# Protecting and empowering your connected organization

with Microsoft Enterprise Mobility Suite (EMS)

# Contents

## Executive summary

As an IT leader, identity management, device management, and information protection are an important part of what you do. Yet there's a big change happening in all three areas that you might not be aware of.

Traditionally all three of these relied on software that ran inside your own organization. This was a good solution when identities, devices, and information were also largely inside your organization. But today the people who work in your organization take their mobile devices everywhere, and those devices are used to access both on-premises and software-as-a-service (SaaS) applications.

Your users want to access SaaS applications like Office 365, Salesforce.com, and ServiceNow. They also want to access your organization's custom applications running on cloud platforms such as Microsoft Azure and Amazon Web Services (AWS). And they want to do all of this from their Windows 10, iOS, and Android devices, whether they're sitting in one of your conference rooms or waiting in line at Starbucks. This is the cloud-centric, device-centric world that the modern workforce expects.

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 from your own datacenter to the cloud. Doing this lets you provide everything your users expect, while still giving you the protection and control you need. Just as important, the services you choose should be built from the ground up for a mobile-first, cloud-first world. No other approach will work because the problems presented by this world are different from those you've traditionally faced.

These services must also work well together. Without this you can't do things like granting a user access to an application only if she's using a correctly configured device in a known location. And trying to integrate disparate cloud solutions yourself is unlikely to be successful. You need a solution that's designed to work together.

Microsoft Enterprise Mobility Suite (EMS) was created to help you address a transformation to coordinated services. Its three core components—Azure Active Directory Premium, Microsoft Intune, and Azure Rights Management Service—were built from the start as cloud services. They were created to work together, providing an integrated technology family that's unique in the market today. To detect attacks on-premises, EMS also includes Microsoft Advanced Threat Analytics. Using EMS, you can empower your people to be productive on the devices they love while protecting your company's assets.

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.

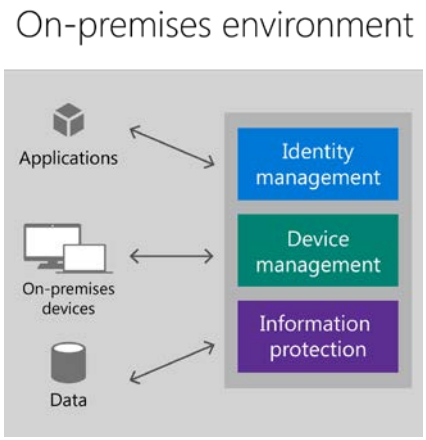


**Figure 1: Identity management, device management, and information protection were once done entirely within an organization's on-premises environment.**

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).

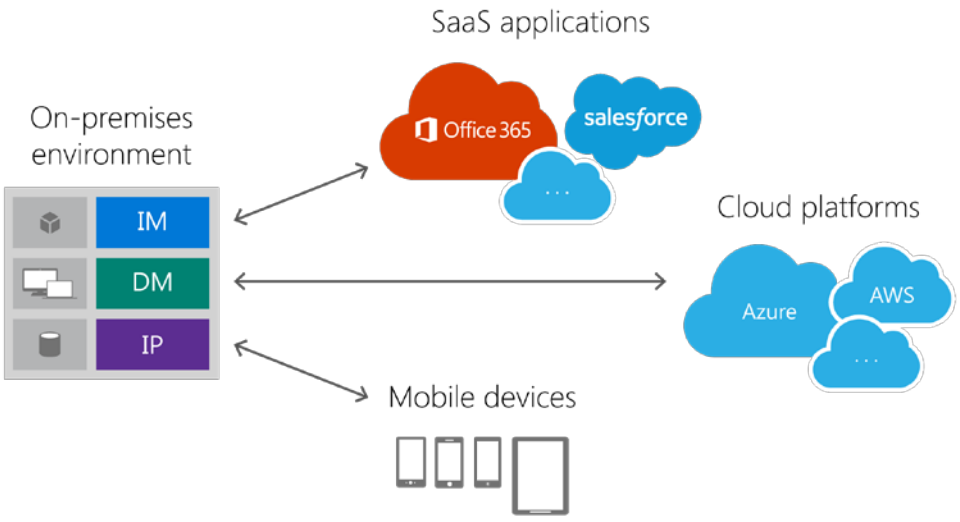


**Figure 2: Today enterprise computing includes SaaS applications, cloud platforms, mobile devices, and perhaps more.**

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. And the information you must protect lives not just inside your firewall but also on those devices and in the cloud.

The traditional approach to doing all of these things, which relied on on-premises technologies alone, no longer works. Instead, your organization should move to a cloud-based solution (Figure 3).

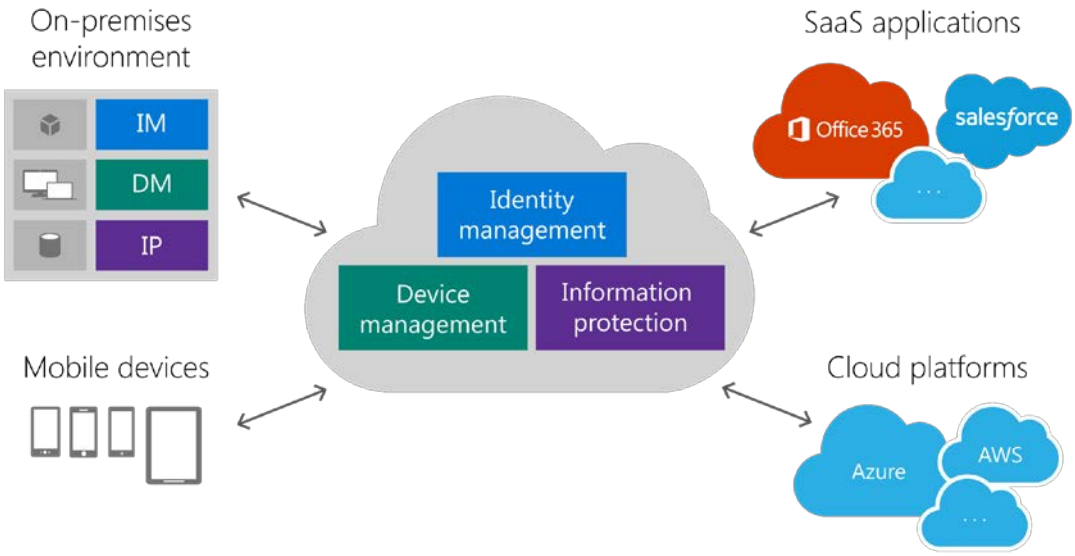


**Figure 3: Today the core technologies for identity management (IM), device management (DM), and information protection (IP) should run in the cloud.**

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 the *Enterprise Mobility Suite (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, enabling things such as conditional access, where a user's ability to access information can be gated based on who the user is, where he's located, what device he's using, and other factors.

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.

## Examining the change: why is it happening?

Managing identity, managing devices, protecting information: none of these is simple. To understand the issues, and to grasp why cloud 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.

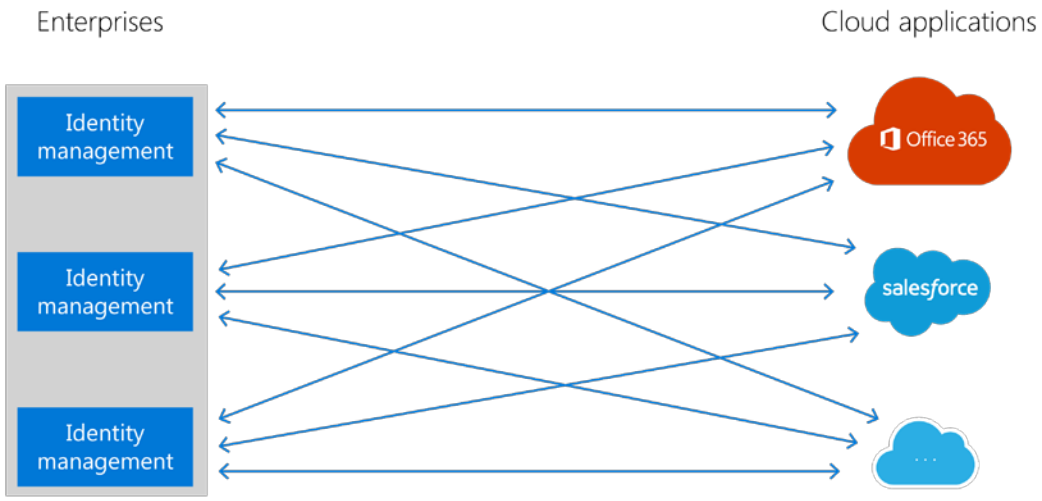


**Figure 4: Creating a direct connection between every organization's identity management solution and every SaaS application would quickly become too complex to manage.**

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).

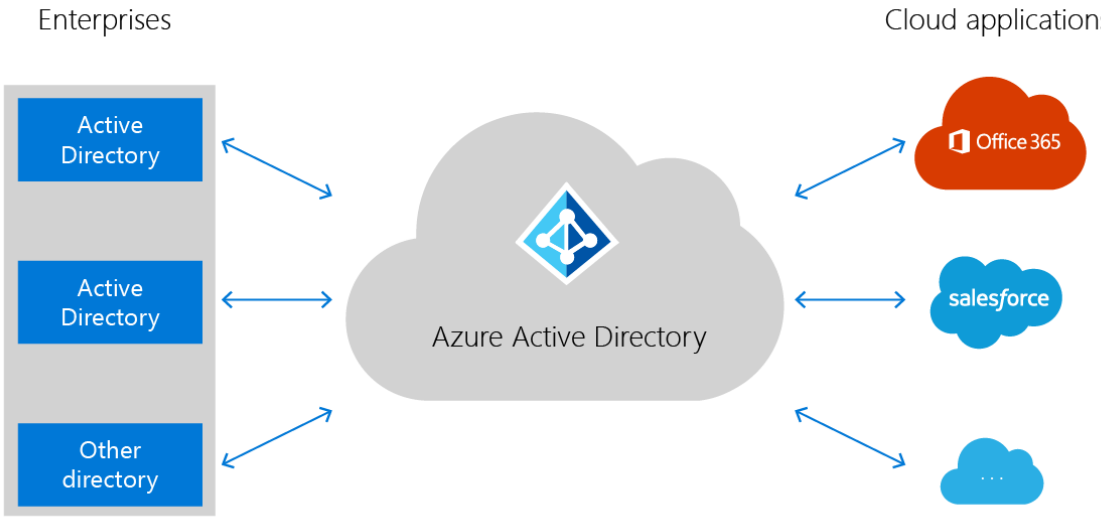


**Figure 5: Cloud-based identity management with Azure Active Directory greatly simplifies managing single sign-on to SaaS applications.**

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.

More than 80 percent of employees admit to using non-approved SaaS applications in their jobs
*– Stratecast, Frost & Sullivan*

"The hidden truth behind shadow IT: Six trends impacting your security posture," November 2013

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

- Support for multi-factor authentication (MFA) which lets you require your users to provide both a password and something else, such as a code sent to their mobile phone, to sign on
- A tool for discovering which SaaS applications your employees are actually using
- Secure remote access to on-premises applications without using a virtual private network (VPN)
- Integration with some of the most popular SaaS applications, including Salesforce, Workday, and others that goes beyond SSO—for example, you can automatically add a user to these applications when a new user is added to Azure AD

## 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).

Fifty-two percent of information workers across 17 countries report using three or more devices for work
*–Forrester Research*

"BT Futures Report: Info workers will erase boundary between enterprise & consumer technologies," February 21, 2013

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 6).

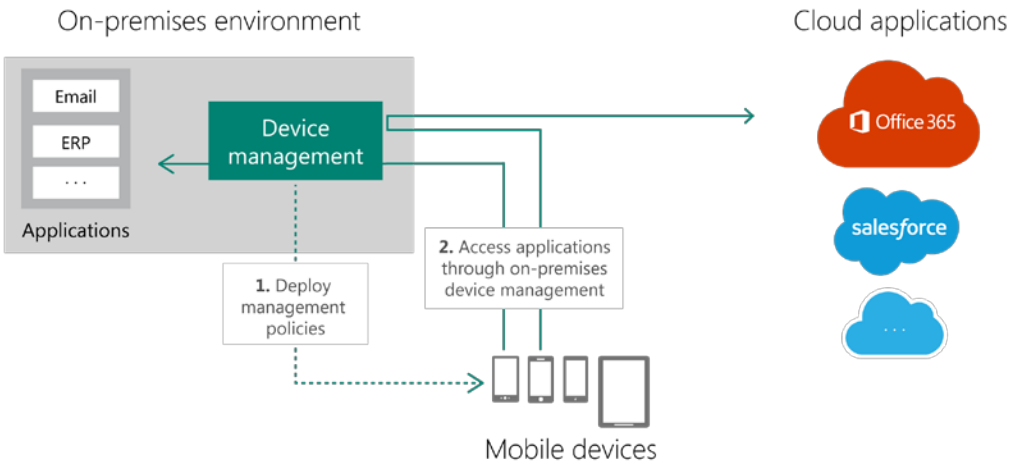


**Figure 6: Traditional solutions for MDM and MAM often require communication between mobile devices and cloud applications to go through an on-premises bottleneck.**

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 (step 2).

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 7).

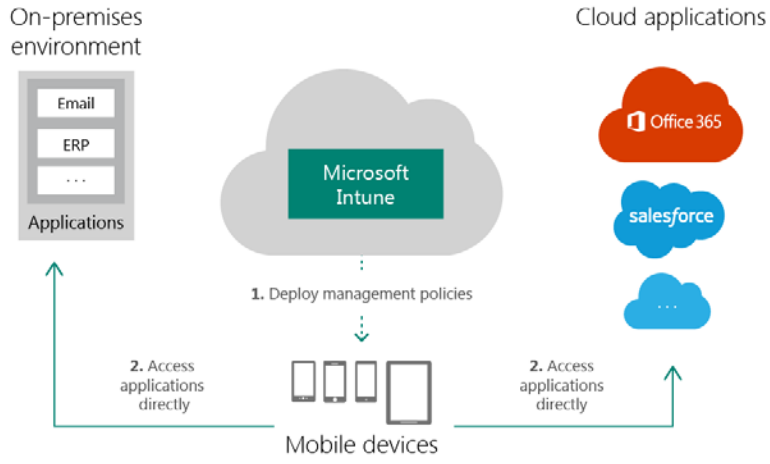


**Figure 7: By providing MDM and MAM as a cloud service, Microsoft Intune provides a simpler, more sensible approach.**

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. Similarly, 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 benefits. They include the following:

- The unique ability to effectively control Office mobile applications on your users' iOS, Android, and Windows devices (we'll look more closely at what this means later)
- The ability to remotely delete all corporate information from a user's device while leaving his personal data intact—for example, you might do this when an employee leaves your organization or when his device falls out of compliance.
- A unified endpoint management solution that lets you manage your organization's mobile devices and desktop PCs from the same administrative environment; this relies on the tight integration Microsoft has created between Intune and System Center Configuration Manager

## 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 for a number of years. Yet addressing this problem with an on-premises solution has limitations (Figure 8).

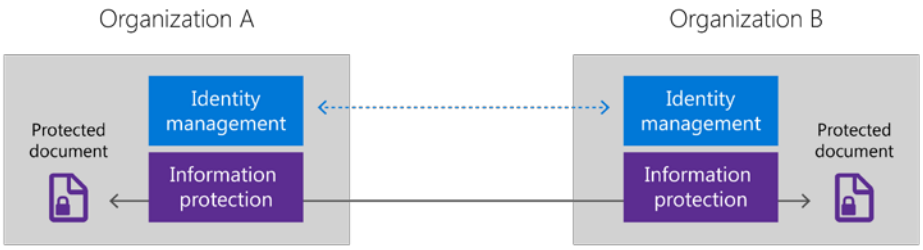


**Figure 8: Relying on an on-premises technology for information protection requires manually configuring point-to-point connections for identity management between individual organizations.**

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. With cloud solutions, however, doing this gets much simpler (Figure 9).

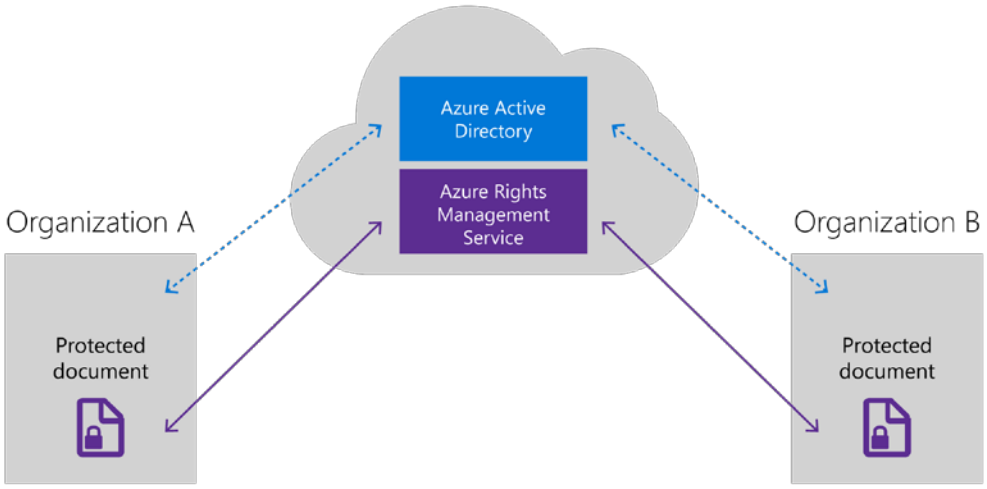


**Figure 9: Using a shared cloud solution for identity management and information protection greatly simplifies controlling access to documents.**

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 Rights Management Service (RMS)—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 RMS also provides other benefits, including:

- Support for custom policy templates, which allow defining policies for sharing protected documents—for example, an organization might define a template that restricts access to a particular document only to people in its marketing group
- Document tracking that monitors successful and unsuccessful access attempts by recipients of a protected document, giving document owners insight into how the document is used (or abused); it also provides the ability to revoke access to a document
- The option to encrypt documents using your own key rather than one provided by Microsoft

### Detecting attackers before they strike: Advanced Threat Analytics

Important parts of your infrastructure—identity management, device management, and information protection—are moving to the cloud. But 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 all the relations between users, devices, and resources. For example, ATA keeps track of the devices employees typically use, which resources they access (including applications), and the times this access occurs. If a user unexpectedly begins accessing atypical applications from different devices at odd times, ATA will warn your security staff, which can then investigate the situation. An attacker may have assumed this user's identity, probably by stealing his or her username and password.

Rather than wait for an attacker to damage your organization, ATA helps you detect attacks much earlier. This offering also helps your organization in other ways, such as detecting known malicious attacks. And while ATA runs on-premises, it can be licensed as part of EMS.

## Scenarios: what EMS can provide

Taken individually, there's a compelling argument for doing identity management, device management, and information protection 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 three scenarios:

- Managed mobile productivity
- End-to-end information protection
- Identity-driven security

### Managed mobile productivity

We use mobile devices because they make us so much more productive. But if these devices can't be effectively managed, the trade-off isn't worth it; the risks are too great. Because of this, you should think about improved productivity and effective management as a single goal. What you need is managed mobile productivity.

To see how Microsoft EMS makes this possible, we'll start by looking at an example of how a current user—let's call her Anna—adds a new iPad to your corporate network (Figure 10).

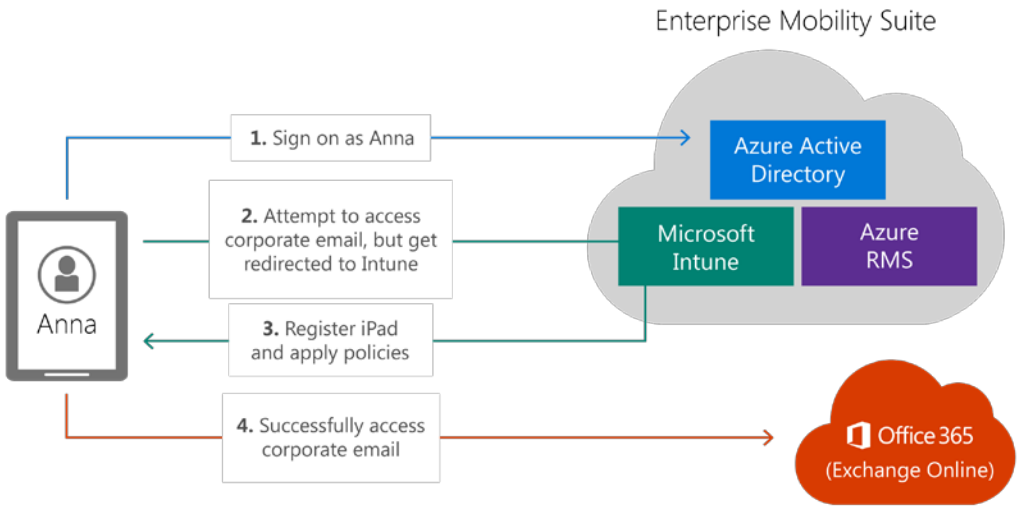


**Figure 10: EMS can automatically enroll a device, then enforce policies for accessing applications.**

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 re-directed 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.

## 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 RMS all working together (Figure 11).

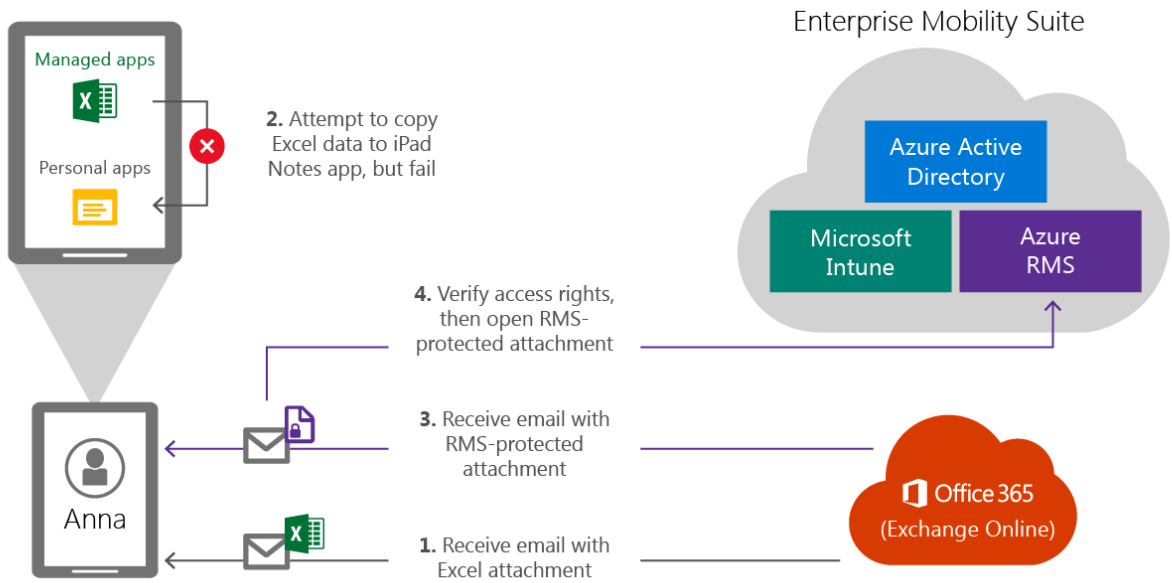


**Figure 11: EMS protects corporate information by letting it be used and copied only within a managed environment and by embedding access controls directly into encrypted files.**

Sixty-one percent of workers mix personal and work tasks in their devices *–Forrester*

"BT Futures Report: Info workers will erase boundary between enterprise & consumer technologies," February 21, 2013

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 identity. 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 accidently 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 RMS was created to solve problems like these. If the attachment Anna received is protected by Azure RMS, it's encrypted, which means that no software can open it without first contacting this cloud service (step 4). Azure RMS 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.

Azure RMS protects information 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.

## Identity-driven security

Everything described so far relies on identity. Intune uses Anna's identity to decide which policies to apply to her device, and Azure RMS decides what access she has to a protected document based on her identity. Identity is central to everything that EMS does.

> Seventy-five percent of network intrusions exploited weak or stolen credentials
> *–Verizon 2013 data breach investigation report*

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. For example, Azure AD can detect potentially invalid sign-ons, then warn your security staff about these risks (Figure 12).

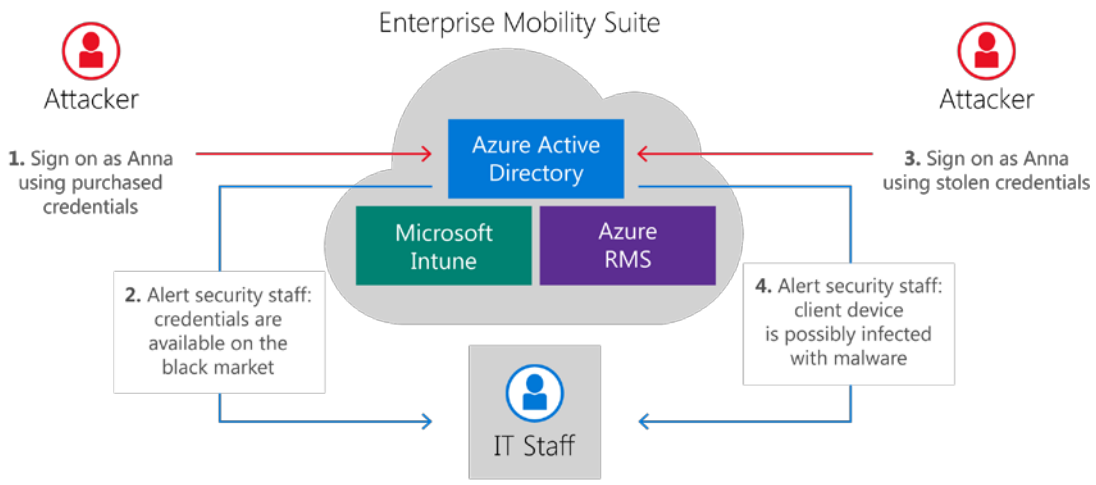


**Figure 12: Azure AD can warn about several kinds of spurious sign-ons.**

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 spurious sign-ons 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).

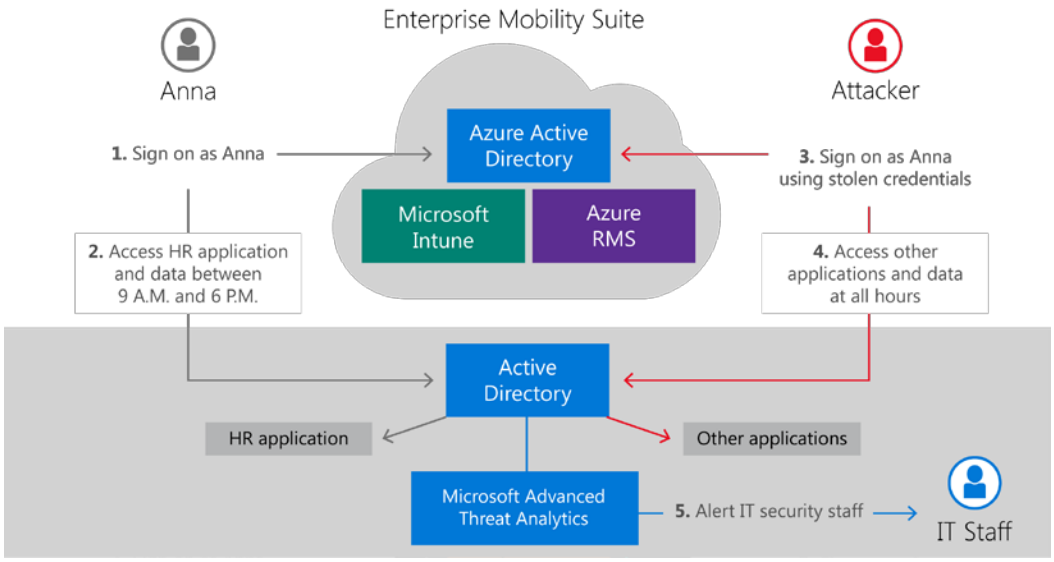


**Figure 13: With ATA, EMS can detect and flag suspicious activity, alerting security staff when an account might have been compromised.**

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.

## Summary

Microsoft Enterprise Mobility Suite 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.