mobile mentor

Intune for Security

BUILDING A FORTRESS FOR YOUR ENDPOINTS

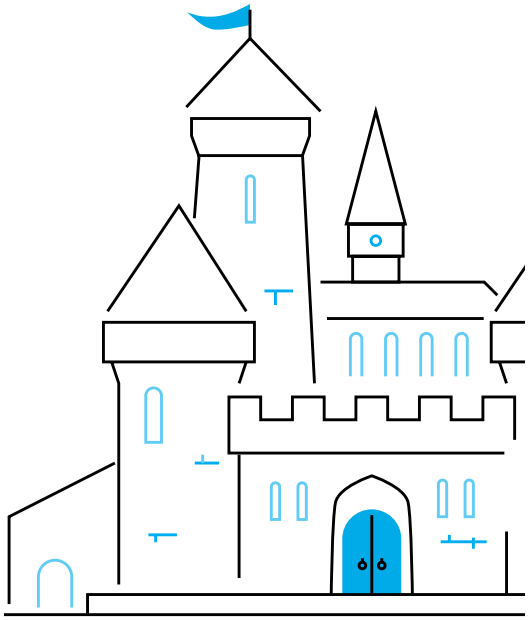
CONTENTS

Intune for Security: Introduction

Are your endpoints truly secure? Every unlocked device, unpatched app, or misconfigured policy is a potential entry point for cyberattacks. Discover how Microsoft Intune can transform your security posture and empower IT teams to defend every digital doorway.

Intune integrates device management, application deployment, and policy enforcement into a single platform. It consolidates what used to require multiple systems, reducing complexity while increasing visibility and control.

With Intune, your business can **maintain robust security, achieve continuous compliance, and adopt proactive vulnerability management from day one.** Employees enjoy seamless access, and IT gains confidence in the business's endpoint security.



A Modern Fortress

Endpoints are now the primary perimeter. Laptops, tablets, and mobile devices serve as gateways to sensitive business data, making them prime targets for cyberattacks.

Ransomware evolves daily, phishing campaigns trick employees, and shadow IT introduces unmonitored applications. Traditional security measures struggle to protect modern, distributed workforces, leaving IT teams with blind spots and employees frustrated with cumbersome access controls.

Imagine your enterprise as a fortress.

Each device is a tower, each application a gate, and every policy a vigilant guard. **Intune acts as the architect and warden**, orchestrating automated provisioning, continuous monitoring, and adaptive defenses to protect your digital kingdom while enabling smooth operations for employees.

Apply a Secure Posture

Out-of-the-Box Security

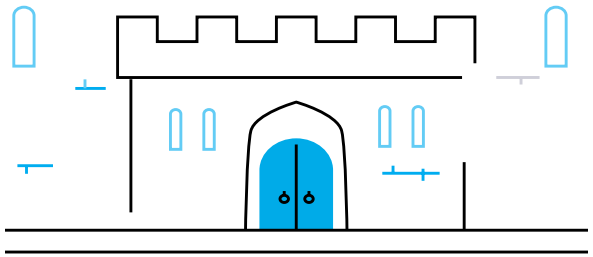
Like fortifying a castle before opening the gates, **Intune ensures devices are secure from day one.** Using Autopilot, Windows devices are provisioned automatically, eliminating misconfiguration and human error. Similar tools for Mac (Platform SSO), Android (Enterprise or Knox enrollment), and iOS create a secure, standardized setup across all platforms.

Passwordless Access and MFA

Windows Hello and phish-resistant MFA create strong authentication barriers. Entra Conditional Access ensures only compliant devices gain entry, while SSO reduces the friction of multiple logins.

Device Hardening and Encryption

Intune applies Microsoft Security Baselines, CIS benchmarks, and WDAC policies. BitLocker and FileVault encrypt data, while Cloud LAPS secures administrative credentials. Windows 365 virtual desktops extend protection for remote or untrusted endpoints.



Automated Device Provisioning

Direct connections to hardware suppliers enable Intune to act as the central provisioning hub. Each device is deployed with secure configurations, applications, and policies, ensuring compliance from the start.

Platform Integration: Windows, Mac, Android

Platform SSO allows users to authenticate seamlessly with Entra ID. Add Android Enterprise and Knox Mobile Enrollment, and all major devices can join the fortress with minimal friction.

App and Data Protection

Company Portal guarantees that only authorized applications are installed. Edge browser controls, OneDrive sync, Intune Tunnel, and expiring access links help secure data in transit and at rest, protecting against leaks and ransomware.

Detect and Eliminate Vulnerabilities

Defender for Endpoint Integration

Like sentries scanning for intruders, Defender for Endpoint continuously monitors devices. It applies attack surface reduction policies and integrates threat signals with Intune for automated remediation.

Vulnerability Management

Defender Vulnerability Manager prioritizes patching for the riskiest systems, including third-party applications often exploited by attackers.

Third-Party Application Management

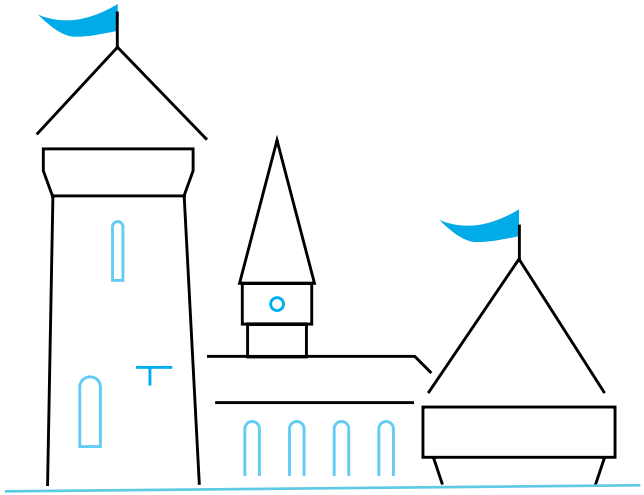
Integration with Enterprise App Manager or PatchMyPC ensures third-party apps are patched in real-time, removing weak links in the fortress walls.

Breach Recovery with Autopilot

If a tower is breached, Autopilot enables rapid reimaging and redeployment, minimizing downtime and restoring security efficiently.

Autopatch and Hotpatch

Windows OS, firmware, drivers, and Microsoft 365 apps are automatically updated. Hotpatch reduces downtime and accelerates vulnerability remediation by requiring fewer Windows restarts.



Improve Compliance

Continuous Compliance Posture

Intune enforces compliance continuously, not as a one-time checklist. Endpoint health, update status, encryption, and antivirus coverage are monitored in real-time.

Cloud App Governance and DLP

Defender for Cloud Apps and Microsoft Purview enforce DLP policies, govern SaaS usage, and protect sensitive data which is critical in the era of Gen AI and public LLMs.

Endpoint Analytics and RBAC

Analytics provide a single-pane view of device compliance across all platforms, including Windows, Mac, iOS, Android, Linux, and Windows 365 VMs. RBAC enforces least privilege principles, tailoring compliance policies by role or department

Zero Trust Enforcement and Conditional Access

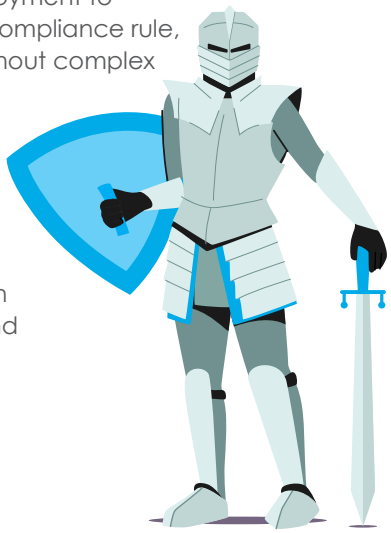
Policies are applied dynamically based on device health and configuration. Noncompliant devices are denied access, maintaining strict security boundaries.

Certificate-Based Compliance

Cloud PKI allows certificate deployment to devices, which can become a compliance rule, adding an extra layer of trust without complex infrastructure

Endpoint Privilege Management (EPM)

EPM enables safe execution of privileged tasks without full admin rights, ensuring accountability and reducing attack surfaces.



The Intune Control Plane Advantage

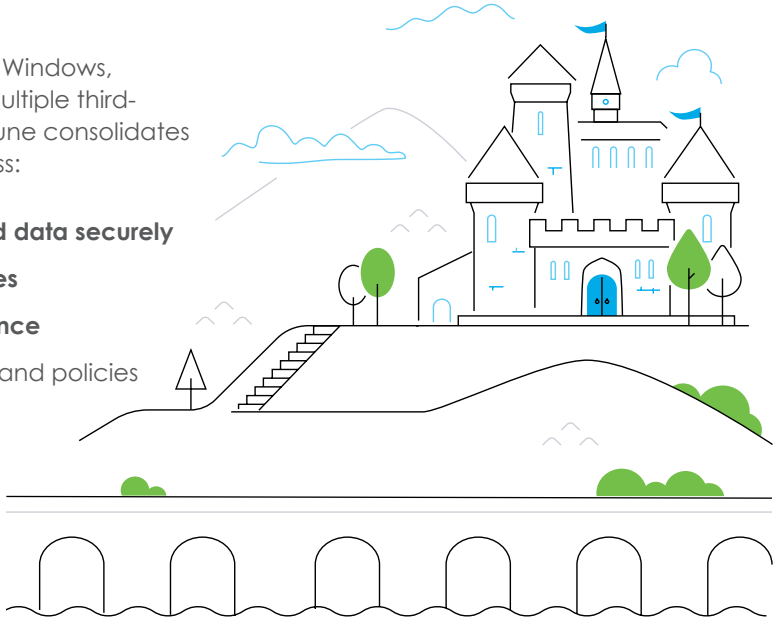
Intune acts as the central control tower of your fortress, managing devices, applications, policies, and data. Its integration with the Defender suite, Purview, Cloud PKI, EPM, and Endpoint Analytics ensures proactive threat detection, fast remediation, and centralized compliance management.

Consolidation: One Tool, One Fortress

Previously, IT teams juggled SCCM/WSUS for Windows, JAMF for Macs, AirWatch for mobile, and multiple third-party tools like CyberArk or TeamViewer. Intune consolidates these capabilities, delivering a unified fortress:

- **Provisioning endpoints, applications and data securely**
- **Detecting and remediating vulnerabilities**
- **Enforcing security policies and compliance**

For the first time in history, all devices, apps, and policies are managed from a single system.



Are You Ready?

What are you waiting for?

Mobile Mentor has guided thousands of businesses through their Intune deployment and secured millions of devices around the world. As Microsoft's Partner of the Year in Modern Endpoint Management, our engineers are ready to unlock the full potential of Intune for your business.

Mobile Mentor offers flexible service options to match your business's needs, for example:

1. **Intune health check and fixed price deployment packages**
2. **Mentoring program – doing the technical work together to make your team the experts**
3. **Intune managed service (including all patching) with agreed SLAs**

Don't wait until a breach occurs. Proactively secure your endpoints today with Intune to prevent ransomware, phishing, and other attacks from compromising your business.
The tools are ready. The strategy is proven.
The only question is: are you ready to build your fortress with Intune for Security?
Check out our other whitepapers on Intune and Modern Endpoint Management here.

mobile mentor