Forescout and Phosphorus

Consistent IoT Lifecycle and Security Management at Enterprise Scale

The Challenges

The Internet of Things (IoT) is experiencing exponential growth across all industries as well business, industrial, public and personal domains. While IoT devices provide new services and sources of data with many benefits, they also introduce extensive management inefficiencies and security risks. Research tells us that "84% of security professionals believe IoT devices are more vulnerable than computers due to poor patching and credential rotation". To proactively combat IoT risk factors, it is critical to have continuous visibility into connected devices, their location on the network, whether they are compliant to password and patch policies and are behaving as expected.

IoT devices, unlike traditional IT, are typically unmanaged, lack basic hygiene, out of compliance and unable to run third party software. As a result, these devices introduce extreme risk and safety issues. Massive IoT proliferation connectivity and internet access creates a plethora of potential threat vectors if these devices are not managed, secured and segmented properly.

IoT devices cannot host agents that allow traditional enterprise-level IT systems to manage and secure them, resulting in high management overhead and risk due to lack of cohesive visibility, manageability and security. If a new firmware update or patch is required, thousands of man hours are required to find all affected devices, then schedule, dispatch and manually update each device through its own management interface and potentially at each location. These management inefficiencies also increase risk since a malicious actor could take advantage of non-remediated vulnerabilities on both managed and unmanaged/unseen devices.

> **By 2023, the average CIO will be responsible for more than 3 times the endpoints they managed in 2018** [1]
>
> GARTNER

The Solution

The integration of Forescout and Phosphorus Spyglass address these challenges by providing a dynamic, agentless and consistent IoT lifecycle, performance and security management solution at enterprise scale. The joint solution discovers, classifies, onboards, and manages IoT devices, streamlining IoT lifecycle management. The combined solution mitigates credential and vulnerability risks across the IoT landscape.

The joint solution provides organizations with the ability to automatically find and fix:

- Unpatched Firmware
- Default credentials
- Backdoors
- Bots
- Vulnerabilities
- Malicious devices

Forescout and Phosphorus Spyglass – Better Together

By integrating Phosphorus Spyglass' agentless IoT security and remediation with Forescout's agentless and continuous device visibility, threat monitoring and control capabilities, you can increase operational efficiency and reduce risk with the following capabilities through a consistent management interface for your organization's vast landscape of heterogeneous IoT devices.

- Automatically discover, classify and onboard connected IoT devices for management
- Monitor device health, configuration and network behavior
- Dynamically manage, patch, control network access and segment IoT devices at scale
- Continuously enforce device compliance
- Discover default passwords and manage credentials

How it Works

Forescout acts as a universal enterprise IoT platform to Phosphorus Spyglass by enabling real-time heterogeneous device insight, manageability and security. Forescout does not rely on endpoint/device agents but instead relies on a

BENEFITS

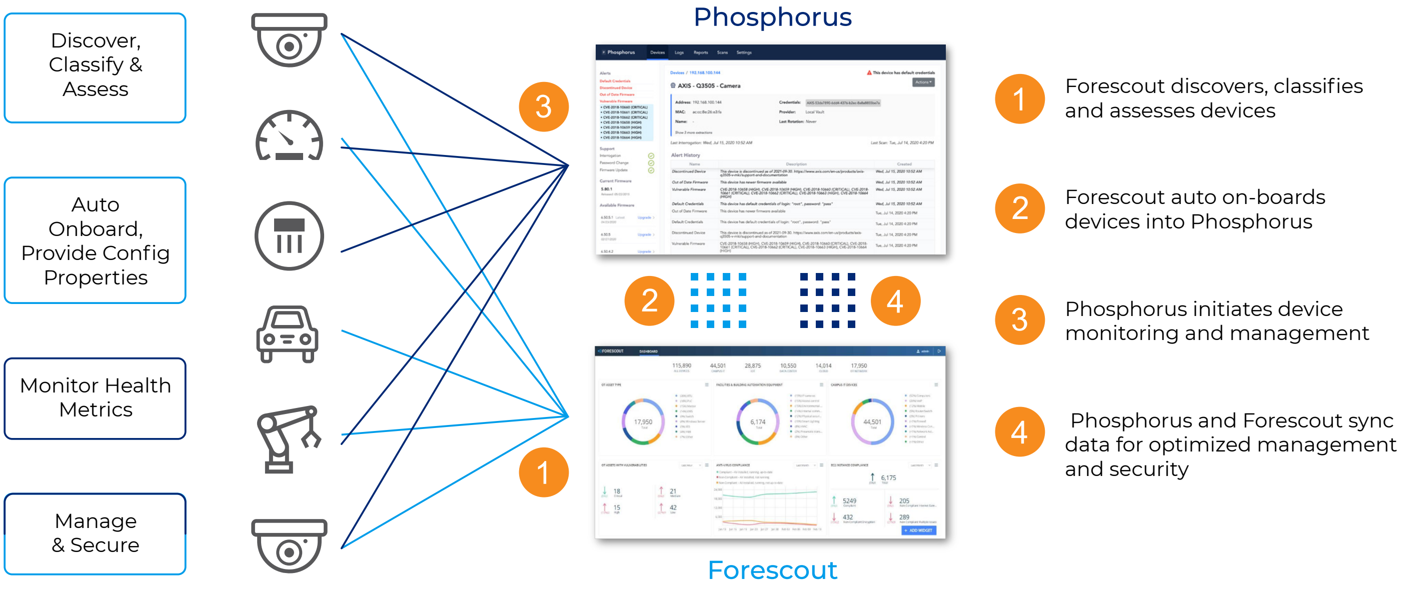
- Gain deep IoT Insight and consistently manage lifecycle
- Reduce IoT management overhead and inventory audit costs
- Mitigate risk by continuously enforcing IoT device security and configuration compliance
- Holistic visibility of enterprise-wide IoT deployments

HIGHLIGHTS

- Dynamic enterprise-scale IoT lifecycle, performance and security management
- Real-time IoT device discovery, classification, assessment and onboarding
- Comprehensive IoT data intelligence and utilization
- Continuous IoT device health and security monitoring
- Granular policy creation and automatic enforcement
- Remediation campaigns across multiple devices simultaneously

range of passive, and active if desired, discovery methods to achieve enterprise-wide connected device visibility and rich context - regardless of device vendor, type or its location on the network. Upon connection, Forescout immediately discovers, classifies and continually assesses devices. Forescout knows whenever a new device connects or any time there are changes in configuration, behavior or network location. Forescout shares this information with Spyglass to validate enrollment and configuration compliance. If a device is not enrolled, Forescout can automatically onboard it into Spyglass via orchestrated workflows. If non- compliant, Forescout also controls network access and can facilitate remediation.

Once a device is onboarded, Spyglass collects detailed metadata (e.g. firmware/ OS version, serial numbers, telemetry data, etc.), enriches with threat and vulnerability data (e.g. CVE details, End of Life, etc.) and combines with Forescout data provided (e.g. device type, manufacturer, function, classification, network location, network behavior, user, etc.). This comprehensive insight enables a baseline setting for anomaly detection and creation of granular policies that can be automatically enforced with confidence. Forescout can leverage any device property from the combined dataset to automatically trigger policy-driven actions that, for example, limit or eliminate network access, dynamically segment, send notification(s) and facilitate IoT remediation through Phosphorus. Orchestrated remediation workflows can include installing missing patches, updating firmware and changing passwords across IoT devices.


Discover, Classify & Assess
Auto Onboard, Provide Config Properties
Monitor Health Metrics
Manage & Secure
Phosphorus
Forescout
1
2
3
4
1 Forescout discovers, classifies and assesses devices
2 Forescout auto on-boards devices into Phosphorus
3 Phosphorus initiates device monitoring and management
4 Phosphorus and Forescout sync data for optimized management and security

Forescout – Phosphorus Workflows

Summary

The combination of Phosphorus Spyglass and Forescout offers the most comprehensive, intelligent, and dynamic enterprise-scale IoT lifecycle, credential and security management solution. The joint solution streamlines IoT device discovery, classification, onboarding, monitoring, management and security. Benefits include increasing operational efficiency, reducing risk and management costs, plus dynamically embracing and securing new IoT devices to safely foster future innovations.

About

Phosphorus

Phosphorus Spyglass is the only market solution conducting agentless IoT remediation. Phosphorus is uniquely advancing IoT security by providing IoT device lifecycle, credential and security management at scale while leveraging your existing tools, such as Forescout, Privileged Access Management and SIEMs, to provide a complete solution.

Forescout

Forescout is the leader in Enterprise of Things security, offering a holistic platform that continuously identifies, segments and enforces compliance of every connected thing across any heterogeneous network. The Forescout platform is the most widely deployed, scalable,enterprise-class solution for agentless device visibility and control. It deploys quickly on your existing infrastructure – without requiring agents, upgrades or 802.1X authentication. Fortune 1000 companies and government organizations trust Forescout to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity.

Forescout also orchestrates information sharing and workflows with third-party security and management systems, such as Phosphorus Spyglass, to close security gaps and increase operational efficiency.

[1] Gartner Top Strategic IoT Trends and Technologies Through 2023, September 2018

> **The riskiest device groups include smart buildings, medical devices, networking equipment and VoIP phones. IoT devices, which can be hard to monitor and control, exist in every vertical and can present risk to modern organizations, both as entry points into vulnerable networks or as final targets of specialized malware. The device types posing the highest level of risk are those within physical access control systems.**
>
> FORESCOUT RESEARCH LABS
>
> **The Enterprise of Things Security Report,**
> **The State of IoT Security in 2020**

Don’t just see it.
Secure it.™

Contact us today to actively
defend your Enterprise of Things.

www.Forescout.com alliances@forescout.com www.Phosphorus.io

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com and Phosphorus.io