


# How Devicie leveraged Microsoft Intune to reinvent end-user device security



Devicie and Microsoft Intune have a synergistic relationship. Intune is the foundation on which Devicie is built, allowing Devicie to deliver a mix of security and productivity in a way that has not been possible before.



## Intune is a powerful enabling technology

Intune has powerful cloud-based Mobile Device Management (MDM) and Mobile Application Management (MAM) capabilities. However, Intune is not an out-of-the-box solution. Much like ERP, it is an enabling technology where the value is gained after extensive customisation.

This is a recognised challenge for many organisations, affecting small, medium and large enterprises. Intune has historically required highly qualified IT people to make it work successfully for a business. Many organisations have Intune licenses available for employee devices as part of their Microsoft 365 subscription.

# Intune and Device are an **outstanding security combo**



Device presents the potential for your organisation to harness Intune by automating its customisation, configuration and deployment across your fleet of end-user devices. Device also leverages Intune to facilitate automated management and ongoing deployment of best-practice security across your end-user devices. Both of these are achieved with minimal hands-on IT effort, timing delay and no agents required.

Microsoft ensures Intune is secure and highly compliant while Device secures the end-user side of the equation. Device deployment is completely automated, configuring and deploying Intune so that it is ready to provide its full capability to your employees, often in a matter of hours. To ensure your people are enabled, autonomous and any potential issues are addressed before an organisation-wide deployment, we then run a two-week production validation with your pilot group.

End-user experience is paramount.

## How Device enhances your Microsoft 365 experience

Organisations with Microsoft 365 that choose Device for their end-user security management can easily take full advantage of Microsoft's advanced security capabilities.

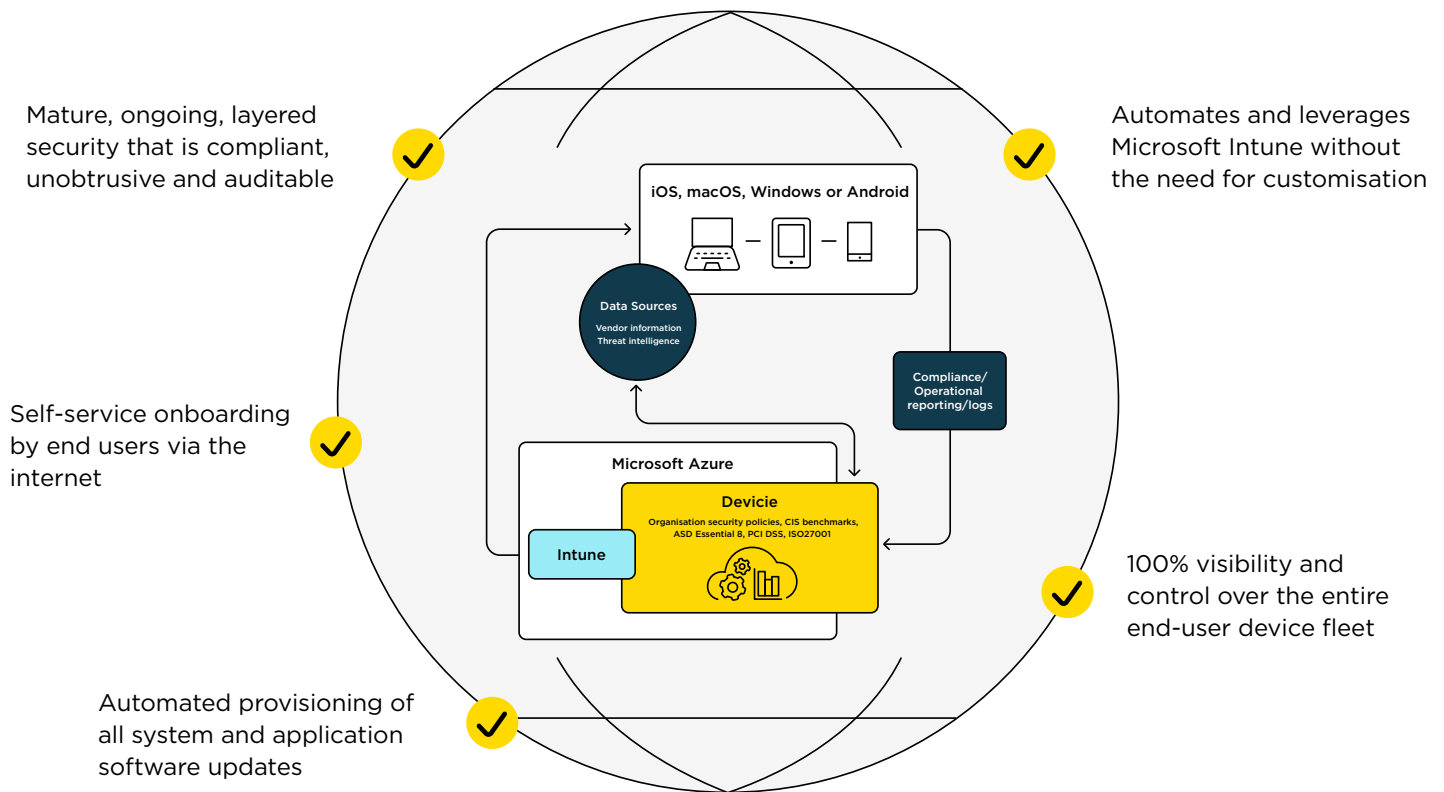
- ✓ Device fully automates Intune and integrates with Azure Active Directory (AAD)
- ✓ Device makes Intune enterprise-ready by automating its customisation
- ✓ Device delivers automated, best-practice, layered security natively via Intune
- ✓ Device fully supports your organisational change processes, as well as your audit, security and operational requirements
- ✓ Device optimises device security and management to improve your team's experience and productivity.

**We are often asked, “Can’t we do this ourselves?” and our answer is, “Why would you?”**

You would have to be able to source and pay for a 6-12 month project filled with SOE and Intune experts, and be willing to pay for expert resources, to attempt to maintain that solution going forward. It would cost you significantly more to pay for Intune implementation and maintenance than Device will cost to install and be available in two weeks.

# What is Device?

Device is a **cloud-native platform** that delivers a modern workplace as a service across every end-user Windows, macOS, iOS and Android device, wherever they are located.



## Make agentless endpoints the new boundary for your organisation

With Device, endpoint devices can become a secure barrier for organisations, rather than the most vulnerable and susceptible to cyber attacks.

Device has no need for configuration or support from your IT team, and manages every machine without an agent. The result is that your IT and security teams will have 100% visibility of the compliance and security posture of every end-user device, wherever it is being used, ensuring they are consistently patched, up-to-date and included in reporting. Furthermore, you'll be championing a better end-user experience that is both flexible and scalable.

Device doesn't require an agent because it leverages Intune to natively manage end-user devices, irrespective of the operating system or location. Device integrates Intune, removing the time, expense and complexity required to configure Intune for an organisation.

**Device is already compatible with Windows, macOS, iOS and Android devices via Intune.**



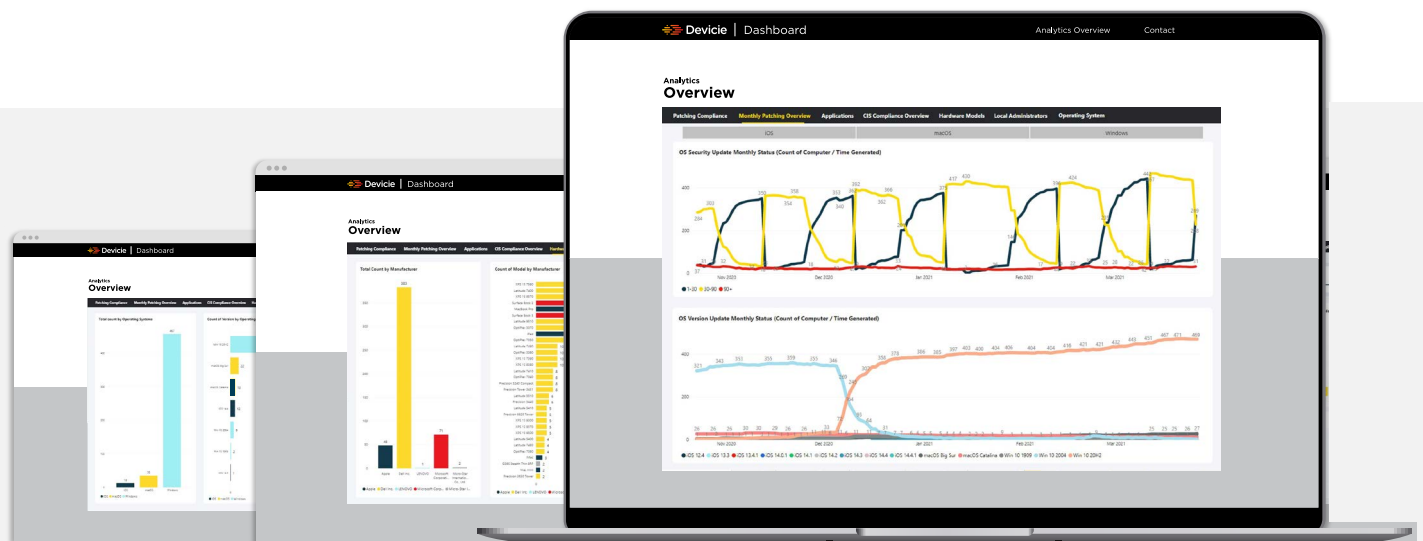
# Devicie benefits

**Devicie automates end-user device security and management so your people can do their best work safely and productively.**

## The benefits of Devicie's approach

Organisations with Office 365 who choose Devicie for end-user security and management can easily take full advantage of Microsoft's advanced security capabilities.

- ✓ Provides a single management console and reporting view for all end-user devices across an organisation, regardless of the operating system
- ✓ Significantly reduces the time, cost and complexity of securely managing and monitoring end-user devices
- ✓ Improves control and visibility over compliance and security issues, making it faster and easier to mitigate threats as they inevitably arise
- ✓ Removes the 'blind spot' attack surface associated with unmanaged machines
- ✓ Automates the mundane and repetitive IT task of manual device set-up, maintenance and management
- ✓ Gives every user a fantastic device experience, and ensures they always have the most up-to-date security, applications and policies to enable their work.



# Devicie **waited** for Intune

Devicie's founders followed Intune from its infancy. For years we had been looking for ways to fully secure and manage end-user devices over the internet. We knew Intune was the best candidate due to its native support within the solution, ahead of third-party solutions requiring agents. Once Intune matured to allow for deployable applications, we knew we had found our agentless foundation for Devicie.

Being able to fully manage an end-user device online without having to perform an in-person deployment was a game changer. We knew we could create a complete, automated, organisation-wide end-user security management solution that required no human IT resources, and in fact, would be far superior to humans trying to do it.

We realised the potential Intune created for an employee or student to take a new laptop out of its box, and have that machine automatically installed with applications deployed, with a simple log-in. Devicie would then configure, secure and manage that device so that no one – including the organisation, its IT team or the end user – would ever have to worry about or be inconvenienced by it again. Best of all, the Devicie dashboard would be available at all times to provide valuable data and extensive reports for compliance, audit and management that proved everything was being managed securely, productively and efficiently.

**We knew we could create a complete, automated, organisation-wide end-user security management solution, that required no human IT resources, and in fact, would be far superior to humans trying to do it.**



## ABOUT DEVICIE

Devicie automates an uncompromising level of end-user device security for organisations, and does this in a way that provides a radically better enablement and management experience for end users and IT teams. We have solved the security versus productivity dilemma for end-user devices, with a cloud-native solution that delivers a modern workplace as a service.

**Website** [devicie.com](https://devicie.com)  
**Email** [askus@devicie.com](mailto:askus@devicie.com)  
**LinkedIn** 