Forescout and VMware Pulse IoT Center

Consistent IoT Lifecycle and Security Management at Enterprise Scale

> "By 2023, the average CIO will be responsible for more than 3 times the endpoints they managed in 2018 [2]"
>
> **— Gartner**

The challenge

The Internet of Things (IoT) is experiencing exponential growth across all industries as well as 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 nearly half (48%) of U.S. organizations using some sort of IoT network have experienced a recent security breach[1] and that by 2023, the average CIO will be responsible for more than 3 times the endpoints they managed in 2018.[2] 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 and are behaving as expected.

IoT devices, unlike traditional IT, run lightweight proprietary operating systems with many devices only running firmware embedded in the device. As a result, each device type and/or vendor typically has its own management system, most likely with remote access capabilities as well. This of course requires network connectivity, often IP-based. Massive IoT 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 security patch is required, many hours or days might be needed 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.

Benefits

- Gain deep IoT insight and consistently manage device lifecycle
- Reduce IoT management overhead and inventory audit costs
- Mitigate risk by continuously enforcing IoT device security and configuration compliance
- Streamline adoption of new IoT innovations

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
- OTA remediation campaigns across multiple devices simultaneously
- Proactive anomaly detection and threat defense

The Solution

The integration of Forescout and VMware Pulse™ IoT Center address these challenges by providing a dynamic, consistent IoT lifecycle, performance and security management solution at enterprise scale. The joint solution continuously discovers, classifies and onboards IoT devices, streamlines IoT lifecycle management and mitigates risk across heterogeneous device types and network tiers.

VMware Pulse IoT Center extends VMware's industry leading IT expertise and high standards to the edge, thereby providing enterprise-scale edge infrastructure and IoT lifecycle and security management. With Pulse IoT Center, you can streamline IoT deployments, manage and monitor device health and security standards, and optimize the value of your IoT data.

Forescout is the leading IT, IoT and operational technology (OT) device visibility and control platform. Forescout provides agentless, continuous and absolute device visibility, contextual data insight, anomaly detection, threat monitoring,[3] and policy-driven network and system controls to mitigate and remediate risk in real-time. Forescout also orchestrates information sharing and workflows with third-party security and management systems, such as VMware Pulse IoT Center, to close security gaps and increase operational efficiency.

Forescout and VMware Pulse IoT Center – Better Together

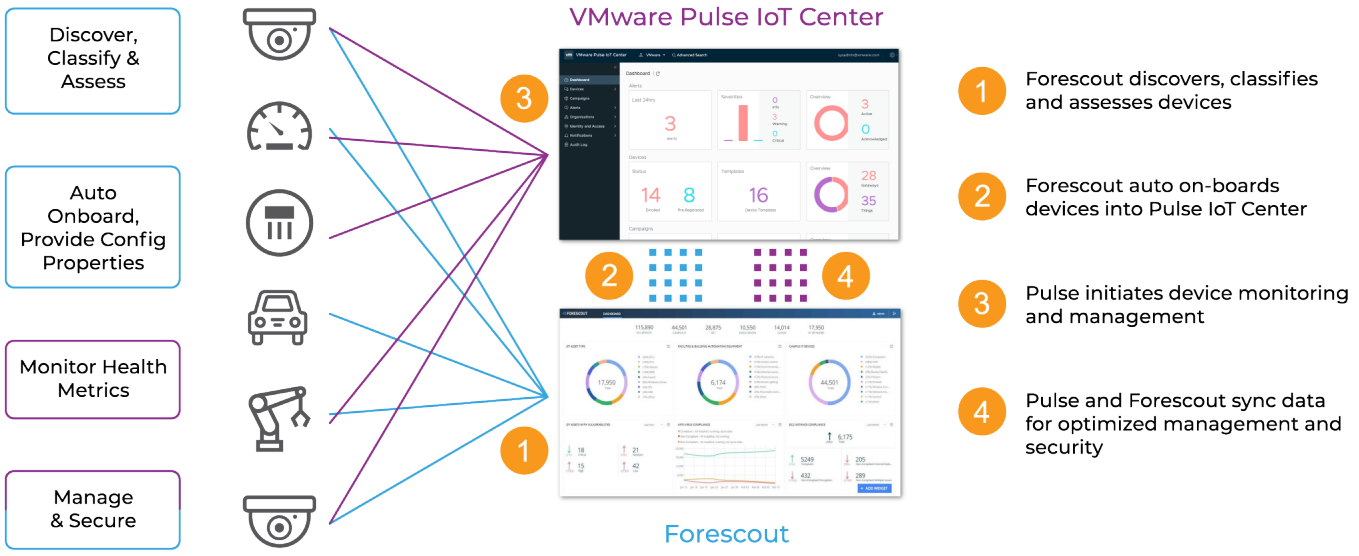
By integrating VMware Pulse IoT Center's lifecycle, performance and security management with Forescout's continuous device visibility, threat monitoring and control capabilities, you can increase operational efficiency and reduce risk with the following capabilities through a consistent management interface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

- Automatically discover, classify and onboard connected IoT devices
- Monitor device health, configuration and network behavior
- Dynamically manage, patch and segment IoT and edge systems at scale
- Continuously enforce device compliance

How it Works

Forescout essentially acts as a universal IoT device gateway to Pulse IoT Center by enabling real-time heterogeneous device insight, manageability and security. Forescout does not rely on endpoint/device agents but instead relies on a 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 also knows whenever a new device connects or any time there are changes in configuration, behavior or network location. Forescout shares this information with Pulse IoT Center to validate enrollment and configuration compliance. If a device is not enrolled, Forescout can automatically onboard it in Pulse IoT Center via orchestrated workflows. If non-compliant, Forescout can facilitate remediation.

Once a device is onboarded, Pulse IoT Center collects health metrics (e.g. firmware/OS version, temperature readings, stage in lifecycle, custom data, etc.) and combines with Forescout data provided (e.g. device type, function, classification, network location, network behavior, user, etc.). Pulse IoT Center also shares its lifecycle and performance health data with Forescout to sync valuable information across both systems. This comprehensive insight enables baseline setting for anomaly detection and the creation of granular policies that can be automatically enforced with confidence. Forescout can leverage any device property to automatically trigger policy-driven actions that, for example, limit or eliminate network access, dynamically segment, send notification(s) and facilitate remediation. Orchestrated remediation workflows with Pulse IoT Center can include installing missing patches, updating firmware, turning off or restarting a device/service. Pulse IoT Center can also leverage Forescout to facilitate over the air (OTA) remediation campaigns to all applicable devices simultaneously.



Forescout – VMware Pulse IoT Center Workflows

Summary

VMware is the leader in providing enterprise-scale IT virtualization and datacenter management. VMware Pulse IoT Center is carrying VMware's IT expertise and standards to the edge by providing IoT device lifecycle, performance and security management at scale. Forescout is the leader in enterprise-wide agentless and continuous device visibility, control and threat defense across IT, IoT and OT. The combination of VMware Pulse IoT Center and Forescout offers the most comprehensive, intelligent, and dynamic enterprise-scale IoT lifecycle, performance 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.

> "I refer to the Forescout platform as our Rosetta stone. It is our device that allows other networked devices, security appliances, firewalls and more to communicate in a universal language and share information. I believe wholeheartedly in integration, but not everything talks nicely to each other – Forescout allows me to do that. To achieve this, State Garden takes a multilayer security approach, which includes the Forescout platform, which helps improve visibility and control of all connected traditional IT, IoT and OT devices."
>
> **– Billy Lewis, Director of Information Technology, State Garden**




1. Altman Vilandrie & Co. https://enterpriseiotinsights.com/20170602/security/20170602securitystudy-iot-security-breaches-tag23
2. Gartner Top Strategic IoT Trends and Technologies Through 2023, September 2018
3. Enhanced threat monitoring for OT networks is provided by Forescout SilentDefense

FORESCOUT

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/VMware