INDUSTRY · DATA CENTERS

Securing The World's Largest Data Center Environments

Customer Background

A leading provider of Data Center solutions, this organization spans the globe with tens of millions of square feet in current and in-construction mega-scale Data Center and Colocation space. Covering a wide range of needs — from digital entertainment to transportation and energy to gaming — this customer is a leader in its industry. Priding itself on robust connectivity and white-glove service, they give clients direct access to information on water consumption and power usage, right down to the rack. Uptime and availability is critical to their offering, and extends to their Cyber-Physical Systems (CPS), which include a diverse set of mission-critical IoT and OT devices.

Business Need

To meet the needs of an escalating client list and growing physical footprint, the security and operations team aimed to establish complete, high-fidelity visibility across all of its IoT and OT devices. Having built a security program around Enterprise IT Service Management (ITSM) asset discovery, vulnerability management, remediation, and patching, they lacked a best-of-breed platform that could FIND, FIX, and MANAGE their ever-growing **x**IoT estates — while integrating ServiceNow into their Configuration Management Database (CMDB) and Data Center Infrastructure Management (DCIM) systems.

Their expansive estates — environmental sensors, Static Transfer Switches, communication cards, chillers, PDUs, rack cabinets, Building Management Systems, HVACs, cameras, KVMs, and more — had been operated by autonomous groups across multiple national and international facilities. The objective: a comprehensive, high-fidelity discovery to achieve an accurate inventory and risk assessment of every IoT and OT device across all sites.

This required a "low-impact tool with high-impact output" that could safely find ALL **x**IoT assets — including mission-critical devices — without disruption, then manage and act on device vulnerabilities at scale, all while integrating seamlessly with existing workflow investments including ServiceNow.

AT A GLANCE

A Quickly Growing Global Data Center Network

Tens of millions of square feet of mega-scale Data Center & Colocation space across the globe.

THE CHALLENGE

- Independent groups overseeing building & energy management systems.
- Disparate IoT/OT device categories lack central visibility.
- Mission-critical **x**IoT require safe, low-impact discovery.

xIoT RISK POSTURE

- Devices with Default Passwords
- Devices with Vulnerable Firmware
- Poor Visibility Segmented by Groups and Locations

The Solution

To address these challenges, the global Data Center network turned to Phosphorus, seeking a best-of-breed CPS Protection Platform capable of safely and accurately discovering and fully assessing all of their IoT and OT assets — while enabling proactive device hardening, remediation, and monitoring across all facilities worldwide. Phosphorus easily met the requirement for a lightweight, agentless, software-based on-premise deployment (with a cloud-based option) that delivered all **x**IoT functionality in one unified platform.

This enabled their teams to achieve complete visibility of all **x**IoT assets — including sensitive Operational Technology — while enabling proactive risk remediation without disruption. In an initial proof-of-value deployment, the platform discovered, identified, and fully profiled **"...a LOT of xIoT devices that we didn't know we had,"** surfacing high-risk, high-impact vulnerabilities including default passwords, critical CVSSs, outdated firmware, and banned or end-of-life devices.

xIoT Attack Vectors

LOW BARRIER OF ENTRY — HIGH POTENTIAL FOR IMPACT

Results

Phosphorus, now part of the Dragos portfolio, delivered immediate benefits to a network spanning millions of square feet — ensuring complete visibility, risk assessment, and remediation across a sprawling **x**IoT environment. The platform provided faster-than-expected time-to-discovery, accelerated vulnerability assessment, scalable device hardening and remediation, integration with ServiceNow and other systems, and the ability to monitor and manage sensitive IoT/OT devices at scale — without downtime or lost revenue.

The organization was further impressed by another element they found while using the product: its people. *"The demonstrable professionalism, agility, nimbleness, and receptiveness of the Phosphorus team to roll up their sleeves and partner with us to create value surprised us."*

BENEFITS

This global Data Center network gained these benefits to solve their business needs with the Phosphorus Unified **x**IoT Security and Management Platform.

- ✓ Safe, fast, and comprehensive **x**IoT discovery
- ✓ Complete IoT/OT asset inventory and risk assessment
- ✓ Proactive device hardening and remediation
- ✓ Continuous device monitoring and management
- ✓ Agile support and seamless integration with ServiceNow

"While we believe the platform to be unique in supporting its many capabilities, we found the account team to be a key differentiator in their approach to our needs.

We felt that the team clearly demonstrated what a true partnership could achieve and thus created a value multiplier which will pay dividends over the life of the product."