jamk.fi

Enhancing security of cloud services with Microsoft Enterprise Mobility + Security

Anttu Pekkarinen

Master's thesis
November 2018
School of Technology
Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Pekkarinen, Anttu	Master's thesis	24.11.2018
		Language of publication: English
	Number of pages: 111	Permission for web publication: Yes

Title of publication

Enhancing security of cloud services with Microsoft Enterprise Mobility + Security

Degree programme

Master's Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Häkkinen, Antti

Karjalainen, Mika

Assigned by

Tieto Finland Oy and Telia Inmics-Nebula

Abstract

The security of cloud services is usually a concern for enterprises. IT service providers must understand the challenges concerning the security of cloud services and find solutions for securing their customers' cloud based IT-environments in a proper way. The variety of different solutions available on the market is huge, which makes the selection of proper solutions for protecting cloud services a challenge.

Microsoft Enterprise Mobility + Security (EM+S) offering includes many tools for securing cloud environments. The offering contains many different technology solutions, and for many enterprises it is challenging to understand how these technologies can be used effectively to gain benefit from their use.

The objective was to summarize the main challenges of identity and access management and mobility when using cloud services, and to evaluate how to use the offering's technology to enhance security. An additional objective was to describe the technologies to produce information, which is beneficial for product and service development purposes.

Security challenges were identified by interviews and by using existing research information. The solutions and EM+S offering description were defined by using existing documentation of the products and by utilizing the writer's own experience from working life.

The information gathered within this research has helped to identify most important security challenges within the scope of this thesis. The documentation created helps to understand the technology inside the offering and how it can be effectively used to enhance cloud services security. The information has also been utilized in product and service development.

Keywords/tags (subjects)

Microsoft, Enterprise Mobility + Security, EM+S, Azure, Office 365, Cloud security

Miscellaneous

Tekijä(t)
Pekkarinen, Anttu

Julkaisun laji
Opinnäytetyö, YAMK

Päivämäärä
24.11.2018

Julkaisun kieli:
Englanti

Sivumäärä
111

Verkkojulkaisulupa myönnetty: kyllä

Työn nimi
Pilvipalveluiden tietoturvan parantaminen Microsoft Enterprise Mobility +Security tarjooman avulla

Tutkinto-ohjelma
Master's Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)
Häkkinen, Antti
Karjalainen, Mika

Toimeksiantaja(t)
Tieto Finland Oy ja Telia Inmics-Nebula

Tiivistelmä

Pilvipalveluiden tietoturva on usein huolenaihe yrityksille. IT-palveluntarjoajien täytyy ymmärtää pilvipalveluiden tietoturvahaasteet ja löytää ratkaisut asiakkaiden IT-ympäristöjen asianmukaiseen suojaamiseen. Erilaisten ratkaisujen määrä markkinoilla on valtava, ja näin ollen yrityksien on haasteellista valita oikeanlaiset ratkaisut pilvipalveluiden suojaamiseen.

Microsoft Enterprise Mobility + Security (EM+S) tarjoama sisältää useita työkaluja pilviympäristöjen turvaamiseen. Tarjoama sisältää paljon erilaisia teknisiä ratkaisuja, ja monille yrityksille on haastavaa ymmärtää, miten niitä voidaan käyttää tehokkaasti hyödyksi.

Tavoitteena oli muodostaa yhteenveto identiteetin ja pääsynhallinnan sekä liikkuvuuden haasteista käytettäessä pilvipalveluita sekä arvioida, miten tarjoaman teknologialla voidaan kohentaa tietoturvaa. Lisäksi tavoitteena oli kuvata teknologiat ja tuottaa tietoa, joka on hyödyllistä tuote- ja palvelukehitykselle.

Tietoturvahaasteet tunnistettiin haastatteluiden avulla sekä käyttäen olemassa olevaa tutkimustietoa. Ratkaisut ja EM+S tarjoaman kuvaus määriteltiin tuotteiden dokumentaation avulla ja hyödyntämällä kirjoittajan kokemuksia työelämästä.

Tutkimuksessa kerätty tieto on auttanut tunnistamaan tärkeimpiä tietoturvahaasteita opinnäytetyön laajuuden puitteissa. Luotu dokumentaatio auttaa ymmärtämään tarjoaman teknologiaa ja miten sitä voidaan käyttää tehokkaasti kohentamaan pilvipalveluiden tietoturvaa. Tietoa on myös hyödynnetty tuote- ja palvelukehityksessä.

Keywords/tags (subjects)
Microsoft, Enterprise Mobility + Security, EM+S, Azure, Office 365, Cloud security

Miscellaneous

Contents

Figures

GLOSSARY

AD	Active Directory
AAD	Azure Active Directory
ATA	Advanced Threat Analytics
ATP	Advanced Threat Protection
AD FS	Active Directory Federation Services
BYO	Bring Your Own
BYOD	Bring Your Own Device
EM+S	Enterprise Mobility + Security
HR	Human Resources
IAM	Identity and Access Management
IT	Internet Technology
LOB	Line Of Business
MAM	Mobile Application Management
MDM	Mobile Device Management
MIM	Microsoft Identity Manager
MFA	Multi-Factor Authentication
PIM	Privileged Identity Management
SaaS	Software as a Service
SIEM	Security Information and Event Management
SSO	Single Sign-On

1 Introduction

1.1 Background and objective

This thesis was assigned by two Finnish IT service provider companies: Tieto Finland Oy and Telia Inmics Nebula. Both of the companies provide end-to-end IT services and their offering also covers cloud services.

Tieto is the largest IT service provider in the Nordic countries and it is active in more than 20 countries with approximately 14 000 employees. (Tieto 2018)

Telia Inmics-Nebula is medium sized IT service provider providing services mainly for small and medium-sized enterprises on Finland. Telia Inmics-Nebula has approximately 400 employees and it is part of Telia Company. (Telia Inmics-Nebula 2018)

The security is often a concern when talking about cloud services. IT service providers must understand the challenges of the security of cloud services and find solutions for securing their customers' cloud based IT environments in a proper way. The variety of different solutions available on the market is also huge and selecting proper solutions meeting with the requirements is challenging. The complexity level even increases when using a hybrid cloud while service components are on-premises and dispersed across the cloud.

Securing cloud services requires typically different approach than securing on-premises environments. The importance of network level access controls are not that important as in on-premises environment. The access control on the cloud services is more based on the users' digital identity and device identity than controlling network

level access. Identity and access management including authentication are essential parts of cloud services security.

One of the interesting security offerings on the market is Microsoft Enterprise Mobility + Security (EM+S). It provides variety of tools for securing cloud services and is focused in identity based security, device management and information protection.

The objective of this thesis was to summarize the main challenges of cloud security, and to evaluate how it is possible to enchance the security with Microsoft Enterprise Mobility + Security offering (EM+S). The main focus was on identifying identity, access and mobility management related security challenges.

In addition, a holistic description of EM+S was generated to give a detailed overview of the products and to describe the features available for enhancing security. The aim was to produce information which is beneficial for product and service development purposes (i.e. to scope and describe services for supporting EM+S).

1.2 Content and structure

The thesis is divided into three sections as described below.

The first section summarizes and describes the identity and access management / mobility related security challenges on hybrid cloud services.

The second section concentrates on describing Microsoft EM+S and the products included in it. There is a need to understand the technology before there can be described solutions based on it.

The third section describes how the features can be used to enhance security. The emphasis of this thesis is on describing identity, access and security management related features.

2 Research questions and methods

2.1 Research questions

The following research questions were formed based on the goals of the thesis:

- What kind of identity, access and mobility management related security challenges do enterprises face in public/hybrid cloud environments?
- How can Microsoft EM+S be used effectively to enhance security on public/hybrid cloud environments?

The first question scoped the challenges of the cloud services and mobility to describe where enterprises require security enhancements. The second question aims to describe the Microsoft EM+S and how it can be used to enhance security in public and hybrid cloud environments.

2.2 Research methods

This thesis utilizes the qualitative research method, and the information was collected by interviewing and analyzing existing third party researches (e.g. researches by Forrester and Gartner).

In addition, user tacit knowledge based on real life experiences was used for the thesis, however, it has not been documented. The experiences are based on customer projects, sales cases and discussions with customers, partners and vendors. One of the goals of this thesis is to document this tacit information in order to be able to forward the knowledge.

For interviews, a questionnaire form was created, which was then used as a basis for the interviews. Following requirements were also set for the interviewees:

- Interviewee should have a general understanding of the Identity & Access management and mobility.
- Interviewee should have a common understanding of cyber security.
- Interviewee should be working within IT environments of one or multiple enterprises and have a common understanding of IT requirements.

The interviewees were selected from known contacts working in the area of identity & access management or who know enterprises' requirements more widely. The interviewees included existing connections from service provider companies, which were assigned clients for this thesis. In addition, customers of service provider companies and the personnel of partner companies (e.g Microsoft) were interviewed.

The actual interviews were conducted in meetings mainly over Skype for Business. The interviews were kept open to discuss the topic more generally also outside the specified questions. During the interviews notes were taken based on the discussions. The results were used to form an overview of the security challenges related to the identity, access and mobility management of cloud services

3 Literature review

3.1 Literature overview

Following researches were evaluated as the most relevant for this thesis. The researches contain information about identity and access management related challenges and trends.

A Forrester Consulting thought leadership paper commissioned by Microsoft: Overcome security and identity management challenges in enterprise mobility with the right IT Infrastructure (2014)

Forrester Consulting thought leadership paper was commissioned by Microsoft for evaluating the challenges of enterprise Mobility in IT organizations. Forrester has developed a hypothesis to test the assertion for building the right infrastructure to support robust mobile ecosystem. (Forrester 2014)

Forrester conducted an in-depth survey including 200 North American and European IT decision makers responsible for mobile strategy or initiatives at enterprises with more than 250 employees. They found out that business groups are still assessing the possibilities of mobility even though they are excited about those. Security, identity management, integration and costs are the pain points to be assessed before a mobile ecosystem can thrive. (Forrester 2014)

The key takeaways of the research are following (Forrester 2014):

- Enterprise support teams see both the potential and the risk in integrating mobility across the enterprise.
- Security is the biggest concern for mobile support professionals.
- Tomorrow's mobile-ready IT infrastructure requires investment today.

BT Futures Report: Info workers will erase boundary between enterprise & consumer technologies (2013)

Forrester has created a report based on several existing surveys and researches. The research is based on almost 10 000 global information workers and 32 000 IT decision-makers. (Forrester 2013)

The key takeaways of the report are listed below:

- Employees who use computing devices for work no longer keep their work and personal lives separate. 61% of workers mix personal and work tasks in their devices.
- 52% of information workers across 17 countries report using three or more devices for work.
- Users expect to work from many locations, not just the office, and use the office for personal activities.
- Benefits of supporting mobility will lead into benefits such as improved worker productivity, attraction/retention of high-potential employees and more successful workplace or customer technology offerings which increases the odds of projects success.

Figure 1 shows how the market perception differs from the behavioral reality related to personal and work usage of devices. (Forrester 2013)

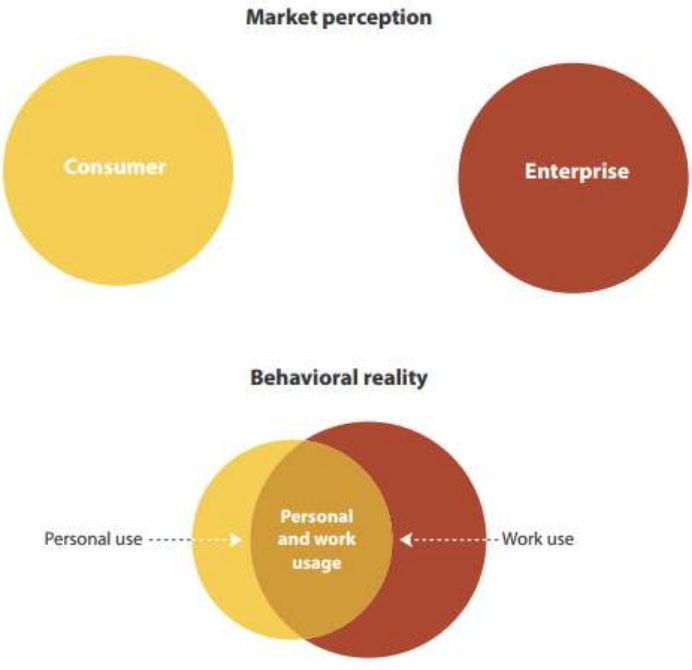


Figure 1. Technology markets are colliding

Forrester report - AD in the cloud is a reality (2016)

Forrester conducted an online survey fielded in January 2015 to over 3 000 business and technology decision-makers globally. The research provides demand side insights into the priorities, investments and customer journeys of business and technology decision-makers and the workforce across the globe. (Forrester 2016)

The key takeaways of the research are as follows:

- Cloud based Active Directory is a compelling option.
- Cloud based Active Directory Solutions provide full functional parity with on-premises solutions. In the past, cloud AD solutions have lacked support for important key features such as group; however, this is no longer the case.
- Organizations should conduct risk assessment to assess if SaaS based AD offerings fit into their business, while they can provide benefits for organizations.
- 34% of enterprises were implementing or implemented moving IAM to the cloud in 2015.

The benefits of cloud based identity and access management solutions include (Ibid.):

- Lower administrative and infrastructure costs
- More easy integration with SaaS applications
- Support for app development and testing in the cloud

Figure 2 shows statistics related to the plans of organizations for adopting cloud based identity and access management technologies. (Ibid.)

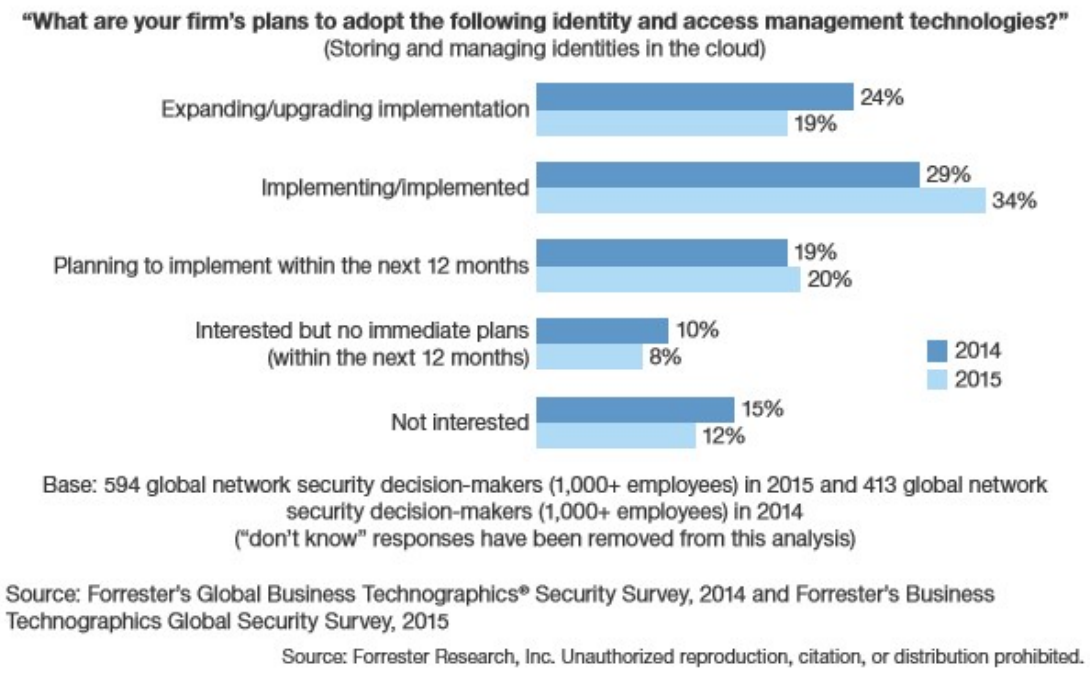


Figure 2. Plans to move IAM to the cloud (Forrester 2016)

3.2 Conclusions

When looking at the results of the researches, multiple trends can be seen which indicate that enterprises have opportunities and challenges on enabling cloud based services and mobility.

The benefits include increased productivity and more satisfied end users by allowing them to use devices and operating systems of their choice and by allowing users to work from any location. This improves the attraction/retention of high-potential employees and makes the workplace more successful. (Forrester 2013)

The factor slowing down enabling of mobility is that the security is the major concern for enterprises. There need to be sufficient protections in place before the benefits of mobility can be utilized. The risks include the mixing of the work and personal data and applications on the devices, which might lead into leaking sensitive data outside the company. (Forrester 2013)

Another concern is the manageability of the dispersed devices. There is a wide range of different operating systems and device types to be managed, which makes it challenging to support especially the Bring Your Own Device (BYOD) policy where users can make the selection of their devices themselves.

What comes to cloud based identity and access management solutions, trends can be seen indicating that cloud based Active Directory is a compelling option today. Many enterprises are already deploying such solutions and a trend can be seen that access and identity management is moving into the cloud.

The factors behind this change are business benefits, such as lower administrative and infrastructure costs, more easy integrations with SaaS applications and support for application development and testing in the cloud.

4 Identity, access and mobility management security challenges on hybrid cloud environments

4.1 Overall view into security challenges

Following chapters aim to describe the security related challenges identified in the research.

Based on the interviews there is a huge amount of different security challenges related to identity and access management in hybrid cloud environments. IT services used by enterprises are no longer located only in their data centers. Instead, they are dispersed across different locations. On some locations enterprises controls for the security are very limited (e.g. some 3rd party SaaS applications).

Over 70 different types of challenges were mentioned in the interviews. The challenge map below aims to visualize the most commonly mentioned challenges in a one diagram. The top challenges are highlighted as almost all interviewees mentioned them. The following chapters describe these challenges in detail.

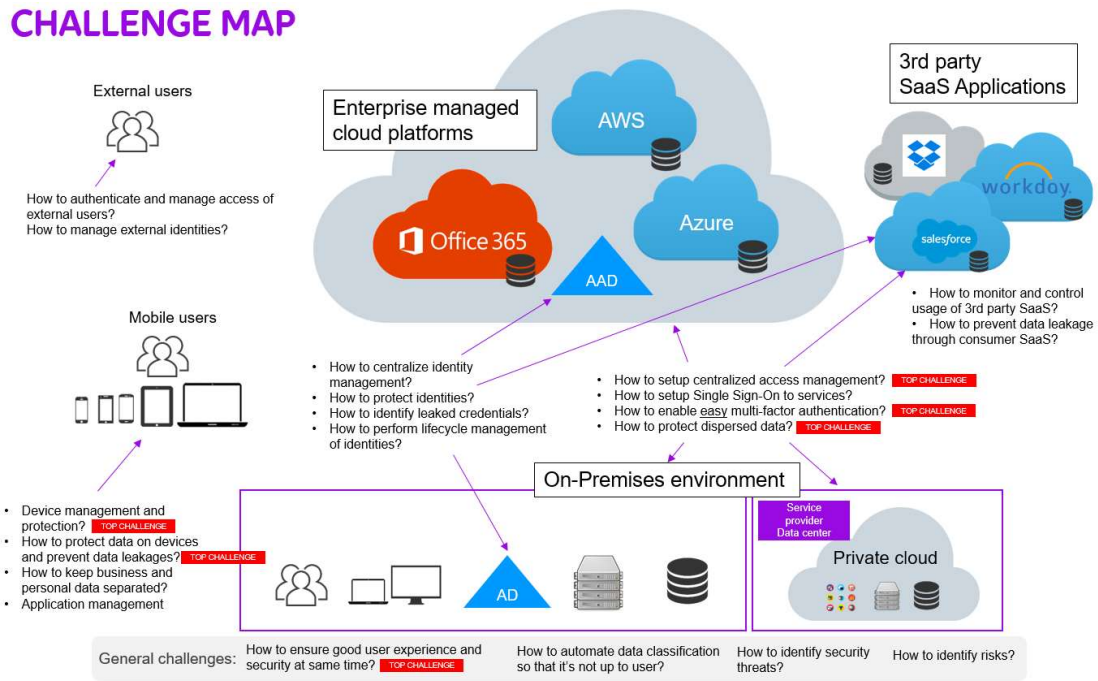


Figure 3. Challenge map

4.2 Identity and access management challenges

4.2.1 Management of user identities

Identity and access management is one of the biggest challenges in today's IT. There is a variety of different types of users, using different types of devices, and they need to be able to securely access a variety of different services. The services can be located in a company's own data center, in company managed cloud environment (e.g. Office 365), 3rd party cloud, or they can be hosted by third parties on their data center.

Based on the interview research one of the most identified challenges is the access management into different applications and services. Multiple user identities make the access management and accounts lifecycle management complex. It is challenging to ensure that users' access priviledges are at a proper level, and all accounts and access rights are removed or updated, in case employees are changing their role or ending their employment. Typically, cloud services remain accessible from any location even if user no longer has any more access into organizations premises. If access rights are not removed, users still have access to the applications and business data.

4.2.2 Access management and Single-Sign On

Another top challenge identified was the enabling of an easy access to a wide range of applications. Enterprises also want to avoid the use of multiple user identities because end-users are getting confused when using them and trying to remember multiple usernames and passwords. The preferred requirement is that all business applications should be accessible by using only one user identity across the on-premises environment and different cloud services. The use of a single user identity also reduces the workload generated from the management of the different identities in different systems.

Employees also want to use the device of their choice for accessing the services. The devices might also be owned by employees instead of company and hence, they are

not by default managed by the company. The connectivity should be possible from any location where the user is, at the time when the business services are needed. It has become a significant challenge to maintain the control how employees are accessing their applications across data center and cloud platforms.

There are several requirements for the accessibility of the services and for enabling mobile productivity. Accessing the services should be easy. At the same time, enterprises need to make sure that their data and sensitive information is secured. The security and productivity also needs to be in balance. The protection of access and information should not make the accessibility of the data complex for the end-users. This is a real challenge for the enterprises.

4.2.3 Authentication of external users

Many enterprises have needs to allow access for external users to their own IT-services and applications. These users can be partner organizations, customers or some other stakeholders. Based on the interviews, it is challenging for some enterprises to find an effective way to perform lifecycle management of identities. Authentication and access management also cause challenges while the services should be accessible from any network location.

Enterprises would like to avoid managing of the accounts in their own directories; however, they would like to control the access of the users to their applications in a centralized way. Especially, local accounts in different SaaS applications are hard to manage. The amount of applications used in the organization might be huge and it is hard to attach lifecycle management related processes to all the applications related identity repositories. SaaS applications are typically also accessible from any location. It is not enough to revoke the network access of the users when there is a need to revoke the access of the user into services.

4.2.4 Protection of user identities

Many interviewees mentioned that stolen or leaked user credentials generate a significant security risk related to user identities , which causes information leakage. It is challenging to ensure that identities are protected against identity thefts. The 3rd

party research data also confirms this. Based on Verizone research, 75% of network intrusions are exploited through weak or stolen credentials. (Verizon 2013)

According to Microsoft security intelligence report volume 22, there has been a 300% increase in user accounts targeted attacks when comparing the beginning of 2016 and 2017. Figure 4 from the report illustrates the figures. (Microsoft Security Intelligence report 2018)

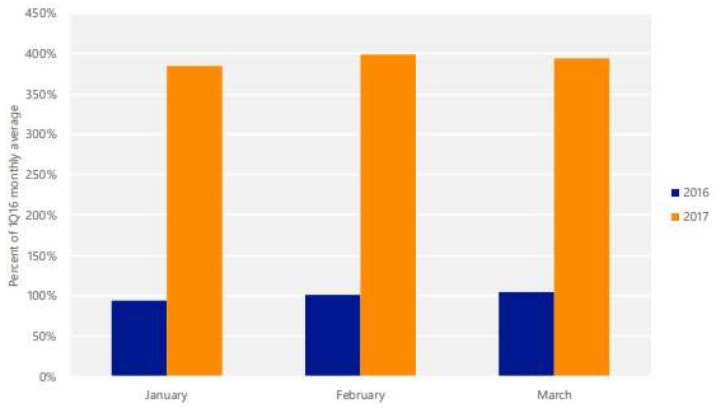


Figure 4. Observed accounts under attack during the first three months of 2016 and 2017

According to Microsoft, attackers have become effective in stealing credentials leveraging 3rd party breaches and sophisticated phishing attacks. After the attacker has access to user credentials, it is relatively easy to access sensitive information. To prevent this from happening, user identities needs to be protected regardless of their priviledge level. (Azure Active Directory Identity Protection documentation 2017)

The interviewees also mentioned that it is very important to be able to monitor the usage of user identities to be aware how, where and when identities are used to identify possible leakages. Compromized credentials should be identified to prevent using them into malicious activities. With traditional user identity management solutions it is very challenging to identify compromized credentials.

4.2.5 Multi-factor authentication for cloud applications

Most of the interviewees mentioned that they have faced challenges on providing multi-factor authentication for cloud applications. The main challenge is how to implement an authentication solution with an easy and secure access for end users

at the same time. The user experience should be similar on a variety of devices, operating systems and applications. Many enterprises do not use multi-factor authentication while it is challenging for the users. The missing multi-factor authentication causes risks of malicious access to an organization's business data.

Many enterprise have needs to set up conditional access policies to improve the user experience in such use scenarios. For example, when accessing the services from external networks, there must be sufficient security controls in place. These include completing multi-factor authentication before allowing users to access the services. However, when accessing the services from internal networks or using a device managed by the company IT, there should not be complex multi-factor authentication workflow needed before accessing the services.

When setting up conditional access policies there are also challenges related to managing devices which can be used for accessing the company's cloud services. The managed devices need to be identified when users are accessing services. This is challenging, while a wide range of operating systems and device types are available, and the user experience should be the same for all these.

This has been identified as one of the most challenging areas on access management. If the user experience on company provided services is bad, end users aim to use workaround which may cause security risks.

4.3 Data protection

Based on the interviews, data protection has several challenges. It is not easy to find a suitable protection mechanism which is is easy to use/implement and which provides a sufficient level of protection.

The traditional protection mechanisms do not suffice any more. The protection has been based on data location, however, nowadays data is dispersed into multiple locations and services. The requirements are that the protection should be preferredly automatic and the protection needs to stay with data wherever it is located.

Data protection with cloud services and mobility is challenging due to dispersed data locations. Data needs to be protected when it is stored on the cloud services during transmission of the data and also when it is stored on end-user´s devices. There need to be safe procedures for sharing the data within company's internal personnel and also with customers and business partners.

Based on the interview reseach, a challenge was identified on how to prevent data leakage outside the company and set policies so that data is accessible only for authorized personnel. More specifically, this means that the challenge is how to protect and prevent leakage of information stored in the user´s devices or stored by end users in non-company managed systems.

The storing of data into Software as a Service applications meant only for consumers is a risk for enterprises. Services such as Dropbox and OneDrive consumer version are getting more and more popular. If data is stored there without any protection, the access to data is not controlled by the company IT. This may cause leakage of sensitive information.

Data should be protected by setting encryption and access policies, which stay with the data wherever the data is located. These policies should control who is able to access the data and what users can do with the data. Sensitive data should be typically accessible for company personnel only. There should also be a way to share the data with external parties in a safe way by ensuring that only specified personnel have access to it.

4.4 Keeping business data and personal data separated

Related to the data protection, there is also a challenge how to keep company and personal consumer data separated on their devices. Today's end users mix their personal and business tasks on their devices, which causes a risk that the business data is then copied into consumer related applications and services which do not provide sufficient protection for the data. It should be prevented that the business data can be copied into the consumer related applications and services.

A solution for this would be to allow only company managed applications and services to be used for handling the data. On end-users devices there should be

policies in place preventing the copying of business data outside the company managed applications to prevent the data leakage.

4.5 Device management and protection

Today's enterprises have many challenges related to managing and protecting the devices used at work for tasks. There are different types of devices with different operating systems and it is challenging to manage the diversity of devices. These include the company owned devices and in many cases also some devices owned by the end users, which employees use for their daily tasks.

Based on the interviews, the challenges include the management of a variety of different devices and securing their usage. The lack of support in MDM (Mobile Device Management) solution for certain device type and operating system combinations causes challenges. The supporting of the BYOD (Bring Your Own Device) model causes challenges in particular. The usage of company services should be easy for the end users and still secure enough.

Enterprises also expect to be able to manage security on BYO devices. For example, implementing basic security settings such as PIN code and encryption or wiping out the data when needed is important. Many interviewees were conserned about lost or stolen devices.

Providing access to the cloud services with the BYO devices is also challenging. Behind this there is typically a requirement for Multi-Factor Authentication on organization's security policy. Multi-Factor Authentication setup might make the use of the application worse, while the end user needs to conduct manual actions before s/he is allowed to access the application. The solution to make the access easier would be to allow access to only known devices and use the device identity as the second factor. This is typically challenging when devices are not owned by the company.

The reasons behind the need to support BYOD are that supporting mobility will lead to benefits such as improved employee productivity, attraction/retention of high-potential employees and more successful workplace or customer technology offerings, which increases the odds for successful projects. (Forrester 2013)

Mobile and applications security is one of the highest priorities for enterprises. According to Forrester, 46% of enterprises have indicated that mobile security improvement is a high priority for them. 22% of them indicated that it is critical.

Only 30% of enterprises have the policies and sufficient tools in place for BYO Devices owned by employees. (Windows Server 2012 R2 Access and Information Protection Datasheet 2017)

Almost all interviewees mentioned that device management is a challenge. It was also identified that many small or medium-sized enterprises do not use any Mobile Device Management Solution for managing the security of their devices. This causes risks related to data leakage.

4.6 Application management

In addition to device management, also the managing of applications on the devices causes challenges to enterprises.

Based on the interviews, first of all the challenges include how to get the applications available for end users so they can use them and how to remove them if needed. Some of the interviewees mentioned that it is challenging to limit what applications are installed to employee's devices. Some of the installed applications might have serious vulnerabilities.

The data included in the applications also needs to be controlled. It would be beneficial to be able to separate the business and personal data. Based on Forrester research 61% of information workers are mixing personal and work tasks in their devices. More than 80% of employees admit to using a non-approved SaaS application in their jobs. (Forrester 2013)

In addition, end users' behavior causes a risk while they use personal apps to solve problems. These applications are typically SaaS services for consumers.

The risk related to using consumer SaaS services instead of company-managed services could possibly lead into leakage of data and sensitive information. A practical example of this is the use of for example Dropbox (consumer version) to save the documents there for accessing them with any device. The data saved into third party

services is not protected with company security policies and protections and hence, it is potentially vulnerable for leakage.

The usage of 3rd party SaaS should be controlled and there should be company managed options available for accomplishing similar tasks. Automatic information protection and encryption of the data could also improve security.

According to Microsoft Hybrid Identity whitepaper, this is a challenging task for enterprises because consumer-based devices are getting more popular and consumer SaaS applications are very easy to adopt for end-users. Maintaining the control of user's accessibility to applications across datacenters and different cloud platforms is challenging. (Hybrid identity whitepaper 2017)

4.7 Third party SaaS challenges

In addition to company managed SaaS such as Office 365, enterprises are typically also using multiple third party SaaS applications. On top of that, end users also use their own consumer SaaS applications e.g. Dropbox or consumer OneDrive for example when sharing files. There are risks related to data leakage when saving business data into these applications while many times these applications are not that well protected as company managed applications. Regulations such as GDPR (General Data Protection Regulation) also set compliance requirements for securing the personal data, which forces enterprises to find out ways to manage the usage of these applications.

First, enterprises would require visibility to usage of SaaS applications to understand where users save data. Secondly, some controls are needed for the usage of these applications to prevent the data leakages through e.g. consumer SaaS.

Other types of challenges are related to identity and access management. Many 3rd party SaaS applications have their built-in identity repositories and it is hard to maintain the lifecycle management of all these user accounts. The access management to these applications sets another layer of challenge. The interviewees mentioned that it is hard to find a solution which would be capable of managing access to all of these applications.

5 Microsoft Enterprise Mobility + Security (EM+S) offering

5.1 Overview of Microsoft Enterprise Mobility + Security (EM+S) offering

Microsoft's Enterprise Mobility + Security offering (EM+S) is a collection of products used to secure organizations' productivity, enhance collaboration and secure the information. Formerly EM+S offering used the name Microsoft Enterprise Mobility Suite; however, the naming and content were updated during July 2016. The new EM+S offering is also a part of Microsoft's more overall Secure Productive Enterprise offering. (Conway 2016)

The following figure illustrates the product family of Enterprise + Security offerings. (Enterprise Mobility + Security)

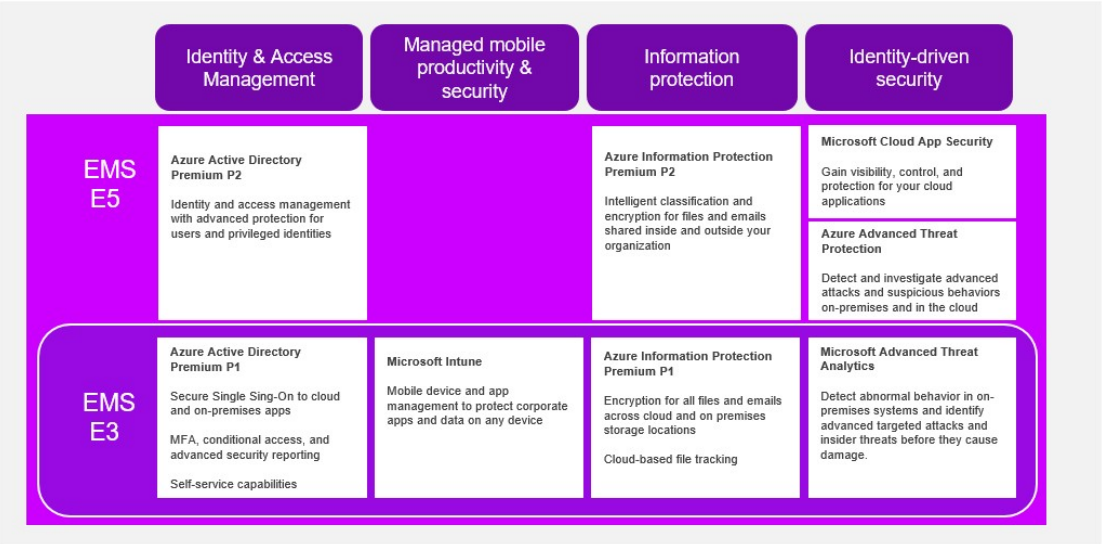


Figure 5. Microsoft Enterprise Mobility + Security offering

The Offering includes the following capabilities (Enterprise Mobility + Security):

- Identity and access management
- Visibility into user, application and data activity
- Data and information protection
- Mobile Device Management (MDM) and Mobile Application Management (MAM)
- Threat analytics and anomaly detection

The products included in Enterprise Mobility + Security E3 offering are listed below (Enterprise Mobility + Security)

- Azure Active Directory Premium P1
- Microsoft Intune
- Azure Information Protection Premium P1
- Microsoft Advanced Threat Analytics

The products included into Enterprise Mobility + Security E5 offering are as follows (Ibid.):

- All products included in EMS E3 offering
- Azure Active Directory Premium P2
- Azure Information Protection Premium P2
- Microsoft Cloud App Security
- Azure Advanced Threat Protection

With Identity and access management (IAM) capabilities EMS provides secure Single Sign-On (SSO) to thousands of Software as a Service (SaaS) applications and additionally to on-premises applications. It also includes self-service tools generating cost savings through automation of basics user and group management tasks. (Identity + Mobile Management + Security 2016)

IAM features also help to manage and secure users' identities and their access to applications. Conditional access policies help to keep the access to applications easy and at the same time provide sufficient security controls including optional Multi-Factor Authentication (MFA). (Conway 2016)

EMS Mobile Device Management (MDM) and Mobile Application Management (MAM) capabilities help to improve employees' productivity by enabling the usage of their favorite applications and devices. It helps organizations to protect and manage applications and data on Windows, iOS and Android devices. It also helps to enable the Bring Your Own Device (BYOD) concept. (Identity + Mobile Management + Security 2016)

EMS also includes plenty of other security features. Information protection capabilities provide encryption of sensitive information and safe sharing of it. Threat analytics capabilities help to identify advanced security threats before they cause damage to the organization and assist to mitigate the successfull attacks. There are

also multiple machine learning based mechanisms which protect against password related attacks and malware. (Identity + Mobile Management + Security 2016)

Microsoft EMS provides a cloud solution with comprehensive management capabilities related to user identities, devices application, and more. It helps to build security for modern hybrid cloud solutions which include components from on-premises environment, different cloud platforms and SaaS applications. It also ensures the productivity by enabling use of single protected user identity which can be used to access all applications across the dispersed service environment. Figure 6 illustrates the management capabilities of EMS. (Protecting and empowering your connected organization with Microsoft Enteprise Mobility + Security 2017)

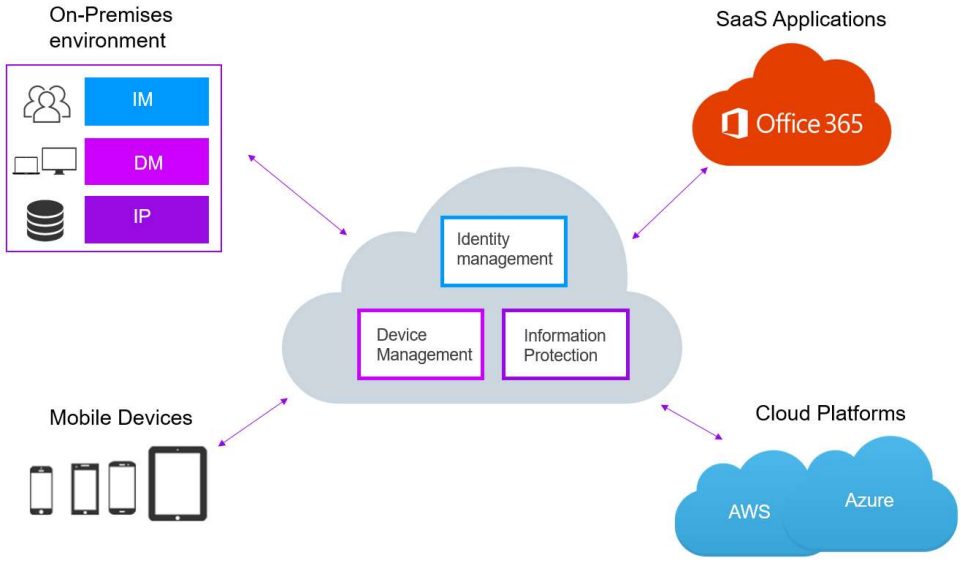


Figure 6. Cloud based management for identities, devices, applications and information

During the time of the writing the thesis, Enteprise Mobility + Security offering has leading position on the market with over 27 000 enterprise customers. More than one third of Fortune 500 enterprises have deployed EMS. (Conway 2016)

Microsoft has also been identified as a leader on Identity and Access Management as a Service offerings in Gartner's Magic quadrant. (Identity + Mobile Management + Security 2016)

The following sections discuss the content of the products included in EMS offering in more detail.

5.2 Azure Active Directory Premium P1

Azure Active Directory Premium is a cloud-based identity and access management solution. It enables organizations to manage their user and device identities in centralized way across their own data centers and cloud environment. It provides a cloud-based directory where identities of users and devices can be securely stored (Identity + Access Management 2016)

There is two licensing levels available for Azure AD Premium: P1 and P2. P1 includes already lot of features but the more advanced features are included into P2-licensing level. (Identity + Access Management 2016)

The cloud directory of Azure AD is the core store for the identities. In addition, a comprehensive set of services is built to provide other functions needed for efficient and secure use of identities. Figure 7 below illustrates high level service components of Azure AD. (Identity + Access Management 2016)

Figure 7. Azure AD high-level components

Azure AD helps to improve productivity by providing a single identity for end users for accessing all services. The end user experience also remains the same with all device types. End users will also save time with self-service features such as password reset and requesting of access to business applications. Azure AD has also integrations to thousands of third party SaaS applications, which makes it very easy to set up Single Sign-on to new applications. (ibid.)

With Azure AD, organizations can provide remote access with Single Sign-On to business applications in the cloud and on-premises data center. Azure AD's cloud based identity management helps to manage and control the access into the applications and to ensure that connectivity is secure, no matter whether the application is located in the cloud or in on-premises data center. There are plenty of security features, such as Multi-Factor Authentication, available including conditional access policies and advanced reporting and auditing capabilities. Potential security issues can be identified through machine learning based monitoring and alerting of suspicious activities. (Identity + Access Management 2016)

Azure Active Directory also provides multiple capabilities for expanding on-premises Active Directory capabilities and integration into cloud environment. Those capabilities include (ibid.):

- Synchronization with AD domain services
- Federations with AD domain services
- Cloud-only authentication
- SaaS applications Single Sign-On

These capabilities enable adoption of hybrid identity and usage of hybrid cloud solutions, which are a combination of on-premises and cloud components. (Hybrid identity whitepaper 2017)

While Azure AD enables accessing all applications with single user identity, it is even more important to protect the identities to prevent their malicious use. Azure AD Identity protection brings tools for protecting the identities. What comes to administrative identities, privileged identity protection can be used to ensure that those critical user identities are protected. Machine learning based behavioral analytics is also used to detect suspicious user activities and logins. Identifying of suspicious activities enables detection of attacks before they cause damage. (Identity driven security 2017)

In addition, Azure AD provides visibility into organizations cloud applications usage and helps to take those applications usage in control. (ibid.) Azure active directory provides comprehensive monitoring and reporting functionality, which enables to know who has access to applications and when those have been used. (Managing applications with Azure Active Directory 2107)

The sections below provides a brief introduction of Azure Active Directory features in detail.

5.2.1 Single Sing-On capabilities

Typically, organizations start using cloud service by connecting their on-premises environment into cloud-based services. To ensure that user experience stays at good level and users' productivity can be maximized, there is needed Single Sign-On to resources that users are using. In an optimal scenario, users can access their services across on-premises and cloud-based services with a one common identity. (Hybrid identity whitepaper 2017)

Azure AD provides identity federation and SSO allowing users to use single credentials for logging into multiple applications located inside or outside company network. Users are authenticated by Azure AD, which acts as identity provider. Azure AD can then use the federation to pass user identity information to applications (service providers). Azure AD can also use other sources for authenticating users. A good example is authenticating the users against on-premise's Active Directory through Active Directory Federation Services. The protocols used for federation include SAML, OpenID Connect, OAuth and WS-Federation. The following diagram illustrates these possibilities. (Madden 2016)

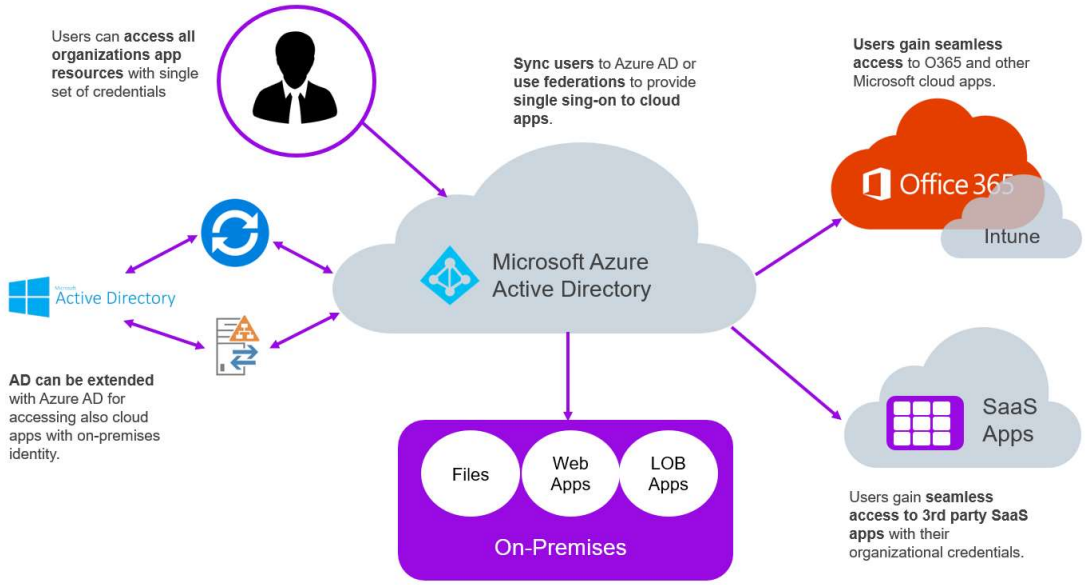


Figure 8. Accessing applications through Azure AD with single user identity

There are several benefits in using a single user identity. One of them is that it is easy for end users. Users have only one password to remember. There is also a security benefit in this because when users remember their passwords, they less likely use unsecure practices such as writing down the password. Authentication is also performed by a single service, which allows that Multi-Factor Authentication process needs to be done only once and all services authorized for the user are then accessible. (Madden 2016)

Azure AD Single Sign-on capabilities benefits can be summarized as follows:

- By synchronizing or federating users across on-premises AD and Azure AD, there can be provided Single Sign-On to 3rd party cloud applications.
- Users are able to access all company resources with a single set of credentials.
- Users can be authenticated also across different companies by using federation's trust and Azure AD B2B capabilities.
- Multiple persons can use company's social media account without sharing the credentials of the account. Instead, the users use their own user identities to sign-in, and they are still allowed to post social media sites with corporate identity.

5.2.2 Providing cloud identity

Azure AD provides a cloud directory for hosting the identities and authenticates users accessing cloud-based applications. When using cloud identities, users will have an identity which do not have any connection to their accounts they us in on-premises environment. They will have a new set of credentials that work with cloud applications only. This model works for companies, which do not have on-premises infrastructure at all, and in projects or collaboration scenarios between companies where there is a need for access only to cloud based applications. (Hybrid identity whitepaper 2017)

5.2.3 Azure AD Connect

The first step in bridging identity between on-premises AD domain services and Azure AD is to implement an integration between the directories by using synchronization engine. (Hybrid Identity Whitepaper 2017)

Azure AD Connect is a tool that can be used to synchronize users, groups and attributes in on-premises Active Directory to Azure AD. It can also synchronize password hashes. Many companies are still selecting the federation instead of synchronizing the password hashes. (Madden 2016)

Azure AD Connect handles the simple synchronization of one directory as well as complex synchronization scenarios where there are multiple domains, forests and other different identity stores such as Lightweight Directory Protocol (LDAP) directories. It also provides a write-back of attributes from Azure AD to on-premises directory. Write back capabilities include the synchronization of users, groups and passwords. (Hybrid Identity Whitepaper 2017)

Before write back capability was published, all changes to user attributes had to be made in the on-premises directory and then synchronized to the cloud directory. Write-back capability enables the management of the attributes in the cloud and then synchronizing the changes into the on-premises directory. (ibid.)

The ability synchronizes different databases directly to Azure AD, supports cloud-first viewpoint and enables using the cloud directory as a centralized user repository. The following diagram from Hybrid identity whitepaper describes the synchronization of the different directories into the cloud by using AAD Connect. (ibid.)

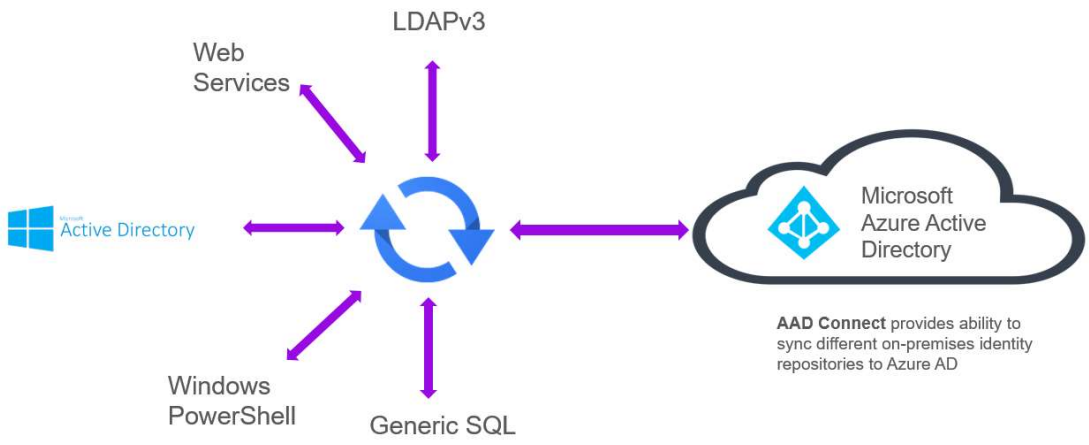


Figure 9. Synchronizing directories with Azure AD

5.2.4 Azure AD Connect health

Azure AD Connect Health is a feature that allows monitoring of on-premises identity infrastructure (i.e. Active Directory and AD FS) and synchronization services. By monitoring functionality of these services, it is easier to ensure reliable connection between on-premises components and cloud services like Office 365. It also makes it easier to access usage information of these components. All this information is available through Azure AD Connect Health portal. (What is Azure AD Connect Health 2018)

Azure AD Connect Health allows sending email notifications about critical alerts in case when for example AD FS service stops functioning or in the case sync engine or domain controllers are not healthy. Administrators are able to use the dashboard to check healthiness of identity infrastructure and make better decisions in example when troubleshooting issues. (ibid.)

5.2.5 Access management

Azure AD contains multiple features for the access management of applications. With these features, companies can secure access to their applications and data. Organizations are able to set policies for defining which users are authorized for accessing different business applications. The requirements for granting the access can also be defined. (Madden 2016)

Azure AD has lot of visibility into user behavior. It is possible to find out what applications users are accessing. In addition, details like user location, time and which device was used for accessing applications can be found out. This visibility can also be used to provide more security through setting access policies. (ibid.)

Azure AD enables the implementation of access policies for making conditional access decisions and defining what happens when a user accesses the application in specific conditions. Policies can allow or block users' access, for example based on device registration status, device management status, device-health status or user location. If there is an identified malicious activity, user identity can also be to instantly disable user's access or enforce Multi-Factor Authentication. (ibid.)

Azure AD's access management capabilities also improve the productivity of employees while they can easily access their business applications from any location by using any device. (Enable secured productivity from anywhere, on any device 2017)

In addition, Azure AD enables cross-organizational collaboration through Azure AD B2B features. It helps to provide access to applications for vendors, contractors and partners. (Protecting and empowering your connected organization with Microsoft Enteprise Mobility + Security 2017)

5.2.6 SaaS Single Sign-On and App gallery

Azure AD provides Single Sign-On (SSO) capabilities to many popular SaaS applications. This feature allows users to sign in different cloud applications with organization's own user identity with single login. This feature makes it also possible to grant users rights to use a common corporate account (i.e. corporate Facebook or Twitter account) without knowing the underlying password for the account and by using only their own user credentials, helping to protect company account from rogue access, terminated employees and minimizes the risk for leaking the passwords. (Hybrid Identity Whitepaper)

Azure AD also provides application gallery where users can browse the SaaS applications which they have access rights. Organizations can also add their own business applications, add them into the application gallery and provide SSO to them as well. (ibid.) The following figure from Active Directory team blog illustrates the app gallery user view. (Application access enhancements for Windows Azure Active Directory 2017)

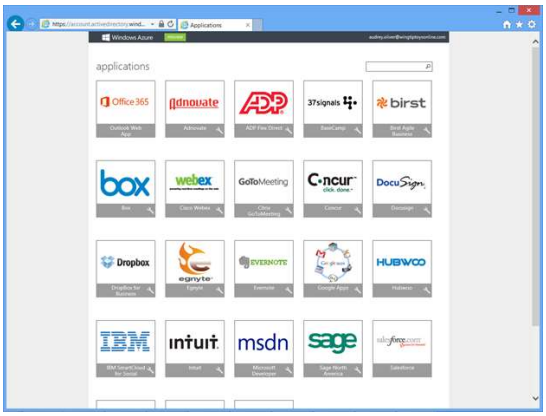


Figure 10. App Gallery user view

Users can also request access rights to organization managed applications. A work-flow can be included for the approval process (i.e. for sending approval request to team manager).

Application gallery can include Microsoft applications, pre-integrated 3rd party apps, apps connected for Single Sign-On, apps published with Azure AD application proxy and custom-made applications. Applications can be added from App gallery by signing up into 3rd party SaaS apps through Azure AD management portal. There are also other various ways to add apps as well as ways to control who is able to add applications. (How and why applications are added to Azure AD 2017)

5.2.7 Multi-Factor Authentication

Multi-factor authentication is an authentication that requires more than one verification methods and add additional layer of security to user sign-in. The two authentication methods should include two or more of the following methods (ibid.):

- Something you know
- Something you have
- Something you are

Something you know is typically a password known by the user. *Something you have* can be as an example a trusted device owned by the user, e.g. a mobile phone. *Something you are* can be for example biometrics factor. (What is Azure Multi-Factor Authentication 2018)

Azure Multi-Factor Authentication (MFA) is Microsoft's solution for two-step verification. It helps to secure access to data and applications while simplifying the sign-in process for making the user experience better. It provides a strong authentication with a variety of different verification methods. The authentication methods are text message, phone call and mobile application verification. The service first validates user's credentials and then performs a multi-factor authentication with one of those methods. If authentication is passed, the user is allowed to access the application. (ibid.)

Azure Multi-Factor Authentication is a cloud-based service that can be integrated also into on-premises Active Directory and applications. The service helps to prevent

unauthorized access to cloud and on-premises applications. It can help to keep organization's data safe and provide protection against stolen credentials and phishing attacks. It helps also to meet with security and compliance needs. (What is Azure Multi-Factor Authentication 2018)

Figure 11 describes the architecture of the service and different options to implement it. The service can be integrated into on-premises applications by using a multi-factor authentication server that integrates the service into on-premises Active Directory. Active Directory is used as a user database that is needed for validating user's credentials and in example phone number. Multi-factor authentication server can be also integrated to Active Directory Federation Services or directly to applications. (What is Azure Multi-Factor Authentication 2018)

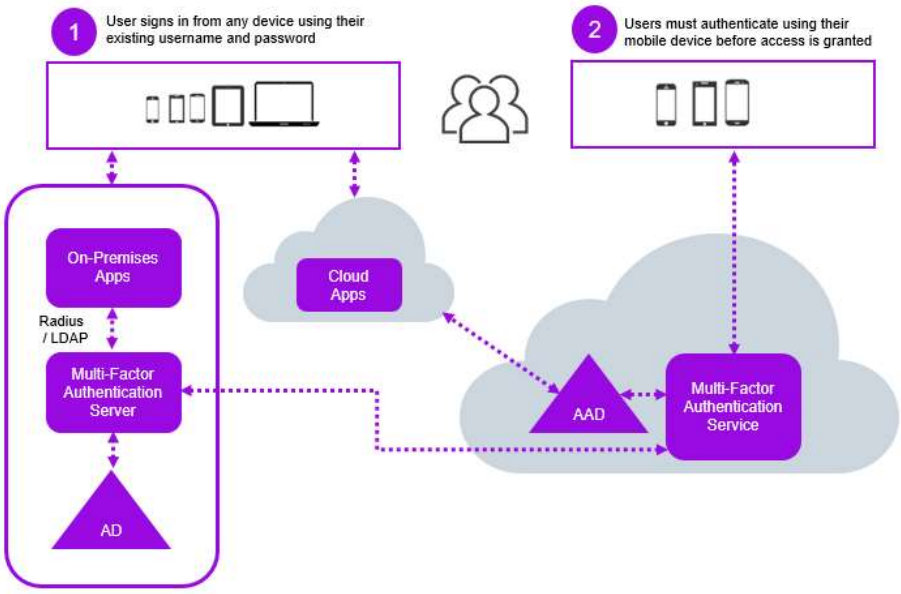


Figure 11. Azure AD Multi-Factor Authentication

5.2.8 Conditional access

Conditional access provides the control and protection for keeping data secured while allowing easy access to business applications with any device. It helps to fine tune the authentication experience for different use scenarios. With conditional access policies Azure AD checks specific conditions which are configured to be required when user accesses an application. If the requirements are met, user is

authenticated and allowed to access the application. (Enable secured productivity from anywhere, on any device 2017)

Azure Active Directory enables creating of policies providing contextual controls based on the user, location, device and application accessed. The access can be blocked or users can be challenged with Multi-Factor Authentication, device enrollment or password change. Machine learning based identity protection can also detect suspicious behavior and apply risk-based conditional access for protecting applications and company data in real time. (Enable secured productivity from anywhere, on any device 2017)

Azure AD protects all applications in any cloud or on-premises managed by Azure AD. Conditional access policies can also be used to eliminate the need for VPN or other legacy web access management solutions. (ibid.)

Figure 12 illustrates the conditional access functionality.

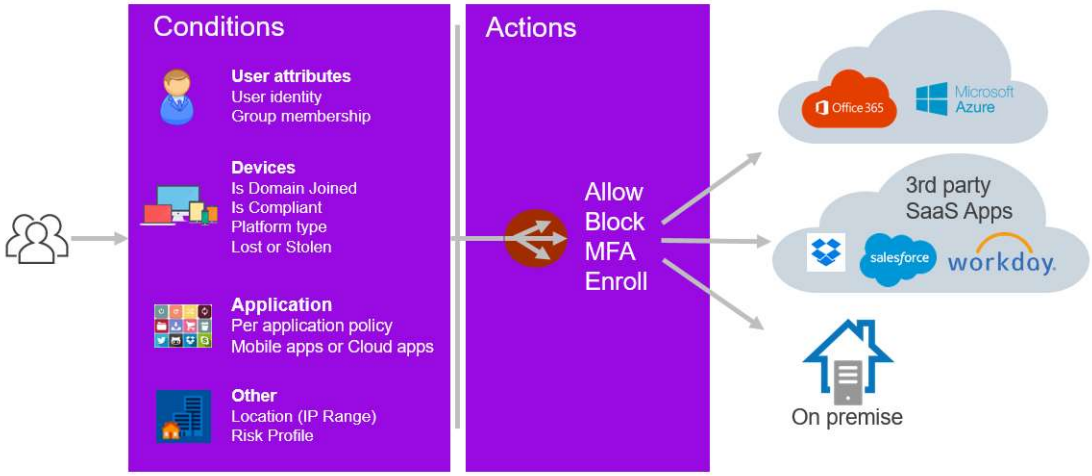


Figure 12. Conditional access

The following conditions can be set into conditional access policies (ibid.):

- Group membership (user access can be controlled based on security group membership)
- Device platform (User device platform condition (such iOS, Android or Windows) as a condition)

- Device-enabled (Block disabled devices, which no longer meet with policy requirements or are stolen)
- Client app (Set the client apps condition to grant or block access when am access attempt is made from browser or mobile/desktop client application)
- Cloud app (Select applications where policy is applicable to)
- Location (require multi-factor authentication or block access when user accesses from non-trusted networks)
- Sign-in user risk (Control i.e. multi-factor authentication based on Azure AD Identity Protection risk level)

The following controls can be set to enforce conditional access policy (Enable secured productivity from anywhere, on any device 2017):

- Multi-factor authentication (require strong authentication to block unauthorized access)
- Block
- Compliant devices (require devices to be domain joined or to be enrolled into a device management system like Intune)

Application conditions

Different applications can have different requirements for access. For simplifying the sign-in experience for the users, multi-factor authentication can be required only when accessing applications containing sensitive information. Other applications that do not contain sensitive information can be allowed to access without multi-factor authentication. MFA is then requested only when necessary. (Azure AD Conditional Access Documentation 2018).

Application policies can be applied to any cloud SaaS applications or on-premises applications protected with Azure AD. (Enable secured productivity from anywhere, on any device 2017)

Device compliance conditions

Access can be also restricted based on device conditions. As an example only known, managed and/or compliant devices can be allowed to access specific applications. (Conditional access in Azure Active Directory 2017)

With device based conditional access, the devices are registered into Azure AD and shall meet with specific condition which are configurable. Domain join (AAD Hybrid),

Intune enrolment and by third-party mobile device management system enrolment can be used as compliance condition. (Enable secured productivity from anywhere, on any device 2017)

Device compliance can be used as a factor in the conditional access policies. As an example there can be set policies to block unmanaged devices access into some specific application. Users can be prompted to enroll their devices before access is granted. This is useful when it needs to be ensured that devices used for access are configured with company security policies. This way files are not allowed to be downloaded to unmanaged devices. (Enable secured productivity from anywhere, on any device 2017)

Location conditions

There can be set policies that block access from untrusted locations for most groups. For example if there is an application containing highly sensitive data, location-based conditional policy can be applied to block access for users who are working from untrusted locations. (Enable secured productivity from anywhere, on any device 2017)

Group membership conditions

When blocking some location from normal users, it might be still required that some of the users (i.e. higher management) still needs to have privileges to be able to access data from any location. These controls can be configured by using the security groups in the access policies. Access policies can be applied to all users or multiple security groups. Groups can be also excluded from policies. (ibid.)

Risk based conditions

Azure AD identity protection capabilities can be used in configuration of conditional access policies, which allows advanced dynamic functionality in access protection. For example if unusual activity is detected, the sign-in risk score is rated as high for this event, and the activity is then blocked. This type of functionality is called a risk-based conditional access policy. There can be configured policies that trigger specific controls based on various levels of risk. Actions such as block enforce Multi-Factor Authentication or require password reset can be required. The risk level is calculated for every user and every sign-in event. (ibid.)

5.2.9 Device Registration Service

Azure AD has an important role in device management and device's enrollment into management platforms. Device identities stored in Azure AD's directory can be used to create conditional access policies. (Madden 2016.)

Windows, iOS and Android devices can be registered with Azure AD through Device Registration Service. When the device is registered, a certificate is installed on the device and a device identity is created in Azure AD. Created device identity is also tied into user's identity. This feature is also known as Workplace Join. On Windows 10 device, the registration is called with name Azure AD Join and it provides several additional capabilities. (Madden 2016.)

A registered device can be used as a second factor in authentication policies to allow seamless Multi-Factor Authentication without a need to perform manual actions. This improves the user experience significantly, especially on mobile devices. The registered device can also be used to pass user authentication, so that users can access applications without a need to fill in credentials. (ibid.)

Device registration also allows easier enablement of BYOD. Users can be allowed to use their organization's business services with their registered (and managed) mobile devices. (CIO's Guide To Azure AD 2018)

Azure AD does not have any direct control into registered devices. This is the main difference into domain join feature. (Madden 2016)

5.2.10 Azure AD Application Proxy

For publishing on-premises applications, Azure AD has a feature called Application Proxy. It is a cloud-based reverse proxy service enabling secure remote access into organizations' web applications located in a data center. Application Proxy also includes a possibility to create different access policies including multi-factor authentication. (ibid.)

The functionality of Azure AD Application Proxy is based on a connector agent installed to Windows Server located in on-premises data center. The connector is creating a tunnel into Azure AD Application Proxy service. To publish the application an

endpoint needs to be configured for the application into the service. The published application can then be accessed directly with the configured URL or through My-Apps portal. Azure AD authenticates the incoming users and routes the application requests through the connector to the on-premises application. (How to provide secure remote access to on-premises applications 2018)

Azure AD Application proxy supports publishing of applications using Integrated Windows Authentication (IWA/Kerberos) and form-based or header based access. Also web APIs, the applications behind Remote Desktop Gateway and rich client applications integrated with Azure AD Authentication Library (ADAL) can be published. (How to provide secure remote access to on-premises applications 2018)

5.2.11 Self Service and automation capabilities

With Azure AD self-service capabilities a user can get things done immediately without contacting and waiting for example for help desk to perform some simple tasks for them. Users can request access to resources and applications. They can change and reset their passwords and edit their profile information to correct errors and keep things up to date. They can also manage their own security or mail distribution groups. To maintain control to resources access, the IT staff and authorized users can manage access requests for resources and group memberships. (Hybrid Identity Whitepaper 2017)

Self-service capabilities help end-users to be productive while they can focus on their job without using time to perform tasks such as resetting their password. Self-service capabilities also reduce the work of service desk and reduce the support costs. Figure 13 describes the productivity benefits of self-service. (Hybrid Identity Datasheet 2014)

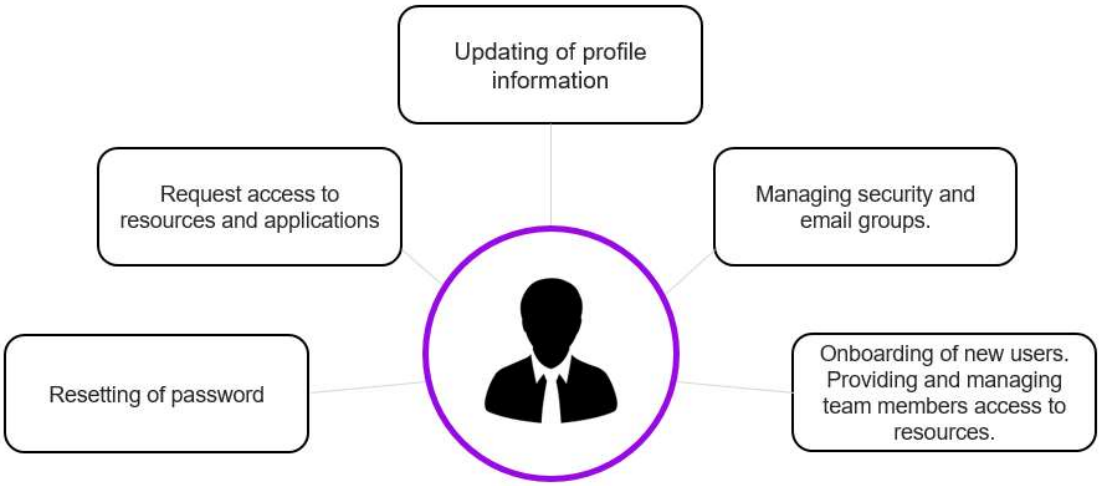


Figure 13. Self-service capabilities

Self Service Password Management

Azure Active Directory Password Management is a capability which allows users to manage their passwords from any location with any device. Users can change or reset their exprired or non-expired passwords and unlock the accounts themselves without contacting service desk or system administrator. Administrators can also initiate password reset from the Azure management portal. The security is also ensured with configurable policies. (Azure Active Directory password reset for IT administrators 2017)

A password management activity report is also available where administrators can see the activity related to password reset and registration. With Azure AD writeback capability, passwords can be also synchronized from the cloud directory to on-premises Active Directory. (Azure Active Directory password reset for IT administrators 2017)

Password management capability aims to reduce costs of support activities, improve user experiences and enable mobility. Users don't need to call help desk and wait on the line and they are able to reset their passwords from anywhere. (ibid.)

Self-service group management

Self-service group management allows users to create and manage security and Office 365 groups by themselves. Users are able to request access to groups, and the

workflow for granting the permissions can be automated. The control of group membership, i.e. access to application resources, can be delegated to specified people such as team members, supervisor of the team or business owner of the application resource. (Set up Azure Active Directory for self-service group management 2017)

Self-service group management minimizes the work that IT personnel needs to conduct for managing the groups. It can also improve the user experience while the access granting processes can be setup to be faster, while there is no need to wait for IT administrators to update the group memberships. IT administrators still remain in control and can see who is able to access applications and block access when needed. (Ibid.)

Dynamic membership groups

Dynamic membership groups enable assigning of users to groups based on identity attributes instead of manually assigning user to specific group. For example, if users' department value is set to marketing, users can be added automatically to a group used to assign access rights for marketing department personnel. Users can also be removed simultaneously from some other department related groups. (CIO's Guide to Azure AD 2018)

Automatic password rollover for group accounts

Automatic password rollover for group accounts enable the use of single corporate social media account by multiple users. Users do not have to know the actual password of the account. An account password is stored in Azure AD and encrypted securely. The password can also be changed anytime without user interaction required. Automatic password rollover reduces the risk of the account compromise. It is available for example for Facebook, Twitter and LinkedIn platforms. (ibid.)

HR App integration

Azure AD can also be integrated into HR Applications. HR App integration enables creating of user accounts and granting access rights automatically when onboarding a user into HR Application, which reduces the workload related to users' access rights

management and also makes it faster to provision access rights needed for the employees' daily tasks. Lifecycle management of the users also improves while when user is leaving company HR app integration, also efficient de-provisioning of the access rights is enabled, which also enhances security. (CIO's Guide to Azure AD 2018)

Provisioning and de-provisioning of users

Azure AD has the possibility to automate the process of provisioning and de-provisioning of users. Changes can be triggered by changing attributes or group memberships of the accounts. (ibid.)

5.2.12 Azure Active Directory and Windows 10

Azure AD is integrated into Windows 10, which enables several features. Firstly, users can use their Azure AD credentials for logging into Windows 10 devices. With login information users have access and SSO into applications they have permissions to use. The user settings can also be roamed across the Azure AD-joined Windows 10 devices, which makes the user-experience seamless on all different devices. (Madden 2016)

A feature named out of the box experience enables easy provisioning of Windows 10 devices. Users can buy almost any Windows 10 device, and it can be joined to Azure AD. During Azure AD joining, the device is automatically enrolled into mobile device management system (MDM). This way almost any Windows 10 device can be deployed as a company machine without re-imaging. The requirement is that the operating system edition is Windows 10 Pro. (ibid.)

Users can also sign in with Azure AD account to their personally owned devices. This happens by adding "work account" through settings. Users will then have SSO into their business applications. What comes to security, MDM enrollment can be required during the sing-in process. Security policies can be implemented through MDM. (Madden 2016)

Domain-joined devices can also be joined to Azure AD for providing same benefits to users. (ibid.)

The identity management is simplified by Azure Active directory through federation of identities and making signing in into multiple services more simple and secure. Users can login into Windows 10 workstation with organizational credentials and in optimal scenario have access to all resources where users have access rights. (Arsenault 2015)

5.3 Microsoft Identity Manager (MIM)

Microsoft Identity Manager is a solution for on-premises identity and access management. It can synchronize identities between different directories, databases and application. It helps to provide self-service capabilities like password, group and certificate management. It can also be used to increase administrative security with different policies and role based access management. (Microsoft Identity Manager Datasheet 2018)

Microsoft Identity Manager can be used to provide automated workflows for identity lifecycle management. It can be integrated with many types of platforms in on-premises data center and on the cloud for automating identity provisioning and group management. (Microsoft Identity Manager 2017) For example, when a new employee comes into an organization and his/her details are filled into the HR system, Microsoft Identity Manager may then provision an account for the user and configure it with proper group memberships. The user will then have automatically access into the resources that the user will need in his/her daily work. Afterwards users can also be allowed to self-manage their group memberships with proper rights management processes integrated into the workflow. The approvals can be sent for example to team members or managers so that they can themselves manage who has access to their contents.

The synchronization rules of Microsoft Identity Manager are flexible, which is the main difference compared to Azure AD Connects' synchronization capabilities. It can perform synchronization with various different directories. It can connect Active Directory identities with other directories, applications and databases, which helps to provide Single Sign-On to applications. (Microsoft Identity Manager Datasheet 2018)

Microsoft Identity Manager also enables bridging of multiple on-premises identity stores (including AD, LDAP and Oracle) with Azure Active Directory. (Microsoft Identity Manager Datasheet 2018)

5.3.1 Cloud App Discovery

Cloud App Discovery enables the discovering of unmanaged cloud applications used by the users in the organization. It enables discovering the applications used and in addition, it provides information about the usage such as number of users, volume of traffic and number of web requests to the application. It also identifies the users who have been using the applications. (Find unmanaged cloud applications with Cloud App Discovery 2017)

Cloud App discovery functionality is based on usage agents installed on user's computer. Agents collect application usage data and send it over an encrypted connection to the Cloud App Discovery service that then analyzes the data and generates a report. The following figure illustrates the functionality. (ibid.)

Figure 14. Cloud App Discovery functionality

Cloud App Discovery helps to provide visibility into shadow IT and manage it. When the organization is aware of the applications used by the users, it can set controls for usage of specific applications or even block the usage of those. (Find unmanaged cloud applications with Cloud App Discovery 2017)

5.3.2 Azure Active Directory reporting and monitoring capabilities

Azure Active Directory includes comprehensive reporting capabilities providing visibility into risk events in the environment. The reporting capabilities help to determine how the applications and services are utilized, detect potential risks affecting the health of the environment and identify security risks.

Security reports help to protect organizations' identities by identifying activities that are out of ordinary. There are two types of security reports available (Azure Active Directory reporting 2017):

- Users flagged for risk – Report provides and overview of potentially compromised users.
- Risky sign-ins – Report provides indicators about sign-in attempts which might have been performed by someone else than the owner of the user account.

Figure 16 shows the available reports. (Ibid.)

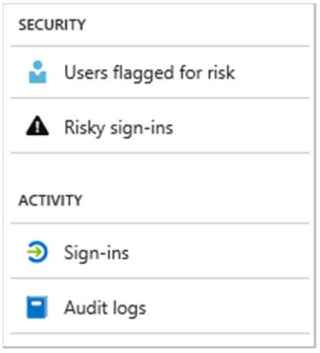


Figure 15. Security reports

Activity reports provide information about the usage of applications. There are two types of activity reports in Azure Active Directory:

- Audit logs – Report provides access to the history of every action performed in the tenant by the users and administrators. The report helps to determine what has happened in the environment and in case e.g. a security incident has occurred.

- Sign-ins – Report provides sign-ins activity and helps to determine who has performed the task reported by the audit logs report. The report also provides useful information about sign-in amounts and patterns. (Azure Active Directory reporting 2017)

Azure AD reporting provides a programmatic access to the reporting data through REST APIs. The data can be used by applications such as SIEM (Security Information and Event Management) and other audit and business intelligence tools. (ibid.)

Azure AD also provides advanced alerting capabilities. Azure AD monitors user activity and uses machine learning based analysis to identify anomalies and patterns of inconsistent access. Azure AD can then prevent attacks by e.g. requesting multi-factor authentication for identifying whether the user is who he claims to be. In addition, administrators can be alerted about suspicious activity. (CIO's Guide to Azure AD 2018)

5.4 Azure Active Directory P2

5.4.1 Identity protection

Azure Active Directory Identity Protection (later AAD Identity Protection) is a security capability helping to identify compromised user identities. It detects suspicious activities of end users and privileged identities like brute force attacks, leaked credentials, sign-ins from unfamiliar locations and infected devices. AAD Identity protection then creates a risk severity for users based on those activities. The administrator can then configure risk-based policies for protecting the identities against threats and use risk severity levels on those configurations. (Simons 2016)

AAD Identity Protection enables detecting of potential vulnerabilities affecting the identities stored in Azure AD directory. There can be configured automated responses to detected suspicious activity, or they can be reported as incidents. Then the suspicious activity related incidents can be investigated and appropriate actions can be taken to resolve them. (ibid.)

Azure AD uses machine learning algorithms and heuristics to detect anomalies and suspicious activity which indicate potentially compromised identities. It generates reports and alerts that administrators can evaluate detected issues and take appropriate actions for remediating issues. (Simons 2016)

Risk-based policies can be configured to respond to issues in real time when a specified risk level has been reached. These policies can automatically block or prompt users to, for example, perform multi-factor authentication or password reset. (Azure Active Directory Identity Protection documentation 2017)

Azure AD Identity Protection is a tool that potentially helps to identify and mitigate account compromise based attacks.

Capabilities of identity protection capabilities include functionalities described below. (Azure Active Directory Identity Protection documentation 2017).

Detecting vulnerabilities and risky accounts:

- Providing customer recommendation and highlighting of vulnerabilities
- Calculating sign-in risk levels
- Calculating user risk levels

Investigating risk events:

- Sending notifications about identified risk events
- Investigating risk events
- Providing of basic workflows for tracking investigation
- Easy access to remediation actions like password reset and multi-factor authentication.

Risk-based conditional access policies:

- Policy for mitigating risky sign-ins by blocking or by requiring multi-factor authentication
- Policy for blocking risky user accounts
- Policy for users to register for multi-factor authentication.

Figure 17 from AAD Identity Protection documentation illustrates the Identity Protection dashboard. This dashboard provides access to reports related to risky users, risk events and vulnerabilities. It also provides access to configuration of security policies, notifications and multi-factor authentication registration. (Ibid.)

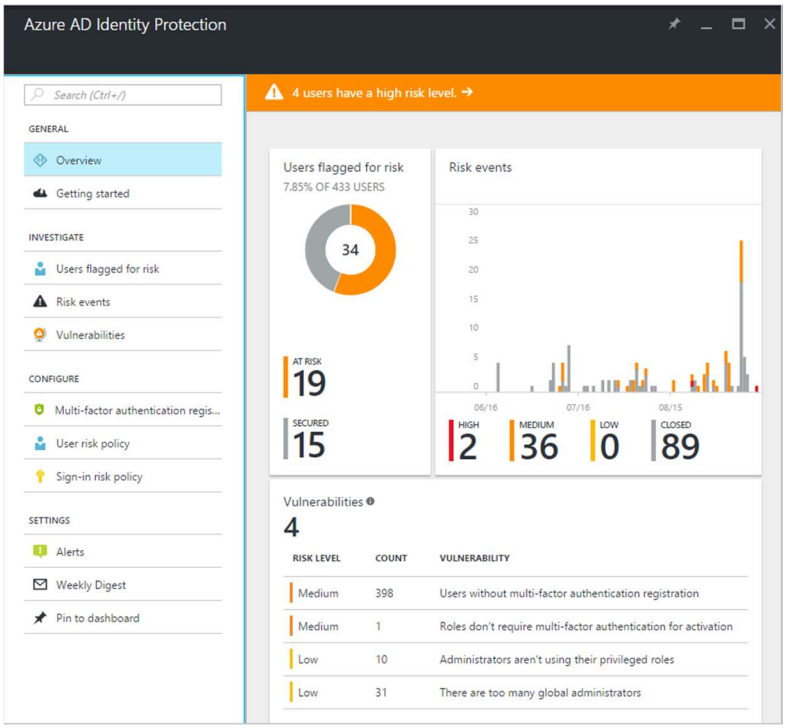


Figure 16. Identity Protection Dashboard

Suspicious actions identified by AAD Identity protection are stored as risk events. Currently there are six types of risk events, which are (Azure Active Directory Identity Protection documentation 2017):

- Users with leaked credentials
- Sign-ins from anonymous IP addresses
- Impossible travel to a typical location
- Sign-ins from unfamiliar locations
- Sign-ins from infected devices
- Sign-ins from IP addresses with suspicious activity

Figure 18 from AAD Identity Protection documentation provides an overview of the user interface of the service and identified risk events (ibid.):

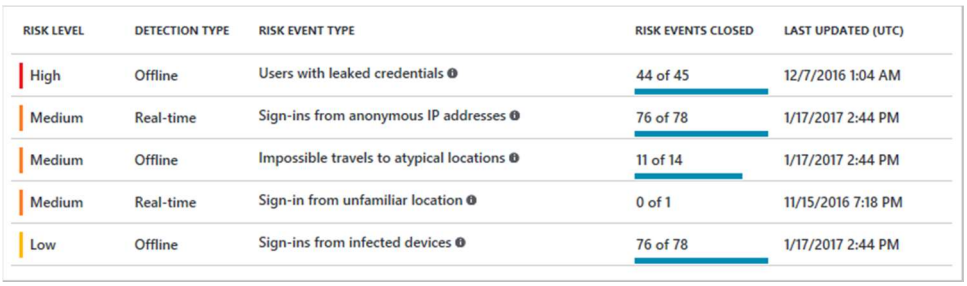


Figure 17. AAD Identity Protection risk events

As illustrated in Figure 19, risk severity can also be categorized as high, medium or low. This categorization helps to prioritize the actions. Risk calculation is based on confidence and severity of the risk. (Azure Active Directory risk events 2017)

Figure 18. AAD Identity Protection risk calculation

5.4.2 Privileged Identity Management

Azure Active Directory Priviledged Identity Management allows management, control and monitoring of privileged user accounts and their access to the resources in Azure AD and other Microsoft online services such as Office 365 and Intune. (What is Azure AD Privileged Identity Management 2017)

Azure AD Privileged Identity Management helps to find out which users are Azure AD administrators and enable on-demand temporary adminstrative access to Microsoft online services. It provides reports about accounts' access history and information about what changes they have made. It also provides alerts about access to privileged roles. It can manage the built-in Azure AD administrative roles such as global administator and services adminators. (ibid.)

Figure 20 from the documentation of Azure AD Privileged Identity Management illustrates the dashboard of the product. The dashboad shows the alerts about opportunities for improving security, number of users which have privileged roles, number of eligible/ permanent administators and information about ongoing access reviews. (ibid.)

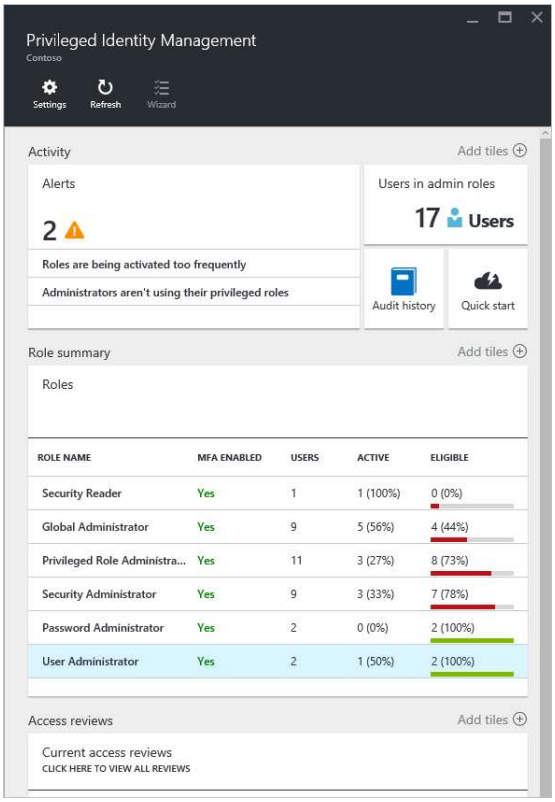


Figure 19 - Azure Active Directory Privileged Identity Management dashboard

The alerting feature of the product is generating alerts when potentially unsafe activity is identified in the environment. Alerts are shown on the dashboard (as shown in Figure 21) from the product documentation. These alerts are also visible in the reports. (How to configure security alerts in Azure AD Privileged Identity Management 2017)

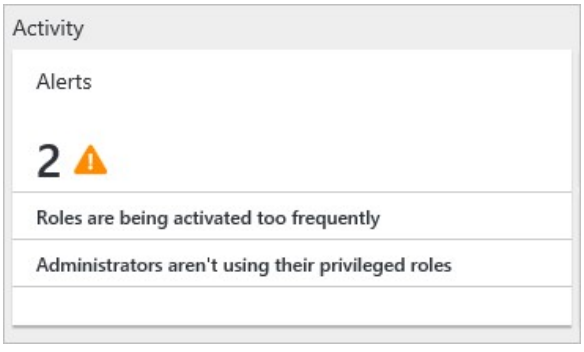


Figure 20. Azure Active Directory Privileged Identity Management alerting functionality

The tracking of activity of privileged roles provides an audit history in graphical format. It tracks all changes and activations history that the administrators have made. Figure 22 of the product documentation illustrates the audit history. (What is Azure AD Privileged Identity Management 2017)

Figure 21. Azure Active Directory Privileged Identity Management audit history dashboard

Azure AD Privileged Identity Management also includes an access review feature. With that, the administrators can set a review period and get detailed data from privileged accounts activity and identify accounts which are not used anymore. Role administrators should regularly review these roles with this feature and disable privileged roles that are not needed to reduce the risk associated with these stale role assignments. (How to start an access review in Azure AD Privileged Identity Management 2017)

Azure AD Privileged Identity managed can also be used to require multi-factor authentication when signing-in or when they activate roles in the service. In addition, it is possible to change the MFA requirement settings for a specific role. (How to require MFA in Azure AD Privileged Identity Management 2017)

5.5 Other Azure Active Directory features

There are also other features in Azure Active Directory which are not within the scope of Enterprise Mobility + Security licensing. The following sections will provide a brief introduction to some of those features.

5.5.1 Azure AD B2C

Azure AD Business to Consumer (B2C) is a cloud identity service that enables authenticating users into business services by using consumer's third party accounts such as Facebook, Microsoft, Google and LinkedIn accounts. Azure AD B2C connects the user accounts by using protocols like SAML, OpenID Connect AND OAuth. (Azure Active Directory B2C 2017)

Azure AD B2C includes built-in policies for simple connectivity scenarios. These help to enable simple authentication to consumer facing applications. In addition, it provides identify experience framework enabling building of customer policies for integrating into systems not within the scope of built-in policies. (ibid.)

Security controls for protecting the user profiles can also be implemented (e.g application or policy-based multi-factor authentication). (ibid.)

Azure AD B2C is free until first 50 000 user/authentications and after that it is priced per usage (both: stored users and authentications). (Azure Active Directory B2C 2017)

5.5.2 Azure AD B2B

Azure Active Directory Business to Business (B2B) is a capability enabling secure collaboration of organizations. Organizations using Azure AD B2B can provide access to business resources such as applications and documents to their business partners while maintaining the security controls into the data. (What is Azure AD B2B collaboration 2017)

Azure AD B2B customers can work with any users from any partner (with or without Azure AD). Partners can use their own credentials for accessing the applications and other business data. (ibid.)

5.5.3 Azure Active Directory Domain Services

Azure Active Directory Domain Services enable managed domain services in Azure, which provide AD DS features such as domain join, LDAP, NTLM and Kerberos authentication. These features are widely used in legacy applications used by organizations. (Azure Active Directory Domain Services 2017)

After deploying Azure AD Domain Services, Azure virtual machines can be joined to domain service hosted in the cloud in the similar way as to on-premises Active Directory, without deploying domain controllers. After joining the virtual machines into domain, the users or administrators can login to virtual machines using their corporate Azure AD credentials. In addition, there is a limited edition of Group Policy available for managing security settings of the virtual machines. (ibid.)

Azure AD Domain Services makes it easier to migrate legacy directory aware applications to Azure platform. By using the domain services there is no need to deploy and manage domain controllers as Azure virtual machines or use VPN connection between on-premises for integrating into on-premises AD. AD Domain Services is easy to setup and it is priced on hour basis, which makes it a viable option for development purposes. (ibid.)

5.6 Azure Information Protection

Azure information protection provides comprehensive information protection capabilities. It is a feature that enables protection of the data at document level so that it can be moved across devices and services in a secure way. (Hybrid identity white paper 2017)

The protection capabilities start from classification and labeling of the data. Administrators can configure policies for data protection to define how specific type of data is identified and how it is protected. Azure information protection can identify the source, context and content and automatically classify the data. It can be also configured to only recommend protection or allow user to classify the data manually. During the classification process the data is labeled. (Plastina 2016)

Once data is classified and labeled, protections can be added for securing the data. The classification can be automatic or the user can manually protect the data. (Plastina 2016)

The protection of the data is persistent and it travels with the data wherever it is transferred. The data is protected in storage and transit. Protection is applied also when data is on mobile devices. (Ibid.)

Azure information protection enables secure sharing of the information with customers and partners. It also makes sure that internal information is accessed only by organizations' personnel who have rights to use the information. There can be applied rules, for example, for viewing, editing printing and forwarding. (ibid.)

The classification and protection controls are integrated into Office applications. When the Azure Information is enabled, the options for protection will be visible in the Office applications options. Those options are simplified so that users can use on-click selections for securing the data in a proper way. The notifications an guide the users to protect sensitive data if automatic protection is not a wanted scenario. (ibid.)

Azure Information Protection enables also visibility and controls for the shared data. Document owners can track how the data has been shared and accessed. They can also revoke the access into the data if needed. Logging and reporting can also be used to monitor the shared data and identify if someone is trying to access it in a malicious way. (Plastina 2016)

Azure Information Protection can be used to protect data in cloud or on-premises environments. Organizations can also select how the encryption keys are managed. (ibid.)

5.7 Intune

The use of mobile devices has exploded during last years and for many of the organizations it has become essential to manage mobile devices. In addition to managing devices, it is also important to manage a mobile application installed on those de-

vices. Microsoft solution for Mobile Device Management (MDM) and Mobile Application Management (MAM) is Microsoft Intune. (Protecting and empowering your connected organization 2017)

Microsoft Intune is a cloud service providing MDM and MAM capabilities without needing to implement on-premises infrastructure for this functionality. Mobile devices can be protected by enrolling them into the Intune management. After enrolling an MDM profile can be installed and the device is then protected with appropriate security settings configured by the administrator. (MAM) is Microsoft Intune. (ibid.)

The needed applications can be installed to mobile devices during device enrollment and users can be allowed to install an organization's own application from the self-service portal. Also certificates, Wi-Fi, VPN and email profiles can be added automatically. This makes the deployment of the new device easy for the users. From the management perspective administrators have comprehensive management over the mobile devices security settings such as passcode, device lock and encryption of the data. (Manage BYOD and corporate-owned devices with MDM solutions 2017)

In addition to MDM, Intune provides mobile application management without the enrollment of the devices. This makes it possible to control for example Office applications and the data on apps. In addition, other applications on the iOS, Android or Windows devices can be managed. Intune enables separating the consumer data and business data on the applications. Business data can be then protected in a proper manner. For example, copying the data to other non-managed applications can be prevented with policies. (Manage BYOD and corporate-owned devices with MDM solutions 2017)

The business data on the devices can be wiped out by removing apps, email, data and networking profiles from the user's devices remotely. This might be necessary when the device is lost, stolen or retired from use. The devices can be wiped out so that the user's personal data remains untouchable. There is also a possibility to wipe out everything on the device, however, that is not a wanted scenario in many cases. (ibid.)

Intune provides capabilities for managing software versions of devices and applications. With this feature it can be ensured that devices are functional and have their security updates installed, which reduces the attack surface and the amount of known vulnerabilities. (Manage BYOD and corporate-owned devices with MDM solutions 2017)

In addition to management of mobile devices and applications, Intune also provides management of PCs from the same console. There is an integration to System Center Configuration Manager, which makes this possible and allows consistent management experience across all organization's devices. (Protecting and empowering your connected organization 2017)

5.8 Advanced Threat Analytics

Advanced Threat Analytics (ATA) is an on-premises service enabling detection of suspicious user activity and advanced targeted attacks. It uses a behavioral analytics with self-learning and advanced intelligence. The learning is continuously updating and adapting to the changes in the environment and behavior of the users and business. Figure 24 from Microsoft documentation illustrates the analysis, learning and detection process. (What is Advanced Threat Analytics 2018)

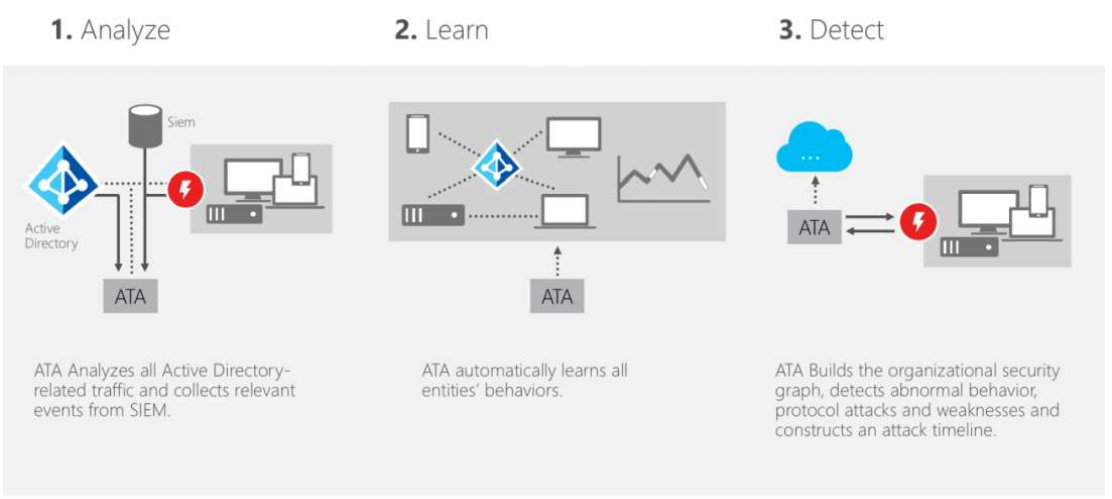


Figure 22. Advanced Threat Analytics learning and detection process

ATA collects the data for analysis from domain controllers through port mirroring or by a piece of software called as ATA Lightweight Gateway on domain controller. ATA

can also collect information from SIEM by using syslog and Windows devices through Windows Event Forwarding. (What is Advanced Threat Analytics 2018)

Figure 25 illustrates ATA architecture (ibid.)

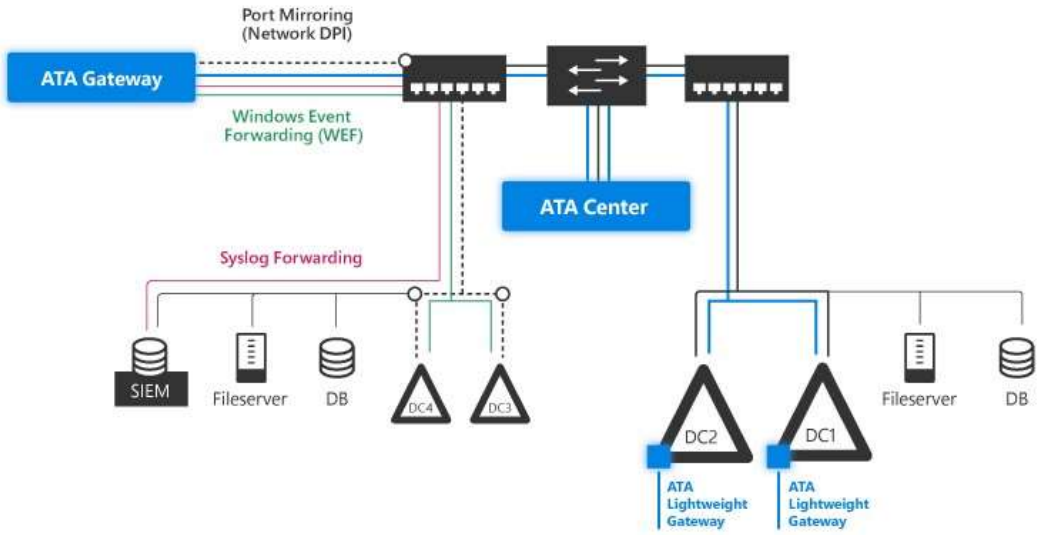


Figure 23. Advanced Threat Analytics architecture

ATA is able to identify known attack types mainly related to identities. For example, if Kerberos or NTLM tickets are manipulated or some one is trying to brute force accounts password, ATA recognizes this as a possible attack. In addition to known attack types, it recognizes configuration issues (e.g. if credentials are sent as clear text) and anomalous activities which could be related to an advanced targeted attack. (What is Advanced Threat Analytics 2018)

For identifying anomalous activities ATA builds a map about the common access of the users of applications and keeps track how they are typically used. In case applications are accessed from different devices at suspicious times, it is possible that a user account has been hacked. ATA identifies this as a possible attack and generates an alert. Alerts can be sent by email, and information is also visible on ATA's attack timeline which can be viewed from ATA user interface. (Protecting and empowering your connected organization 2017)

ATA is a good tool for in example to identify compromized AD accounts and identity related attacks. It helps to identify possibly leaked credentials and alerts administrators so that they can investigate issues more deeply and mitigate attacks.

5.9 Cloud App Security

Cloud App Security is a service which provides visibility, controls and protections for cloud applications. Cloud App Security can identify over 13 000 cloud applications. As a difference to Cloud App Discovery, Cloud App Security does not require any agents installed to end user devices. The information is collected from organizations' firewalls and proxies. (Protecting and empowering your connected organization 2017)

Cloud App Security provides visibility into apps, devices and data activity for uncovering suspicious activities, user mistakes and potential threats. It uses behavioural analytics and machine learning for providing such functionality. Microsoft security intelligence database is also used in the analysis of the events. (ibid.)

Figure 26 from Microsoft vision whitepaper illustrates the Cloud App Security functionality.

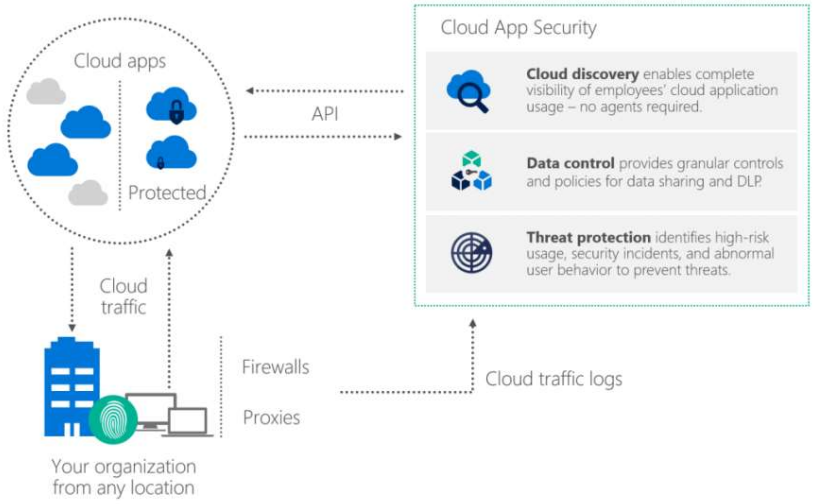


Figure 24 - Cloud App Security

5.10 Azure Advanced Threat Protection

Azure Advanced Threat Protection is a cloud service that can be used to protect hybrid cloud environments from advanced targeted cyber-attacks. Azure ATP is a technology similar to Advanced Threat Protection. The main difference is that Azure ATP is cloud-based solution. (What is Azure Advanced Threat Protection 2018)

Azure ATP collects information from multiple sources to learn the behavior of the users and network entities. It collects information with sensors installed to domain controllers or with standalone sensors attached to domain controllers through port mirroring. Azure ATP can collect information also from multiple sources such as SIEM and Windows endpoints logs. (ibid.)

Azure ATP detects attacks deterministically and by identifying abnormal behavior by utilizing its security analytics capabilities. When attacks or other abnormal behavior is detected, alerts are visible from Azure ATP workspace portal. Alerts can be also sent to administrators or security staff by email. (ibid.)

Figure 27 from Microsoft product illustrates Azure ATP architecture. (Azure ATP Architecture 2018)

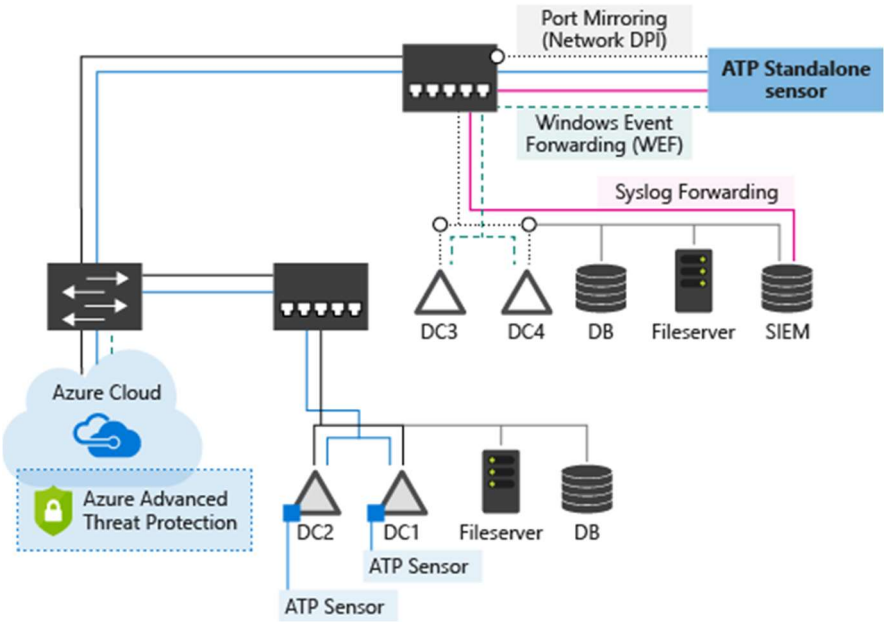


Figure 25. - Azure ATP Architecture

6 Enhancing security with Microsoft Enteprise Mobility + Security

6.1 Solutions overview

This chapter describes how technology of the Microsoft Enterprise Mobility + Security offering can be used for enhancing security of enterprise environment and cloud services. The aim is to describe solutions to the challenges identified in the research.

The following solution map aims to provide an overview of the different solution areas. Solution areas are described in detail in the sections below. They also discuss capabilities not mentioned in the solution map which are fulfilling the overall solution.

Found solutions cover almost all top challenges identified in the research.

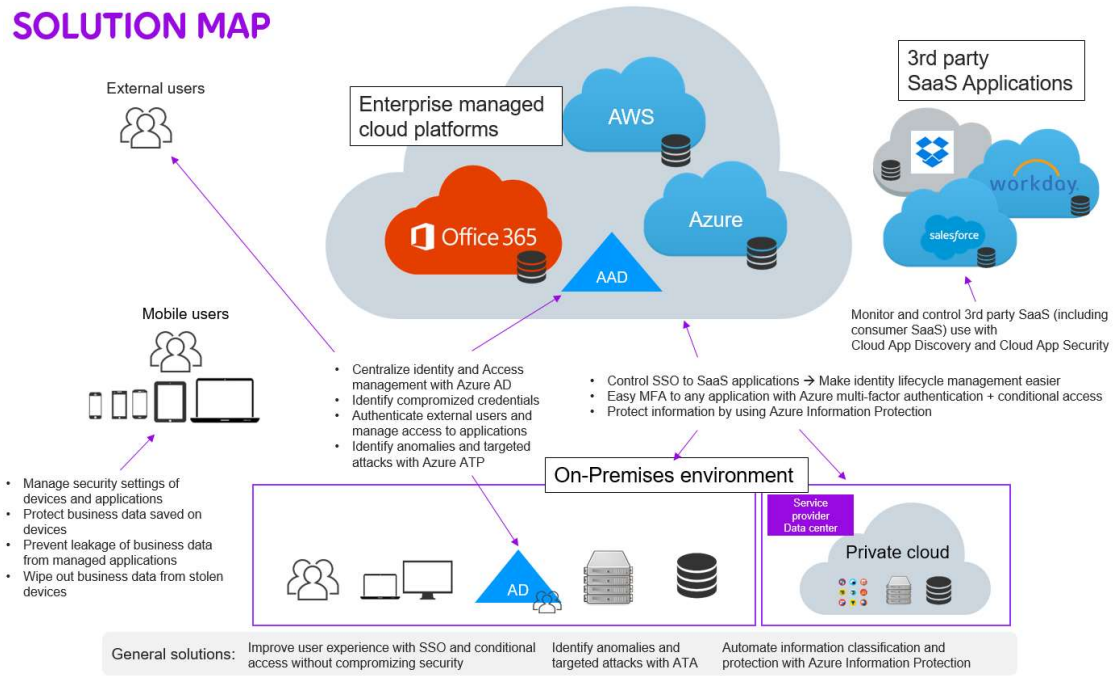


Figure 26 - Solution map

6.2 Identity and access management

6.2.1 Centralizing identity and access management with hybrid identity

Hybrid identity

To reduce the amount of discrete identities and passwords for multiple services a hybrid identity is needed. Hybrid Identity is a user identity for authentication and authorization, which can be used to access any type of resource, regardless of service location.

Currently the de facto standard for directory services is Microsoft Active Directory which is used in most of the enterprises (Active Directory Facts.). To extend the Active Directory to the cloud and to enable hybrid identity, some additional tools are needed. With Microsoft technologies there are two primary ways to provide hybrid identity.

The first option is to use identity synchronization tools such as Azure AD Connect or Microsoft Identity Manager to synchronize the identities and passwords between different directories. Typically, the syncronization is carried out between on-premises Active Directory and Azure Active Directory, which is the corresponding identity store in Microsoft cloud. When accessing cloud services through Azure AD, this synchronized identity can be used for authentication. To avoid synchronization of passwords to Azure AD, there can be used Pass-through authentication (PTA).

The second option is to use identity federation. This can be provided with Active Directory Federation Services (AD FS). AD FS is based on WS-federation protocol and Security Assertion Markup Language (SAML). When using AD FS, the authentication of the user can be performed against the on-premises AD even when the service is located e.g. in the cloud. AD FS also enables Single Sign-On (Active Directory Federation Services 2018)

By using AD and these tehcnologies together, authentication and Single Sign-On can be enabled into most of the applications relying on on-premises data center and Microsoft cloud. Federations can also be used to create trust relationships and enable authentication to application services of other organizations. These

applications include also third party SaaS which supports federated authentication. (Hybrid identity whitepaper 2017)

Benefits of hybrid identity

When using hybrid identity there is no need to create multiple accounts to different application services. Hybrid identity makes management of identities easier and enables efficient lifecycle management of accounts. This has also security benefits while users' access rights can be removed easily when needed.

Hybrid identity also makes the user experience better while users need to use only single user identity for logging in into services. A Single Sign-On also makes this seamless to end-users. Security is also improved while there is no need to write down passwords for different applications and there is no need to store them in an insecure way.

Figure 29 demonstrates the different options for authentication when using hybrid identity. Using of hybrid identity also allows the use of other advanced security features of Azure AD for improving the security and making its management easier. Azure AD monitoring capabilities also become available for getting visibility into identity related security events and applications usage.

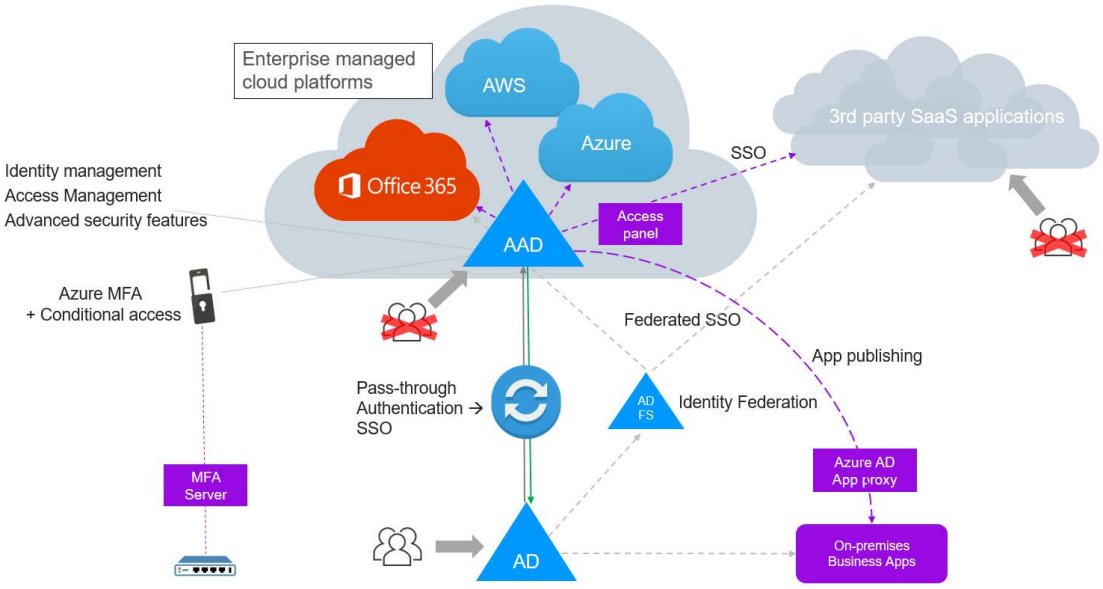


Figure 27. Using hybrid identity to centralize identity and access management

The benefits of hybrid identity are summarized below:

- Minimizing separately managed identity stores. Less management overhead.
- More effective identity lifecycle management.
- More effective way to lock down specific users' access into organizations resources (e.g. in case an employee leaves the organization).
- Seamless access to almost any application with single user identity. Better user experience and improved productivity.
- Avoidance of a risk related to writing down credential information to insecure locations.
- Easy enforcement of multi-factor authentication to services which require it.
- Possibility to enable Azure AD advanced machine learning based identity protection and management features.
- Comprehensive monitoring of identities related activities and applications usage.

6.2.2 Bridging of identity stores

Microsoft Identity Manager (MIM) allows to extend the hybrid identity capabilities to also other than Active Directory based identity stores such as LDAP, Oracle and MySQL based identity databases. With MIM, it possible to bridge the identities of those identity stores with AD and Azure AD by synchronizing the identity information across different identity stores. (Microsoft Identity Manager Datasheet 2018)

This capability brings the capability to authenticate with AD identity also into applications not supporting AD integrated authentication or federated authentication. Figure 30 below from Microsoft Identity Manager Datasheet illustrates the idea of this bridging. (ibid.)

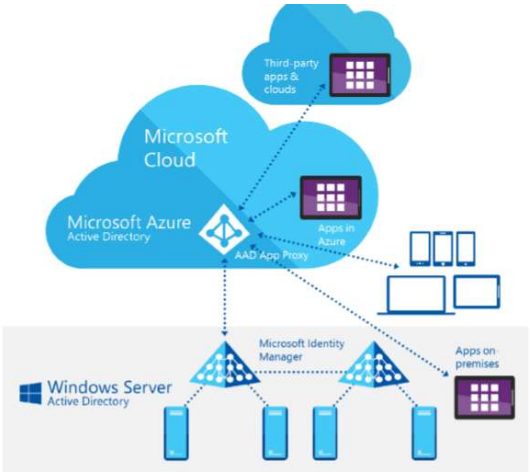


Figure 28. Microsoft Identity Manager Identity stores bridging

Identity bridging enables integration with HR systems, which makes the lifecycle management of the identity more effective. User accounts can be provisioned through HR system, roles and user permissions can be updated, and in case an employee leaves the company, HR can disable the user's account. Figure 31 illustrates integration of HR and other systems with Active Directory services.

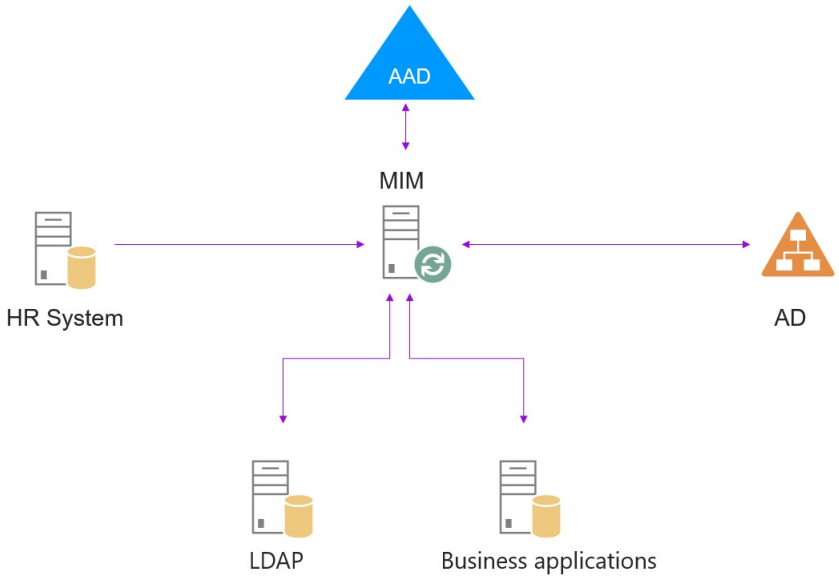


Figure 29. Integrating HR and other systems with Active Directory services

6.2.3 Self-service capabilities

After hybrid identity is in place, it is possible to benefit from Azure AD self-service capabilities.

With ***self-service password management*** users can be allowed to reset their and unlock their accounts by themselves without contacting service desk. Multi-factor authentication makes this process also more secure. Activity reports also makes it easy to follow up password reset activities.

Self-service group management helps teams to manage access rights of the applications inside the team. The access rights can be provided faster and there is no need to use IT resources for handling access right requests. The approval process still en-

sures that access rights are given by the person with the right to provide them. Provisioning of access right can also be completely automated in case that there is no need for any approvals.

Dynamic groups can be used to control an application's access for the group of users by controlling identity attributes. For example, it can be used to provide access rights based on department value of the user account. This enables role based access management.

In addition to Azure AD built in capabilities, Microsoft Identity Manager can be used for ***automating workflows*** related to the identity lifecycle. For example, by integrating the HR system Microsoft Identity Manager can take care of adding a user into right security groups after the user has been created in the HR system. Automated decisions can be based, for example, on an employee role.

These self-service capabilities aim to reduce the workload needed for specific tasks, make performing them faster and allow carrying them out at any time of the day. Users will be more productive and IT personnel will have more time for more important tasks.

Security benefits include a more secure way to reset users' password or reset an account. Automated user access rights processes and role based access rights management also make sure that the access rights are approved in a proper manner. They also help to keep track of the granted permissions, which is typically challenging for enterprises. Identity lifecycle management related tasks, such as removing access rights when an employee leaves company, can be also automated.

6.2.4 Identity protection

Azure AD P1 built-in features

Azure Active Directory provides warnings about several kinds of suspicious sign-ins which are possibly caused by attackers or malware. These suspicious activities can be e.g. logins made within a few minutes from different geographical areas. Brute-force attacks and use of new devices can be also identified.

In addition to providing alerts to security staff, Azure AD can automatically take an action to prevent malicious access. For example, a user can be forced to change a password or use multi-factor authentication for future logins. (Protecting and empowering your connected organization 2017)

Azure AD Identity Protection

Azure AD Identity Protection is a service included in Azure AD P2 and EM+S E5 licensing providing more advanced capabilities for protecting identities.

Azure AD Identity Protection can be used to identify compromised user identities in automated way on a cloud directory. AAD Identity protection uses machine learning algorithms and heuristics to detect suspicious activities related to users. It then calculates the risk severity for a user based on the users' activity.

Risk severity can be used in configuration of risk-based policies for protecting the identities against threats. Risk based policies enable real time automated responses to issues. Policies can automatically block user, force multi-factor authentication or password reset. These policies can be used also in conditional access configuration to block risky users accessing services or at least ask them to proof their identity before access.

AAD Identity Protection also provides a consolidated view into suspicious sign-in activity, highlights risky users on the tenant, flags identified vulnerabilities related to those and provides recommendations for the administrator. The administrator can then take actions to mitigate the security issues. This information can be also provided as a report through email.

AAD identity protection provides more confidence that identities are properly protected by providing automated configurable controls for mitigating risky sign-ins and by providing visibility into risk events and vulnerabilities. It can be used as a tool for identifying leaked user accounts on Azure AD and controlling the access of those users into business data. Figure 32 illustrates the idea of AAD Identity Protection.

Figure 30 - Azure AD Identity Protection

6.2.5 Protecting administrative access

Importance of securing administrative access

Administrative accounts are the most risky accounts in the cloud environments. A good example is Office 365 or Azure Global Administrator account which typically have access into almost any resource in the cloud environment.

When administrative account is breached, it can result in a long investigation. Even if the compromised account has been closed, it can be hard to investigate what kind of malicious activities the attacker has performed with the account and if there are some backdoors or other security holes in the environment.

It is extremely important to protect administrative accounts well, since they are common targets for the attackers.

Basic protection

The first thing to do is to minimize the amount of administrative accounts in the environment to reduce the attack surface.

The second thing is to enable multi-factor authentication for all administrative accounts. Multi-factor authentication is a built-in feature in Office 365 and Azure and available without EM+S.

These are the very basic actions to take; however, there are more tools available in EM+S for providing better visibility and protection of administrative accounts.

Azure AD Privileged Identity Management

Azure AD Privileged Identity Management (PIM) is a service that can be used to protect and monitor privileged access into Microsoft cloud resources. It first discovers all privileged accounts. It is important to understand who manages the cloud environment to be able to control the access. (What is Azure AD Privileged Identity Management 2017)

Azure AD PIM also monitors those accounts and tracks the changes made by them. This is important for identifying are those accounts really active and used for administrative purposes. Change tracking can be used to review the actions of specific actions; for example, in a situation when there is a reason to believe that an account is compromised. Tracking capability can be handy when investigating security incidents. Azure AD PIM can be also configured to alert about unsafe activities or unused roles in the environment. (ibid.)

Azure AD PIM also provides information about the ways privileged accounts are protected. To name an example, it shows if the multi-factor authentication is enabled for the accounts and if the privileged role is eligible or permanent. Figure 33 illustrates the Azure AD PIM dashboard that can be used for review. In addition, Azure AD PIM also enables configuring the MFA requirement on role basis making sure that all accounts with specific privileged roles will be protected properly. (ibid.)

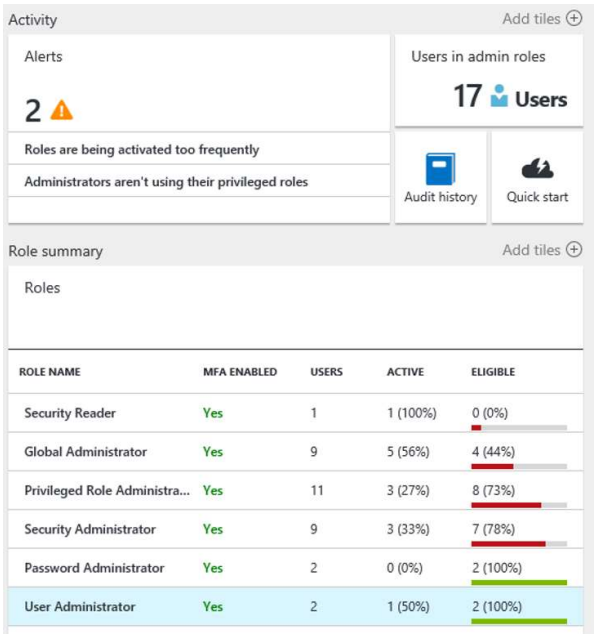


Figure 31. Azure Active Directory Privileged Identity Management dashboard

Minimizing active privileged roles with Azure AD PIM

Typically, the amount of administrator accounts is challenging to keep minimized; in particular for organizations using managed service providers. Managed services are usually provided by a team of specialists and multiple persons need administrative access for providing services. There might also be several teams specialized in a specific area of the service. This leads into a situation that there are too many administrator accounts in the environment and some of them might be rarely used. This increases the attack surface and the risk related to breaches.

For minimizing active privileged accounts, Azure AD PIM enables the concept of eligible administrators. Eligible administrators are users who are able to enable a privileged role (such as global administrator) for a needed time period. The privileged role is inactive until the user needs the administrative access. (What is Azure AD Privileged Identity Management 2017)

Activation of the role requires user to perform an activation process. In the activation process multi-factor authentication can be required for checking the identity of the user or required an approval before activation (ibid.)

In addition, an incident or service request ticket number might also be required related to the activation request. Other administrators can also be notified by email about role activation. The activation requirements can be configured on a role basis. It can also be set how long the role will be active for the user. (What is Azure AD Privileged Identity Management 2017)

Figure 34 from product documentation represents the role activation settings panel. All role activations are also recorded and it is possible to audit them afterwards. (ibid.)

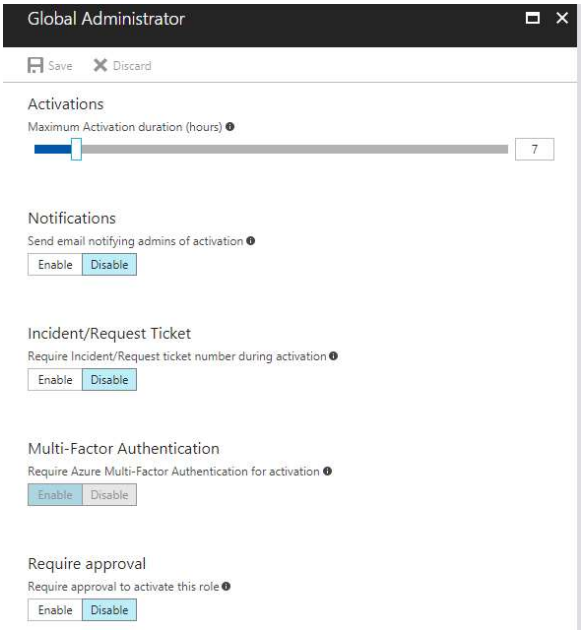


Figure 32. Activation settings for eligible administrator role

Using eligible administrator roles and time bound access is a good way to minimize active privileged roles and reduce the attack surface related to accounts. It can also be used for minimizing risks related to administrative accounts which cannot be protected with multi-factor authentication because of technical reasons (e.g. PowerShell management requirements).

Identifying risks related to privileged identities

Azure Active Directory Identity Protection (capabilities described in detail in the previous section) can be used to control and monitor privileged identities and their access. Identity Protection is able to identify risky administrative accounts which are

potentially breached or have vulnerabilities and provide alerts about them. It can also identify attacks targeted to accounts.

For automating the protection, administrators can configure conditional access policies to block admin accounts to prevent risky accounts from accessing the environment or require MFA or password reset. (Securing privileged access in Azure AD 2018)

6.2.6 Identifying identity thefts

Identity thefts can be identified in several ways by using the technology included in the EM+S licensing.

Azure AD built-in capabilities

Azure AD creates reports about users´ security related events which can be reviewed regularly by security staff. The reviewing of these reports is a manual way to identify abnormal behavior and identify possibly compromised user accounts.

In addition, Azure AD provides automated alerts about suspicious activities.

Azure AD Identity Protection

As discussed in the previous sections, Azure AD Identity Protection provides a consolidated view into suspicious sign-in activity and highlights risky users on the Azure AD tenant. This information can also be provided as a report through email. Azure AD Identity Protection helps administrators or security personnel to easily identify risky accounts and execute needed actions.

Azure AD Identity protection can be configured to perform automated actions in case a potentially compromised account is identified.

Advanced Threat analytics

Advanced Threat Analytics (ATA) can be used to monitor on-premises Active Directory users' behavior and identify suspicious activities performed by them. ATA keeps track what applications users commonly access, devices they typically use and on what times they typically access them. In case of abnormal behavior, ATA will generate an alert. Security staff can then investigate if this is a real event and if a user's account is possibly compromised. Figure 35 from ATA product documentation shows an example of suspicious activity alert. (What is Advanced Threat Analytics 2018)

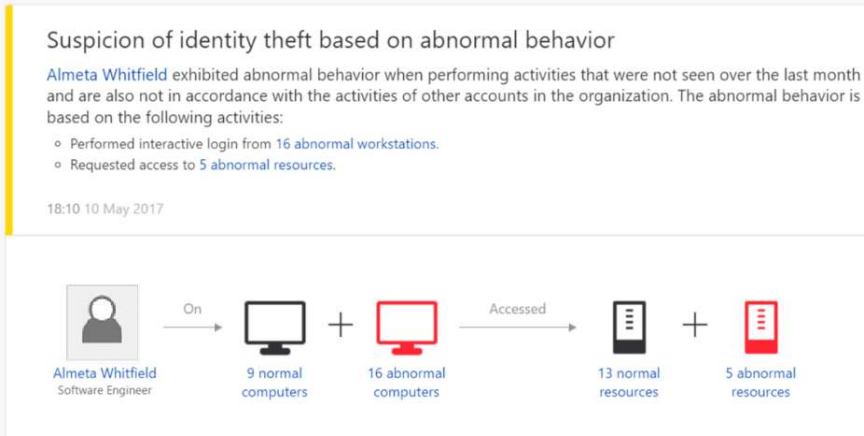


Figure 33. ATA suspicious activity alert

ATA can identify known attack types related to identities in case someone tries to gain access into users' session or execute an identity theft. Figure 36 of product documentation shows an example of attack activity alert (ibid.)

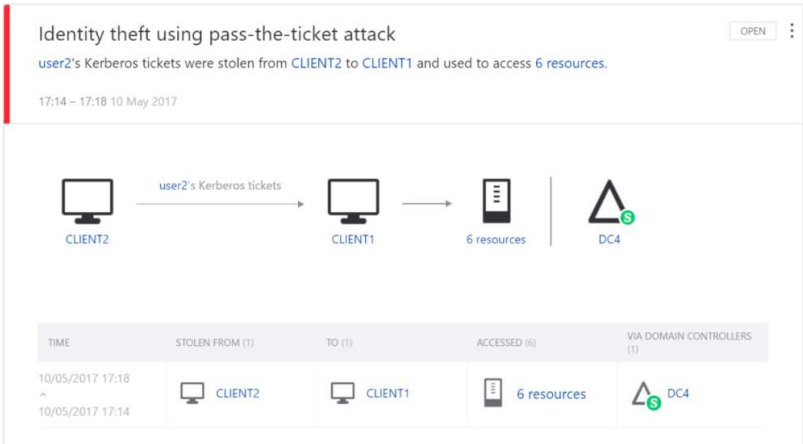


Figure 34. ATA malicious attack alert

SIEM integration

To make identifying identify thefts more effective, Advanced Threat Analytics and Azure Active Directory can be integrated into Security Information and Event Management system (SIEM). SIEM can be then used to analyze the alerts and activity logs. Activities can also be correlated with other events in the environment to get wider understanding if the identy is compromized and possibily used for malicious actitivies . SIEM integration enables an efficient way to centralize the handling of the events and investigate if suspicious activities are real threats or false positives. Figure 37 illustrates the idea.

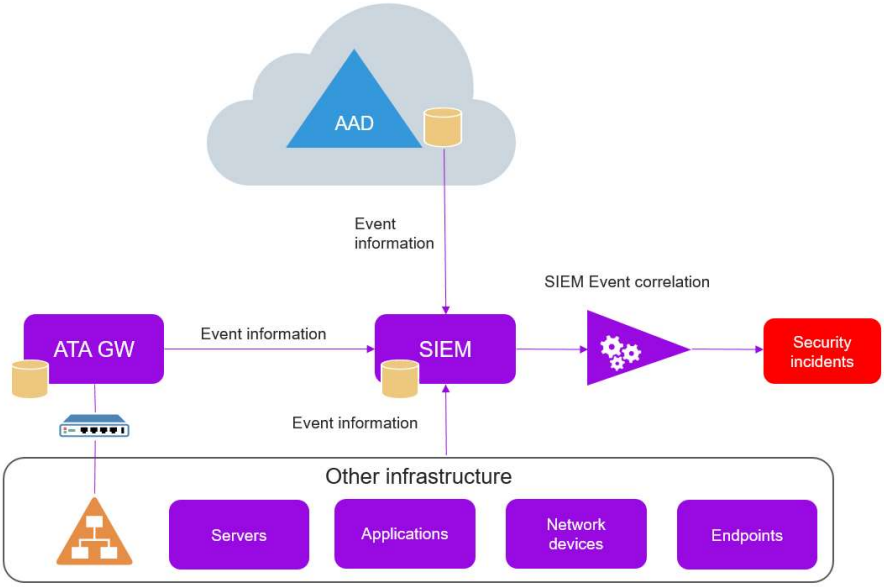


Figure 35 - Using SIEM for event correlation of identity activities

6.2.7 Securing access to on-premises web-applications

Azure Active Directory also enables access management of on-premises web applications through the cloud. Azure AD Applications Proxy can be used to securely publish web-applications located in on-premises data center. It provides reverse proxy, enables authentication and access policies for securing the access into applications. For more security, multi-factor authentication can be enabled in the access policies.

Azure AD Applications Proxy is a lightweight publishing capability which suits well for organizations which do not already have or do not want to invest in application publishing infrastructure.

Figure 38 illustrates Azure AD Application Proxy architecture and functionality. The only on-premises components required are connector software agents, which can be in theory installed into almost any server in a target network. The requirement is that there is an outbound Internet access from the network, which allows creating a secure tunnel between Agent and Azure AD Application proxy cloud service.

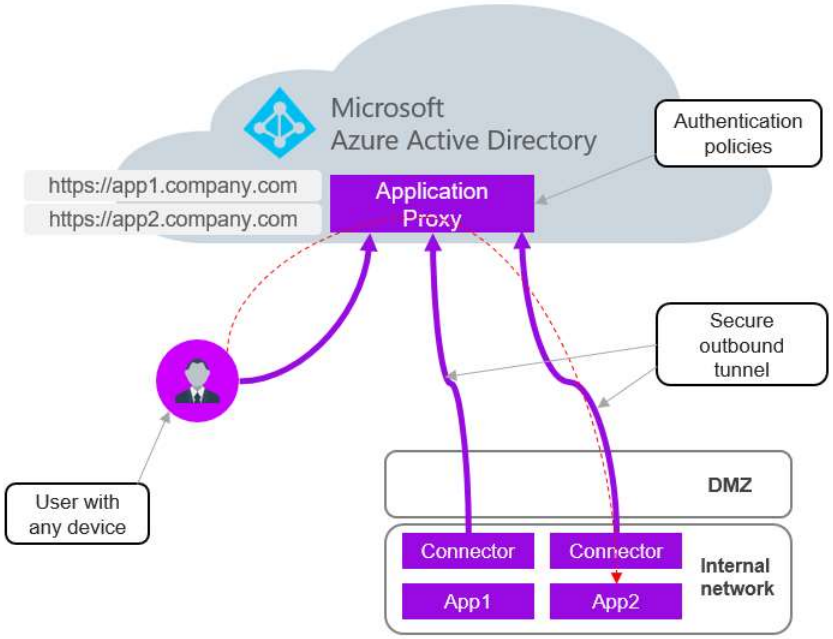


Figure 36. Azure AD Application Proxy

6.2.8 Access management and authentication of SaaS applications

Enterprises typically use multiple SaaS applications for running their daily businesses. Many times, separate user accounts are created on SaaS applications and access rights are managed in the application itself. When there are multiple applications, this means that a single user may have a huge amount of different accounts for logging into applications. This may be difficult for the users while they need to remember several accounts and passwords to them. From management perspective, the challenge is how to handle the lifecycle management of the dispersed accounts; for example, how to ensure that access rights are removed when users' employment contract is ending.

Azure AD Single Sign-On capabilities help with these challenges by enabling authentication into SaaS applications using users' AD or Azure AD identity. Azure AD support thousands of popular SaaS applications commonly used by enterprises.

User Identities and access rights can be managed in Azure AD and there is no need to create accounts for SaaS applications. If a user's contract is ending and the account disabled or removed, the user's access rights into all applications within the scope will be disabled. This enhances security and makes user experience better while users do not have to remember multiple accounts and passwords.

To enhance security more, it is possible to use Azure multi-factor authentication for securing the applications access. In addition, other security capabilities included into Azure AD can be used to protect identities and access.

6.2.9 Multi-factor Authentication and conditional access

Many organizations struggle with enabling multi-factor authentication while users complain that it is too difficult. Many times this leads into a situation where the multi-factor authentication is not deployed in the organization.

Azure multi-factor authentication together with conditional access policies and device registration allow building a modern authentication experience to almost any application. When using these technologies together in a right way, it is possible to create authentication so that it meets with enterprise security policies and at the same time, the user experience is simple and easy.

Azure multi-factor authentication

Azure Multi-factor authentication enables a basic strong authentication for the applications and secures the access by verifying users' identity in a trusted manner. The disadvantage of using multi-factor authentication is that it is difficult for the users in many access use cases (e.g. when using services from mobile devices). Multi-factor authentication request may be also time consuming and annoying for the end users.

To solve these user experience issues, conditional access is a recommended feature, which helps to build authentication policies so that e.g. multi-factor authentication is requested in access scenarios only when really needed. These access scenarios may

include accessing company services from external networks, and when using devices that are not company managed. At the same time, users may access services without multi-factor authentication from internal networks and company managed devices, which reduces the amount of multi-factor authentication requests dramatically and ensures a good user experience.

Device registration

To recognize which devices are company managed, ~~there can be used~~ Intune device registration can be used. Company devices can be registered to Intune management in device deployment process (or by instructing users to register their devices) and after that, Azure AD is aware of the users' devices. The device identity can be then used as a second factor in authentication policies configured with conditional access. This is a seamless and transparent multi-factor authentication while first the device identity is checked (something you have) followed by checking also the user credentials (something you know).

BYO devices may also be enrolled to company management and configured with applicable security policies. This way users may use the device of their choice to perform their work.

Single Sign-On (SSO)

When combining the benefits of a Single Sign-On (SSO) to this scenario, user experience starts to be at a very good level. Single Sign-On minimizes the times when credentials need to be asked from the user. The user may fill the credentials only once when logging into the user's device, and this same login information will be used to access company services.

Risk-based conditional access

To enhance the security even more, risk-based access policies enabled by Azure AD Identity Protection can be used. Azure AD Identity Protections machines learning algorithms and heuristics detect anomalies and suspicious activity indicating potentially compromised identities. When user risk level is set to high, risk based conditional access policies can trigger multi-factor authentication, user password reset or even block the access to application when it is necessary to minimize the risks.

Trusted device authentication model

These technologies together enable an easy and secure access to company services and there is no reason to skip the deployment of multi-factor authentication. All of the most risky access scenarios can be protected with proper authentication policies and the non-risky scenarios can remain as simple as possible for the end users.

Figure 39 illustrates a one type of scenario that can be built using conditional access. In this scenario, trusted devices may access the services with seamless multi-factor authentication (device identity as a second factor) and when the user uses some other device, multi-factor authentication is requested to check the user's identity.

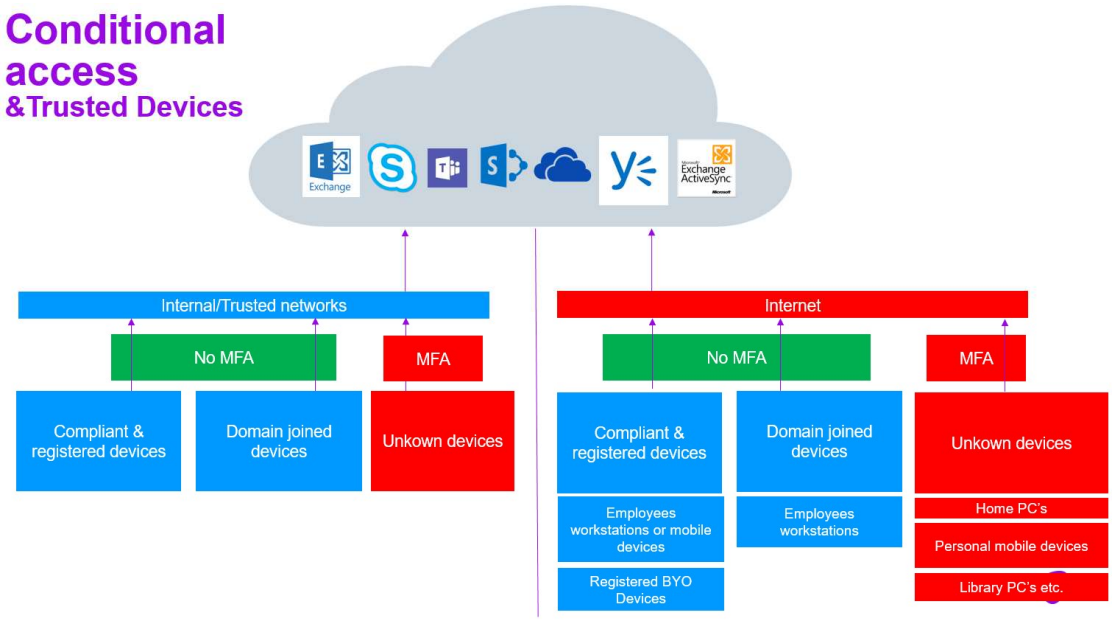


Figure 37. Conditional access and trusted devices

6.2.10 Providing application access for external users

Azure Active Directory Business to business capability enables the authentication of the external users to allow access into their business applications and other resources. Organization is able to grant access rights for the user identities from another company's Azure AD. If partner organization doesn't have their own Azure AD, also free Microsoft accounts can be used in similar way.

By granting access to partner organizations identities, organizations can avoid using of complex authentication or directory solutions and management of external accounts. In addition, the users experience is seamless and easy for business partners while they don't need any additional accounts.

6.3 Information protection

Azure Information Protection can be used to protect information in several ways. This section describes the main scenarios of how Azure Information protection can be used to protect information.

6.3.1 Recommended steps before implementing information protection solution

Before starting to implement any information protection solution, it is good to have an understanding of the kind of information the enterprise handles and categorize it. This helps to plan how the protections should be built. But how to do this? The enterprise might have a huge amount of data and it might be challenging to categorize all of it.

Good practice is to use information classification to define the sensitivity levels for information. These sensitivity levels can be almost anything, e.g. public, internal and confidential. The levels should be defined based on business environment requirements. It is anyways recommended to use a simple approach that is easy to understand.

These defined sensitivity levels can be later on used to label the data. Typically, information creator or owner defines the sensitivity level. Labeling is important for categorizing the information for applying protections. In manual information classification, these labels mean the sensitivity levels marked into the right top corner of each page of a document (Word documents). These labels are typically added when a document is created by the information creator or owner.

In addition, a definition is needed concerning the ways needed in order to protect the information of a specific sensitivity level. It is good to understand who should be

able to access information and what kind of actions are allowed to be done with information. This understanding helps when implementing information protection solution.

6.3.2 Azure Information Protection basic settings

Azure Information protection can be used in multiple ways to protect information. Before going through the use cases, there is a need to understand how the service is configured to make them work.

Administrators are able to configure policies to help users to protect their files and automate information protection when specified conditions are met. Azure Information can be configured with global policies that apply to all users in Azure tenant. Other policies can also be specified which are applied to specified groups in the organization. This capability helps to target policies to different departments and build information protection settings according to their requirements.

Inside these policies, administrators can define labels according to their sensitivity levels described earlier. These labels will then be used to categorise information and apply the configured information protection settings.

In protection settings the administrators are able to select if the information with the label should be protected or not. When protection is set on, documents will be automatically encrypted. Administrators can also select groups of users able to access the information, block users from sharing information, set adding watermarks or headers and set retention settings. In addition, there are some more advanced settings available. Applying of labels can also be automated in defined conditions. Figure 40 illustrates the settings panel. (Azure Information Protection 2018)

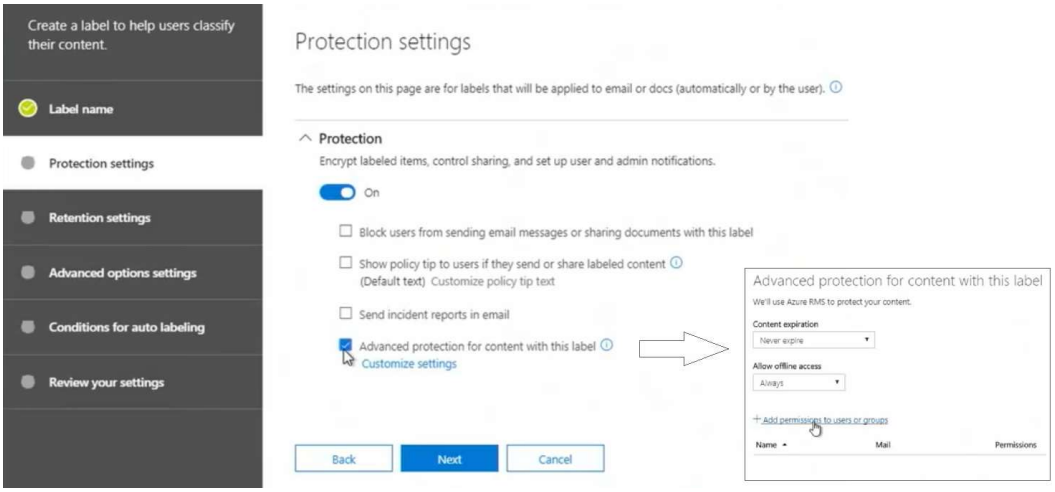


Figure 38. Configuring labels for Azure Information Protection

Azure Information Protection also creates corresponding rights management templates based on label settings. Rights management templates are used to protect information in some of the use cases of Azure Information protection. (What is Azure Information Protection 2018)

These labels and templates will be a basis for many protection capabilities and visible for the defined users. It is recommended to plan them well to make the information protection easy and effective.

6.3.3 Enabling users to protect files on-demand

Azure Information Protection enables several ways for on-demand file protection. First of all native options are available which are integrated into Office applications after enabling Azure Information Protections service. In addition the capabilities can be extended with Azure Information Protection client.

With all of these protection scenarios files will be encrypted and protected according to selected options. After protection, the files can be moved to any location securely, e.g. sent by email. Only people with permissions are able to access the protected files and perform only the defined actions. The protection stays with the file wherever it is sent.

File protection on Office applications

After Azure Information Protection is enabled and Office applications are connected into the service, information protection capabilities will become available for the end users. Users are then able to protect Office documents through “Protect Document” option on document settings.

Users can choose to select from predefined templates or define protection settings manually. Users can define the users or groups and set the level of access for them. In advanced settings the user can set printing and copying rules and set an expiration date for a document. Figure 41 shows the options panel for applying the protection.

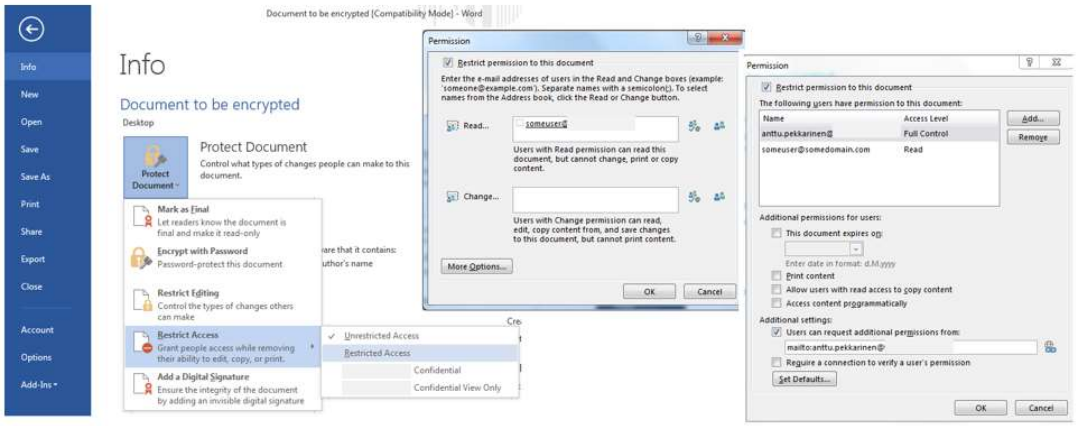


Figure 39. Azure Information Protection on-demand file protection

By installing Azure Information Plugin, there will be available also labels ribbon on Office Applications. From label ribbon the user can select the sensitivity class for the document for applying proper protections. With condition rules the administrators can configure the ribbon to also provide recommendations for selecting label based on content of the document. (Van’t Hag 2017)

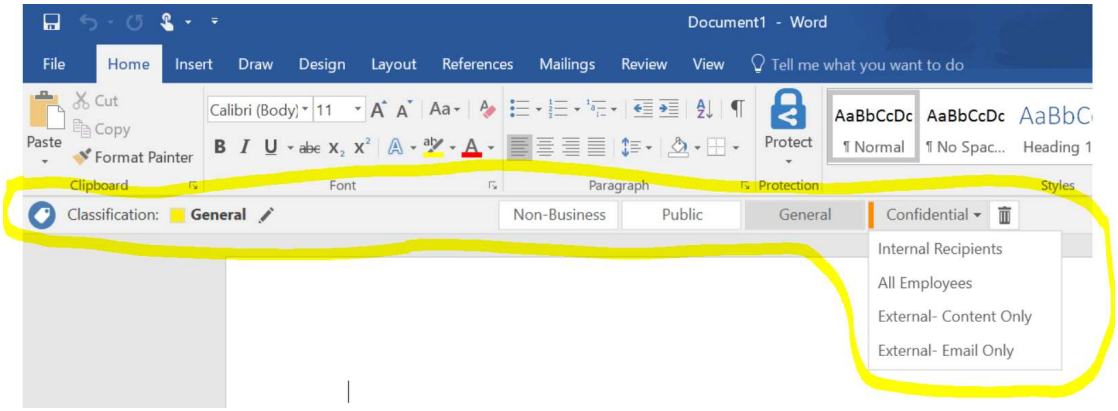


Figure 40. Azure Information Protection labels ribbon

Protecting files with Azure Information Protection Client

Azure Information Protection client is an application installed into a workstation needed for some use scenarios of Azure Information Protection. After installation information protection options will be available under a file's right click option panel. It also integrates with Office applications and there will be information protection ribbon on the Office applications. Figures 43 and 44 illustrates the options available.

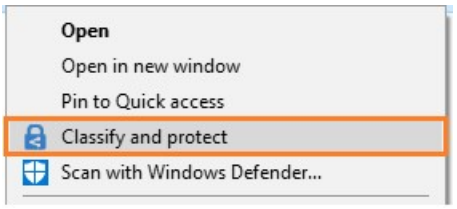


Figure 41. Azure Information Protection client options on right click panel

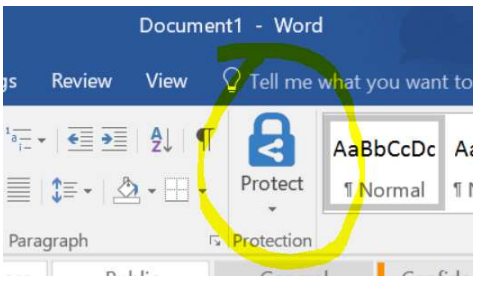


Figure 42. Azure Information Protection client ribbon on Office applications

With the Azure Information Protection client, users can simply right click the file they want to protect. The user can then select to use pre-defined labels for protecting the document or specify protection settings manually. Through manual settings, users

can select the level of permissions they want to give for the user (from predefined options) and select the users/users' groups which should be able to access the file. The user can also set an expiration date for the permissions. Users can find a shortcut for this protection option also from Office tools ribbon.

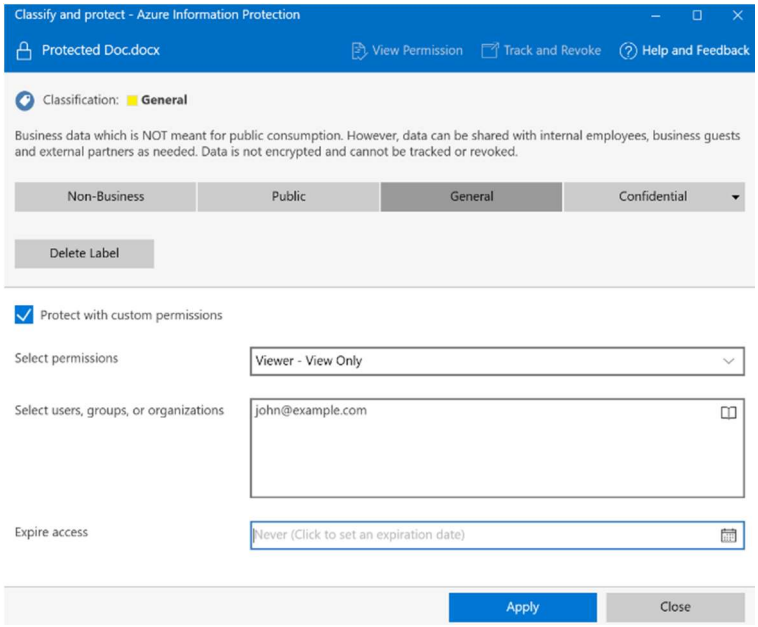


Figure 43. Azure Information Protection client

As a difference to the native protection option, Azure Information Protection client can be used to protect any type of file. The protected file is saved in a different file format ("p-file") which is kind of a shell for the original file. In case the original file is ".txt" the protected file will be ".ptxt". In addition, in case the original file is .ppt the protected file will be .pppt.

6.3.4 Enabling users to protect emails and attachments

With Azure Information Protection, users are able to protect emails by using pre-defined RMS-templates as they protect Office documents. The same functionalities for using labels are also available. By selecting template or label, selected protections are applied into message content and attachment. In addition, a "Do not forward" button is available in the Outlook message ribbon, which disables the forwarding option in email. (Gulati 2017)

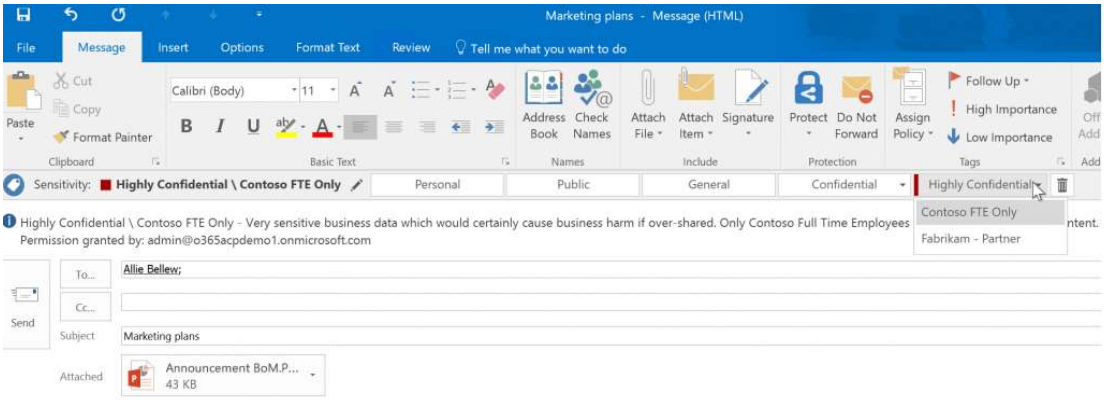


Figure 44 - Protecting emails with Azure Information Protection

In case Azure Information Protection Client is installed, users can also use the ribbon options (blue “Protect” button) to protect the email attachment. This option does not protect the email itself.

6.3.5 Automating information protection

By configuring conditions for auto labelling, Azure Information Protection can be set to provide recommendations for selecting the label and protections for a user. The recommendations are based on information types or custom phrases defined in condition settings. Azure Information protection has the most common sensitive types defined as built-in options. This capability works in both, documents and emails. Figure 47 shows how it the user sees it. (Azure Information Protection documentation 2018)

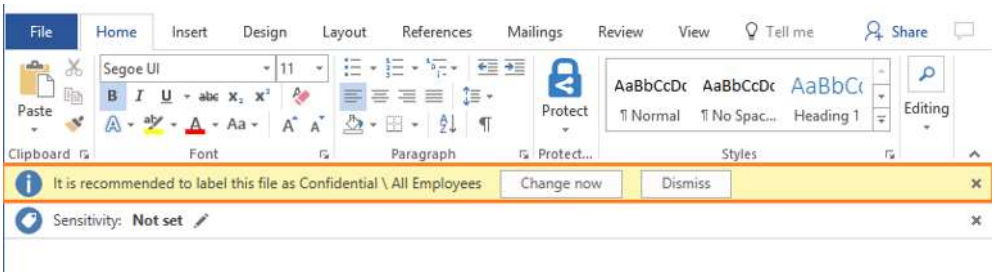


Figure 45. Azure Information Protection label recommendations

With same condition rules, Azure Information Protection can be configured to automatically apply a specific label into the document or email. For example, if a document or email includes credit card or social security numbers, information protection can be automatically applied for protecting sensitive data.

Applying of label can also be forced. In the general settings (see Figure below) of Azure Information Protection it is possible to define settings, which requires that all documents and email must have a label applied. (Van't Hag 2017)

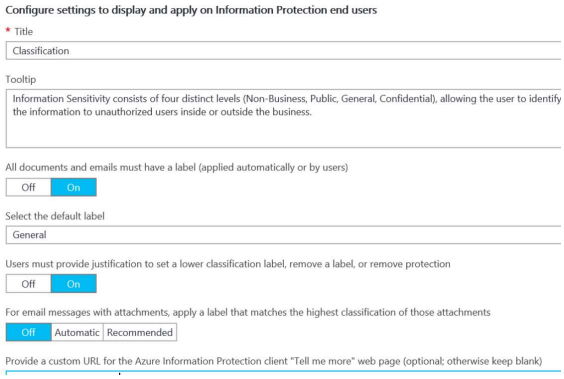


Figure 46 - Azure Information Protection settings

Recommendations and automatic protection capabilities help to ensure that information protections are applied and risks into data leakages can be reduced.

6.3.6 Revocation of information

Azure Information Protection also enables tracking and revocation of documents. The document owner may then e.g. disable access to document sent erroneously. The document owner may also view the access history of protected document. Figure 49 shows the portal for document tracking.

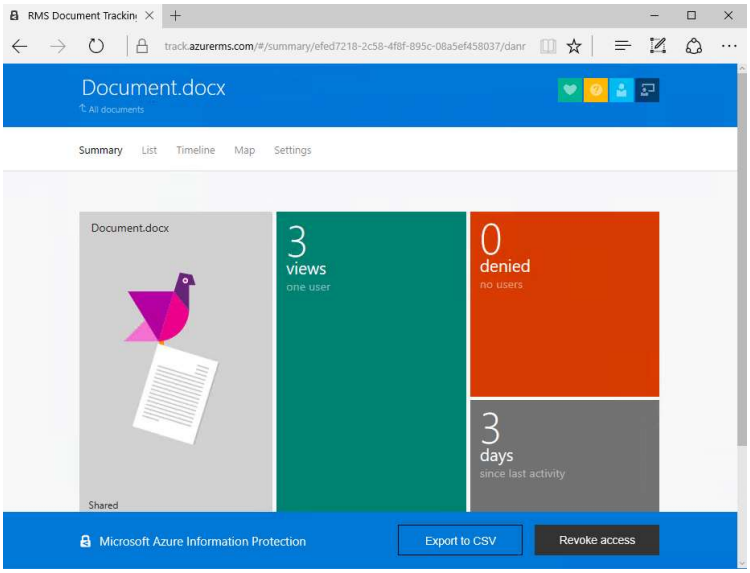


Figure 47. Revoking access to document

6.3.7 Preventing data leakages through third party apps and SaaS services

Intune app protection policies enable the prevention of data leakages by providing data protection controls for managed Office applications. Company data can be protected on applications even if devices are not enrolled into device management.

Without additional protections, users are able to work on business documents on Office applications and save files to any location, also into consumer applications which are not safe. Many times data is also synchronized into 3rd party cloud services.

App protection policies can be used to control saving and copying the data outside Office applications. Users can be allowed to save data into Office applications including OneDrive and copy paste data inside the Office applications freely. With app protection policies it is possible to prevent saving and copying the data outside these applications, which makes sure that the data is not leaked through non-safe consumer applications and after that into third party cloud services. (What are app protection policies 2018)

Applications control policies separate business data from the consumer's personal data and keep the confidential information saved in managed applications secured. (ibid.)

6.3.8 Automatic information protection for SharePoint libraries

Azure Information protection can be used to automatically encrypt files uploaded or created into SharePoint or SharePoint Online library. The files are accessible to only persons with access rights to the files. In case files are moved outside the library, protection travels with the files and the same protections still apply, which decreases the risk of data leakages.

Automatic information protection is not recommended for all enterprises; however, it is available for those who have such needs to protect a specific subset of highly confidential files. (Secure SharePoint Online sites and files.)

When enabling automatic information protection for SharePoint libraries, it is good to understand that the content of the files is not usable anymore by services such as Office 365, which means that some features will not be usable anymore. (Protect SharePoint Online files with Azure Information Protection.)

6.3.9 Automatic information protection for OneDrive

Azure Information Protection can be integrated with Cloud app security for automatically protecting files downloaded to cloud applications such as OneDrive for Business, SharePoint Online and Box.

Azure Information Protection automatically applies classification labels to files based on the configured policy. The policy can be configured to search specific substrings from content of the file, metadata and file name (see Figure 50 for settings). If some of those details match with the configured policy, a document classification label is added into the file. Cloud App Security can even replace the existing Azure Information protection label.

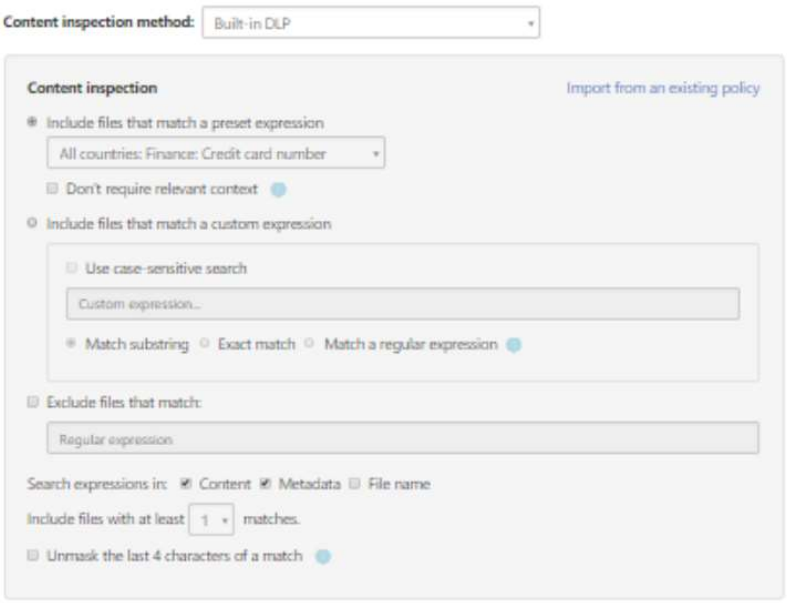


Figure 48. Content inspection settings

Cloud App protection can be used to ensure that confidential files are automatically protected properly when uploaded to OneDrive for Business. (Azure Information Protection Integration 2018)

6.3.10 Automatic information protection for file shares

Azure Information Protection together with File Classification Infrastructure (FCI) enables automatic protection of files, which match with the configured conditions, on Windows file shares. Conditions can be configured by using built in content classifiers or by using a custom value strings.

Automatic protection can be used to enhance security and reduce the risk of data leakages by protecting confidential information uploaded into the file share. (RMS protection with Windows Server File Classification Infrastructure 2018)

6.4 Device management

Microsoft Intune provides device management capabilities as a cloud service. It enables management of mobile devices and controlling of security settings. In addition, it also provides lightweight management of workstations. This section

presents some basic capabilities of Intune product which can be used to enhance security of devices.

Deployment and management of mobile devices

Intune makes the deployment process of devices easy. After a mobile device is delivered to an end user, the user just needs to install management portal app and login (multi-factor authentication can be required), which is an easy task and can be instructed to the user. After this, the device will be automatically enrolled and made MDM managed.

MDM profile installed to a device will configure device security settings according to the policies defined by administators. After the security on the device is compliant, it is safe to allow access to business information with it. The enrollment can also be set as a requirement for accessing e.g. corporate email or other applications, which forces users to enroll their devices into management before access to business data is allowed with the device. This guides the users to enroll their devices into MDM. (Manage BYOD and corporate-owned devices with MDM solutions 2017)

In addition, Intune enables controlling the application installations on mobile devices. Applications can be distributed and installed into mobile devices automatically. For example, when a user's devices are deployed into use, the needed applications will be installed after enrolling process. Administrators are also able to distribute and manage certificates, VPN profiles and email profiles installed to devices. (ibid.)

With these capabilities, the administrators can ensure that the devices are secured and fully ready for business use after enrollment.

Securing mobile devices

Mobile devices can be secured with Intune in multiple ways. The most basic protection is to set the requirements for using passcode. Before accessing a mobile device, the user can be required to fill in a PIN code, or authenticate with fingerprint sensor or face recognition. The length and complexity of PIN code settings can be set according to requirements. The screen lock time can be controlled for requiring the passcode, after the device has been unused for a period of time.

To protect access to data without entering passcode, Intune can control a devices´ data encryption settings. However, there are some differences how it is possible to control these settings on different device operating systems. (Configure device restriction settings in Microsoft Intune 2018)

In case a device is lost or stolen, the business data on the devices can be wiped out by removing the apps, email, data and networking profiles from the user's devices remotely. Device data can also be completely wiped out.

For controlling software vulnerabilities Intune provides capabilities for managing the software versions of devices and applications. This feature ensures that the devices are functional and have their security updates installed. This reduces the attack surface and the amount of known vulnerabilities. (Protecting and empowering your connected organization 2017)

Intune includes a variety of different security controls for devices beyond these basic protections.

Deployment and provisioning of Windows 10 devices – Modern management

Intune with Windows 10 enables a modern way of deploying and provisioning new devices into organizational use. It is possible to create self-contained provision packages using Windows Imaging and Condifuration Designer (ICD). These enable dynamic provisioning and transforming of new devices into fully-configured and managed devices without re-imaging. Dynamic provisioning makes it possible that end-users are able to self-provision their devices. In theory, a user may be allowed to pick a Windows 10 device from any supermarket and provision it as a business device. (The Path to Modernizing Windows Management 2018)

Self-provisioned devices are not AD-joined devices but are managed by Intune and can be joined to Azure AD with "Azure AD join" feature. This is called "modern management". Many organizations still require devices to be joined to AD to provide full capabilities and management. Some of the important security settings cannot still be controlled with Intune. (The Path to Modernizing Windows Management 2018)

Modern management is just another option for the use of scenerios where lightweight management fullfills the requirements. It is a modern way to enable for

example CYOD (Choose Your Own Device) and BYOD (Bring Your Own Device) management. It enables basic security controls of devices so that a secure access into organizations´ business applications can be allowed.

Unified device management

In addition to the management of mobile devices and applications, Intune also provides the management of PCs from the same console. There is an integration to System Center Configuration Manager, which makes this possible and allows consistent management experience across all organizations devices. (Protecting and empowering your connected organization 2017)

6.5 Mobile Application Management (MAM)

Intune Mobile Application Management (MAM) makes it possible to control applications and the data on mobile apps with or without enrollment of the devices.

Application management enables installation of mobile apps to employees' devices, updating applications, configuring the applications and controlling how the data on the application can be used. (What is Intune 2018)

Application management can also be used to manage applications on devices not enrolled into MDM management, e.g. on Bring Your Own device scenarios. Application management can be used in co-existence with other vendors´ DM products. (ibid.)

How Application Management enhances security?

On MDM managed devices Application Management enables control into applications what can be installed on devices. Harmful applications can be blocked to avoid security risks and there is a visibility into installed applications. Organizations can also publish managed business applications through a company portal. In addition to installations, Intune enables controlling of settings of the applications for ensuring that those are configured in a secure manner. (ibid.)

The updating feature of applications is useful for vulnerability management. In case a known security vulnerability is identified, it is easy to check if there are vulnerable business applications on a user's devices. Vulnerable business applications can then be easily updated also on devices that are not enrolled to MDM. (ibid.)

Application control policies enable separating the consumer data and business data on the applications. Business data can be then protected in a proper manner. For example, copying the data to other non-managed applications can be prevented with policies. In addition, a remote wipe feature enables wiping out the business data from users' business applications if a mobile device is lost or stolen (without removing other personal data or applications). (Protecting and empowering your connected organization 2017)

6.6 SaaS applications usage protection

Shadow IT causes risks of data leakages when saving business data to applications that are not secured properly. According to Stratecast research, over 80% of employees admit that they use non-approved SaaS applications for work purposes. Hence, it is very likely that some business data is also copied into unsecure applications. (EMS Vision Whitepaper.)

Cloud App Security provides visibility into Cloud Applications usage by collecting information from organizations' firewalls and proxies. This information can be then used to identify non-approved applications usage. It can also identify suspicious activities, user mistakes and other potential threats related to SaaS applications usage.

Cloud App Security also provides controls for managing the access and limiting the usage of non-approved applications. In case a non-approved application is identified, Cloud App Security can also be used to block them. In case this strong action is not wanted, users can be also guided to use safe applications instead of unsecure applications. (Protecting and empowering your connected organization 2017)

7 EM+S as a part of overall security controls of cloud services

Microsoft Enterprise Mobility + Security offering provides a rich toolset for providing security controls, which helps to secure hybrid cloud identity infrastructure, access to services, mobile devices, mobile applications and information itself. Security capabilities can also be extended into on-premises side. When thinking about the overall security of cloud services, there are still many parts not covered by EM+S. To secure cloud services well, also other practices and security controls are required to cover these areas.

Overall security of cloud services

Figure 51 illustrates some of the areas needing additional attention. Everything begins with understanding the enterprise's own responsibilities. Many times cloud services have built-in security capabilities; however, if those are not deployed correctly, they do not provide any security. Typically, these security controls also need at least some administration and management, which is daily work that has to be done by someone. Practices, processes and manuals are also important for keeping the cloud services secured. Cloud services, people and security threats are constantly changing and the security state of the services needs to be evaluated from time to time, to ensure that security controls are up to date.

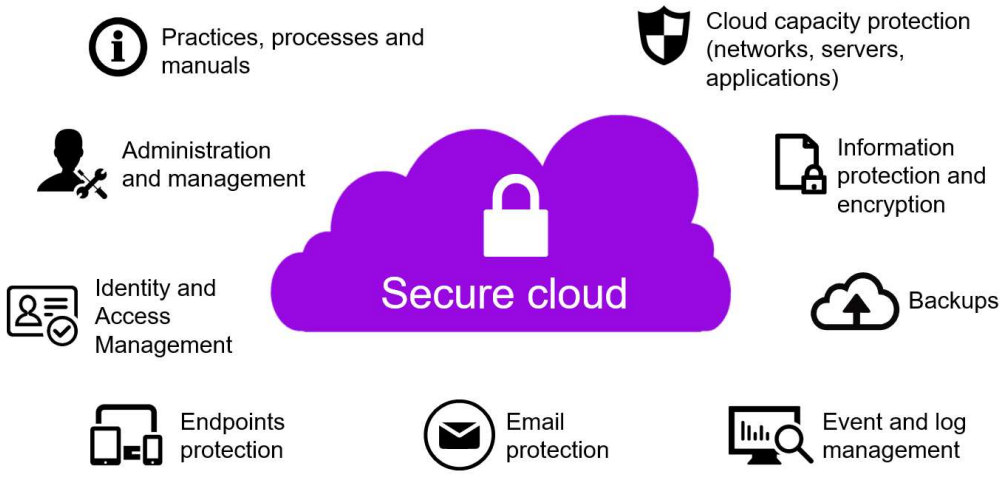


Figure 49. Security building blocks of cloud services

Identity and Access Manament

Identity and Access Management is an area where EM+S tools are very useful. Identity and Access Management still requires proper processes and the controls on the on-premises side if there is a hybrid identity infrastructure.

Endpoints protection

To secure endpoints, EM+S currently provides management capabilities for mobile devices and applications. It also has some features for workstations management, however, currently these capabilities do not cover all the same controls available as an example through Group Policy. The endpoints should also have virus and malware protections in place.

Email security

Email security is one of the most important additional security controls required, email being one of the most used applications in enterprises. Typically, an additional service is needed to cover good security protections of email and especially phishing protections. Azure Information, included in EM+S, covers only the protection of the sensitive information included in emails and data sent by email, when used correctly.

Information Protection

Azure Information Protection covers the information protection part quite widely. However, it is good to remember that on cloud infrastructure and applications the data might require other information protection capabilities, such as encryption of disks or databases.

Backups

Backups are something commonly forgotten by enterprises when using cloud services. Cloud services are also vulnerable to malware such as ransomware, and technical issues that potentially can corrupt the data saved on the services. Typically, cloud providers take care of the backups of the cloud service and maybe the infrastructure part; however, the applications´ data backups are typically not included in the standard service. It is recommended to backup cloud data outside the cloud infrastructure in a safe location.

Event and log management

Cloud services typically have event and log management capabilities built-in. Enterprises need to ensure that auditing is enabled and needed logs are collected. For managing the log data and storing it a required time period, also log management or Security Information and Event Management (SIEM) system might be required.

Cloud capacity protection

When using cloud capacity services such as Azure, it is good to remember that the same security protections are still needed on the cloud side as in the on-premises infrastructure. Network architecture needs to be built in a secure way and there should be firewall and IDS/IPS capabilities just like in on-premises network (in case they are required from security or compliance perspective).

Servers and applications still need similar attention including antivirus and hardenings of the configuration. Especially application security still requires attention while enterprises might use custom business applications running on cloud infrastructure. Vulnerability management is one of the key controls to get visibility and controls to application vulnerabilities. Security updates of servers and applications should not be forgotten as well.

Overall, there are dozens of different matters to think about when implementing security controls for cloud capacity just as there are in on-premises environment.

8 Conclusions and discussion

This master's thesis was a theoretical research where information was collected about identity, access and mobility management related challenges on cloud services. The research was a highly interesting and an educational experience. During this thesis a huge amount of literature and documentation were processed about the topic, which increased personal knowledge. In addition, there was opportunity to meet real professional , who shared information based on real experiences. Meeting those professionals was eyes opening.

The first part of the thesis was a research about security challenges related to the topic. A large amount of existing reseach material was gathered from sources such as Forrester and Gartner for understanding the current challenges. These researches created a basis for interviewing people working around these challenges in real life. There was an opportunity to discuss these with real experts and ask more detailed questions and opinions about specific topics. It was interesting to see how differently people think about some of the areas. In all interviews a new type of challenges were identified. One issue common for the interviews was that the balancing between security and user experience is challenging when securing cloud services. Challenges identified in the reseaches were related to earlier experiences from daily work and customer's real life challenges.

For this thesis officially interviewed were approximately 10 different professionals working around identity, access and mobility management related roles and they were well aware of security challenges as well. During daily work many other highly respected professionals were met, who were not officially interviewed but information was collected during business conversations and meetings. The interviewees included employees from IT service provider companies (Tieto Finland Oy, Inmics Oy), their customers, partners and vendors. The employees worked in different roles mainly between technology and business (e.g. architects, IT managers or consultants). In interviews almost 70 different challenges were discovered. The most common challenges are introduced in the solution map in section 7.1.

The finding of suitable interviewees was one of the most challenging parts of the thesis. There could have been more interviewees for wider and more creditable results.

The technology stack in Microsoft Enterprise Mobility + Security (EM+S) offering is very wide and contains a huge amount of services which help to secure enterprise environments. It was highly beneficial to go through all this technology and learn about their benefits. Before writing this thesis, it was not clear how these technologies are related to each other; however, documenting the most important parts of the technologies helped to understand their relations.

The selected research method (qualitative research) worked as expected in the thesis and it was easy to use. The data that needed to be collected was non-numeric data which was not easy to expect without research. The combination of collecting existing research data and interview data, combined with tacit information based on real life experiences was a perfect combination to gather the needed information. After the information was collected, it was quite easy to write the documentation and create a structure for the thesis.

The objectives of this thesis was fulfilled very well and the research questions were answered through the results. The first objective was to identify the main challenges of hybrid cloud security on identity, access and mobility management. The challenges were identified and documented. Based on the interviews and customers' real life challenges, it was easy to identify relations and see that the identified challenges are real. As an experimental validation method, social media (LinkedIn) was also used to evaluate the challenges. The social media experiment gave an extra validation for challenges, and comments from respected industry influencers gave more thoughts and led into the right direction.

Tacit information collected during this thesis is also included in the work and can be easily forwarded through this thesis.

Another objective, a holistic description of EM+S, was created and it gives quite a comprehensive overview of and explanations about technologies in the offering. It has been useful also in daily work while the documentation gives a shortened basic

overview of specific technologies. It is easy to find the information that is needed and forward it to others.

Creating of holistic description of EM+S was the task that generated the major workload. The available information amount was huge and it was hard to select which source materials to use. Technology stack on EM+S is so wide that it was time consuming to go through all of its parts.

The most important part of the thesis and a primary objective was to identify and describe the solutions on how EM+S offering can be used to enhance security. Some level of solution was found into almost all most common security challenges identified in research. As a conclusion, seems that Microsoft has designed EM+S offering based on actual business needs.

The solution descriptions have been a huge help in product and service development work and they also have supportive concerning security enhancements on customer environments. They help to identify how EM+S can be effectively used to enhance security and define the service part around the technology. In addition, solution descriptions help enterprises to identify capabilities of EM+S and get the most out of their technology investment.

In addition, an explanation was shortly documented on which parts of the security EM+S cannot cover. This might be useful when thinking about technology investments and identifying the parts not within the scope of EM+S. Explanations fulfill the solution part by providing additional information beyond the original scope of this thesis.

Research work could have continued with comparing technologies from different vendors in addition to EM+S offering's technology. Most of the technologies have also corresponding solutions available from other vendors. It would be useful to understand the differences of Microsoft technologies and third party technologies when selecting tools for securing cloud environments.

References

Application access enhancements for Windows Azure Active Directory. Microsoft web page. Accessed on 29.10.2017. Retrieved from https://ppe.blogs.technet.microsoft.com/ad/2013/07/07/application-access-enhancements-for-windows-azure-active-directory/

Active Directory Federation Services. Microsoft web page. Accessed on 20.1.2018. Retrieved from https://msdn.microsoft.com/en-us/library/bb897402.aspx

Arsenault B. 2015. Enterprise security for our mobile-first, cloud-first world. Accessed on 12.8.2016. Retrieved from http://blogs.microsoft.com/blog/2015/11/17/enterprise-security-for-our-mobile-first-cloud-first-world/#sm.0019o98ldc4udyk10la1djc17t38q

Azure Active Directory B2C. Microsoft web page. Accessed on 30.12.2017. Retrieved from https://azure.microsoft.com/en-us/services/active-directory-b2c/

Azure Active Directory Domain Services. Microsoft web page. Accessed 30.12.2017. Retrieved from https://azure.microsoft.com/en-gb/services/active-directory-ds/

Azure Active Directory Identity Protection documentation. Microsoft web page. Accessed on 1.3.2017. Retrieved from https://azure.microsoft.com/en-us/documentation/articles/active-directory-identityprotection/

Azure Active Directory password reset for IT administrators. Microsoft web page. Accessed on 16.3.2017. Retrieved from https://docs.microsoft.com/en-gb/azure/active-directory/active-directory-passwords

Azure Active Directory reporting. Microsoft web page. Accessed on 30.12.2017. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-azure-portal

Azure Active Directory risk events. Microsoft web page. Accessed on 30.12.2017. Retrieved from https://docs.microsoft.com/en-gb/azure/active-directory/active-directory-identity-protection-risk-events

Azure AD Conditional Access documentation. Microsoft web page. Accessed on 16.9.2018. Retrieved from https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/

Azure ATP Architecture. Microsoft web page. Accessed on 15.9.2018. Retrieved from https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-architecture

Azure Information Protection. Microsoft web page. Accessed 25.4.2018. Retrieved from https://microsoftmechanics.libsyn.com/azure-information-protection

Azure Information Protection Documentation, Accessed 25.4.2018. Retrieved from https://docs.microsoft.com/en-us/azure/information-protection

Azure Information Protection integration, Accessed 27.7.2018. Retrieved from https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

CIO's Guide To Azure AD. Microsoft web page. Accessed on 1.1.2018. Retrieved from https://info.microsoft.com/CIOsGuideToAzureAD.html?ls=Website

Conditional access in Azure Active Directory. Microsoft web page. Accessed on 7.3.2017. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access

Configure device restriction settings in Microsoft Intune. Microsoft web-page. Accessed on 14.10.2018. Retrieved from https://docs.microsoft.com/en-us/intune/device-restrictions-configure

Conway A. 2016. Introducing Enterprise Mobility + Security. Accessed on 12.8.2016. Retrieved from https://blogs.technet.microsoft.com/enterprisemobility/2016/07/07/introducing-enterprise-mobility-security/

Enable secured productivity from anywhere, on any device. Microsoft web page. Accessed on 1.3.2017. Retrieved from https://www.microsoft.com/en-us/cloud-platform/conditional-access

Forrester. 2012. Forrester research: BT Futures Report: Info workers will erase boundary between enterprise & consumer technologies. Accessed on 2.8.2016. Retrieved from https://www.forrester.com/report/Info+Workers+Will+Erase+The+Boundary+Between+Enterprise+And+Consumer+Technologies/-/E-RES77881

Find unmanaged cloud applications with Cloud App Discovery. Microsoft web page. Accessed 30.12.2017. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-cloudappdiscovery-whatis

Forrester. 2014. Forrester Consulting Thought Leadership Paper (Commissioned by Microsoft): Overcome Security And Identity Management Challenges In Enterprise Mobility With The Right IT Infrastructure. Accessed on 2.8.2016. Retrieved from http://www.evros.ie/_fileupload/Documents/Overcome_Security_and_Identity_Management_Challenges_in_Enterprise_Mobility_with_the_Right_IT_Infrastructure.pdf

Forrester. 2016. Forrester report - AD in the cloud is a reality. Accessed on 2.8.2016. Retrieved from https://www.forrester.com/report/Brief+Active+Directory+In+The+Cloud+Is+A+Reality/-/E-RES133331

Gulati, G. 2017. Extended email security and compliance with Azure Information Protection. Accessed 25.4.2018. Retrieved from https://cloudblogs.microsoft.com/enterprisemobility/2017/10/24/extended-email-security-and-compliance-with-azure-information-protection/

How and why applications are added to Azure AD. Microsoft Web page. Accessed on 29.10.2017. Retrieved from https://docs.microsoft.com/en-gb/azure/active-directory/develop/active-directory-how-applications-are-added

How to configure security alerts in Azure AD Privileged Identity Management. Microsoft web page. Accessed 2.3.2017. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-privileged-identity-management-how-to-configure-security-alerts

How to provide secure remote access to on-premises applications. Microsoft web page. Accessed on 2.3.2018. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-application-proxy-get-started

How to require MFA in Azure AD Privileged Identity Management. Microsoft web page. Accessed on 30.12.2017. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-privileged-identity-management-how-to-require-mfa

How to start an access review and Azure AD privileged Identity Management. Microsoft web page. Accessed on 5.3.2017. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-privileged-identity-management-how-to-start-security-review

Hybrid Identity Datasheet. Microsoft pdf file which has been received from Microsoft. 2014.

Hybrid identity whitepaper. Microsoft product whitepaper. Accessed on 7.11.2017. Retrieved from http://download.microsoft.com/download/d/b/a/dba9e313-b833-48ee-998a-240aa799a8ab/hybrid_identity_white_paper.pdf

Identity driven security. Microsoft web page. Accessed on 5.6.2017. Retrieved from https://www.microsoft.com/en-us/cloud-platform/identity-driven-security

Identity + Access Management. Microsoft web page. Accessed on 18.8.2016. Retrieved from https://www.microsoft.com/en-us/cloud-platform/identity-management

Identity + Mobile Management + Security. Microsoft web page. Accessed on 14.8.2016. Retrieved from https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility

Inmics website. Accessed 9.9.2018. Retrieved from https://www.inmics.fi/

Madden, J. 2016. Azure Active Directory. Identity and Access Management and Windows 10 – Whitepaper. Accessed 18.8.2016. Retrieved from https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-Whitepaper-JMActiveDirectoryandIdentityWhitepaper.pdf

Manage BYOD and corporate-owned devices with MDM solutions. Microsoft web page. Accessed on 5.6.2017. Retrieved from https://www.microsoft.com/en-us/cloud-platform/mobile-device-management

Managing applications with Azure Active Directory. Microsoft web page. Accessed on 5.6.2017. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-enable-sso-scenario

Microsoft Identity Manager Datasheet. Microsoft product whitepaper. Accessed on 1.12.2018. Retrieved from https://www.keyon.ch/en/Produkte-Loesungen/Microsoft-MIM/Microsoft_Identity_Manager_2016_datasheet.pdf

Microsoft Identity Manager. Microsoft web page. Accessed on 29.10.2017. Retrieved from https://www.microsoft.com/en-us/cloud-platform/microsoft-identity-manager

Microsoft security intelligence report volume 22. Microsoft web page. Accessed on 25.8.2018. Retrieved from https://www.microsoft.com/en-us/security/intelligence-report

Plastina, D. 2016. Announcing the Azure Information Protection, Accessed on 7.1.2018. Retrieved from https://cloudblogs.microsoft.com/enterprisemobility/2016/06/22/announcing-azure-information-protection/

Protect SharePoint Online files with Azure Information Protection, Accessed 27.7.2018. Retrieved from https://docs.microsoft.com/en-us/office365/enterprise/protect-sharepoint-online-files-with-azure-information-protection

Protecting and empowering your connected organization with Microsoft Enteprise Mobility + Security. Microsoft web page. Accessed on 5.6.2017. Retrieved from https://info.microsoft.com/protecting-and-empowering-your-connected-organization.html?ls=website

RMS protection with Windows Server File Classification Infrastructure, Accessed 27.7.2018. Retrieved from https://docs.microsoft.com/en-us/azure/information-protection/rms-client/configure-fci

Secure SharePoint Online Sites and files, Accessed 27.7.2018. Retrieved from https://docs.microsoft.com/en-us/office365/enterprise/secure-sharepoint-online-sites-and-files.

Securing privileged access in Azure AD. Microsoft web page. Accessed on 23.4.2018. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/active-directory-securing-privileged-access

Set up Azure Active Directory for self-service group management. Microsoft web page. Accessed 19.11.2017. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management

Simons. A. 2016. Identity and security innovations for your enterprise. Accessed 9.9.2018. Retrieved from https://cloudblogs.microsoft.com/enterprisemobility/2016/02/24/identity-and-security-innovations-for-your-enterprise/

The Path to Modernizing Windows Management. Accessed 26.4.2018. Retrieved from https://cloudblogs.microsoft.com/enterprisemobility/2016/03/23/the-path-to-modernizing-windows-management/

Telia Inmics-Nebula. Telia Inmics-Nebula web site. Accessed 29.10.2018. Retrieved from https://www.inmicsnebula.fi/fi/telia-inmics-nebula

Tieto. Tieto web page. Accessed 9.9.2018. Tieto web site. Retrieved from https://www.tieto.fi/tiedosta

Van't Hag, R. 2017. Modern Workplace Management with Enterprise Mobility + Security – Part 3, Accessed 25.4.2018. Retrieved from http://bright-streams.com/?tag=azure-information-protection

Verizon. 2013. Verizon's 2013 Data Breach Investigations Report. Accessed on 12.8.2016. Retrieved from http://www.thesecurityblogger.com/verizons-2013-data-breach-investigations-report/

What are app protection policies, Accessed 26.7.2018. Retrieved from https://docs.microsoft.com/en-us/intune/app-protection-policy

What is Advanced Threat Analytics. Microsoft web page. Accessed on 22.4.2018. Retrieved from https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata

What is Azure AD B2B. Microsoft web page. Accessed on 30.12.2017. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-what-is-azure-ad-b2b

What is Azure AD Connect Health. Accessed 22.7.2018. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/connect-health/active-directory-aadconnect-health

What is Azure AD Privileged Identity Management. Microsoft web page. Accessed on 1.3.2017. Retrieved from https://azure.microsoft.com/en-us/documentation/articles/active-directory-privileged-identity-management-configure/

What is Azure Advanced Threat Protection. Microsoft web page. Accessed on 2.9.2018. Retrieved from https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp

What is Intune, Accessed 27.7.2018. Retrieved from https://docs.microsoft.com/fi-fi/intune/introduction-intune

What is Azure Information Protection. Microsoft web page. Accessed 25.4.2018. Retrieved from https://docs.microsoft.com/en-us/azure/information-protection/understand-explore/what-is-information-protection

What is Azure Multi-Factor Authentication. Microsoft web page. Accessed on 5.3.2017. Retrieved from https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication

Windows Server 2012 R2 Access and Information Protection Datasheet. Microsoft web page. Accessed on 2.3.2017. Retrieved from http://download.microsoft.com/download/C/7/8/C78D5EC8-2356-423D-8760-D0A8BAFC5C66/Windows_Server_2012_R2_Access_and_Information_Protection_Datasheet.pdf

Appendices

Appendix 1: Interview questions form

Master's thesis research questions – Identity/Access management and mobility related security challenges with cloud services

1. What kind of identity and access management related challenges are enterprises facing with cloud services? Name top three general challenges.

   a) _____

   b) _____

   c) _____

2. What is the biggest security threat related to user and device identities?

   _____

3. Do you see the mobile security as a challenge for enterprises? How big a challenge is on the scale of 0-5?

   ☐ Yes
   ☐ No
   Rating: Choose an item from this list

4. What kind of challenges do enterprises face on mobility?

   _____

   _____

   _____

5. What kind of challenges do enterprises face in data protection when using cloud services?

   _____

   _____

   _____

6. How big an issue is the separation of corporate and personal data on a scale of 0-5?

Rating: Choose an item from this list

7. What kind of challenges are enterprises facing today on applications' access, when using hybrid cloud services?

8. What kind of challenges do enterprises face with device management?

9. What kind of challenges do enterprises face with applications management?

10. What kind of challenges do enterprises face with user experience when using cloud services. Name top three challenges?

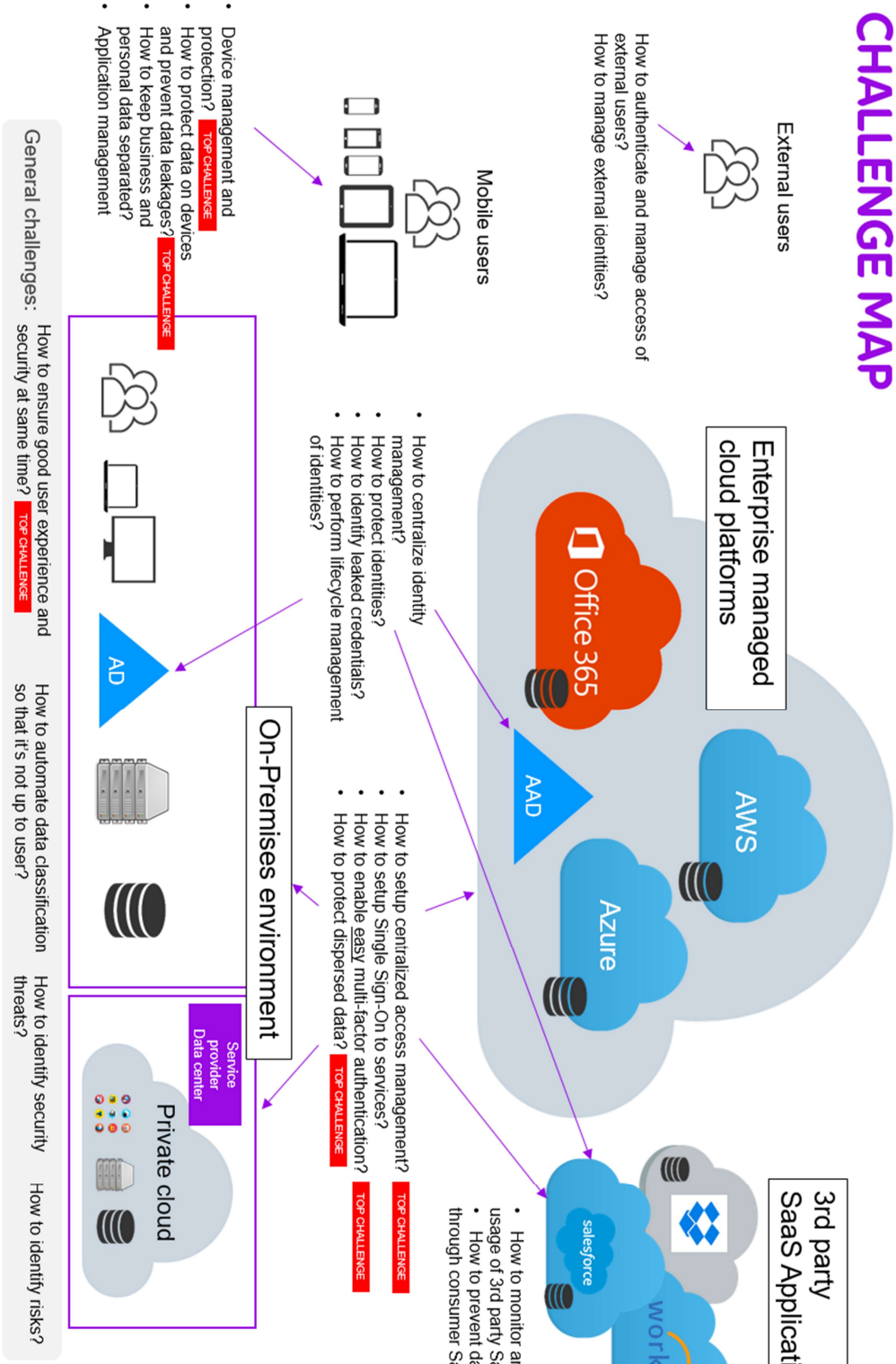
a)

b)

b)

11. Name the biggest challenge for enterprises from these options:
    - ☐ Security management in general
    - ☐ Identity management and protection of the identities
    - ☐ Access management & secure applications access
    - ☐ Data protection
    - ☐ Device management
    - ☐ Mobile applications management
    - ☐ Enabling good user experience while maintaining sufficient security controls

Appendix 2: Challenge map



Appendix 3: Solution map