# Zero Trust with Microsoft Intune

Summarize this article for me

Microsoft Intune is a mobile device management solution that supports your organization's Zero Trust journey.

Zero Trust isn't a product or service. Instead, it's a modern cybersecurity strategy that assumes no implicit trust - not even within the corporate network. Instead of trusting users, devices, or applications by default, a Zero Trust approach explicitly verifies every access request, continuously assesses risk, and enforces least privilege access across the entire digital estate.

Core principles of Zero Trust include:

Expand table

| Verify explicitly | Use least privilege access | Assume breach |
|---|---|---|
| Always authenticate and authorize based on all available data points. | Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection. | Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses. |

## Device and application authentication, authorization, and protection for Zero Trust

You can use Intune to protect both access and data on organization-owned devices and your user's personal devices that they use for work. Intune use of Microsoft Entra as its identity service helps you enforce device compliance policies that align with your organization's requirements while providing reports that help you monitor and achieve your Zero Trust objectives.

Expand table

| Zero Trust principle | How Intune helps |
|---|---|
| Verify explicitly | Intune supports creation of policies for apps, security settings, device configuration, compliance, Microsoft Entra Conditional Access, and more. These policies become part of the authentication and authorization process of accessing resources. |
| Use least privilege access | Intune simplifies app management with a built-in app experience, including app lifecycle management. You can distribute apps from your private app stores, enable Microsoft 365 apps, deploy Win32 apps, create app protection policies, and manage access to apps and their data.<br><br>Intune's Endpoint Privilege Management (EPM) helps you move your organization's users to run as standard users without administrator rights while enabling those same users to complete tasks and run apps that require elevated privileges.<br><br>Intune policies for Local Administrator Password Solutions (LAPS) for both Windows and macOS can help you secure and manage the local administrator accounts on your managed devices. |
| Assume breach | Intune integrates with mobile threat defense services, including Microsoft Defender for Endpoint and third-party partner services. With these services, you can create policies for endpoint protection that respond to threats, do real-time risk analysis, and automate remediation.<br><br>When you integrate Intune and Defender, you can use evolving tools like the Vulnerability Remediation Agent for Security Copilot. This agent identifies Common Vulnerabilities and Exposures (CVEs) on your managed devices and provides you with step-by-step guidance you can use to remediate them. |

# Next steps

Learn more about Zero Trust and how to build an enterprise-scale strategy and architecture with the Zero Trust Guidance Center.

For device-centric concepts and deployment objectives, see Secure endpoints with Zero Trust.

For Intune in Microsoft 365, see Manage devices with Intune Overview.

Learn more about other Microsoft 365 capabilities that contribute to a strong Zero Trust strategy and architecture with Zero Trust deployment plan with Microsoft 365.

---

Last updated on 08/28/2025