

Optimizing Endpoint Management: How Action1 Complements Microsoft Intune

EXECUTIVE SUMMARY

Microsoft Intune is a powerful cloud-native platform for managing and securing devices—especially within the Microsoft ecosystem. It offers strong capabilities in device provisioning, configuration policies, and mobile device management across Windows, macOS, iOS, and Android. However, many IT administrators find Intune lacking when it comes to real-time visibility, efficient patching, and streamlined operational workflows.

Action1 addresses these gaps with automated OS and third-party patching, real-time vulnerability assessment, and remote management capabilities—all while supporting both Windows and macOS. When used together, Intune and Action1 form a cohesive, cloud-native endpoint management strategy that balances control, automation, and security.

WHY USE BOTH INTUNE AND ACTION1?

Strengths of Microsoft Intune

Intune is well-suited for:

- Device provisioning through Autopilot
- Cloud-based configuration policies
- Mobile device management (MDM) across platforms
- Security baselines and compliance rules
- Application assignments via Microsoft Store or custom packages
- Integration with Microsoft Defender and Azure AD

Yet Intune has notable limitations:

- No automated third-party patching (only manual app packaging or reliance on Microsoft Store)
- Limited real-time visibility into update status and software inventory
- Patch control gaps and complexity in scheduling
- No built-in remote scripting or ad-hoc device actions


WHERE ACTION1 ENHANCES INTUNE

Action1 is an autonomous, cloud-native endpoint management platform that eliminates routine maintenance tasks and strengthens security with features designed for modern, distributed environments.

Key Action1 benefits:

- Autonomous OS and third-party patching
- Peer-to-peer patch distribution to reduce bandwidth use
- Real-time vulnerability assessment without the need for a VPN
- Remote scripting and on-demand actions (restarts, uninstall apps, run diagnostics)
- Live dashboards showing patch compliance, software inventory, and alerts
- Support for remote and hybrid devices, regardless of location

Recommended Use Cases

Use Case	 Microsoft Intune	<i>Action1</i>
Device provisioning	✓ Autopilot	—
Policy enforcement	✓ Configuration profiles	— (Limited)
OS patching	✓ Windows only, basic control	✓ Windows & MacOS, autonomous
Third-party app updates	✗ Manual/Store-based only	✓ Fully automated
Remote software deployment	✓ With manual packaging	✓ One-click or scheduled
Real-time device monitoring	✗ Limited	✓ Comprehensive
Remote scripting	✗ Minimal	✓ Built-in & scriptable
Multi-platform support	✓ Windows, MacOS, iOS, Android	✓ Windows, MacOS
Security & compliance tracking	✓ Azure-based	✓ Built-in dashboards

WHEN TO USE ACTION1 WITH INTUNE

For IT teams already leveraging Microsoft 365 licensing, Intune is a logical choice for identity-driven policy enforcement and cross-platform device enrollment. But Intune was not designed to be a complete patching and monitoring solution—especially for third-party software.

This is where Action1 comes in. It works alongside Intune to:

- Automate patching of operating systems and third-party apps
- Provide real-time insight into device health and vulnerabilities
- Execute remediation tasks remotely, even for off-network devices
- Improve operational efficiency by reducing manual work

By combining Intune's policy management with Action1's automation and monitoring, IT teams gain both strategic control and tactical flexibility.

Need More Help?

For additional resources or tools to streamline your patch management efforts, visit [Action1's website](#).

About Action1

Action1 is an autonomous endpoint management platform that is cloud-native, infinitely scalable, highly secure, and configurable in 5 minutes—it just works and is always free for the first 200 endpoints, with no functional limits. By pioneering autonomous OS and third-party patching - AEM's foundational use case - through peer-to-peer patch distribution and real-time vulnerability assessment without needing a VPN, it eliminates costly, time-consuming routine labor, preempts ransomware and security risks, and protects the digital employee experience. Trusted by thousands of enterprises managing millions of endpoints globally, Action1 is certified for SOC 2 and ISO 27001.

The company is founder-led by industry veterans Alex Vovk and Mike Walters, American entrepreneurs who founded Netwrix, which has grown into a multi-billion-dollar industry-leading cybersecurity company.