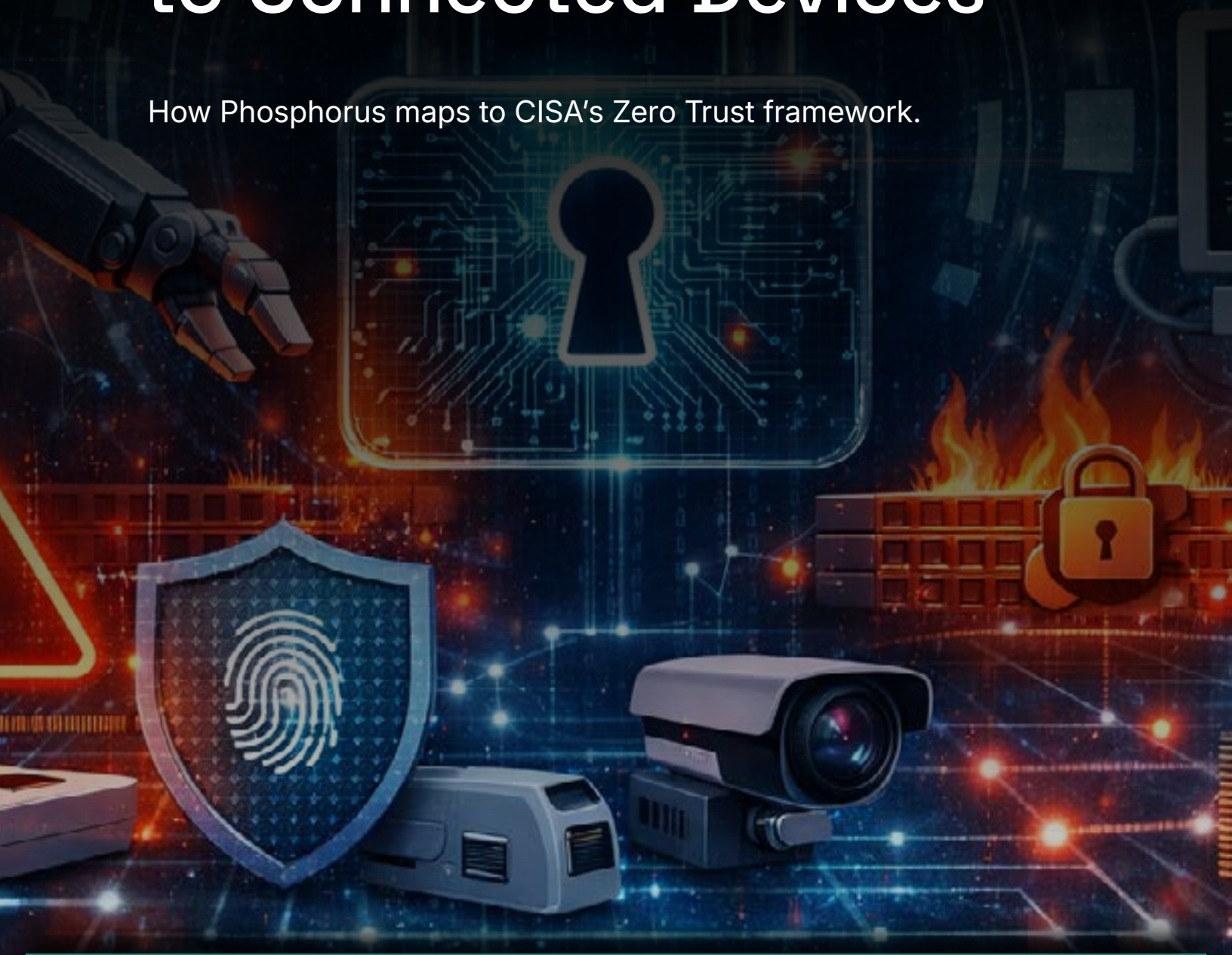
DRAGOS

SOLUTION BRIEF

Extending Zero Trust to Connected Devices

How Phosphorus maps to CISA's Zero Trust framework.



Phosphorus
A DRAGOS COMPANY

ZERO TRUST MAPPING SOLUTION BRIEF

INTRODUCTION

A National Cybersecurity Imperative

Zero Trust is no longer a concept reserved for forward-thinking IT shops — it is now a national cybersecurity imperative, backed by Executive Order 14028, OMB M-22-09, and formalized through CISA's Zero Trust Maturity Model (ZTMM v2). While many organizations have made progress securing user identities, applications, and core infrastructure, one critical area remains largely unaddressed: **x**IoT, or extended Internet of Things.

This brief outlines how Phosphorus, now part of the Dragos portfolio, enables organizations to extend Zero Trust principles across all connected devices by mapping directly to each pillar of CISA's Zero Trust model.

THE CHALLENGE

xIoT as the Unmonitored Attack Surface

xIoT encompasses the vast ecosystem of unmanaged, cyber-physical devices, including IoT, OT, IIoT, and IoMT assets. Traditional vulnerability scanners are often blind to the **x**IoT attack surface, exposing organizations to unmanaged risk and long-term persistence by sophisticated threat actors. While these devices are often mission-critical, they are rarely inventoried, secured, or monitored. **Common examples include:**

01

Unmonitored Building Systems

— HVAC, UPS, and elevator controllers often run on default credentials, with no visibility into firmware or device state.

02

Legacy and End-of-Life Assets

— OT devices remain in production long after vendor support ends, often with known, unpatched vulnerabilities.

03

Banned Devices

— white-labeled or disguised behind Western branding, hiding firmware that may contain backdoors.

04

Unknown Devices

— connect to the network, presenting inventory gaps and unknown risk.

05

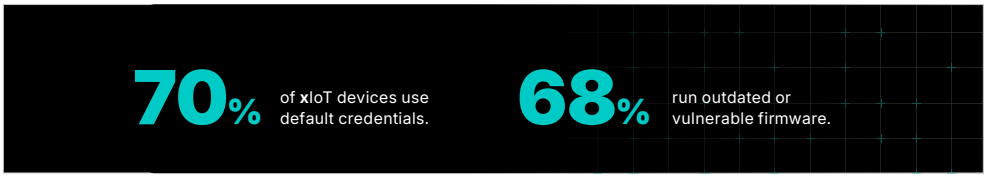
Networked Devices

— printers, remote terminals, badge readers, and IP cameras relying on expired or self-signed certificates.

06

Outdated Firmware

— insecure configurations and weak or default access controls serve as low-effort entry points for threat actors.



Source: Phosphorus research

These conditions create a perfect storm of exploitable weaknesses. Without centralized visibility, authentication, and control, these devices present an ideal attack surface for adversaries — from ransomware like Akira to nation-state APTs targeting commercial and critical infrastructure.

THE PLATFORM

Mapping Phosphorus to CISA's Zero Trust Pillars

How Phosphorus capabilities align with the five core pillars of the CISA Zero Trust Maturity Model.

01

Identity Pillar

All users and devices are identified and authenticated.

Phosphorus provides high-fidelity, in-depth device discovery and classification that enables organizations to accurately identify assets and continuously assess risk. By interacting directly with device firmware instead of relying on low-fidelity MAC address or OUI lookups, Phosphorus uncovers granular device intelligence and security risks that traditional network analysis tools cannot detect.

- Identify detailed device attributes, including manufacturer, model, firmware, IP/MAC address, protocols, services, and device-specific metadata.
- Detect security risks such as default passwords, outdated firmware, known CVEs, insecure configurations, and expired or self-signed certificates.
- Verify true device origin, including white-labeled and prohibited devices, through direct firmware interaction rather than network traffic alone.
- Support role-based access control and automated management, including password rotation, firmware updates, and configuration changes.
- Enable continuous device trust evaluation and ongoing risk assessment with rich, actionable device intelligence.

02

Device Pillar

Devices are authorized, managed, and secured.

Phosphorus enables management of what has traditionally been unmanaged, with direct remediation and hardening of **x**IoT assets:

- Automated credential rotation to eliminate default credentials
- Vulnerability detection, CVE criticality assessment, and integrated firmware patching, upgrades, and downgrades
- Configuration management — disabling unnecessary or insecure protocols (SSH/Telnet/FTP)
- Tagging and isolating non-compliant or unauthorized devices

03

Network Pillar

Traffic is segmented, monitored, and dynamically enforced.

Phosphorus provides granular device-level detail about assets, giving teams the context to prioritize remediation effectively:

- Complete **x**IoT discovery, with device-level risk detail essential for effective remediation
- Least-privilege communication enforcement by disabling unnecessary remote services (FTP, Telnet, SSH)
- Direct device isolation, including flagging and remediating devices from untrusted or sanctioned vendors
- Identification of insecure digital certificates, enforcing strong, valid certificates for authenticated communications

04

Application Workload Pillar

Applications are secure, and access is governed.

Not applicable.

05

Data Pillar

Data is protected at rest and in transit.

Phosphorus extends Zero Trust data protection into **x**IoT environments by delivering device-centric intelligence, state control, and policy enforcement:

- Identifies and secures **x**IoT devices that interact with sensitive data (cameras, medical systems, ICS)
- Restricts data exposure by disabling sensitive services (FTP, Telnet) and enforcing least-privilege configurations
- Enforces strong encryption in transit, replacing insecure, expired, or self-signed certificates
- Tracks devices for state changes — configuration, firmware, and password drift — to support compliance monitoring
- Isolates or restricts non-compliant, high-risk devices to prevent lateral movement toward sensitive data

COMPLIANCE & STRATEGIC ALIGNMENT

Aligned With The Frameworks Shaping Zero Trust

Phosphorus enables alignment with the key Zero Trust and cybersecurity initiatives shaping federal and industry requirements today:

CISA Zero Trust Maturity Model (ZTMM)

The federal framework this brief maps Phosphorus against, pillar by pillar.

OMB M-22-09

Federal Zero Trust strategy and associated maturity milestones.

Binding Operational Directive (BOD) 23-01

Asset visibility requirements for federal civilian agencies.

NDAA Section 889

Prohibits procurement or use of banned Chinese-manufactured devices.

FISMA, HIPAA Security Rules, FDA HICP, HITRUST, NIST 800-53, and NIST CSF

Sector and control frameworks Phosphorus supports through device-level evidence and enforcement.

CONCLUSION

Closing the Gap in Zero Trust Architectures

Zero Trust is a powerful model, but only when applied consistently across the complete **x**IoT attack surface. For most organizations, connected devices remain the largest unmanaged, unmonitored, and unprotected part of their infrastructure. Phosphorus enables Zero Trust for **x**IoT — bringing visibility, risk management, and continuous monitoring to every connected thing, safely, with precision, and without requiring agents or network disruption.

Learn more at Phosphorus.io

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