Data Sheet

Phosphorus

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 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.

Key **Statistics**

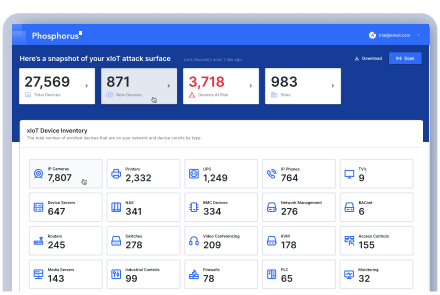
70% of IoT & OT devices deployed with default credentials.

68% of deployed xIoT devices have CVEs of 8 or above.

26% of xIoT devices are end-of-life and no longer supported.

DISCOVER & ASSESS

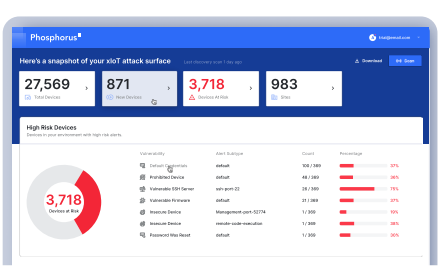
Visibility across tens of thousands of connected devices with high-fidelity data on device attributes, vulnerabilities, misconfigurations, and policy compliance gaps.



xIoT asset discovery

No reckless scanning.

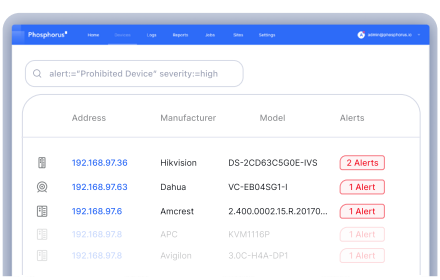
We utilize native device protocols to interact with devices safely, enabling the discovery and profiling of devices with over 15 attributes. These include device type, manufacturer, model/series, IP address, active protocols, firmware version, open ports, active services, and device-specific information.



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 self-signed certificates.



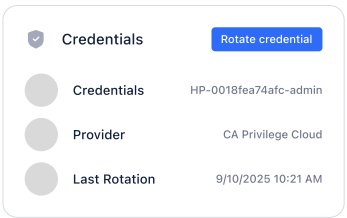
Prohibited device detection and response

Compliance-Driven risk mitigation.

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

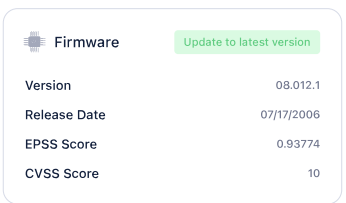
HARDEN & REMEDIATE

Don’t just find it. Fix it. Remediation tasks can be scheduled across thousands of devices within defined maintenance windows.



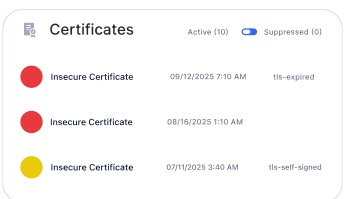
Password management

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

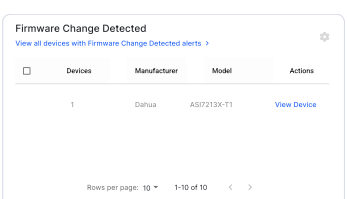
Identify devices operating with expired, self-signed, or improperly configured certificates and automatically update them at scale.

Configuration management

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

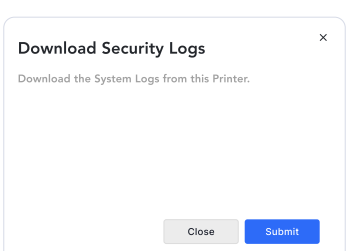
MONITOR & MANAGE

Centrally monitor and manage device configurations, security analytics, and ransomware resilience with backup and restoration.



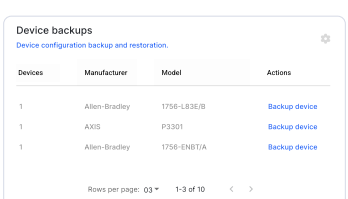
Device state monitoring

Continuously monitor xIoT 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.



Device backups

Increase resilience against ransomware with device configuration backup and restoration.

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. No hardware, agents, SPAN ports, or TAPs required. Full device discovery and assessment in minutes. Automate remediation with a few clicks.

High Fidelity Data. Deep Device Insights.

Identify assets with precision and detect risks that traditional network traffic analysis tools can not detect.

Scale with Confidence

Designed for enterprises managing tens of thousands to hundreds of thousands of devices.

Reduce Risk Exposure

Close the window between vulnerability discovery and remediation with built-in KEV and EPSS context.

Lower Operational Burden

Free security and operations teams from manual, device-by-device remediation with autonomous actions.

Protect Business Continuity

Apply fixes safely and efficiently, protecting uptime and operations continuity.

Phosphorus

See Phosphorus in Action

Request a demo today to learn more at phosphorus.io