Transforming technical IT security architecture to a cloud era

Case: Aalto University

Marko Loukkaanhuhta

Master's thesis
May 2021
School of Technology
Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Loukkaanhuhta, Marko

Transforming technical IT security architecture to a cloud era. Case: Aalto University

Jyväskylä: Jyväskylä University of Applied Sciences, May 2021, 64 pages.

School of Technology, Degree Programme in Information Technology, Cyber Security. Master's thesis.

Permission for web publication: Yes

Language of publication: English

Abstract

Like many other organizations, Aalto University has enabled its users to take advantage of the flexibility and ease of data processing provided by SaaS cloud services. SaaS cloud services can be usually described as separate island tied to organization identity, separate from the rest of the organization's IT infrastructure, to which the user has access regardless of time and place. The user's easy access to the data also allows easy access for the cybercriminals in case user's credentials got into the wrong hands. Different threats also affect data processed in the cloud in different ways. However, during the cloud transition, the security architecture of organizations has often remained almost unchanged and reflected a time when security focused mainly on protecting the local network from external threats. This raised the question of how the cloud transition will affect an organization's security capabilities.

The answer to the question was sought by looking at the capabilities of the perimeter-centric security architecture against cloud security threats. It was very quickly noticed, that if there is no connection between the on-premises security systems and the cloud, other than the identity synchronized or projected into the cloud, there is no visibility to cloud security events. To address this, a proposal for a security architecture was designed. Architecture proposal took advantage of the security features included with the Microsoft 365 A5 and EMS E5 licenses. Once the architecture with better cloud security was designed, it was also put into practice. The security situation, alerts and observations were examined over a period of one month and the results obtained were analyzed. A technical security expert, who is also responsible for the organisation's SOC activities, was interviewed in order to obtain a qualitative view of the implemented architecture and its security capabilities.

The results showed that perimeter-centric security is not sufficient in the era of cloud services. Some visibility into the cloud can be achieved by importing the logs, provided by the cloud, into the SIEM system. But the best result was obtained when the log data was processed with CASB and Sentinel products in the cloud. The limitations of the local SIEM system in handling cloud logs were also noted. Even if the logs were imported into the SIEM system, it does not eliminate the problem, that security controls are not present in the cloud security. Cloud security controls should be implemented using cloud tools, utilizing advanced machine learning and artificial intelligence products whose alarms were found to be less frequent.

Keywords/tags (subjects) Cloud security, UEBA,

Cyber Security, Microsoft 365, Azure Sentinel, MCAS, CASB, UEBA, Machine learning, AI jamk

Kuvailulehti

Loukkaanhuhta, Marko

Transforming technical IT security architecture to a cloud era. Case: Aalto University

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2021, 64 sivua.

School of Technology, Degree Programme in Information Technology, Cyber Security. Master's thesis.

Julkaisun kieli: englanti

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Aalto-yliopisto on monen muun organisaation tavoin mahdollistanut käyttäjiensä hyödyntää SaaS-pilvipalveluiden tuomaa joustavuutta ja vaivattomuutta datan käsittelyyn. SaaS-pilvipalvelut ovat yleensä vain identiteetillä sidottu erillinen saareke irrallaan organisaation muusta IT infrastruktuurista, jonne käyttäjällä on pääsy ajasta ja paikasta riippumatta. Käyttäjän helppo pääsy dataan mahdollistaa helpon pääsyn myös verkkorikolliselle, mikäli käyttäjän tunnistetiedot joutavat vääriin käsiin. Myös erilaiset uhat kohdistuvat eri tavalla pilvessä käsiteltävään dataan. Organisaatioiden tietoturva-arkkitehtuuri on kuitenkin pilvisiirtymän aikana usein pysynyt lähes muuttumattomana ja kuvastanut aikaa jolloin tietoturvassa panostettiin lähinnä lähiverkon suojaamiseen ulkoisilta uhkilta. Tämä nosti esiin kysymyksen, miten pilvisiirtymä vaikuttaa organisaation tietoturvakyvykkyyteen.

Vastausta kysymykseen lähdettiin hakemaan tarkastelemalla lähiverkon tietoturva-arkkitehtuurin kyvykkyyttä pilven tietoturvauhkia vastaan. Hyvin nopeasti havaittiin, että jos lähiverkon ja pilven välillä ei ole muuta yhteyttä kuin pilveen synkronoitu tai projisoitu identiteetti, ei näkyvyyttä pilven tietoturvatapahtumiin ole olemassa. Tämän ratkaisemiseksi suunniteltiin ehdotus tietoturva-arkkitehtuurista, jossa hyödynnettiin Microsoft 365 A5 ja EMS E5:n lisenssien mukana tulevia tietoturvaominaisuuksia. Kun paremman pilvitietoturvan mahdollistama arkkitehtuuri oli suunniteltu, se toteutettiin myös käytännössä. Tietoturvatilannetta, hälytyksiä ja havaintoja tutkittiin kuukauden ajanjaksolta ja saadut tulokset analysoitiin. Teknistä tietoturva-asiantuntijaa, jonka vastuualueeseen myös organisaation SOC-toiminta kuuluu, haastateltiin jotta myös laadullinen näkemys toteutetusta arkkitehtuurista ja sen tietoturvakyvykkyyksistä saatiin.

Tuloksista voitiin todeta, että lähiverkkoon keskittyvä tietoturva ei ole riittävä SaaS-pilvipalveluiden aikakautena. Jonkinasteinen näkyvyys pilveen voidaan saavuttaa tuomalla pilven tarjoamat lokit organisaation käyttämään SIEM järjestelmään, mutta paras tulos saatiin kun lokidata käsiteltiin pilvessä olevilla CASB ja Sentinel -tuotteilla. Myös paikallisen SIEM järjestelmän rajallisuudet pilvilokien käsittelyn suhteen huomattiin. Vaikka lokeja tuotiin SIEM järjestelmää, se ei kuitenkaan poista sitä ongelmaa, että tietoturvakontrollit pilven tietoturvaan puuttuvat. Tietoturvakontrollit olisi hyödyllistä toteuttaa pilvityökalujen avulla hyödyntäen kehittyneitä koneoppimista ja tekoälyä hyödyntäviin tuotteisiin, joiden tuottamien hälytysten todettiin olevan harvemmin aiheettomia.

Avainsanat (asiasanat)

Kyberturvallisuus, Microsoft 365, Azure Sentinel, MCAS, CASB, UEBA, Machine learning, AI

Contents

Figures

Tables

ACRONYMS

AD	Active Directory
API	Application Programming Interface
ADFS	Active Directory Federation Services
CASB	Cloud App Security Broker
EM+S	Microsoft Enterprise Mobility + Security
ERP	Enterprise Resource Planning
ISMS	Information Security Management System
MCAS	Microsoft Cloud App Security
NIST	National Institute of Standards and Technology
SaaS	Software as a Service
SOC	Security Operations Center

1 Introduction

This thesis was assigned to writer by his employer, Aalto University, to plan and implement security architecture for Identity and Access Management in Cloud Computing using Microsoft provided cloud-based security tools and to research the impact and effectiveness of them in Aalto IT security use case. Architecture plan was generalized to help other organizations to get benefit from this thesis.

Since beginning of consumerization of IT, users have been wanting easy and effortless ways to access data and use their applications. Naturally, since beginning of the smartphone's era, this has been increasingly true in modern countries' consumer perspective. Smart phones and their apps, using cloud services as a backend, has been a norm almost two decades. This usability leap for easy access to information has permanently shaped the way how and where we use the data as a consumer. In the end of the day, business user is also a consumer, and once consumer has learned how effortlessly one can use applications on their mobile device or laptop, the business user inside us, starts to except the same from business applications.

It is not just because of consumerization of IT that drives shift to the cloud. Organizations have seen cloud shift bringing value to the business in different ways. One important aspect is that studies have shown that sharing and collaboration culture can benefit organizations by creating mutual trust and strengthening social networks which can aid transfer of knowledge between workers. (Ahmed et al. 2016) According to Safari et al. (Safari, F., Safari, N., & Hasanzadeh, A., 2015) sharing and collaboration culture was one of the five highest ranking reasons for the SaaS adoption. Other reasons were relative advantage, competitive pressure, social influence and security and privacy.

1.1 Security of the cloud

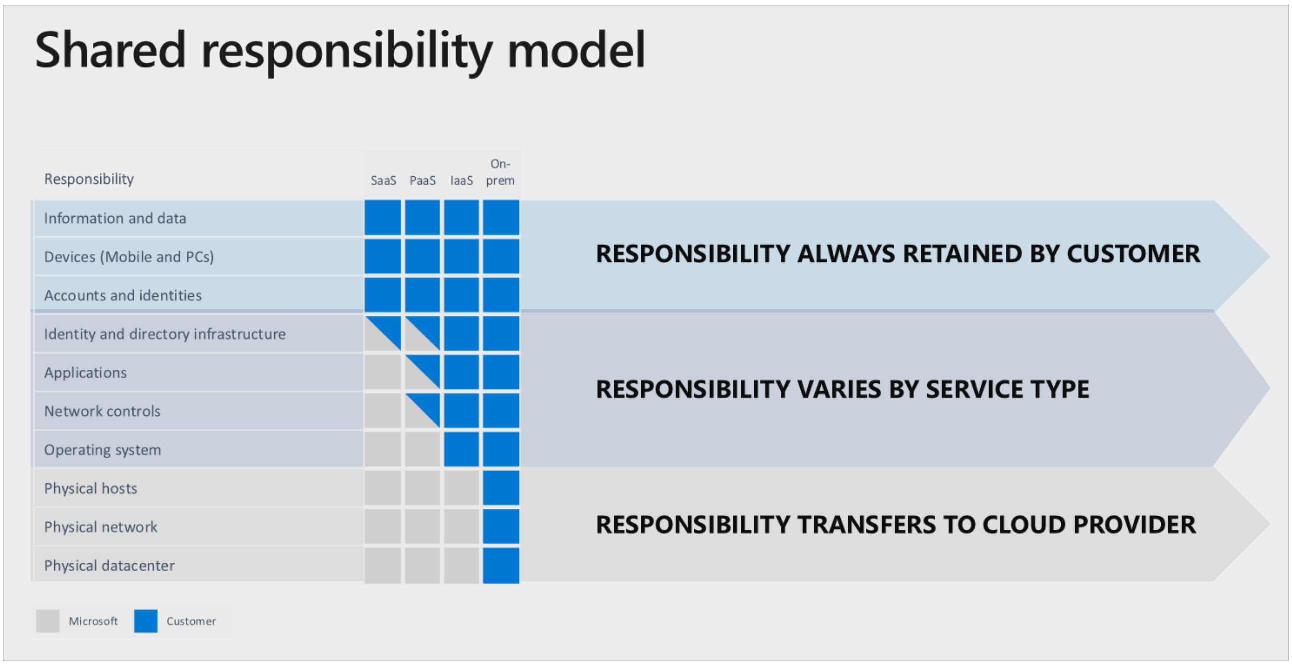
While studying literature about the topic, it was noticed that attitude toward cloud computing and its security has been evolving from untrusted and unsecure to trustworthy and secure. Security and data protection have not always been top driving force to the cloud, quite opposite. Ten years ago, most IT leaders did not saw cloud computing mature enough. Reason for this was, various security concerns, as Deloitte found out when they surveyed European CIOs who were not yet invested in cloud computing. Deloitte also pointed out, that in another survey at that time, indicated that 78% of IT managers thought that security concerns were the biggest issues towards cloud adoption. (Deloitte, 2011) Eight years later, Deloitte surveyed over 500 IT leaders and executives to find out what are the reasons for cloud adoption in organizations. Surprisingly, 58 percent of responders put security and data protection as a top two reasons for cloud adoption. (Deloitte, 2020) In recent years cloud computing has gain more and more traction in business, and cloud computing providers has been investing significant amount of money and resources to build secure computing services in cloud.

Software giants are shifting their products and ecosystems from locally installable products to cloud based products for business and security reasons. Economy of scale and continuous improvement and continuous delivery models allows building and deployment of cloud-based SaaS applications for massive scale for many customers with relatively little effort.

Because of how SaaS applications typically work, software makers usually provide powerful APIs for managing application, importing, exporting, and manipulating the data in cloud. Availability of APIs enables organizations to implement new services based on existing data, that can be reused and consumed in different applications. APIs has also democratized the software development and data management in organizations. These benefits have introduced more business reasons to move services to cloud.

Cloud platforms and SaaS offerings are typically built from ground up for security and compliance. For example, Microsoft cloud offerings comply with tens of different compliance standards, backed by 3rd party and government audits. (Microsoft, 2021e)

Cloud computing, including SaaS offerings, typically have shared responsibility model. This means, that while security of platform is provider’s responsibility, customer has its own responsibilities.



Shared responsibility model

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and identities	🟦	🟦	🟦	🟦
Identity and directory infrastructure	◩	◩	🟦	🟦
Applications	⬜	◩	🟦	🟦
Network controls	⬜	◩	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

RESPONSIBILITY VARIES BY SERVICE TYPE

RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER

⬜ Microsoft 🟦 Customer

Figure 1. Shared responsibility model. (Microsoft, 2021h)

Even if cloud platforms itself are built in secure way, due to the nature of cloud computing, but if organization have not carefully planned and taken systematic and governed approach to cloud computing and its security, cloud computing can lead to even less secure environment than in traditional computing and it may lead to a compliance incidents and leakage of data. (Gartner, 2018)

1.2 Cloud shift’s impact on IT security

When approaching a question about cloud shift’s impact on IT security, we first need to understand that cloud computing is basically imposed by same security threats as all computing. Main differences include that different cloud service models have different security responsibility for provider and customer. As seen on Microsoft shared responsibility model in Figure 1, customers responsibilities vary between cloud service models. In on-premises environment customer has sole responsibility for every aspect of security from hardware to data, while in SaaS service model, customer is responsible for its information and data, devices, accounts, and identities and partly for identity and directory infrastructure.

Before cloud computing, traditional IT security has been built using clearly defined perimeter security boundaries, that have had well defined access controls in place for on-premises and remote access. Users outside of organization networks have been authenticating themselves in the network boundary and if successful, then got access to organization network and data. Network security controls and file system access control lists have been used for limiting users' access to network resources.

Data usage and data access have moved towards cloud, enabling data access from almost any device and location. When data and identities start to span out from enterprise boundaries to the cloud, existing on-premises security controls and security monitoring tools are not enough to protect organization's services and data. Access controls defined on organization perimeter do not span to the cloud. Organization's network, server, and file access monitoring tools cannot see what is happening in the cloud. In cloud computing, particularly in SaaS model, traditional perimeter has vanished, and data in different cloud locations is the protected asset and identities are the new security plane. It is safe to say, that when data and applications are moving to cloud, security paradigm shifts from perimeter centric security to data and identity centric security.

1.3 Aalto University

Aalto University was founded in January 2010 when Helsinki School of Economics, Helsinki University of Technology and the University of Art and Design Helsinki merged. It has six schools, 12000 students and 4000 members of faculty and staff.

The School of Arts, Design and Architecture was founded in 1871 as Craft School. It has grown into one of the most international schools in Finland. It is the largest in its field in the Nordic countries and one of the most respected in the world. The Aalto University School of Business was established in 1911. It is the first business school in the Nordic countries to have received the Triple Crown, i.e., all three labels of excellence from the world's leading business school accreditation bodies: AACSB, AMBA, and EQUIS. Helsinki University of Technology was founded in 1849. The four schools of technology at Aalto University have a leading position in Finland and are internationally renowned (Aalto University, 2021a).

Aalto University has centralized IT department with various functions. Aalto University has deployed Information Security Management System (ISMS), a suite of information security policy, rules and guidelines based on the ISO/IEC27001 code of best practices for information security. (Aalto University, 2021b)

1.4 Background

Author of this thesis has been architecting and implementing Microsoft 365 and Microsoft Azure cloud services and their cloud service security in collaboration with Aalto University IT Security as part of his job role as Identity and Access Management Specialist.

During the thesis project, global COVID-19 pandemic hit the world. Aalto University made decision, like many other higher education institutions in Finland, that employees and students will be moved to remote working mode. In Aalto University numerous digitalization processes were already implemented, that helped students and staff to facilitate IT in remote mode quite impressive ways from day one. That did not mean that every service was ready for remote work. Decision about remote working mode accelerated many projects in Aalto University, including those that were related to cloud and cloud identities. Cyber security improvements of SaaS services and greater visibility to the cloud were one of the key activities.

While organization have implemented ISMS, system based on ISO27001 structure, and it is followed by IT personnel who architect and build IT solutions, ISMS does not mandate what product and what kind of controls should be used for cloud visibility and controls. Organization cloud strategy and organization’s information classification documents dictate what kind of data can be stored and handle in cloud. Administrative documents and strategies are guidelines and cannot be enforced without suitable controls.

Comprehensive discussions and complicated decisions were needed during the process. Decisions were made about what restrictions and what controls should be deployed to enable the usage, but still make cloud safe place to work. Cloud residual risks needed to be handled and change management issues needed to be solved. During the architecture process, it was hard to find easily understandable and compact information package that discusses about different matters that organization should take in consideration when data and users are moving to a cloud or SaaS service, and how to gain adequate visibility to security signals, and control of data and identities.

2 Research

2.1 Research problem

Organizations have started to use cloud-based SaaS services for different reasons and with different pace. During the literature review, it was noted that there seems to be great consensus about the importance of planning and governance in cloud adoption and its effect on cloud security. If organization have failed to establish well governed and well-planned approach towards cloud computing, this lack of governed and planned approach leads to poorly designed and built security infrastructure regarding cloud data access controls and visibility to cloud. (Gartner, 2018)

In typical organization, on-premises infrastructure has been established with its own security measures and controls. Even if these measures and controls are state of the art, they do not necessarily enable control and visibility to cloud data and data access. This controversary might lead to a situation, where Organization's ability to detect and response to cloud-based security incidents is limited. Existing on-premises IT security solutions can rarely be used by itself to gain visibility and control to the cloud. Cloud security posture is non existing and situational awareness is limited. Even in hybrid identity model, where organization manages its identities and authentication of cloud access in on-premises servers, visibility and control to the cloud will be missing.

Most of the Finnish Higher Education Institutions have licensed Microsoft Office 365 SaaS offerings. These licenses, depending on their license level, might include cloud-based security products that can be used to build effective security solutions that compliments existing on-premises IT security solutions and can help to gain visibility and control to cloud data and data access.

While there are large number of documentations on how to configure and use these Microsoft cloud-based security tools, there are not so much about how to construct effective security solution and architecture in a fast and cost-effective way. Besides the marketing material, there seem to be lack of information about real world effectiveness and impact of these tools for organization IT security management.

Generally, there seems to be a lack of knowledge about how to properly connect and extend cloud-based Microsoft provided security tools to on-premises security architecture and what are their effectiveness towards organization’s IT security when security paradigm shifts from perimeter-centric security to data/identity-based security. Aim of this thesis is to deliver answers and insights to these matters and increase knowledge of this phenomenon.

2.2 Some research in the field

During the literature review, other thesis work was also reviewed. Bachelor thesis from Ville Halminen (Halminen, 2019) with title Pilvipalvelun käyttöönoton tietoturva, covered the topic of Office 365 security control applicability against current Finnish regulations and requirements for public sector cloud computing. Thesis reviewed Office 365 security control on higher level and tried to find out if Office 365 employ necessary controls to fulfill the requirements for cloud service security of Finnish public sector. In his thesis, Halminen did not discuss about architecture or challenges about adequacies of on-premises IT security infrastructure towards cloud IT.

Master’s thesis from Anttu Pekkarinen (Pekkarinen, 2018) with title Enhancing security of cloud services with Microsoft Enterprise Mobility + Security, covered the topic of challenges in cloud services and how Microsoft EM+S security suite would help to solve these challenges. Thesis reviewed quite extensively EM+S security suite features that were current at the time of publication. Pekkarinen interviewed IT personnel and security specialists for his work to find challenging topics in cloud service security field.

Both theses that was reviewed, had good content, but they both were written from different point of view and their content were already somewhat dated, highlighting the challenge of everchanging cloud computing scene.

Even if cloud computing itself is no longer a new thing, it is evolving fast. This might be one reason for lack of proper literature of cloud security implementation planning and design. Microsoft has published some architecture models, but they mainly consider IaaS model implementations. Only few publications were found, but they were either outdated or too general.

Product suppliers seem to advertise their products with different functionalities, and even provide detailed documentation about how to configure product in use, but sample implementations were hard to find. Like (Koskinen & Simola, 2019) noted about cloud security literature, that it is surprising low in quantity and quality, while need for cloud security research is in demand. Literature was searched from Theseus for other theses on the field and Aalto University library's electronic publications search engine that has access to thousands of e-publications, standards, and journals. Sources like NIST, Enisa, Microsoft, Gartner, Deloitte, and Cloud Security Alliance were also utilized.

2.3 Research questions

When doing the formalization of the research problem and assignment in question, following research question was raised: **How security paradigms' shift from perimeter-centric security to identity- and data-centric security affects IT security capabilities?** Strong assumption by expertise and experience, hinted that this does have negative impact IT security capabilities. To study what one can do to mitigate the negative impact, sub question raised: **How organization can improve visibility in Microsoft SaaS services with cloud-native security features and tools?** Next hypothesis was that these tools can help organization to improve cyber security strength, but how and which way? To formalize this in proper question, last research sub question was formed: **What is the added value for organization's Cyber Security management regarding Identity and Access Management when organization adopts Microsoft provided cloud native security tools?**

2.4 Research objectives

To achieve answers to research questions and fulfill the aim of this research, following objectives needed to be facilitated:

1. Identify organization's security responsibilities and common threats in SaaS service model.
2. Analyze effectiveness of on-premises based IT security tools against SaaS responsibilities and threats.
3. Plan and build cloud security architecture that uses Microsoft cloud native tools as an extension to on-premises IT security tools.
4. Evaluate impact of these tools to IT security management in terms of effectiveness and cost.
5. Provide recommendations to further development IT security with cloud native tools.

2.5 Research methods

Thesis was conducted using Design science research methodology. Selection of applicable security controls in architecture was made using comparative study on available IT security controls in on-premises and cloud against NIST security control list.

Suggested solution for improving organization cyber security capabilities against SaaS cloud-based threats using Microsoft provided native cloud-based security tools was introduced and built.

Capabilities against these threats and model use cases were analyzed and evaluated based on real data from built infrastructure. Modifications and improvements to original architecture plans were made during the build phase.

Results and conclusions were formed after the technical analysis of incidents, use case evaluation and interview. Thesis produced information about impact of cloud-based security tools for organization cyber security capabilities against common SaaS threats and architecture model for implementing such capabilities.

Diagram of the research, as seen on Figure 2. below, visualizes research method and outcome relations.

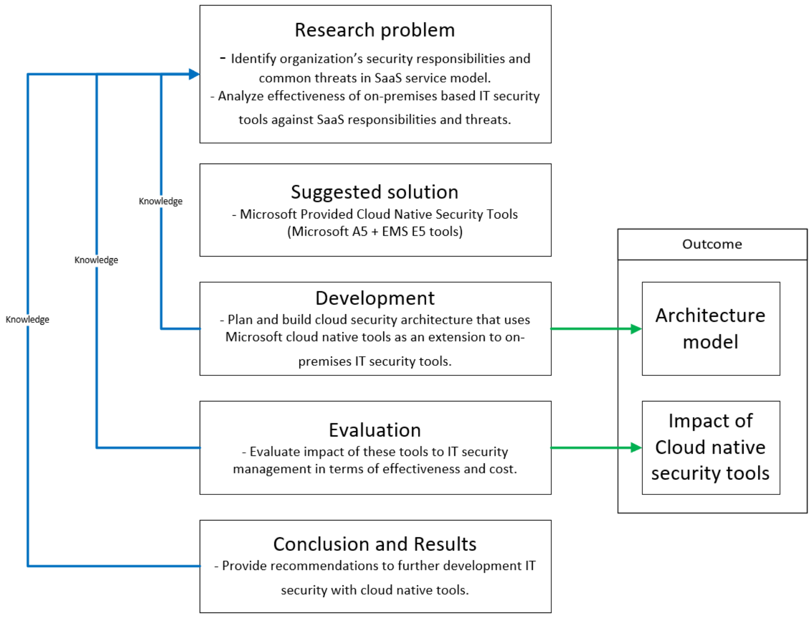

Research problem
- Identify organization’s security responsibilities and common threats in SaaS service model.
- Analyze effectiveness of on-premises based IT security tools against SaaS responsibilities and threats.
Suggested solution
- Microsoft Provided Cloud Native Security Tools (Microsoft A5 + EMS E5 tools)
Development
- Plan and build cloud security architecture that uses Microsoft cloud native tools as an extension to on-premises IT security tools.
Evaluation
- Evaluate impact of these tools to IT security management in terms of effectiveness and cost.
Conclusion and Results
- Provide recommendations to further development IT security with cloud native tools.
Knowledge
Knowledge
Knowledge
Outcome
Architecture model
Impact of Cloud native security tools

Figure 2. Diagram of the Research (Loukkaanhuhta, 2021)

2.6 Scope of the thesis

This thesis examines what are the organization’s responsibilities regarding SaaS services in shared responsibility model and what measures should be taken into consideration when planning SaaS security controls and visibility regarding Identity and Access Management.

Thesis will give overview about how to handle identity related exceptions and incidents, what kind of security controls can be implemented in the cloud, what kind of detection and monitoring capabilities cloud tools has and what kind of incident response capabilities cloud tools has.

Existing on-premises security controls are reviewed and their visibility against SaaS threats and effectiveness are analyzed in scope of organization’s security responsibilities in SaaS service model.

Security architecture and solution is planned and built using Microsoft cloud native security tools. Solution is evaluated against relevant security control framework in terms of capabilities and by interviewing Aalto University Security Specialist who act as SOC analyst.

Thesis examines what kind of impact selected cloud-based controls and monitoring tools can make to organization’s visibility to SaaS security threats. This thesis does not focus on how to configure different tools or how to use them. This thesis does not describe comprehensively all the capabilities and features that these tools might have and does not describe best practices you should follow to secure cloud infrastructure or cloud applications.

This thesis likes to introduce one possible way to build cloud-based security architecture with existing products that many Finnish Higher Education Organizations already have in part of their licensing agreement with Microsoft. Compliance, legal aspects, privacy, risk handling and management, administrative aspects, change management handling, cloud service residual risks, cloud service provider risks, organization policies, information classification processes, identity sourcing and handling, operative instructions, user adoption, awareness, training, on-premises operations, best practices, and such are not in scope of this thesis.

3 Microsoft SaaS services and identity and authentication models

3.1 Microsoft SaaS services

Microsoft has multiple SaaS service offerings ranging from individual Microsoft 365 services, from Word Online application to complete ERP software solutions. Common nominator for Microsoft SaaS services is that they all use Azure AD as an identity and access control plane. SaaS applications are connected to Azure AD by using Service principals also known as Enterprise application in Azure AD context. Service principal is instance of Application object, either in tenants' directory or in application publisher tenant. (Microsoft, 2020b)

3.2 Microsoft Azure AD

Azure AD is cloud-based directory with identity and access management services. Azure AD provides identity and access management capabilities for Microsoft 365 and Azure services and works as a backbone for services. It enables sign into thousands of different SaaS applications like OneDrive, Salesforce, Dropbox, organization custom developed cloud applications and more. (Microsoft, 2020g)

Azure AD is licensed product and is available with three different tiers. Azure AD Free provides basic directory features with on-premises synchronization and single sign-on to Azure, Office 365, and other SaaS applications. Azure AD Premium P1 adds i.e., support for on-premises access, dynamic groups and cloud write-back functionality and conditional access policies. Azure AD Premium P2 adds to Free and P1 tiers Azure AD Identity Protection functionality and Privileged Identity Management to name a few. Azure AD also has B2C (Business-to-Consumer) functionality which allows identity and access management solutions for customer facing apps and enables customers to authenticate to organization cloud applications for example their social media credentials. (ibid.)

Each Azure AD instance is controlled and operated by customer. Azure AD architecture is called multi-tenant architecture. Each Azure AD directory, or tenant, is insulated from other tenants. (ibid.)

3.3 Azure AD applications and service principals

Azure AD applications can be used to connect applications to Azure AD identity and access control features. Azure AD application integration provides application and user authentication and authorization, SSO capabilities, Role-based access control capabilities, OAuth authorization services, application publishing and possibilities for directory schema extension attributes. Applications are represented with two different ways, as an application object and as a service principal. Application object is typically considered as definition of an application and it includes definition and parameters of application properties such name, redirect URIs, secret that are used to authenticate the application, API dependencies, published APIs, resources and scopes, roles etc. Application object is always tenant dependent, even when it is configured as multi-tenant application and external directory service principals are supported. This basically means that application object itself only exists in applications' home tenant. Service principals are instances of applications, and they normally reference to application object. They can be used to hold information on user or group application-role assignments, conditional access policies, claim rules, attribute mappings, etc. (Microsoft, 2020b)

Azure AD application relations to service principals can be observed in figure 3. below.

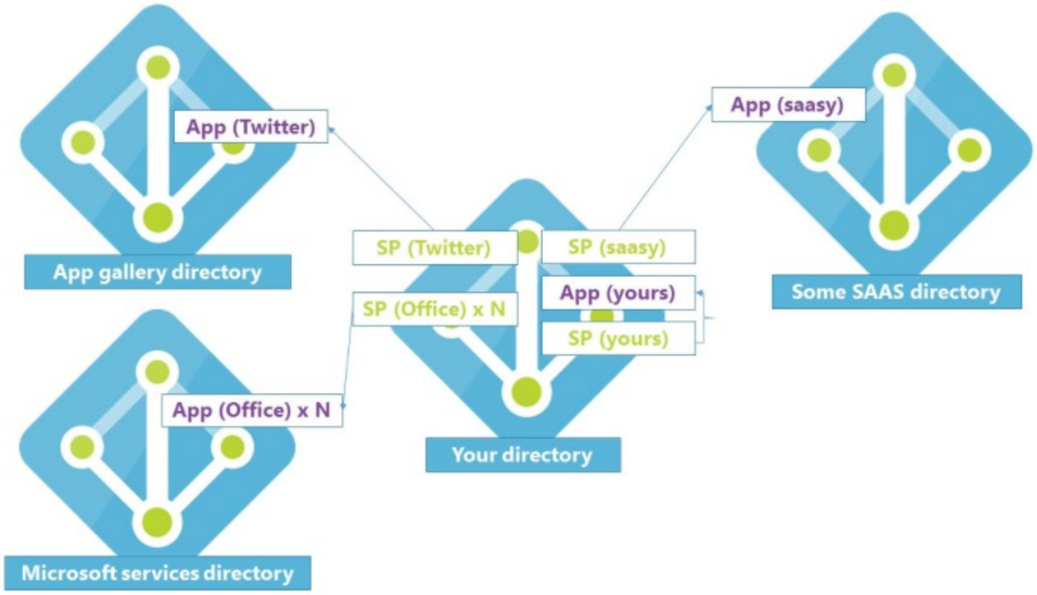


Figure 3. Azure AD Applications and Service Principal relations (Microsoft, 2020b)

3.4 Cloud only identity model

Cloud only identity model, in Microsoft SaaS model context means, that user identities are stored and managed exclusively in cloud directory called Azure AD. (Microsoft, 2020f)

In Cloud only Identity model, Azure AD is the provider for authentication services for user and device authentication. Authentication process, and authentication information is evaluated directly against Azure Active Directory. (Microsoft, 2020f)

3.5 Hybrid identity model

It is common situation today's organizations where cloud consuming user needs to have access both, on-premises data and applications and cloud data and applications. Microsoft's approach to this use case has been to create identity solution that spans through on-premises and cloud, creating common identity that works on-premises and in cloud, this is so called hybrid identity. Hybrid identity is built on top of on-premises directory and cloud directory, by synchronizing user identities from on-premises directory, which typically is Active Directory, to cloud based directory called Azure AD. In this model, users are sourced and managed in on-premises directory. (Microsoft, 2019b)

There are three different authentication mechanisms that can be used with Azure AD hybrid identities. Password Hash Sync (PHS), Pass-through Authentication (PTA) and Active Directory Federation Services (ADFS). All three hybrid identity authentication mechanisms above need identity synchronization component installed on-premises datacenter, Azure AD Connect. Azure AD Connect is responsible for user, group, and other object synchronization between on-premises and cloud directory. (Microsoft, 2019b)

Decision about what is the right method for selecting hybrid identity model, varies depending on requirements that organization has. Below is a Microsoft's decision tree for helping to select the right hybrid identity solution.

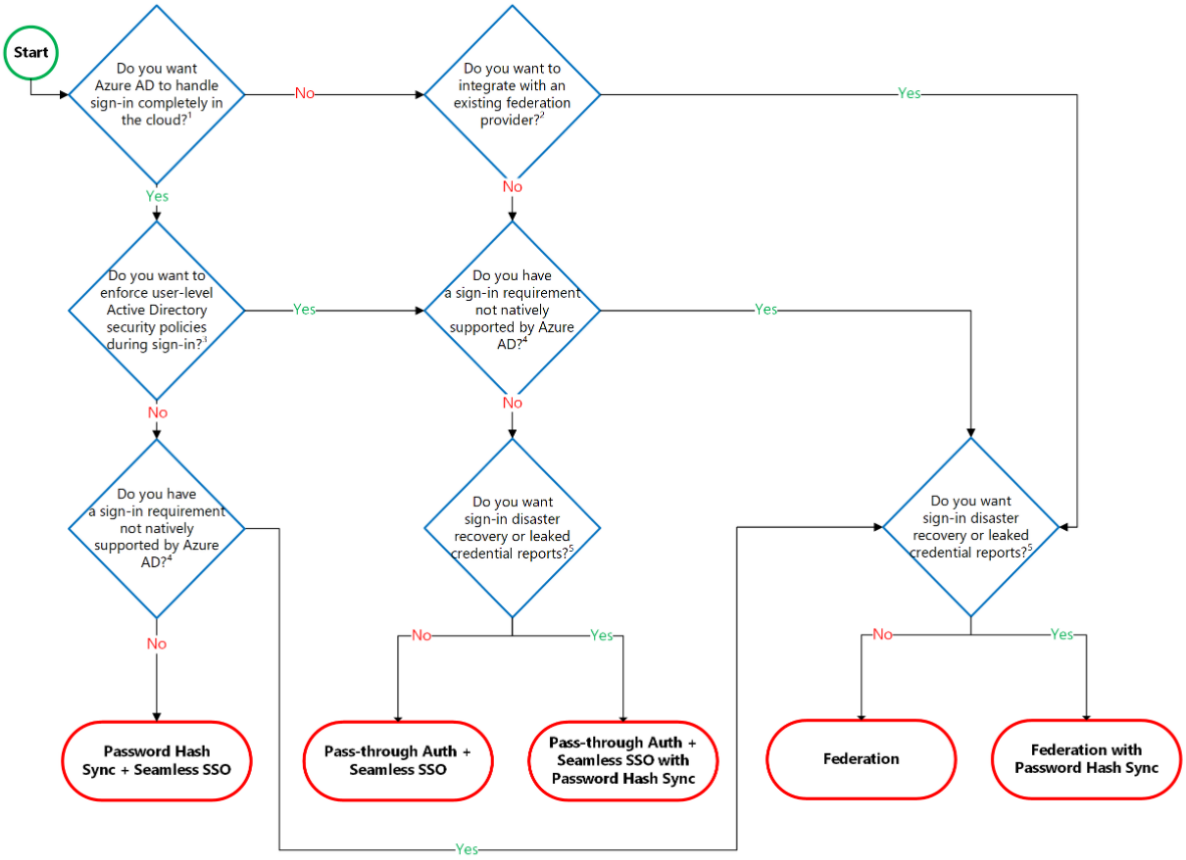
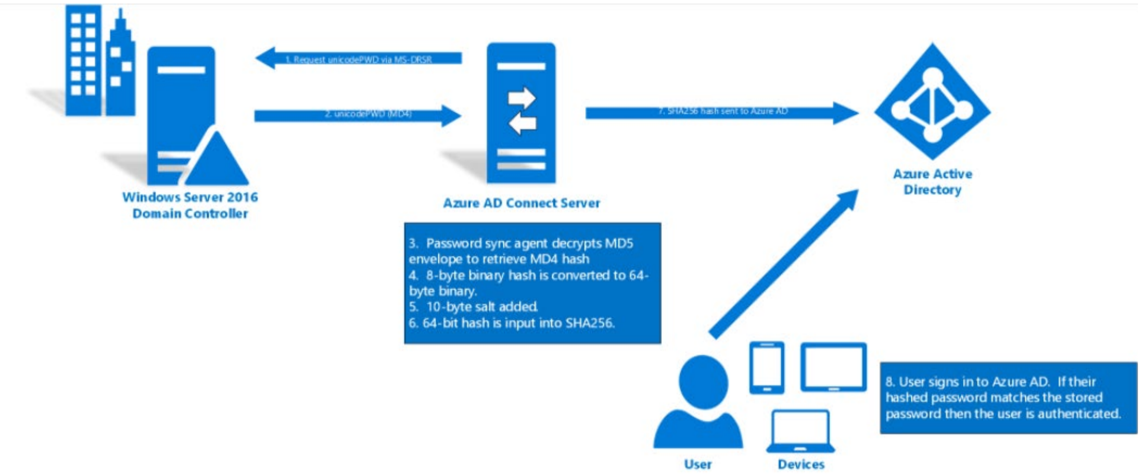

Start
Do you want Azure AD to handle sign-in completely in the cloud?1
No
Do you want to integrate with an existing federation provider?2
Yes
Yes
No
Do you want to enforce user-level Active Directory security policies during sign-in?3
Yes
Do you have a sign-in requirement not natively supported by Azure AD?4
Yes
No
No
Do you have a sign-in requirement not natively supported by Azure AD?4
Do you want sign-in disaster recovery or leaked credential reports?5
Do you want sign-in disaster recovery or leaked credential reports?5
No
No
Yes
No
Yes
Password Hash Sync + Seamless SSO
Pass-through Auth + Seamless SSO
Pass-through Auth + Seamless SSO with Password Hash Sync
Federation
Federation with Password Hash Sync
Yes

Figure 4. Decision tree for hybrid identity selection (Microsoft, 2019b)

3.5.1 Password Hash Sync

Password Hash Sync (PHS) synchronizes on-premises user’s password hash value to Azure AD, where user can authenticate to services using on-premises credentials. PHS can be taken in use on Azure AD Connect service configuration phase. This is the easiest method to start using hybrid identity authentication.

In PHS scenario, hash value of user’s Active Directory password hash is created in on-premises directory synchronization service, Azure AD Connect, by using one-way mathematical function that prevents reconstituting the password from the hash and is then synchronized and stored in Azure AD. Hash function is using MD4+salt+PBKDF2+HMAC-SHA256 with 1000 iteration of HMAC-SHA256 algorithm to ensure, that resulting hash cannot be reconstituted to user Active Directory password. Hash itself cannot be used to authenticate user in on-premises domain. When user attempts to sign in at Azure AD, password undergoes same hashing process and resulting hash is compared to hash stored in Azure AD, and if hashes match, authentication is successful. Password hash sync can also be used in addition to Active Directory Federation Services (ADFS) enabling fall back method for authentication if on-premises ADFS services face availability problems and using password hash sync in addition to ADFS or Pass-through authentication methods, also enables usage of Leaked Credentials functionality in Azure AD Premium feature called Identity Protection. (Microsoft, 2020j)



3. Password sync agent decrypts MD5 envelope to retrieve MD4 hash
4. 8-byte binary hash is converted to 64-byte binary.
5. 10-byte salt added.
6. 64-bit hash is input into SHA256.

8. User signs in to Azure AD. If their hashed password matches the stored password then the user is authenticated.

Figure 5. How Password Hash Sync work (Microsoft, 2020j)

3.5.2 Pass-Through Authentication

Azure AD Pass-Through Authentication (PTA) uses on-premises installed and Azure AD registered authentication agents to directly authenticate Azure AD sign ins against on-premises Active Directory using persistent Azure Service Bus connection that is initiated during authentication agent initialization process. If authentication is successful, Azure AD STS allows user sign in process to continue. PTA is the second easiest method to create hybrid identity functionality. Authentication agent can be installed during the Azure AD Connect configuration or as independent installation. For high availability scenarios, multiple authentication agents can be installed. (Microsoft, 2018c)

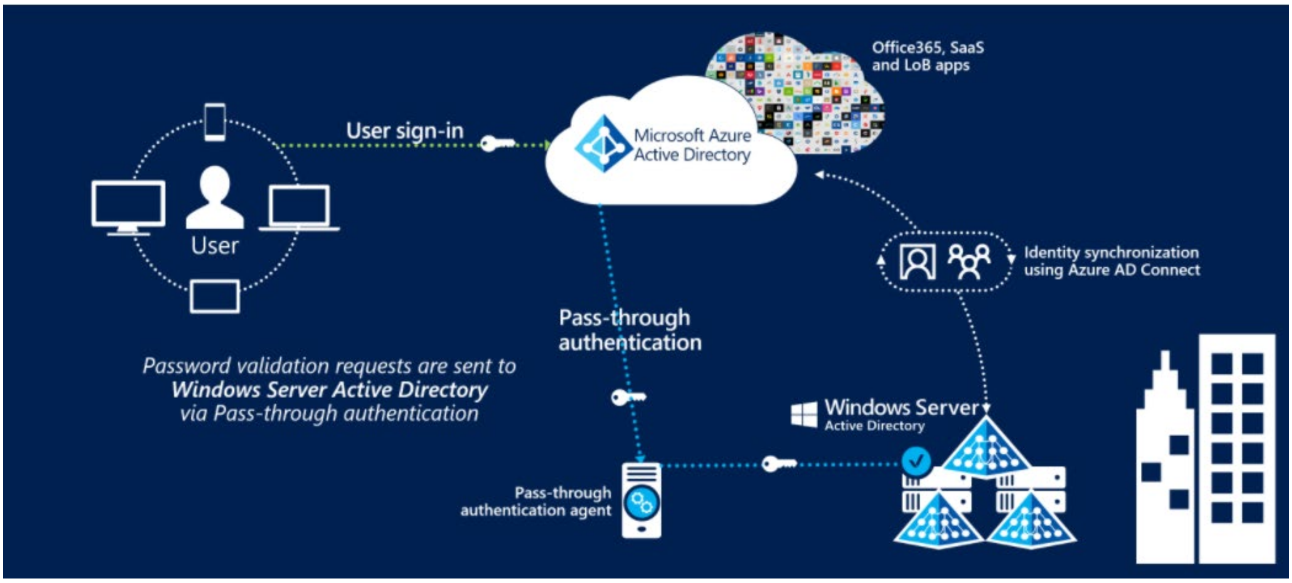


Figure 6. How the Pass-through Authentication Works (Microsoft, 2018c)

3.5.3 Active Directory Federation Services (ADFS)

ADFS is Microsoft's implementation of federation services. ADFS can be used to federate Active Directory with Azure AD. In a short, federation means mutual trust between different domains, this trust usually means authentication and authorization trust. With ADFS authentication, all user authentication is done on-premises servers against Active Directory. (Microsoft, 2018b)

ADFS can be used in more complex scenarios than Password hash sync authentication or Pass-through authentication, because ADFS also supports usage of on-premises MFA solutions and smartcard authentication and more complex logics in authentication claims.

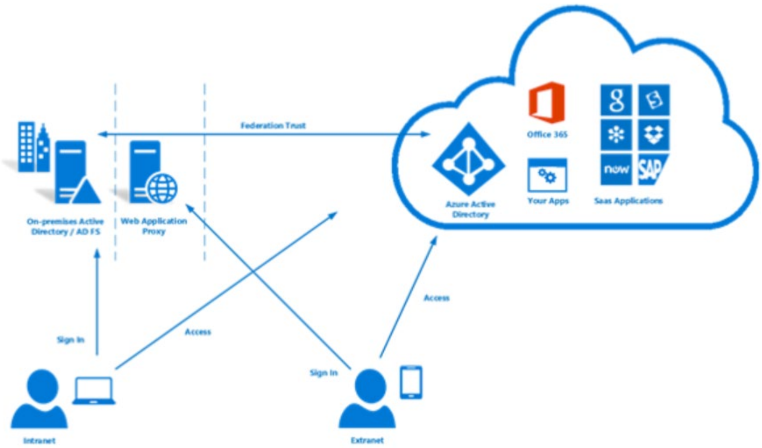


Figure 7. How the Active Directory Federation authentication works (Microsoft, 2018b)

3.6 Tokens and authentication flow

Whatever Azure AD authentication method is used against SaaS cloud services; Azure AD STS is the ultimate control plane for authentication. After successful credential validation, Azure AD STS is responsible for token issuance for users, applications, or devices. After successful credential validation, access is granted directly or conditionally using conditional access policy. With conditional access policies, access can be granted or rejected based on account, device, application, location etc. or combination of them. Azure AD STS issues tokens that contain different kind of authentication related information depending on which authentication scenario is considered and which kind of device or application is used. (Microsoft, 2016)

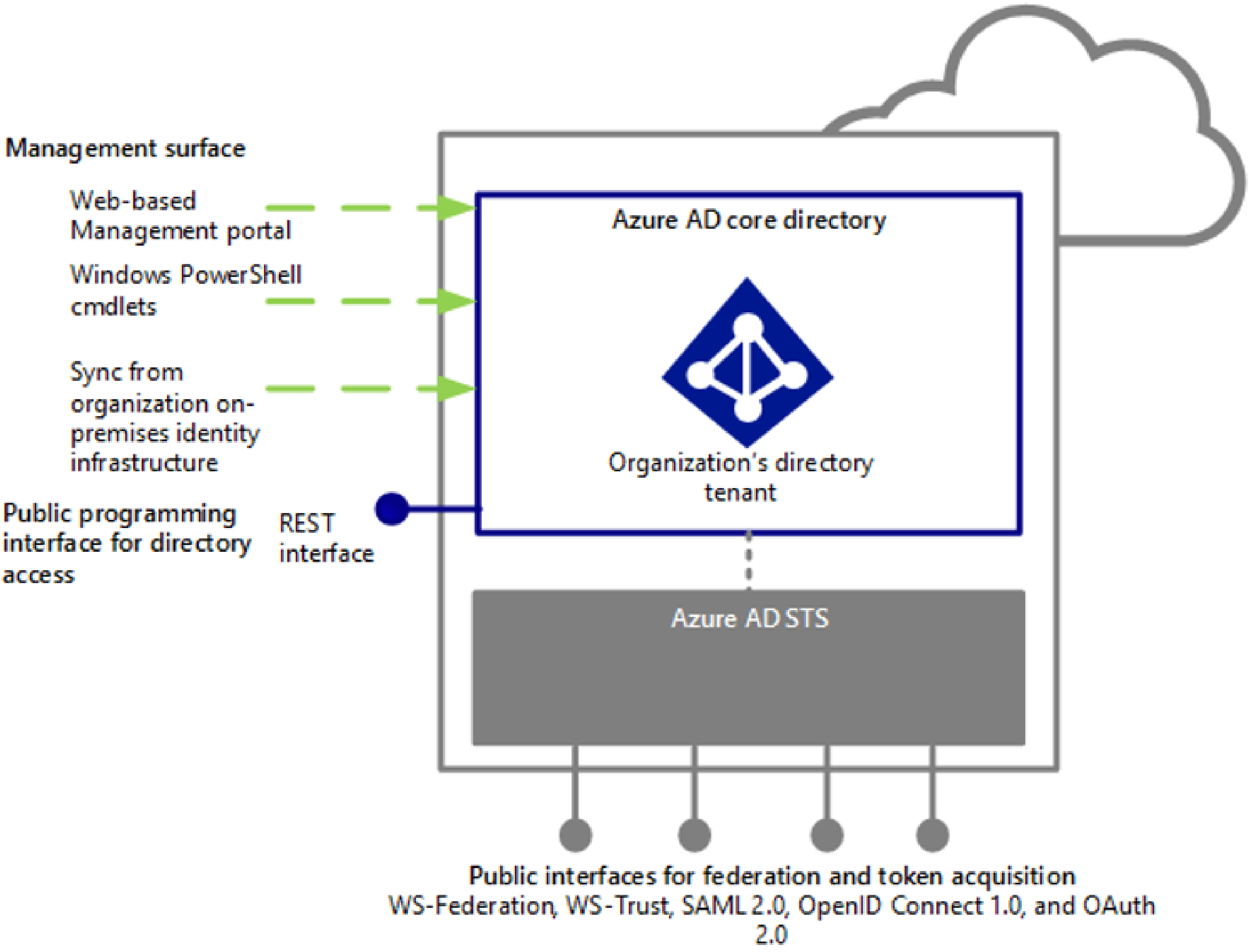

Management surface
Web-based Management portal
Windows PowerShell cmdlets
Sync from organization on-premises identity infrastructure
Public programming interface for directory access
REST interface
Azure AD core directory
Organization's directory tenant
Azure AD STS
Public interfaces for federation and token acquisition
WS-Federation, WS-Trust, SAML 2.0, OpenID Connect 1.0, and OAuth 2.0

Figure 8. Azure AD STS (Microsoft, 2016)

Microsoft SaaS services like Microsoft 365 and Azure AD uses OAuth 2.0 authentication protocol for authentication. Below is the simple authentication flow in case where user is authenticating to some web service using OAuth 2.0 protocol against Azure AD.

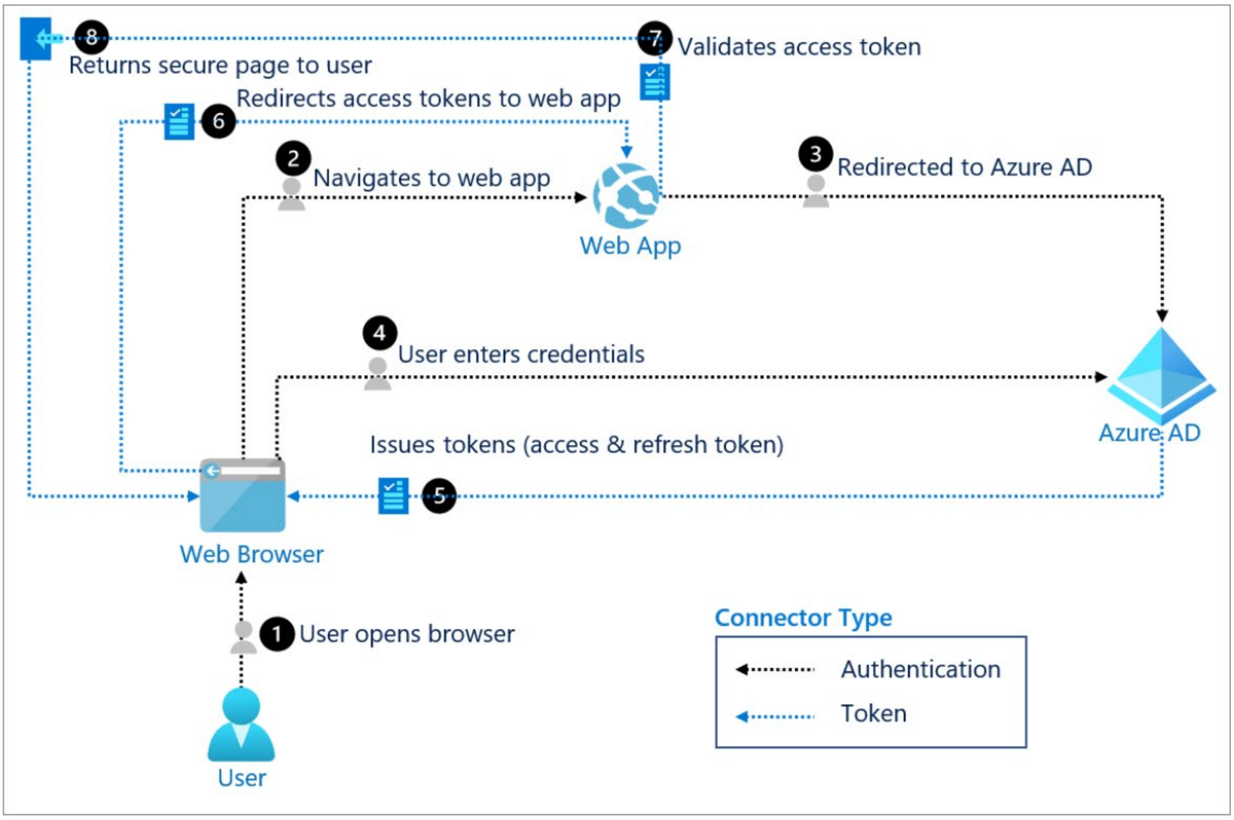


Figure 9. OAuth 2.0 flow (Microsoft, 2020e)

4 Cloud based security controls and security tools

4.1 Microsoft SaaS services security

Microsoft SaaS and cloud services are designed with defense-in-depth approach. Customer data is physically protected in highly secure datacenters that employs multiple layers of security protections against unauthorized access, security breaches, natural and environmental threats. Multiple copies of customer data are kept across geographically distributed datacenters. (Microsoft, 2017)

Logical security prevents unauthorized administrator access to customer data using different safeguards, controls, and processes. Customer can use Customer Lockbox feature that completely denies Microsoft personnel access to customer data without explicit consent. Customers' Global Admin role has complete visibility and access to all features and controls in the cloud with admin center functionality. Customers have ability to control who can access in which data, from which location or device or any combinations of those and more. (Microsoft, 2017)

Data confidentiality and integrity is managed with encryption at rest and in transit using industry renowned cryptographic protocols and encryption standards. Data volumes that hold messaging data or SharePoint or OneDrive data are encrypted using BitLocker volume encryption with AES 256-bit encryption. OneDrive and SharePoint Online uses file-level encryption top of volume encryption, every file has its own unique encryption key. (Microsoft, 2017)

Access controls like Conditional Access, Multi-Factor Authentication, sharing controls, and Application and device management ensures that customer has complete control over which data is accessed from which identity, from which device, from which application and from which location. Multiple policies can be combined for granular control. Advanced audit controls allow tracking of changes and user activity in atomic level. Every user action is recorded for full audit trail. Customer can create alerts for different activities that is happening. (Microsoft, 2017)

Microsoft cloud services are regularly audited by independent third-party auditors, and Microsoft holds key certifications like EU Model Clauses, FedRAMP, FERPA, FISMA, HIPAA, ISO/IEC 27001 and more. (Microsoft, 2017)

4.2 Microsoft Information Protection

Microsoft Information Protection or Azure Information Protection (MIP/AIP) is family of cloud-based tools that are intended for discovering, classifying, labeling, protecting, and monitoring organizations' sensitive and important data. MIP uses automatically or manually applied labels defined in a form of organization created taxonomy. MIP can protect labeled documents using encryption, access restrictions and visual label markings to help user who is using the data to understand which level of sensitivity information for example that specific data has. Monitoring capabilities allows to know where documents with sensitive information resides, who has access to them and who opens, or edits protected documents. MIP has labeling client for classifying, encrypting, decrypting individual documents, those documents can also be stored outside of cloud service. MIP protected documents can be consumed with web-based Office 365 tools as well as client applications with MIP client. Client is available for Windows, MacOS and Android. (Microsoft, 2019a)

4.3 Information Barriers

Information Barriers is Microsoft 365 feature that is intended for creating information barriers in Microsoft Teams, SharePoint Online and OneDrive to prevent collaboration and information sharing between different parts of organization. For example, in Teams, information barriers prevent searching a user, adding user to team, chatting to user, invite user for a meeting, sharing the screen, calls and sharing files between users between defined barriers. (Microsoft, 2021b)

4.4 Azure AD

4.4.1 Azure AD logs

Azure AD produces five different types of logs that are categorized in two different categories, Activity and Security. Activity category consists of Sign-ins -log that provides information of usage of managed applications and user sign-ins. Audit logs, that provides all changes done to Azure AD objects and settings, Provisioning logs provides visibility of provisioning service activities. Security category consists of Risky sign-ins -logs that contains sign-in attempts that might performed by some other party than account legitimate owner and Users flagged for risk -log that contains user account that might be compromised. (Microsoft, 2020a)

Azure AD log retention time varies based on the plan. In Azure AD free log retention time is 7 days for all logs, Azure AD Premium P1 retention time for all logs is 30 days and Azure AD Premium P2 retention time is 30 days for all other logs than Users at risk and Risky sign-ins that has 90 days of retention period. (Microsoft, 2020d)

Azure AD log retention time can be extended when logs are stored in Log analytic workspace, for example in Azure Sentinel.

Azure AD logs are backbone for all advanced analytics that cloud-based security tools provide. These logs can also be streamed or transferred to external systems via API.

4.4.2 Azure AD MFA

Multi-Factor Authentication (MFA) is an authentication process that utilizes multiple authentication methods for user authentication. In authentication process, user must provide two or more authentication means to system for successful logon, thus preventing successful logon when user has lost his password in wrong hands. Azure AD Multi-Factor authentication requires user to provide two or more authentication methods. Something you know, like password, and something you have, like trusted or managed device, phone, or hardware key and/or something you are, like biometric fingerprint or face scan. (Microsoft, 2020c) Azure AD Multi-Factor authentication can be enabled by forcing MFA for users, using Azure AD Security Defaults or by using Conditional Access policies.

4.4.3 Conditional Access

Conditional Access is the main access control plane in modern identity and data-centric security landscape. It works as bringing different signals together for to decide for granting the access and enforce organizational policies. Visualization of functionality can be observed in Figure 10.

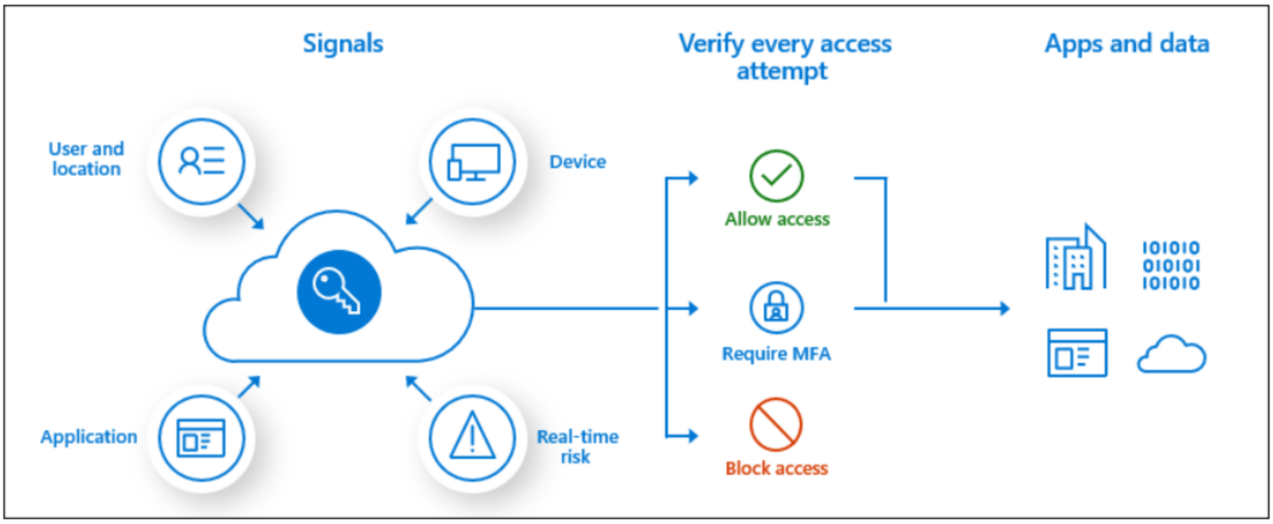


Figure 10. Conditional Access (Microsoft, 2021c)

Conditional Access policies compares different signals like user or group membership, administrative role membership, IP address location, protocol used, device used, application used, real-time and calculated risk detection and MCAS/CASB session control signals and makes decision about access requirements or blocks access. (Microsoft, 2021c)

4.4.4 Microsoft Identity Protection

Microsoft Identity Protection automates detection and remediation of identity-based risks. Behind the scenes is machine learning and heuristics system the provides risk scores for about 20 billion login attempts a day for about billion distinct accounts. This machine learning and heuristics system is fed by signals from different Microsoft products that Microsoft analyses about 6,5 trillion per day. Administrators can review risk detections of three risk categories, Risky users, Risky sign-ins and Risk detections and act on them in Azure portal. These risk detections can also be exported to on-premises SIEM using API. (Microsoft, 2021l)

Table 1. Identity Protection risk detection types (Microsoft, 2021l)

Risk detection type	Description
Anonymous IP address	Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs).
Atypical travel	Sign in from an atypical location based on the user's recent sign-ins.
Malware linked IP address	Sign in from a malware linked IP address.
Unfamiliar sign-in properties	Sign in with properties we have not seen recently for the given user.
Leaked Credentials	Indicates that the user's valid credentials have been leaked.
Password spray	Indicates that multiple usernames are being attacked using common passwords in a unified, brute-force manner.
Azure AD threat intelligence	Microsoft's internal and external threat intelligence sources have identified a known attack pattern.
New country	This detection is discovered by Microsoft Cloud App Security (MCAS).
Activity from anonymous IP address	This detection is discovered by Microsoft Cloud App Security (MCAS).
Suspicious inbox forwarding	This detection is discovered by Microsoft Cloud App Security (MCAS).

4.4.5 Privileged Identity Management

Privileged Identity Management (PIM) provides just-in-time and time-bound role activation capabilities to assign privileged access to Azure AD, Azure resources, Microsoft 365, and Intune. Using PIM eliminates administrator standing access to data and resources. With PIM, privileged management access rights can be bound for approvals, so whenever privileged access is needed, other party approval is required before role activation. When privileged role is activated, justification for role activation can be requested, MFA to activate any role can be enforced, notification from role activation can be sent to other parties. PIM maintains audit history of role activation. (Microsoft, 2021j)

4.5 Microsoft Cloud App Security

Microsoft Cloud App Security is so called Cloud App Security Broker (CASB) product that works like a policy enforcing gatekeeper between users and data. CASB can be used to discovering cloud usage and to provide visibility to Shadow IT and app usage, monitoring and controlling user activities of anomalous behavior, protecting against bad actors, assessing compliance of cloud services, and classifying and preventing sensitive information leaks. CASB provides granular visibility and control over user activities and sensitive data, not only Microsoft cloud solutions, but large portions of other vendors SaaS, HR, ERP, IaaS, PaaS, CRM, and other cloud-based solutions. (Microsoft, 2021d)

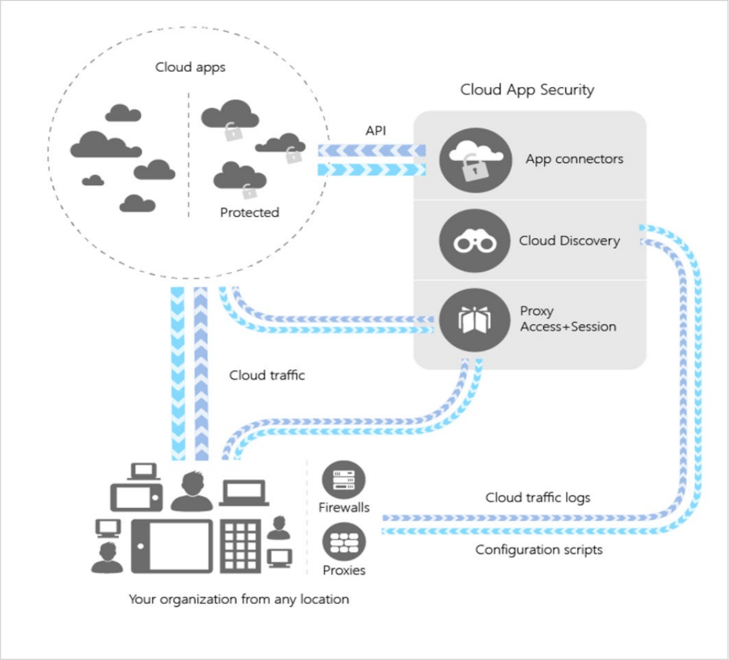
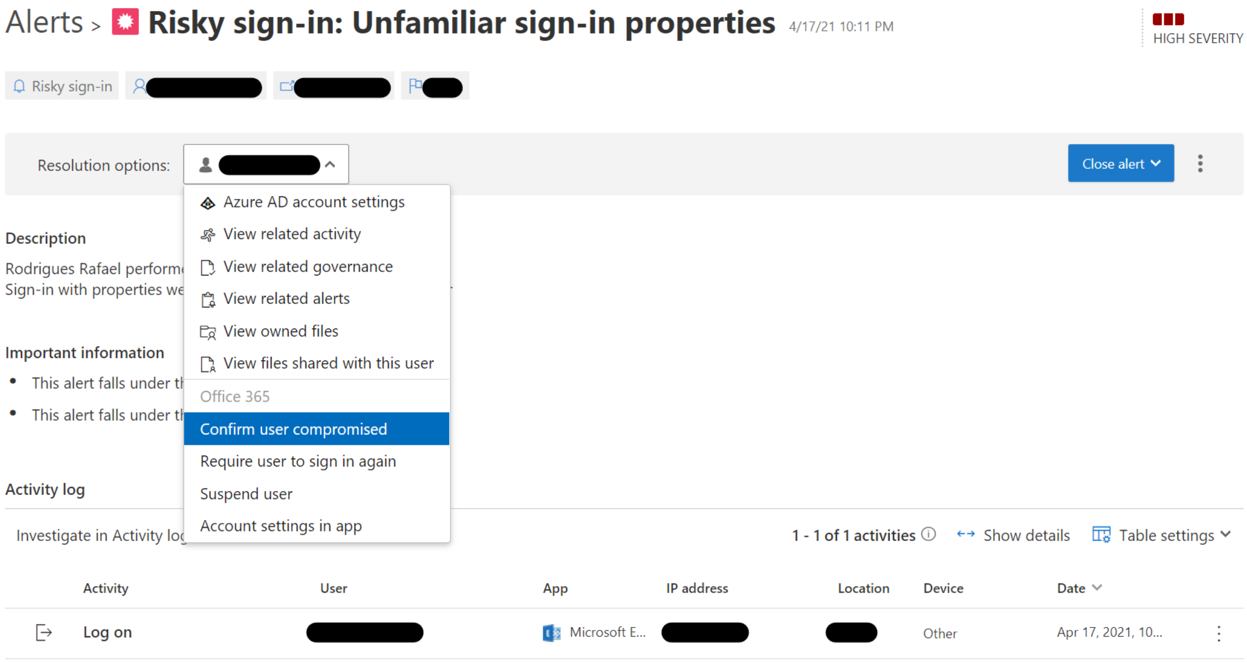


Figure 11. CASB architecture (Microsoft, 2021d)

4.5.1 Policies and governance actions

Microsoft Cloud App Security allows creating multiple policies for risk assessment and information protection. Policy violations generates alerts in Cloud App Security portal and if connected, in connected services like on-prem SIEM or Azure Sentinel. Alerts can be resolved using various methods like digging deeper into user actions, suspend user, require user to sign in again or confirm user compromised. Connections with other Microsoft cloud security tools, security orchestration is easy to arrange. For example, if using Confirm user compromised -resolution option, user account risk score in Azure AD is raised to High level, and if Azure AD Identity protection action for High risk is defined, that action is executed in real time. (Microsoft, 2018a)



Alerts > Risky sign-in: Unfamiliar sign-in properties 4/17/21 10:11 PM

HIGH SEVERITY

Risky sign-in [redacted] [redacted] [redacted]

Resolution options: [redacted]

Description

Rodrigues Rafael perform

Sign-in with properties we

Important information

- This alert falls under th
- This alert falls under th

Activity log

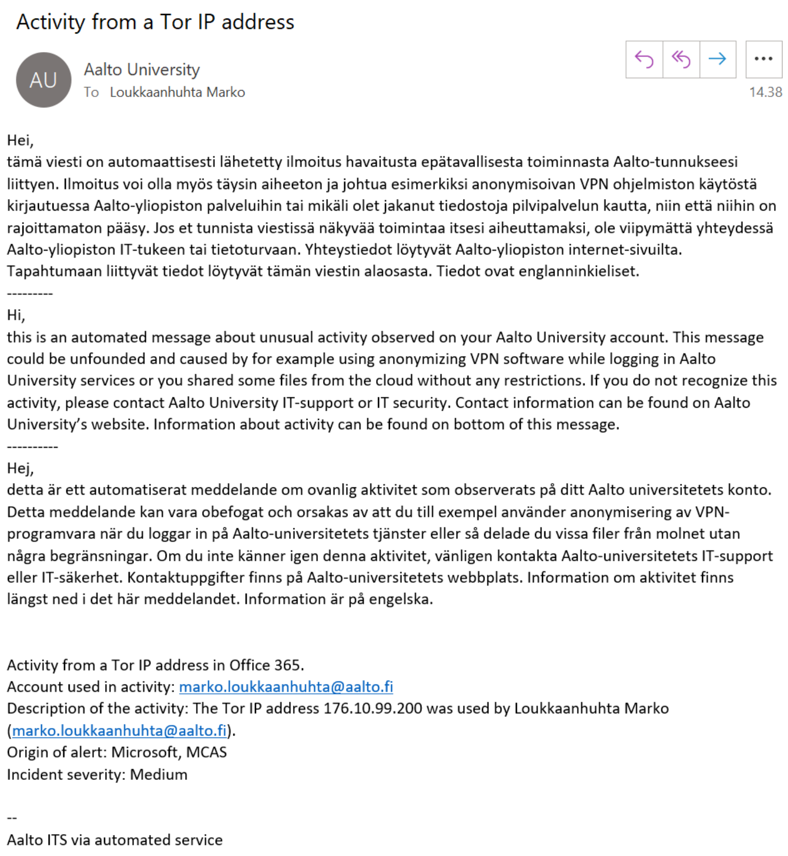
Investigate in Activity log

1 - 1 of 1 activities

Activity	User	App	IP address	Location	Device	Date
Log on	[redacted]	Microsoft E...	[redacted]	[redacted]	Other	Apr 17, 2021, 10...

Figure 12. MCAS/CASB resolution options for Risky sign-in (Loukkaanhuhta, 2021)

Governance actions can be set directly in policies, inside alerts or in File log. Governance actions linked to the policy will automatically applied if specific alert matching the filter is generated. Default governance actions that are selectable for all apps include user notification, notify additional users, suspend user, require user to sign in again and confirm user compromised. It is also possible to create own playbook actions with Microsoft Power Automate. (Microsoft, 2018a)



Activity from a Tor IP address

AU Aalto University
To Loukkaanhuhta Marko

14.38

Hei,
tämä viesti on automaattisesti lähetetty ilmoitus havaitusta epätavallisesta toiminnasta Aalto-tunnukseesi liittyen. Ilmoitus voi olla myös täysin aiheeton ja johtua esimerkiksi anonymisoivan VPN ohjelmiston käytöstä kirjautuessa Aalto-yliopiston palveluihin tai mikäli olet jakanut tiedostoja pilvipalvelun kautta, niin että niihin on rajoittamaton pääsy. Jos et tunnista viestissä näkyvää toimintaa itsesi aiheuttamaksi, ole viipymättä yhteydessä Aalto-yliopiston IT-tukeen tai tietoturvaan. Yhteystiedot löytyvät Aalto-yliopiston internet-sivuilta. Tapahtumaan liittyvät tiedot löytyvät tämän viestin alaosasta. Tiedot ovat englanninkieliset.

Hi,
this is an automated message about unusual activity observed on your Aalto University account. This message could be unfounded and caused by for example using anonymizing VPN software while logging in Aalto University services or you shared some files from the cloud without any restrictions. If you do not recognize this activity, please contact Aalto University IT-support or IT security. Contact information can be found on Aalto University's website. Information about activity can be found on bottom of this message.

Hej,
detta är ett automatiserat meddelande om ovanlig aktivitet som observerats på ditt Aalto universitetets konto. Detta meddelande kan vara obefogat och orsakas av att du till exempel använder anonymisering av VPN-programvara när du loggar in på Aalto-universitetets tjänster eller så delade du vissa filer från molnet utan några begränsningar. Om du inte känner igen denna aktivitet, vänligen kontakta Aalto-universitetets IT-support eller IT-säkerhet. Kontaktuppgifter finns på Aalto-universitetets webbplats. Information om aktivitet finns längst ned i det här meddelandet. Information är på engelska.

Activity from a Tor IP address in Office 365.
Account used in activity: marko.loukkaanhuhta@aalto.fi
Description of the activity: The Tor IP address 176.10.99.200 was used by Loukkaanhuhta Marko (marko.loukkaanhuhta@aalto.fi).
Origin of alert: Microsoft, MCAS
Incident severity: Medium

--
Aalto ITS via automated service

Figure 13. Sample of automated email for user (Loukkaanhuhta, 2021)

Automated actions can be used for example educate user about his own actions like using Tor network while connected to Office 365 services or if user is accidentally shared files from cloud service for too broad audience.

4.6 Microsoft Intune

Microsoft Intune is cloud based mobile device management (MDM) and mobile application management (MAM) solution, that can be used to manage organization's mobile phones, tablets, and laptops. With Intune device and application policies can be enforced to devices and their compliance to organizational policies can be assessed. Intune integrates with Azure AD and Azure Information protection, so it allows access controls and data protection in mobile devices. Managed devices allow corporate data bubbles for removing organizational data from device if device is lost or stolen and device protections that are essential features for example when MFA is used with mobile devices, allowing requirement of biometrical or PIN code access controls for device unlock. Azure AD conditional access can use device compliance or information about managed device as one of the requirements for data access, like access to SharePoint can be set only for organization managed devices or Exchange Online can be used only with Outlook Mobile app. (Microsoft, 2020j)

4.7 Microsoft Azure Sentinel

Microsoft Azure Sentinel is cloud native SIEM (security information event management) and SOAR (security orchestration automated response) solution that delivers intelligent security analytics and threat intelligence. Sentinel is complete solution for alert detection, visibility, hunting and threat response across all users, devices applications and infrastructure. Sentinel can be connected to multiple clouds and on-premises infrastructures and applications. (Microsoft, 2020h)

Sentinel uses in the background proven Azure solutions like Log Analytics, Logic Apps and Machine Learning. Power of Sentinel is in its connectivity capabilities and massice cloud computing power. Correlations are automatically created near real time between different data from multiple sources, like Microsoft 365 Defender, Office 365, Azure AD, Microsoft Defender for Identity, and MCAS/CASB, and more. Even multiple vendors connectors for Firewall logs are available and most common general formats like CEF and Syslog are also available for different security related data. (Microsoft, 2020h)

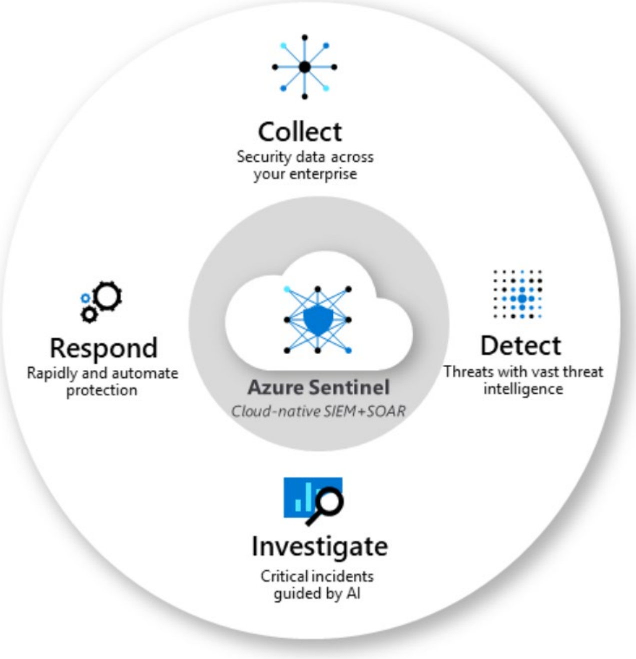
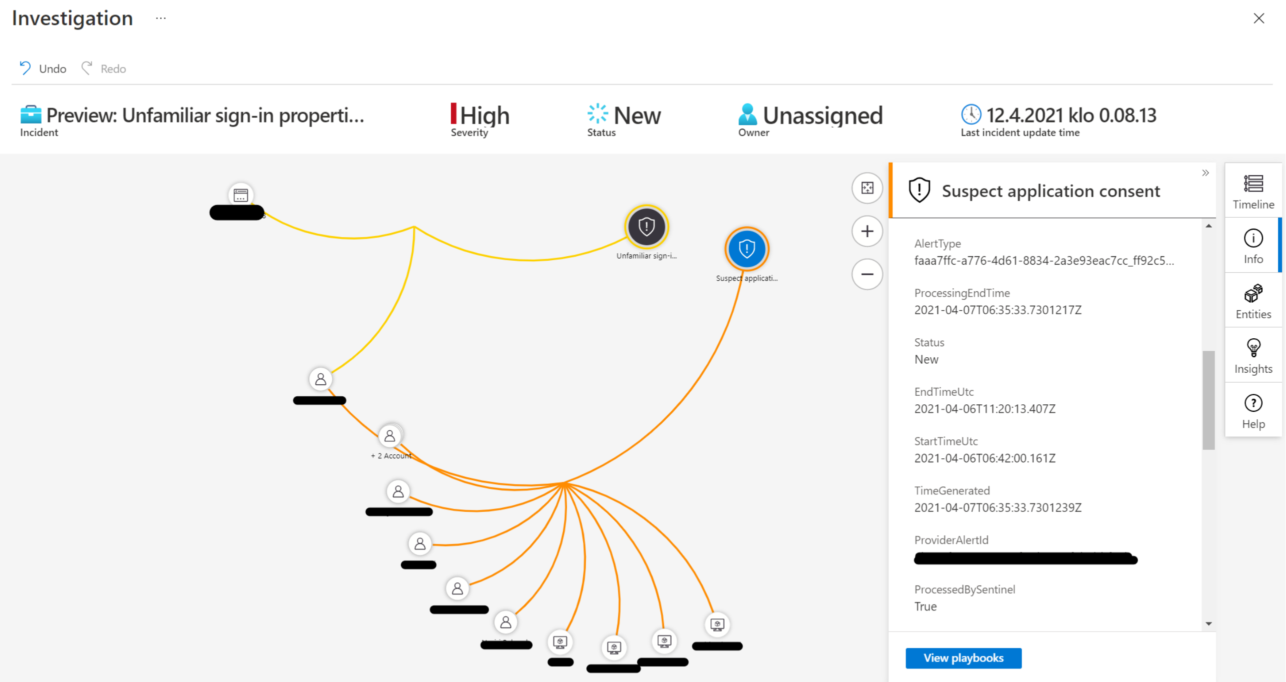

Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Azure Sentinel
Cloud-native SIEM+SOAR
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI

Figure 14. Microsoft Azure Sentinel Overview (Microsoft, 2020h)

Sentinel creates incidents by using automated analytics that correlates alerts together. Incidents in Sentinel are actionable items that can be further investigate and resolved. Sentinel has built-in rules that are customizable, and it is of course possible to create correlation rules from the scratch.


Investigation ···

↶ Undo ↷ Redo

Preview: Unfamiliar sign-in properti...
Incident

High
Severity

New
Status

Unassigned
Owner

12.4.2021 klo 0.08.13
Last incident update time

Suspect application consent

AlertType
faaa7ffc-a776-4d61-8834-2a3e93eac7cc_ff92c5...

ProcessingEndTime
2021-04-07T06:35:33.7301217Z

Status
New

EndTimeUtc
2021-04-06T11:20:13.407Z

StartTimeUtc
2021-04-06T06:42:00.161Z

TimeGenerated
2021-04-07T06:35:33.7301239Z

ProviderAlertId
[redacted]

ProcessedBySentinel
True

View playbooks

Figure 15. Azure Sentinel fusion data incident investigation (Loukkaanhuhta, 2021)

4.7.1 Automation in Microsoft Azure Sentinel

In Sentinel common tasks and security orchestration can be automated using Playbooks. Playbooks are automation assets created with Azure Logic Apps. Playbooks can be created from scratch or by using gallery of Playbooks. All playbooks can be customized for needs, and Azure Logic Apps have more than 200 different API connectors to use for automation such as Jira, Teams, HTTP requests, Slack, Microsoft Defender, Cloud App Security and more. (Microsoft, 2020h)

Below, in figure 16, is sample of automation workflow for security incident handling in Azure Sentinel.

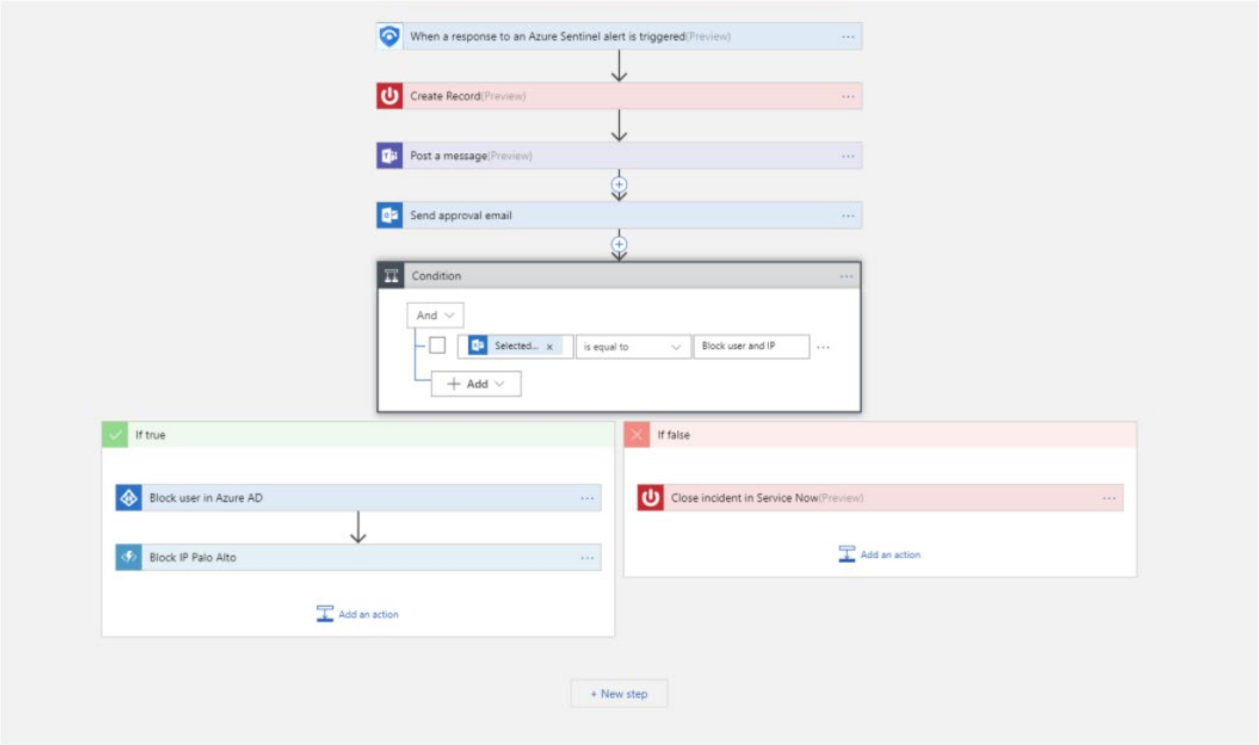


Figure 16. Sample of Azure Sentinel Automation (Microsoft, 2020h)

With Sentinel automation features, growing burden of number of security alerts are easy to resolve.

4.8 Microsoft 365 Defender

Microsoft 365 Defender suite is unified solution of pre- and post-breach coordination. It provides natively integrated protection against advanced attack scenarios. Defender coordinates natively detection, prevention, investigation, and response across endpoints as well as identities, email, and applications. It combines signals from those sources and produces information about scope and impact of threat. M365 Defender can take automatic actions to prevent or stop the attack. It can also automatically purge threats from mailboxes, endpoints, and identities. (Microsoft, 2021c)

4.8.1 Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is endpoint security platform to prevent, detect, investigate, and respond to advanced threats using endpoint behavioral sensors, cloud security analytics and threat intelligence. Sensors, analytics, and threat intelligence are used by service to automatically generate alerts based on that data when any threat is observed at endpoint sensor collected data.

Defender for Endpoint collects endpoint data to Microsoft Security Center and combines easy to observe analytics of current state of risks, vulnerabilities and threats against network and endpoints. It provides insight of endpoint device patch levels, vulnerabilities and recommendations and mitigations for emerging threats. Defender for Endpoint has automatic investigation and remediation capabilities that can be used to fight against incidents that has spread in volume and thus reducing the manual workload. (Microsoft, 2021f)

4.8.2 Microsoft Defender for Identity

Microsoft Defender for Identity is cloud based security solution utilizing on-premises Active Directory signals for identifying, detecting, and investigating advanced threats, compromised identities, and insider threats in on-premises environments. It is used in hybrid environments to detect advanced attacks using user monitoring, entity behavior and activities using advanced analytics based on past behavior. Defender for Identity monitor and learn on user activities and it creates behavioral baseline for each user and entity, and alerts if it recognizes activity that is not in line with past behavior. Defender for Identity is able to detect for example Lateral Movement Paths, users or devices using clear-text passwords, reconnaissance attempts of users, group memberships, IPs and more, brute force attacks, failed logins, group membership changes, Pass the Ticket, Pass the Hash, Overpass the Hash, remote code execution on DC, DC Shadow, malicious DC replication, Golden Ticket etc. (Microsoft, 2020i)

4.8.3 Microsoft Defender for Office 365

Microsoft Defender for Office 365 is security product for safeguarding organization emails, links, and collaboration tools. Defender for Office 365 comes with two pricing plans, Plan 1, and Plan 2. Plan 1 includes Safe Attachments, Safe Links, Safe Attachments for SharePoint, OneDrive and Teams, Anti-phishing, and real-time detections functionality. Plan 2 has all Plan 1 capabilities plus Threat Tracker, Threat Explorer, Automated investigation and response, Attack Simulator, and Campaign Views functionality. These functionalities can be tailored by using policies available for configuration. Real-time reporting functionality allows holistic view for monitoring Defender for Office 365 performance and organization threat level considering email and collaboration related threats. (Microsoft, 2021g)

Automated Investigation and Response (AIR) of Defender for Office 365 can be launched manually or when alert occurs. AIR analyzes email in question and entities related to that email. After the investigation, details and results can be viewed and recommended actions are introduced depending on the investigation results. Security operator can then initiate remediation actions. (Microsoft, 2021a)

4.9 Microsoft 365 Security Center

Microsoft 365 Security Center is a unified portal that combines protection, detection, investigation, and response to email, collaboration, identity, and device threats in single portal for improved clarity and easiness to view and control current security threats in those areas in organization. Functionalities of Office 365 Security & Compliance center, Microsoft Defender for Office 365, Microsoft Defender for Endpoint are built in. Incident & alerts, Hunting, Action Center and Threat analytics functions can be used against all signals coming from devices, email analytics, collaboration tools at the same time, providing rich visibility to what is happening in IT security. Unified investigations in Microsoft 365 Security Center allows security operator to drill down deeper from incidents and alerts to user or entity actions CASB, Azure AD, AD, and range of sources. (Microsoft, 2021i)

5 On-premises security controls for cloud services

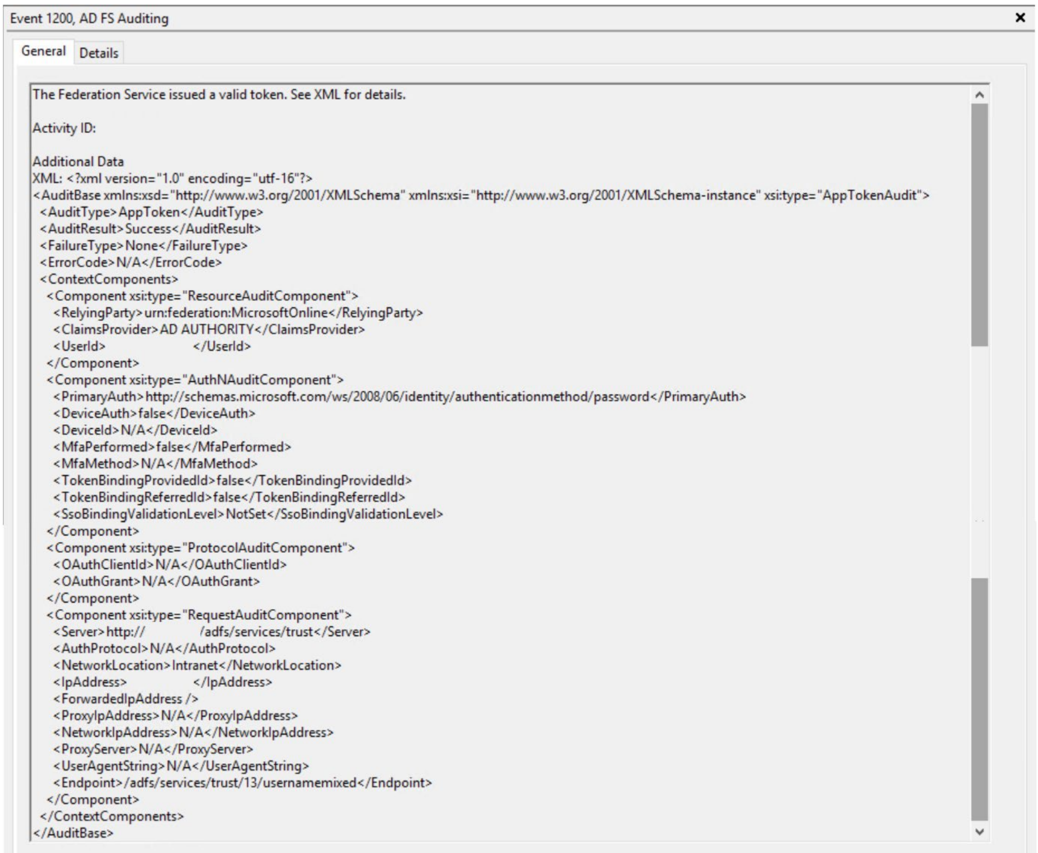
On-premises security controls and analytic systems are considered effective in case where data or identity is used in on-premises environment. In SaaS, or any cloud service, data itself and cloud identity resides in cloud and in most part is a user accessing those cloud services and data. However, there are exceptions in identity when using hybrid identity model. In hybrid identity model, user account authentication is done against on-premises systems and typically user account group membership, user properties, account status and account policies are projected to cloud identity. This means for example, that if user account is locked or disabled, user is no longer able to use its cloud identity.

5.1 Visibility to data and applications in the cloud

With the data and cloud applications, there are no such exceptions like with identities. When data is in the cloud service, and data user is outside of corporate network, only on-premises control between the data and user is the identity itself. For example, when user is signing into his OneDrive in Microsoft 365 SaaS service with browser application, browser is first redirected Azure AD sign-in page where email address (UPN) of the user is requested. When user enter his email address, Home Realm Discovery (HRD) process in the backend will read user and organization settings and redirects user browser either organization own Idp (ADFS) or represent password screen for user. After successful credential validation, user is redirected to Azure AD STS service with token, that will be exchanged to valid access and refresh token. These tokens allow user to access his OneDrive and other Microsoft 365 services that allows access to that user with his credentials.

When examining closer the hybrid identity authentication case against ADFS, which log entry is in picture below, it can be noticed, that only information about what resource user is going to access is the relaying party: urn:federation:MicrosoftOnline, which is known as Azure AD.

As can be seen in figure 17 below, and given the fact, that token lifetime is minimum of hours, on-premises logging lacks all the detailed and important information about what, how and when user is accessing cloud content or application.



```
The Federation Service issued a valid token. See XML for details.

Activity ID:

Additional Data
XML: <?xml version="1.0" encoding="utf-16"?>
<AuditBase xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="AppTokenAudit">
 <AuditType>AppToken</AuditType>
 <AuditResult>Success</AuditResult>
 <FailureType>None</FailureType>
 <ErrorCode>N/A</ErrorCode>
 <ContextComponents>
  <Component xsi:type="ResourceAuditComponent">
   <RelyingParty>urn:federation:MicrosoftOnline</RelyingParty>
   <ClaimsProvider>AD AUTHORITY</ClaimsProvider>
   <UserId>                    </UserId>
  </Component>
  <Component xsi:type="AuthNAuditComponent">
   <PrimaryAuth>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password</PrimaryAuth>
   <DeviceAuth>false</DeviceAuth>
   <DeviceId>N/A</DeviceId>
   <MfaPerformed>false</MfaPerformed>
   <MfaMethod>N/A</MfaMethod>
   <TokenBindingProvidedId>false</TokenBindingProvidedId>
   <TokenBindingReferredId>false</TokenBindingReferredId>
   <SsoBindingValidationLevel>NotSet</SsoBindingValidationLevel>
  </Component>
  <Component xsi:type="ProtocolAuditComponent">
   <OAuthClientId>N/A</OAuthClientId>
   <OAuthGrant>N/A</OAuthGrant>
  </Component>
  <Component xsi:type="RequestAuditComponent">
   <Server>http://             /adfs/services/trust</Server>
   <AuthProtocol>N/A</AuthProtocol>
   <NetworkLocation>Intranet</NetworkLocation>
   <IpAddress>                </IpAddress>
   <ForwardedIpAddress />
   <ProxyIpAddress>N/A</ProxyIpAddress>
   <NetworkIpAddress>N/A</NetworkIpAddress>
   <ProxyServer>N/A</ProxyServer>
   <UserAgentString>N/A</UserAgentString>
   <Endpoint>/adfs/services/trust/13/usernamemixed</Endpoint>
  </Component>
 </ContextComponents>
</AuditBase>
```

Figure 17. ADFS Log Entry for Cloud Sign-in (Loukkaanhuhta, 2021)

5.2 Cloud log handling in on-premises

Microsoft Azure AD, the cloud identity plane, and most SaaS applications provide APIs or other means to stream or export cloud generated sign-in and activity logs. These logs can be imported, consumed, and analyzed in on-premises log analytic solutions, like on-premises SIEM. Correlations and alerts can be created for different use cases, but due to complexity of SIEM rules needed and amount of log data, using the on-premises log analytics is not feasible in many cases. When reviewing some publicly found price lists about different commercial SIEM system license, price range was from few thousand euros to hundreds of thousands of euros, depending on which features were included and how much data is ingested and recommended hardware for mid-level implementation would likely cost several tens of thousands of euros.

SaaS services produce incredible amounts of audit data, and if organization would like to have complete vision to all systems with full audit trail and correlation, then all the data from SaaS services should be ingested to on-premises SIEM system and build SIEM use cases and automated correlations between different datapoints. Even then, on-premises SIEM system would not receive sign-in or audit data in near real time and is not able to automate actions in the cloud. Automatic response functionality would be most likely to cost vast amount of premium over SIEM solution. Because of the amount of data and likely huge expenses of on-prem based cloud SIEM system is not feasible option in many organizations.

6 Implementation of on-premises connected cloud IT security architecture

6.1 Planning the architecture

Current operational environment, requirements from assigner and cloud-based security tool capabilities were limiting factors for architecture planning. Most suitable and flexible security control framework was selected for security control mapping.

6.1.1 Operational environment

When using hybrid identities in SaaS service model, user accounts are sourced from on-premises directory to Azure AD, while data itself resides in the SaaS service, as seen on Figure 6. Consuming, creating, and sharing the data is done in the cloud using Azure AD authenticated identity, using either managed or unmanaged device. Authentication is done against on-premises ADFS, and it produces security log event in ADFS, which can be interpreted as login to Azure AD services. But, as found in table (Appendix 1.), and from Chapter 5. on this thesis, on-premises security solutions have only limited means for preventing anything by itself in the cloud, and they have only limited visibility in any action in cloud.

As learned in Chapter 3.3, in Cloud Only Identity model, authentication is done directly against Azure AD. This means that when cloud only account is used, authentication information never exists in on-premises. As per Microsoft’s recommendations, administrative accounts should use cloud only identities. This is largely because in case of on-premises infrastructure failure or connectivity issues, administrator’s authentication is impossible if organization is not using password hash sync functionality and thus cloud management is not possible. Using cloud only identities with administrators will also improve security of cloud. If bad actor gains access to on-prem infrastructure and has way to tamper user data or group memberships or configuration of Azure AD Connect service that syncs account and groups to cloud, then cloud only identity is not affected. And when this recommendation is followed, any administrative access is not seen in on-premises logon activity logs.

To summarize the operational environment dilemma before cloud security control connectivity has been built, we can say that, on-premises security controls and logging are insufficient regarding the cloud by themselves even if hybrid identities are used and user authentication is done against on-premises infrastructure. To gain cloud visibility and control capabilities in on-premises security systems, minimum of cloud log connectivity to on-premises security infrastructure must be created.

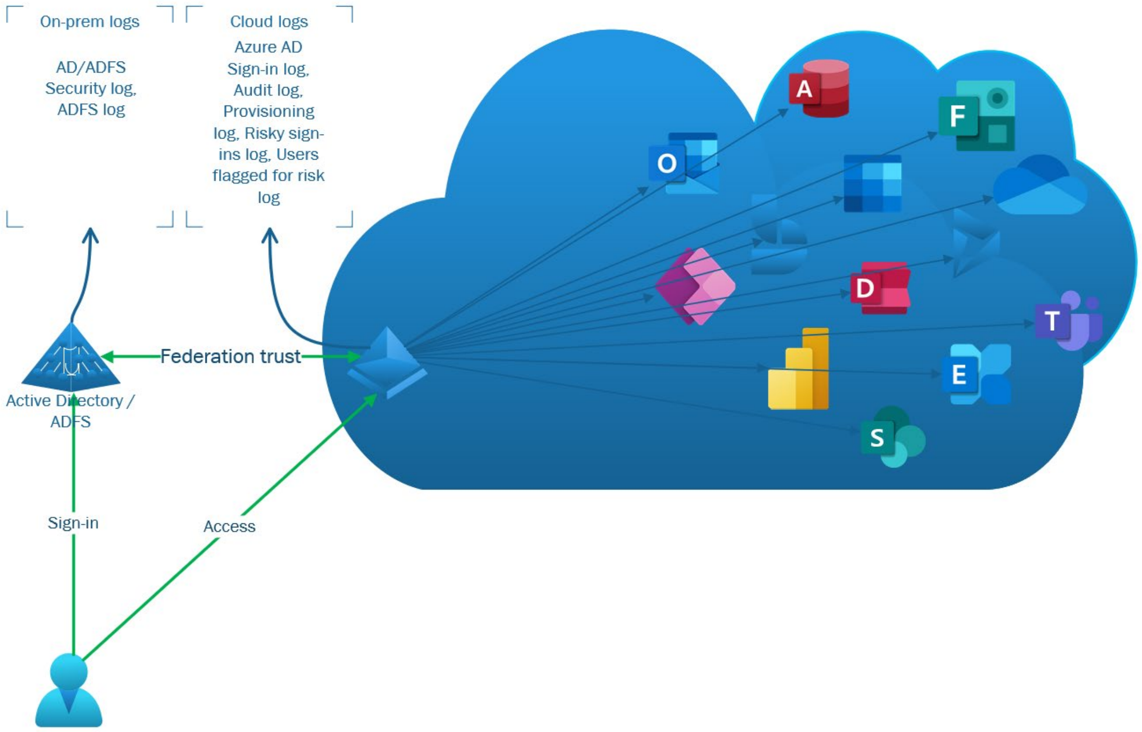

On-prem logs
AD/ADFS Security log, ADFS log
Cloud logs
Azure AD Sign-in log, Audit log, Provisioning log, Risky sign-ins log, Users flagged for risk log
Federation trust
Active Directory / ADFS
Sign-in
Access
A
F
O
D
T
E
S

Figure 18. Operational environment dilemma (Loukkaanhuhta, 2021)

6.1.2 Requirements for implementation

While there were not any hard requirements other than implementation should follow best practices and should not introduce more threats or privacy issues, it was agreed that while visibility and control will assumably greatly improve, quality of alerts and their handling should also be improved. During the multiple discussions with IT security personnel, automatization, AI analyzing capabilities and configuration possibilities should be used to achieve visibility and remediation.

Cost-wise it was agreed that cloud-based log retention and analysis capabilities would be used for log data produced in cloud, because amount of data cloud produces it would introduce challenges in log handling and licensing in on-premises log analytics. Alerts and some log data would need to be exported to on-premises log collectors for further analysis. In start phase, only limited amount of on-premises log data would be imported to cloud-based log analysis.

Four sample use case were provided, and implementation should be able to contribute solution for those use cases. Sample use cases were:

1. Leaked credentials
2. Credential lock-out
3. Phishing and malware
4. Data is shared too broadly

Because no upper limits for how comprehensive the implementation should be, it was agreed that if it has no monetary impacts and time allows and it improves security or security management, that can be implemented. Since sample use cases were comparably trivial to achieve in some scale, more advanced use cases were studied on top of those. Assigner wanted to take full advantage of already made investments to licenses, so implementation should try to take full advantage of licensed capabilities.

6.1.3 Security control frameworks and control selection

When planning security controls in security architecture implementation, numerous security control frameworks can be used as a reference, like ISO 27002, PCI-DSS or NIST 800-53. Some cloud specific security control frameworks are also available, like cloud controls matrix from the Cloud Security Alliance. These frameworks provide exhaustive list of security controls, but not all of them are usable or relevant in all cloud implementations and building every security control mentioned in frameworks are not feasible or economical. (Deloitte, 2011)

Finding a suitable framework that fulfills all the relevant requirements and needs but is not presenting itself as a security control cornucopia, seems hard to find as finding a unicorn. With cloud services and different organizations, one size fits all solution do not exist. During the literature review, it was noted, that while different methods for choosing the controls exists, none of them fitted precisely to this case. While different standardized security control frameworks were reviewed, and most versatile solution, NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations, was selected. NIST 800-53 has comprehensive list of controls and guidance for control selection and applicability. (NIST, 2020) Applicable and relevant technical security controls for SaaS use case were selected from NIST list and effectiveness of chosen controls were reviewed and compared against on-premises and cloud security controls. Resulting table (Appendix 1.) lists which on-premises or cloud-based security control can be used in SaaS use case for fulfilling control requirement.

6.1.4 Building blocks for implementation

To summarize the framework of implementation, following should be taken into an account:

- Implementation should utilize and take advantage of Microsoft A5/E5 + EMS E5 license functionalities.
- Alerts from the cloud should be sent to on-premises SIEM.
- NIST 800-53 applicable technical controls for SaaS use case should be implemented.
- Solutions for sample use cases should be included in implementation.
- Quality and number of alerts should be reasonable: AI, analytics and automatization should be used.
- Log data produced in cloud should be analyzed in cloud.

NIST 800-53 security controls list was studied thoroughly, then curated, and applicable security controls were mapped to available security controls, other capabilities and products that can be used to create control. These products and capabilities can be found on table. (Appendix 1.)

6.2 Architecture model

Architecture model was created based on the requirements of implementation and based on capabilities cloud-based tools offered. Basic principle was that controls would be implemented with most versatile means and every action, from authentication to data access, is logged and analyzed. Resulting architecture model can be observed in picture below.

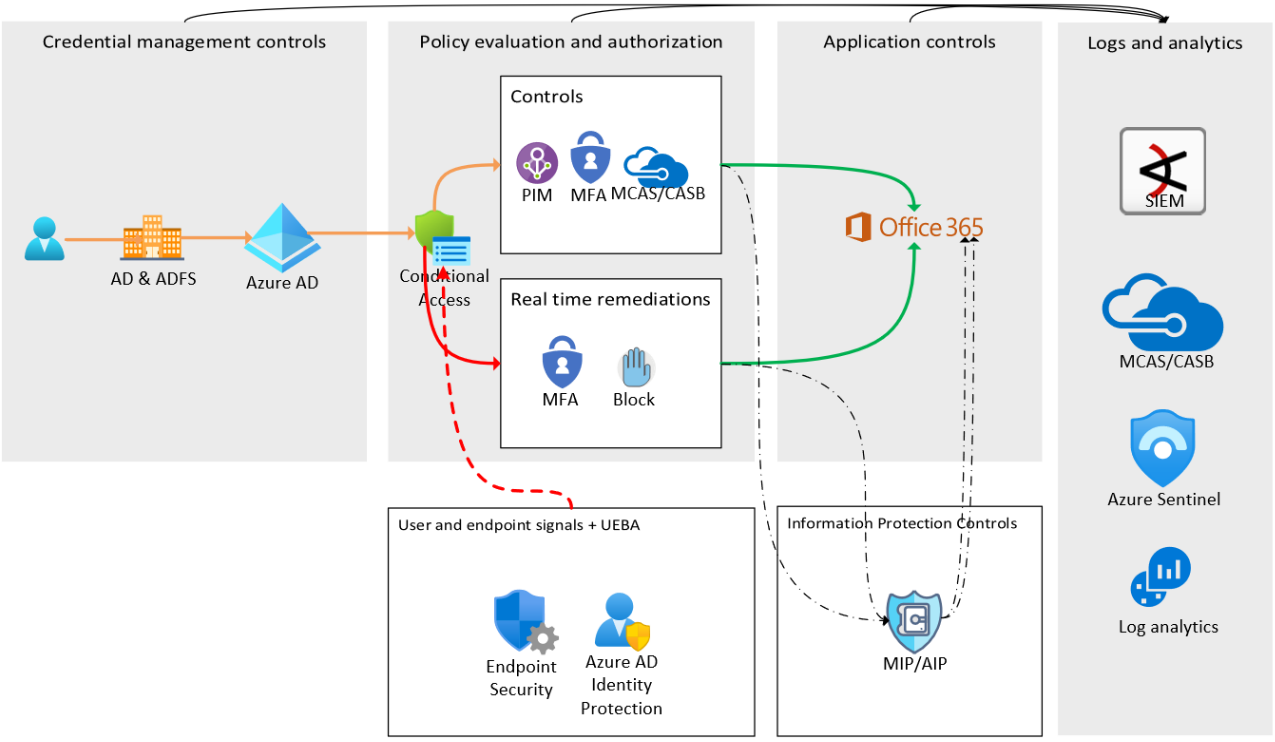


Figure 19. Architecture model (Loukkaanhuhta, 2021)

6.2.1 SOC workflow

Because vast majority of data, identity and security related functionality was already built on-premises infrastructure, implementation of cloud security architecture was planned to connect and extend security posture to the cloud, taken into a consideration unique risks of the cloud.

As current SOC workflow was taken into consideration and decision was made to route all alerts from Azure Sentinel and CASB, and some log data to on-premises SIEM system which was considered as main SOC window to security situation. Other important SOC utilization points were Azure Sentinel and Microsoft Cloud App Security (MCAS/CASB) portal which were planned for closer investigation resource.

Azure Sentinel planned to be used to dig deeper in alerts by its own tools like log queries and workbooks. Sentinel is also capable to send email alerts for alerts and incidents based on log queries. Automation workflows for minor incident automatic remediations were built to fight against alert fatigue.

CASB utilizes risky user and risky sign-in information from Azure AD Identity protection component, these create alerts that are remediated in CASB user interface, alerts are also forwarded to on-premises SIEM system. CASB alerting supports natively SMS alerting, and that has been engaged for high severity alerts to maximize notification of high severity incidents. Custom CASB policies were created for advanced scenarios where signals from multiple sources were combined, and alerts were generated based on multiple variables. Automation workflows were created for user notification and remediation of content-based threats.

During the time of ongoing research, unified Microsoft 365 Security Center was announced, and some of the functionalities from different products, like Defender for Endpoint and Defender for Office 365 portal functionality has been moving to unified portal.

6.2.2 Authentication and Control Architecture

User account control is placed in on-premises Active Directory and user authentication is implemented in ADFS. Authorization is provided by Azure AD with Conditional Access Policies. Conditional Access Policies include controls and requirements for accessing SaaS services.

Evaluation of conditions may include client details, user account details, user risk score, sign-in risk score, IP address of client, user or entity behavior-based risk analysis, anomaly detection, device compliance etc. Multiple policies are evaluated, and decision about access will be made based on signals. Some combination of signals may lead to blocking the access, while some signal combinations will grant the access. Every step is audited, logged, and analyzed.

6.2.3 Log and signal flow architecture

On-premises SIEM receive logs and signals from on-premises part of hybrid identity components, Active Directory and ADFS, via log collectors. Azure Sentinel generated alerts and incidents as well as MCAS/CASB alerts and activity are sent to on-premises SIEM system using connectors. Office 365 and Azure AD logs and activities are fetched by SIEM connector thru Office 365 Management Activity API.

Azure Sentinel receive logs and signals with its built-in connectors that are configured to connect different log sources. In SaaS use case following connectors and their data sources were configured.

Table 2. Sentinel connectors and data sources (Loukkaanhuhta, 2021)

Connector	**Data source**
Azure Active Directory	Sign-in logs, Audit logs, Non-interactive user sign-in log, Service principal sign-in logs, Managed Identity Sign-in logs, Provisioning logs
Azure Active Directory Identity Protection	SecurityAlert(IPC)
Azure Information Protection	InformationProtectionLogs_CL
Dynamics365	Dynamics365Activity
Microsoft 365 Defender	DeviceInfo, DeviceNetworkInfo, DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceRegistryEvents, DeviceLogonEvents, DeviceImageLoadEvents, DeviceEvents, DeviceFileCertificateInfo
Microsoft Cloud App Security	Alerts, Cloud Discovery Logs
Microsoft Defender for Endpoint	SecurityAlert(MDATP)
Microsoft Defender for Identity	SecurityAlert(AATP)
Microsoft Defender for Office 365	SecurityAlert(OATP)
Office 365	OfficeActivity (SharePoint), OfficeActivity (Exchange), OfficeActivity (Teams)

Microsoft Cloud App Security receive its log information from Azure AD and Office 365, risk signals and data from Identity Protection and Defender for Identity integration and endpoint sensor signals and cloud discovery data from Defender for Endpoint integration.

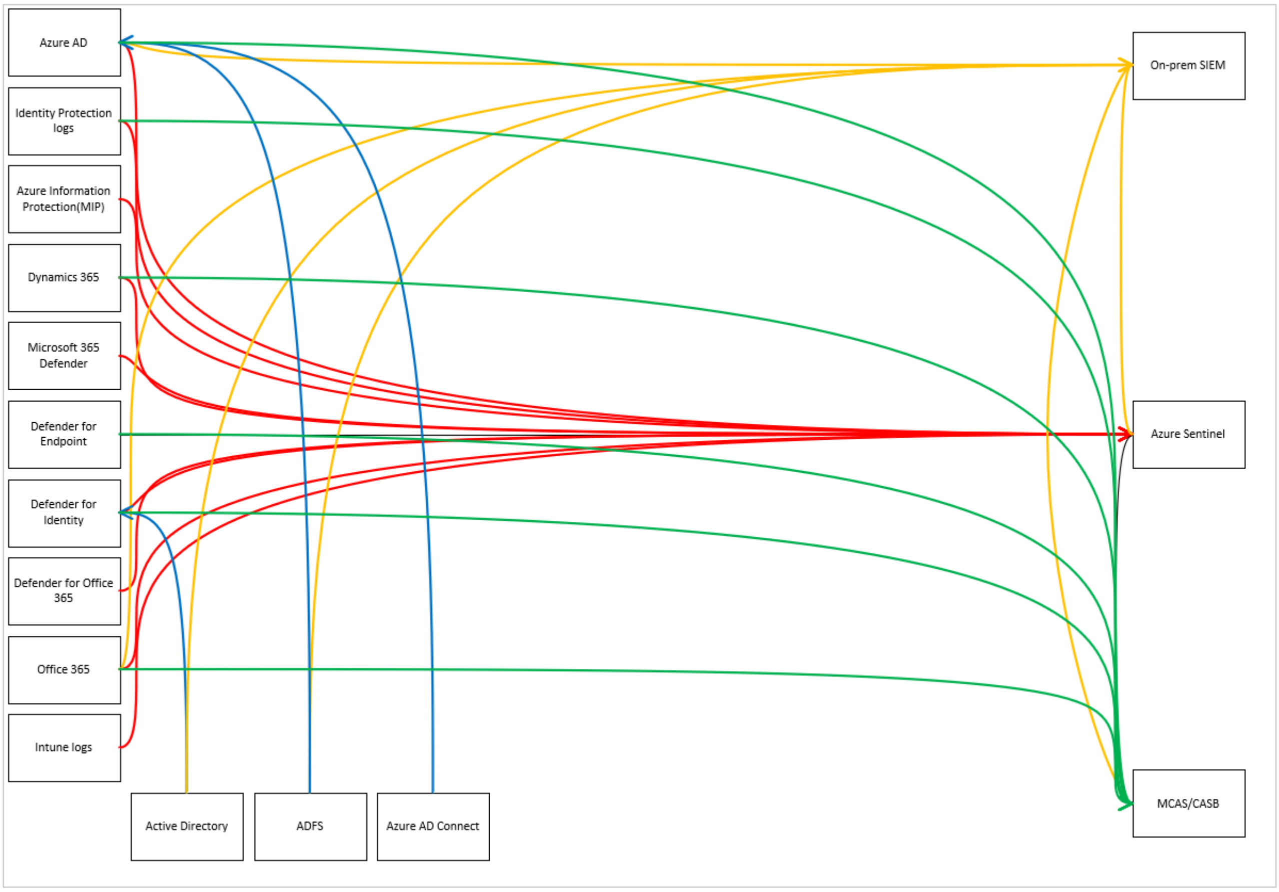


Figure 20. Log and Signal Flow of Implementation (Loukkaanhuhta, 2021)

6.3 Technical implementations

In technical implementation planning, product selection was done by going thru NIST 800-53 security control list and finding applicable controls from different on-premises and cloud-based tools. This product selection method produced a table of applicable technical controls and tools, that were used to implement the controls in architecture.

6.3.1 Access control related products and functionality

Active Directory and Azure AD Connect is used for account disablement and blocking. Account is disabled in Active Directory, and to get effect in cloud, account synchronization is needed. Azure AD Connect will synchronize account information to Azure AD, and Azure AD will block the account in cloud on next synchronization cycle.

Azure Active Directory (Azure AD) is used as cloud directory where user's cloud account resides. Account can be blocked directly in Azure AD user properties and for example using Suspend user - functionality in CASB. In case of hybrid identity however, if user was disabled on cloud, that account block will be unblocked on the next synchronization cycle if on-premises account is not disabled.

Azure AD Conditional Access Policies is used for evaluating access to resources depending on the requirements in different use cases and for session termination functionality. Enforcement of MFA is carried out using Conditional Access policies.

Microsoft Information Protection is used for classifying and securing the content in SaaS services.

ADFS Extranet Smart lockout and Azure AD Smart lockout are used to implement prevention of account lockout abuse.

Microsoft Cloud App Security (MCAS/CASB) is used for alert creation and handling, policy creation, account monitoring for atypical usage and session control.

Microsoft Identity Protection is used for enforcing risky user and risky sign-in actions. Maintains list of user's risk level. Different policies are enforced on different level of risk. Risk level can be raised by signaling from CASB to enforce harder policies to users if atypical behavior is recognized.

Microsoft Sentinel is used as cloud based SIEM and to gather all logs in one place and allows automatic analysis of signals.

Privileged Identity Management (PIM) is used to remove any standing admin access from users. Role elevations are required to be done thru PIM.

On-premises SIEM is used as a receiver of some logs and alerts from cloud services. SIEM use cases for atypical account activity monitoring can be created when cloud logs are received.

6.3.2 Audit and accountability related products and functionality

Microsoft 365 Advanced Audit Logs are enabled by assigning license to users. After enablement of advance logging, all user actions across Office 365 will be logged and is visible in Office 365 audit log search. All log information is read only, so tampering is not possible. Administrative actions are included in the log.

On-premises SIEM is used to pull Azure AD and Office 365 activity from Office 365 Management Activity API. CASB sends all alerts and activities to SIEM with remote syslog connectivity. On-premises SIEM could be connected to Microsoft Graph Security API to pull all alert information, but in this case product APIs were used to get meaningful data easily to on-premises SIEM.

Microsoft Cloud App Security is used to search and analyze user actions as well as enrichment of activities from other log sources. Can be used for central review and analytics for Office 365 usage. Provides automatic processing and correlation of log data as well as alerting. Alerts are streamed to on-premises SIEM and Azure Sentinel with security extension SIEM connector. Conditional Access App Policy is used for session control and monitoring. Session control and monitoring policy automatically creates reverse proxy for SaaS applications, and it can be used to restrict actions in sessions, real time, e.g., block download of files if user is connected from unknown device.

Microsoft Azure Sentinel is used as central analytic and orchestration service. Sentinel analyzes logs automatically based on built analytic rules and workbooks and behavioral analytics. It is connected to all cloud log sources and it produces alerts and automatically creates actionable incidents for SOC workflow.

6.3.3 Identification and authentication related functionality

Active Directory thru ADFS works as authentication plane. Active Directory is source for user identity and group membership information. Password policies and user restrictions will follow AD password policies and restrictions.

Azure AD is authorizing party for user identities in cloud for SaaS applications.

Azure AD Conditional Access Policies are used to enforce different identity and access enforcements. CA policies are used in different situations like requirement of MFA or when resource should be allowed to use only with organization devices, or access should be granted only from organization network or enforcing short lifetime sessions with MFA for administrators.

Azure AD external identities functionality can be used for cross organization collaboration.

7 Results

Research produced three kinds of results. Review of architecture implementation's effectiveness towards selected use cases, qualitative results from the interview of SOC analyst and technical evaluation of incident data with quantitative results and analysis from incidents.

7.1 Reference use cases

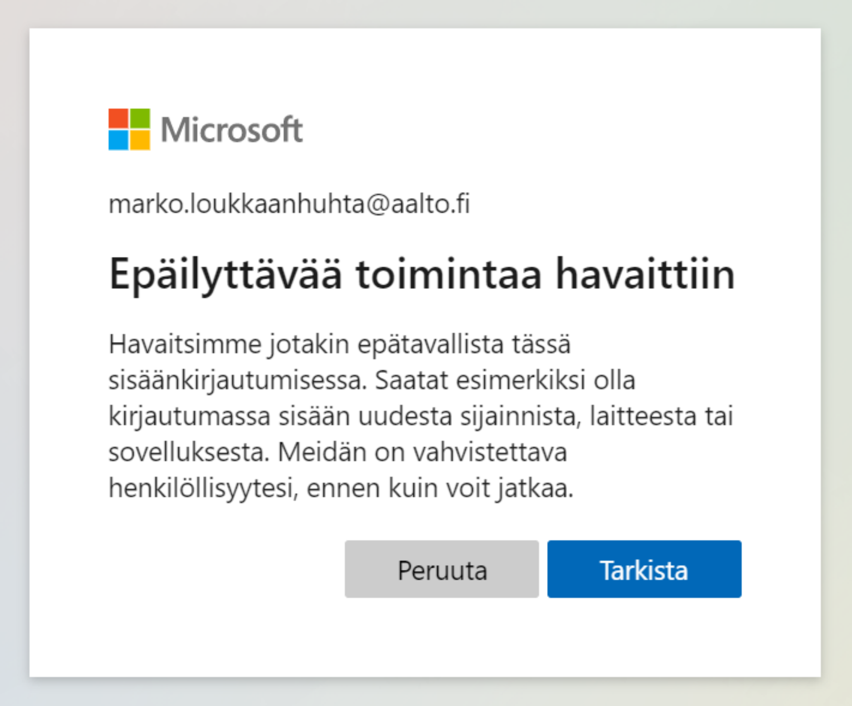
Aalto University IT suggested during the thesis planning phase, that four use cases could be reviewed with SaaS use cases. These topics were selected as a reference use cases for the implementation. Use cases were later tested and analyzed against implemented solution for their effectiveness. Implementation was not planned and built for these cases specifically.

1. Leaked credentials
2. Credential lock-out
3. Phishing and malware
4. Data is shared too broadly

7.1.1 Leaked credentials

Prevention of credential leak is complicated task which consist of user education and technical means. Technical implementations may include password policies, password protection functionality in AD and Azure AD, credential leak detection using cloud intelligence, multifactor authentication, or moving to password-less authentication methods like authenticator app or FIDO2 security keys.

Detection and remediation of credential leak is done automatically by the system when configured correctly. Azure AD Identity Protection alone will stop authentication attempts when using credentials with unfamiliar sign-in properties. This was tested by signing in from device in different country, from TOR network or using different kinds of clients. When something unusual were detected, user was prompted to use MFA to continue. Implementation was configured with rather tight settings to detect anything unusual. These policies should detect almost all activity when trying to get access to cloud data with leaked credentials.



Microsoft

marko.loukkaanhuhta@aalto.fi

Epäilyttävää toimintaa havaittiin

Havaitsimme jotakin epätavallista tässä sisäänkirjautumisessa. Saatat esimerkiksi olla kirjautumassa sisään uudesta sijainnista, laitteesta tai sovelluksesta. Meidän on vahvistettava henkilöllisyytesi, ennen kuin voit jatkaa.

Figure 21. Real-time Remediation of Risky sign-in (Loukkaanhuhta, 2021)

Attack investigation can be done with Azure Sentinel, which allows complete timeline review in visualized way and digging deeper into logs using KQL queries in log analytics workspace in Sentinel.

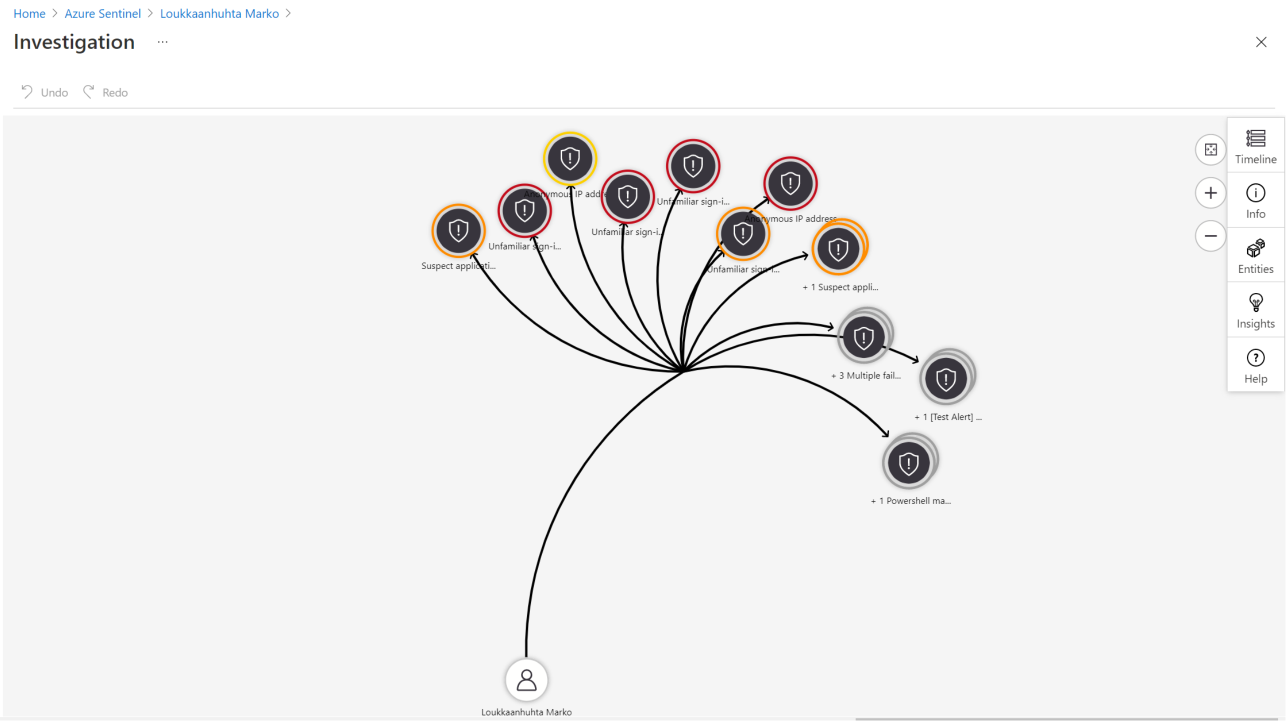


Figure 22. Investigation of account related incidents in Azure Sentinel (Loukkaanhuhta, 2021)

When someone tries to sign-in with unfamiliar properties, Identity Protection generated alert. This alert is also visible in CASB and Sentinel and forwarded to on-premises SIEM.

CASB and Sentinel allows examination of user activities thoroughly, so any actions that account has conducted can be seen.

7.1.2 Credential lock-out

Credential lock-out DoS attacks or brute forcing user passwords may lead to user account locking and credential owner is not allowed to sign-in even on-premises in hybrid identity architecture. In this implementation, hybrid identities are used, meaning that in most cases, user is directly authenticated against on-premises ADFS. In some situations, it might be possible for trying to authenticate against the cloud first, for example if legacy authentication protocols are used to authenticate user, like with IMAP protocol to Exchange Online service.

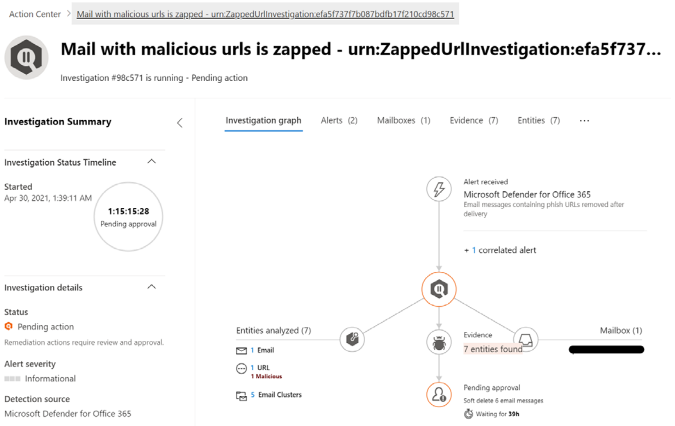
In case of ADFS, extranet smart lockout feature is used to protect from account lockouts. When bad credentials are used, it increments bad password count in AD, and AD lock-out policy will lock account when threshold is reached. Extranet smart lockout feature will temporarily cease account login from abusive IP before AD lock-out policy threshold is reached. IP addresses are stored in Risky IP table in ADFS and are transferred from there to Connect health service. List of these IP's can be downloaded from Connect health and list can be used in IP blacklisting in firewalls if needed.

Azure AD has its own similar functionality, Smart lock-out, for preventing credential lockouts in cases where password hash-sync or pass-thru authentication is used. It is configurable in Azure AD password protection.

Testing this functionality failed because of load balancer configuration, which lead to inconsistencies in client IP detection. To test and properly take advantage of the functionality, some infrastructure changes are needed.

7.1.3 Phishing and malware

Implementation could find all test emails and test malwares sent to recipients, and Microsoft Security center was able to automatically find related messages and sent them thru automatic investigation to Action center, where SOC operator could take actions to specific detect email or whole email cluster if sent to multiple users. On investigation view, SOC operator can verify if automated investigation has created false or true alerts before taking the action.



Action Center > Mail with malicious urls is zapped - urn:ZappedUrlInvestigation:efa5f737f7b087bdfb17f210cd98c571

Mail with malicious urls is zapped - urn:ZappedUrlInvestigation:efa5f737...

Investigation #98c571 is running - Pending action

Investigation Summary

Investigation Status Timeline

Started
Apr 30, 2021, 1:39:11 AM

1:15:15:28
Pending approval

Investigation details

Status
Pending action
Remediation actions require review and approval.

Alert severity
Informational

Detection source
Microsoft Defender for Office 365

Investigation graph | Alerts (2) | Mailboxes (1) | Evidence (7) | Entities (7) | ···

Alert received
Microsoft Defender for Office 365
Email messages containing phish URLs removed after delivery

+ 1 correlated alert

Entities analyzed (7)
1 Email
1 URL
1 Malicious
5 Email Clusters

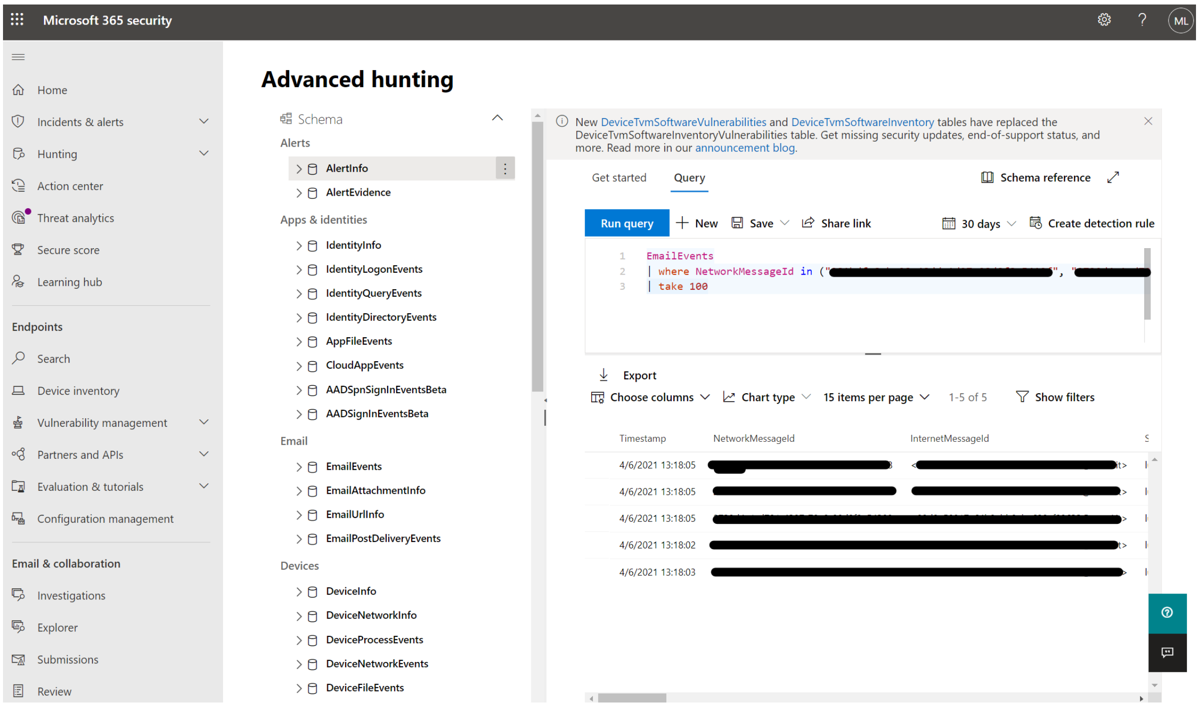
Evidence
7 entities found

Mailbox (1)
[redacted]

Pending approval
Soft delete 6 email messages
Waiting for 39h

Figure 23. Investigation summary for automated investigation (Loukkaanhuhta, 2021)

Advanced hunting can be used to further examine the data.



Advanced hunting

New DeviceTvmSoftwareVulnerabilities and DeviceTvmSoftwareInventory tables have replaced the DeviceTvmSoftwareInventoryVulnerabilities table. Get missing security updates, end-of-support status, and more. Read more in our announcement blog.

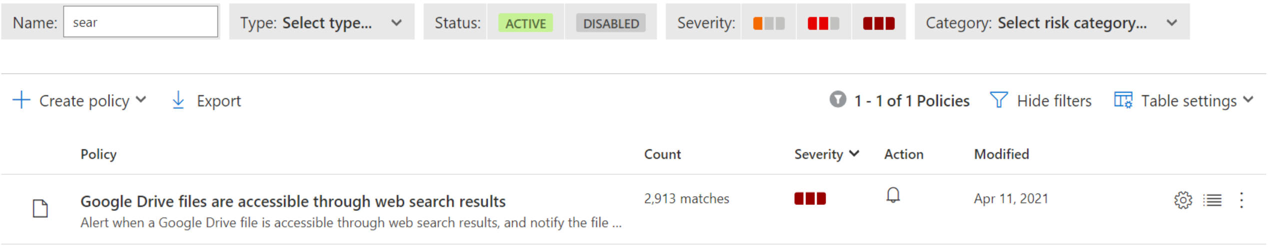
```
EmailEvents
| where NetworkMessageId in ("[redacted]", "[redacted]
| take 100
```

Timestamp	NetworkMessageId	InternetMessageId
4/6/2021 13:18:05	[redacted]	[redacted]it>
4/6/2021 13:18:05	[redacted]	[redacted]>
4/6/2021 13:18:05	[redacted]	[redacted]>
4/6/2021 13:18:02	[redacted]	[redacted]t>
4/6/2021 13:18:03	[redacted]	[redacted]>

Figure 24. Advanced hunting in Microsoft 365 security (Loukkaanhuhta, 2021)

7.1.4 Too broadly shared data

Too broadly shared data is detected with CASB policies. Build-in policies allows to detect and automatically mitigate too broadly shared data. Policy was created that send automized email for user who has shared files from cloud storage without any controls, i.e., files that are searchable via Google search.



Name: sear

Policy	Count	Severity	Action	Modified
Google Drive files are accessible through web search results Alert when a Google Drive file is accessible through web search results, and notify the file ...	2,913 matches	■■■		Apr 11, 2021

Figure 25. Policy for detecting accidentally too broadly share Gdrive documents (Loukkaanhuhta, 2021)

7.2 Interview

7.2.1 Interview arrangements

Aim of the interview was to get qualitative data of the implementation impact from IT security specialist/SOC analyst who is the main person analyzing IT threats in organization IT security management. Interview session was arranged by using Microsoft Teams audio meeting. Interview followed predetermined topics, using semi-structured questions. Interview was done in Finnish. In the start of the interview, short summary about the architecture and implementation was brought to interviewee to remind what has been done along the implementation process.

Interview answers were written down in Finnish during the interview. After the interview, questions were summarized and sent back to interviewee to confirm that everything was correctly interpreted, and literation was done properly. After interviewee's review of literation, questions and answers were analyzed and interview summary was translated to English.

7.2.2 Interview questions

Interview questions were originally Finnish, following is the English translated question list:

1. What are the concrete IT security implications, from an IT security departments perspective, after the Microsoft's cloud-based IT security products were deployed?
2. Has the deployment of cloud-based IT security products been reflected in the organization's security statistics, has the number of cases decreased or has the time taken to resolve them changed, or has the ability to detect the incidents improved?
3. What effects do you think the introduction of the products has had, for example, do you feel that you have facilitated / complicated or improved / degraded security management, has it increased / decreased workload, clarified / blurred the overall security situation?
4. IT security products produce signals, generate alerts and notifications. What kind of improvements have cloud-based products bring in examining these notifications, i.e., does tools make easier to distinguish unnecessary alerts from relevant ones, and have UEBA (user and entity behavior analysis) functions highlighted events that might not otherwise have been detected?
5. During the deployment phase, we ended up in a decision for sending automatic alerts to users as well, e.g., when alert was created after user account were signed in from TOR network, or user were sharing files accidentally too broadly from cloud storage or user had saved malware on his cloud storage. How do you see that the automatic message to the user has affected the user's actions after receiving the notification of suspicious activity related to his account?

6. At the design phase of the thesis, IT security department wanted to find some ways or means for four use cases, which were: Leaked account, including MFA scenarios (what to do and how to determine the extent of impact), Account lockouts (in the cloud), phishing and malware discovery management, accidentally shared data too to widespread / wrong persons. Did cloud security products provide a means to investigate and resolve these use cases?
7. Signals and alerts from cloud security products have now been brought into the on-premises SIEM system through various integrations, so some visibility of the cloud has been brought into the on-premises solution as well. How would you estimate the future development of IT security solutions as more and more applications and data go to the cloud, i.e., will cloud-based IT security solutions play a more important role in the future than on-premises solutions?

7.2.3 Interview results and analysis

Interview were tried to lead in the way, that IT security person's subjective opinions about impact of implementation of cloud-based Microsoft security tools were able to be acquired and any future improvements or pain points would be recognized.

In overall, interview revealed that visibility in IT security on cloud services has clearly improved and is still increasing after the cloud-based security tools implementation. Situation awareness has improved and got more depth. Cloud-based tools have highlighted few incidents, that could not be seen at all, because bad actor targeted only cloud services.

Some parts of implementation, like MFA, is now seen as a natural commodity that protects cloud services. Good experience about MFA protection has been a driving force for also starting MFA implementations to protect local services, and few projects are already underway.

Cloud-based IT security tools were able to detect some anomalies that were previously been unnoticed, those anomalies have now been able to visualize and treat. It was said that Microsoft Cloud App Security particularly have helped a lot, with its rich information, to resolve incidents that have been detected elsewhere. University's on-premises SIEM system and on-premises ATA along with the cloud-based tools has helped to identify some feasible incidents.

Automatic notification of users, about suspicious activity on their user accounts, seems to have changed user behavior according to interviewee, also number of malware findings on user's cloud storage have decreased. Interviewee felt that fine tuning Conditional Access Policies and thus generating alerts only from clear cases, would make automatized user notifications as great addition to their security portfolio. Automated notifications were also seen to commit users in IT security.

Only couple of leaked credentials have been detected since these tools and no phishing or malware from the cloud mail were seen. Handful of too broadly shared data from cloud services have been detected. According to interviewee, for example, with cloud mail and its security, the situation looks quite promising considering phishing and malware. At the time of interview, organization's cloud email transition was still underway, and interviewee pointed out, that it is interesting to see how the bigger masses affect the situation.

The supply of tools in the cloud was defined as already quite extensive, but the final breakthrough will take place when these tools are consolidated into a fewer management views from which it is easy to move to the so-called look and feel while maintaining the specific tools that work below. As a positive side effect, as it was seen, that cloud-based security tools implementation has also improved on-premises IT security.

At first, improved reconnaissance abilities of cloud-based IT security tools increased number of incidents, but situation has been since then gradually normalized said interviewee. Also, it was felt that amount of work has increased since new tools were introduced, but later that has been normalizing. Number of new tools were felt little overwhelming, new things needed to learn and it was difficult to find right place where most significant threat indicators were found. Overall cloud security (Microsoft) was felt little scattered and needed some time to adjust to new. Interviewee hopes that these tools will migrate to or at least fewer portals. Gathering more know-how of these tools and strengthening of usage of cloud based SIEM (Azure Sentinel) was seen as solutions that will also bring some help to situation.

Interviewee was interested to see, what kind of new improvements would be available when more on-premises sources was connected to cloud-based tools, e.g., Defender for Endpoint brings signals from endpoint sensors to the cloud.

Mitigation means for the account lockouts will probably require changes in the topology as per interviewee, but the hope is high for that as well.

The amount of data (including the logs) in the cloud is huge and interviewee does not think it makes sense to transfer them to limited resources on-premises systems. Data growth is currently fast and the best platform for handling this is provided by the cloud. In the future, as the number of logs and observations may change in the other direction as well, the cloud will have a clear advantage due to its scalability. This is not what on-premises solutions offer, meaning iron and licensing does not scale very easily, if at all said interviewee. Interviewee pointed that their current operating model is to decentralize on-premises and cloud logs, respectively, and to import the most important pieces of logs and alerts from the cloud to on-premises SIEM. Interviewee told that, operating model will be reviewed all the time and decisions will be reflected from the maturity, costs and the ongoing changes to the licensing and service model of our current on-premises solution.

Interviewee sees that cloud-based security tools are currently evolving faster than on-premises solutions. Some of the current players are already looking for the cloud and moving their services there (malware management, spam handling, SIEM products) e.g., in the name of easier scalability.

“But players who have started in the cloud (like Microsoft) have gained a clear lead over these and will, capture a big piece of cake.”, interviewee said. This seems to be true at least in case of Microsoft. In January 2021 it was reported that Microsoft has surpassed 10 billion dollars in revenue on security business with over 40 percent growth in year to year. Microsoft has been investing in cloud security for years with over 1 billion dollars per year, and it seems to pay off.

Interview results indicated that real life experiences were in line with the hypothesis about positive impact of implementation of Microsoft cloud-based IT security tools to enhance visibility and control to cloud based threats.

7.3 Technical evaluation of identity and access related incident data

7.3.1 Identity and access related incident data sources

Examination of identity and access control related incident sources were undertaken on Azure Sentinel because it allows effectively filter incidents with different parameters, like source product of incident, incident severity and owner of incident. Timeframe used for analysis was one month and incidents were picked from live data between 29th March 2021 to 29th of April 2021. In that timeframe, over 1,7 million cloud service authentications were analyzed. Three most important sources for identity and access related incident data were selected for further examination, Microsoft Cloud App Security (MCAS/CASB), Identity Protection and Azure Sentinel.

7.3.2 Incident data analysis

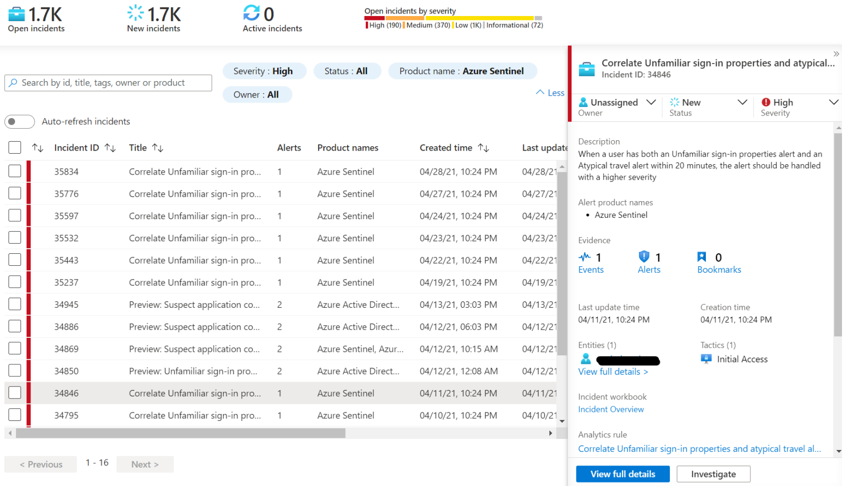
As can be seen on Table 3. below, Identity Protection generated most of the incidents and they were classified as medium severity. Medium severity incidents in Identity Protection are typically generated when user is signing in from new or unseen device or client that is not line with past properties, signing in from country where user has not signed before, or user is signing in from multiple locations same time, or sign-ins from different countries are conduct in less time that physically traveling to those locations were possible or signing in from anonymous IP. Identity Protection can be seen as a key signal source for advanced CASB and Sentinel data analysis. Signals about any suspected user, device or other anomalies from Identity Protection are used for enhancing quality and accuracy of CASB and Sentinel alerts. Finding highlights the importance of Identity Protection signals in other products.

Table 3. Identity and access related incidents and severity (Loukkaanhuhta, 2021)

Source	**Low**	**Medium**	**High**	**Total**
MCAS/CASB	9	102	127	**238**
Identity Protection	951	159	51	**1161**
Azure Sentinel	63	107	16	**186**

From incident statistics (Appendix 2.), it can be seen, that while CASB is utilizing different data sources like Identity protection for creating alerts and incidents, it truly excels in content-based threats. In this timeframe when research was conducted, number of content-based incidents were surprising low from what has been seen earlier.

Azure Sentinel uses more advanced rules for detections. Threshold for alert generation is commonly higher that is with Identity Protection and CASB. Sentinel can raise alert severity based on number of evidence and this is used in current implementation to reduce the excessive number of minor alerts.



1.7K Open incidents | 1.7K New incidents | 0 Active incidents

Open incidents by severity: High (190) | Medium (370) | Low (1K) | Informational (72)

Search by id, title, tags, owner or product

Severity : **High** | Status : **All** | Product name : **Azure Sentinel** | Owner : **All**

Auto-refresh incidents

Incident ID	Title	Alerts	Product names	Created time	Last update
35834	Correlate Unfamiliar sign-in pro...	1	Azure Sentinel	04/28/21, 10:24 PM	04/28/21
35776	Correlate Unfamiliar sign-in pro...	1	Azure Sentinel	04/27/21, 10:24 PM	04/27/21
35597	Correlate Unfamiliar sign-in pro...	1	Azure Sentinel	04/24/21, 10:24 PM	04/24/21
35532	Correlate Unfamiliar sign-in pro...	1	Azure Sentinel	04/23/21, 10:24 PM	04/23/21
35443	Correlate Unfamiliar sign-in pro...	1	Azure Sentinel	04/22/21, 10:24 PM	04/22/21
35237	Correlate Unfamiliar sign-in pro...	1	Azure Sentinel	04/19/21, 10:24 PM	04/19/21
34945	Preview: Suspect application co...	2	Azure Active Direct...	04/13/21, 03:03 PM	04/13/21
34886	Preview: Suspect application co...	2	Azure Active Direct...	04/12/21, 06:03 PM	04/12/21
34869	Preview: Suspect application co...	2	Azure Sentinel, Azur...	04/12/21, 10:15 AM	04/12/21
34850	Preview: Unfamiliar sign-in pro...	2	Azure Active Direct...	04/12/21, 12:08 AM	04/12/21
34846	Correlate Unfamiliar sign-in pro...	1	Azure Sentinel	04/11/21, 10:24 PM	04/11/21
34795	Correlate Unfamiliar sign-in pro...	1	Azure Sentinel	04/10/21, 10:24 PM	04/10/21

< Previous 1 - 16 Next >

Correlate Unfamiliar sign-in properties and atypical...
Incident ID: 34846

Owner: Unassigned | Status: New | Severity: High

Description
When a user has both an Unfamiliar sign-in properties alert and an Atypical travel alert within 20 minutes, the alert should be handled with a higher severity

Alert product names
- Azure Sentinel

Evidence
1 Events | 1 Alerts | 0 Bookmarks

Last update time: 04/11/21, 10:24 PM
Creation time: 04/11/21, 10:24 PM

Entities (1): [redacted]
Tactics (1): Initial Access

Incident workbook: Incident Overview

Analytics rule: Correlate Unfamiliar sign-in properties and atypical travel al...

Figure 26. Azure Sentinel automatic alert severity decisions (Loukkaanhuhta, 2021)

When summing up and examining the indicators that were used to generate an incident, following diagram reveals that while some rules create incident from one indicator, but most of the incidents are generated from rules that uses multiple indicators and utilizes machine learning and AI for detections, like unfamiliar sign-in properties, which compares current sign-in behavior and properties against past behavior and properties.

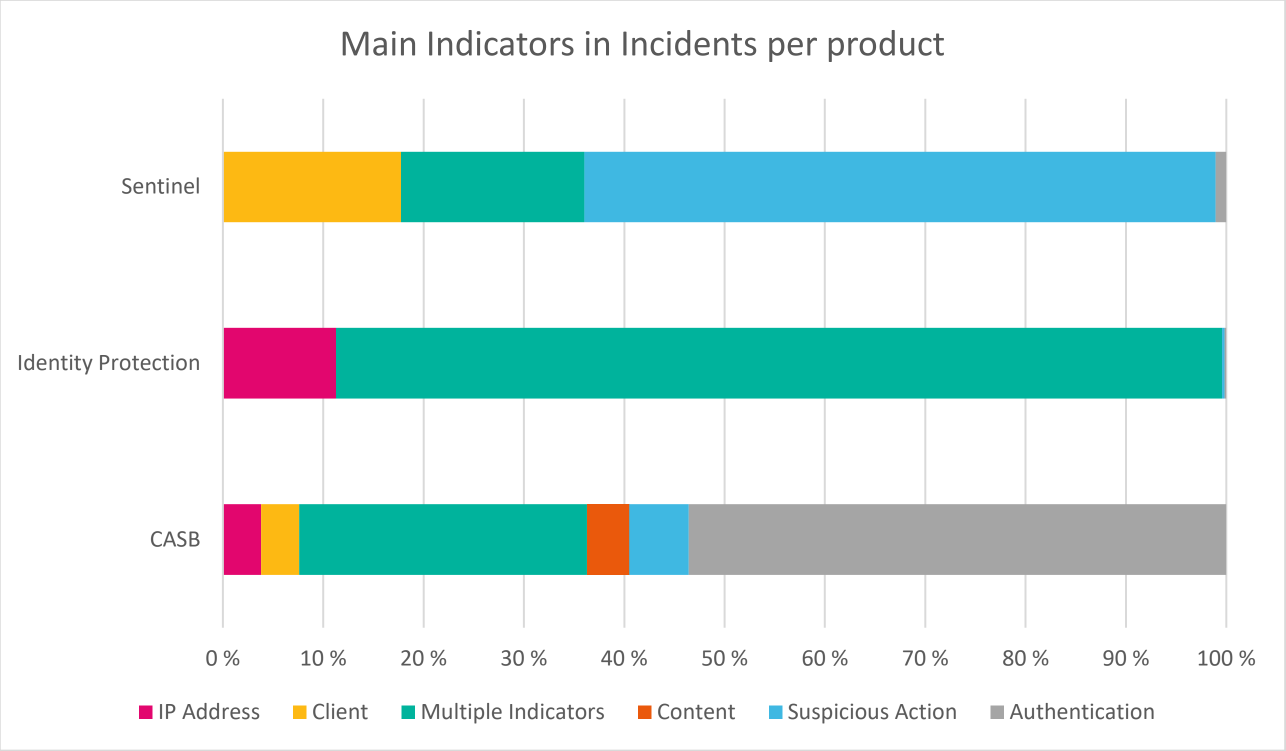


Figure 27. Main indicators in incidents per product (Loukkaanhuhta, 2021)

High number of authentication failures with high severity were detected in CASB, but further examination revealed that almost all were false positives that was caused by MFA/VPN configuration combination, which requires use of MFA when IP address changes. This can happen if user did not supply second method MFA when requested by client software at computer wake-up phase before VPN was connected. When authentication failures were taken off from the diagram, it visualizes more clearly advantages of machine learning capabilities of cloud-based security tools.

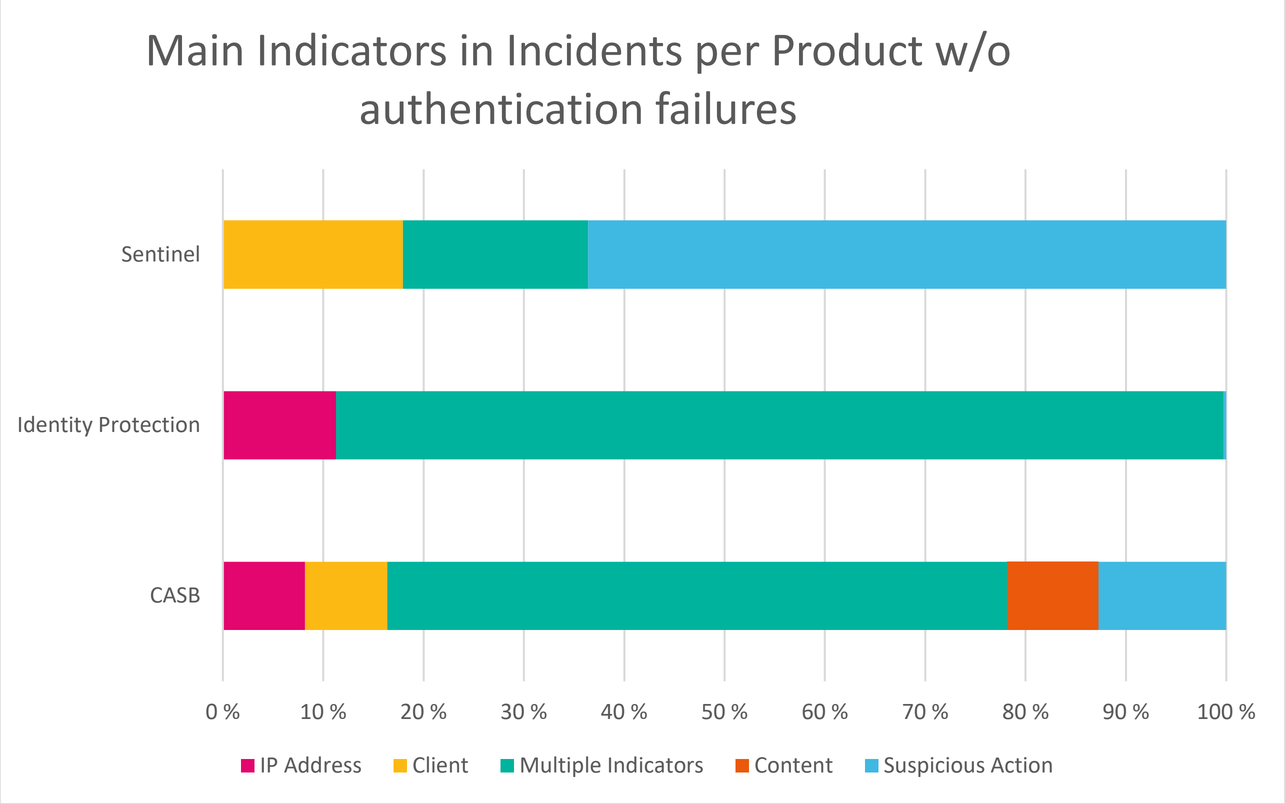


Figure 28. Main indicators in incidents per product without authentication failures (Loukkaanhuhta, 2021)

7.4 Summary of results

On-premises security tools does not have visibility or control in the cloud, other than in authentication phase in case where hybrid identities are used. Without connecting logs and/or alerts from cloud-based security tools to on-premises security systems, what happens in the cloud, stays in the cloud. These two environments can be defined as loosely connected distinct islands with common identity. Microsoft SaaS products do have some controls and monitoring capabilities by itself, even security related, without paying extra from licenses. Closer look revealed that their ability is quite low when requirements for log data retention is high or when advanced detection and protection capabilities are needed.

After the implementation was built, it was examined. Cloud-based IT security implementation effectiveness towards reference use cases was successful, despite technical challenges in infrastructure against credential lock-out DoS attacks. Numerous ways to prevent credential leak could be utilized and detection of leaked credentials was automatic with cloud-based tools. Phishing and malware cases were able to handle with selected tools. For too broadly shared data, built-in detection and alert rule existed for Google Drive sharing and custom rule were implemented for OneDrive and Dropbox data.

Interview results highlighted importance of cloud-based tools and their effectiveness towards cloud-based threats. MFA was found as one of the most important pieces of puzzle in cloud security incident prevention, and it can and should be employed to protect local services as well. While cloud-based tools are effective, multitude of them seem to be burden for SOC analysts, as well as number of alerts they generate at start. Cloud-based security tools were able to detect incidents that would have remain unnoticed without them. Cloud based attacks would not been noticed without implemented architecture. Automatic user notification implementation has changed how users act in cloud; it was also seen to commit users in IT security. Visibility and situation awareness was clearly improved and got more depth after the cloud-based security tools implementation process. Surprisingly, cloud-based implementation did help a lot in investigations in cases where incidents were detected in on-premises systems.

Incident data analysis indicated that different products generate alerts via different means. Vast number of incidents were generated with indicators from machine learning and AI based rules. Information Protection functionality fed its signals to CASB and Sentinel, and these two systems processed signals further to generate alerts. Sentinel processes data from huge amounts of sources, and alert generation quantity greatly depends on which kind of rules are created. Sentinel is capable of incident severity adjustment based on number of evidence found on incident data, there are built-in rules that employs it, and custom rules are easy to do.

Conditional access policies, MFA enrollment and Identity Protection are components that, if utilized, can prevent most of the identity-based threats in cloud. When CASB and Azure Sentinel are taken in, cloud data can be protected, and data leaks, as well, could be detected and automatically prevented. Sentinel is powerful tool for detecting, as well as, investigating threats and incidents. If quality of alerts is more important than number of alerts, automatization should be employed in alert handling. To minimize alert count in SOC workflow where on-premises SIEM is tool used for analysis and alerts, connecting only Sentinel alerts to on-premises SIEM should be taken into consideration.

8 Conclusions and discussion

8.1 Conclusions

Aim of the research was to increase knowledge about phenomenon how security paradigms' shift from perimeter-centric security to identity- and data-centric security affects IT security capabilities and to deliver answers and insights to this matter.

1. How security paradigms' shift from perimeter-centric security to identity- and data-centric security affects IT security capabilities?
2. How can organization improve visibility in Microsoft SaaS services with cloud-native security features and tools?
3. What is the added value for organization's Cyber Security management regarding Identity and Access Management when organization adopts Microsoft provided cloud native security tools?

Thesis was able to deliver answers to all research questions. Answer to main question "How security paradigms' shift from perimeter-centric security to identity- and data-centric security affects IT security capabilities?" was able to be answered as early as in introductory part, and it is quite self-evident. When on-premises and cloud are only connected thru identities, these two environments can be defined as loosely connected distinct islands with common identity. This was also verified by mapping cloud applicable security controls from NIST 800-53 to security controls available in on-premises and in cloud.

First sub question "How organization can improve visibility in Microsoft SaaS services with cloud-native security features and tools?" was answered in chapter 6, where solution was designed and built. Designed IT architecture solution was tested and found greatly improving visibility in Microsoft SaaS services. Cloud-based security tools were not just comprehensive, but also included much anticipated advanced features for fighting back of advanced threats.

Answer to second sub question "What is the added value for organization's Cyber Security management regarding Identity and Access Management when organization adopts Microsoft provided cloud native security tools?" was answered in chapter 7, where results from reference use cases, interview and technical evaluation identity and access related incidents were conducted and reported. Designed IT architecture was able to gain much needed visibility and control to Microsoft SaaS services and it brought broad and depth to situational awareness. Numerical analysis was difficult to apply on this research, but it was able to provide evidence of what kind of threats are present and what are their indications and share of different kind of threats in real world situations.

Answers were not delivered in exhaustive and definite form, but on proposed solution with multiple products was designed, executed, and examined. Additionally, for answering the research questions, this thesis introduced main cloud security components and their functionalities and relation to other tools and how they can be connected and what kind of tuning can be done to achieve desired amount of information or alerts from cloud services to on-premises security systems.

Thesis may be significant eye opener for any IT management personnel for understanding the importance of cloud security and for IT security personnel to see how real-world incident data is formed in cloud-based security tools and what are their indicators. Thesis was also able to demonstrate and highlight significance of user and entity behavior analytic based security controls in defending against user identity related threats.

Key points noticed in this research that should be highlighted:

1. On-premises logging and monitoring and as well as access controls are not capable of recognize nor react in cloud-based threats without properly expanding security capabilities to cloud services.
2. Cloud native security features and tools allows almost full visibility to cloud.
3. Almost full visibility to all actions in cloud allows adaptive access controls based on user and entity behavior, automated correlations of signals across systems, automated actions to threats, automated mitigations, impressive alerting capabilities, risk scoring of login attempts and more with very little money.
4. With lots of configuration options and automation, alert fatigue can be easily avoided by automating low priority threat mitigations and prioritizing high impact threats.
5. Cloud-based tools are economic choice, and they are effective for most of the threats.
6. Cloud native tools are easy to integrate to different systems with native connectors and standard log file support.
7. User and Entity Behavior (UEBA) capabilities are VERY effective for stopping bad actor's sign-in attempts.
8. IT Security department was really impressed about cloud visibility increase and for all the capabilities that basically cost nothing more than work.

8.2 Reliability

Thesis consisted of planning, building and evaluation of on-premises connected cloud-based IT security architecture that was implemented for the organization that assigned the thesis. It was generalized in some extent to allow it to fit for different kinds of organizations and use cases and allow highlighting main issues and solutions that may be common to many cases.

While architecture was generalized in some ways, it does not fit for all situations. Differences in configurations and design choices would not fulfill requirements that some organizations could have.

Building, testing, and reviewing the solution was conducted by same person, and while trying to be as objective one can be, there still is possibilities for unintentional bias in results. Lack of complete documentation of control functionalities may also lead to false assumptions about their functionalities, but these were tried to test as thoroughly as possible in sensible time available for this work.

Quantitative results represent findings in this specific organization, with specific configuration and only in certain and limited timeframe. This leads to situation, that results are valid only in context of this thesis.

8.3 Discussion

Moving to the cloud changes lot in terms of user's ability to work. It also poses unique challenges for protecting data and user identities. Advanced threats are more and more common than ever, and fight against new and more advanced threats is just beginning. Adversaries are targeting to users and user devices with more advanced methods. Living of the land binaries and web shells have brought new challenges to on-premises and device security landscape. Email phishing and malware are increasingly used to gain access to inside the organization, while old methods are still in used by attackers. Threat landscape is broadening with huge speed. When attackers use multiple methods in multiple places together to get foothold in organization, defense should also acquire signals with multiple methods from multiple places. Correlation of signals from complete system stack is important to detect advanced threats effectively.

On-premises SIEM systems used as cloud data analyzing may quite fast hit the economic wall due hardware limitations and licensing costs if all cloud logs and signals are routed there. This may suggest, that in future, cloud-based security tools will play even more bigger part in many organizations.

While it may be obvious for person working in IT, that on-premises security controls and tools cannot see what is happening in cloud or SaaS services, it may not be so obvious for management that will ultimately decide funding and resourcing for security tools. Even if organization is not leaning toward fighting advanced threats, utilizing cloud native security tools may be the right choice if flexibility, effortless and economic reasonings are important.

Cloud security is not all about tools and their capabilities. This thesis did not focus important things like residual risk of cloud services and risk acceptance or contracts between suppliers and with users, all equally important aspects when data is moving to cloud. Information management plan and how it dictates what data can be handled in cloud is first step to governed and systematic approach for cloud transformation. Planning the continuity and resilience etc. These should be the priority before moving to cloud.

Cloud security expertise is currently in huge demand, and area that cloud security consist of is huge. It is impossible for one person to handle cloud security holistic and in details, because variety of cloud services and security tools are growing every day. It is still important to understand basic concepts and tooling for cloud security.

8.4 Proposals for further research

Proposal for further research raises from the observation that cloud-based security tools are gaining foothold in organizations. It would be interesting area to study what kind of impact of on-premises log data analysis with cloud-based tools would have in organization IT security. Studied Microsoft cloud-based security tools can analyze full cloud stack and they have connectors and capabilities to analyze on-premises data also.

References

Aalto University, 2021b. *Aalto University Aitivision*. Accessed on 15 March 2021. Retrieved from https://www.aalto.fi/en/cyber-security

Aalto University, 2021a. *Aalto University History*. Accessed on 22 March 2021. Retrieved from https://www.aalto.fi/en/aalto-university/history

Ahmed, F., Shahzad, K., Aslam, H., Bajwa, S. U., & Bahoo, R., 2016. The Role of Collaborative Culture in Knowledge Sharing and Creativity among Employees. *Pakistan Journal of Commerce and Social Sciences*, 335-358. Accessed on 23 March 2021.

Deloitte, 2011. *How to ensure control and security when moving to SaaS/cloud applications.* Accessed on 12 March 2021.Retrieved from https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/ensure-control-security-saas-cloud-applications_SHU.pdf

Deloitte, 2020. *Why organizations are moving to the cloud*. Accessed on 25 March 2021. Retrieved from https://www2.deloitte.com/us/en/insights/industry/technology/why-organizations-are-moving-to-the-cloud.html

Gartner, 2018. Clouds Are Secure: Are You Using Them Securely? (J. Heiser, Ed.) Accessed on 18 March 2021. Retrieved from https://emtemp.gcom.cloud/ngw/globalassets/en/doc/documents/350439-clouds-are-secure-are-you-using-them-securely.pdf

Gartner, 2020. *Successfully Align Your Threat Detection and Incident Response Requirements to Your Service Providers*. Accessed on 19 March 2021. Retrieved from https://www.gartner.com/document/3989586?ref=gfeed

Halminen, V., 2019. Pilvipalvelun käyttöönoton tietoturva. [IT security of Cloud Service Deployment.] Jyväskylä: Jyväskylä University of Applied Sciences. Accessed 1 May 2021. Retrieved from http://urn.fi/URN:NBN:fi:amk-2019060314181

Koskinen, P., & Simola, V., 2019. Self-assessment of security in cloud deployment. Jyväskylä, Finland. Accessed on 15 March 2021. Retrieved from http://urn.fi/URN:NBN:fi:amk-201904175484

Microsoft, 2016. An overview of Azure Active Directory. Microsoft France. Accessed on 10 March 2021. Retrieved from http://download.microsoft.com/download/f/c/a/fca7c6e3-7153-4fb1-9825-0b1bb26f14e0/an-overview-of-aad.docx

Microsoft, 2017. SharePoint and OneDrive for Business Securing your content in the new world of work. Accessed on 15 April 2021. Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=55242

Microsoft, 2018a. *Control*. Accessed on 15 April 2021. Retrieved from https://docs.microsoft.com/en-us/cloud-app-security/control

Microsoft, 2018c. *What is Azure Active Directory Pass-through Authentication?* Accessed on 19 February 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

Microsoft, 2018b. *What is federation with Azure AD?* Accessed on 24 March 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

Microsoft, 2019a. Azure Information Protection Deployment Acceleration Guide. Accessed on 3 April 2021. Retrieved from https://aka.ms/AIPDAG

Microsoft, 2019b. *Choose the right authentication method for your Azure Active Directory hybrid identity solution*. Accessed on 28 April 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

Microsoft, 2019c. *What is hybrid identity with Azure Active Directory?* Accessed on 19 April 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity

Microsoft, 2020a. *Audit activity reports in the Azure Active Directory portal*. Accessed on 5 March 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

Microsoft, 2020b. *How and why applications are added to Azure AD*. Accessed on 19 February 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

Microsoft, 2020c. *How it works: Azure AD Multi-Factor Authentication*. Accessed on 28 April 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Microsoft, 2020d. *How long does Azure AD store reporting data?* Accessed on 30 April 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention

Microsoft, 2020j. *Implement password hash synchronization with Azure AD Connect sync*. Accessed on 7 April 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

Microsoft, 2020f. *Microsoft 365 identity models and Azure Active Directory*. Accessed on 28 April 2021. Retrieved from https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide

Microsoft, 2020g. *What is Azure Active Directory?* Accessed on 15 January 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Microsoft, 2020h. *What is Azure Sentinel?* Accessed on 1 May 2021. Retrieved from https://docs.microsoft.com/en-us/azure/sentinel/overview

Microsoft, 2020i. *What is Microsoft Defender for Identity?* Accessed on 27 March 2021. Retrieved from https://docs.microsoft.com/en-us/defender-for-identity/what-is

Microsoft, 2020i. *Microsoft Intune is an MDM and MAM provider for your devices.* Accessed on 5 March 2021. Retrieved from https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft, 2020e. *OAuth 2.0 authentication with Azure Active Directory*. Accessed on 27 February 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-oauth2

Microsoft, 2021a. *Automated investigation and response (AIR) in Microsoft Defender for Office 365*. Accessed on 2 February 2021. Retrieved from https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-air?view=o365-worldwide

Microsoft, 2021b. *Learn about information barriers in Microsoft 365*. Accessed on 25 April 2021. Retrieved from https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide

Microsoft, 2021c. *Microsoft 365 Defender*. Accessed on 20 April 2021. Retrieved from https://docs.microsoft.com/fi-fi/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide

Microsoft, 2021d. *Microsoft Cloud App Security overview*. Accessed on 22 February 2021. Retrieved from https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

Microsoft, 2021e. *Microsoft compliance offerings*. Accessed on 18 March 2021. Retrieved from https://docs.microsoft.com/en-us/compliance/regulatory/offering-home?view=o365-worldwide

Microsoft, 2021f. *Microsoft Defender for Endpoint*. Accessed on 16 April 2021. Retrieved from https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide

Microsoft, 2021g. *Microsoft Defender for Office 365*. Accessed on 16 April 2021. Retrieved from https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/defender-for-office-365?view=o365-worldwide

Microsoft, 2021h. *Shared responsibility in the cloud*. Accessed on 8 April 2021. Retrieved from https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Microsoft, 2021i. *The unified Microsoft 365 security center overview*. Accessed on 29 April 2021. Retrieved from https://docs.microsoft.com/en-us/microsoft-365/security/defender/overview-security-center?view=o365-worldwide

Microsoft, 2021j. *What is Azure AD Privileged Identity Management?* Accessed on 22 April 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Microsoft, 2021k. *What is Conditional Access?* Accessed on 11 April 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Microsoft, 2021l. *What is Identity Protection?* Accessed on 12 March 2021. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

Morrow, T., 2018. *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*. Accessed on 21 March 2021. Retrieved from https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

NIST, 2020. *SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations.* Accessed on 2 April 2021. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Pekkarinen, A., 2018. Enhancing security of cloud services with Microsoft Enterprise Mobility + Security. Jyväskylä: Jyväskylä University of Applied Sciences. Accessed on 21 February 2021. Retrieved from http://urn.fi/URN:NBN:fi:amk-2018121822165

Safari, F., Safari, N., & Hasanzadeh, A., 2015. The adoption of software-as-a-service (SaaS): ranking the determinants. *Journal of Enterprise Information Management, Vol. 28 No. 3, 2015*, 400-422.

Appendices

Appendix 1. Control Mapping against NIST Special Publication 800-53 Revision 5

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	On-prem Security Controls	Cloud Security Controls	Security Control established with
AC-2(3)	DISABLE ACCOUNTS	x	x	Azure AD connect synchronization, account state inherited from AD. Azure AD, CASB can block user sign in from cloud.
AC-2(5)	INACTIVITY LOGOUT		x	Azure AD Conditional Access Policy, session control, “Sign-in Frequency”. Per policy setting.
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT		x	Privileged Identity Management (PIM) for administrative roles.
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT		x	Privileged Identity Management (PIM) for administrative roles.
AC-2(11)	USAGE CONDITIONS		x	Azure AD Conditional Access Policy, CASB policy/alert.
AC-2(12)	ACCOUNT MONITORING FOR ATYPICAL USAGE	Partly	x	On-Prem: SIEM. Cloud: Azure AD Identity Protection, CASB policies, Sentinel.

AC-3	Access Enforcement		x	Access controls in object level and with Conditional Access Policies. MIP labeling.
AC-3(2)	DUAL AUTHORIZATION		x	Privileged Identity Management (PIM) for administrative roles and Azure resources.
AC-3(3)	MANDATORY ACCESS CONTROL		x	Information Barrier Policies in Office 365. Will restrict usage of content between classification levels.
AC-3(4)	DISCRETIONARY ACCESS CONTROL		x	Microsoft Information Protection.
AC-3(7)	ROLE-BASED ACCESS CONTROL	x	x	Possible with Administrative Roles. Possible with Identity Governance / Access package. Possible to use synced AD groups in some roles. In some roles, must use identity, not group, i.e., Security Center.
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS	x	x	Immediately by revoking sessions and tokens in Azure AD or CASB. Disabling on-premises account will affect after next Azure AD Connect sync cycle.

AC-3(9)	CONTROLLED RELEASE		x	Data can be released controlled when data is protected with Microsoft Information Protection (MIP). Labels/encryption/audit.
AC-3(11)	RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES		x	MIP labeling, Information Barriers.
AC-3(13)	ATTRIBUTE-BASED ACCESS CONTROL	x	x	On-prem: IDM level to AD groups, Cloud: Azure AD dynamic user security groups, based on synced AD attributes.
AC-3(14)	INDIVIDUAL ACCESS		x	Individual Access is part of “Data subject request” in Compliance manager.
AC-3(15)	DISCRETIONARY AND MANDATORY ACCESS CONTROL		x	Access controls in object level and with Conditional Access Policies, MIP.
AC-7	Unsuccessful Logon Attempts	x	x	On-prem: AD account policies, ADFS smart lockout for IP’s, Azure AD adaptive smart lockout, CASB policies.
AC-7(1)	AUTOMATIC ACCOUNT LOCK		x	Intune policies for Mobile devices.
AC-7(2)	PURGE OR WIPE MOBILE DEVICE		x	Intune policies for Mobile devices.

AC-7(4)	USE OF ALTERNATE AUTHENTICATION FACTOR		x	SSPR (Self-service-password-reset) functionality allows account lockout with MFA.
AC-8	System Use Notification	x	x	On-prem: During ADFS logon it is possible to notify user, but it is in authentication phase. Cloud: Possible with CASB per SaaS application.
AC-9	Previous Logon Notification		x	In some SaaS services, and for all services: mysignins.microsoft.com
AC-12	Session Termination		x	Azure AD Conditional Access Policy, session control, “Sign-in Frequency”. Per policy setting.
AC-16	DYNAMIC ATTRIBUTE ASSOCIATION		x	CASB allows pseudonymization of some private information. Revealing user is controlled by roles and audited in Governance log.
AC-19(1)	USE OF WRITABLE AND PORTABLE STORAGE DEVICES		x	Azure AD Conditional Access Policy, “Require Compliant Device”
AC-19(2)	USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES		x	Azure AD Conditional Access Policy, “Require Compliant Device”

AC-19(3)	USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER		x	Azure AD Conditional Access Policy, “Require Compliant Device”
AC-21(1)	AUTOMATED DECISION SUPPORT		x	Can be enforced by SaaS service or with MIP.
AC-24(1)	TRANSMIT ACCESS AUTHORIZATION INFORMATION		x	Azure AD Conditional Access Policy, Azure AD sign-in risk policy, Azure AD user risk policy, CASB policies.
AC-24(2)	NO USER OR PROCESS IDENTITY		x	Azure AD Conditional Access Policy, location condition.
AU-3	Content of Audit Records	x	x	On-Prem: Microsoft 365 Advanced Audit Logs can be streamed to SIEM from cloud. Cloud: M365 Advanced Audit Logs can be connected to Sentinel, streamed to CASB, viewable thru M365 portal, M365 management API
AU-3(1)	ADDITIONAL AUDIT INFORMATION		x	Multisource enrichment can be done on Sentinel and CASB
AU-4	Audit Log Storage Capacity	x	x	On-Prem: Challenging and costly to gather all cloud logs, monitoring is possible for storage capacity alerts. Cloud: No capacity cap, but retention time cap. Allows up to 10 years retention in M365, with Azure longer times

				possible if logs are stored in Storage Account.
AU-4(1)	TRANSFER TO ALTERNATE STORAGE	x	x	Can be stored or streamed alternate storage.
AU-6(4)	CENTRAL REVIEW AND ANALYSIS	Partly	x	On-Prem: SIEM. Cloud: Sentinel and CASB.
AU-7	Audit Record Reduction and Report Generation	Partly	x	On-Prem: SIEM. Cloud: Sentinel and CASB.
AU-7(1)	AUTOMATIC PROCESSING	Partly	x	On-Prem: SIEM. Cloud: Sentinel and CASB.
AU-8	Time Stamps	x	x	On-Prem: NTP synced source and processing. Cloud: UTC zone everywhere.
AU-9	Protection of Audit Information		x	Cloud: Source logs are read only, not possible to alter or delete.
AU-10	Non-repudiation		x	Cloud: Using MFA for proofing the identity and M365 advanced logging, full Azure AD audit and Sign-in logs has complete visibility actions performed.
AU-12	Audit Record Generation		x	Full system-wide, time correlated audit trail. Can be streamed in standard format to external SIEM with connectors from API or thru Azure Event Hub.

				Allows defining of rights to log data in granular way. Allows complete log analyzing via Sentinel.
AU-14	Session Audit		x	Possible with CASB Conditional Access App Policy.
AU-14(3)	REMOTE VIEWING AND LISTENING		x	Possible with CASB Conditional Access App Policy.
IA-2	Identification and Authentication (Organizational Users)	x	x	On-Prem: Identification and authentication phase 1. in ADFS. Cloud: Authentication phase 2. and authorization in Azure AD.
IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS		x	Azure AD Conditional Access Policies.
IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS		x	Azure AD Conditional Access Policies.
IA-2(6)	ACCESS TO ACCOUNTS — SEPARATE DEVICE		x	Azure AD Conditional Access Policies.
IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT		x	Using FIDO2 device for Azure AD authentication.
IA-2(10)	SINGLE SIGN-ON		x	Azure AD issued tokens.

IA-2(13)	OUT-OF-BAND AUTHENTICATION		x	Azure AD Conditional Access Policies.
IA-3	Device Identification and Authentication	x	x	Azure AD Conditional Access Policies, managed, compliant device.
IA-7	Cryptographic Module Authentication		x	Using FIDO2 device for Azure AD authentication.
IA-8	Identification and Authentication (Non-Organizational Users)		x	Using Azure AD external identities.

Appendix 2. Incident statistics during the research timeframe

CASB	**Number of incidents**
(Low) Activities from suspicious user agents	9
(Med) Activity from a Tor IP address	7
(Med) Activity from infrequent country	1
(Med) Impossible travel activity	67
(Med) Investigation priority score increase	1
(Med) Malware detection	10
(Med) Mass delete	3
(Med) Mass download	5
(Med) Multiple failed login attempts	2
(Med) Ransomware activity	2
(Med) Unusual addition of credentials to an OAuth app	4
(High) Administrative activity from a non-corporate IP address	1
(High) Multiple failed user logon attempts to a service	125
(High) System alert: Salesforce App connector error	1
Identity Protection	
(Low) Anonymous IP address	50
(Low) Malware linked IP address	37
(Low) Unfamiliar sign-in properties	861
(Med) Anonymous IP address	40
(Med) Atypical travel	21
(Med) Unfamiliar sign-in properties	103
(High) Anonymous IP address	4
(High) Password Spray	2
(High) Suspect application consent leading to atypical travel	1
(High) Suspect application consent leading to Unfamiliar sign-in properties	2
(High) Unfamiliar sign-in properties leading to Suspect application consent	1
(High) Unfamiliar sign-in properties	41
Azure Sentinel	
(Low) Rare and potentially high-risk Office operations	27
(Low) Rare subscription-level operations in Azure	25
(Low) Suspicious Resource deployment	11
(Med) Attempts to sign in to disabled accounts	3
(Med) Brute force attack against Azure Portal	2
(Med) Explicit MFA Deny	30
(Med) SharePoint File Operation via devices with previously unseen user agents	30
(Med) Sign-ins from IPs that attempt sign-ins to disabled accounts	18
(Med) Suspect application consent	24
(High) Correlate Unfamiliar sign-in properties and atypical travel alerts	12
(High) Suspect application consent leading to atypical travel	1

(High) Suspect application consent leading to Unfamiliar sign-in properties	2
(High) Unfamiliar sign-in properties leading to Suspect application consent	1