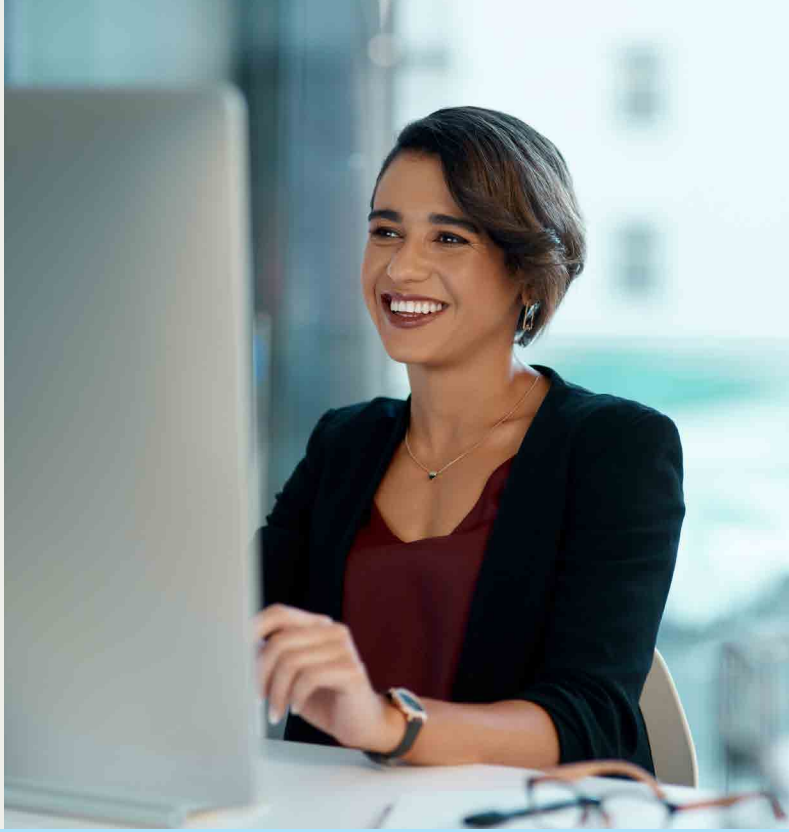
Introducing the Microsoft Security Suite

Create a multi-layered defence for your business with a full stack of security solutions from Microsoft

Tackling the ever-evolving threat environment

The modern workplace is more Cloud-empowered than ever, with Cloud technologies facilitating previously unprecedented levels of collaboration, connection and flexibility. However, while businesses across the globe are benefitting from the impressive operational capabilities of the Cloud, they do so at their own risk.

As so much of our valuable data is now stored online, cyber criminals are presented with an extremely attractive target – one that is not always properly protected. In order to avoid the negative consequences of a cyber attack, businesses need to implement a multi-layered cyber security posture.

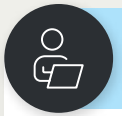


In this guide, we will demonstrate how you can use the Microsoft security suite to defend your business' most valuable assets. We will explore:

- The dramatic rise in Cloud attacks
- Why SMBs need to invest in cyber security
- The multi-layered capabilities of the Microsoft security suite
- How to get started with your Microsoft security journey
- And much more

The rise of Cloud attacks

As the Cloud is an infinitely capable environment, cyber criminals are always looking for new ways to target and compromise it. The most prevalent of these Cloud attacks include:



Misconfiguration

Misconfiguration refers to the incorrect set up of Cloud assets, making them vulnerable to malicious activity, including data breaches and account takeovers.

Ransomware

Ransomware is a form of malware that encrypts or blocks access to data until a ransom is paid. 59% of encryption ransomware incidents involve the public Cloud as it is both the platform from which the data is stolen, and where the attacker stores it while they demand the ransom.

Phishing

Phishing is a form of social engineering attack in which cyber criminals pose as legitimate correspondents and send targeted messages to trick victims into revealing sensitive information or downloading malware. Phishing has now even evolved to use deep fake technology to create false audio or video recordings of authority figures to add legitimacy to their attacks.

Account takeover

As so much of our data is now stored in the Cloud, if a cyber criminal can gain access to a privileged user's account, they can wreak havoc. During an account takeover, an attacker uses stolen employee credentials to impersonate specific users, steal data or plant malware.

Lack of visibility

As most organisations operate in the public Cloud, they do not own the infrastructure. This means that their Cloud resources are stored outside of their corporate network, causing poor visibility. This makes it harder to recognise and locate attacks.

Denial of Service attacks

A Denial-of-Service (DoS) attack renders Cloud resources or services unavailable by overwhelming them with heavy amounts of traffic. This compromises a business' ability to use their important Cloud assets.

The importance of Microsoft security

In recent years, Irish businesses have seen a rise in the number of cyber attacks they are facing, as demonstrated by these startling statistics:

90% of Irish businesses have seen a rise in cyber attacks in the last 12 months (compared to 72% globally).

44% of cyber teams in Ireland say they are lacking the budget to sufficiently manage their cyber-related challenges.

52% say they are more exposed to a major breach than they should be and require additional investment in their cyber defences.

(Source: Irish Examiner)

While the cost of a successful cyber attack is more than just monetary – affecting your business' operational capabilities and reputation – the financial consequences cannot be ignored. The average cost of a cyber attack for SMEs in Ireland was €3.1million in 2021. Additionally, the cost of cyber security insurance is higher if clients do not take preventative measures to protect themselves. Some insurers even offer discounts if your organisation has already established recognised cyber security defences, such as Cyber Essentials.

Implementing a centralised identity and access service reduces the risk of identity compromise across both your Cloud and on-premises services. Additionally, it will help you to avoid the two-fold costs of a cyber attack and higher cyber security insurance premiums.

Identity and access management

Microsoft's solution for multi-Cloud identity and access management is Azure Active Directory (AAD). This helps businesses to manage user access permissions and manage any device that connects to your domain. Going far beyond Multi-Factor Authentication (MFA), Azure Active Directory offers complete visibility and control, helping to avoid access-based threats, like account takeover.

Streamlining the management of devices and access allows you to mitigate insider threats and the risk of data loss. Azure Active Directory also facilitates simpler ongoing device maintenance and management, reducing your overall risk by removing older systems that could be exploited.

Single Pane of Glass

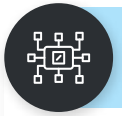
Manage access to your services and resources through a single pane of glass, granting you full visibility and control of your environment.

Single Sign-On

Access your apps simply and securely from anywhere. Azure Active Directory integrates into over 4,500 SaaS apps for Single Sign-On, giving clients one source of truth.

Authentication

Keep malicious actors out by establishing minimum password criteria, setting up Multi-Factor Authentication (MFA) and enacting Smart Lockout procedures for unexpected login activity.



Conditional Access

Set up strict criteria for application log ins and adaptive access policies to prevent unrecognised devices, security setups or connections from accessing your apps.

Device Management

Using threat detection capabilities, AAD identifies malicious files that may have been uploaded to any of Microsoft's key file exchange apps, isolates unsafe files and restricts user access.

Identity Governance

Efficient, automated identity governance ensures that only authorised users have access to certain apps and data – and only when they need it.

Device Management

Microsoft Endpoint Manager, comprised of Microsoft Intune and Configuration Manager, is a unified endpoint management platform, providing comprehensive Cloud-based security. Endpoint Manager supports the Cloud-based, hybrid workforce effectively, allowing businesses to secure, deploy and manage users, apps and endpoint devices without disrupting everyday operations or existing processes. The addition of Microsoft Intune provides a granular administration experience, allowing you to configure specific policies to control applications and devices.

Endpoint Manager lets you manage Windows, iOS, Android and Mac, making it ideal for companies with Bring Your Own Device (BYOD) policies. You can manage all these operating systems simultaneously and set conditions targeting the specific ecosystems.

Cloud security

Protect user devices against cyber threats using Zero Trust technology from Microsoft.

Comprehensive management

Simplify automated provisioning, configuration management and software updates for all your endpoints

Visibility and control

Maintain full visibility and control of the devices that have access to your systems and data.

Achieve Zero Trust

Zero Trust is a cyber security strategy that eliminates the principle of implicit trust, be it from inside or outside of an organisation. Anyone attempting to connect to a business' system must be continually verified at every stage of the digital interaction. This creates a far more secure environment for your data and valuable assets. Think of it this way – you wouldn't trust just anyone to enter your home and rifle through your personal possessions, so why would you treat the environment that houses your data any differently?

The Microsoft security suite enables the implementation of a secure Zero Trust strategy. The access management technologies previously discussed in this guide facilitate a more secure and controllable IT environment. By combining Microsoft Endpoint Manager, Microsoft Intune and Azure Active Directory's Conditional Access, businesses can create their own Zero Trust security posture, ensuring that only devices being managed by these Microsoft solutions can connect to their servers and access their resources and data. You can retain full knowledge and control of the devices connecting to your environment and can prevent any non-managed device from accessing your valuable assets.

Data protection and compliance

Data management poses a significant challenge for small and medium-sized businesses.

43% of all data breaches involve SMBs.

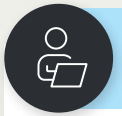
61% of all SMBs have reported at least one cyber attack in the previous year.

Only 14% of small businesses consider their cyber attack and risk mitigation ability as highly effective.

(Source: Cyber Security Magazine)

The issue of data management is further compounded by the need to comply with GDPR and other industry-specific data security regulations. Suffering from a data breach could not only impact your business financially and operationally, but legally too. This could have significant repercussions moving forward.

Microsoft 365 Business Premium provides SMBs with enterprise-grade technology to help identify and protect your sensitive data. Users will be able to manage your data in a more granular way than ever before, ensuring that you prevent accidental and malicious data breaches across your estate. This helps to avoid potential compliance penalties. From the access control to sensitive data protection across devices, Microsoft 365 Business Premium compliance services are best-in-class.



Mobile device management

Apply granular security policies to protect business data across company devices and remove data from lost or stolen devices.

Secure remote access

Allow employees to securely access business applications using conditional access and protect against password theft with advanced multi-factor authentication.

Protect business data

With Microsoft Purview, you can implement data loss prevention by defining and applying DLP policies. These allow you to identify, monitor, and automatically protect sensitive items across endpoints, Clouds, applications and Microsoft 365 services.

Mobile application management (MAM)

Microsoft Intune's MAM allows you to manage and protect your business' data within an application, preventing it from laterally moving on smart devices.

Data labelling

With Azure Information Protection you can configure policies to classify, label, and automatically protect data based on its sensitivity. This allows you to track and control exactly how your data is used.

Dealing with advanced threats

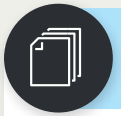
Unfortunately for your business, cyber criminals rarely take a day off. Cyber risks are a constant presence that you need to be prepared for. As a result, you need a technology fabric that is always evolving and watching for emerging threats.

With Microsoft 365 Business Premium, SMBs receive access to two solutions that help to protect you from ever-developing cyber threats: Microsoft Defender for Office 365 and Microsoft Defender for Business.

Microsoft Defender for Office 365

In the digitally enabled workplace, nearly all businesses engage with Office 365 applications. As the usage is so high, it is perhaps no surprise that cyber criminals view the Office 365 suite as a goldmine of opportunity for attack.

Fortunately, with Microsoft Defender for Office 365, you can detect and prevent threats in your Office 365 environment in real time, using the following features:



Safe Attachments

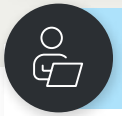
This feature checks email attachments for malicious links by opening them in a controlled virtual sandbox environment. All incoming emails are covered by default built-in protection, but admins can also define their own safe attachment policies.

Safe Links

Safe Links scans embedded URLs and rewrites inbound email messages to ensure they do not link to malicious sites. It also implements a 'Time-of-Click' verification to ensure that URLs are re-analysed when accessed by an end-user.

Safe Attachments for SharePoint, OneDrive & Teams

This feature detects and blocks any malicious files that have been uploaded to SharePoint, OneDrive or Teams. Unsafe files are then automatically isolated and user access is restricted.



Anti-Phishing

Defender's default anti-phishing policy provides out of the box spoofing protection. Administrators can also set advanced controls to protect against user impersonation and implement mailbox intelligence to analyse email patterns and whitelist trusted senders.

Real-Time Detection

As the name suggests, Real-Time Detection detects and responds to threats entering your Office 365 environment in real-time, providing comprehensive reporting.

Microsoft Defender for Business

While all Microsoft 365 plans offer baseline protection and security with Microsoft Defender Antivirus, as Microsoft 365 Business Premium includes Microsoft Defender for Business, it also offers threat protection, data protection and device management features.

Microsoft Defender for Business is Microsoft's new endpoint protection solution that manages threats across Windows, iOS, macOS and Android operating systems, helping SMBs get closer to Zero-Day threat protection. With next-generation antivirus and endpoint detection and response capabilities, your business will be comprehensively defended against sophisticated ransomware attacks across devices.

Automated Investigation & Response (AIR)

AIR examines alerts and takes action to resolve breaches immediately. This significantly reduces the volume of alerts, allowing security operations to focus on more sophisticated threats.

Block at First Sight

Block at first sight is a next-generation threat protection feature that detects new malware and blocks it within seconds.

Cross-Platform Support

Benefit from a unified view of threats across Windows, iOS, macOS, Linux and Android operating systems, allowing you to respond to threats in your environment more quickly.

Endpoint Detection & Response

EDR capabilities provide advanced, real-time and actionable attack detections. Related alerts are aggregated into 'incidents' making it easier for analysts to respond.

Enhanced ASR

Attack surfaces refer to areas where your organisation is vulnerable to cyber threats. Defender includes several capabilities to help reduce your attack surfaces and minimise the chance of attack.

Tamper Protection

Tamper protection prevents malicious actors from disabling security features, such as antivirus protection, on your machines and devices.

Threat Analytics

Threat analytics are a set of detailed reports from Microsoft security experts, each providing a detailed analysis of a threat and guidance on how to defend against it.

Threat Vulnerability & Management

This delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices. It prioritises the largest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk.

Web Content Filtering

Web content filtering enables your organisation to track and regulate access to websites based on their content categories, helping to avoid issues including compliance and bandwidth.

With Microsoft 365 Business Premium, you can benefit from enterprise grade security, powered by the might of the Microsoft Cloud and democratised for the SMB community.

Begin your Microsoft security journey with MSP X

The Microsoft security suite is exactly that – a suite of complementary solutions that interconnect to provide a comprehensive and multi-layered defence for your business. You should view your security journey as a cycle, with each step further strengthening your cyber security posture and minimising the risk of a cyber attack.

By implementing the solutions laid out in this guide, you will be simultaneously advancing your business' protections and maximising your existing Microsoft 365 investment.

Never fear; you don't have to embark upon your security journey alone. The Microsoft experts at MSP X are here to guide you through the process. To get started, why not assess your cyber security posture by taking our free assessment today, or book a workshop to learn more about these innovative technologies.

GET IN TOUCH