

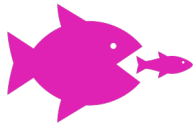


INDUSTRIAL CYBERSECURITY FOR FOOD & BEVERAGE

How Claroty empowers food & beverage companies to enhance efficiency, batch consistency, and uptime while hardening their production lines against cyber threats.

PART I: The Industrial Cybersecurity CHALLENGE in Food & Beverage

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



Extreme Competition



High Inflation



Varietal Demand



Sustainability Urgency



Global Shortages

These conditions are motivating many companies to accelerate digital transformation



Automation

Plants are replacing once-manual tasks with computerized automation throughout their OT environments to accelerate delivery, enhance product consistency, and boost uptime



IT/OT Connectivity

Cloud migrations and remote work are extending connectivity across the entire enterprise from IT via ERP, MES, and other systems to OT to improve efficiency, maintenance, and quality control



Cyber-Physical Systems (CPS)

Plants are further embracing Industry 4.0 by augmenting their automated, connected OT environments with more, newer CPS to optimize monitoring and delivery while reducing costs

Digital transformation is exposing food & beverage operations to cyber attacks

From processing to packaging, most food & beverage manufacturing operations still depend considerably on outdated OT infrastructure with legacy (and, therefore, unsecured) systems.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. Since nearly all food & beverage companies have low-margin, high-volume business models, their tolerance for downtime is, understandably, low.

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 food & beverage companies, ultimately exposing their revenue-generating, 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 food & beverage companies to secure OT

The Molson Coors, JBS, Lion, and Dole ransomware attacks are merely a few of seemingly countless disruptive cybersecurity incidents that have affected the food & beverage sector 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 food & beverage companies take action to secure OT. Key compliance developments include:



NIS2 Directive (EU)













The SOCI Act (Australia)



CISA 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 food & beverage sector are fundamentally different from their IT counterparts, which is why securing OT requires a unique approach. Some of these 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 Food & Beverage

Claroty's Approach to Securing OT: Key Principles for Food & Beverage Companies

Recognizing that securing the OT environments that underpin food & beverage operations 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 all segments of the food & beverage sector must attain a complete inventory of all OT, IoT, and BMS assets and other CPS across all processing and packaging operations.

It's also why Claroty is proud to deliver the unmatched visibility our food & beverage customers need to secure the OT environments on which their business-critical production lines rely.



2. Integrate IT Tools with OT

Since most CPS in food & beverage processing and packaging 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 food & beverage sector to lack essential security controls and consistent governance – especially across different sites and regions.

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 Food & Beverage Companies to Drive Resilience from IT to OT

Claroty's comprehensive industrial cybersecurity portfolio and team of domain experts empower food & beverage 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 food & beverage customers to more-easily and effectively satisfy regulatory requirements, implement industry standards, best practices, and frameworks, streamline audits, and minimize noncompliance.



NIS2



SOCI



CPGs



NIST CSF



IEC 62443

Why 8 of the World's 10 Largest Food & Beverage Companies Trust Claroty

Food & beverage leaders globally trust Claroty to protect the critical CPS on which the safety, nourishment, and stability of our society depend. Here are a few of the key factors that set Claroty apart and have been integral in enabling 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 food & beverage sector. Complementary strategic guidance from Claroty's experts further enables food & beverage customers 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 (XIIoT). 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.