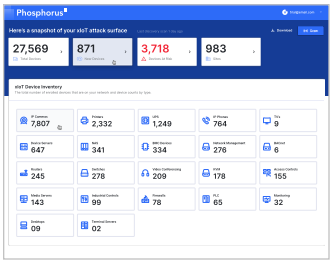
Phosphorus

Don't just see **x**OT risks. **Eliminate** them.

Closing The Gap Between Visibility and Action

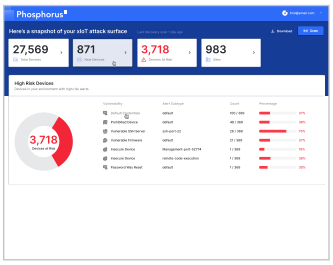
Most security tools used in xOT environments stop at identifying devices and vulnerabilities, leaving remediation to overburdened security and operations teams. Phosphorus, now part of the Dragos portfolio, enables organizations to discover and assess all connected devices, harden and remediate exploitable risk, and monitor and manage **x**OT environments continuously from a single platform.

01 | DISCOVER & ASSESS



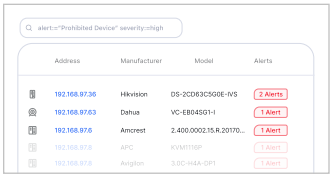
xOT Asset Discovery

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.



xOT 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.



Prohibited Device Detection and Response

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

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 xOT devices have **CVEs of 8 or above.**

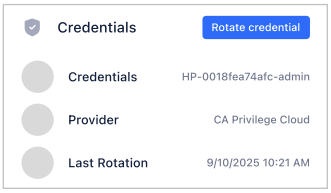
26%
of **x**OT devices are **end-of-life** and no longer supported.

ONE PLATFORM. COMPLETE CONTROL.

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

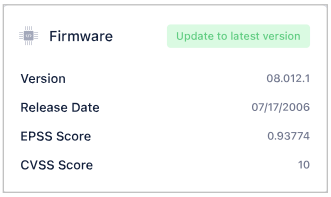
© Dragos, Inc. All Rights Reserved.

02 | HARDEN & REMEDIATE



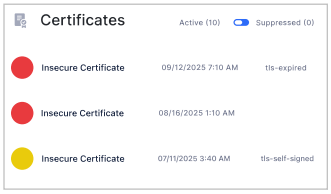
Password Management

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



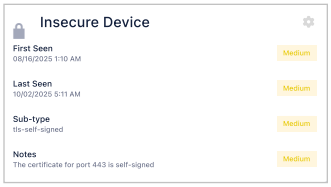
Firmware Management

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



Certificate Management

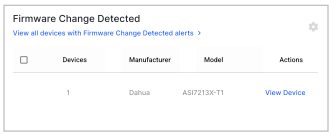
Identify devices operating with expired, self-signed, or improperly configured certificates and automatically update them at scale.



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



Device State Monitoring

Continuously monitor **x**OT estates to detect and alert on device drift and operational changes.



Device Log Retrieval

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

Why Phosphorus

Legacy discovery solutions' 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

© 2026 Dragos, Inc. All Rights Reserved.