DRAGOS

CASE STUDY

Securing xIoT Across a Global Manufacturing Enterprise

How a 130-year-old global manufacturer secured 100+ sites in 25 countries after legacy passive tools stalled.

Phosphorus
A DRAGOS COMPANY

Manufacturing Case Study

INTRODUCTION

A Digital and Physical Transformation — And A Vast New Attack Surface

The industrial world is undergoing both a digital and physical transformation with the rapid proliferation of network-connected embedded devices — or **x**Tended Internet of Things (**x**IoT) that include IoT, OT, and IIoT Cyber-Physical Systems (CPS) — opening new avenues for efficiency and innovation. The convergence of IT and IoT/OT has also created a vast, vulnerable attack surface for cybercriminals.

From the heart of production lines to the edge of the network, Cyber-Physical Systems — including PLCs, HMIs, Robotics, Industrial Gateways, HVAC controllers, ruggedized printers, IP cameras, and more — form the lifeblood of today's manufacturing organizations. However, the security vulnerabilities inherent in these devices pose significant risks to operational continuity, data integrity, safety, and overall business resilience.

This case study presents a detailed real-world account of a major global manufacturer who embarked on a comprehensive journey to secure its extensive **x**IoT environment. With over 115 plants spanning 25 countries, this enterprise faced daunting challenges in gaining visibility and control over its vast network of connected devices. Through a meticulous analysis of their initial struggles with legacy solutions and their eventual success with Phosphorus, now part of the Dragos portfolio, this paper provides valuable insights for other organizations grappling with similar **x**IoT security challenges.

115+
Manufacturing Plants Worldwide

25
Countries Across Six Continents

130+
Years of Operating History

THE MANUFACTURER'S PROFILE

A 130-Year-Old Global Leader In Building Systems

This major manufacturer is a venerable institution with a rich history spanning over 130 years. As a global leader in the development and deployment of building systems, software, and services, the company's footprint is vast, with operations across six continents and a diverse range of products that are integral to modern living. Their portfolio includes everything from building and energy management systems and HVAC systems to security solutions and facilities management — all of which are increasingly reliant on connected devices.

Key Characteristics of The Manufacturer

Global Reach	Operations in 25 countries with over 115 manufacturing plants.
Diverse xIoT Environment	Management of a wide array of devices, including Allen-Bradley PLCs, IP cameras, Building Management Systems (BMS), and more.
Focus on Sustainability	Emphasis on data-driven processes and continuous uptime to ensure efficiency and security in its operations.

15K-20K

IP cameras across the estate — a significant portion operating with default passwords, representing just one slice of a sprawling, mission-critical **x**IoT footprint.

THE CHALLENGE

The Challenge of Securing xIoT

The manufacturer's expansive operations presented several security challenges.

01 Limited Visibility Across Sites

With a vast, geographically dispersed network operated by different teams in various locations, the company struggled to maintain consistent visibility into **x**IoT devices across 100+ manufacturing sites — creating blind spots that increased the risk of cyber-attacks and operational disruptions.

02 Misconfigurations and Default Credentials

Many mission-critical devices were deployed with insecure default settings — open ports and weak, static, or default credentials. A significant portion of the company's 15,000–20,000 IP cameras were operating with default passwords, posing a critical security risk.

03 Banned and End-of-Life Devices

Across environments with hundreds of thousands of devices, Phosphorus sees about 26% as end-of-life (EoL) — no longer supported by manufacturer updates. The manufacturer needed a way to identify and remove EoL and government-banned devices at scale.

04 Operational Continuity Requirements

The nature of the business necessitated that certain devices remain operational at all times, making traditional security solutions — which often require downtime — impractical.

05 Integration Challenges

The existing security infrastructure, including a partial deployment of a traditional passive discovery solution, was not fully integrated — resulting in siloed data and inefficient workflows.

SIDE BY SIDE

The Current State vs. Phosphorus

	Current State	Phosphorus Platform
xIoT Discovery	**Slow, Incomplete Asset Discovery** Passive monitoring and deep packet inspection takes weeks, with incomplete and inaccurate results.	**Fast, Safe, Comprehensive Discovery** Patented Intelligent Active Discovery safely and accurately discovers and assesses all **x**IoT in as little as 15 minutes.
Deployment	**Complex and Costly; Delayed Time-to-Value** Heavy hardware-based deployment is slow, expensive, and does not scale globally. No device hardening or remediation.	**No Hardware, Agents, or Hassles** Software-based, agentless platform deploys in minutes and delivers full discovery, hardening & remediation at scale.
Patching & Remediation	**No Patching or Remediation** Manually patching vulnerable **x**IoT devices can take hundreds of labor hours and dedicated effort.	**Automatically Find, Fix & Manage** With automated CPS Protection, safely & efficiently patch and remediate even the most sensitive, mission-critical **x**IoT devices — with full control.
Password Management	**No Credential Management** Changing, managing, and hardening device configurations & passwords is simply not possible with passive monitoring tools.	**Automated, Native Credential Management** Harden device configurations, change default passwords, and rotate credentials at scale — in as little as 30 minutes.
Real-Time Monitoring	**Passive, Low-Fidelity, Post-Event Alerts** Passive monitoring and deep packet inspection provide only low-fidelity, post-incident alerts requiring manual investigation and triage.	**Complete Visibility & Stateful Monitoring** Native **x**IoT communication identifies and validates device state to detect environmental & configuration drift, and alerts you on any changes.

A TALE OF TWO DEPLOYMENTS

The Current State: Legacy Passive Discovery

A traditional passive discovery solution was rolled out to only **three of the 117 plants**, highlighting the challenges of scaling the solution across the manufacturer's global operations.

$300K
COST PER SITE

9 Months
TIME TO DEPLOY 1 SITE

3 of 117
SITES COVERED

Key Takeaways

01 **Limited Deployment**
A traditional passive discovery solution was rolled out to only three of the 117 plants.

02 **Heavy Infrastructure**
Deploying the legacy tool at one small site required tens of thousands in hardware, software, and licenses — plus expensive packet brokers and TAPs.

03 **Slow**
Deploying at just one small site proved lengthy — taking more than nine months and requiring an exorbitant amount of human resources.

04 **Incomplete Visibility**
The partial deployment meant many of the company's IoT and OT devices remained unknown, unfound, and unseen.

05 **No Remediation**
While the passive tool provided some visibility, it lacked the ability to harden and remediate vulnerabilities.

06 **High Costs**
A single proof-of-concept deployment at just one small site amounted to more than $300,000 in total costs.

A TALE OF TWO DEPLOYMENTS

...vs. Phosphorus

Phosphorus was able to safely and actively discover and assess the customer's **x**IoT estates across **more than 100 global sites in just 5 hours**.

$100Ks
PER-SITE SAVINGS

5 Hours
TIME ACROSS 100+ SITES

100+
SITES COVERED

Key Takeaways

01 **Rapid Deployment**
The customer deployed Phosphorus' software-based, agentless platform on-prem or in the cloud in minutes — without appliances or infrastructure.

02 **No Infrastructure**
No appliances, packet brokers, or TAPs required — eliminating heavy capital investment.

03 **Fast**
The platform deployed in minutes and scaled across more than 100 sites in hours — all with fewer resources.

04 **Comprehensive Visibility**
Discovered and assessed xIoT across 100 sites, including make/model, firmware, configurations, and vulnerabilities.

05 **Full Remediation**
Unlike the legacy tool, Phosphorus fundamentally reduced business risk by automatically remediating device vulnerabilities with full control.

06 **Rapid Time-To-Value**
Saved the customer time, money, and resources — delivering immediate time-to-value and saving hundreds of thousands of dollars per site.

THE PHOSPHORUS SOLUTION

A Paradigm Shift In xIoT Security

Recognizing the limitations and cost of their existing approach, the manufacturer sought out Phosphorus and our **x**IoT Security and Management Platform. The Phosphorus unified, agentless platform is designed specifically to address the unique challenges of securing sensitive, mission-critical **x**IoT environments on a global scale.

01 - RAPID DEPLOYMENT ACROSS ALL SITES

Swift roll-out: Phosphorus was able to safely and actively poll and assess more than 100 global sites in half a day — a stark contrast to the multi-month roll-out time experienced with their legacy passive discovery solution at a single small site. This rapid deployment was achieved without the need for hardware, agents, TAPs, or packet brokers.

Scalability: The platform's ability to scale across the manufacturer's entire global footprint was a critical factor in its selection. Phosphorus' on-premise and SaaS-based solution was not only faster to deploy but also more cost-effective, eliminating the need for expensive hardware and complex configurations.

02 - COMPREHENSIVE VISIBILITY & GRANULAR CONTROL

Complete device inventory: Phosphorus provided a complete inventory of all **x**IoT devices across its 100 sites, offering detailed visibility into device make/model/series, firmware versions, default configurations, and other critical attributes.

Intelligent Active Discovery: The platform's patented Intelligent Active Discovery technology allowed it to safely and efficiently find and assess embedded IoT, OT, and IIoT devices on the network with precision — ensuring no device was left unseen.

> **"I'm already getting requests from senior leadership to determine how we can pull the Phosphorus data into a CIO dashboard.**
>
> *- CUSTOMER*

THE PHOSPHORUS SOLUTION

Full Remediation and Seamless Integration

Recognizing the limitations and cost of their existing approach, the manufacturer sought out Phosphorus and our **x**IoT Security and Management Platform. The Phosphorus unified, agentless platform is designed specifically to address the unique challenges of securing sensitive, mission-critical **x**IoT environments on a global scale.

03 - FULL REMEDIATION CAPABILITIES

Automated remediation: Unlike passive discovery-only solutions, Phosphorus enabled the manufacturer to fundamentally reduce business risk by automatically remediating vulnerabilities with full control — rotating credentials, updating vulnerable firmware, hardening devices with default configurations, identifying and isolating banned devices, and updating expired certificates.

One unified, collaborative console: The platform provided a unified interface for managing and monitoring all **x**IoT devices, significantly reducing the operational burden on the manufacturer's security, IT, and operations teams.

04 - SEAMLESS INTEGRATION WITH EXISTING IT

ServiceNow integration: Phosphorus seamlessly integrated with the manufacturer's existing IT stack, including ServiceNow, enabling enriched **x**IoT device information to be shared across teams for efficient, automated vulnerability response.

Improved operational efficiency: The integration capabilities allowed the manufacturer to streamline its security operations, freeing up resources to focus on other high-priority projects.

> **I believe we have a better chance of succeeding & reducing our risk exposure from IoT and OT devices by using the remediation capabilities of Phosphorus.**
>
> *- CUSTOMER*

DETAILED BUSINESS BENEFITS

Cost Reduction, Risk Mitigation & Operational Efficiency

Deploying Phosphorus' **x**IoT Security and Management platform significantly transformed the manufacturer's approach to **x**IoT security. The benefits extended far beyond improved visibility and remediation, leading to substantial cost savings and enhanced risk mitigation.

$30M+

AVOIDED ACROSS 100+ SITES

Traditional solutions incurred a per-site deployment cost of $300,000 — which, extrapolated across all 100+ sites, would have exceeded $30 million. The manual remediation approach, involving extensive travel and resource expenses, would have taken years and added millions in outsourcing costs. Phosphorus' rapid deployment and automated remediation effectively eliminate these exorbitant costs.

01 Cost Savings

Elimination of hardware costs - The agentless solution required no appliances or packet brokers, resulting in a considerable reduction in capital expenditure.

Reduced operational costs - Rapid deployment and automated remediation minimized manual labor, letting the manufacturer reallocate resources to strategic initiatives.

02 Risk Reduction

Comprehensive risk assessment - A complete, accurate assessment of risk posture across all **x**IoT devices, with real-time monitoring for drift and immediate alerts on insecure states.

Extensive risk reduction - Automating remediation significantly reduced exposure to cyber threats and enforced secure configurations for compliance with internal policies and industry regulations.

03 Operational Efficiency

Streamlined security operations - Integration with ServiceNow and other tools enabled more efficient workflows and faster time-to-resolution for incidents.

Improved asset management - Detailed visibility allowed more effective asset management, reducing the risk of unaccounted-for devices serving as entry points.

COMPARATIVE ANALYSIS

Phosphorus vs. Legacy Solutions

The manufacturer's experience with both a traditional passive discovery solution and Phosphorus provides a compelling comparison of the two approaches to **x**IoT security. While a traditional passive solution offered some initial visibility, it was ultimately limited in scope, costly and complex to deploy, and lacked the remediation capabilities to fundamentally reduce risk.

In contrast, Phosphorus delivered a comprehensive, scalable solution addressing the full spectrum of **x**IoT security challenges — FINDING, FIXING, MONITORING, and MANAGING their vulnerable IoT, OT, and IIoT estates. This higher efficacy translated to greater enterprise-wide visibility, fewer unaddressed vulnerabilities, and substantial risk reduction.

DEPLOYMENT & COST

LEGACY SOLUTION	PHOSPHORUS PLATFORM
Limited to three sites with a protracted roll-out process and high costs for hardware, software, and additional equipment.	Deployed across 100 sites in half a day without the need for hardware or additional costs, providing immediate value.

VISIBILITY & CONTROL

LEGACY SOLUTION	PHOSPHORUS PLATFORM
Partial visibility with no remediation capabilities, leaving many vulnerabilities unaddressed.	Full visibility across all sites with the ability to remediate vulnerabilities automatically, ensuring a secure **x**IoT environment.

INTEGRATION & EFFICIENCY

LEGACY SOLUTION	PHOSPHORUS PLATFORM
Limited integration with existing IT infrastructure, resulting in siloed data and inefficiencies.	Seamless integration with existing tools, streamlining security operations and improving overall efficiency.

BROADER IMPLICATIONS & FUTURE OUTLOOK

A Blueprint For Securing Global xIoT

For the first time, this manufacturer gained visibility and risk assessment across global facilities on a scale that was previously unattainable — fundamentally reducing risk by addressing the poor security hygiene of over a third of their organizational attack surface. As more manufacturers embrace digital transformation, the need for robust, scalable **x**IoT security only grows. This case study serves as a blueprint for other organizations looking to secure their IoT, OT, and IIoT estates.

Increased Adoption of Agentless Security

The success of Phosphorus' agentless, software-based approach is likely to drive increased industry adoption as manufacturers seek to reduce risk and minimize costs while preventing operational disruptions.

Greater focus on Integration & Automation

Seamless integration and automation capabilities highlight their growing importance in modern security solutions, as organizations streamline operations and reduce the burden on security teams.

Rising Cyber Threats

The increasing frequency and sophistication of attacks targeting xIoT devices underscore the importance of comprehensive, proactive security with full visibility and remediation.

Operational Resilience

As manufacturers grow more reliant on connected Cyber-Physical Systems, securing these systems is critical to maintaining operational resilience and business continuity.

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