

# Forescout eyeExtend for Microsoft® Intune

## Automate mobile device enrollment, improve security management and enforce continuous compliance

In today's enterprise, 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 mobile 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 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 solutions such as Microsoft Intune to help manage mobile devices accessing their corporate networks. But the security management challenge remains for mobile devices accessing the corporate network that are not visible, compliant or enrolled in the enterprise mobility management platform. This is where the Forescout platform and Forescout eyeExtend for Microsoft Intune comes in. The joint Microsoft Intune and Forescout solution provides robust, enterprise-wide mobile device management and security to help IT and security administrators streamline the process of managing and securing today's expanding suite of mobile devices.

### Challenges

- Discovering, classifying and monitoring all corporate and BYOD mobile devices, as well as off-premise devices accessing corporate resources
- Ensuring all mobile devices are enrolled in Intune for unified management
- Reducing IT and security staffs' manual workload of managing device hygiene and compliance
- Reducing lengthy response times and manual processes to address security threats posed by noncompliant or compromised mobile devices

### The Solution:

Forescout eyeExtend for Microsoft Intune orchestrates information sharing and workflows between the Forescout platform and Microsoft Intune to help organizations improve security, compliance and control of mobile devices accessing corporate data.

Forescout helps organizations streamline and automate enrollment of unregistered mobile devices in Intune. Forescout works with Intune to reduce any manual workload that your IT staff has for enrolling devices not listed in Intune as they come onto your network.

In addition to helping with mobile device enrollment, Forescout also ensures that as devices connect to the network, they have the right security posture and are compliant throughout the time they are connected to the network. Forescout continuously



eyeExtend

### Benefits

- <> Gain complete visibility across all IP-connected devices, including mobile devices accessing corporate networks
- <> Increase operational efficiency through real-time assessment and enrollment of mobile devices in Intune
- <> Reduce security risk by continuously enforcing proper device configuration and security policies
- <> Automate remediation and response for noncompliant or compromised mobile devices

### Highlights

- <> Real-time discovery of diverse mobile devices such as iOS, Android, Windows, and macOS without requiring agents
- <> Seamless enrollment of non-registered devices to Microsoft Intune
- <> Policy-driven device actions such as full wipe or device lock in case of jailbroken or noncompliant devices
- <> Network access control by dynamically quarantining or blocking deviant devices from accessing the corporate network

monitors all devices against Intune policies. If a device falls out of compliance or gets compromised as identified by Forescout or Intune, Forescout eyeExtend for Intune can help orchestrate the remediation process automatically with Intune to help increase security operations efficiency while reducing business risk in real time.

In summary, with Forescout you gain unified security management for mobile devices on your network, regardless of the type (personal computer, tablet, smartphone), connection (wired, wireless, VPN), location (on-premises or off-premises) or ownership of the device (corporate or personal).

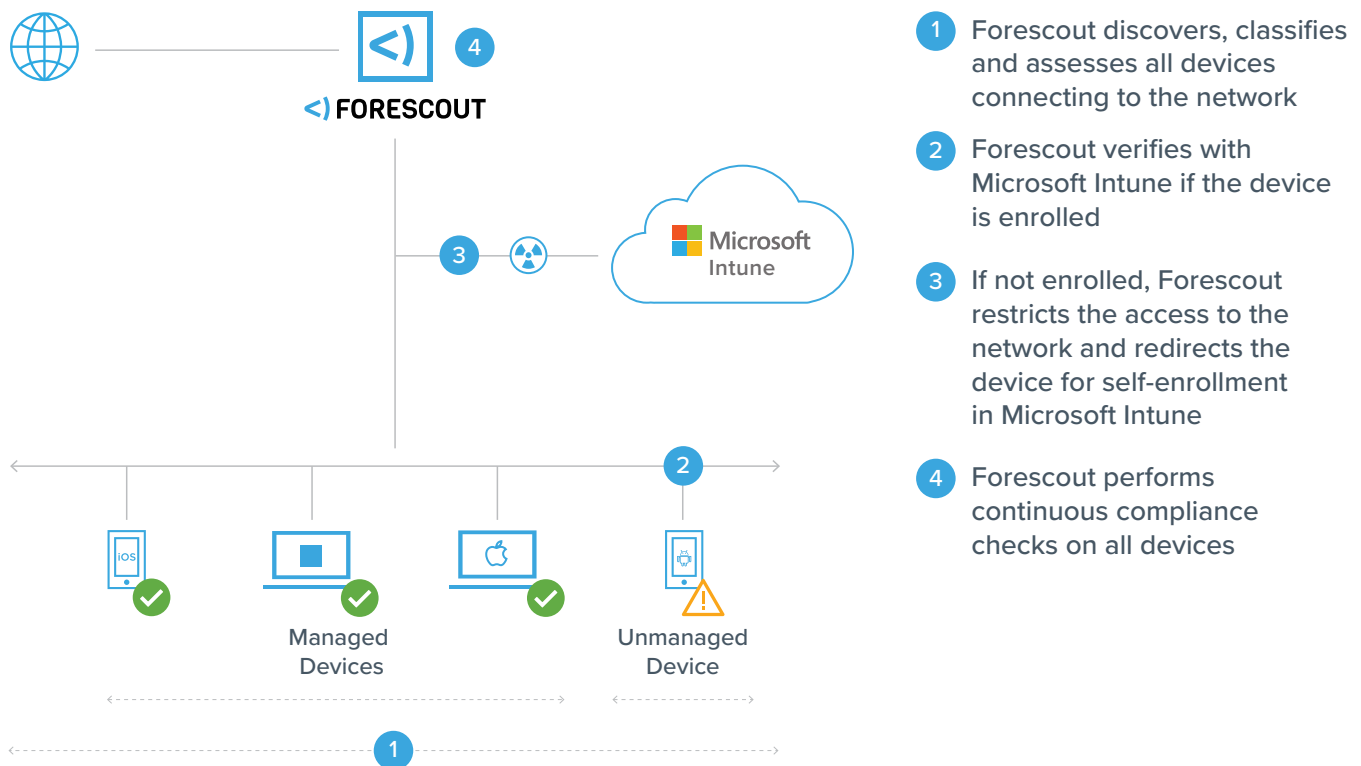
## Use Cases

**Automate device enrollment:** The Forescout platform helps drive mobile device enrollment in Intune by continuously discovering diverse iOS, Android, Windows and macOS devices the moment they connect to the network. It automates device onboarding by redirecting new devices for self-registration in Intune thus helping drive device enrollment in Intune in real time.

**Enforce Device Compliance:** In case of devices deviating from security policies, the Forescout platform restricts their access to the network and notifies the security and IT administrators. Forescout can automatically take policy-driven actions such as full wipe or device lock in case of jailbroken or other noncompliance issues either natively or through Intune.

**Apply custom network access controls:** Forescout enables you to control access to your enterprise resources based on user profile (guest, employee, contractor) and device classification by operating systems. You can apply differentiated access for guest and BYOD mobile devices by limiting their access to the guest wireless network.

**Accelerate response actions and remediation:** When a device is identified as either noncompliant or compromised, Forescout can dynamically quarantine or block the device from accessing the network and can initiate remediation workflows until the device is deemed compliant and healthy. Forescout can also proactively target remediation actions such as installing required security software, updating agents or applying security patches.



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

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

Learn more at [Forescout.com](https://www.forescout.com)

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at [www.forescout.com/company/legal/intellectual-property-patents-trademarks](https://www.forescout.com/company/legal/intellectual-property-patents-trademarks). Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 07\_19