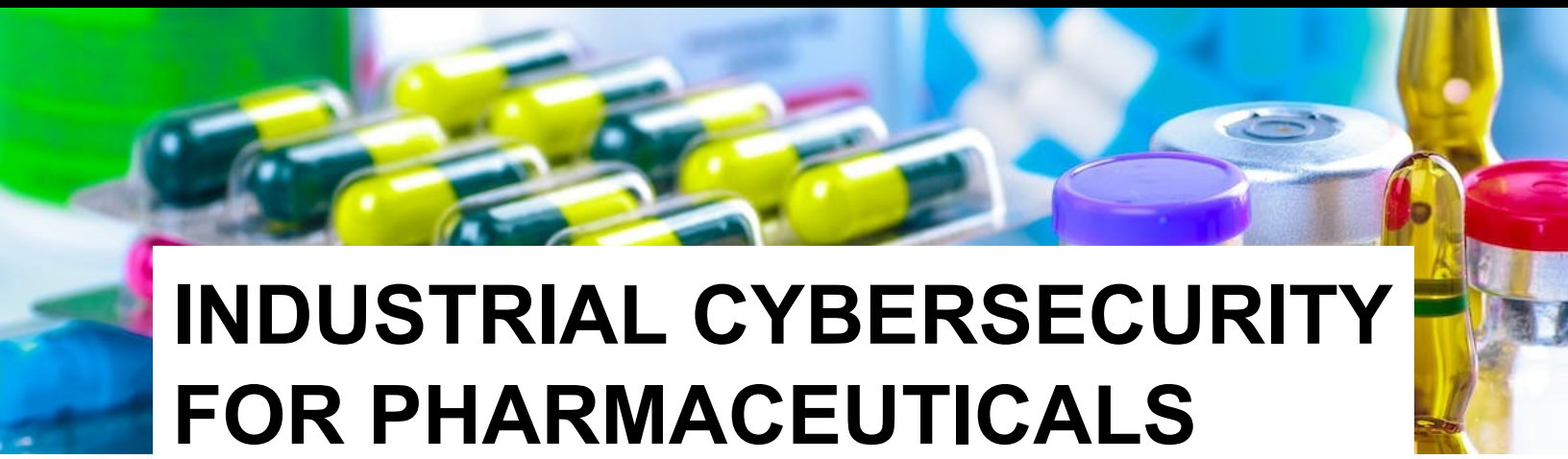
CLAROTY

SOLUTION BRIEF



INDUSTRIAL CYBERSECURITY FOR PHARMACEUTICALS

How Claroty enables pharmaceutical companies to enhance batch consistency, safety, and uptime by hardening their plant operations against cyber threats.

PART I: The Industrial Cybersecurity CHALLENGE in Pharmaceuticals

The sector is facing complex economic, environmental, and geopolitical conditions

Rising Competition | **High Inflation** | **Aging Population** | **Sustainability Urgency** | **Supply Chain Constraints**

These conditions are motivating many companies to accelerate digital transformation

Automation

Plants are replacing once-manual, error-prone tasks with computerized automation systems to increase production efficiency, optimize quality assurance, and boost safety

IT/OT Connectivity

Cloud migrations and remote work are connecting IT and the cloud to OT via remote monitoring, CIP, and ERP solutions to improve productivity, streamline audits, and enhance sanitation

Cyber-Physical Systems (CPS)

Pharma companies are embracing Industry 4.0 by augmenting their automated, connected OT environments with even more CPS to boost OEE and throughput

Digital transformation is exposing pharmaceutical manufacturing to cyber attacks

From biochemical manufacturing to packing, operations across all segments of the pharmaceutical sector still depend considerably on outdated OT infrastructure with legacy (and, therefore, unsecured) systems. Replacements can be prohibitively expensive not only due to equipment costs – but also due to the downtime that new installations and upgrades often require.

At the same time, the sector continues to embrace digital transformation – resulting in more and more manufacturing operations being underpinned by a complex patchwork of legacy OT equipment intertwined with modern, internet-connected devices and other CPS. This ever-growing connectivity is inadvertently expanding the attack surface for many pharmaceutical companies, ultimately exposing their business-critical processes to cyber threats. This unfortunate reality has repeatedly manifested in the form of ransomware and other attacks that exploit security weaknesses in OT environments across the sector.

Governments are increasingly urging pharmaceutical companies to secure OT

The WannaCry, NotPetya, and Novartis cyber attacks are merely a few of seemingly countless disruptive and even dangerous cybersecurity incidents that have affected pharmaceutical leaders in recent years. Upticks in the frequency and impact of such incidents has since elicited robust responses from governments in the form of new recommendations and regulations that encourage – or, in some cases, mandate – that pharmaceutical companies take action to secure OT. Key developments include:

NIS2 Directive (EU)

SOCI (Australia)

cGMPs (US)

CPGs (US)

Since OT is distinctly different from IT, securing OT requires a different approach

OT environments – and the CPS that underpin them – in all segments of the pharmaceutical sector are fundamentally different from their IT counterparts, which is why securing OT requires a unique approach. Some of these key differences include:

	Purpose	Top Priorities	Typical Composition	Patching Frequency	Compatibility
IT:	*Control the Flow of Information*	*Confidentiality, Integrity, Availability*	*Standard Protocols & IT Systems*	*Very Frequent*	*Compatible with IT Security Tools*
OT:	*Control Physical Processes*	*Safety, Availability, Reliability*	*Proprietary Protocols & Legacy OT Systems*	*Relatively Rare*	*Incompatible with IT Security Tools*

PART II: The Industrial Cybersecurity SOLUTION for Pharmaceuticals

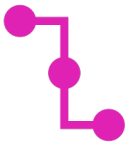
Claroty's Approach to Securing OT: Key Principles for Pharmaceutical Companies

Recognizing that securing the OT environments that underpin pharmaceutical manufacturing can be a complex endeavor, Claroty has tailored our industrial cybersecurity portfolio to reflect three principles that help streamline and optimize this journey.

1. Gain visibility into all CPS in OT

Visibility is foundational to securing OT— which is why pharmaceutical companies must attain a full inventory of all OT, IoT, and BMS assets and other CPS across all plants.

It's also why Claroty is proud to deliver the unmatched visibility our pharmaceutical customers need to secure the OT environments on which their business-critical operations rely.



2. Integrate IT Tools with OT

Since many CPS in pharmaceuticals use proprietary protocols and legacy systems, they are incompatible with IT solutions — but that doesn't mean such solutions have no place in OT.

Rather than require customers to expand their already-extensive tech stacks, Claroty integrates with them. As a result, customers can simply extend their IT tools and workflows to OT.

3. Extend IT controls to OT

Unlike their IT counterparts, it is common for OT environments in all segments of the pharmaceutical sector to lack essential security controls and consistent governance.

After providing visibility into all CPS and integrating IT tools and workflows with OT, Claroty extends existing IT controls to OT — unifying security governance and driving resilience across IT and OT.

How Claroty Equips Pharmaceutical Companies to Drive Resilience from IT to OT

Claroty's comprehensive industrial cybersecurity portfolio and team of domain experts empower pharmaceutical manufacturers to extend — and further optimize — the following cybersecurity use cases and governance controls from IT to OT:

Vulnerability Management

Network Segmentation

Endpoint Protection

Secure Remote Access

Threat Detection

Asset & Change Management

The above use cases and capabilities also enable pharmaceutical customers to more-easily and effectively satisfy regulatory requirements, implement industry standards, best practices, and frameworks, streamline audits, and minimize noncompliance.

NIS2

SOCI

CPGs

cGMPs

NIST CSF

IEC 62443

Why Pharmaceutical Leaders like Pfizer Trust Claroty

Pfizer is just one of dozens of the world's top pharmaceutical companies that trust Claroty to protect the critical CPS on which the health, safety, and stability of our society depend. Here are a few of the key factors that have helped us to earn this trust:

40+

Awards

Our comprehensive cybersecurity platform has earned dozens of accolades for seamlessly enhancing the safety, security, and efficiency of OT, IoT, IIoT, BMS, and other CPS.

420+

Disclosures

Our award-winning Team82 researchers have disclosed more vulnerabilities than any other group, enhancing our customers' protections while drive security industry-wide.

Top 3

Industrial Automation Vendors

The Top 3 automation vendors (Rockwell Automation, Schneider Electric, and Siemens) invest in, partner with, and are loyal customers of Claroty, validating our leadership.

About The Claroty Portfolio

Unlike generic solutions, Claroty's industrial cybersecurity portfolio is purpose-built for the unique security and operational needs of the pharmaceutical sector. Complementary strategic guidance from Claroty's experts further enables pharmaceutical manufacturers to not only secure OT – but also drive business value on their industrial cybersecurity journey. Solutions include:

Claroty xDome

Claroty xDome is a highly flexible, modular, SaaS platform purpose-built for all use cases & types of CPS on the entire industrial cybersecurity journey.

Claroty CTD

Claroty Continuous Threat Detection (CTD) is an on-premises solution that offers robust cybersecurity controls for critical infrastructure environments.

Claroty SRA

Claroty Secure Remote Access (SRA) delivers frictionless, reliable, secure remote access and management for internal and third-party OT personnel.

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for asset visibility, asset and change management, risk and vulnerability management, network segmentation, endpoint protection, threat detection, secure remote access, and more.

Backed by the world's largest investment firms and industrial automation vendors, 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.