

SOLUTION BRIEF

Phosphorus xIoT Compliance Dashboard

Compliance mapping, enforcement, and reporting for your xIoT environment.

INTRODUCTION

**Compliance as a
Function of Device
Control**

Phosphorus is now part of the Dragos portfolio. The Phosphorus compliance report redefines compliance as a function of device control, not interpretation. Regulatory requirements are expressed through the actual state of devices and resolved through direct action on those devices. Compliance is no longer a snapshot assembled for auditors — it is the observable result of how devices are configured, accessed, and maintained.

THE CHALLENGE

**State of the xIoT
Attack Surface**

Compliance breaks down where regulatory language meets device reality. Security teams identify device risk. Compliance teams translate findings into controls. Operations teams remediate devices using separate platforms.

The result is a disconnected workflow where compliance status lags behind actual device state and audit evidence is assembled manually.

This disconnect is amplified in xIoT environments, where:

01

Devices do not conform to IT-centric compliance tooling

02

Regulatory frameworks overlap across regions and industries

03

Remediation must occur at scale, often under audit pressure

The industry has built tools to document compliance and tools to manage devices.
It has not built a system that unifies both.

THE PLATFORM

The Phosphorus Approach

Phosphorus approaches compliance from the device outward.

Phosphorus derives this understanding from active device interrogation. The platform collects granular configuration and state data directly from devices, including authentication posture, firmware state, exposed services, and security and operational-relevant configuration. These concrete device attributes form the basis for control mapping, replacing inferred compliance with verifiable technical evidence.

Built for Regulated Device Environments

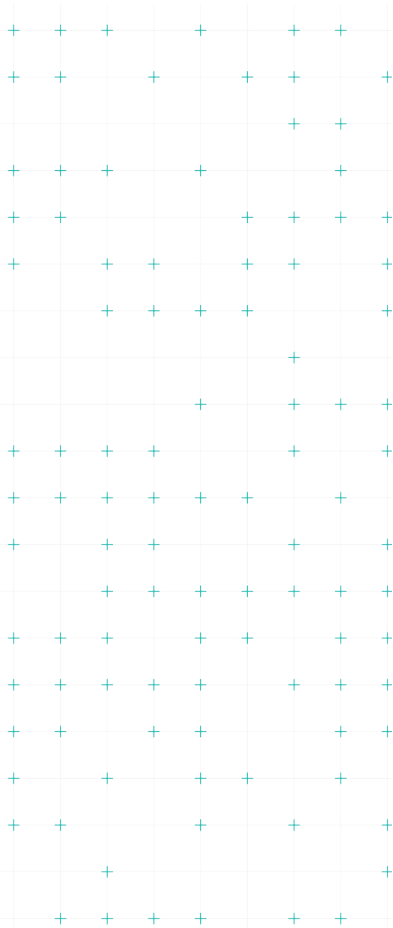
The Phosphorus compliance report supports xIoT device-centric regulatory frameworks across government, critical infrastructure, healthcare, and global operations, including:

OTCC	IEC 62443
NERC CIP	HIPAA
NDAA Section 889	NIS2
NIST 800-53 & NIST 800-82	

The compliance report is built on the premise that regulatory controls are enforced, or violated, by specific device-level conditions. Firmware versions, credential states, configurations, exposed services, and vendor attributes are the mechanisms through which compliance succeeds or fails.

By anchoring compliance directly to device state, Phosphorus eliminates the need to translate between security findings, regulatory language, and operational action. When devices change, compliance status changes. When remediation occurs, it is reflected automatically in compliance outcomes.

Compliance becomes measurable, enforceable, and defensible through active discovery and remediation.



IN ACTION

Compliance Dashboard

Standards can be applied by region to reflect real-world regulatory scope and operational boundaries.

With Phosphorus, compliance does not stop at identification. The same platform that establishes control impact is responsible for resolving it. Remediation is not a downstream process or external workflow — it is intrinsic to how compliance is achieved.

Compliance status is derived from executed actions on real devices, without reconciliation, duplication, or manual validation.

Phosphorus

Home

Devices

Logs

Reports

Jobs

Zones

Settings

admin@phosphorus.io

Reports

Security Overview

Response & Remediation

Compliance

Alert Overview

Device Overview

Excluded Devices

Firmware Overview

Custom Reports

Compliance

This report highlights areas of non-compliance based on device-level findings detected by Phosphorus. These results reflect technical conditions mapped to specific regulatory or industry controls and do not represent a certification of full compliance. Many standards also require organizational processes and governance activities beyond device telemetry. This view summarizes how many of your devices matched alert conditions for each control. Region filters adjust the report focus, though many standards are adopted internationally. Select a control to see the associated devices and underlying findings.

Region

All Regions

Standard

All Standards

Control

Filter by Control Name...

Standard	Control ID	Control Name	Failing Condition	Non-Compliant	Devices
USA HIPAA	§164.308(a)(5)	Security Awareness and Training	Malware Exposure Risk (Protection from Malicious Software)	153 Devices	View Devices
USA HIPAA	§164.308(a)(5)(ii)(B)	Protection from Malicious Software	Malware Exposure Risk (Out-of-date firmware, vulnerable s...	153 Devices	View Devices
USA HIPAA	§164.312(a)(1)	Access Control	Unique User Identification	8 Devices	View Devices
USA HIPAA	§164.312(c)(1)	Integrity	ePHI must not be improperly altered	128 Devices	View Devices
IEC 62443	SR 1.1	Human User Authentication	User Authentication Requirements	8 Devices	View Devices
IEC 62443	SR 1.2	Software Process Authentication	Service Authentication	8 Devices	View Devices
IEC 62443	SR 6.1	Audit Log Accessibility	Audit Log Availability	120 Devices	View Devices
IEC 62443	SR 6.2	Continuous Monitoring	Real-time Security Monitoring	185 Devices	View Devices
NDA Section 889	§889(a)(1)(B)	Prohibited Equipment	Banned Vendor Equipment	29 Devices	View Devices
NERC CIP	CIP-007-6	Cyber Security - Systems Security Management	Patch Management and Malware Prevention	166 Devices	View Devices

Rows per page: 10 1-10 of 27

Phosphorus

Home

Devices

Logs

Reports

Jobs

Zones

Settings

Reports

Security Overview

Response & Remediation

Compliance

Alert Overview

Device Overview

Excluded Devices

Firmware Overview

Custom Reports

Compliance

This report highlights areas of non-compliance based on device-level findings detected by Phosphorus. These results reflect technical conditions mapped to specific regulatory or industry controls and do not represent a certification of full compliance. Many standards also require organizational processes and governance activities beyond device telemetry. This view summarizes how many of your devices matched alert conditions for each control. Region filters adjust the report focus, though many standards are adopted internationally. Select a control to see the associated devices and underlying findings.

Region

All Regions

Standard

All Standards

Control

Filter by Control Name...

Standard	Control ID	Control Name
USA HIPAA	NIST 800-53	Security Awareness and Training
USA HIPAA	NIST 800-82	Protection from Malicious Software
USA HIPAA	IEC 62443	Access Control
USA HIPAA	NDA Section 889	Integrity
USA HIPAA	NERC CIP	Human User Authentication
USA HIPAA	NIS2	Software Process Authentication
USA HIPAA	HIPAA	Audit Log Accessibility
IEC 62443	OTCC	Continuous Monitoring
IEC 62443	SR 1.2	Prohibited Equipment
IEC 62443	SR 6.1	Cyber Security - Systems Security Management
IEC 62443	SR 6.2	
NDA Section 889	§889(a)(1)(B)	
NERC CIP	CIP-007-6	



OPERATIONAL COMPLIANCE

Operational
Compliance,
Not Static
Reporting

Traditional compliance tools capture intent. Phosphorus’ strategy establishes outcome. The Compliance Report is directly integrated with Phosphorus’ unified management platform, enabling teams to resolve compliance failures through controlled, auditable actions such as:

- Credential Rotation**
Rotate passwords/keys automatically.
- Firmware Management**
Update firmware safely across devices.
- Configuration Enforcement**
Continuously enforce secure baselines and remediate drift.
- Privileged Access Enrollment**
Sync xIoT credentials into your secure vault for centralized governance and compliance.

OUTCOMES

What This Enables

The Phosphorus compliance report is an operational compliance layer for xIoT environments, where regulatory requirements are enforced through direct control of devices.

Audit Readiness

Compliance evidence reflects current device state and executed remediation, not point-in-time attestations.

Risk-Driven Remediation

Operational effort is prioritized by regulatory impact rather than alert volume.

xIoT Coverage

Compliance enforcement extends beyond traditional IT to include OT and IoT environments.

Supply Chain Assurance

Vendor-based restrictions are validated against discovered devices, not assumed inventories.



Scope

The Phosphorus compliance report addresses technical, device-enforceable controls. Organizational controls, policy, training, governance, and procedural requirements all remain outside its scope and are intended to complement existing GRC programs.

Phosphorus®

Home

Devices

Logs

Reports

Jobs

Zones

Settings

Trevor Tomlinson@phosphorus.io

Devices

alert:="Out of Date Firmware" OR alert:="Vulnerable Firmware"

Displaying 1 - 10 of 202 Total Devices

Select All Devices

Response Time: 207ms

Address	Zone	Hostname	Manufacturer	Model	Type	Firmware	Alerts	KEVs
192.168.104.168	default		HP	LaserJet P2055dn	Printer	20701025	▲ 9	
192.168.98.62	default		HP	LaserJet 4250	Printer	68.012.1	▲ 8	
192.168.99.23	default		APC	KVM178P	KVM	1.0.088	▲ 8	
192.168.97.16	default		Sony	SNC-EM601	IP Camera	2.6.0	▲ 7	
192.168.98.33	default		Ricoh	IM C2300	Printer	784	▲ 7	♥ 2
192.168.99.86	default		Dell	iDRAC6	BMC	1.88	▲ 7	
192.168.97.21	default		AXIS	Q3505	IP Camera	6.50.2.2	▲ 6	♥ 1
192.168.99.85	default		Dell	iDRAC7	BMC	2.50.50.50	▲ 6	
192.168.98.116	default		Openner	IMT248-2-DAC	Network Management D...	4.0.0u1	▲ 6	

default

199

3

EC2 Instance 203

Show All

High

98

Medium

107

Low

199

Show All

Out of Date Firmware

183

Vulnerable Firmware

108

Discontinued Device

94

Insecure Certificate

68

Insecure Device

40

Show More

The Phosphorus compliance report is an operational compliance layer for xIoT environments, where regulatory requirements are enforced through direct control of devices.

Learn more at [Phosphorus.io](https://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

