Forescout eyeExtend for VMware Workspace ONE® UEM Powered by AirWatch®

Automate end-user device enrollment, enforce continuous compliance and reduce risk

Today's organizations cannot rely on computing devices staying in one place. Mobile devices such as laptops, mobile phones and tablets have become an intrinsic part of how a workforce accesses corporate resources and data. Not only are such devices used in traditional campus IT environments, they are increasingly being used to manage, monitor and control IoT (Internet of Things) devices in OT (operational technology) networks. With mobile devices accessing hyper-connected networks, threats can easily jump from one part of the network to another.

To safeguard against security threats, organizations are deploying enterprise mobility management (EMM) or more comprehensive solutions such as unified endpoint management (UEM) for all end-user devices. VMware Workspace ONE® UEM powered by AirWatch® ("AirWatch") helps holistically manage corporate and employee owned end-user computing devices. However, security management and compliance challenges still exist for devices that are not corporate owned, not managed or are non-compliant with, for example, an out-of-date UEM agent. The integrated Forescout and VMware AirWatch solution overcomes these challenges by streamlining the process of onboarding, managing and securing today's constantly expanding array of end-user devices.

Challenges

- Discovering, classifying and monitoring all corporate and BYOD end-user devices, including off-premise managed devices
- Ensuring all end-user devices are enrolled in AirWatch for unified management
- Reducing IT and security staffs' manual workload of managing device hygiene and security compliance
- Reducing lengthy response times to mitigate and remediate security threats posed by noncompliant and compromised devices

The Solution

Forescout eyeExtend for VMware AirWatch module orchestrates information sharing and workflows between the Forescout platform and VMware Workspace ONE powered by AirWatch to improve security, increase compliance and strengthen both endpoint and network protection.

eyeExtend

Benefits

- Gain complete visibility of all end-user devices connected to your network, including unmanaged devices
- Increase operational efficiency through real-time assessment and enrollment of devices in VMware Workspace ONE UEM / AirWatch
- Reduce security risk by continuously enforcing proper device configuration and security policies
- Automate remediation workflows for noncompliant or compromised end-user devices

Highlights

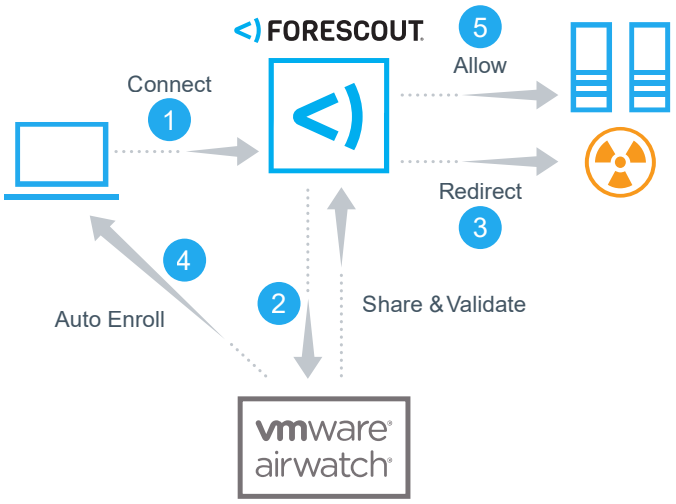
- Real-time discovery of diverse end-user devices without requiring agents
- Seamless enrollment of non- registered devices to VMware Workspace ONE UEM / AirWatch
- Policy-driven device actions such as full wipe or device lock in case of jailbroken or non-compliant devices
- Dynamic network access control by automatically isolating or redirecting non-complaint devices

Forescout discovers and assesses all network-connected devices, then Forescout eyeExtend helps automate enrollment of all required end-user devices in AirWatch. This dramatically reduces manual tasks and optimizes AirWatch device management protection. Forescout also reduces risk by isolating roque, non-compliant or compromised devices until remediated.

Forescout continuously validates devices for compliance with security policies contained in both Forescout and AirWatch, such as AirWatch agent must be installed, up to date and functioning. If Forescout or AirWatch determine a device is out of compliance or compromised, Forescout can automatically restrict network access and orchestrate remediation with AirWatch.

Forescout eyeExtend can also orchestrate AirWatch agent installation on required devices by restricting network access and directing them to an installation web page. Forescout allows access once device passes all required compliance checks.

In summary, the Forescout eyeExtend module enables integration of Forescout and VMware Workspace ONE UEM powered by AirWatch, to provide unified lifecycle and security management of all required end-user devices, regardless of the type (personal computer, tablet, smartphone), connection (wired, wireless, VPN), location (on-premise or remote) or ownership of the device (corporate or personal). Security operations efficiency and effectiveness is increased, while business risk is reduced in real time.



1. Forescout discovers and assesses devices upon connection
2. Forescout shares device properties and validates AirWatch enrollment
3. Forescout redirects or isolates device if found non-compliant
4. Forescout automates AirWatch enrollment and agent installation
5. Forescout allows network access once compliant

Use Cases

Maximize end-user device protection: Forescout drives end-user device enrollment in AirWatch by continuously discovering diverse set of devices the moment they connect to the network - at any time, any network tier. Forescout automatically redirects new or rogue devices for self-registration in AirWatch.

Enforce greater device compliance: If either Forescout or AirWatch detect a device is out of compliance, Forescout automatically helps mitigate risk by restricting network access, notifying security and IT administrators, and can orchestrate remediation.

Apply granular network access controls: The combination of Forescout and AirWatch information equips Forescout to enforce more granular network access policies based on user (guest, employee, contractor) and device (type, configuration, function) profiles. As profiles change, Forescout will dynamically apply the applicable policy-driven network or system controls, including enforce segmentation rules.

Accelerate threat response and remediation: Gain continuous protection from infected, compromised, jailbroken or rooted devices. As Forescout or AirWatch deems devices as compromised or non-compliant, Forescout can automatically isolate or remove devices from the network until remediated. Forescout can also orchestrate policy-driven native or AirWatch actions to remediate such as install AirWatch agent, apply required security patches and do a full wipe or device lock of “jailbroken” devices.

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