greymatter

Microsoft Security Solutions

Gold
Microsoft Partner

Stay secure and productive anywhere, on any device, with identity and intelligence-driven innovations from Microsoft.

Enterprise Mobility + Security

Microsoft Enterprise Mobility + Security (EM+S) is an intelligent mobility management and security platform that aids productivity. It gives you a suite of tools that help you to proactively defend against breaches and effectively isolate incidents. While empowering your employees to work in new and flexible ways.

Why trust Microsoft security solutions?

Microsoft invests more than USD 1 billion annually on cybersecurity research and development. It employs more than 3,500 security experts completely dedicated to your data security and privacy. And, Azure has more compliance certifications than any other cloud provider.

What are the main components of Microsoft Enterprise Mobility + Security?

Microsoft Azure Active Directory (AD) Premium

Azure AD manages more than 1.2 billion identities and processes over 8 billion authentications every day.

Azure AD is for:

IT Admins to control access to apps and app resources.

You can enable multifactor authentication (MFA) for certain resources, automate user provisioning between existing Windows Server AD and cloud apps. As well as, protect user identities and credentials.

App Devs can use it to add single-sign-on (SSO) to apps. It has APIs that allow you to build personalised app experiences using existing organisational data.

Microsoft 365, Office 365, Azure, and Dynamics CRM online subscribers all already have Azure AD automatically and can easily manage access to integrated cloud apps.

Azure Information Protection

Azure Information Protection allows you to control and secure emails, documents and sensitive data that you need to share with stakeholders outside of our company.

Using it, you can classify your data based on sensitivity. Adding labels and permissions to your data that follows it wherever it is shared or stored. You can define who can view, share and edit data. You can track activities on shared data and revoke access should you need to.

Integrated with Microsoft Office, data can be secured with one click and notifications within documents can help users to make the right decisions.

Microsoft Endpoint Manager

Microsoft Endpoint Manager is a culmination of Microsoft System Center Configuration Manager (rebranded Microsoft Endpoint Configuration Manager), Intune, Desktop Analytics and AutoPilot.

Microsoft Intune

Microsoft Intune enables you to securely manage iOS, Android, Windows and macOS. Streamline and automate deployment, provisioning, policy management, app delivery and updates.

Intune app protection policies provide granular control over Office 365 data on mobile devices, even when you don't manage the devices used by employees to access work files.

Integrated data protection and compliance capabilities that let you be precise about what data different users can access as well as what they can do with the data within Office and other mobile apps.

Microsoft Cloud App Security

Microsoft Cloud App Security is a multimode Cloud Access Security Broker (CASB). It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.

Microsoft Advanced Threat Analytics

Microsoft Advanced Threat Analytics (ATA) gives you a real-time view of the attack timeline. It identifies normal and suspicious user and device behaviour with built-in intelligence.

It is an on-premises platform to help you protect your enterprise from advanced targeted attacks by automatically analysing, learning, and identifying normal and abnormal entity (user, devices, and resources) behaviour.

- Detects malicious attacks instantly as the occur
- Detects abnormal behaviour leveraging machine learning
- Identifies known security issues using world-class security research

Microsoft Azure Advanced Threat Protection

Microsoft Azure Advanced Threat Protection (ATP) detects and investigates advanced attacks on-premises and in the cloud. It:

- Identifies suspicious user and device activity
- Analyses threat intelligence from cloud and on-premises
  Protects user identities and credentials stored in Active Directory
- Gives a simple attack timeline with all the information you need to triage
- Monitors multiple entry points by integrating with Windows Defender Advanced Threat Protection

Microsoft security solutions and Grey Matter

You can easily purchase EM+S through our online cloud marketplace GMCirrus when you sign up to our Cloud Solution Provider programme. You can increase and decrease licenses via our self-serve portal and get access to a free tier of technical support.

If you're already using Windows 10 and Office 365, you may be able to get EM+S for little or no additional cost by purchasing Microsoft 365 which includes all three – Windows 10, Office 365 and EM+S.

Did you know?

If you've purchased Microsoft System Center Configuration with Software Assurance, you can get Microsoft Intune for free today!

Microsoft Cloud Security Assessment

As businesses adopt remote working and embrace Cloud solutions to best enable their employees, we have created our Cloud Security Assessments to help organisations identify possible security risks and exposure to cyber treats.

Over the course of 3 days our Cloud Security Specialists will utilise their experience and a suite of Microsoft tools to assess your environments security posture covering four core areas and recommended steps required to remediate any issues identified.

- **Secure Score**

  We aim to help you get insights into your security position by helping you better understand what Microsoft security features you have enabled, as well as provide guidance on what other security features are available to increase your security level.

- **Shadow IT**

  We give you visibility into the cloud apps and services used in your organisation and asses their risk, enabling you to make an informed decision about whether you want to sanction the apps discovered or block access.

- **Windows Security**

  We assess the current security posture of Windows clients within your organization, identify machines which require attention, as well as provide recommendations for actions to further reduce the attack surface.

- **Attack Simulator**

  We help identify vulnerable users within your organisation by analysing user preparedness for spear phishing attacks and user password quality by performing attack simulations, allowing you to position training or remediation options.

Our managed services

Microsoft 365 Business

Complete lifecycle management of Microsoft 365 licences as well as proactive monitoring of your cloud health. We will:

- Provision and de-provision licences as needed
- Manage user and shared mailboxes, security groups and other Exchange Online features
- Manage Teams and / or Skype for Business

Microsoft 365 Enterprise

Complete lifecycle management of Microsoft 365 licences as well as proactive monitoring of your cloud health.
We will:

- Provision and de-provision licences as needed
- Manage user and shared mailboxes, security groups and other Exchange Online features
- Manage Teams and / or Skype for Business
- Manage SharePoint online, including user permissions and cloud service functions and configurations
- Maintain OneDrive for Business
- Manage Power Platform service-related issues
- Provide a security package including: investigation and response, risk event management, creation of identity security policies such as MFA and conditional access