DRAGOS

Phosphorus, A Dragos Company
DATA SHEET

Phosphorus xIoT Certificate Management

Eliminate certificate weaknesses. Enforce trusted identity across every device.

The Challenge

xIoT devices rely on digital certificates to authenticate connections, encrypt traffic, and verify device identity. Yet across most enterprise environments, certificates are aging out, misconfigured, or unmanaged entirely. **Common risks include:**

- Devices running on **expired or self-signed certificates** weaken authentication.
- Incorrectly **chained or misconfigured certificates** that break secure communication.
- Weak cryptographic ciphers or outdated TLS and 802.1x configurations expose traffic to interception.
- No centralized visibility into certificate posture across large, diverse device fleets.

Attackers exploit these weaknesses to impersonate devices, intercept data, and move laterally inside networks. Traditional certificate management tools cannot integrate with the constraints of embedded IoT and OT systems, which prevents at-scale automation.

The Phosphorus Advantage

Phosphorus, now part of the Dragos portfolio, delivers the industry's first and only **xIoT Security and Management Platform** with **native, automated certificate lifecycle management** for IoT, OT, IIoT, and IoMT devices.

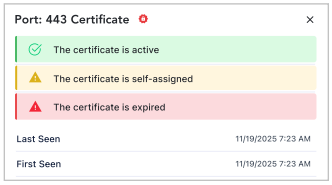
Through Intelligent Active Discovery, organizations gain detailed visibility into certificate posture and can remediate issues safely and at scale.

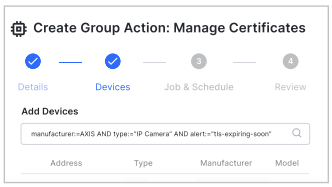
AT A GLANCE

Key Benefits

- Automatic discovery of certificates and expiration risk
- Identify invalid or misconfigured certs
- Replace and deploy certificates at scale
- Enforce consistent certificate standards
- Automate renewal workflows across thousands of devices
- Stronger authentication & encryption

Core Capabilities

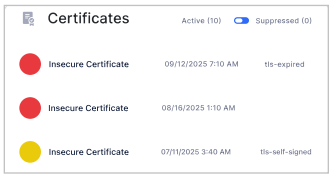




1. **Automated Certificate Discovery with Risk Context**
   Automatically identifies certificate attributes on every connected device—including expiration status, self-signed or improperly chained certs, weak ciphers or deprecated TLS settings, and services lacking valid certificates—enriched with device metadata for targeted, risk-informed remediation.
2. **Certificate Renewal and Replacement at Scale**
   Automate certificate updates for thousands of devices—installing CA-signed certificates, replacing self-signed ones, updating expiring certs before impact, and enforcing strong cryptographic and TLS and 802.1x configurations using—using safe, native device interactions.
3. **Automated Certificate Deployment Across Diverse Device Types**
   Rapidly deploy new certificates across heterogeneous device fleets—applying updates by device type, model, vendor, or policy group—to standardize certificate practices and eliminate inconsistent or manual updates.
4. **Operationalizing Certificate Management at Scale**
   Create recurring jobs to enforce renewal cycles, apply organization-wide certificate standards, run maintenance within approved windows, and integrate seamlessly with PKI, NAC, SIEM, and ITSM systems to maintain consistent certificate hygiene over time.

Customer Outcomes

With Phosphorus, enterprises and organizations across critical infrastructure achieve:

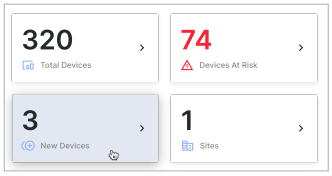


Immediate Visibility Into Certificate Posture

Instantly identify devices using expired, self-signed, or insecure certificates.

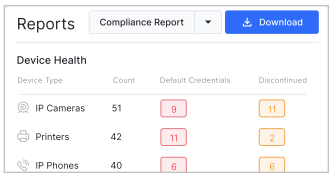
Stronger Authentication Across All Connected Devices

Ensure every device uses trusted certificates that support encrypted communication.



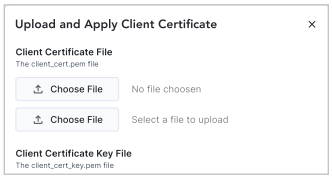
Reduced Attack Surface And Lateral Movement Risk

Prevent impersonation attacks and protect in-transit data.



Simplified Compliance With Internal And Regulatory Requirements

Strengthen certificate governance across healthcare, manufacturing, energy, finance, and more.



Lower Operational Overhead Through Automation

Eliminate manual certificate updates that cannot scale across diverse **x**IoT environments.

For CISOs and CIOs

Phosphorus delivers strategic resilience by unifying fragmented device security processes into a single autonomous platform. It empowers leadership to ensure enterprise-wide compliance, reduce attack surface risk, and extend zero-trust principles to their entire **x**IoT environments.

Why Phosphorus

We secure and manage connected devices at machine scale; safely, automatically, continuously, with human oversight, not limitations.

DISCOVER AND ASSESS

- ✓ Asset Discovery
- ✓ Vulnerability Assessment
- ✓ Prohibited Device Detection and Response

HARDEN & REMEDIATE

- ✓ Password Management
- ✓ Firmware Management
- ✓ **Certificate Management**
- ✓ Configuration Management

MONITOR & MANAGE

- ✓ Device State Monitoring
- ✓ Device Log Retrieval
- ✓ Device Backup

FAST VALUE REALIZATION

Deploys quickly with no agents, hardware, SPAN ports, or packet brokers.

LEVERAGE EXISTING INVESTMENTS

Integrates with SIEM, SOAR, PAM, and ITSM systems for complete downstream visibility.