Protecting and empowering your connected organization with Microsoft Enterprise Mobility + Security
Contents

1 Executive summary

2 What’s next: control in the cloud

3 Addressing the challenges of a mobile-first, cloud-first world
   Identity management
   Identity-driven security in the cloud
   Identity-driven security on-premises
   Device management
   Information protection
   Administrative challenges

4 How customers are using EMS
   Identity-driven security
   Managed mobile productivity
   End-to-end information protection
   Streamlined deployment and management
   Summary
Executive summary

There’s a big change happening in IT as companies undergo a digital transformation to mobility and the cloud. This has significant impacts to how IT thinks about security.

What was once largely limited to the confines of an on-premises world now extends to the cloud and a myriad of mobile devices. Employee interactions with other users, devices, apps, and data have become increasingly more complex, generating new blind spots for IT. The sophistication of attack vectors continues to increase. What’s more, many companies struggle to keep up with traditional, single-point solutions. Limited budgets only add to the challenge.

How can existing on-premises solutions for identity management, device management, and information protection effectively address this modern world? The answer is simple: They can’t. Instead, the control plane for all of these services needs to move, over time, from your own datacenter to the cloud. Doing this gives you the control and protection your business requires without compromising the familiar mobile and desktop experiences that employees expect.

This is the idea behind Microsoft Enterprise Mobility + Security (EMS) - the only comprehensive mobility solution designed to help manage and protect users, devices, apps, and data in a mobile-first, cloud-first world.

With EMS, we start with one protected common identity for secure access to all corporate resources. We then protect this data with innovative security technologies - including powerful machine learning to protect data from new and changing cybersecurity attacks. And because EMS is a cloud-based solution, set-up is fast and easy with scalability and updates to ensure your investment is ready for the future.

EMS also works well with your current on-premises investments. Azure Active Directory Premium connects with your existing Active Directory, for example, while Microsoft Intune connects with System Center Configuration Manager to work with all of your client devices. Used together, these integrated cloud and on-premises technologies can protect and manage your identities and your data on all of your devices, wherever they might be.

The IT world is changing—again—and every IT leader must change with it. Microsoft EMS has an important role to play in helping you navigate this shift.
What’s next: control in the cloud

One of the biggest challenges for IT leaders is recognizing major technology shifts and then adjusting their organization to benefit from those changes. Today many of these shifts arise from the demands of employees, partners, and customers to use the devices they love together with the power of the cloud.

One important example of this is the change happening in how we manage and protect identity, devices, and data. In the pre-cloud world, the technologies you used to do these things ran solely in your on-premises environment (Figure 1). Where else could they run? Before the advent of cloud computing there was no real alternative.

The world was a simpler place then. Most of what you had to worry about was contained within your network perimeter and was largely under your control.

Those days are long gone. Today every IT leader must contend with a much more complicated world, one that contains not just traditional clients and servers, but also mobile devices, cloud platforms, SaaS applications, and maybe more (Figure 2).
Now the requirements for identity are much more demanding. The devices you must manage are more diverse and they’re often outside your network perimeter. The information you must protect lives not just inside your firewall but also on those devices and in the cloud.

Meanwhile, the cybersecurity attacks that threaten your entire infrastructure are not only growing more sophisticated but changing every day, requiring increasingly more sophisticated security tools and strategies.

The traditional approach to managing all of these things, which relied on on-premises technologies alone, no longer works. Instead, your organization should move to a more flexible, cloud-based solution (Figure 3).
Figure 3: Now the core technologies for identity management (IM), device management (DM), and information protection (IP) should run in the cloud.

Your existing on-premises technologies for working with identity, devices, and information are still important and they will be for some time. But without cloud solutions you just can’t solve the problems raised by the modern world. Because of this, expect your focus in all of these areas to move from the on-premises approach you might use today to a new hub in the cloud.

To help you address this shift, Microsoft has created Enterprise Mobility + Security (EMS). Individually, the components in EMS provide cloud solutions for identity management, device management, information protection, and more. Used together, these technologies are even more powerful, providing you with benefits like identity-driven security - a holistic approach that addresses the sophisticated challenges of the today’s new attack landscape. And because these technologies are tightly integrated with productivity tools (like Office and Office 365) that your employees use every day, you actually gain tighter control and increased security without having to impose complex processes and changing the way people work.

How fast you move your identity and management solutions to the cloud is up to you. What’s important now is that you realize why this shift is happening, then understand what you need to do to benefit from the change. What follows explains this, showing how Microsoft EMS supports this transition.
Addressing the challenges of a mobile-first, cloud-first world

Managing identity and devices, protecting information, addressing a new attack landscape: none of these is simple. Factor in today’s mobile-first, cloud-first world as well as limited budgets and resources and the challenges become even more complex. To better understand and tackle these issues, and to grasp why a combination of cloud and on-premises solutions are essential, we need to walk through them one at a time. We also need to look at how the components of EMS address each of these areas.

Identity management

Every user wants single sign-on (SSO) to multiple applications. We all hate remembering different sign-on names and passwords. This is why our organizations have long used on-premises identity management technologies such as Microsoft Active Directory.

Yet, with the increasing popularity of SaaS applications, relying solely on identity management on premises is no longer enough. The reason is simple: to provide SSO, an on-premises technology like Active Directory must connect to each of the applications that users want to access. If all of those applications are in your own datacenter, this is easy to do: each application connects to its local instance of Active Directory. As more applications move to the cloud, problems arise. If every SaaS application connects directly to every enterprise’s on-premises identity management technology, the result is chaos (Figure 4). This is exactly the situation in which many organizations find themselves today.

Figure 4: Creating a direct connection between every organization’s identity management solution and every SaaS application would quickly become too complex to manage.

A simpler approach is to use a cloud solution for identity management: Azure Active Directory (AD) Premium. Your on-premises directory service is still essential, but it now connects only to Azure AD. Azure AD can then connect directly to each SaaS application (Figure 5).
Protecting and empowering your connected organization

The result is SSO without the chaos. Your users’ identities can still come from your own directory service—you’re still in control—but by exploiting the power of the cloud, you’ve given them easy access to both local and SaaS applications with a single sign-on. You’ve made life better for your users and simpler for your IT administrators.

Azure AD currently provides SSO to more than 2,000 cloud applications, including Office 365, Salesforce.com, Box and ServiceNow. This service does more than just single sign-on, it also offers:

- **Risk-based conditional access** – which can help eliminate the risk of unauthorized access. Conditional access offers an intelligent assessment of granting or blocking access, or enforcing MFA based on factors such as group membership, application sensitivity, device state, location, and sign-in risk.

- **Built-in multi-factor authentication (MFA)** – for an additional security layer for protected authentication. With MFA, you can require your users to provide both a password and something else, such as a code sent to their mobile phone, to sign on.

- **Privileged identity management** – which provides additional control over user identities that require privileged access, including the ability to discover, restrict, and monitor them - and provide just-in-time administrative access for eligible users.

- **Secure remote access** – to enable secure access to on-premises applications published with Azure AD without using a virtual private network (VPN)Azure Active Directory Premium features multi-factor authentication (MFA); access control based on device health, user location, and identity; and holistic security reports, audits, and alerts.

- **Cross-organizational collaboration** – to make it easier to grant vendors, contractors, and partners with risk-free access to in-house resources with Azure AD B2B collaboration.

---

Figure 5: Cloud-based identity management with Azure Active Directory greatly simplifies managing single sign-on to SaaS applications.

More than 80 percent of employees admit to using non-approved SaaS applications in their jobs

– Stratecast, December 2013
Identity-driven security in the cloud

Just as legacy security solutions lack the ability to provide efficient access to your cloud applications, they are also not designed to protect the data within these apps.

There are several reasons for this. Traditional network security solutions, such as firewalls and IPS, don’t offer visibility into the transactions that are unique to each application, including how data is being used and stored. Classic controls also monitor only a small subset of cloud traffic and have limited understanding of app-level activities.

So how can you maintain visibility, control, and protection of your cloud apps? With EMS, you get Microsoft Cloud App Security (CAS) - a comprehensive service that provides deeper visibility, comprehensive controls, and improved protection for your cloud applications. CAS is designed to help you extend the visibility, auditing, and control you have on-premises to your cloud applications (Figure 6).

More than 80% of employees admit using non-approved SaaS apps for work purposes.

– Stratecast, December 2013

CAS can identify over 13,000 cloud apps. No agents are required; instead, information is collected from your firewalls and proxies to give you complete visibility and context for cloud usage and shadow IT. Deep visibility into apps, devices, and data activity uncovers suspicious activities, user mistakes, and potential threats before they become real ones. And with behavioral analytics, machine learning, and unique Microsoft security intelligence, you can secure your corporate files and data while freeing your employees to get their work done on the go.
Identity-driven security on-premises

While EMS provides powerful security features for your cloud apps and data, this doesn’t make securing your on-premises environment any less important. Microsoft recognizes this, which is why EMS also encompasses Advanced Threat Analytics (ATA).

ATA doesn’t run in the cloud—it operates entirely inside your organization—and its purpose is to help you identify suspicious activities before they cause damage. To do this, it builds a map of what applications your users commonly access. It also keeps track of the devices they typically use, the times that access occurs, and more. If a user unexpectedly begins accessing atypical applications from different devices at odd times, it’s a safe bet that this user has been hacked. An attacker has assumed her identity, probably because the attacker has stolen her username and password.

ATA detects this kind of threat. When abnormalities appear, ATA will warn your security staff so they can take action immediately. Rather than wait for an attacker to damage your organization, ATA helps you detect and stop attacks much earlier. And while ATA runs on-premises, it can be licensed as part of EMS (Figure 7).

Figure 7: Microsoft Advanced Threat Analytics (ATA) helps protect your enterprise from advanced targeted attacks by automatically analyzing, learning, and identifying normal and abnormal entity (user, devices, and resources) behavior.

Advanced Threat Analytics also provides other benefits. They include the following:

- **Adapt to the changing nature of cyber-security threats.** ATA continuously learns the behavior of organizational entities (users, devices, and resources) and adjusts itself to reflect the changes in your rapidly-evolving enterprise. As attacker tactics get more sophisticated, ATA helps you adapt to the changing nature of cyber-security threats with continuously-learning behavioral analytics.

- **Focus on what is important with a simple attack timeline.** The constant reporting of traditional security tools and sifting through them to locate the important and relevant alerts can get overwhelming. The attack timeline is a clear, efficient, and convenient feed that surfaces the right
things on a timeline, giving you the power of perspective on the who, what, when, and how. ATA also provides recommendations for investigation and remediation for each suspicious activity.

- **Reduce false positive fatigue.** Traditional IT security tools are often not equipped to handle the rising amounts of data, turning up unnecessary red flags and distracting you from the real threats. With ATA, these alerts happen once suspicious activities are contextually aggregated to its own behavior, as well as to the other entities in its interaction path. The detection engine also automatically guides you through the process, asking you simple questions to adjust the detection process according to your input.

**Device management**

Mobility is the new normal. Because of this, managing mobile devices such as phones and tablets has become essential for most organizations. Managing the devices themselves, commonly called mobile device management (MDM) is important, and so is managing the applications on those devices, known as mobile application management (MAM).

Mobile devices became popular before the rise of cloud computing, and so traditional MDM and MAM solutions run on-premises. As long as the remote applications users accessed from these mobile devices also ran on-premises, this made sense. Today, however, those remote applications are at least as likely to run in the cloud. Yet if your device management solution still runs on premises, you’re commonly required to route communications between devices and applications through on-premises servers (Figure 8).

![Figure 8: Traditional solutions for MDM and MAM often require communication between mobile devices and cloud applications to go through an on-premises bottleneck.](image)

As the figure shows, a device management solution typically deploys management polices to the devices being managed (step 1). Once those policies are in place, apps on the managed devices can access on-premises and SaaS applications. All of that communication, even to SaaS applications, is commonly routed through the on-premises device management solution.
This approach raises some obvious concerns, including performance and scalability. Why limit the speed of interaction between devices and cloud applications to what an on-premises device management solution can handle? Why require your own IT organization to worry about scaling to do this? Moving device management—both MDM and MAM—to the cloud makes much more sense (Figure 9).

![Diagram of device management with cloud applications](image)

**Figure 9:** By providing MDM and MAM as a cloud service, Microsoft Intune provides a simpler, more sensible approach.

With this approach, exemplified by Microsoft Intune, mobile devices still receive policies deployed by the device management solution (step 1). Once these policies are in place, however, apps on those devices can communicate directly with both on-premises and cloud applications (step 2). The on-premises bottleneck is gone.

Moving device management to the cloud has other benefits too. For example, rather than requiring you to run and manage your own servers and software for device management, Microsoft Intune does this for you. Think about the challenge of updating the device management software. iOS, Android, and Windows 10 are all updated frequently, often in ways that affect how those devices are managed. This requires updates to the device management software that take advantage of these new features. With on-premises device management, MDM and MAM vendors must ship new patches to every customer, which takes time. Every customer—including you—must then install and test these patches, which takes more time. Multiply this by the number of different mobile operating systems you’re supporting, and the result is clear: you’ll probably never be current.

With device management in the cloud, this problem goes away. When a new version of iOS, as an example, rolls out, Microsoft itself updates Intune to support whatever changes this update brings. You’re always up to date, and you never need to worry about installing patches.

Microsoft Intune also provides other features and benefits. They include the following:

- **Mobile application management without enrollment** - gives you the flexibility to control Office Mobile and other applications on your users’ iOS, Android, and Windows devices without enrolling the device on Intune (we’ll look more closely at what this means later).
• **Multi-identity management** – enables users to access both their personal and work accounts using the same Office mobile apps while only applying the MAM policies to their work account, providing a seamless experience while employees are on the go.

• **Selective wipe of corporate data** – removes apps, email, data, management policies, and networking profiles from user devices remotely while leaving personal data intact.

• **A unified endpoint management solution** – lets you manage your organization’s mobile devices and desktop PCs from the same administrative environment. This is made possible through the tight integration Microsoft has created between Intune and System Center Configuration Manager.

• **Self-service capabilities** – enable users to perform tasks like updating passwords and joining and managing groups via a single portal to help save your IT helpdesk time and money. This applies across all iOS, Android, and Windows devices in your mobile ecosystem.

**Information protection**

Who is allowed to access a particular document? What kind of access is permitted: reading, writing, or something else? How do you make sure the data is protected from birth and that the protection travels with the data wherever it goes? Providing this kind of control was important even before the advent of mobile devices and cloud computing. In a mobile-first, cloud-first world, with users and applications spread all over the planet, it matters even more.

This style of information protection was traditionally provided by on-premises solutions. For example, Microsoft has offered what’s now called Active Directory Rights Management Service (RMS) for a number of years.

Yet offering this kind of protection with an on-premises solution has limitations (Figure 10).

---

**Figure 10**: Relying on an on-premises technology for information protection requires manually configuring point-to-point connections for identity management between individual organizations.

Suppose that two organizations, A and B, wish to share a protected document. Maybe only a certain group of people in each company are allowed to read this document, so an attempt to open it must be verified by an information protection service. This problem can be solved with an on-premises information protection technology, but achieving this requires setting up a point-to-point relationship between the identity management solutions that the information protection technologies relied on.
Going to this much trouble just to share protected documents often wasn’t seen as practical, and so sharing documents across organizational boundaries wasn’t as secure as it should have been. However, with the new Azure Information Protection solution running from the cloud, doing this gets much simpler (Figure 11).

As the figure shows, the two organizations are no longer required to set up direct connections to each other. Instead, they can each connect to the cloud services—Azure AD and Azure Information Protection—just once. No matter how many other organizations yours might share documents with, you each need to connect only once to the cloud services. With this model, the complexity that bedeviled cross-organization sharing of protected documents goes away.

Azure Information Protection also provides other benefits, including the ability to:

- **Classify, label and protect data** – at the time of creation or modification. Use policies to classify and label data in intuitive ways based on the source, context and content of the data. Classification can be fully automatic, user-driven or based on a recommendation. Once data is classified and labeled, protection can be applied automatically on that basis.

- **Provide users with simple, intuitive controls** – to protect data while staying productive. Data classification and protection controls are integrated into Office and common applications. These provide simple one-click options to secure data that users are working on. In-product notifications provide recommendations to help users make the right decisions.

- **Gain visibility and control over shared data** - document owners can track activities on shared data and revoke access when necessary. IT can use logging and reporting to monitor, analyze and reason over shared data.

- **Protect data whether it is stored in the cloud or on-premises** - and choose how your encryption keys are managed with Bring Your Own Key options.
Administrative challenges

As companies scramble to keep up in a mobile-first, cloud first world, many are left with too many point solutions and not enough resources to manage them. Products are often hard to set up, integrate and maintain, and an ever-evolving attack landscape can quickly outdate protection. Compounding these challenges are limited IT budgets. Prioritizing these budgets to tackle new security challenges is no easy task for many of our customers.

EMS provides an integrated set of solutions that are designed to work together with your on-premises investments, avoiding the need for costly and complicated integration efforts across point capabilities. To make deployment even easier, EMS comes with FastTrack – a Microsoft service that includes best practices, tools, resources, and experts committed to make your experience with EMS a success. As a cloud solution, EMS also takes the worry out of scale, maintenance, and updates.

Scenarios: What EMS can provide

Taken individually, there’s a compelling argument for doing identity management, information protection and device management in the cloud. But the argument gets even stronger when these cloud services are used together, as they are in EMS. To show why this is true, we’ll look at four scenarios:

1. Identity-driven security
2. End-to-end information protection
3. Managed mobile productivity
4. Streamlined deployment and management

Identity-driven security

As we have seen, Identity is central to everything that EMS does. But what happens if an attacker is able to compromise Anna’s identity? Suppose she chooses a guessable password or someone cons her credentials out of her through social engineering. This is exactly the kind of attack used in several recent high-profile breaches—it’s a real threat.

Detecting this type of threat requires identity-driven security, something EMS provides in a number of ways. Let’s start with an example of how it protects at the front door. For example, Azure AD can detect potentially invalid sign-ons, then warn your security staff about these risks (Figure 12).
Suppose an attacker purchases Anna’s sign-on name and password from a hacker site, then uses these to sign onto your organization (step 1). Because Microsoft monitors these sites, Azure AD knows that Anna’s credentials are available on the black market. When it sees this sign-on, Azure AD can warn your security staff about this situation (step 2). Or suppose another attacker signs on with Anna’s credentials, but the client device that sign-on comes from is infected with malware (step 3). Azure AD can issue a warning to your security staff about this as well (step 4).

The ability to detect these kinds of sign-on threats is a unique capability of Azure AD, and it depends on Microsoft’s broad cloud resources. Information that Microsoft gets from attacks on any of its cloud offerings—Office 365, Azure, Xbox, and others—is fed into Azure AD to help make your enterprise more secure. It’s also possible to take action when this kind of problem is detected. For instance, once your security staff learns that Anna’s credentials have been stolen, it might require her to change her password and then use multi-factor authentication for all sign-ons.

Azure AD reports other unusual behavior as well. If Anna signs onto her account from Los Angeles, California, then five minutes later signs on from Lima, Peru, something is clearly wrong—Azure AD will report this. It will also flag other out-of-the-ordinary behavior, such as using an Android tablet for the first time when Anna normally uses an iPad. And, of course, Azure AD reports on the usual concerns, such as exceeding a set number of sign-on attempts.

Yet suppose an attacker manages to get by all of these barriers. How can this kind of attack be detected once the sign-on has happened? The answer depends on recognizing that an attacker using a stolen identity behaves differently than the rightful owner of that identity. ATA can detect these differences, then alert your security staff to the problem (Figure 13).

---

**Figure 5:** Azure AD can warn about several kinds of sign-ons by attackers.

---

63% of confirmed data breaches involve weak, default, or stolen passwords

— Verizon 2016 Data Breach Report
Figure 13: With ATA, EMS can detect and flag suspicious activity, alerting security staff when an account might have been compromised.

Suppose that Anna signs onto Azure Active Directory (step 1), then works her typical daytime schedule. Anna is part of your human resources department, so she mostly accesses your organization’s HR application and data (step 2). Now suppose an attacker signs on as Anna using her stolen credentials (step 3). Will he also access mostly HR resources during your normal work day? Almost certainly not; instead, the attacker will access other applications and other kinds of data. He’ll also likely do this at different times, if only because he might be working from a time zone on the other side of the world (step 4).

This variation in behavior can be detected by ATA. By monitoring traffic in and out of your on-premises Active Directory, then using machine learning technology to analyze this traffic, ATA can quickly learn the usual access patterns of your users. When a user deviates from those patterns, as Anna has here, ATA can alert your security staff to the possible breach (step 5).

Once an attacker has penetrated an organization, he commonly lurks for months looking for opportunities. He’s often not discovered until he’s already exploited these opportunities (and maybe not even then). Using ATA together with the reporting services provided by Azure AD can help you detect and stop these attacks before they damage your business. With Azure AD in the cloud and ATA on-premises, EMS provides a comprehensive solution for identity-driven security.

Of course, there are other scenarios where a security breach is not malicious, but done accidentally by an internal user. This is where EMS technologies like Cloud App Security work to protect data. For example, with CAS, you can set policies that automatically scan the cloud apps that your users access for sensitive content like credit card numbers or medical records. When CAS finds this data, it gives you the tools to identify who uploaded or accessed the data and take action such remove permissions, quarantine the user, and so on.

In the next section, we’ll explore other ways that EMS helps to protect data even before it has been accidentally distributed to unauthorized users or applications.
End-to-end information protection

Once Anna has access to Exchange Online, she’ll start receiving her corporate email. Even though she’s using her iPad to do this, perhaps from an airport lounge or some other public place, her mail contains information that your organization needs to protect. You need a way to stop her from (accidentally or intentionally) sending this information to outsiders, such as through email or copying to unapproved applications. You need end-to-end information protection. EMS can provide this through Azure AD, Intune, and Azure Information Protection all working together (Figure 14).

Suppose Anna receives a corporate email with an attached Excel spreadsheet (step 1). She opens this attachment using the Excel mobile app on her iPad, then tries to copy and paste data from the spreadsheet to the iPad’s built-in Notes app. With EMS in place, this attempt will fail (step 2).

The reason it fails is that Intune separates managed apps on her iPad from personal apps. As the figure shows, Anna’s Office mobile apps are all marked as managed, which means that data from these apps can’t be copied to non-managed apps. In this example, the Paste option just won’t appear when she tries to move data from the Excel spreadsheet to the iOS Notes app. She’s free to move information between the managed apps, such as from an Excel spreadsheet to a Word document, but that’s all. And while it’s not shown in the figure, managed apps can also be acquired from other software vendors or be custom-built by your organization—you’re not limited to using Microsoft apps.

Only Microsoft can provide this kind of information protection for the Office mobile apps on iPads and Android devices; no other MAM vendor is able to do it. And if Anna wants to use the Office mobile apps for both business and personal work, she’s free to do this—all she needs to do is sign on with a different

33% of user breaches come from user error.
– VansonBourne, February 2014

Figure 14: EMS protects corporate information by letting it be used and copied only within a managed environment and by embedding access controls directly into encrypted files.
Protecting and empowering your connected organization

Intune will make sure that corporate policies get applied to corporate data, while leaving personal data alone.

The information protection that Intune provides for mobile devices is essential, but it’s not enough. Suppose that Anna receives an email with another attachment containing confidential corporate data (step 3). She might never open this on her iPad, but suppose she accidentally forwards it to an outsider—what then? Or what if the attachment was sent to Anna by mistake, and she’s not supposed to have access to it? Providing end-to-end information protection requires addressing these concerns.

Azure Information Protection was created to solve problems like these. If the attachment Anna received is protected by Azure Information Protection, it’s encrypted, which means that no software can open it without first contacting this cloud service (step 4). Azure Information Protection uses Anna’s identity, provided via Azure AD, along with information in the protected document itself to determine what access rights she has. She might be able only to read this document, for instance, or to read it and modify it, or to do other things, based on what the document’s creator has allowed.

Along with controlling what Anna can access, Azure Information Protection can also control what Anna can forward, providing yet another powerful tool to prevent data leakage. For example, administrators can create policies that can automatically detect sensitive data (such as credit card information) and automatically apply protection (such as Do Not Forward). At the same time, Azure Information Protection makes it easy for users to apply their own protection, with convenient control built right into the Office ribbon.

Azure Information Protection keeps data safe wherever a document might be. Intune protects information when it’s accessed on mobile devices. These two components, along with the identity information provided by Azure AD, allow EMS to provide true end-to-end information protection.

Managed mobile productivity

Your employees use mobile devices for both personal and work tasks. While making sure your employees can be productive, you also want to prevent data loss, intentional and unintentional. In addition, you want to have the ability to protect company data accessed using devices even in the case where they are not managed by you.

You can use Intune mobile app management (MAM) policies to help protect your company’s data. Because Intune MAM policies can be used independent of any mobile-device management (MDM) solution, you can use it to protect your company’s data with or without enrolling devices in a device management solution. In this way, EMS gives you the flexibility to manage devices or apps or a combination of both.

To see how Microsoft EMS makes this possible, we’ll start with a managed device scenario. In this case, we’ll looking at an example of how a current user—let’s call her Anna—adds a new iPad to your corporate network (Figure 15).
Identity is the foundation for everything else, so the process starts with Anna signing on with Azure AD (step 1). The iPad she’s using might be her own, or it might be one that your organization has provided for her. In either case, the first thing she does after signing on is try to access a SaaS application. In this example, that application is Exchange Online, part of Office 365—Anna wants to access her corporate email. But because her new iPad is currently unmanaged, this request is redirected to Intune (step 2).

Intune then establishes a management relationship with Anna’s iPad (with her permission, of course) to allow this device to be managed, applying whatever policies are defined for iPads (step 3). For example, your administrators might have specified that being part of your corporate environment requires an iPad to have an unlock password set, to encrypt the corporate data it stores, and have managed email. Defining and applying these policies relies on both Azure AD and Intune.

Now that her device is managed, Anna can successfully access her corporate email (step 4). Before she’s able to do this, Azure AD and Intune work together to make sure that Anna is compliant with another policy: the one defined for this specific application. An Exchange Online policy, for instance, might require requests to come from Intune-managed devices that have applied all available updates. This is an example of conditional access, where a user is allowed to do something only if several conditions are met: the right identity, the right kind of device with the right characteristics, and perhaps more. Conditional access is a powerful feature and it’s only possible when multiple services work together, as in EMS. This synergy is an essential aspect—and a clear benefit—of a unified cloud solution.
Figure 16: EMS also provides the flexibility of mobile application management without enrollment.

While many organizations will want to manage all devices used by employees, there are many scenarios where employees will want to use their own, unmanaged devices while also taking advantage of corporate apps. So how does EMS protect Office app data in these cases? Using the Intune MAM without enrollment feature, organizations can secure data on devices with Office mobile and other apps installed - without the need to enroll those devices in Intune MDM (Figure 16).

This also means that, for customers who already have an MDM vendor, or don’t wish to manage their users’ devices via MDM, they can still protect access to Office and company data. This includes cut/copy/paste restrictions, preventing ‘save-as’, jailbreak detection, PIN requirements and the ability to remote wipe MAM protected data.

Streamlined deployment and management

In this paper, we’ve seen how the cloud-based architecture of EMS simplifies set up and management of solutions for even the most complex mobility security scenarios. But we wanted to take ease of administration even further by adding a service we call FastTrack.

FastTrack is a benefit delivered by Microsoft engineers to help you quickly get started with your EMS deployment. For example, these engineers can create user accounts, move identities to cloud, set up test apps and configure self-service in MyApps site. They can set up user groups and activate rights management for users, including test templates. They can also integrate on-premises System Center Configuration Manager with Intune for comprehensive control of both PCs and mobile devices.

Along with faster deployment, FastTrack also leaves more time for your Microsoft partner to focus on other high-value services related to EMS including customization, remediation, company-wide device setup, user growth, management and enhancement of overall solution.

This ability to provide a comprehensive solution is also what makes EMS an exceptional value. Unlike point solutions available from other vendors, EMS packs everything you need into one, integrated solution, including one account team and one, streamlined licensing structure. And because EMS runs in the cloud, you have less on-premises hardware to purchase and manage for even greater cost-savings.
Summary

Microsoft Enterprise Mobility + Security lets you empower your people to be productive on the devices they love while protecting your company’s assets. By moving what were on-premises services to the cloud, EMS helps your organization be more productive, better managed, and more secure in today’s mobile-first, cloud-first world. And by integrating these services with each other and with their on-premises cousins, it provides a complete solution unlike anything else in the industry today. By deploying EMS, you can make life better for your employees, your business partners, and your customers.