



# ForeScout eyeExtend for Microsoft Intune®

## Empowering Hybrid Workplaces with Comprehensive Endpoint Management

**Manage risks.  
Contain events.  
Mitigate threats.**

**The ForeScout Platform** continuously identifies, protects and helps ensure the compliance of all managed and unmanaged cyber assets – IT, IoT, IoMT and OT.



**ForeScout eyeExtend** helps you improve your security posture, enforce compliance and increase security operations efficiency by automating security processes and response across products.

Gain 360° visibility, network access control and automated threat response for people, devices, and apps regardless of their location.

Organizations depend on Microsoft Intune for endpoint management of devices, desktop computers and virtual endpoints. As hybrid and remote workforce has become mainstream, organizations struggle to provide consistent management and protection across a wide range of endpoints.


By combining the device visibility and automated threat response provided by the ForeScout® platform with Microsoft Intune cloud-based endpoint management, organizations can support BYOD scenarios for hybrid workforces while adhering to zero-trust security principles, enhancing their overall security posture.


### Challenges


- ▶ Gaining real-time visibility across managed and unmanaged devices.
- ▶ Applying security policies across wide range of endpoint devices.
- ▶ Providing granular network access control for specific devices and apps.
- ▶ Lack of automated remediation and response for non-compliant or compromised devices.

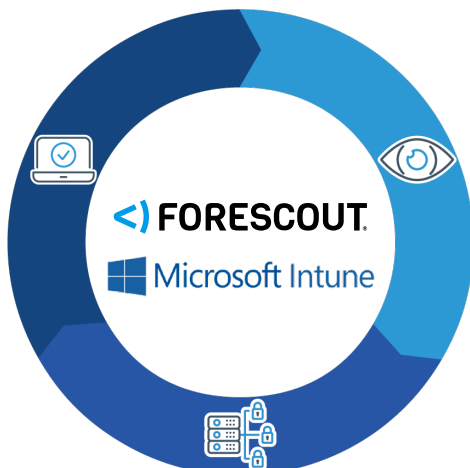
### Joint Value Proposition

Enterprises that already rely on ForeScout® eyeSight and eyeControl for visibility and network access control can now further leverage their Microsoft Intune investments, with the addition of ForeScout® eyeExtend. ForeScout eyeExtend for Microsoft Intune offers a comprehensive solution, addressing challenges in endpoint management and security, providing organizations with the tools needed to navigate the complexities of the modern workplace.




 Single pane of glass for visibility and compliance of all connected devices.

 Network access control and permissions based on Intune enrollment and compliance.

 Automation of compliance and threat response workflows across multi-vendor, multi-tier, policy enforcement points.



## Highlights

-  Complete device visibility including unmanaged BYOD, guest, IoT, IoMT and OT devices
-  Enriched endpoint telemetry for more holistic and granular classification and compliance
-  Automated governance and compliance for endpoint devices

## Use Cases

### Minimize Risk and Exposure

Validate all corporate assets comply to network access control and Intune enrollment policies.

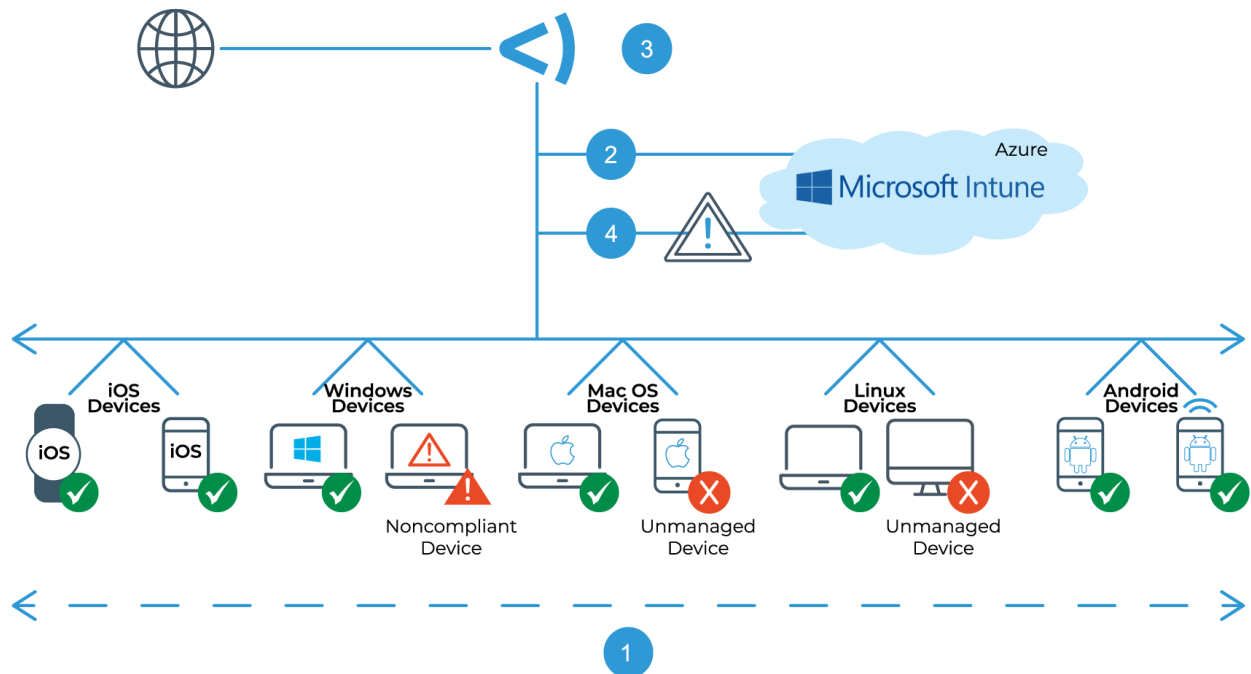
### Zero Trust Access

Enforce remediation and restrict actions for non-compliant devices based on Forescout and Intune compliance policies.

### Enhanced Classification

Enrich Forescout host properties and improve classification based on Intune host properties.

## Forescout and Microsoft Intune Integrated Solution



**1.** Forescout eyeSight discovers, classifies and assesses all IP- connected devices as they connect to the network

**2.** Forescout eyeExtend for Microsoft Intune verifies the device enrollment in Intune and checks for compliance against Intune policies

**3.** If not enrolled, eyeControl redirects the device for self-enrollment in Microsoft Intune

**4.** Forescout performs continuous compliance checks on all devices and eyeControl limits access to the network in real time in case of non compliance