The Microsoft 365 security journey

The five essential steps to securing your data

ramsac
the secure choice

The working world has changed

Covid advanced our working practices and digital transformation quicker than any other event in living memory.

The way we work is entirely different to the way we worked 5 years ago. Our teams demand flexible working and with the current rates of inflation, our work force is more expensive than ever before, so leaders need to ensure that they are working with the best, and that every working hour is productive.

Equally, cyber threats are growing at an increasing rate, as are the legal and ethical obligations on us to protect sensitive data. There isn't a single day that passes without our support team receiving a call to say that someone has clicked on an unsafe link, or shared data unwittingly with someone who may use it maliciously.

And these days of course, our data doesn't sit neatly behind a firewall in our office, because our office is now no longer where our data is stored, and in many cases, it's no longer the only place our teams do their work. Our staff demand fast, always available flexible IT solutions that allow them the same access and interaction regardless of the device they are using or where they are working from.

- Our workforce wants to work flexibly, from multiple locations.
- Our customers and stakeholders demand that we are keeping their data safe.
- Our Finance Directors want to drive down spend and avoid the risk of expensive data losses.
- A data breach often leads to fines, financial losses and damage to an organisations reputation.

This is a reality for almost every organisation we work with.

ramsac
the secure choice

Understanding the tools already at your fingertips

Microsoft are not in the business of making licensing easy to understand! However, recent changes to the way you buy 365 have actually resulted in a very comprehensive bundle, that, if configured and utilised correctly, allow you to create arguably the most secure, flexible IT estate you are likely to need. The applications included in Microsoft 365 Business Premium, give you an impressive array of tools to lock down and control your data, it can just be tricky to understand exactly what's available to you, and what it all means.

Microsoft 365 offers a vast array of useful tools, from the traditional Word and PowerPoint, to cloud storage apps such as OneDrive and SharePoint, as well as productivity and communication tools like Planner, ToDo, Project and Teams. All of these apps can be accessed simultaneously from a PC, laptop, smartphone and tablet. That leaves you with countless places per user to secure your data. And remember, this is no longer hidden behind a neat firewall, this is on the train, at home or in Starbucks! Add to that, the fact that you probably don't have the IT budget to give people a company owned and controlled ipad and mobile device ontop of their PC or laptop, so your users are probably using personal tech along side their work issued laptop.

So, how do we keep all of that safe, how do we control who can access what, and how do we revoke access when a user leaves, or loses a personal or work owned device?

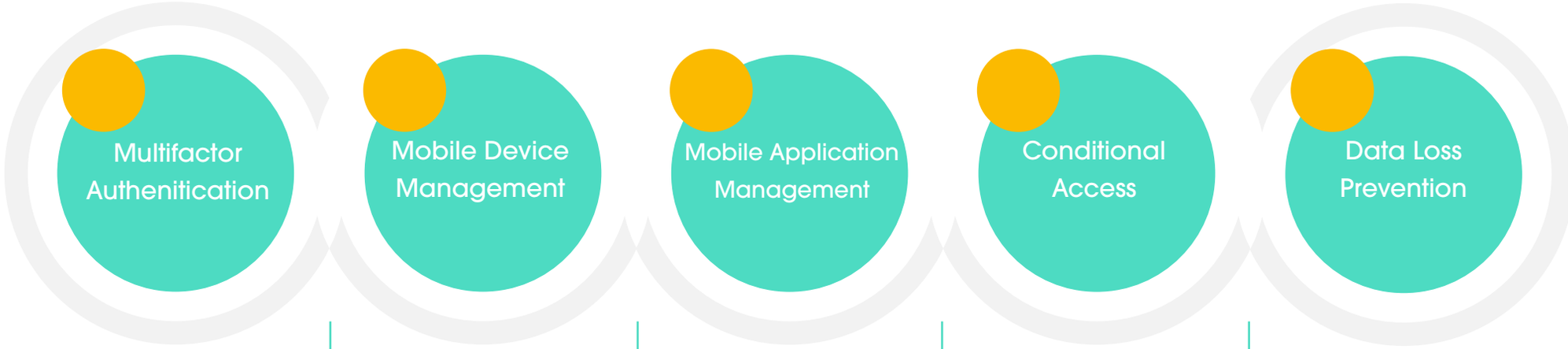
This is where the Microsoft Security Suite, especially a product called Microsoft Intune, comes in to play. Intune is effectively a suite of tools that allow us to address the various security challenges that mobile workforces face. In this report we will cover the five key tools that every organisation should be deploying to take you on a journey from least secure, to most secure.

Microsoft Intune

ramsac
the secure choice

Microsoft 365 security journey - Overview

Least secure ..... Most secure



Multi-factor authentication (MFA) verifies the identity of users by requiring them to provide two or more pieces of evidence, such as a password, a code sent to their phone, or a biometric scan.

Mobile device management (MDM) is the tool that allows you to authorise and enrol the mobile devices that access your data.

Mobile application management (MAM) secures defined applications that you can approve to access your corporate data.

Conditional Access controls allow administrators to apply a set of rules that determine what a user can access and from where.

Data loss prevention (DLP) turns on the ability to classify a document or set of documents, with a certain sensitivity tag, and then controls what a user can do with that document.

ramsac
the secure choice

Multifactor Authenitication

The first step, which most organisations should have already implemented, is Multi Factor Authentication, or MFA.

At ramsac we strongly advise all our clients to enforce MFA across their entire estate, this really just isn't optional. Now organisations are not working behind firewalls or setting up VPNs, their entire 365 data can be accessed with an email address and a password. And those two things are really easy to obtain. Anyone can buy thousands of passwords on the dark web for just a few pounds. It's what phishing attempts are all about, luring users to type in their email address and password, because if a cyber criminals steals that, without MFA they are unstoppable.

MFA however, means as well as a user name and password, the cyber criminal also need to steal a physical device, probably your mobile phone, and if the Intune policies are set up right, that phone is also protected by biometrics (such as Face ID) or a password. That stolen password is now fairly useless to the cybercriminal, because without the ability to also access and unlock your device, the access remains firmly locked.

It's worth mentioning that increasingly we're seeing that cyber insurance policies will not pay out if MFA hasn't been fully deployed across all users, so it's a big thing to check and have properly configured.

ramsac
the secure choice

ramsac
the secure choice

Mobile Device Management

The next stage in the 365 security journey, is setting up mobile device management.

Mobile Device management (MDM) is the tool that allows you to authorise and enrol the mobile devices that access your data. Mobile doesn't just mean phones, a laptop or tablet is very much a mobile device.

Mobile Device Management allows us to create a trusted relationship between a device and your IT estate. It means that the system is expecting data to be accessed from that specified device, which creates the first level of trust. But furthermore, MDM allows us to then manage and enforce security settings before access is granted each time, that could include policies around whether that device has to have the latest operating system, whether it has to be using Face ID or biometrics for security, if it has to be encrypted and if your chosen Anti-Virus is installed, for example.

It also allows us to determine what happens if that device is lost, stolen or is no longer in use, allowing us to effectively wipe any stored data and prevent further access. We can even then see if that blocked device later tries to access the system, which can indicate an attempted cyber attack.

Mobile Application Management

As we've already discussed, not all access happens on devices you issue. Staff want to be able to make use of personal devices such as their own phone for example, and there are lots of cost benefits to you in enabling that, for a start, you don't have to issue work phones to all users!

However, if staff are using their own devices, that raises different problems. For example, if they leave the organisation, you want to be able to wipe your data, but you have no right to wipe their personal phone, potentially wiping out their files, contacts, social channels and photos for example.

That's where Mobile Application Management comes in. Mobile Application Management, or MAM for short, allows us to sandbox data that's yours and keep it separate from personal data. With MDM we are securing the whole device. With MAM, we're securing defined applications that we then approve to access our corporate data.

A good example of this is Outlook data. In an unmanaged set up, a user can simply enter their Exchange details into their device and synch their email, calendar and contacts with Microsoft Exchange using the default calendar and mail applications. The IT team have no way of controlling this. With a MAM policy in place, the user can only access this data using the Microsoft Outlook app on their personal device. Then the IT department can say that in order to access email, The user needs to have biometrics or a PIN code set up on that specific application, and if they leave, or lose their phone, IT can wipe just that company data.

It means you can provide people with the flexibility to work on the device of their choosing, avoid the cost of issuing and running company owned mobile devices, but still retain full control over your data.

ramsac
the secure choice

Conditional Access

Conditional Access controls allows administrators to apply a set of rules that determine what users can access, based on whether or not they pass or fail a defined set of conditions.

So, regardless of the device a user is trying to access data from, we can define a set of rules that considers for example, what device they are using, whether the company owns the device or not, where the user is geographically located, what user group they belong to, how up to date or compliant their device is, etc.

Based on how many of the agreed criteria are met, we can then determine, whether they get access in full, whether they get to access applications or just a web view, whether they need MFA, or indeed, whether access should be blocked and the device locked.

For example, you could decide that a certain group of users, only ever gets access from the office and never gets access when not in the building. Another group may be allowed to access from anywhere in the UK, another, from anywhere in the world, or from any country in the world where they frequently travel for work, but you might block access altogether from a set of countries which we know to be at higher risk of cyber threat, such as Afghanistan, Myanmar and Namibia, which currently top the global list of high cyber risk countries.

Equally you might choose to have different access rules for devices that are owned and managed by your organisation, with a more restrictive set of access available to non company owned devices.

ramsac
the secure choice

Data Loss Prevention

Another important element of the security journey, is the implementation of Information and Data Loss Prevention, or DLP. DLP turns on the ability to classify a document or set of documents, with a certain sensitivity tag, and then controls what a user can do with that document. For example, a user could download the document to a USB key, and all the time they are logged in using their work credentials, they can access it. But if that user then leaves the organisation, even though they still have the file copy on the USB drive, they no longer have a 365 account with you, and so they will no longer be able to access the file.

Similarly, you can set controls to prevent documents being attached to emails, or shared externally to your organisation.

DLP helps organisations prevent sensitive data from being lost, stolen, or mishandled. It monitors and controls the flow of data within an organisation, ensuring that sensitive data is not being transmitted or stored inappropriately. DLP solutions can also monitor user behaviour to detect potential data breaches or violations of data handling policies.

ramsac
the secure choice

Defender for Business

Another important Microsoft security feature to discuss is Defender for Business, which is also now included in the 365 Business Premium subscription. Defender for Business is a bundle of antivirus and security tools from Microsoft with features that include:

Endpoint protection - An enterprise grade anti-virus and anti-malware protection tool

Next-generation protection - Helps to prevent and protect against threats at your front door with anti-malware and antivirus protection on your devices and in the cloud.

Attack surface reduction - Reduces your attack surface (places that your organisation is vulnerable to a cyber attacks) across your devices and applications using capabilities such as ransomware mitigation, application control, web protection, network protection, network firewall, and attack surface reduction rules.

Threat and vulnerability management - Helps you to prioritise and focus on the weaknesses that pose the most urgent and the highest risk to your organisation. By discovering, prioritising, and remediating software vulnerabilities and misconfigurations you can proactively build a secure foundation for your environment.

Endpoint detection and response (EDR) - Get behavioural-based detection and response alerts allowing you to identify persistent threats and remove them from your environment. Manual response actions within Defender for Business will allow you to act on processes and files, while live response will put you in direct control of a device to help ensure it's remediated, secured, and ready to go.

Automated investigation and remediation - Helps to scale your security operations by examining alerts and taking immediate action to resolve attacks for you. By reducing alert volume and remediating threats, Defender for Business allows you to prioritize tasks and focus on more sophisticated threats.

Sophos Intercept X

Not all organisations want to use Microsoft for virus defence, here at ramsac, we use Sophos. Sophos has excellent anti encryption technology and we prefer to include an external provider in our line of defence.

Doing more for less?

The features highlighted in this security journey, are all included in Microsoft Business Premium, so there's a chance that you're already paying them, you maybe just need help in setting up the polices and deploying these new tools. If you layer on all the other tools provided in 365, such as Office, SharePoint, Teams and the productivity tools such as Planner, Project and ToDo, you really can centralise the majority of your IT needs, into one monthly license.

From our professional point of view, what we love about keeping it all in one central platform, is that control of access and data becomes much simpler to manage. When a device is lost, breached, stolen, or a user leaves, we don't have to start thinking about the plethora of platforms that user may have had your data stored, and how many passwords and control may need to set up.

The security journey offers you robust, multi-layered protection across multiple areas, including identity protection, advanced cyberthreat protection, and defenses against phishing and ransomware. All of which are critical for the cyber resilience of your organisation.

We always liken cybersecurity, to the protection you would deploy for your physical premises, or your home for that matter. There is no point putting great locks on the door, if the door is left open at night. No point putting automatic closers on the door, if the windows aren't locked. No point having a great CCTV system if no one is checking it's still switched on. In the same way, modern cybersecurity demands multiple layers of protection. Intune isn't the only thing we need to think about, we also need to consider cyber monitoring through something like our secure+ service, and end user training and awareness for example, but by making the most of the Microsoft licences you may already be paying for each month, you could be making significant strides in making your organisation more secure.

ramsac
the secure choice

ramsac Limited

www.ramsac.com
01483 412 040

ramsac
the secure choice