Intune For Cost Savings

CONTENTS

Reduce Costs with Intune

If you're managing devices and users in today's economic climate, chances are you're being asked to do more with less. You're expected to maintain strong security, deliver a great user experience, and—somehow—cut costs at the same time. It's a tough ask, especially when every tool and decision impacts your team and your business.

Our team at Mobile Mentor has deployed Intune for millions of users and devices and we have seen our customers benefit in 3 ways:

1. **Better security**
2. **Better user experience**
3. **Lower costs**

You've probably already seen how Microsoft Intune can strengthen security and streamline the user experience. But what's often overlooked is its potential to deliver real, measurable cost savings. Here are the three main strategies we've seen deliver real, hard cost savings with Intune.

Intune Suite Product Images Courtesy of Microsoft

1. Consolidate the Tech Stack

Manage All Devices with Intune

With Microsoft Intune, businesses can now manage Windows, macOS, iOS, iPadOS, and Android devices from a single platform. Even ChromeBooks, Linux servers, and some specialty devices can be managed at a basic level. This means IT teams can finally move toward a true "single pane of glass" for all device management.

That opens the door to simplifying toolsets and retiring legacy platforms like SCCM, CMG, WSUS, JAMF, AirWatch, ManageEngine, Altiris, and BigFix—and consolidating on Intune as the foundation for cloud-native modern endpoint management
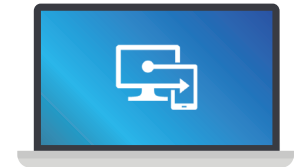
1. Consolidate the Tech Stack

BYOD with Intune

For businesses supporting BYOD, there's even better news. Intune offers powerful App Protection Policies that secure corporate data within Microsoft 365 apps on unmanaged mobile devices. These policies allow companies to restrict actions like copy/paste, save-as, and open-in, helping prevent data loss without needing to manage the device itself.

This can be done while the device remains unmanaged giving your employees peace of mind that their employer cannot see their location, browsing habits, personal apps, etc.

So, instead of paying for company devices, you can have a modern BYOD program, with a great balance between employee privacy and company security at virtually no cost!

Best of all, everything mentioned here is available with standard Microsoft 365 E3 or EMS E3 licenses.

1. Consolidate the Tech Stack

Leverage the Intune Suite

In addition to having 2 or 3 different endpoint management tools, most companies have another set of products for privilege elevation, certificate distribution, 3rd party patching, analytics and remote support. Common vendors are CyberArk, Beyond Trust, Tanium, PatchMyPC, Automox, NexThink and TeamViewer.

Microsoft introduced a powerful collection of tools called the Intune Suite. These native solutions are designed to replace many of the third-party tools, giving businesses the option to manage everything within their existing Microsoft tenant—more integrated, more secure, and often more cost-effective.

Intune Suite gives you the ability to do the following:

- **Publish and distribute certificates to every endpoint without PKI infrastructure**

- **Elevate users from "standard user" to "local admin" for a specific time and purpose**

- **Patch 3rd party applications to eliminate vulnerabilities in real-time**

- **Identify problem devices and applications before the user needs to raise a ticket**

- **Resolve issues quickly with a seamless interface between Sys Admin and end user**

1. Consolidate the Tech Stack

Embrace Zero Trust

VPNs worked well in a traditional, on-premise environment—but they're no longer the best fit for today's modern workplace.

Now, you can replace legacy VPN infrastructure with a modern Zero Trust architecture using tools already included in Microsoft 365 E3.

By combining **Conditional Access** policies, **phish-resistant MFA**, and **Azure App Proxies**, users can securely access on-prem resources and line-of-business (LOB) applications from anywhere—**without the need for a VPN**. It's a more secure, flexible, and modern way to work.

Phish-resistant MFA

Conditional Access

Zero Trust

Azure App Proxies
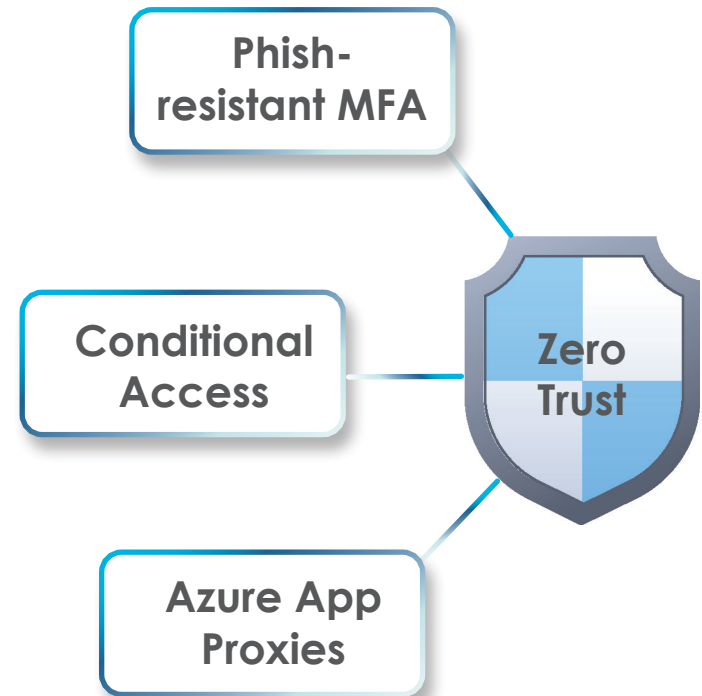
2. Automate Legacy Processes

Provisioning with Autopilot

One of the biggest costs—and headaches—for IT teams has always been provisioning new Windows devices. For decades, system admins had to unbox each machine, set it up manually, then re-pack and ship it to the end user. It's a time-consuming, expensive process.

With **Windows Autopilot**, all of that can be eliminated. Devices can now be shipped directly to employees and configured automatically, saving time, reducing costs, and getting users up and running faster.

Your new Windows machines can be drop-shipped to the end-user for a highly automated out-of-box experience that takes about **20 minutes, not 2 hours**, and doesn't require IT to be involved. This is the magic of Autopilot and Zero-Touch Provisioning.

You can also take advantage of the new features in Autopilot Device Provisioning to streamline the setup process. This allows you to sequence the build activities in a way that best fits your users' needs, reducing setup time and improving efficiency.

Or, you can go a step further and use a Whiteglove Pre-provisioning service so that the out-of-box experience is reduced to about 2 minutes instead of 20 minutes.

2. Automate Legacy Processes

Autopatch

The next major cost—and headache—for IT teams is patching. This includes updates for the OS, firmware, drivers, core Microsoft applications, and third-party apps. Keeping all of these up to date has traditionally been a full-time job for many engineers.

Intune now includes **Autopatch**, which automates security, feature, and quality updates for the Windows OS, along with updates for firmware, drivers, and all Microsoft 365 applications.

Hotpatch is the icing on the cake and enables updates to be deployed with 65% fewer restarts according to Microsoft. While this may save money directly, it reduces downtime by allowing employees to stay in their workflow without needing to restart their device.

2. Automate Legacy Processes

One Drive Sync

Companies with legacy file shares for document storage incur huge hidden costs.

Sharing a document typically involves downloading, editing, renaming, and emailing it back and forth—an inefficient and costly process that can happen multiple times a day for each employee. OneDrive enables people to share a hyperlink to the file so that everybody is collaborating on the same version. Companies who have mastered this also discourage the practice of attaching files to emails.

Intune can selectively sync OneDrive folders and files to a device during zero-touch provisioning, ensuring employees have access to their department files from day one.

2. Automate Legacy Processes

Password Management

The third major cost is password resets and manual authentication. Companies still relying on their Service Desk for password resets are wasting money, as **SSPR (self-service password reset)** offers a seamless, automated solution. While many businesses have moved past this, they often find themselves stuck between managing passwords and fully transitioning to a passwordless system.

Intune includes Windows Hello policies for biometric sign-in to a Windows device. Entra includes Conditional Access policies, phish-resistant MFA and native SSO (single sign-on) to most applications.

Combine these elements, and you have a passwordless strategy that requires no additional licenses, saves money by eliminating the need for a password management tool, reduces the need for password resets, and cuts down on time spent typing passwords every day.
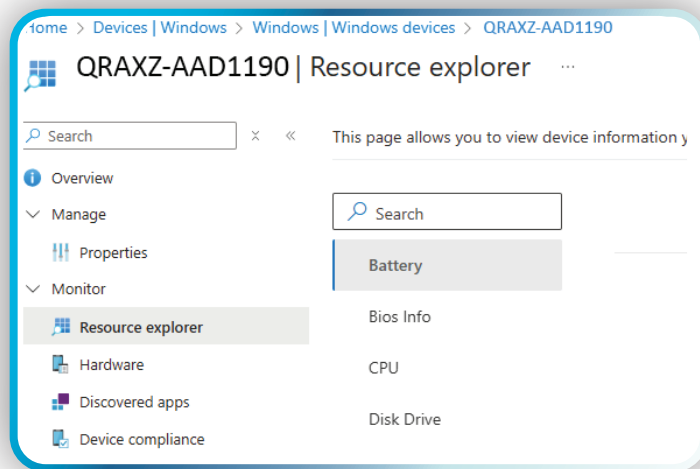
3. Endpoint Lifecycle Management

Asset Tags

Many companies apply physical asset tags to their device. However, the real cost isn't in the tags themselves—it's in the time and resources spent unboxing, tagging, repacking, and managing inventory. Inventory management is costly, leads to product obsolescence, and requires manual stocktaking.

Intune now includes **Resource Explorer**, allowing you to examine a device in great detail.

This eliminates the need for physical asset tags, as Intune can automatically upload key device information—such as the serial number, hardware specs, processor, memory, and available ports.

This data can be integrated into a CMDB, providing a real-time view of assets without the need for tags, storage, or manual stocktakes.

3. Endpoint Lifecycle Management

End User Support and the 30-Minute Rule

Windows devices are notoriously difficult to troubleshoot, especially for remote users in distant locations. Obscure problems can take days for IT support teams to isolate and resolve, ultimately costing thousands of dollars. Simultaneously, there is an adverse impact on the end user's productivity.

Intune changes everything, and some of our customers have adopted the "30-minute rule." If a Windows device has an issue that can't be resolved within 30 minutes, the Service Desk agent can wipe the device and start fresh. They reload the configuration from Autopilot, sync content from OneDrive, and the user is back up and running in about 30 minutes.

With 30 minutes for troubleshooting and 30 minutes to rebuild the device, any issue can be resolved in an hour, freeing the IT team from getting bogged down in costly problems.

3. Endpoint Lifecycle Management

Device Reprovisioning / Retirement

When an employee leaves and a device needs to be reprovisioned, it's typically shipped back to the IT department. There, the team unpacks it, manually deletes the data, starts the provisioning process from scratch, and then ships it to the next user.

Likewise, when devices reach EOL and need to be retired, they have to be shipped, unpacked, wiped, repacked and sent away for recycling. This process is really expensive!

Intune allows IT to remotely wipe data and reprovision the device for the next user, without ever needing to physically handle it.
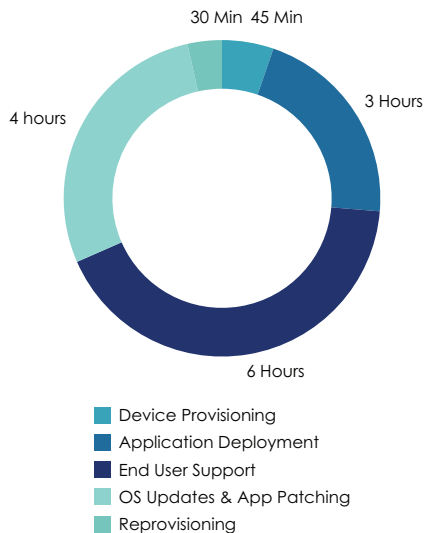
Case Study:

Intune saved 14.25 hours per Windows user per year

A client in Pennsylvania reported the following saving per year.

14.25 Total Hours Saved

30 Min 45 Min

4 hours

3 Hours

6 Hours

■ Device Provisioning
■ Application Deployment
■ End User Support
■ OS Updates & App Patching
■ Reprovisioning

Device Provisioning
2 hours were saved by avoiding double-shipping, double-packing, manual imaging and testing. If this is spread over the device lifecycle, it works out to be ~45 minutes saved per year.

Application Deployment
Packaging, deploying and testing applications typically takes several hours per year but this process is reduced by 3 hours per device when using Intune with the Intunewin protocol.

End User Support
The volume of tickets is reduced with Intune as the configuration is simpler and the time to resolve is ticket is shorter. Applications can be reinstalled, policies and profiles can be updated, OneDrive can be synced. This client uses the 30-minute rule aggressively and regularly reprovisions devices from Autopilot to start over with a fresh build. The combined saving for the Service Desk is 6 hours per device per year.

Case Study:

Intune saved 14.25 hours per Windows user per year

Continued

14.25 Total Hours Saved
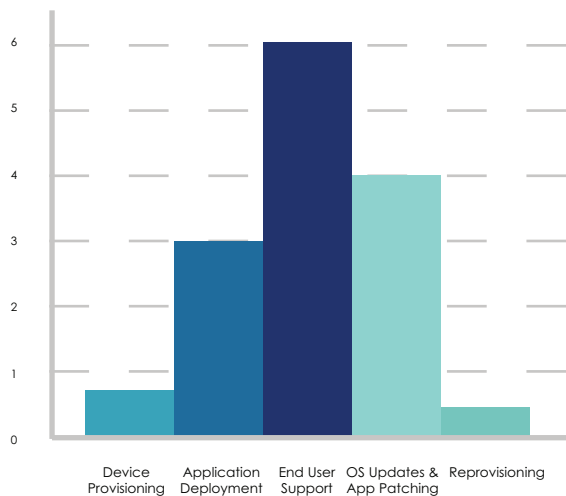
Updates and Patches
Hours are saved by automating OS Updates, firmware and drivers with deployment rings. However, the greatest time saving is in patching 3rd party applications. Historically each update had to be repackaged, tested and redeployed. When application patching is automated, the combined saving is 4 hours per device per year.

Reprovisioning
90 minutes are saved per device per year from the reprovisioning / device retirement process and the associated packing, shipping and double-handling.

Bottom Line
Of the 14.25 hours saved above, 8.25 hours were Sys Admin / engineering hours, and 6 hours were Service Desk. Using industry average wages for these roles and applying a 20% corporate overhead, the cost saving is $711 per Windows user per year.

Scale this across your company to quickly determine the savings Intune can bring.

Are You Ready?

Are you ready to harness the savings potential of Microsoft Intune? For a free consultation, reach out here.

Mobile Mentor is a global leader in the endpoint ecosystem and Microsoft's Partner of the Year in Modern Endpoint Management. Certified by Microsoft, Apple and Google, our engineers specialize in designs that balance endpoint security with employee experience for our clients. Check out our other whitepapers.