



Microsoft Intune

Reduce the attack surface,
simplify endpoint security
management, and lower
costs with streamlined
Microsoft licensing





Challenges of endpoint security

With the shift to the hybrid workplace, the complexity of enterprise digital estates has grown exponentially. The number of devices security teams must secure has exploded—everything from smartphones to IoT devices. And as environments grow, so does tool sprawl. In a recent report, two-thirds of responding security teams reported using over ten tools to manage their digital estates.¹ With the sheer number of other responsibilities that IT teams and CIOs must manage—application modernization, AI readiness and implementation, and cloud migration, all while lowering costs—it is easy to see why tool consolidation has fallen behind in endpoint management.

External threats continue multiplying, with threat actors finding new ways to manipulate generative artificial intelligence (GenAI) to create more sophisticated attacks. Security leaders increasingly leverage Microsoft Intune to counter internal complexity and external threats.





What is Microsoft Intune?

Unified endpoint management (UEM) consolidates the security management of all your organization's endpoint devices, such as laptops, servers, mobile devices, etc., into a single-pane-of-glass control panel. Enterprises use the UEM platform Microsoft Intune to deploy, monitor, and manage how the identities, devices, and applications that make up their digital estate interact. Intune uses the latest technology to secure and manage your devices and data, including, most recently, generative AI through Microsoft Copilot (currently in public preview).

Intune addresses the current challenge of endpoint security by simplifying workflows with consolidation, automation, and integration with other Microsoft and third-party tools.

Key benefits of Intune

- **Single-pane-of-glass controls:** Security team members can securely log into the Intune dashboard from any Internet-connected device, saving valuable time and reducing tool sprawl.
- **Compliance:** Microsoft Intune offers vital security features that help organizations on their journey to zero-trust security, a critical framework in many compliance guidelines and the gold standard of cybersecurity.
- **Streamlined management:** Consolidate device, identity, and application security and management into a single tool.
- **Streamlined endpoint onboarding:** Intune auto-enrollment capabilities enable employee devices to automatically be registered in Intune when devices are signed in, improving efficiency for employee onboarding and device replacement experiences.
- **Cost efficiency:** Save on IT overhead by reducing the overall number of security tools and creating more efficient workflows.
- **Strengthen security posture:** Improve security by reducing attack surfaces and mitigating vulnerabilities through compliance and patching, role-based access and VPN controls, and safeguarding data for BYO devices.
- **AI-powered security features:** Utilize Microsoft Copilot to streamline troubleshooting with natural language processing (NLP) prompts and automate remediation efforts.

Innovative features of Intune

- **Remote Help:** This secure, cloud-based solution connects help desk support to end users, making it crucial for IT teams, especially with more workers operating remotely or in the field. It allows support teams to remotely troubleshoot desktop and mobile devices using the user's secure enterprise identity.
- **Endpoint Privilege Management:** This feature ensures that the appropriate users have the proper privileges at the right time, minimizing security risks and easing the burden on help desks for routine tasks, such as setting up local printers.
- **Tunnel for mobile application management:** Microsoft Tunnel allows employees to securely access company resources using their mobile devices. It is a lightweight VPN solution that provides seamless access to corporate resources from personal devices without needing enrollment.
- **Advanced application management:** This solution offers controls for easy app discovery, deployment, updates, and vulnerability patching.
- **Specialty device management:** A comprehensive suite of device management, configuration, and protection tools tailored for specialized, purpose-built devices like AR/VR headsets, large smart screen devices, and conference room meeting equipment.
- **Cloud certificate management:** A cloud-based solution for managing certificates effectively to ensure secure authentication and streamline Wi-Fi scenarios.
- **Advanced analytics:** Intune includes advanced endpoint analytics that deliver insights to help IT administrators enhance user experience across the organization by addressing risks from outdated apps.
- **Emerging AI features:** Copilot in Microsoft Intune is currently in preview. It facilitates identifying and responding to vulnerabilities while saving time with AI-generated security insights and data-driven troubleshooting, simplifying endpoint management. Intune leverages the capabilities of Copilot for Security, providing summaries of existing policies and detailed information on setting them up, including recommendations and potential conflicts. It also offers device details and troubleshooting assistance.

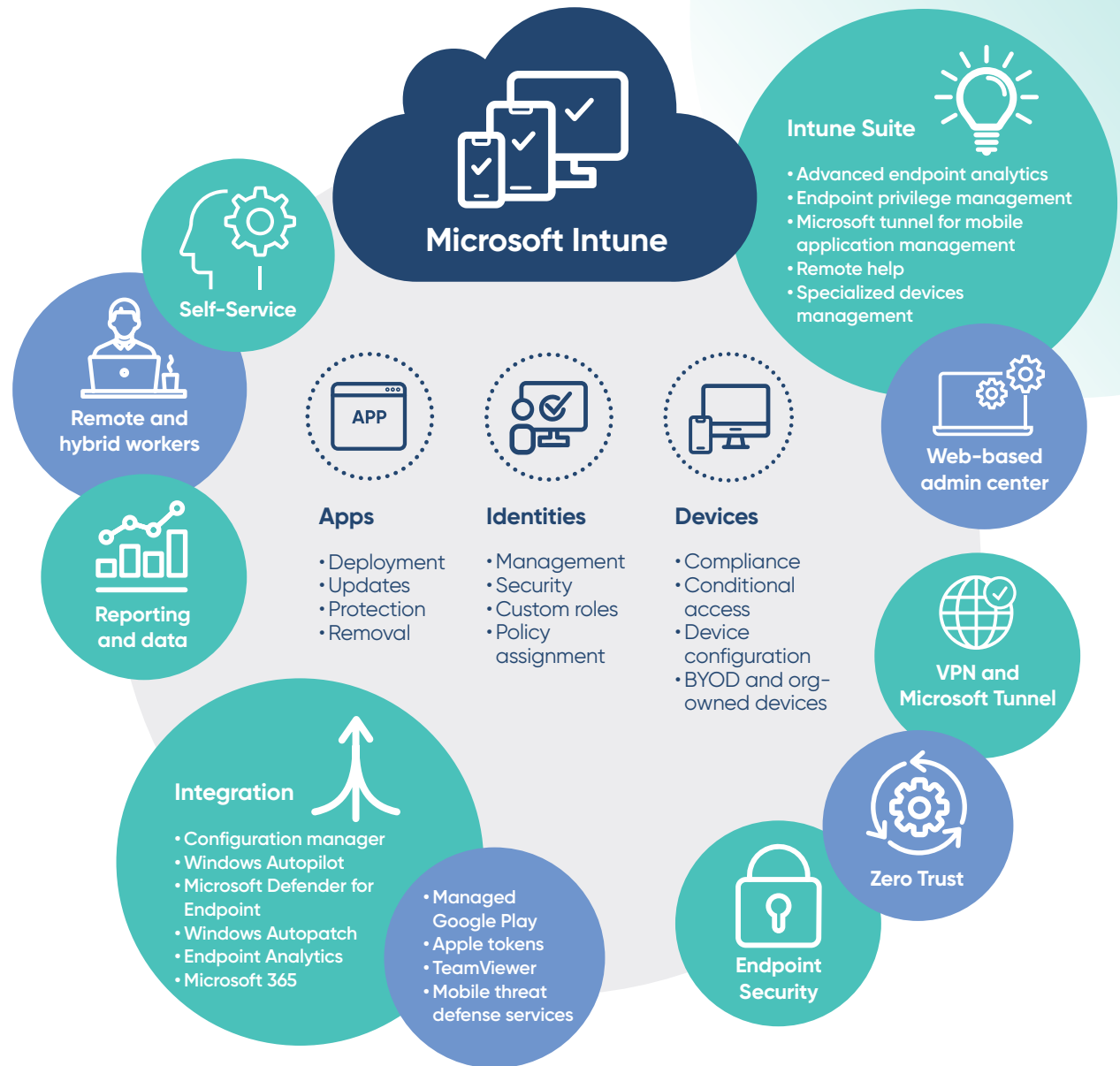


How Intune works

The Intune admin center is a game-changer for endpoint management, especially with its focus on data-driven reporting. As an administrator, you can quickly sign in from any device with Internet access.

With Intune, you can control what content employees can access, strengthening your organization's cybersecurity. The ability to remotely deploy applications and updates means vital tools like Microsoft Teams and Outlook can be synced effortlessly across devices. Plus, you can ensure compliance by automatically flagging devices that do not meet security requirements. For personal devices, there are flexible options—users can enroll for full access or just utilize selected apps like Outlook, all while keeping your organization's data secure. This balance between security and user autonomy is essential in today's hybrid work landscape.

Intune is priced monthly based on the number of users. It is included in many standard Microsoft licenses or can be purchased as a standalone plan. Working with an experienced integration partner like CBTS, you can leverage our experience and relationship with Microsoft to ensure you get the best price as part of an efficient bundle.






Challenges of implementing Intune

Intune integrates fully with the Microsoft Suite, which is likely a good fit if your organization already uses Microsoft products. Intune works with non-Microsoft environments such as Apple and Linux but may not function at the same level.

When using Microsoft Intune, it is crucial to have a comprehensive approach to implementation and ongoing management. Regular updates are necessary to ensure the system remains secure and efficient. Establishing clear enrollment strategies helps streamline the device onboarding process. Segmenting policies effectively to address different user needs and scenarios is also essential. Providing adequate training for users and administrators will enhance overall effectiveness and maximize the benefits of Intune in your organization.



How CBTS helps your organization get the most out of Intune

CBTS offers comprehensive support for managing your Intune deployment and processes, ensuring a smooth integration into your organization. Our services include:

- Intune assessments, remediation, and deployments: CBTS can assist with assessing customer environments to prepare for Intune adoption as well as guiding customers through a full Intune deployment. CBTS can also assess and remediate issues occurring in existing Intune environments.
- Endpoint management policies: Our team assists in activating and maintaining configuration policies, compliance policies, security policies, auto-enrollment policies and more as well as enrolling devices into the Intune ecosystem.
- Application management: CBTS can help with deployment, management, and support of Microsoft 365 applications, iOS applications, Android application and also some Line of Business and Win32 applications.

- Policy development, segmentation, and implementation: We can help you formulate tailored policies that fit your organization's needs. This includes segmenting devices and users based on roles and requirements and effectively implementing those policies to ensure compliance and governance efficiency.
- IT admin support and troubleshooting: Our team is here to help when Intune policy adjustments are needed, remote locking/wiping of endpoints, device and application update issues, application version rollback and more. We can also escalate tickets to Microsoft for support if needed.
- Recurring environment reviews: Quarterly or monthly reviews to stay up to date on your current Intune endpoint and application landscape, review the status of support tickets, and plan for your roadmap.

Did you know that most Intune capabilities come included with common Microsoft 365 licensing subscriptions?

Our team can help you understand what's included and maximize the value of your licensing. This strategic approach simplifies your licensing and can lead to significant savings, allowing you to allocate resources to other critical areas of your business.

With CBTS as your Microsoft Intune partner, you gain access to a wealth of expertise and support, empowering your organization to utilize your Microsoft investments fully.



**Intune is a leader in
The Forrester Wave™:**

*Unified Endpoint
Management,
Q4 2023.²*

**Intune is a leader in IDC
MarketScape: Worldwide**

*Unified Endpoint
Management Software
2024 Vendor Assessment.³*

Why Microsoft?

Microsoft has established itself as a leader in cybersecurity and endpoint management, providing comprehensive solutions that address the evolving security needs of organizations. Their cybersecurity offerings are designed to protect against a wide range of threats, ensuring data integrity, confidentiality, and availability across various platforms and environments.

One key component of Microsoft's cybersecurity strategy is the integration of advanced threat protection technologies, such as artificial intelligence and machine learning, which help detect and respond to potential threats in real time. This proactive approach to security enables organizations to stay ahead of cybercriminals and mitigate risks effectively.

Microsoft emphasizes the importance of a layered security approach, combining various technologies and practices. This methodology includes identity and access management, encryption, and regular security assessments to identify vulnerabilities. With a focus on zero-trust architecture, Microsoft encourages organizations to verify every request as if it originated from an open network, further strengthening their defenses. This holistic approach positions Microsoft at the forefront of cybersecurity, providing organizations with the tools and support to navigate an increasingly complex digital world.

Why CBTS?

CBTS has a longstanding partnership with Microsoft, reflecting our deep commitment and expertise in the Microsoft ecosystem. With numerous Microsoft certifications under our belt, we have successfully assisted hundreds of organizations in maximizing their utilization of Microsoft technologies for many years.

Leverage the benefits of CBTS managed security services to enhance your organization's cybersecurity posture. With 24x7 monitoring and threat detection capabilities, you can free up your technical staff to focus on strategic IT initiatives while accessing specialized skills from top cybersecurity professionals. This approach will not only help you uncover and address concealed risks, but it will also assist in meeting your compliance obligations and reduce your overall ownership costs.

Do not compromise on safety. Team up with our specialists to safeguard your assets and maintain a secure environment with the latest endpoint security tools from Microsoft.

Contact us to get started.

660+

Microsoft
certifications across
portfolio solutions

188+

Professionals certified
by Microsoft

Sources

1. Managing the Endpoint Vulnerability Gap | Enterprise Strategy Group, TechTarget
2. Forrester names Microsoft Intune a Leader in the 2023 Forrester Wave™ for Unified Endpoint Management | Microsoft
3. IDC MarketScape: Worldwide Unified Endpoint Management Software 2024 Vendor Assessment | IDC

 **Microsoft**
Solutions Partner

Security

Specialist
Cloud Security
Identity and Access
Management



From developing and deploying modern apps and the secure, scalable platforms on which they run, to managing, monitoring, and optimizing their operations, CBTS is the trusted partner businesses need to thrive in the application era.