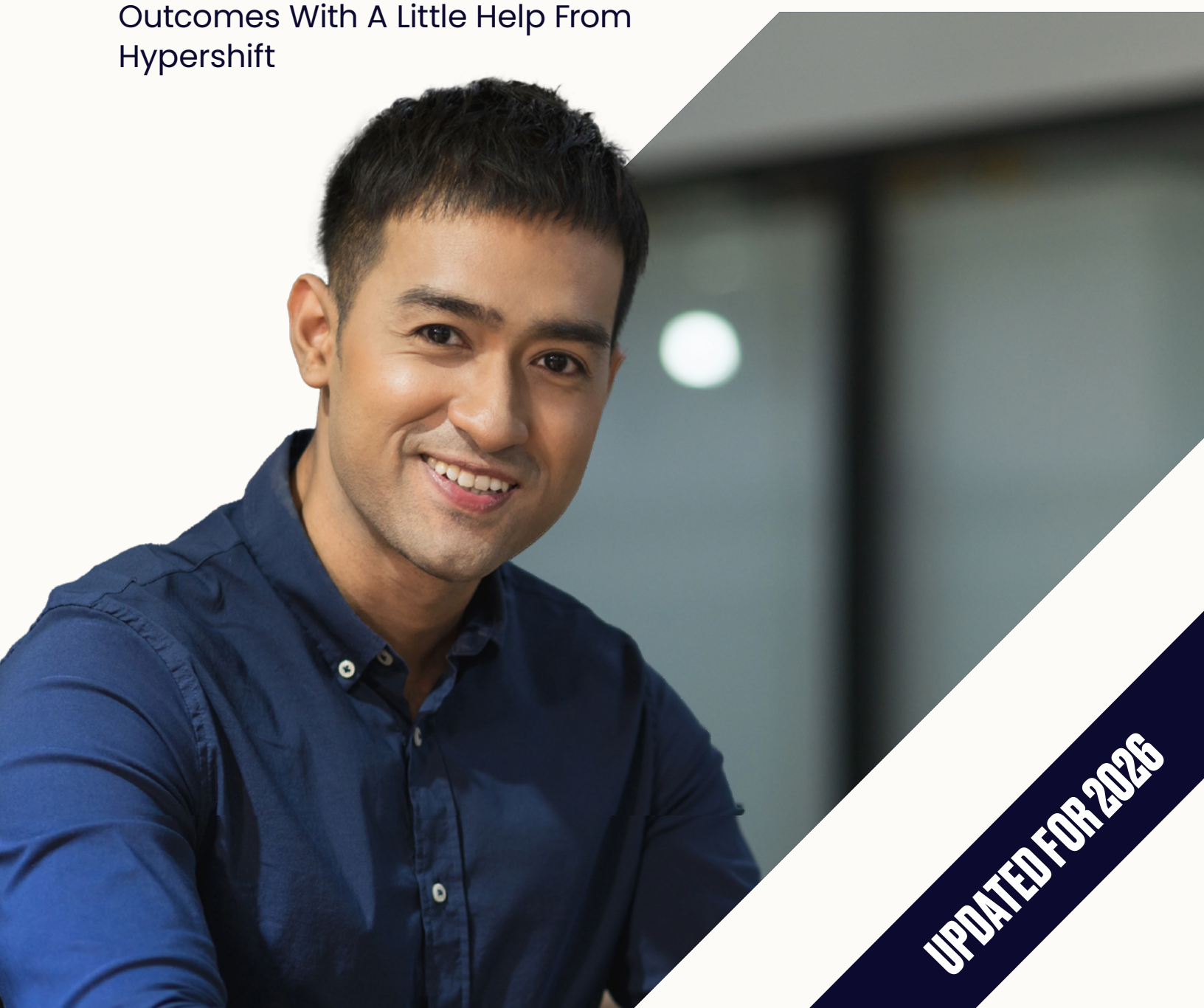
Hypershift

HYPERSHIFT.COM

EBOOK

YOUR COMPLETE GUIDE TO MICROSOFT INTUNE

Guide Your Whole Team To The Best Outcomes With A Little Help From Hypershift



UPDATED FOR 2026

TABLE OF CONTENTS

WHY INTUNE, WHY NOW?

68%
of organizations have experienced one or more endpoint attacks that compromised data and IT infrastructure.

Introduction

The way we work has changed forever.

Employees are no longer tied to office desks or company-issued devices. They're working from home, from airports, on personal smartphones, and across laptops that may or may not be patched.

At the same time, attackers are becoming faster, smarter, and more opportunistic, targeting the gaps created by hybrid work and BYOD policies.

For IT leaders, this has created a perfect storm:

- **Too many devices**: Windows, macOS, iOS, Android, Linux; all connecting from everywhere
- **Too many risks:** Unpatched laptops, unmanaged phones, phishing campaigns, and compliance audits looming
- **Too many tools:** Legacy solutions that don't talk to each other, siloed consoles, and manual processe that drain resources

Microsoft Intune is designed to solve this. As part of Microsoft's broader Endpoint Manager and Zero Trust strategy, Intune brings devices, apps, and security policies under one roof — giving IT teams visibility, control, and automation across the entire environment.

But here's the truth: Intune isn't a magic switch you can flip. Without a clear plan, it's easy to end up with misconfigurations, frustrated users, and compliance gaps. Deploying Intune successfully requires strategy, expertise, and ongoing management.

That's why we created this guide. Inside, you'll find:

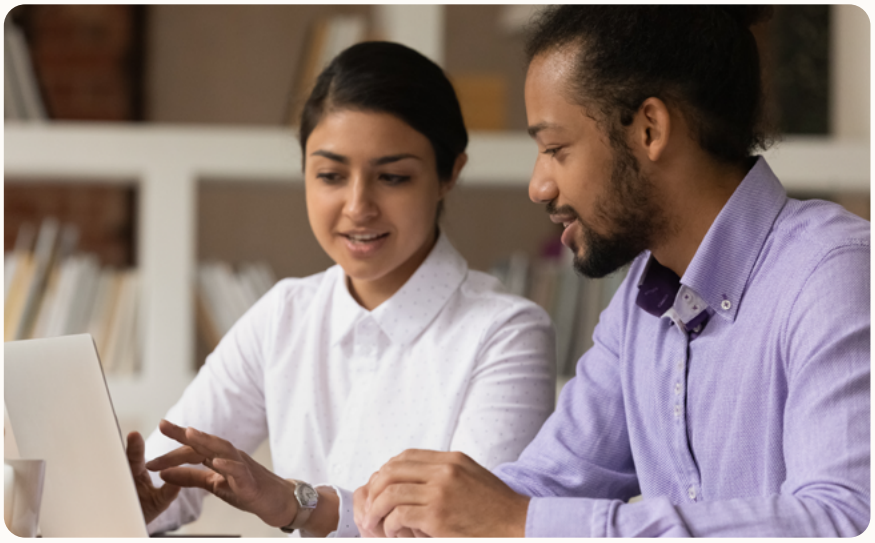
- A breakdown of what Intune does best (and where it struggles)
- The most common deployment challenges and how to avoid them
- Best practices and pitfalls to watch out for
- Where Intune fits in the bigger UEM (Unified Endpoint Management) landscape
- How SCCM, co-management, and hybrid strategies fit into the journey

Moving ahead without a clear success factor often leads to failed deployments.

And most importantly, you'll see how Hypershift helps organizations like yours make Intune work — securely, efficiently, and in a way that scales with your business.

The bottom line: Endpoint management is no longer optional. With the right approach, Microsoft Intune can be the backbone of a secure, compliant, and productive workplace. This ebook will show you how.

WHAT IS MICROSOFT INTUNE & WHY DO WE NEED IT?



The New Reality of Endpoint Management

Hybrid work and BYOD have dissolved the traditional network perimeter. Employees are just as likely to log in from an airport lounge or a personal smartphone as they are from a company-issued laptop in the office.

For IT, this creates chaos: multiple operating systems, inconsistent patch levels, shadow IT, and increasingly sophisticated attackers exploiting every gap.

This is the reality modern organizations face, and also why Microsoft Intune has become such a critical piece of the puzzle.

Why We Need Intune

Microsoft Intune is a cloud-based endpoint management platform that brings order to the chaos.

Instead of juggling disconnected tools, Intune provides a single pane of glass to manage Windows, macOS, iOS, Android, and Linux devices.

The benefits are clear:

- **Visibility across all devices:** IT knows exactly what's connecting, its health, and whether it's compliant.
- **Risk reduction:** Conditional Access policies ensure that risky or compromised devices can't access sensitive data.
- **Operational efficiency:** Automation replaces manual patching and app deployment.
- **Better user experience:** Policies apply at the app level, protecting corporate data without intruding on personal devices.

In short, Intune consolidates endpoint management into one platform, reducing risk while boosting productivity.

How Intune Solves Today's Challenges

Let's look at some of the biggest pain points IT leaders face, and how Intune's built-in tools address them.

1. The Visibility Gap → Web-Based Admin Center

Without a centralized tool, IT teams are left guessing which devices are compliant or even connected. Intune closes this gap with a web-based admin center that provides real-time insight into every managed device, from Windows laptops to Android tablets.

Admins can create policies, push apps, and troubleshoot issues directly from a browser — no VPN or heavy consoles required.

Within the Microsoft Intune suite of tools, you'll find advanced endpoint analytics and a VPN tunnel explicitly designed for mobile apps.

2. Remote Work Chaos → Microsoft Tunnel + Zero Trustr

Remote work introduces new risks: employees log

in from unsecured Wi-Fi, coffee shops, and personal devices. Intune combines Microsoft Tunnel (secure VPN) with Zero Trust enforcement, so every access request is validated by device health, user identity, and compliance.

If an employee's laptop is unpatched or a phone is jailbroken, access is blocked until the issue is resolved. This keeps remote productivity seamless while reducing attack surfaces.

3. BYOD Headaches → Enterprise App Management & Controls

Employees want flexibility, but IT needs to protect sensitive data. Intune solves this by applying Mobile Application Management (MAM) at the app level. For example, corporate data in Outlook and Teams can be encrypted, copy-paste restricted, and routed through VPN — while personal apps like Spotify or photos remain untouched.

This strikes the balance between security and user freedom.

Microsoft Intune works on the zero-trust model, which considers all traffic suspicious by default.

4. Manual Patching & Onboarding → Windows Autopilot + Automated Updates

Manually provisioning devices and deploying patches wastes time and exposes vulnerabilities. Intune's Windows Autopilot allows new devices to ship straight from the manufacturer to employees, preconfigured and secure from first boot.

At the same time, automated OS and app updates ensure devices stay current without constant IT intervention. Together, these tools eliminate onboarding delays and shrink the window of exposure for unpatched devices.

5. Security Blind Spots → Defender for Endpoint Integration

Traditional antivirus tools aren't enough against modern threats. Intune integrates natively with Microsoft Defender for Endpoint, combining endpoint detection and response (EDR) with real-time policy enforcement.

If Defender flags suspicious activity, Intune can automatically quarantine the device, enforce stricter Conditional Access, or trigger admin alerts. This closed-loop protection keeps threats contained before they spread.

The Configuration Manager makes it easier to manage a distributed network by helping with things like patch management and other changes.

6. Overloaded IT Teams → Self-Service Portal + SCCM Integration

Help desk tickets for lost devices, password resets, or sync issues drain IT resources. Intune reduces the load with a self-service portal, empowering employees to wipe or sync their devices themselves.

For organizations still reliant on on-premises tools, SCCM integration (co-management) provides a gradual migration path, allowing workloads like compliance policies to move to the cloud without disrupting existing workflows.

With Defender, users can manage device compliance policies and set up conditional device access policies.

Strengths & Limitations

Pros

- Ideal for cloud-first and hybrid workplaces
- Broad OS support across Windows, macOS, iOS, Android, and Linux
- Strong security and compliance enforcement

Microsoft Intune has the capacity for self-service. This platform includes device reports and device compliance reports, as well as application inventory reports, user reports, and more.

Enterprise App Management allows leaders to set up devices to set rules on a per-app basis.

Cons

- Admin console can feel complex for small IT teams
- Non-Windows platforms sometimes encounter quirks during enrollment
- Requires a solid Azure AD identity infrastructure

What's New in 2025

Intune continues to evolve from a basic MDM tool into a comprehensive endpoint governance platform. Notable updates include:

- **Endpoint Privilege Management with wildcards:** Automates admin rights handling, reducing manual rule creation.
- **Cross-platform security improvements:** Apple screen capture restrictions, Android Bluetooth lockdown, Linux exclusions.
- **Policy Reporting v3:** Real-time deployment insights.
- **Autopilot app enforcement:** Devices must install required apps before accessing resources.
- **Multi-admin approvals:** Adds safeguards for critical actions like device wipe.

Together, these updates show Microsoft's commitment to improving both security depth and administrative efficiency.

How Hypershift Helps

Deploying and managing Intune isn't just about flipping a switch. It requires thoughtful migration planning, policy design, and ongoing monitoring. Hypershift has helped more than 160 financial institutions modernize their Microsoft 365 and endpoint strategies.

In terms of when to use Intune, many agree that this sort of endpoint protection is most effective for enormous networks and organizations with many employees and locations.

We provide:

- Migration planning and execution
- Policy design and enforcement aligned to compliance needs
- Continuous monitoring and health checks
- Tailored managed services that keep your environment secure while freeing IT teams for strategic work

10 INTUNE DEPLOYMENT CHALLENGES & HOW TO SOLVE THEM

Why Deployment Isn't Always Easy

Rolling out Microsoft Intune can feel like trying to change the tires on a moving car. On paper, the benefits are obvious: one platform to manage devices, enforce policies, and secure data.

But when it comes time to actually deploy, reality sets in: devices don't always enroll smoothly, apps misbehave, and your IT team ends up chasing down strange sync errors at 2 a.m.

The good news? These bumps in the road are normal, and they're solvable. Let's break down the 10 most common challenges we see during Intune deployments and, more importantly, how to overcome them without losing your sanity.

Challenge 1: Sync & Connectivity Issues

It always starts innocently: a device refuses to show up in the right group, or a user swears they can't access email even though they're "in Intune." Nine times out of ten, the culprit is a sync timing mismatch between Intune and Azure AD.

💡 *Our tip*: Don't panic. Use user group filtering to avoid those weird mismatches, and run Microsoft's Network Connectivity test to pinpoint where the connection is breaking down.

Challenge 2: Device Enrollment Failures

You've planned your rollout, shipped devices, and… some just won't enroll. Maybe they retire halfway through, maybe apps don't uninstall cleanly.

💡 *Our take*: This is where bulk enrollment profiles and a solid test group save the day. Re-enrollment usually clears up stubborn cases, but if it doesn't, don't be shy about escalating with Microsoft support. (We've all been there.)

Challenge 3: Application Deployment Roadblocks

For the most part, Intune is smooth when deploying apps. But custom, in-house apps? They're the wild-card. If they aren't packaged correctly, you'll hit errors.

Roll out new policies in phases. Start small, verify compliance, and only then scale up.

💡 *Pro move*: Always repackage and pilot test before you unleash apps on the entire organization. The Win32 app packaging tool is your friend here. Think of it as the dress rehearsal before opening night.

Challenge 4: Policy Misconfiguration

Intune policies are powerful — but also unforgiving. If a compliance policy is even slightly off, users can find themselves locked out of resources. Cue the help desk flood.

💡 *Best practice*: Roll out new policies in phases. Start small, verify compliance, and only then scale up. Think of it like flipping switches gradually, not slamming the main breaker.

Use role-based access control (RBAC) to keep teams focused only on what they need.

Challenge 5: Data Security Gaps

One of the worst scenarios: a device fails to set up its container, leaving corporate data sitting unprotected on someone's personal phone.

💡 *Golden rule*: If the container isn't working, wipe and re-enable. Don't try to duct-tape it. And lean on MAM (Mobile Application Management) to enforce protection at the app level, so even personal devices stay safe without invading privacy.

Challenge 6: OS Compatibility

Here's a classic: half your fleet is running the latest OS, the other half is clinging to versions that belong in a museum. Intune won't always play nice with outdated systems.

💡 *Lesson learned*: Do an OS readiness audit before rollout. Publish requirements early and plan for upgrades or replacements. It's easier to have that conversation with leadership up front than explain why enrollment failed later.

Challenge 7: Console Complexity

The Intune console is powerful, but let's be honest: it can feel like navigating an IKEA warehouse. Every new feature adds another menu, and suddenly your admins are lost in the maze.

💡 *Our suggestion*: Use role-based access control (RBAC) to keep teams focused only on what they need. And if it still feels overwhelming, don't hesitate to bring in experts. (Hypershift's team lives in this console daily — we know the shortcuts.)

Challenge 8: AD Integration & Authentication Failures

It's always the little things. Something as simple as a username format can stop authentication cold. If users don't log in as <username>@<domain>, Intune won't recognize them.

💡 *Quick win*: Double-check your Azure AD Connect settings and federation. Sometimes the fix really is that simple.

Challenge 9: MFA & Continuous Authentication Issues

Multi-factor authentication is essential, but it can also frustrate users. SMS codes fail, biometrics misfire, and suddenly productivity takes a hit. Worse, some MFA methods aren't as secure as they should be.

Push toward phishing-resistant MFA methods like FIDO2 keys or Microsoft Authentica-

💡 *Pro tip*: Push toward phishing-resistant MFA methods like FIDO2 keys or Microsoft Authenticator. They're not only safer, but they cut down on support tickets from annoyed users.

Challenge 10: Monitoring & Compliance Fatigue

Here's the hard truth: deployment is just the beginning. Without ongoing monitoring, even the best setup will drift out of compliance. Policies get outdated, devices slip through the cracks, and visibility erodes.

💡 *What works*: Invest in continuous monitoring. Tools like Policy Reporting v3 give real-time feedback, but someone still has to act on it.

Keys to Success

The difference between a painful rollout and a successful one comes down to planning and follow-through.

- Define what success looks like (cost savings, fewer tools, stronger compliance).
- Balance security with user experience so employees don't feel punished.
- Treat deployment as a long-term strategy, not a one-and-done project.

Why It's Worth It

When you push through these challenges, Intune pays off:

- One solution for both MDM and MAM
- Support for both BYOD and corporate-owned devices
- Full separation of personal and corporate data
- Remote wipe, retire, and re-enroll at your fingertips
- Inventory and asset control in one place
- Compliance with frameworks like GDPR, HIPAA, and PCI-DSS

Double-check your Azure AD Connect settings and federation. Sometimes the fix really is that

That's not just IT efficiency, it's organizational resilience.

How Hypershift Can Help

Here's the thing: you don't have to tackle all of this alone. At Hypershift, we've helped hundreds of organizations — from banks to healthcare providers — roll out Intune without the headaches.

We handle the heavy lifting:

- Designing and testing policies
- Integrating Intune with SCCM and Microsoft 365

- Monitoring compliance 24x7
- Offering everything from air cover support to full managed services

So whether you need an extra set of hands during rollout or a long-term partner to keep Intune running smoothly, we've got you covered.

WHERE INTUNE DEPLOYMENTS GO WRONG (AND HOW TO GET THEM RIGHT)

The Trap of "Plug-and-Play" Thinking

Microsoft Intune can be a game-changer, but only if it's deployed with a plan. Too often, teams treat it like flipping a switch: you set up a few policies, enroll some devices, and assume you're done.

Here's the catch: Intune isn't plug-and-play. Skip key steps, and you're not just making IT's life harder, you're exposing the business to risks that are expensive and sometimes invisible until it's too late.

Rolling out Intune without a roadmap is like installing firewalls without rules. Technically, the firewall is there. Practically, you're wide open.

Why Getting It Wrong Is So Costly

We've seen it happen: an org skips Conditional Access during deployment because it feels "too complicated," or a compliance policy never gets enforced because no one tested it. Everything looks fine… until an auditor shows up or a phishing campaign sneaks in.

And the cost isn't just financial, though that's real, with HIPAA or PCI-DSS fines climbing into the six figures.

There's also:

- Operational chaos: unmanaged devices, stalled updates, locked-out employees.
- Lost productivity: users frustrated by misconfigured access rules.
- Reputational damage: a breach or compliance failure doesn't just cost money, it costs trust.

The bottom line: Without proactive planning, Intune can create more work, not less.

The Six Most Common Mistakes

1. Skipping Conditional Access Setup

Conditional Access is the cornerstone of modern security. Without it, even a jailbroken iPhone with stolen credentials could waltz into your apps.

💡 *Pro tip*: If you're nervous about lockouts, start in report-only mode. You'll see what would happen before you enforce it. That way, there's no excuse to leave the doors wide open.

2. Treating Policies as "One-and-Done"

Too many teams create policies during deployment and never revisit them. The business grows, new apps appear, hardware changes — but the policies stay frozen in time.

💡 *Our advice*: Treat policies like patching. Do quarterly audits and adjust for new realities. And document everything. A bloated, outdated policy set is just as dangerous as no policy at all.

3. Firewall Misconfigurations

One of the more frustrating problems: Intune "stops working" — but the issue isn't Intune. It's the firewall quietly blocking traffic after a firmware update.

💡 *What works*: Maintain a living checklist of Intune's required ports and IPs. Share it with your firewall team. And subscribe to Microsoft's service tag updates so you're not caught off guard when endpoints change.

4. Weak or Misconfigured MFA

We still see admin accounts protected by SMS-based MFA. It's better than nothing, but it's also easy to phish. Worse, legacy portals sometimes get overlooked.

💡 *Strong stance*: Use phishing-resistant MFA like Microsoft Authenticator or FIDO2 keys. And don't forget your break-glass accounts — those need the tightest controls of all.

5. Too Many Admin Rights

In the early days of deployment, it's tempting to give broad admin rights "just to get things working." Fast forward a few months, and suddenly half the IT team has Global Admin. That's a recipe for privilege escalation.

💡 *Fix it fast*: Embrace role-based access control (RBAC) and Privileged Identity Management (PIM). Global Admin should be temporary and rare, not the default.

6. Compliance Policies That Don't Actually Work

Imagine: your compliance dashboard says everything's fine, but devices aren't really compliant. Maybe BitLocker didn't enable properly, or a required OS version never enforced.

Before, during, and after the Microsoft Intune deployment, organizations need to create a list of success factors to govern their strategy for MDM/MAM.

💡 *Best practice*: Test with pilot groups before you go wide. Check enforcement logs, and communicate clearly with end users about what "compliance" means. Otherwise, you'll get pushback when their devices suddenly stop working.

Best Practices from the Start

The good news? Every one of these mistakes is avoidable if you take a best-practices-first approach.

1. **Define Conditional Access from Day 1**
   Only allow access from compliant devices. Validate in report-only mode before enforcing.
2. **Schedule Policy Reviews Like Patch Cycles**
   Quarterly audits keep Intune aligned with reality. Document and prune to avoid sprawl.
3. **Maintain an Approved Firewall Rule Set**
   Keep ports, IPs, and services up-to-date. Publish them. Circulate them. Monitor changes.
4. **Enforce MFA with Strong Fallbacks**
   Protect admin accounts with phishing-resistant MFA. Lock down break-glass accounts with extra care.
5. **Use Role-Based Access, Not Blanket Rights**
   Assign permissions by job function. Make Global Admin temporary via JIT elevation.
6. **Compliance Policies with Remediation in Mind**
   Don't just detect issues, configure automatic remediation (like alerts or device isolation) before going nuclear with outright blocks.

Intune is an adaptive security control enabler. This platform helps maintain compliance by hardening devices, enforcing user policies, and protecting sensitive data.

Why Best Practices Pay Off

Following best practices isn't just about reducing help desk tickets (though it does that, too). Done right, Intune enables:

Organizations must staff and budget for proper monitoring, incident response, and remediation.

- Faster productivity — users get the right apps and updates without delay.
- Secure BYOD adoption — protecting company data while keeping personal use flexible.
- Fewer IT fires — less time on troubleshooting, more time on strategic initiatives.

Let Hypershift Be Your Shortcut

All of this takes planning, and planning takes time — time most IT teams don't have. That's where we come in.

At Hypershift, we've guided over 160 organizations through Intune deployments, helping them avoid these pitfalls from the start. Whether you're migrating from another MDM, integrating with SCCM, or tightening compliance, we've seen the roadblocks and know how to steer around them.

Our services cover:

- Deployment strategy and architecture
- Policy and compliance design
- Ongoing monitoring and managed services

Bottom line: we help you roll out Intune the right way, so you don't have to learn these lessons the hard way.

Let Hypershift help you navigate forward with better technology.

EXPLORING INTUNE ALTERNATIVES IN 2025

Intune is at the center of Microsoft's Zero Trust vision, but it's not the only game in town.

The Bigger Picture: Unified Endpoint Management in 2025

The endpoint management landscape is shifting fast. What used to be simple "MDM vs. EMM" decisions is now a complex UEM (Unified Endpoint Management) ecosystem, with vendors racing to deliver:

- Multi-platform security support (Windows, macOS, iOS, Android, Linux)
- Standardized cloud-based identity management
- Smarter VPN and remote provisioning tools
- API integrations that reduce silos between security, identity, and device management

The key takeaway? Organizations aren't just choosing a tool anymore, they're choosing an ecosystem strategy.

And while Intune is at the center of Microsoft's Zero Trust vision, it's not the only game in town.
Let's look at nine leading Intune alternatives (and complements) shaping 2025.

1. Microsoft Endpoint Manager: Consolidation at Scale

Yes, Microsoft itself is evolving Intune by merging it more deeply into Endpoint Manager. This unified approach bridges cloud, on-prem, and hybrid environments, making it easier to enforce policies consistently.

What's new in 2025:

- Blended on-prem + cloud management
- **Zero Trust expansion:** 24/7 device verification, Defender XDR integration
- AI-driven features for autonomous threat detection and policy recommendations

Endpoint Manager uses a unified approach to bridges cloud, on-prem, and hybrid environments, making it easier to enforce policies consistently.

Why it matters: If you're already invested in Microsoft, Endpoint Manager keeps you aligned with its Zero Trust architecture.

2. Apple-Based Endpoint Management: Jamf, Kandji, Addigy

Apple continues to build out its enterprise features through Declarative Device Management and Apple Business Manager. Apple-first platforms like Jamf and Kandji thrive here.

Highlights:

- Automated compliance with self-healing configurations
- Enhanced privacy-preserving management
- Smooth enterprise app distribution with VPP

Best fit: Apple-heavy organizations that want deep, native Apple integration without compromise.

3. Android Enterprise Management: Flexibility First

Android Enterprise has matured into a serious player, with expanded work profiles and zero-touch enrollment.

Highlights:

- Stronger separation of work/personal data
- Broader device manufacturer support
- Google Play Protect integrations for enterprise-grade threat detection

Best fit: Companies with large Android fleets, field devices, or rugged deployments.

Android Enterprise has matured into a serious player, with expanded work profiles and zero-touch enrollment

4. Linux Endpoint Management: Control for Open Systems

Linux adoption in enterprise environments is accelerating, and 2025 sees better tools for managing open systems at scale.

Highlights:

- Container-aware management
- Standardized security baselines across distros
- Automated drift detection and vulnerability management

Best fit: Engineering-heavy organizations and industries running containerized or Linux-first workloads.

Adopting best practices for endpoint and device security reduces downtime, improves flexibility, and delivers measurable cost savings.

5. VMware Workspace ONE: User Experience at the Core

VMware doubles down on its digital workspace vision, emphasizing seamless employee experience.

Highlights:

- Tight integration with virtualization
- AI-driven policy enforcement
- Deeper Carbon Black integration for advanced threat detection

Best fit: Enterprises prioritizing employee experience and hybrid work scenarios.

6. IBM Security MaaS360: AI-Powered Security

IBM leans on Watson AI to deliver risk-based management and autonomous security operations.

Highlights:

- AI-driven risk scoring
- Automated remediation
- Forensic capabilities and advanced analytics

Best fit: Regulated industries that want AI-driven insights baked into endpoint management.

7. Citrix Endpoint Management: Remote Work Veteran

Citrix extends its workspace-first strategy with endpoint management that complements VDI.

Many organizations use Intune + another UEM to cover gaps, particularly in Apple-heavy, Android-heavy, or Linux-first environments.

Highlights:

- Unified policies across devices and virtual desktops
- Advanced user behavior analytics
- Strong remote work enablement

Best fit: Organizations already invested in Citrix digital workspaces.

8. Cisco Meraki Systems Manager: Network-Integrated Security

Cisco leverages its networking dominance to tie endpoint control into infrastructure.

Highlights:

- Network-based threat detection
- Integrated endpoint + network visibility
- Coordinated policy enforcement across endpoints and infrastructure

Best fit: Enterprises that want network-centric security tightly coupled with device management.

9. Ivanti Unified Endpoint Manager: Automation & Self-Healing

Ivanti builds on its acquisitions with Ivanti Neurons: an AI-driven automation platform.

Highlights:

- Extensive automation
- Self-healing endpoint remediation
- Zero Trust principles across devices

Developing a relationship with Hypershift is a solid step in your IT journey.

Best fit: IT teams looking for maximum automation and efficiency.

So... Why Consider Alternatives?

Alternatives aren't about replacing Intune outright — they're about finding the right fit. Many organizations use Intune + another UEM to cover gaps, particularly in Apple-heavy, Android-heavy, or Linux-first environments. Others evaluate platforms based on:

- Multi-platform depth
- Integration with identity/security ecosystems
- Specialized compliance needs

Hypershift's Take

Choosing the right UEM strategy isn't about chasing features. It's about aligning technology to your environment, compliance needs, and workforce reality. That's why Hypershift works across Intune, SCCM, Apple, Android, Linux, and the leading UEMs covered here.

Deployment of Microsoft Intune is one of the most critical projects for any organization.

We've seen what works — and what doesn't — in financial services, healthcare, and other regulated industries. Our job is to help you:

- Assess your UEM options realistically
- Plan a roadmap that balances security, cost, and user experience
- Manage and optimize the platform long after deployment

With Hypershift, you're not choosing a tool in the dark, you're building an endpoint strategy you can trust.
pillar of its success.

INTUNE VS. SCCM: DO YOU REALLY HAVE TO CHOOSE?

More Than A Tools Debate

On the surface, choosing between Microsoft Intune and System Center Configuration Manager (SCCM) looks like a battle of tools. But the reality? It's about something bigger: how your organization manages risk, supports remote workers, and stays compliant. Here's the twist: These days, most organizations aren't choosing one or the other. They're using both.

Intune and SCCM, in Plain English

- **Microsoft Intune:** A cloud-based Mobile Device Management (MDM) and Mobile Application Management (MAM) solution, built for today's laptops, tablets, and smartphones.
- **System Center Configuration Manager (SCCM):** A traditional, on-premises endpoint management platform designed for PCs, servers, and large-scale software deployments.

Both now fall under the Microsoft Endpoint Manager umbrella, but they each shine in different places.

2025 Trends You Can't Ignore

If you're evaluating Intune vs. SCCM in isolation, you might be solving yesterday's problems. Here's what's shaping decisions this year:

- **Co-Management is the New Normal**: Few organizations are "all cloud" or "all on-prem." Co-management lets you run Intune and SCCM side-by-side, shifting workloads gradually without ripping out infrastructure.
- **Cloud PKI is Taking Off**: Intune's new Cloud PKI eliminates the headaches of on-prem Certificate Authorities (CAs). If you need certificate-based Wi-Fi, VPN, or app access, Intune gives you an edge.
- **Zero Trust is Now Table Stakes**: Frameworks like Zero Trust aren't optional anymore — they're baseline. Intune was built for adaptive access, Conditional Access, and device compliance. SCCM wasn't.
- **Automation is the Differentiator**: Intune leans hard into automation: patch orchestration, compliance checks, app assignments, and onboarding flows. SCCM still requires more manual care and feeding.

Organizations specifically serving federal, state, and local government customers, law enforcement, university research centers, and environments susceptible to increasing hacking activities, including healthcare and financial services, may choose to use SCCM on-premise.

Takeaway: These aren't "nice-to-haves." They're neon signs pointing toward a more cloud-centric, policy-driven future.

What Intune Does Best

Intune is purpose-built for today's remote, hybrid, and mobile-first reality.

Strengths:

- Cloud-native, no infrastructure required.
- Works across Windows, macOS, iOS, Android, iPadOS, and Linux.

The fundamental difference between Intune and SCCM is whether you must manage a strictly on-premise work environment or a distributed work environment with BYOD and other related policies.

- Tight integration with Defender for Endpoint and Entra ID (Azure AD)
- Strong automation for policy enforcement, compliance, and conditional access
- Self-service portal reduces help desk tickets

Limitations:

- No server OS support
- Admin console can feel complex
- Licensing isn't always intuitive, and some features sit behind premium SKUs

In a nutshell: If your team is remote, hybrid, or allergic to VPNs, Intune is your go-to. It handles the device zoo with agility, but it struggles with deep legacy workloads.

What SCCM Does Best

SCCM thrives in environments with heavy on-premises needs and high compliance requirements.

Strengths:

- Excellent for patching, software deployment, and OS provisioning at scale
- Mature workflows for complex apps (App-V, Citrix XenApp, Forefront)
- Strong support for servers and deep Windows estates
- Built-in remote access and diagnostics

If you need total control of desktops and servers, SCCM is still king. But it's infrastructure-heavy and less flexible for the modern, mobile work-force.

Limitations:

- Limited non-Windows support
- Requires on-prem infrastructure and ongoing maintenance
- Licensing is complex and often costly

In a nutshell: If you need total control of desktops and servers, SCCM is still king. But it's infrastructure-heavy and less flexible for the modern, mobile workforce.

BYOD and Hybrid Work: Why Many Teams Need Both

Bring-Your-Own-Device (BYOD) and hybrid work are now the norm. That means you're not just managing a fleet of Windows laptops anymore — you're manag-ing personal phones, tablets, and even the occasional Linux box.

Here's the reality:

- MDM (Intune) → Protects the device
- MAM (Intune) → Protects the apps and data
- SCCM → Handles deep patching, OS deployment, and legacy workloads

That's why many organizations go co-managed: Intune for cloud-first devices, SCCM for legacy infra-structure. It's not either/or — it's both.

Endpoint management isn't just an IT project anymore — it's a business-critical capability.

How to Decide: The Practical Guide

Still on the fence? Here's a quick rule of thumb:

Go with Intune if...
You're modern, mobile, cloud-ready, and want to enforce Zero Trust with minimal infrastructure.

Stick with SCCM if...
You're managing servers, legacy desktops, or need tight control in highly regulated environments.

Use both if...
You're like most enterprises: somewhere in the messy middle.

Hypershift's Role: Building the Right Roadmap

The decision isn't just about picking a tool — it's about aligning with your business strategy.

At Hypershift, we've helped hundreds of IT teams:

- Move cloud-first with Intune
- Stay grounded with SCCM where it makes sense
- Blend both through co-management for flexibility

We know the roadblocks, the licensing pitfalls, and the best practices for long-term success.

Conclusion: Your Next Step with Intune

Endpoint management isn't just an IT project anymore — it's a business-critical capability. Whether you're securing a remote workforce, preparing for your next compliance audit, or just trying to simplify device chaos, Microsoft Intune (and the broader UEM landscape) offers the tools to make it happen.

But tools alone don't guarantee success. What matters is how you deploy, configure, and manage them over time. That's where the difference is made between Intune being "another admin console" and Intune becoming a force multiplier for your IT team and a safeguard for your business.

At Hypershift, we've walked this road with hundreds of organizations including finance, nonprofit, legal services, and enterprise IT. We know the pitfalls, the shortcuts, and the best practices that turn Intune from a promising platform into a reliable backbone of your security and productivity strategy.

At Hypershift, we've walked this road with hundreds of organizations including finance, nonprofit, legal services, and enterprise IT.

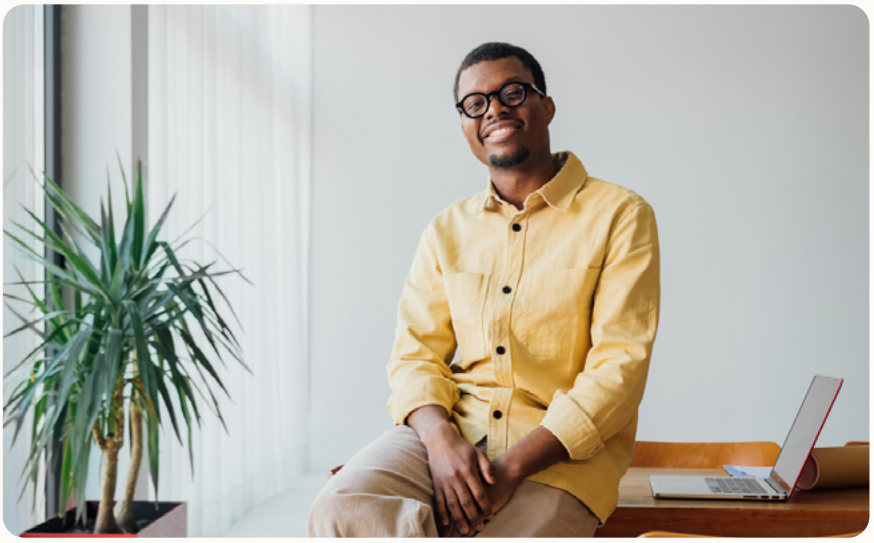
If you take away one thing from this guide, let it be this:

Don't go it alone. The right partner accelerates your rollout, keeps you compliant, and frees your team to focus on what matters most.

Let's build your endpoint management strategy together.

Book a call with Hypershift's Microsoft experts today and start turning Intune into a strategic advantage for your organization.

WHAT'S NEXT?



Thank you for taking the time to enjoy this eBook! Our main goal with this was to stress the importance of Microsoft Intune and SCCM for cybersecurity protection; and, of course, to support your MDM/MAM strategy.

We showed several boutique and enterprise-wide solutions that address securing endpoints, devices, and applications. However, the decision on which solution should become your platform of choice needs to come down to your needs for protecting your data, meeting compliance mandates, and future-proofing against next-generation adversarial AI attacks.

Overall, we hope the contents of this eBook will help your organization successfully protect its most vulnerable attack surfaces: users, devices, and applications.

Hypershift's experience in MDM/MAM and endpoint security shows that choosing the right tools and operations management model to support one's needs can be complex and challenging.

We are here to help, **contact us here.**

ABOUT HYPERSHIFT

Reliable and efficient IT infrastructure is critical to your organization's success. Our IT professionals provide complete consultative service to guide you to your goals.

We're more than just IT consultants; we're your trusted partners. With decades of experience and over 500 companies served, we are passionate about empowering growth. We began by building rock-solid data centers, expanded with storage and disaster recovery, and provided impeccable support to keep IT systems running smoothly.

While we specialize in mid-sized companies, we have partnered with companies of all sizes, including Fortune 100 giants. Our Hypershift managed service division is trusted by over 160 financial institutions. We take pride in being a part of CISA's critical security infrastructure initiative, which helps safeguard organizations.

Being a Cisco Gold Partner means we're recognized for our data center security and networking excellence. We provide SDWAN and Zero Trust Networks expertise to keep your data safe, and we're proud to be

at the forefront of implementing Cisco's advanced security solutions.

Our team is our secret weapon. With 6 CCIE-certified engineers (some who've even earned it multiple times) and over 50 experienced consultants, we have the expertise to handle any size organization. We can confidently manage even the most complex networks with efficiency and precision.

We don't go it alone. With over 70 industry-leading partners, such as Microsoft Intune and Google Cloud, we offer a comprehensive range of solutions and consulting services.

Let Hypershift be a trusted partner in pushing your organization forward with better technology.

Contact us today.