







Endpoint Management with Intune and AADP

Manage and protect your devices, your apps, and your users

Intune highlights

-  Improve your Microsoft Secure Score with Microsoft Endpoint Manager
-  Build management policies that protect your users, company data, and devices
-  Gain insights about your users' endpoints and their compliance with your IT policies
-  Determine the best way to give your users access to the apps they need on the devices of their choosing

MEM/MDM

Get a deep dive into remote deployment, management, and the security of corporate and BYOD devices in your organization. Learn the best ways to configure device settings to meet compliance needs. You can authenticate credentials and manage access while still giving users the freedom to collaborate with others.

- Learn how to improve your management capabilities with Microsoft Intune
- Discover and protect your endpoints by enforcing policies and deploying security tools
- Secure your identities with multi-factor authentication and conditional access from any device
- Enable your users to be productive with the applications they need, on the devices they want and optimize user satisfaction



Experience the power of modern device management within your own environment.

With Microsoft Intune you can leverage device enrollment with intelligent security, risk-based controls, zero-touch provisioning, advanced analytics, and deep integration to the Microsoft products you already use.

Learn how to improve your endpoint and device management capabilities with Microsoft Intune

Discover and protect your endpoints by enforcing policies and deploying security tools.

Secure your users' identities with multi-factor authentication and conditional access from any device.

Enable your users to be productive with the applications they need, on the devices they want.



Endpoint Management with Intune and AADP

AADP highlights



Get a rating of your identity security posture and see how it compares to your peers



Gain insights into apps used in your environment – even ones unsanctioned by IT



Understand how to prevent identities from being compromised



Improve business agility and security with simplified app access

Protect user identities with AADP

Identity is today's control plane for digital transformation. Organizational barriers are blurring between who is in and out of your network. Cloud apps and the increasing use of personal devices and remote work mean that data is no longer centralized behind traditional network security.

With identity attacks on the rise, AAD data and Governance ensures the right people have access to the right resources, and only when they need it.

A single identity control plane grants full visibility and control of your environment: it can help you find identity risks happening now, gain insights on your application landscape, and improve your identity security posture.



Experience the Identity protection within your own environment.

With Azure Active Directory Premium, you can verify user identities with **strong authentication (MFA)**, protect resources with **Conditional Access policies**, detect and respond to compromised accounts, to secure your organization with Zero Trust policies with rich insights.

Optimize identity

Identify potential risks related to identity and see opportunities for improvement.

Assess security posture

Receive a numerical rating of your identity security posture and see how it compares to similar organizations.

Reduce costs

Minimize expenses associated with password reset and helpdesk resources.

Increase visibility

Get a sample survey of apps your employees are using and if IT supports them or not.