Phosphorus

BROCHURE

Phosphorus
Unified xIoT Security Management Platform

Empowering enterprises to go beyond discovery to full xIoT visibility, remediation, and monitoring.

OVERVIEW

Company **Overview**

The Phosphorus Unified xIoT Security Management Platform is the industry's only CPS Protection Platform proactively covering the entire security and management lifecycle for xIoT. Through its unique ability to directly communicate with over one million device models (including over 600 vendors) in their native languages, Phosphorus' platform empowers all organizations to safely discover, remediate, monitor, and manage any IoT, OT, IIoT, and IoMT device, including the most sensitive mission-critical and life-critical assets. It fully automates the remediation of the biggest xIoT device vulnerabilities – including unknown and inaccurate asset inventory, default credentials, out-of-date and vulnerable firmware, risky configurations, banned and end-of-life devices, and expired or self-signed certificates.

The Phosphorus platform is is powered by the industry's first and only scalable Intelligent Active Discovery (IAD) engine that is fast, accurate, and safe, across Cyber-Physical Systems—giving you full visibility into what is on your network and then identifying every device down to the make, model, firmware version, and whether the device is still supported. The software-based and agentless platform enables organizations to go beyond discovery to automatically remediate and monitor vulnerabilities to dramatically diminish the xIoT attack surface, while preventing devices from being used to launch network attacks.

Key **Benefits**

FIND

Safely discover, identify, and assess all xIoT devices quickly and accurately while integrating with 3rd party asset discovery tools.

FIX

Automatically remediate xIoT device vulnerabilities, including passwords, firmware, and certificates, with One-Click.

MONITOR

Continuously monitor all xIoT devices for device drift and other misconfigurations with active alerts and responses.

MANAGE

Centrally manage and change settings and configurations for 1,000,000 xIoT devices through a single pane of glass.

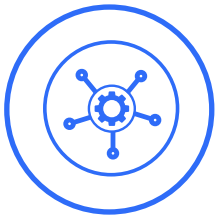
Enterprise xIoT security management for the xTended Internet of Things

More Things means more vulnerabilities. See how Phosphorus can bring enterprise xIoT security to every cyber-physical Thing in your enterprise.

xIoT Discovery & Assessment + **xIoT Hardening & Remediation** + **xIoT Monitoring & Management**

Across all xIoT devices

Enterprise IoT Devices



Operational Technology Devices

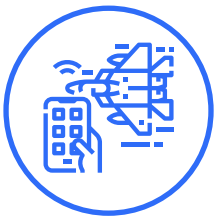
Smart Buildings & Cities

Network & Cloud Connected Devices

Industrial Internet of Things

Internet of Healthcare Things

Smart Ships



Internet of Battlefield Things

INTRODUCING

Phosphorus Intelligent Active Discovery

A new generation of **x**IoT asset discovery & risk assessment.

The Phosphorus Unified **x**IoT Security Management Platform is powered by the industry's first and only scalable Intelligent Active Discovery (IAD) engine that is fast, accurate, and safe, across a wide variety of Cyber-Physical System asset classes, including Office/Workplace IoT devices, OT and ICS devices, IoMT devices, IIoT devices, and other IPv4 or IPv6-enabled embedded devices. The patented Phosphorus IAD approach intelligently calibrates the platform's device interactions, dynamically adjusting discovery parameters such as probe sequencing, packet rates, ports in scope, and more – while ensuring that assets are fully classified with speed, safety, and minimal network impact.

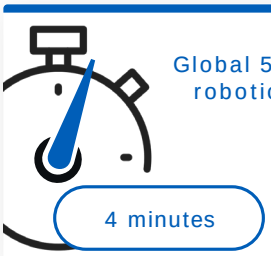
REAL-WORLD EXAMPLES

Fast discovery with immediate results

In multiple large Healthcare and Industrial environments, Phosphorus was able to safely provide a full inventory of IoT, OT, IoMT, and IIoT footprints in minutes or hours, while legacy passive solutions only returned a partial (and inaccurate) inventory in several days or weeks. As a result, Phosphorus is now becoming the solution of choice for enterprise customers with large, multi-homed, highly segmented, global networks—especially considering the ease with which we accommodate physically segmented or air-gapped sites into our centralized management console.

Time-to-discovery for select xIoT customer environments:

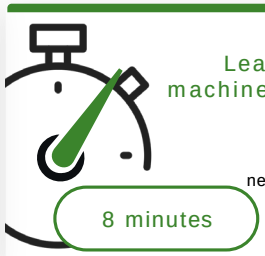
MORE THAN 95% CLASSIFIED



Global 500 machinery & robotics conglomerate

xIoT Discovery across an OT site (1,778 IPs) was accomplished in about 4 minutes.

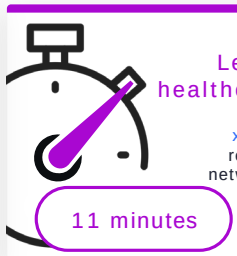
4 minutes



Leading agricultural machinery manufacturer

xIoT Discovery across a representative customer network was accomplished in about 8 minutes.

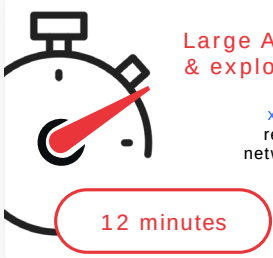
8 minutes



Leading managed healthcare consortium

xIoT Discovery across a representative customer network was accomplished in about 11 minutes.

11 minutes



Large American energy & exploration company

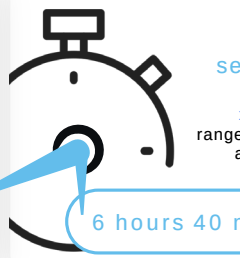
xIoT Discovery across a representative customer network was accomplished in about 12 minutes.

12 minutes

Global economic zone and smart city

xIoT Discovery across the 10.1.0.0/16 network (~65k IPs) was accomplished in about 18 minutes.

18 minutes



Global financial services company

xIoT Discovery across a range of 1.2 Million IPs was accomplished in about 6 hours 40 minutes.

6 hours 40 minutes

WHY PHOSPHORUS?

Why Phosphorus is **unique?**

A Tale of Two xIoT Discovery Approaches

Legacy passive solutions in the market are dependent on network monitoring to perform discovery. The Phosphorus approach does NOT depend on SPAN port traffic analysis for asset discovery. As a result, it doesn't suffer from the many limitations of legacy passive solutions – including limited visibility, incomplete or inaccurate inventory (e.g., OUI lookup-based solutions), slow discovery with long mean-time-to-inventory, network performance impact with strain on network resources, and deployment complexity associated with configuring and maintaining SPAN ports.

THE OTHER DISCOVERY APPROACHES

Dangerous, brute force scanning
Overwhelms devices, often causing harm and interruption.

Assumption-based analysis
Often results in lower confidence & speculation. Not sufficient for device remediation.

Infrastructure dependencies
SPANs & TAPs—requiring big network switching investments.

Unscalable manual effort
Slow, complex, error-prone, costly, and manual.

No remediation
No built-in remediation. Can only isolate using VLANs, which is complex & expensive.

VS

PHOSPHORUS xIoT DISCOVERY APPROACH

Safe, native communication
No reckless scanning. Only safe and intelligent active xIoT discovery using native device protocols.

Evidence-based analysis
No guesswork here. 99% = 0%.
100% device certainty the first time.

No infrastructure or agents
Software-based and agentless. Can be deployed on-prem or in the cloud in minutes.

Automated and scalable
Discovers faster, uses fewer resources, and collects more granular data.

Full remediation
Goes beyond discovery to full risk remediation for passwords, firmware, certificates, configurations.

HOW IT WORKS

How does **Phosphorus work?**

Phosphorus has developed the industry's only **x**IoT discovery and remediation platform for securing the rapidly growing enterprise IoT, OT, IoMT, and IIoT landscape often overlooked by conventional cybersecurity. The software integrates seamlessly with existing network systems and includes three main patented functionalities:

Discover all xIoT 1

Discover & identify IoT, OT, IoMT, and IIoT devices safely, accurately, & without impacting them.

Assess & Identify 2

Assess & show risk posture of **x**IoT devices by identifying weak credentials, out-of-date firmware, EoL assets, or expired certs.

Password Hardening 3

Proactive credential hardening actions, changing default passwords & enabling scheduled rotations to limit password lifespans.

Remediate & Patch 4

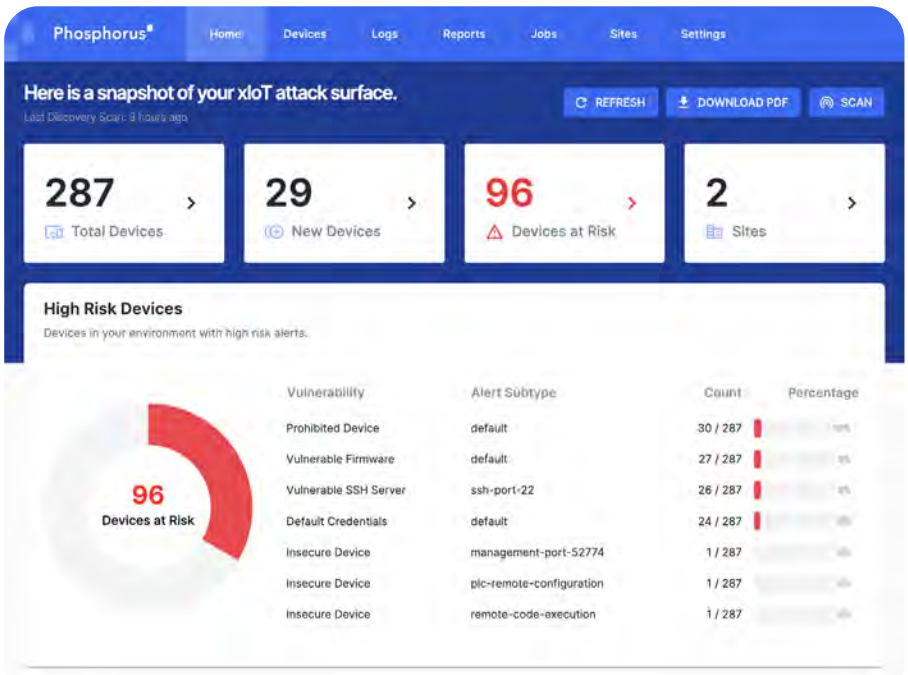
Remediate vulnerabilities with a click of a button while maintaining the control needed in sensitive environments.

Maintain & Respond 5

Continuous monitoring of IoT, OT, IoMT, and IIoT devices for environmental drift or compliance with existing regulations.

THE PLATFORM

The Phosphorus Unified xIoT Security Management Platform is a comprehensive breach prevention solution for securing OT, IIoT, IoMT, IoT and other xIoT devices in organizations. It can:



Discover & identify IoT, OT, IoMT, and IIoT devices safely, accurately, and without impacting them.

Assess & show risk posture of **x**IoT devices by identifying weak credentials, end-of-life assets, CVEs, expired certificates, or out-of-date firmware.

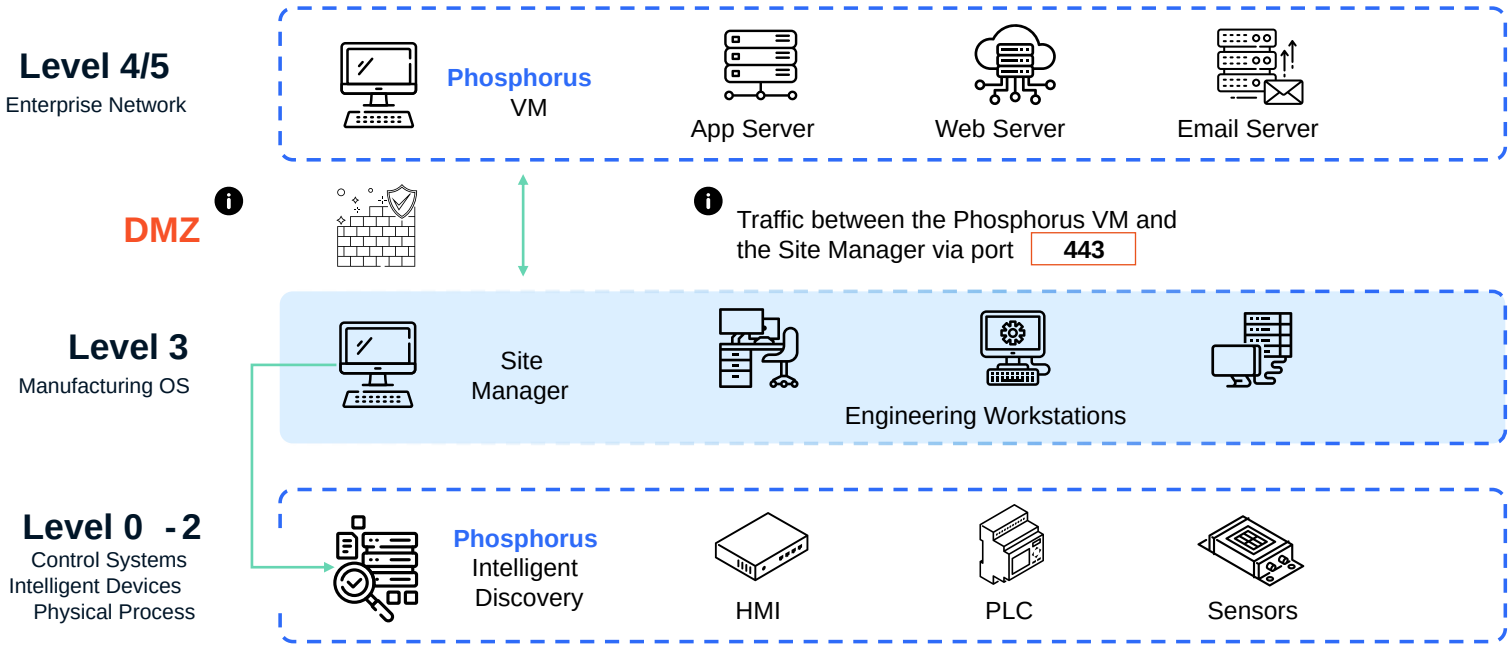
Continuous monitoring & management of IoT, OT, IoMT, and IIoT devices for environmental drift or compliance with existing regulations.

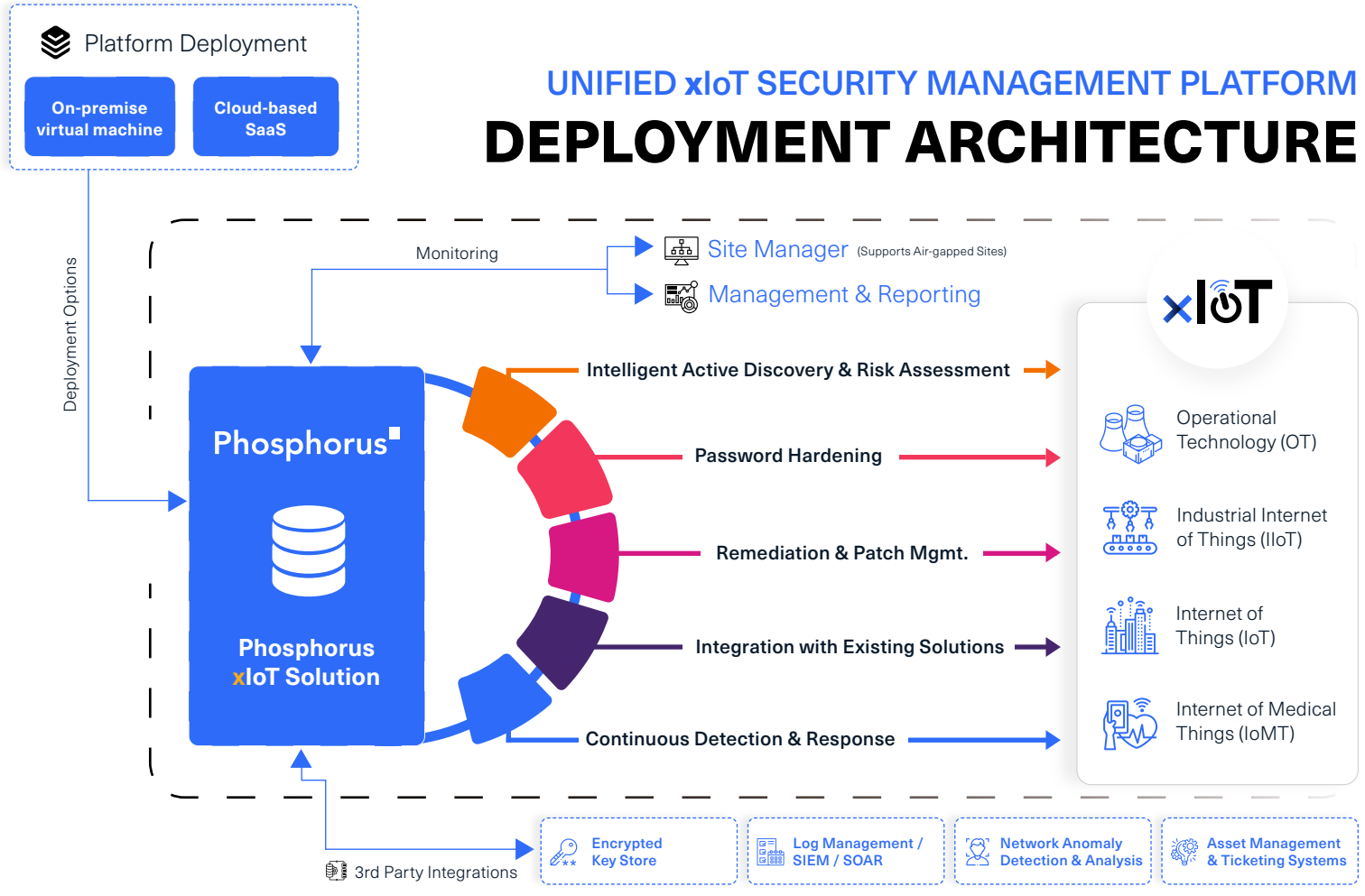
Integrate with existing IT infrastructure like Encrypted Key Store, SIEM, and SOAR for rapid ROI.

Remediate vulnerabilities with full control at your fingertips, while maintaining the control needed in sensitive environments.

Phosphorus and the Purdue Model

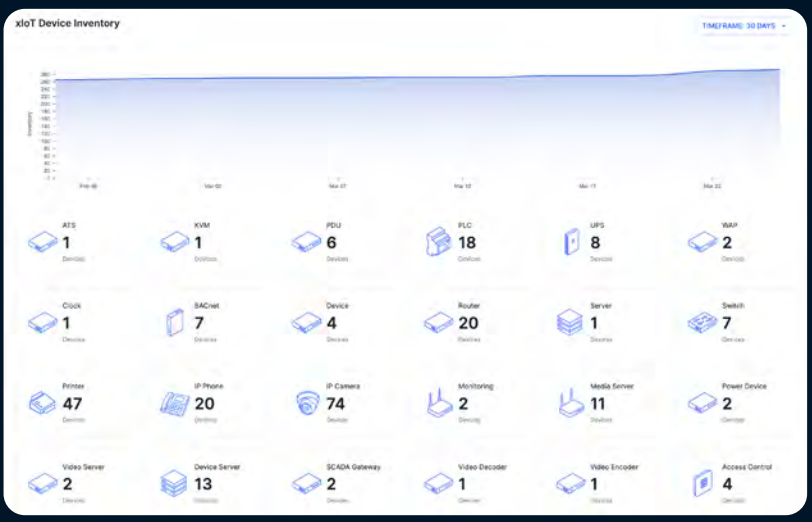
Leveraging Phosphorus Site Manager to negotiate communication through the DMZ.





FEATURES

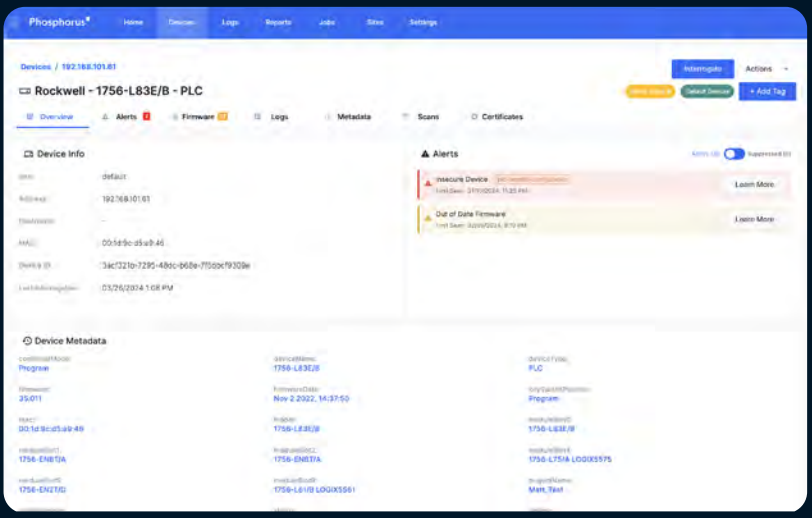
Key **Features**



Intelligent Active **Discovery**

See every xIoT device.

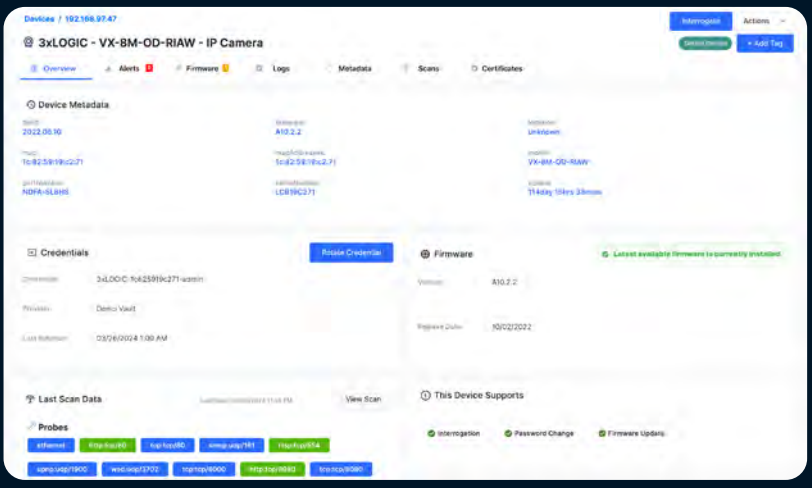
- Complete visibility of all xIoT devices discovered through active polling, not traffic monitoring
- Deterministic discovery means first-time and accurate classification
- High-resolution device detail, with granular device risk assessment & metadata
- Safely discover even the most sensitive, legacy, and critical OT, ICS, and IoMT devices



Risk **Assessment**

Point-in-time xIoT device posture view.

- In-depth posture & risk assessment on every discovered xIoT device
- Identifies issues like default device credentials, out-of-date device firmware, and out-of-date certificates
- Identifies all known vulnerabilities and critical CVEs
- Powered by our extensible high-fidelity xIoT device intelligence



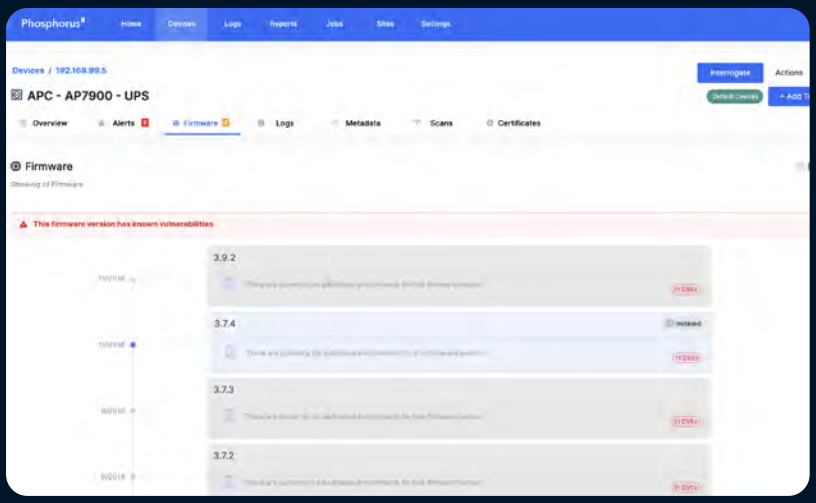
Password & Device **Hardening**

Seamless credential management.

- Have control at your fingertips to update and rotate device credentials at scale
- Automated password rotation and Encrypted Key Store enrollment
- Automated device certificate validation, hardening, and management
- Integrated with leading Encrypted Key Store solutions including CyberArk

FEATURES CONT.

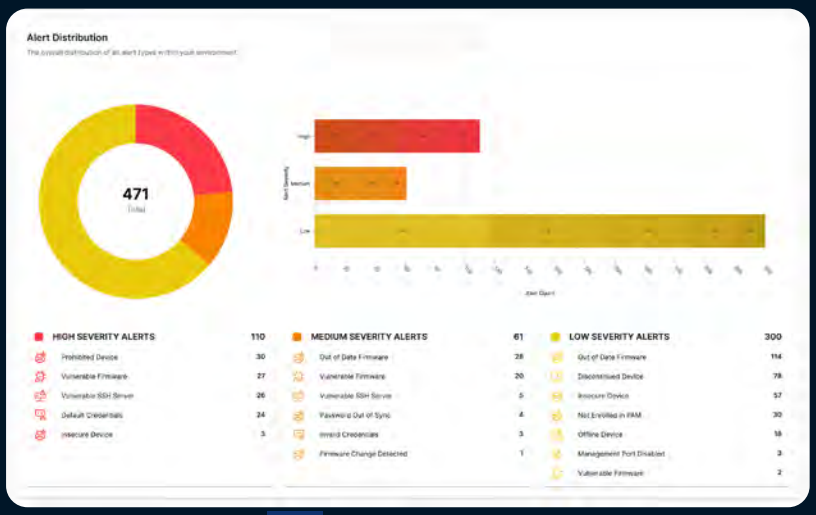
Key **Features Continued**



Remediation & **Patch Management**

Agentless remediation.

- Have control at your fingertips to harden and remediate xIoT device vulnerabilities
- Proactively remediate risky xIoT device configurations and perform certificate updates
- Automatically upgrade and downgrade firmware while maintaining the control needed in sensitive environments
- Flexible and compatible with your unique policies and requirements



Monitoring & **Management**

xIoT monitoring & threat disruption.

- Monitor your xIoT devices to detect & alert on environmental and configuration drift
- Get in-depth alert actions for password resets, expired certificates, EoL devices, CVEs, expired certificates, and out-of-date firmware
- Be in the know about new, unknown, rouge, or prohibited IP-connected xIoT devices
- Extract platform & device activity, alerts, and discovery logs for analysis or investigations

Phosphorus

Connect with us to get started

To learn how your network can be more secure and cost-effective without compromising on performance, please connect with us at **www.phosphorus.io**.

About Phosphorus Cybersecurity®

Phosphorus Cybersecurity® is the leading CPS Protection Platform delivering a proactive approach to security management and breach prevention for the exploding IoT, OT, IIoT, and IoMT attack surface. Designed to find and secure the rapidly growing, unknown, and often unmonitored world of Cyber-Physical Systems across the xTended Internet of Things landscape, our Unified xIoT Security Management Platform provides unmatched security management and breach prevention across every industry vertical—delivering high-fidelity discovery and risk assessment, proactive hardening and remediation, and continuous monitoring and management.

With patented xIoT Intelligent Active Discovery and risk assessment, Phosphorus automates the mitigation and remediation of the most significant IoT, OT, IIoT, and IoMT device vulnerabilities – including unknown and inaccurate asset inventory, default credentials, out-of-date and vulnerable firmware, risky configurations, banned and end-of-life devices, and expired or self-signed certificates.

Follow Phosphorus on LinkedIn, X, and YouTube, and learn more at **www.phosphorus.io.**

PlanetCyber

Planet Cyber Co., Ltd.
157 Soi Ramindra 34, Ramindra Rd., Tarang,Bangkhen, Bangkok 10230
Tel: 02 792 2400 Fax: 02 792 2499
Email : planetcybergroup@planetcomm.com
Website : www.planet-cyber.com