Microsoft

Crash course in EMS

Crash course in EMS

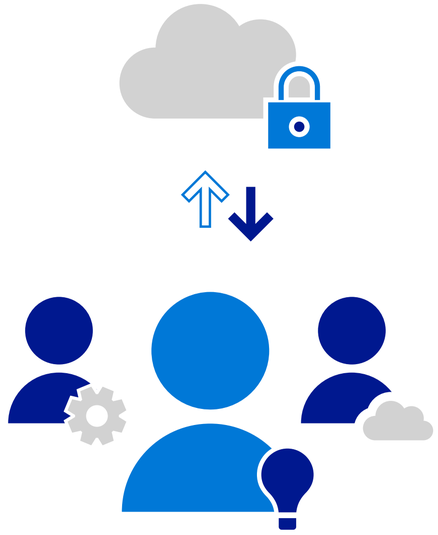
Competing today requires a workplace that focuses on digital transformation and empowering everyone to be creative and work together securely. To create a modern workplace, you must provide seamless access to the tools and data people need, wherever they are, on whichever device they choose. To help keep your modern workplace secure, you need to protect your data effectively as it traverses among many applications, locations and users.

By choosing Office 365, you've made a great investment to help achieve these goals. Its productivity and collaboration tools – plus built-in security – provide a solid foundation for your modern workplace. How you take the next step can enable even greater transformation. With Microsoft 365 you'll add the power of Microsoft Enterprise Mobility + Security (EMS) and Windows 10 to your transformation toolkit.

EMS expands your security capabilities for Office 365, identity, device management and information protection to add advanced solutions that you can extend across your whole environment. This gives your organisation the freedom to create, share and innovate while minimising risk. With EMS, you can generate and manage secure identities for partners, vendors and customers, enabling new levels of teamwork. By tapping into the power of unified endpoint management, your IT team can secure and manage all types of corporate and personal devices, from PCs to tablets to smartphones – all from one centralised location. When you choose Microsoft 365, you get a complete, secure solution to help your business compete in a fast-evolving world, with protection against advanced threats to keep your information safe.

What is EMS?

EMS provides additional protection for Office 365 and expands your capabilities to help you securely deliver all of your apps to any device, safeguard your corporate assets virtually anywhere and protect your infrastructure both on-premises and in the cloud.



- **Identity and access management:**

  Identity is at the centre of how you connect with people, devices and data. Using a single, holistic identity solution provides the flexibility and control you need to increase security, lower costs and improve productivity.

- **Information protection:**

  Discover, classify, protect and monitor your sensitive data, wherever it lives or travels, and however it is shared.

- **Threat protection:**

  Protect your organisation from sophisticated attacks with adaptive, built-in intelligence. Detect and investigate advanced threats, compromised identities and malicious actions across your on-premises and cloud environments.

- **Unified endpoint management:**

  With EMS, you can empower users to be productive with the flexibility to work the way they want on their preferred devices, all while maintaining control of your applications and data security.

EMS includes the following:

- **Azure Active Directory (AD) Premium:**

  Microsoft's multi-tenant, cloud-based directory and identity management service. Azure AD combines core directory services, application access management and identity protection in a single solution, offering a standards-based platform that helps developers deliver access control to their apps, based on centralised policies and rules.

- **Microsoft Intune:**

  Use the cloud-based enterprise mobility management (EMM) service to enable your workforce to be productive while keeping your corporate data protected. Intune integrates with Azure Active Directory for identity and access control, and Azure Information Protection for data protection.

- **Azure Information Protection:**

  Azure Information Protection (sometimes referred to as AIP) is a cloud-based solution that helps an organisation to classify and, optionally, protect its documents and emails by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users or a combination where users are given recommendations.

- **Microsoft Advanced Threat Analytics:**

  Advanced Threat Analytics (ATA) is an on-premises platform that helps protect your enterprise from multiple types of advanced targeted cyberattacks and insider threats.

- **Microsoft Cloud App Security:**

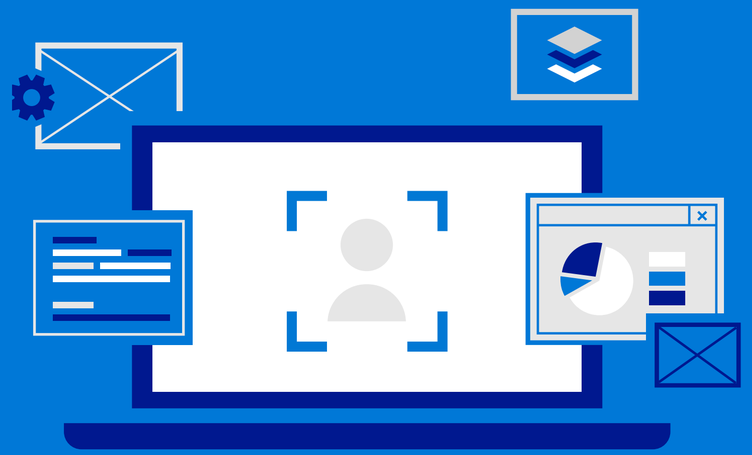
  Cloud App Security is a cloud access security broker (CASB) that can help your organisation take full advantage of the promise of cloud applications, but keep you in control, through improved visibility into user activity. It also helps increase the protection of critical data across cloud applications.

- **Azure Advanced Threat Protection:**

  Azure Advanced Threat Protection (ATP) is a cloud-based security solution that identifies, detects and helps you investigate advanced threats, compromised identities and malicious insider actions directed at your organisation.

01.

Improve the user experience



Save time and improve productivity with single sign-on

Your teams use a variety of applications throughout the day. Managing passwords and logging in over and over can slow them down and increase risk. Azure AD single sign-on (SSO) improves security by extending on-premises AD to the cloud, so people can use their primary corporate identity to sign in to domain-joined devices, company resources and web and software-as-a-service (SaaS) applications.

Enable secure mobile productivity

With EMS, people can work securely from whichever phone, tablet, Mac or PC they prefer – whether it's corporate-owned, employee-owned or a third-party managed device. Easily configure devices with policies and certificates that allow users to access email, Wi-Fi, apps and other corporate resources, so their preferred devices are ready to go with minimal user set-up.

Give users a consistent experience by adding your corporate branding

Apply your company's look and feel to your Azure AD sign-in page, which appears when users sign in to applications that use Azure AD as an identity provider. This option can be configured in the Azure AD admin centre.

Use password-free login for security and ease

Keeping track of passwords can be a major headache for users, leading them to write credentials down in non-encrypted formats – and opening the door to security breaches. Azure AD provides password-free login options that make authenticating easier for users and more secure for businesses. Using Intune, you can enforce strong authentication policies to ensure protection.

Protect data with or without device enrolment

Using Intune, you can create and enforce app protection policies that help keep your company data safe even without enrolling and managing the users' devices. By implementing app-level policies, you can restrict access to company resources and keep data under the control of your IT department. Users can choose the devices they want to use without negatively affecting security.

Simplify password management with Azure AD self-service password reset

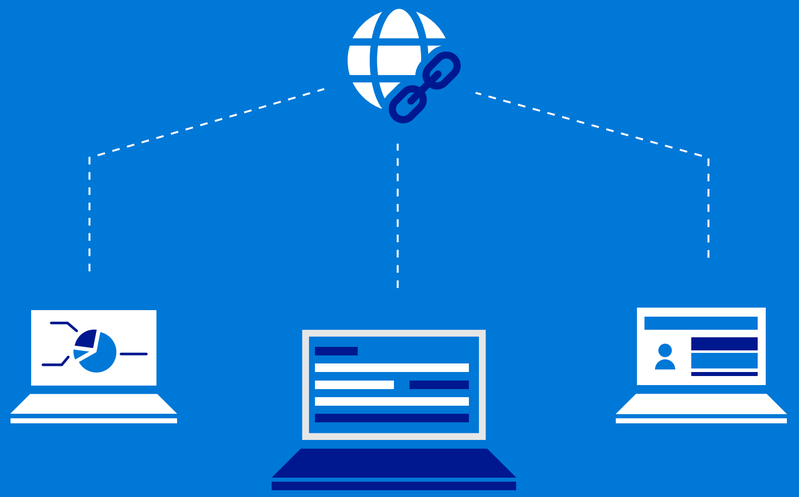
Your IT department should be able to prioritise strategic and mission critical work, rather than spending time resetting passwords. With Azure AD self-service password reset (SSPR), you can enable users to change their passwords and unlock their accounts without calling the helpdesk. It is a full-featured solution, enabling authentication by text message, phone call, email or security questions.

Manage a diverse mobile environment with less work

From desktops to tablets to smartphones, employees are using more devices to get work done than ever. Keeping those devices compliant and secure can be challenging. With Microsoft 365, you can securely manage iOS, Android, Windows and macOS devices from a unified, cloud-based solution, while Intune lets you set policies, remotely wipe, lock and reset devices, and more.

02.

Connect your on-premises and cloud applications as one ecosystem



Integrate on-premises directories with Azure AD Connect

If you use Active Directory on-premises, you can easily benefit from Azure AD by synchronising the two using Azure AD Connect. By providing a single, common identity for accessing both cloud and on-premises resources, you can improve the user experience, support productivity and enable advanced security capabilities. Azure AD Connect can work with Active Directory Federation Services (AD FS) to address complex deployment scenarios such as domain-joined SSO.

Enable easy remote access using Azure Application Proxy

Some traditional access methods for remote workers – such as virtual private networks (VPNs) and demilitarised zones (DMZs) – can be complex and challenging to secure and manage. Azure AD Application Proxy enables SSO and secure remote access for on-premises web applications such as SharePoint sites, Outlook Web Access on Exchange Server or other line-of-business applications. Users can access on-premises and cloud applications using one identity, and there's no need to change network infrastructure or employ VPN.

Engage more effectively with Azure B2B collaboration

Employees aren't the only people who need secure access to your application ecosystem. You might also need to connect with vendors, partners, subsidiaries or other external entities. Using Azure AD B2B collaboration, you can give guest users single sign-on access to applications of your choice, with powerful authentication policies managed by Azure AD.

Advanced application management in one place

With the variety of applications common in today's enterprise environments, unified management is a must. With Intune, you can publish, configure and update mobile apps on enrolled and unenrolled devices, and secure or remove app-associated corporate data.

Extend unparalleled Office mobile app management to all your apps

Add new capabilities to your built-in Office 365 application management. Enable your users to access corporate information more securely with the familiar Office mobile and line-of-business apps they use every day, while maintaining data security. Restrict actions like copy, cut, paste and save-as to protect data accessed through any of the apps you're managing with Intune.

Elevate security for cloud apps and services

Gain visibility, control and protection for your cloud-based apps, while identifying threats, abnormal usage and other cloud security issues. Cloud App Security enables you to identify the cloud apps used in your organisation, assess their risk and leverage lifecycle management capabilities and ongoing analytics to control usage.

03.

Protect your apps and data with identity-based security

Improve security with Azure AD Conditional Access and MFA

In a world of growing cyberthreats, passwords just aren't enough to protect sensitive information, but you don't want to compromise productivity either. Azure AD Conditional Access helps you automate access control decisions that are based on different criteria such as user, location, application and risk. Based on the rules you define, you can require certain actions such as MFA, restrict access or block a user entirely.

Detect and mitigate breaches with Azure AD Identity Protection

If an attacker steals a user's identity – even one with minimal privileges – they may still be able to gain access to critical systems and data. Azure AD Identity Protection helps you detect identity vulnerabilities, investigate and mitigate suspicious access and configure automated responses to potential identity breaches. With Azure AD Identity Protection, you can protect all identities regardless of their privilege level and proactively prevent compromised identities from being abused.

Defend against advanced cyberthreats

With the increasing sophistication of digital criminals, identifying and protecting against threats even as they change and adapt is critical to maintaining a strong security posture. When you deploy EMS as part of Microsoft 365, Azure Information Protection and Azure Advanced Threat Protection help you detect threats quickly using behavioural analytics, focus on important security events, reduce false positives and get actionable recommendations for remediating suspicious activity.

Delegate application controls safely using Azure AD Privileged Identity Management

Users may need privileged access to administrative controls for a variety of reasons. However, dormant or rarely used account privileges can linger unseen and enable access beyond what individuals need – which creates security risk. Azure AD Privileged Identity Management (Azure AD PIM) enables you to provide granular access privileges to Azure AD resources and other Microsoft Online services on a temporary, as-needed or on-request basis, as well as manage, control and monitor those privileges to prevent problems.

Protect company data with app protection policies

With users increasingly getting work done on personal devices, IT has to manage sensitive company data without intruding on employees' privacy. Intune app protection policies give you control over company data on both managed and unmanaged devices – with the important ability to manage and selectively wipe company information without touching the user's personal data. Even on personal devices, company data stays separate and secure from a user's personal data.

Classify and label data using Azure Information Protection

As the amount of data your users deal with grows, empowering them to protect it can help them stay productive virtually anywhere. With Azure Information Protection in EMS you can classify, label and protect data based on its sensitivity. Automatic classification applies labels and protection to data based on rules you define. You can also prompt users to protect data following your recommendations when they're working in files or sending emails. Users can track shared files and revoke access if necessary, while your IT team can use powerful logging and reporting tools to monitor, analyse and reason over data.

With Office 365, you've got your digital transformation moving. Now kick it into high gear with Microsoft 365 including EMS to empower your people, enable more secure productivity and reduce operational overhead. Encourage people to use the applications and devices they prefer while maintaining control over company data wherever it goes. Give users more convenient and secure single sign-on. Free your IT staff from complex device management. Identify and manage all the cloud apps employees use.

Explore how these and other scenarios are made simple by the powerful technologies in Microsoft 365.
Visit: transform.microsoft.com