

Phosphorus Platform

Don't just see xIoT risks. **Eliminate** them.

Closing The Gap Between Visibility and Action

Most xIoT (IoT, OT, IoMT, and IIoT) security tools stop at identifying devices and vulnerabilities, leaving remediation to overburdened security and operations teams. Phosphorus, now part of the Dragos portfolio, enables organizations to discover and assess all connected devices, harden and remediate exploitable risk, and monitor and manage xIoT environments continuously from a single platform.

AT A GLANCE

Key Statistics

Three statistics that highlight why organizations need comprehensive visibility, security, and lifecycle management.

70%

of IoT & OT devices deployed with **default credentials**.

68%

of deployed xIoT devices have **CVEs of 8 or above**.

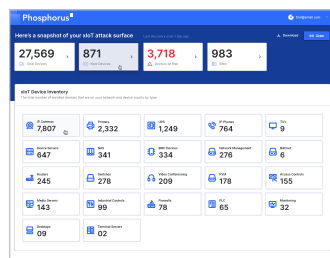
26%

of xIoT devices are **end-of-life** and no longer supported.

ONE PLATFORM. COMPLETE CONTROL.

One agentless platform — deployed on-premise or in the cloud in minutes. No hardware, SPAN ports, or TAPs.

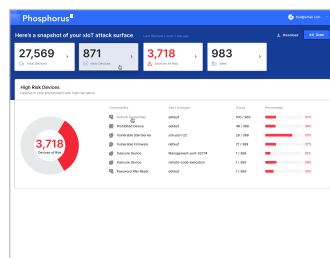
01 | DISCOVER & ASSESS



xIoT Asset Discovery

No reckless scanning.

We utilize native device protocols to interact with devices safely, enabling the discovery and profiling of devices with over 15 attributes. These include device type, manufacturer, model/series, IP address, active protocols, firmware version, open ports, active services, and device-specific information.



xIoT Vulnerability Assessment

We provide in-depth risk assessment information such as:

Default passwords in use, firmware availability, CVEs with added context from CISA's Known Exploited Vulnerabilities (KEV) catalog and FIRST's Exploit Prediction Scoring System (EPSS), end-of-support/life device, insecure configurations, expired or selfsigned certificates.

Search: alert="Prohibited Device" severity=high

Address	Manufacturer	Model	Alerts
192.168.97.36	Hewlett	DS-202630306-105	2 Alerts
192.168.97.83	Dell	VC-E894501-1	1 Alert
192.168.97.6	Amcrest	Z-406.0002.15.R.20170...	1 Alert
192.168.97.5	APC	AVN000000	1 Alert
192.168.97.5	Avigilon	3000-1000-001	1 Alert

Prohibited Device Detection and Response

Compliance-Driven risk mitigation.

Discover and remotely disable devices banned by the US Government (NDAA Section 889 - Chinese-manufactured).

02 | HARDEN & REMEDIATE

Credentials [Rotate credential](#)

Credentials	HP-0018fea74afc-admin
Provider	CA Privilege Cloud
Last Rotation	9/10/2025 10:21 AM

Password Management

Identify default or reused passwords. Schedule automated password rotations with granular controls at scale.

Firmware [Update to latest version](#)

Version	08.012.1
Release Date	07/17/2006
EPSS Score	0.93774
CVSS Score	10

Firmware Management

Automatically identify and prioritize vulnerable firmware with KEV and EPSS context—upgrade or downgrade firmware at scale.

Certificates Active (10) [Suppressed \(0\)](#)

Insecure Certificate	09/12/2025 7:10 AM	tls-expired
Insecure Certificate	08/16/2025 1:10 AM	
Insecure Certificate	07/11/2025 3:40 AM	tls-self-signed

Certificate Management

Identify devices operating with expired, self-signed, or improperly configured certificates and automatically update them at scale.

Insecure Device

First Seen	08/16/2025 1:10 AM	Medium
Last Seen	10/02/2025 5:11 AM	Medium
Sub-type	tls-self-signed	Medium
Notes	The certificate for port 443 is self-signed	Medium

Configuration Management

Disable unused services, enforce encrypted communication, and align devices to secure configuration standards to reduce the pathways attackers can exploit.

03 | MONITOR & MANAGE

Firmware Change Detected

[View all devices with Firmware Change Detected alerts >](#)

Devices	Manufacturer	Model	Actions
1	Dahua	ASD7120V-T1	View Device

Device State Monitoring

Continuously monitor xIoT estates to detect and alert on device drift and operational changes.

Download Security Logs

Download the System Logs from this Printer.

Device Log Retrieval

Centralize log collection and analytics for detailed device-level security analysis, anomaly detection, triage, and forensics.

Why Phosphorus

Legacy discovery solutions require expensive hardware and infrastructure changes that can take years to implement. Worse, their reliance on MAC address and OUI lookups provides incomplete and inaccurate data. They can point out some problems, but can't fix any of them. Phosphorus is different.

- ✓ **TIME TO BENEFIT**
Deploys quickly on-premise or in the cloud. Full discovery and assessment in minutes.
- ✓ **HIGH-FIDELITY DATA**
Deep device insights that traditional traffic-analysis tools cannot detect.
- ✓ **SCALE WITH CONFIDENCE**
Built for enterprises managing tens to hundreds of thousands of devices.
- ✓ **REDUCE RISK EXPOSURE**
Deep device insights that traditional traffic-analysis tools cannot detect.
- ✓ **PROTECT BUSINESS CONTINUITY**
Apply fixes safely and efficiently, protecting uptime and operational continuity.

Phosphorus
A DRAGOS COMPANY

SEE PHOSPHORUS IN ACTION

Request a Demo Today

[Phosphorus.io](#)

