Your Guide to EMS

Contents

Section 1: The Changing Digital Landscape and EMS E3
Section 2: Migration and Azure AD Premium
Section 3: Mobile Devices and Intune
Section 4: Protecting Your Data
Section 5: Threat Prevention and E5
Section 6: How Applied Tech can guide you
The digital landscape has changed. It used to be that if you wanted to access most company data, you had to be in the office at a PC owned by the company, or you had to leverage technologies such as VPN or GoToMyPC, usually from another PC or laptop. The data generally stayed within the secure confines of the company’s own network, even when accessed remotely. Some users may have had their My Docs synced locally to their laptop, or kept some files on a thumb drive, but the bulk of the files resided on company owned servers. As long as there was a good firewall in place and configured correctly, anti-virus software was used throughout the network, and the building was physically secured, there was minimal risk of data being compromised.

Over time it became normal to have constant access to company email via smart phones, and more recently tablets. The use of corporate email on these new mobile devices opened a new window of risk in regards to data being compromised, but it was a risk most companies didn’t give much thought to. This is especially true in environments where employees are allowed to use their own devices, rather than company owned devices, to access email. Some companies invested the time and financial resources to implementing a Mobile Device Management platform to help mitigate this risk, but the majority did not. Also, to access most shared files and applications, you still had those previously mentioned limitations which kept that data more secure.

Today, the current trend is mobility, and it’s now possible (and expected in many organizations) to provide access to all company data and applications from anywhere, anytime, and on any device. Users are frequently leveraging their own personal devices to access that data, rather than company owned and controlled devices, and there has been push-back in terms of how much control a company should be allowed to exert over those personally owned devices.

This trend towards mobility is great in that it removes the tether to the office, making it possible to work effectively from anywhere with a stable internet connection. It does, however, introduce many security challenges that most organizations either aren’t aware of, or don’t yet have systems in place to address.

Are the devices used to access company data configured securely? What happens if the device is lost or stolen, can you be assured that unauthorized access of the data on the device will be prevented? There
are protections built into mobile devices such as data encryption and various screen locking options, but unless you have a robust Mobile Device Management solution in place, these protections are only enabled if each user chooses to do so. There’s also no way to prove these protections were in place if devices are lost or stolen, which can be especially troublesome if the device may have contained PHI or financial data and you’re in a regulated industry.

Today’s challenges

Do you know which devices are being used to access company information, by who, and from which locations? What if an employee’s credentials are compromised, can you still ensure your data is safe? A strong reporting engine can allow you to generate reports showing failed logins or logins from unknown locations. You also have access to reports showing which credentials are known to have been compromised and leaked, and logins that don’t fit a user’s normal sign-in activity patterns. Having this type of information readily available can go a long way towards securing company data and allows for a quicker response and more pro-active approach in the event credentials are compromised.

If an employee leaves the organization, how can you be sure they aren’t taking all of the company data with them on their mobile device? Are you currently able to sandbox company data on all employees’ mobile devices, which then allows for selective wiping of only company data, while leaving their personal data fully intact? This ability allows for a BYOD (bring your own device) scenario in which IT staff can secure company data while being much less intrusive from the end user’s perspective.

Organizations are also leveraging an ever-increasing number of web-based applications, also commonly referred to as Software-as-a-Service (SaaS) or Cloud offerings. This saves the IT department from having to manage and maintain local infrastructure to provide these services, however many of these SaaS applications don’t easily tie into your local Active Directory environment, which means that each application brings with it another set of credentials for the employees and IT staff to manage. This can lead to poor password security habits by the employees, such as using the same password across
In the past, trying to solve these diverse challenges would have been very expensive and time consuming. In many cases, the overall expense would have made it prohibitive for Small to Medium sized businesses to implement the solutions that did exist in the market. Now Microsoft has provided a cost-effective way of dealing with these challenges (and more) as well as providing a consistent mobile experience for employees by bundling multiple products into their Enterprise Mobility + Security (EMS) E3 offering. This bundled offering is available at a significant cost savings compared to purchasing each solution individually. EMS is also natively part of the Office 365 and Azure platforms, which allows for a more seamless integration with services like Exchange Online and SharePoint Online than you would find with other 3rd party products.

In upcoming sections, I will introduce you to each of the products included with EMS E3 and explain the benefits each of them can bring to your business. In my next post, the first product I will cover will be Azure Active Directory Premium.

Section 2: Migration and Azure AD Premium

In the last section, I introduced you to Microsoft’s Enterprise Mobility + Security E3 offering, which is a bundle of various technologies aimed at making mobility secure, while also providing a more consistent mobile experience for employees. Now, I’ll discuss the first technology you get access to when purchasing EMS E3, which is Azure Active Directory Premium.

When companies start to migrate services to Office 365, such as Exchange or SharePoint, they usually continue to maintain an on-premises server infrastructure for a period of time. In order to make identity management as easy as possible for employees, a synchronization service called Azure AD Connect is used to keep local user names and passwords synced to the directory in Office 365, which leverages the Azure service behind the scenes.
One of the most immediate impacts Azure AD Premium provides is that it enables employees to perform self-service password resets and account unlocks from anywhere with an internet connection. They can perform these actions on any Office 365 related website and it’s automatically synced back to the on-premises Active Directory. This is much more efficient in that employees no longer have to rely on the Help Desk to perform these actions, or have direct access to certain systems in the on-premises environment, they can do it on-demand wherever and whenever they need to.

Another great feature of AAD Premium is the ability to provide single sign-on to thousands of cloud based apps, as well as on-premises web based apps. This is done through a simple to use dashboard that is customized for each user to include only the apps that are published to them. This provides a consolidated starting point for all employees to access the applications they need to get their job done, and can help new employees hit the ground running, rather than trying to remember where to find each application they might need.

Many cloud apps have support for true SSO (single sign-on) using the employee’s synced AD credentials. This means there is no separate account to manage, and in many cases a brand new account can be automatically provisioned based on default settings the first time a user accesses an app. This increases efficiency, allows the employee to immediately access an application the first time they need it, and offloads effort from the IT dept. For the apps that don’t support true SSO it can act as a password vault for credentials the employee has access to, or the credentials can be masked from the employee by the IT Dept. while still allowing them to access services using those credentials. This allows for the use of much stronger and unique passwords for each individual app, while for day-to-day use the employee only needs to remember their AD credentials.

An additional benefit of requiring employees to access cloud based apps via their dashboard is that access to these published SSO cloud apps can be controlled by various access rules. These rules can do things such as block access to the application when not on a trusted network, require MFA when not on a trusted network, require MFA all of the time, or only allow access from devices marked as compliant. These rules are configured on a per app basis, which means you can tighten up security for apps that
contain highly sensitive data, while easing access to apps that aren’t as critical or don’t contain sensitive data.

Another benefit on the security front is that AAD Premium allows access to the advanced Azure Multi-Factor Authentication product. This can be enabled on a per-user basis, which provides the flexibility to add this feature only for users who have access to the most sensitive data, or to enable it for all employees within the company. Azure MFA requires the user to not only have the correct username and password, but also access to a trusted device to prove account ownership. For most users this trusted device will be a smartphone or tablet, however it can also be any phone number they have consistent access to. This means that even if an employee’s account is compromised, access to the company data will be denied. Given the ever increasing amount of phishing scams, keylogging malware, and database breaches, this feature is critical when it comes to truly securing your data.

Some other security features include advanced reporting and fraud alerts. With the advanced reporting feature, 30 days of reports are available for many different types of activities. Some of these are irregular sign-in activity, sign-ins from multiple geographies, users with leaked credentials, and password resets. These types of reports can help identify security issues before they turn into actual breaches and compromising of data. The automated fraud alerts can let the IT Dept. know immediately if compromised credentials are used to access any MFA protected systems. As soon as the employee denies the login, an alert is sent to pre-configured email addresses regarding the unauthorized access.

That is a lot of functionality, and I’ve only covered one of the four technologies that make up EMS E3! Next time I’ll discuss Microsoft Intune, which can be used for Mobile Device Management and even better, Mobile Application Management.

Section 3: Mobile Devices and Intune
In the last section, I covered the first product, Azure AD Premium. In this section, I will continue discussing the technologies that are included when purchasing Microsoft’s Enterprise Mobility + Security (EMS) E3 offering as well as Microsoft Intune, which includes both Mobile Device Management (MDM) and Mobile Application Management (MAM).

Employees accessing company resources and data via mobile devices has become standard in today’s workplace. These devices might be smartphones or tablets, most commonly running either an Android or Apple iOS operating system. All of these devices contain features that enhance security of the device, such as screen locking and data encryption. However, by default, these settings are turned off, and many users choose not to enable them for convenience sake. This can lead to significant security holes that may allow some or all the company’s data to be compromised if the device falls into the wrong hands.

Imagine the scenario where an employee has their Exchange mailbox synced to their phone, maybe they have the OneDrive for Business app installed so they can access all their personal and some shared files on the go, and they’ve recently signed into SharePoint online from a browser on the device to access other company files. Now they forget their phone in a restaurant, the back of a cab, or it just falls out of their pocket and they don’t notice. If they don’t have a screen lock configured, anyone that finds that phone now has complete access to all the company data that employee’s permissions allow them to access. If you’re in a HIPAA regulated industry, you’ve now potentially had a very expensive data breach that could cost your company thousands, and sometimes millions of dollars. Also, if data encryption is not enabled, even with a screen lock in place a determined individual could still access most of the information on the device that was lost or stolen. This is just one example of the countless ways data could fall into the wrong hands if the proper security precautions are not taken when it comes to mobility.

Microsoft Intune provides MDM capabilities that can enforce company policies on mobile devices, and block access to company data from devices that aren’t in compliance with these policies. Once a device is registered with Intune, there are a couple of different things that can happen, depending on how the
Intune service is configured, and which security group the employee signed into the device is a member of. It’s possible to enforce and automatically configure certain settings on the device, as soon as it’s registered. This is the most “intrusive” form of MDM if your company has a bring your own device (BYOD) policy, which means employees can use their own personal phones or tablets to access company information. As soon as the device is registered the employee can be forced to configure a screen lock of some sort, device encryption can be enabled, and a bunch of other settings specific to the mobile device’s operating system can be set based on company policy.

A slightly less intrusive method of leveraging MDM still requires the device to be registered with Intune, however instead of forcing certain configuration to take place automatically, prompts are used to inform the user that they can only access company data once they’ve enabled certain security settings. As soon as they do so, the device will be considered to be compliant, and they can then access company resources as needed.

MDM also has other benefits in that you can push email or wireless configurations to devices, configure VPN settings, and deploy apps to managed devices. This can be very beneficial if there are large amounts of company owned devices being deployed, and can save significant time by not having to manually configure all of these things before devices are distributed to employees.

Many employee advocacy groups have argued that traditional MDM technology is too intrusive in BYOD environments, and could possibly lead to the loss of personal data on the employees’ devices in the event a device needs to be wiped to protect company data, so Microsoft developed a new solution called MAM and bundled it into Intune. Instead of setting policies and enforcing configurations at the device level, MAM focuses instead on the applications that are used to access company resources, and ensures those are configured in a secure manner. It essentially creates a secure sandbox on the device for the company data to reside in, while leaving all of the employee’s personal data untouched. It also applies policies within these applications based on the user that is logged into the application, so if you have an environment where multiple employees share a tablet, different policies can be enforce for each of them.

With MAM, which is supported on both iOS and Android devices, you can specify which applications you want to control, such as Word/Excel, OneDrive, Outlook, or a web browser, and then you can limit what employees can do with data they are accessing via those applications. You can limit their ability to backup company data to places like iCloud, prevent Save As, prevent data transfer between managed and un-managed apps, etc.…

Security of company data can be greatly increased using MAM without requiring the device to be enrolled in any form of MDM. When configuring the aforementioned application policies, you are also given the option to enable encryption of any data associated with the managed applications, and also to require the employee to set a 4-digit PIN that must be used to access each managed app. This leaves the individual employees free to decide whether they want to enable encryption and screen locking at the device level, while ensuring these features are protecting company data.

Because MAM policies are assigned to specific security groups, they only take effect when employees are signed into the managed applications with their work identity. For example, in Microsoft Word, when signed in with their work ID they might not be allowed to save files locally on their mobile device, or paste data from other apps into the document they are working on. However, if they sign out and
then sign back into Word with their own personal Live ID, they are allowed full functionality of the application as the MAM policies are no longer applied. So the company data remains protected, while allowing them to also utilize the same apps for personal data as necessary.

The final advantage of MAM is that company data can be selectively wiped from the device. This is great in a scenario where the device is lost, but there is a possibility of finding it. Company data can be wiped remotely, while leaving all personal data intact. If the employee finds their device, the company data can be easily retrieved again the next time they sign in, and they’ll still have their personal photos, contacts, apps, etc.

In environments where the absolute strongest security is required on mobile devices, it’s also possible to layer MDM and MAM policies to protect both the device and company data. I believe most organizations that use the BYOD method of handling mobile devices will choose to use only MAM, but it’s nice to know the option exists to further increase security.

In my next post, I’ll be discussing Azure Rights Management, which is another technology included in the EMS offering. Thanks for reading!

Section 4: Protecting Your Data

In the previous section, I covered Microsoft Intune, which provides Mobile Device Management and Mobile Application Management functionality. This section will cover Azure Information Protection Premium P1, which provides ways of protecting company data both inside and outside of your organization.
Azure Information Protection Premium leverages an underlying technology called Azure Rights Management Services (RMS), which integrates with Exchange and SharePoint Online. Connectors can be installed if your company is running the on-premises versions of these technologies, but most companies start leveraging Azure RMS after migrating these workloads to Office 365.

The Azure RMS integration with Exchange allows for a few different ways to protect emails that you may send both internally and externally. The first type of protection is email encryption. Generally, it’s accepted that you don’t want to encrypt every single email message sent, and only use encryption when particularly sensitive data is contained in an email. There are a few different ways to determine what emails will be encrypted when they are sent. The first is to select a specific keyword that employees can add to the subject line which will force the message to be encrypted. This is the most often used method. It’s also possible to create policies that will watch for patterns specific to sensitive information, such as 16 consecutive digits which is probably a credit card number, or the xxx-xx-xxxx pattern of a Social Security Number. When these patterns are detected, a couple of different things can happen. The first is that the message can just be automatically encrypted. The other is that a tool tip can be used in Outlook to inform the user that their message possibly contains sensitive information, and they should consider encrypting it.

The second type of protection offered within Exchange is the ability to assign an Information Rights Management (IRM) template to a message as you send it. When sending externally, you can protect a message so that the recipient can’t forward, print, or copy the content of the email. When sending internally, other templates can be applied to ensure only certain users or groups are allowed access to the email content, even if a message is inadvertently sent or forwarded to the wrong person. You can also control what can be done with the content such as replying, reply all, copy, print, etc.

With IRM and SharePoint, the protection is enabled on a per-library basis. As a file is downloaded from the library, any rights assigned to the library are then embedded into the file, and stay with it as long as it’s outside of SharePoint. There are many rights that can be configured, such as whether the document can be opened in a browser, whether it can be printed, or how long the document can be used outside
of SharePoint before the content expires. That last feature is useful for documents that change frequently, as it forces employees to download an updated version after whatever time interval is chosen.

Azure Information Protection Premium also allows employees to protect any standalone file that is located either locally on their device or in a file share on a traditional file server. In order to add this protection to a file, they must install a small application on their device. Many device types are supported, such as Windows PCs, Macs, iOS, and Android devices. Once the app is installed, any file can have rights management added to it, which will limit the recipient in regards to what they can do with the file and its content. You can also restrict permissions only to certain recipients, even recipients outside of your company by specifying their email address when protecting the file. If the recipient’s own company already uses Office 365 or Azure Active Directory, they will automatically be able to open the protected file. If not, they just need to sign up for RMS for Individuals, which requires them to prove ownership of the email address for which you protected the document. One example of a situation where this is useful is if you’re e-mailing a quote to a potential customer, and want to be sure they aren’t forwarding on your document to a competitor.

When protecting documents, you can also choose to audit access to the document. Each protected file is given a unique website which allows you to track who is accessing the document, and when. It can also show if anyone without permission attempted to access the document and failed, and also if anyone tried to print or change the document. If you find any inappropriate usage of the file, or if circumstances change, you can revoke access at any time. You can also set an expiration on the content, and after this time period expires the recipient will no longer be able to access the content unless you provide them with a new copy of the file with updated permissions.

Azure RMS is certified for compliance and regulatory requirements such as those found in SOC 2 SSAE 16, HIPAA, and PCI DSS Level 1, among many others. If you are in an industry that is affected by any of these requirements, adding Azure Information Protection Premium to your company’s technology stack is a great way to help ensure your employees have the tools they need to keep sensitive information protected.

Section 5: Threat Prevention and E5

An on-premises solution to identify advanced security attacks before they cause damage

Behavioral Analytics
Detection for known attacks and issues
Advanced Threat Detection
In the previous section I discussed Microsoft’s Enterprise Mobility + Security offering, I covered Azure Information Protection Premium P1, which is a product included in the EMS E3 bundle. In this last section, I will be covering Advanced Threat Analytics, as well as briefly reviewing the other technologies you will gain access to if you upgrade to EMS E5.

Microsoft Advanced Threat Analytics is a product that allows you to protect your on-premises Active Directory environment by detecting possible threats much more quickly than what’s been possible in the past at this price point. When a network intrusion takes place, the average time the attackers are in the network before they are detected is over 4 months. In many cases, they may have access for over a year before something amiss is detected, and the attackers are hopefully purged from the network. I say hopefully because during this time, depending on what accounts are compromised, the attackers may have full administrative privileges to many or all systems on the network, which provides opportunities for them to create backdoor methods of gaining access back into the network, even if their primary means of connecting are found and cutoff.

During the time an attacker is in your network, they have access to all data the compromised accounts have access to, and if the initial account is an account with limited privileges, they now have internal access which can make it even easier to compromise accounts with significantly more access to network resources, including Domain or Enterprise Admin accounts. Once they have this type of access, they can now access shared files, databases, and other data storage areas looking for valuable Intellectual Property, HIPAA related information, and financial data, all of which can be used for their financial benefit.

Attackers may also use network resources for other illegal activities, such as hosting files with stolen content such as music or movies, illicit pornography, or as a jumping off point for other hacking activities, essentially using your network to shield themselves from the consequences of their ongoing criminal activities. These activities could create significant legal issues for the company owning these networks, which in the end may be able to be resolved satisfactorily, but not without a significant investment of time and financial resources.

With Advanced Threat Analytics (ATA), a small agent is installed on each domain controller within an Active Directory based environment. This agent watches all authentication related traffic occurring in Active Directory, as well as scanning event logs for any relevant events. Over time, ATA logs all the information it has gathered and starts to develop something called an Organizational Security Graph. This is a map of interactions between entities within the network, such as users, devices, and other network resources like SQL databases.

Once it has developed the Organizational Security Graph, it is then able to identify anomalous behavior occurring within the network. If any activity that looks out of the ordinary occurs, a red flag is raised and an alert is sent to any configured systems, along with having an entry placed on the ATA dashboard. This allows IT staff to react quickly to either verify the threat and remediate it, or to mark it as an allowable activity. Over time, as ATA learns more about the environment, it becomes even better at detecting anomalies while reducing false positives. ATA also relies on security research that is constantly being done to detect activities that match known attacks and security weaknesses. By layering the contextual learning and detection with these known patterns found by security researches, ATA provides a
powerful tool in the fight to protect your network resources, and can reduce a potential breach window from weeks, months, or years down to just minutes.

To wrap up this section, I will now briefly cover some of the features you get if you step up from EMS E3 to the recently released EMS E5 offering. Everything covered previously in this series of posts would be included in E3, which represents a significant bang for the buck, and can greatly increase security in any environment. For companies that want an even higher level of security, Microsoft has added a few more technologies to the bundle and labeled it EMS E5.

The first product EMS E5 gives you access to is Azure AD Premium P2. This includes all the capabilities in the P1 version, plus adds Azure Identity Protection and Azure Privileged Identity Management. The Azure Identity Protection product leverages existing anomaly detection capabilities available in Azure AD and adds another level of capability using new risk event types, and allowing the configuration of policies that can act automatically if a potential threat is detected. It can also be used to eliminate the need for MFA or other security hurdles that users normally must navigate when low risk situations are detected, such as a user logging into a service during normal days and times and from locations that considered “trusted” networks. If that same user leaves that location and attempts to logon from an untrusted location, MFA would then be required as the risk level has increased.

Azure Privileged Identity Management (PIM) provides better insight within both Azure and Office 365 in regards to user admin privileges. Without PIM, it can be challenging to keep track of which users have access to which parts of those systems, which can lead to security holes or other issues over time. PIM provides a dashboard making it easy to see who has access to what in your environment, along with advanced reporting on the usage of these privileges, as well as alerts when certain roles are accessed, such as the Global Admin role. It also adds functionality called “just in time” administrative access, where you pre-determine who might need certain admin access, but wouldn’t necessarily need it day to day. Those pre-determined users can then temporarily elevate their own privileges when necessary for a specified amount of time. After this time expires, their privileges return to normal.

E5 also gives you access to Azure Information Protection Premium P2. Again, this product includes all the features found in the P1 version, plus adds the ability to automatically classify or encrypt files shared both internally and externally in your organization. In Azure IPP P1 you can prompt users based on file and/or email content to let them know they should consider using the proper classifications to restrict
rights to the data, or possibly use encryption particularly in situations where regulated information is included in the data. IPP P2 lets you create rules to enforce and track that behavior, so you aren’t relying on employees to take the correct actions themselves. This is especially useful for any organizations affected by HIPAA regulations. IPP P2 also allows for Hold Your Own Key (HYOK) for both Azure and Active Directory RMS in highly regulated industries where you can’t have your encryption keys held by 3rd party providers outside of your direct control.

The final product EMS E5 gives you access to is Microsoft Cloud App Security. This is a newer offering from Microsoft that can discover all the cloud apps that are in use in your environment. These apps are many times referred to as “Shadow IT”, because senior leadership or the IT department themselves might not be aware that employees have chosen to leverage certain cloud apps to get their jobs done, or possibly for personal use while on the company network. These unknown and uncontrolled cloud apps can create significant security risks in any environment.

An example scenario is that while it may be company policy to leverage SharePoint and OneDrive for Business to store all company data, an employee may decide to start uploading files to their personal DropBox account to access from home. Having your possibly sensitive company data stored in a personal, uncontrolled cloud account is a recipe for disaster, and Cloud App Security can help detect, report on, and control this type of behavior. It works by tying into supported firewalls and proxies that feed network traffic data into the Cloud App Security platform. This is then used to create easy to navigate dashboards showing all the cloud apps in use from your company network(s), and controls can then be placed on these cloud apps from a central portal. Third-party vendors are incented to work with Microsoft to provide even deeper controls into their products when used in corporate networks, so that they can retain business while helping companies to ensure that their data is being protected as much as possible.

**Wrap Up:**

I hope you’ve found this series of posts on the Microsoft Enterprise Mobility + Security offering useful, and are strongly considering implementing some or all the products contained within this bundle in your own company. Never have so many products of this quality and capability been available to business of all sizes at a reasonable cost, and with new threats to both cloud and on-premises networks emerging daily, implementing even a few of these technologies can significantly increase the security of your data. Thanks for reading!