

CASE STUDY

Securing The xIoT Landscape In The Food, Dairy, and FMCG Industry

How a leading food and dairy producer achieved comprehensive xIoT security with Phosphorus, A Dragos Company.

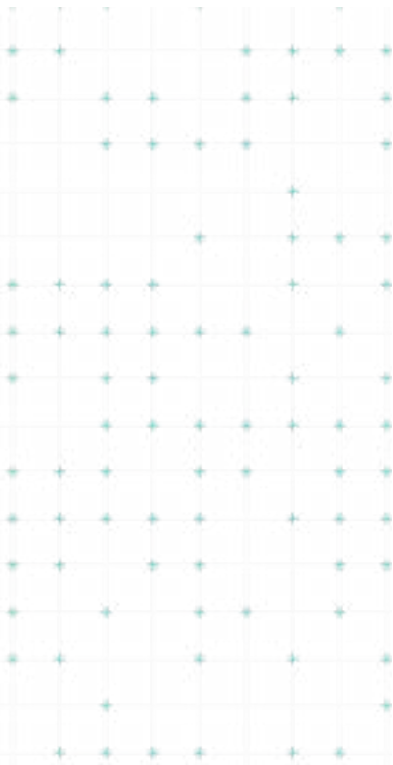


Table of Contents

Executive Summary	3
Introduction	3
The Imperative for Robust xIoT Security	4
Comprehensive xIoT Solution	4
Use Cases in the Food, Dairy, and FMCG Industry	6
Key Benefits	7
Implementation Results	7
Industry Trends and Future Outlook	8
Conclusion	8



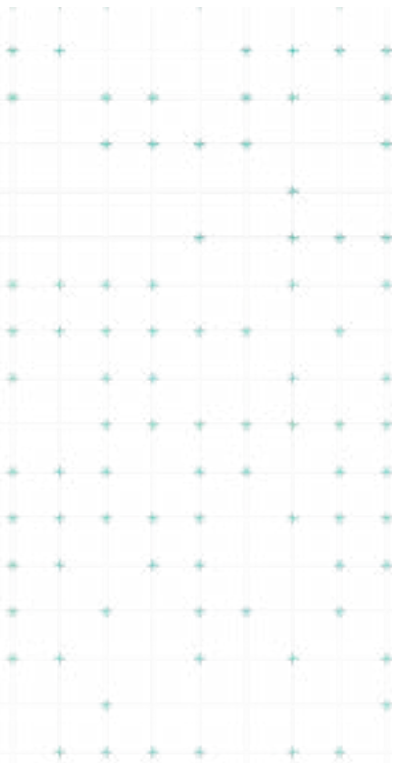
INTRODUCTION

Executive Summary

The Food, Dairy, and Fast-Moving Consumer Goods (FMCG) industry is undergoing rapid digital transformation driven by the adoption of extended Internet of Things (xIoT) devices – including IoT, OT, and IIoT Cyber-Physical Systems. These devices enhance operational efficiency, improve product quality, and streamline supply chain management. However, they also introduce significant cybersecurity vulnerabilities that can jeopardize operational continuity, compromise sensitive data, and lead to regulatory non-compliance.

Phosphorus, now part of the Dragos portfolio, offers a comprehensive solution to secure xIoT devices, providing asset visibility, vulnerability management, automated remediation, and consolidated oversight to protect critical assets and ensure business resilience.

Introduction



The Digital Transformation of the Food, Dairy, and FMCG Industry

The global Food, Dairy, and FMCG industry is embracing digital technologies to meet increasing consumer demands, improve operational efficiency, and comply with stringent regulatory standards. xIoT devices, such as biometric access controls, security cameras, barcode scanners, environmental sensors, label printers, and Uninterruptible Power Supplies (UPS), are integral to modern plant operations. They facilitate real-time monitoring, enhance security, optimize supply chains, and ensure product quality and safety.

The Rise of xIoT Devices and Associated Cybersecurity Challenges

While xIoT devices offer numerous benefits, security has never been a priority – for the manufacturers or the end user – so these critical devices have long gone unmanaged and unmonitored. These connected devices often operate on outdated firmware, lack robust security features, and are not designed with cybersecurity as a priority, making them vulnerable to cyberattacks that can result in production halts, financial losses, data breaches, ransomware, and reputational damage. The complex and diverse nature of these devices, often from multiple vendors, further complicates security management.



WHY IT MATTERS

The Imperative for Robust xIoT Security

Comprehensive xIoT Solution

As cyber threats become more sophisticated, the need for comprehensive security solutions that can protect xIoT devices is critical. Organizations must ensure that all devices connected to their networks are secure, compliant with regulations, and managed efficiently. Failure to do so can have severe consequences, including operational disruptions, legal penalties, and loss of consumer trust.

01

Comprehensive xIoT Asset Discovery and Inventory Management

Effective cybersecurity begins with complete, high-resolution visibility into all Cyber-Physical System assets connected to the network. Without knowing what xIoT devices are present, organizations cannot adequately protect them. The Phosphorus xIoT Security and Management Platform automatically discovers and inventories all CPS devices within the network, including those often overlooked or unknown, providing a real-time asset register with detailed information on manufacturer, model, firmware version, and network location.

- **Monitor Device Statuses:** Keep track of device health and operational status
- **Optimize Costs:** Monitor usage and End-of-Life status to inform procurement planning
- **Detect Unauthorized Devices:** Identify rogue or unauthorized devices that may pose security risks
- **Ensure Compliance:** Verify that all devices meet organizational security policies and regulatory requirements

02

Vulnerability Management and Remediation

xIoT devices are often susceptible to vulnerabilities, such as outdated firmware lacking security patches, default or weak static passwords, and insecure configurations with risky protocols enabled by default, such as Bluetooth and TELNET. Phosphorus conducts continuous vulnerability assessments of all xIoT devices, identifying security gaps and prioritizing them based on risk levels.

- **Detailed Vulnerability Reports:** Comprehensive reports highlighting vulnerabilities and their impact
- **Risk Prioritization:** Helps organizations focus on the most critical vulnerabilities first
- **Automated Remediation:** Provides actionable steps to mitigate identified risks quickly and efficiently

Comprehensive xIoT Solution

03

Automated Firmware Updates and Patch Management

Manually updating firmware on numerous devices from different vendors is time-consuming and prone to errors. Delayed updates leave devices exposed to known vulnerabilities.

- **Automated Patch Deployment:** Schedules and deploys patches without manual intervention
- **Vendor Coordination:** Manages updates across devices from multiple vendors seamlessly
- **Rollback Capabilities:** In case of issues, reverts devices to previous firmware versions

04

Secure Credential and Password Management

Default, weak, or static passwords are a common entry point for attackers. The platform enforces strong password policies and automates credential management across all devices.

- **Identifying Weak Credentials:** Detects devices using default or weak passwords
- **Automating Password Rotations:** Regularly updates passwords to reduce the risk of compromise
- **Centralizing Credential Management:** Manages credentials for all devices from a single interface using the Phosphorus Native Vault or an integrated PAM solution

05

Consolidated Device Management

Managing devices from multiple vendors often requires navigating different dashboards and management systems. Phosphorus consolidates all xIoT devices into a single, user-friendly dashboard.

- **Streamlined Oversight:** Simplifies monitoring and management tasks through a central location
- **Comprehensive Reporting:** Generates reports that provide insights into the overall security posture

REAL-WORLD EXAMPLES

Use Cases in the Food, Dairy, and FMCG Industry

The Food, Dairy, and FMCG industry faces distinct security challenges across its operations. From tracking assets across a plant floor to securing biometric access and safeguarding supply chain logistics, xIoT devices are central to every critical function. Phosphorus delivered targeted solutions that addressed these unique operational requirements while maintaining the uptime and reliability the business demands.



Inventory Control and Asset Visibility

A large dairy processing plant struggled with tracking hundreds of xIoT devices scattered across its facilities. Phosphorus provided complete asset discovery of all connected devices, including previously undocumented ones, real-time monitoring, and improved compliance.



Biometric Access Control Security

Biometric devices, such as fingerprint readers from vendors like ZKTeco, often have outdated firmware, weak authentication mechanisms, and exposure to network threats. Phosphorus automates firmware updates, strengthens authentication protocols, and applies device hardening.



UPS Device Monitoring

UPS devices are critical for maintaining operations during power outages, preventing data loss, and ensuring equipment safety. Phosphorus offers detailed device reports on the health and performance of UPS units.



Security Camera Management

Plants using cameras from different vendors face fragmented management and inconsistent security policies. Phosphorus provides centralized management, uniform security enforcement, and simplified password management.



Barcode Scanners and Label Printers

Compromised scanners and printers can cause inventory discrepancies, mislabeling, and data breaches. Phosphorus ensures device integrity and keeps firmware up-to-date to protect against these risks.



MEASURABLE IMPACT

Key Benefits

Organizations implementing Phosphorus achieve immediate improvements in security posture, operational efficiency, and regulatory compliance — translating directly into reduced risk, lower costs, and confidence that every xIoT device is secure, managed, and compliant.

-  **Enhanced Security Posture**
Significantly reduce the risk of cyberattacks on xIoT devices through comprehensive security measures.
-  **Reduced Operational Risks**
Protects critical devices like UPS units and biometric readers, ensuring operational continuity.
-  **Regulatory Compliance**
Meets regulatory requirements by ensuring devices are secure and data is protected.
-  **Improved Operational Efficiency**
Unified management and automation reduce administrative burdens and free up resources.
-  **Cost Savings**
Preventing cyber incidents while reducing downtime translates into significant savings over time.

Implementation Results

A leading FMCG plant in Saudi Arabia faced challenges managing and securing its diverse xIoT device landscape: over 1,000 xIoT devices from various vendors, multiple security camera systems, biometric access controls vulnerable to attacks, and critical UPS devices without proper monitoring — resulting in lack of asset visibility, security vulnerabilities, operational inefficiencies, and regulatory pressures. Phosphorus deployed its comprehensive platform, delivering complete asset inventory, vulnerability assessment and remediation, automated firmware updates, a unified management dashboard, and secure credential management.

After deployment:



THE PATH FORWARD

Industry Trends
and Future Outlook

The Food, Dairy, and FMCG industry stands at an inflection point where digital transformation and cybersecurity are equally critical to success. Organizations that invest in comprehensive xIoT security today will emerge as industry leaders, protecting both their operations and their customers. Phosphorus is committed to partnering with Food, Dairy, and FMCG enterprises to deliver the visibility, automation, and protection needed to thrive in this connected landscape.

Growing
Importance of
xIoT Security

As the Food, Dairy, and FMCG industry adopts more xIoT devices, the attack surface for potential cyber threats expands. Organizations must prioritize security to protect operations and customers.

Regulatory
Landscape
Evolution

Governments and regulatory bodies are introducing stricter cybersecurity regulations for critical infrastructure sectors, including Food, Dairy, and FMCG. Compliance will become increasingly important.

Phosphorus
Leadership in
xIoT Security

Phosphorus, A Dragos Company is poised to lead in providing proactive and prevention-based security solutions for xIoT devices, continually innovating to meet emerging threats and regulatory demands.

Conclusion

The integration of xIoT devices in the Food, Dairy, and FMCG industry brings significant operational advantages but also introduces substantial cybersecurity risks. Phosphorus Cybersecurity offers a comprehensive, automated, and unified solution to proactively secure and remediate these devices, ensuring operational continuity, regulatory compliance, and protection of critical assets.

By partnering with Phosphorus, organizations can confidently navigate digital transformation while safeguarding their operations and reputation in an increasingly connected world.



About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Washington DC, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com

