DRAGOS

SOLUTION BRIEF

Protect The Process Behind Every Product

Modern cybersecurity must go beyond IT to protect the industrial control systems at the heart of food and beverage manufacturing: the systems that set recipes, hold temperatures, and keep every line running.



Updated November 2026

The Market: A Critical Sector That Never Stops

Food and beverage manufacturing is the largest employer in U.S. manufacturing. The sector employed about 2.1 million people in 2024, 16% of all manufacturing workers, and is projected to add 130,000 jobs by 2034, more than any other manufacturing sector. Output is projected to pass $1 trillion by 2034.

Plants run 24/7 across multiple lines, with thin margins and perishable inventory. That is exactly what makes the sector attractive to ransomware operators: every hour offline is lost product, missed shipments, and pressure to pay. Food and agriculture organizations faced 265 ransomware attacks in 2025.

The stakes reach past the balance sheet. When a tainted product reaches the market, the damage to public health and brand reputation can be irreversible. Food companies spend upward of $55 billion a year on legal, healthcare, and lost productivity costs tied to operational failures. In 2017, after more than two dozen children fell ill with E. coli linked to a soy nut butter product, both the brand owner and its manufacturer filed for bankruptcy within months.

Food Safety Is Now a Cyber Problem

The U.S. Food Safety Modernization Act (FSMA) Intentional Adulteration rule requires food companies to implement mitigation strategies against deliberate contamination, one of the most aggressive “food defense” mandates in the world. Threats range from disgruntled insiders to politically motivated sabotage. If an adversary reaches the industrial control systems (ICS) that manage production, a cyber incident becomes a food safety incident.

The xOT Security Challenges Facing Food and Beverage

ICS control product quality and recipe execution: ingredient ratios, cook and pasteurization temperatures, fill levels, and cold storage before shipment. Any unauthorized change to a controller, from a sophisticated attack or an honest mistake, can produce unsafe product. Food safety demands zero tolerance for unintended process changes, so a suspected issue means the line stops until the problem is found.

Key Challenges

- Legacy controllers with no authentication or encryption
- IT, IIoT, and cloud connections reaching the line
- Proprietary protocols IT tools cannot see
- Incomplete, outdated asset inventories
- Insider error and open vendor access
- Ransomware that halts production from IT

Outcomes & Benefits

BUSINESS

- Less unplanned downtime across lines and shifts
- Protected food safety, product quality, and brand trust
- Support for FSMA food defense plans and audit readiness
- Revenue protected from operational disruption

OPERATIONAL

- Visibility into every system that influences the physical process
- A short, prioritized vulnerability list
- Faster detection, investigation, and recovery
- A documented history of every change

© 2026 Dragos, Inc. All Rights Reserved.

What Makes Food and Beverage OT Hard to Defend

- **Controllers built before security mattered.** Most PLCs and DCS controllers lack authentication, encryption, and authorization. Anyone who can reach them on the network can often change them.
- **Connectivity that outpaced protection.** MES, ERP, historians, wireless sensors, IIoT, and cloud-connected refrigeration now touch the line. Every connection is a path in, and a breach of any IT or OT device puts the whole control network at risk.
- **Proprietary protocols and blind spots.** OT networks speak dozens of industrial protocols IT tools cannot parse, and many plants have no complete, current asset inventory.
- **Insiders and third parties.** Human error is a leading cause of downtime: a change pushed to the wrong PLC, incomplete DCS maintenance, or an integrator's remote session left open.
- **Thin reporting, low awareness.** Few incidents are disclosed, and FDA food defense guidance has historically said little about cyber, reinforcing a false sense of low risk.

By the Numbers

81%

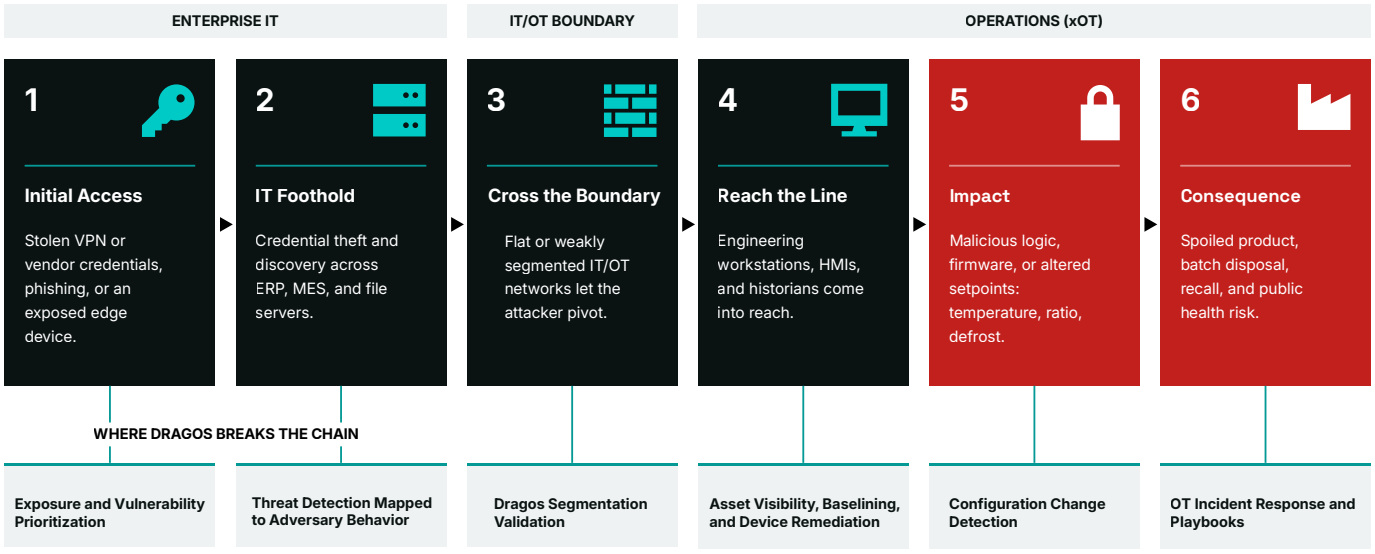
of Dragos services engagements found poor IT/OT segmentation.

73%

of Dragos incident response cases involved exploited or reused VPN and jump-host credentials.

Anatomy of a Breach

How a ransomware intrusion typically moves from a stolen credential to a stopped line, and where Dragos breaks the chain.



Proven in food and beverage. The Boston Beer Company secures its manufacturing environments with the Dragos Platform and OT Watch, modernizing its xOT security program while reducing risk and cost.

© 2026 Dragos, Inc. All Rights Reserved.

Recent Attacks on Food and Beverage

Nov 2026

European grocery chains

Attackers reached internet-exposed refrigeration controllers at dozens of supermarkets across several countries and reset them to defrost. One chain disposed of chilled and frozen product at eight stores. It followed a similar wave at hundreds of French stores in October.

Jul 2026

Fairlife (The Coca-Cola Company)

Ransomware affected production systems at the dairy brand, forcing a suspension of all U.S. production. Canadian operations were unaffected.

Sep 2025

Asahi Group

Qilin ransomware disrupted ordering and shipping and halted most of the brewer's domestic production in Japan. Recovery stretched past a month on manual workarounds.

Jun 2025

United Natural Foods (UNFI)

A cyberattack forced systems offline at the primary distributor to Whole Foods, leaving empty shelves. UNFI projected a $350 to $400 million hit to sales.

Feb 2023

Dole

Ransomware led Dole to shut down systems across North America and temporarily halt production.

May 2021

JBS Foods

REvil ransomware shut every JBS beef plant in the U.S., nearly a quarter of national supply. JBS paid an $11 million ransom.

Sector Signal

265

ransomware attacks hit food and agriculture organizations in 2025, according to the Food and Ag-ISAC.

The Pattern

Most of these incidents began in IT. The production impact came from shutting down, not from adversaries operating the line. Both are preventable with visibility and segmentation.

© 2026 Dragos, Inc. All Rights Reserved.

Common Protocols on the Plant Floor[1]

A food or beverage plant often runs many industrial protocols side by side. Dragos performs deep packet inspection of 600+ industrial protocols, so it understands what each command does, not just that traffic moved.

PROTOCOL	WHERE IT RUNS
EtherNet/IP (CIP)	Line PLCs, drives, packaging, case packing, and palletizing cells
PROFINET / PROFIBUS	Filling, bottling, and process skids
Modbus TCP / RTU	Refrigeration, compressors, boilers, and utility instrumentation
S7comm / S7comm-plus	Controllers running batching, mixing, and thermal processing
OPC UA / OPC Classic	MES, historians, and OEM machine integration (PackML)
BACnet	Cold storage, HVAC, and environmental controls
HART / FOUNDATION Fieldbus	Flow, level, and temperature instruments on pasteurizers and Clean In Place systems
MQTT	IIoT sensors and cloud-connected cold-chain monitoring

[1] These are some of the protocols commonly used in food and beverage operations. This list is representative, not exhaustive.

Key Requirements and How Dragos Helps

01

See every asset across xOT environments

Discover and track every connected device in real time, including dormant wireless headsets and leak sensors that can open a path to a mixing tank.

> **How Dragos Helps:** The Dragos Platform builds an always-current inventory through a multi-detection engine, the Dragos Agent for scheduled collection, and project file import, profiling make, model, and firmware. Dragos Exposure Management extends that inventory across the full xOT environment. Dragos Software Supply Chain checks the firmware and code of assets for backdoors and unverified changes that could be the launching point for a security event.

02

Find and fix vulnerabilities before they are exploited

Actively manage the attack surface from procurement to processing to delivery.

> **How Dragos Helps:** OT-corrected scoring and “Now, Next, Never” prioritization isolate the 3-6% of OT vulnerabilities that need immediate action, with alternative mitigations when a line cannot be patched. Dragos Device Remediation adds credential rotation, firmware updates, and secure configurations at scale.

© 2026 Dragos, Inc. All Rights Reserved.

03

Keep a full audit trail for every configuration change

Know who changed what, when, and recover the last known good state fast.

> **How Dragos Helps:** Configuration detections flag changes to PLC programming modes and settings. Case management and timeline views reconstruct activity, separating a maintenance error from adversary activity.

04

Prove segmentation between business systems and the line

Show that ERP, MES, and vendor access cannot reach controllers they should not.

> **How Dragos Helps:** Dragos Segmentation models the access paths your firewall, router, and switch configurations permit, so teams find overly permissive rules before anyone uses them.

05

Detect threats in operational context and respond with experts

Spot adversary behavior early and contain it without disrupting safe production.

> **How Dragos Helps:** Threat behavioral detections are built on Dragos xOT Threat Intelligence covering 26+ OT threat groups, and Neighborhood Keeper shares insights across the community. OT Watch provides proactive threat hunting, OT Watch Complete adds 24/7 monitoring and triage, and Dragos incident responders bring over a decade of OT-specific experience.

One Intelligence Model, Three Views

The Dragos Intelligence Fabric connects three views of the threat into one picture for food and beverage operations.

- **What has happened.** More than a decade of OT-specific telemetry, adversary research, and incident response shows how attacks on industrial environments have unfolded and what worked to stop them.
- **What is happening.** Dragos xOT Threat Intelligence tracks OT threat groups and the campaigns targeting manufacturers today, so defenses reflect current adversary behavior.
- **What is hiding.** OT Watch threat hunters use that same intelligence to search your environment for activity your alerts have not caught yet.

What one view finds feeds the others, so detections, priorities, and response guidance stay current.

Requirements

- ☑ FSMA Intentional Adulteration Rule (21 CFR 121)
- ☑ SANS Five ICS Critical Controls
- ☑ ISA/IEC 62443
- ☑ NIST CSF 2.0
- ☑ NIS2 (EU food production)

© 2026 Dragos, Inc. All Rights Reserved.

About Dragos

Dragos is the global leader in xOT cybersecurity and is purpose-built to protect the industrial and critical infrastructure that civilization depends on.

The Dragos Platform delivers visibility, continuous monitoring, and threat detection across expanded xOT environments at scale. It is powered by the Dragos Intelligence Fabric, built from over a decade of xOT-specific telemetry, adversary research, and incident response. Dragos EmberAI puts that intelligence directly in analysts' hands so each can operate like a professional regardless of their experience. xOT Threat Intelligence delivers finished threat intelligence built exclusively for xOT, produced by the largest private ICS/OT threat intelligence team in the industry. Dragos Expert Services provide direct access to frontline expertise, from security assessments to 24/7 incident response.

No other organization brings xOT-specific technology, intelligence, and services together under one roof.

Dragos protects organizations across electric, oil and gas, manufacturing, water, transportation, mining, and government sectors, operating globally from its headquarters in Hanover, Maryland.



© 2026 Dragos, Inc. All Rights Reserved.