ramsac
the secure choice

Understanding Microsoft Intune:

Managing security for a mobile/hybrid workforce

Understanding Microsoft Intune:

Managing security for a mobile/ hybrid workforce

The move to the cloud has made IT so much simpler in so many respects. But with more and more organisations relying on platforms such as SharePoint and Microsoft 365 to provide workers with access to emails, files and data, together with more mobile, hybrid and remote workforces, security has never been more important.

It's more important than ever to ensure that sufficient security and access management controls are in place to ensure that your IT function retains control over who can access what, how access can be locked down, and access rescinded, should a device be lost or stolen, or should a member of the team leave.

Microsoft Intune provides your company with the tools needed to manage security and mitigate cybersecurity risks. This whitepaper covers all you need to know about Intune, and how it can benefit your business.

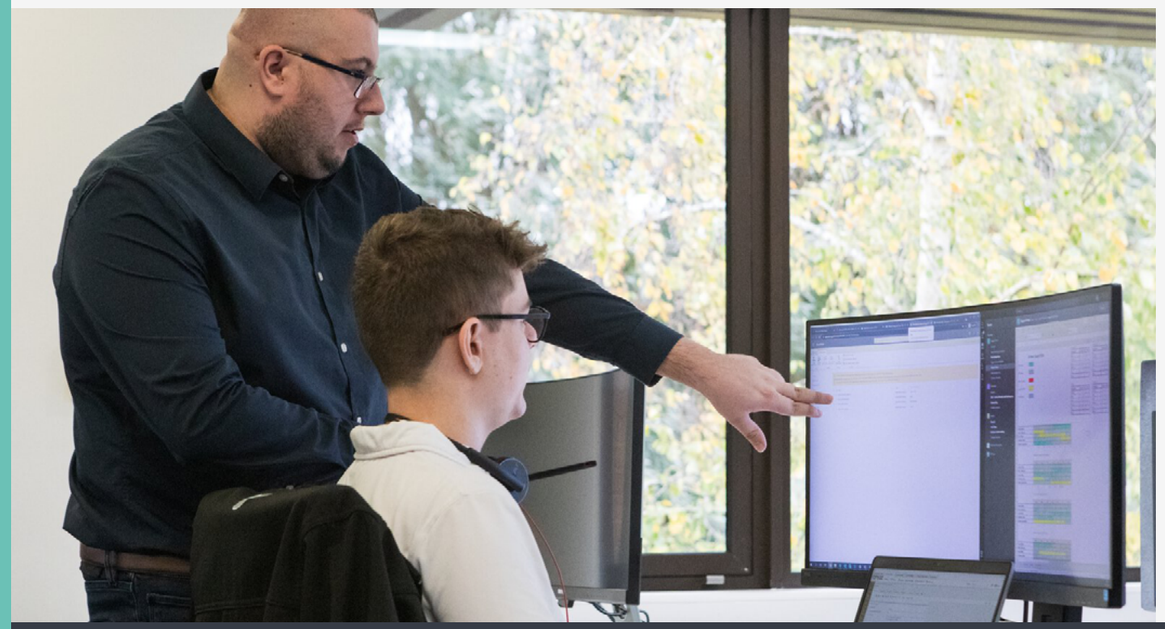
What's inside?

Introducing Microsoft Intune

Microsoft Intune is a cloud-based mobile device management (MDM) and mobile application management (MAM) service from Microsoft that allows organisations to manage and secure mobile devices, PCs, and apps used by employees. Mobile devices are laptops, tablets and phones, or other devices, that aren't left at a fixed address, like a traditional PC would be.

Microsoft Intune was created to address the demand that a hybrid workforce brings. With people working in a variety of locations and in and out of the office, being able to ensure cybersecurity demands are met and all your company devices are protected is essential.

Intune provides a range of features such as device management, app management, and security management, which can be used to protect corporate data and manage the use of mobile devices within an organisation. It also enables your IT team to manage and protect corporate data accessed by personal devices that the organisation doesn't own, such as smartphones and tablets.



Intune works with other Microsoft services such as Azure Active Directory and Microsoft Endpoint Manager, and it can be used to manage devices running various operating systems including Windows, iOS, and Android.

- ✓ **Mobile device management:** Intune allows you to manage mobile devices such as smartphones and tablets that run on various operating systems such as Android, iOS, and Windows. This is all controlled through a central web dashboard.
- ✓ **Mobile application management:** Intune provides the ability to manage and secure mobile applications, including company-owned and bring-your-own-device (BYOD) apps, on various mobile platforms. You can also roll out app updates, manage protection policies and access remotely.
- ✓ **Conditional access:** This service helps to secure access to company data and resources by enforcing policies that require users to comply with security guidelines, such as device compliance and identity verification. These can be created and then rolled out as needed, and different policies can apply to different groups of users.
- ✓ **Mobile threat defence:** When using Microsoft Defender for Endpoint, Intune can detect and remediate security threats as well as address real-time risks on mobile devices using machine learning and artificial intelligence.
- ✓ **Data loss prevention:** Intune offers a range of data protection services, including app protection policies, data loss prevention (DLP), and remote wipe, to help safeguard your organisation's data on mobile devices.
- ✓ **Reporting and monitoring:** Intune provides reports and insights on mobile device and application usage, compliance status, and security issues.
- ✓ **User empowerment:** With Intune, users get more responsibility for requesting password resets, installing apps and joining groups, as well as providing better support options and reducing support calls.

What is mobile device management? (MDM)

Mobile device management (MDM) is a type of security software that enables organisations to manage and secure mobile devices such as smartphones, tablets, and laptops, from a central location.

The goal of MDM is to ensure the security of corporate data and applications on these devices while still allowing employees to use their own personal devices or company-issued devices to access work-related data and services.

MDM allows IT administrators to remotely manage and monitor devices, enforce security policies, and push software updates to devices. This helps to ensure that devices are up to date with the latest security patches and that employees are following company policies, such as password requirements and device encryption.

In addition to security, MDM can also help organisations to improve productivity by providing employees with access to company resources and apps from their mobile devices. This can enable truly productive remote work and improve collaboration among team members.

Overall, MDM plays a crucial role in enabling organisations to protect their sensitive data and maintain control over their mobile devices, while still allowing employees to use their devices to work from anywhere, at any time.

What is mobile application management? (MAM)

Microsoft Intune helps organisations manage and secure the applications that employees use on their mobile devices through mobile application management (MAM). The goal of MAM is to protect corporate data and applications by enforcing policies that control how apps are used and accessed on mobile devices.

Mobile app management as part of Intune involves the following activities:

- **App deployment:** MAM solutions allow administrators to deploy apps to mobile devices in a controlled manner. This means that you can ensure that employees have access to the right apps, while also controlling who can download or access those apps.
- **App configuration:** Configure the apps on employee devices to comply with company policies. For example, you can configure apps to require a password or use encryption to protect data.
- **App management:** Allow administrators to monitor and manage the apps on employee devices. This includes monitoring usage and activity, enforcing security policies, and remotely wiping data from apps or devices.
- **App updates:** Ensure that apps on employee devices are up-to-date and secure by automatically pushing updates and patches to the apps.

Overall, MAM enables organisations to secure and control the apps that employees use on their mobile devices, while still allowing them to work efficiently and productively. MAM is particularly important for organisations that allow employees to use their own personal devices for work, as it helps to ensure that sensitive corporate data is protected even when accessed from personal devices.

What is conditional access?

Conditional access is a security feature that allows organisations to control access to their cloud-based resources based on specific conditions or policies. Conditional access can be used to ensure that only authorised users can access sensitive data or applications and that they are doing so from secure devices and locations.

With conditional access, an organisation can set up policies that determine who can access certain resources and under what conditions. These policies can be based on various factors, including:

- **User identity:** The user's identity can be verified through credentials like a password, multi-factor authentication, or biometric authentication.
- **Device health:** The device's health and compliance can be checked to ensure that it meets the organisation's security standards.
- **Network location:** The user's location and the network they are accessing the resources from can be evaluated to ensure that they are accessing the resources from a trusted and secure network.
- **App used:** The application that the user is using to access the resource can be evaluated to ensure that only trusted and approved apps are being used.

Conditional access helps organisations to protect their resources and data by ensuring that users can only access them under the appropriate conditions. This helps to prevent unauthorised access to sensitive information, even if user credentials are compromised. Additionally, conditional access helps organisations enforce compliance and regulatory standards by controlling access to data based on specific policies.

What is mobile threat defence? (MTD)

Mobile threat defence (MTD) is a type of security solution that helps protect devices, applications, and data from various types of security threats such as malware, phishing, and network attacks. MTD is part of a wider range of tools, and works when combined with a service like secure+, which allows humans to act on the threats raised by Intune.

MTD uses advanced analytics and machine learning algorithms to identify and mitigate security threats in real time.

Some of the key features of MTD include:

- **Threat detection:** Detect and block mobile security threats, including malware, phishing attacks, network attacks, and other types of mobile-specific threats.
- **Mobile app security:** Protect mobile apps, including app vetting and analysis to ensure that only trusted and secure apps are installed on mobile devices.
- **Device security:** Monitor device-level security to detect any potential vulnerabilities or suspicious behaviour that may indicate a security threat.
- **Data protection:** Protect data on mobile devices, including encryption and data loss prevention (DLP) capabilities.
- **Compliance monitoring:** Comply with regulations such as GDPR, HIPAA, and other privacy regulations.

MTD solutions are important for organisations that rely on mobile devices for work, especially with the increasing prevalence of BYOD (bring your own device) policies. This helps to ensure that mobile devices are secure, protecting against potential security threats that can put sensitive data and company resources at risk.

What is data loss prevention? (DLP)

Data loss prevention (DLP) is a type of security solution that helps organisations prevent sensitive data from being lost, stolen, or mishandled. DLP solutions monitor and control the flow of data within an organisation, ensuring that sensitive data is not being transmitted or stored inappropriately.

DLP solutions can help organisations identify sensitive data and determine how it should be handled. For example, an organisation may define certain types of data as “confidential” and require that it be encrypted before it is transmitted or stored.

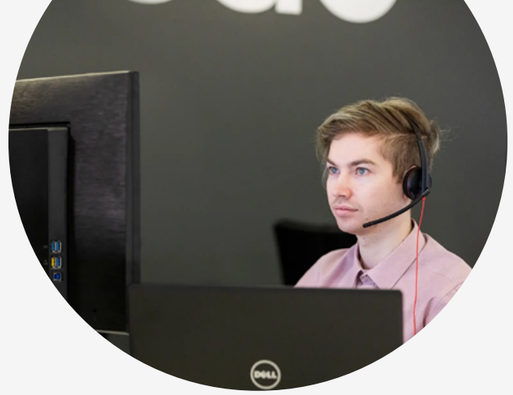
DLP solutions can also monitor user behaviour to detect potential data breaches or violations of data handling policies.

Some of the key features of DLP solutions include:

- **Data Classification:** DLP solutions can automatically classify data based on its sensitivity, enabling administrators to apply appropriate security policies.
- **Data Monitoring:** DLP solutions monitor data flow within an organisation, detecting potential breaches or policy violations.
- **Policy Enforcement:** DLP solutions can automatically enforce policies related to data handling, such as encrypting data or preventing data from being transmitted outside of the organization.
- **Incident Response:** DLP solutions can provide alerts and other notifications when potential data breaches or policy violations are detected, enabling administrators to respond quickly.

Overall, DLP solutions are important for organisations that handle sensitive data, such as financial data, healthcare information, or intellectual property. DLP solutions help to prevent data breaches, protect sensitive data, and ensure compliance with regulatory requirements.

Microsoft Autopilot



Another feature of Intune, Microsoft Autopilot is a cloud-based deployment and management service that helps organisations set up and configure new Windows devices quickly and easily. Autopilot simplifies the device deployment process by automating many of the tasks traditionally involved in the device provisioning process.

With Autopilot, organisations can pre-configure devices with settings, policies, and applications before they are shipped to end-users, simplifying the device setup process. Autopilot also enables users to set up their own devices, reducing the burden on IT administrators and allowing end-users to get up and running quickly.

Some of the key features of Microsoft Autopilot include:

- **Device registration:** Autopilot enables organisations to register devices with Microsoft Intune, allowing administrators to manage them using cloud-based management tools.
- **Configuration profiles:** Autopilot allows administrators to create configuration profiles that can be applied to devices during the setup process. These profiles can include settings such as language, time zone, Wi-Fi settings, and custom applications.
- **Self-service device setup:** Autopilot enables end-users to set up their own devices, reducing the burden on IT administrators and allowing users to get up and running quickly.
- **Simplified deployment:** Autopilot simplifies the device deployment process by automating many of the tasks traditionally involved in the device provisioning process.

Overall, Microsoft Autopilot is a powerful tool for organisations looking to streamline their device deployment and management processes. By simplifying the device setup process and automating many of the tasks involved in device provisioning, Autopilot can help organizations save time and improve productivity.

In summary – the benefits of Microsoft Intune

Microsoft Intune not only gives organisations greater power and control over their devices and data, but also enables employees and users to have access without needing to request information from support teams.

By utilising Intune, it also means that companies are better protected from threats and can respond faster to incidents.

However, the main benefit to companies is the ability to manage devices from one central dashboard. As so much of a company's IT estate is connected to one cloud provider, Microsoft, being able to have a level of control over each aspect, keeps the company safe, adheres to best practices, and ensures any compliance with the relevant legislation is kept.

Intune: the answer to hybrid workplaces' cybersecurity problem

Microsoft Intune is an incredibly powerful piece of software, and one that has many benefits for not only IT administrators but also for every user of IT. By streamlining and automating many aspects of device management, app security and onboarding, companies can overcome the hybrid workplace's cybersecurity problem.

At ramsac, we work with our customers to provide them with an Intune set-up that creates a safer, more secure environment, while encouraging your staff to work in the best way for them.

We're here to set up Intune correctly with a consultation period that enables us to discover your needs and requirements. We'll also work with your staff to ensure any existing security risks are reduced, as well as providing wider education.

Interested? Get in touch today.

Find out more

For more information please get in touch:

Call: 01483 412 040

Email: info@ramsac.com

Visit: ramsac.com

ramsac Limited
Compton House
The Guildway Campus
Old Portsmouth Road
Guildford, GU3 1LR

ramsac.com
01483 412 040

ramsac
the secure choice