DRAGOS

SOLUTION BRIEF

Phosphorus xIoT Compliance Dashboard

Compliance mapping, enforcement, and reporting for your **x**IoT environment.

Phosphorus
A DRAGOS COMPANY

xIoT COMPLIANCE DASHBOARD

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 **x**IoT 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.

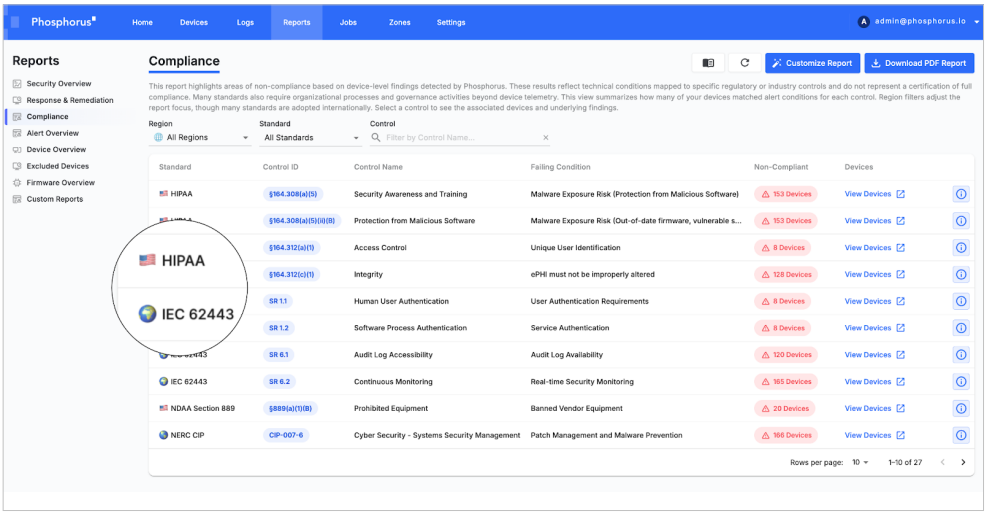
IN ACTION

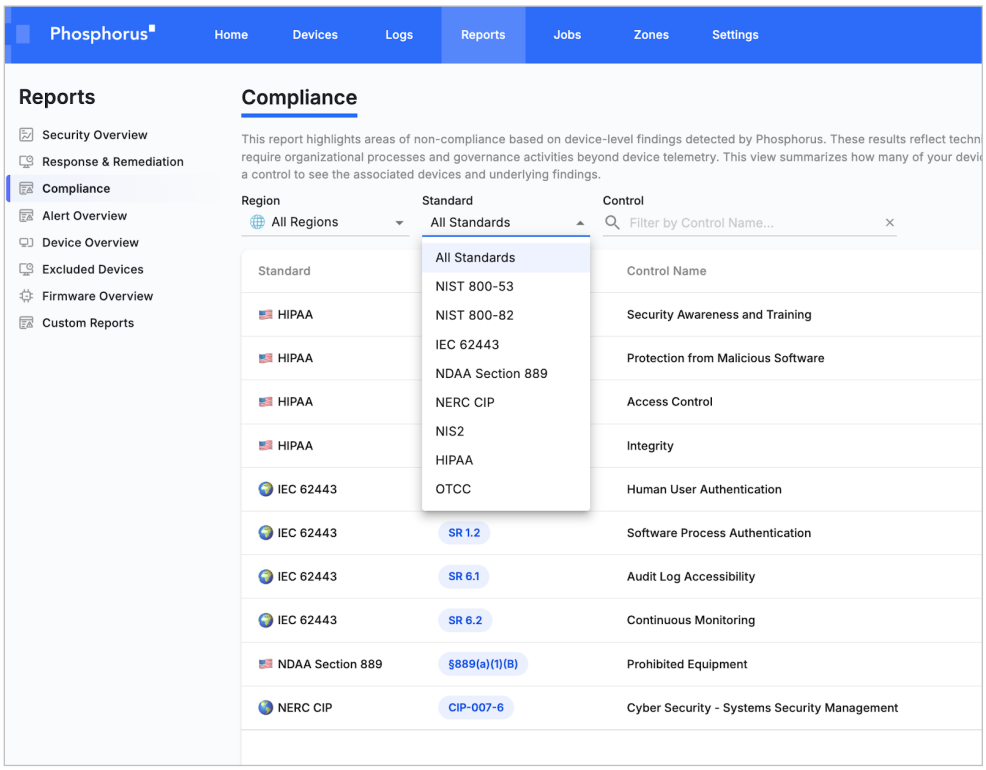
Compliance Dashboard

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.





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 **x**IoT credentials into your secure vault for centralized governance and compliance.

OUTCOMES

What This Enables

The Phosphorus compliance report is an operational compliance layer for **x**IoT 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.

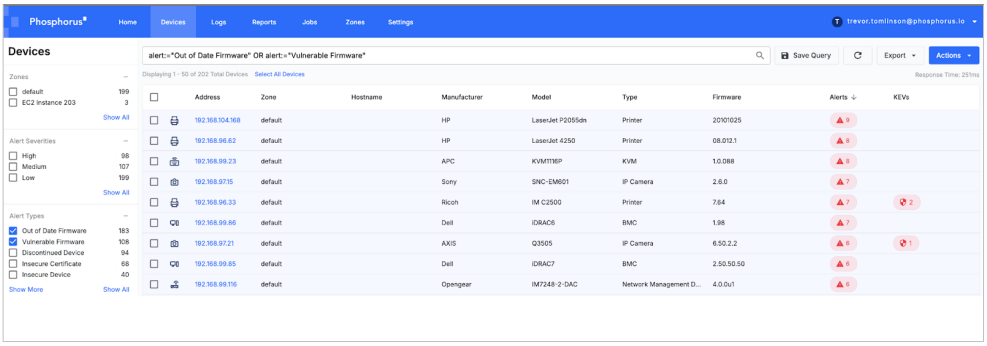
Risk-Driven Remediation
Operational effort is prioritized by regulatory impact rather than alert volume.

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.



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

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