TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Marje Salumets 179898IVSB

ISO 27001 COMPLIANT MANAGEMENT OF MOBILE DEVICES IN A MEDIUM SIZE PRIVATE ENTERPRISE

Bachelor's Thesis

Supervisor: Kaido Kikkas
PhD in Engineering

Alo Press

Expert in the field

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Marje Salumets 179898IVSB

ISO 27001 STANDARDILE VASTAV MOBIILSETE SEADMETE HALDUS KESKMISE SUURUSEGA ERAETTEVÕTTES

Bakalaureusetöö

Juhendaja: Kaido Kikkas

PhD in Engineering

Alo Press

Expert in the field

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Marje Salumets

29.04.2020

Abstract

ISO 27001 compliant Management of Mobile Devices in a Medium Size Private Enterprise

Purpose of this thesis is to offer mobile management solution in terms of BYOD (Bring Your Own Device) to middle size private enterprises. Outcome of this work is ISO compliant implementation guide for medium size private sector company with recommendation how to centrally manage BYOD devices.

On the basis of known risks, the analytical work compares them to ISO requirements. Practical section focuses on top rated products by Gartner and compares their functionality to testing criteria. Test plan was worked out based on information analysis from ISO 27000 materials and from different previous researches, who were handling security risk problems caused by BYOD-s. Goal is to go deeply into UEM and MTD performance and functionality capabilities, impact on mobile devices, analyse how they collect and store user's data, are they easy to use for the administrators and can defend device against different malicious behaviour.

This thesis is written in English and is 76 pages long, including 5 chapters, 3 figures and 7 tables.

Annotatsioon

ISO 27001 standardile vastav mobiilsete seadmete haldus keskmise suurusega eraettevõttes

Käesoleva töö eesmärgiks on pakkuda lahendust mobiilsete seadmete haldamiseks keskmise suurusega eraettevõttes. Seadmeid liigitatakse BYOD (Bring Your Own Device) põhimõtete järgi. Tulemus vastab ISO 27000 nõuetele ja sisaldab soovitusi mobiilsete seadmete haldamiseks ning protseduuri sisseviimiseks.

Praktilise osa ettevalmistuses on arvestatud tuntud riske, mis võivad kaasneda lubades BYOD seadmeid töötegemiseks ja ettevõtte informatsiooni töötlemiseks. Analüüsides riskide vähendamise võimalusi vastavuses ISO raamistikust tulenevatele nõuetele sai koostatud testimiskava, mille käigus uuritakse sügavuti UEM ja MTD suutlikust ja funktsionaalset võimekust, mõju mobiilsetele seadmetele analüüsides, kuidas korjatakse ja salvestatakse andmeid ning hinnatakse kasutusmugavust nii kasutajatele kui ka administraatoritele.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 76 leheküljel, 5 peatükki, 3 joonist, 7 tabelit.

List of abbreviations and terms

API	Application Programming Interface
APP	Application
BT	Bluetooth
BYOD	Bring Your Own Device
COBO	Company Owned/ Business Only
COPE	Company Owned/ Personally Enabled
COSU	Corporate-Owned Single-Use
CPU	Central Processing Unit
CYOD	Choose Your Own Device
E3	Type of software license, released by Microsoft
EDR	Endpoint Detection and Response
EICAR	European Expert Group for IT security
EMM	Enterprise Mobility Management
IDC	International Data Corporation
iOS	Mobile Operating system for Apple products
IS	Information Security
ISKE	IT Baseline Protection Manual
ISMS	Information Security Management System
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
IT	Information Technology
Json	JavaScript Object Notation
LAN	Local Area Network
macOS	Macintosh operating system
MAM	Mobile App Management
MDM	Mobile Device Management
MFA	Multi Factor Authentication
MTD	Mobile Threat Defence
MTM	Mobile Threat Management
MTP	Mobile Threat Protection
NAC	Network Access Control
NIST	National Institute of Standards and Technology
OS	Operating System
OWASP	Open Source Foundation for Application Security
PC	Personal Computer
PCCLM	PC configuration life management
PCMAG	United Kingdom Magazine
PDCA	Plan Do Check Act
RIA	Information System Authority of Estonia
SIEM	Security Information and Event Management
SME	Small Medium Enterprises
Syslog	System Logging Protocol
UEM	Unified Endpoint Management
UWYT	Use What You've Told
VPN	Virtual Private Network
Wi-Fi	Wireless Network
WIPE	Action restores a device to its factory default

Table of contents

List of figures

List of tables

1 Introduction

With the rapid increase of mobile devices has also increased its prevalence in businesses, facing the challenge of mitigating risks posed by these devices within the business network. This trend has increased the need for more detailed and deeper protection of data and mobile devices, wherever they are located. It is hard to find a middle road between high levels of security and user freedom. The final solution might not please all employees, but it will bring more transparency to handling sensitive business information, mitigating risk of data loss, more conscious use of your own device and adds extra layer of security to devices.

Nowadays it is very popular to work from distance or as it is defined in ISO 27000 - teleworking. This gives more freedom for the employee to manage their time efficiently and is considered as benefit, that company can offer to keep staff motivated. Teleworking possibility brings along usage of different mobile devices, that are used from different places which leads us to higher risk of information leakage, data loss or cyber exposure. In some cases, companies provide users with devices for working remotely, that are already preconfigured according to security polices, but in Europe and in Estonia is very popular for employees to use their own devices. This is very convenient for the users although allowing Bring Your Own Device (BYOD) inside the organization enable access to important information and data is a challenge to keep the information safe. One of the best solutions is working out preventive policies inside the company or if don't want to develop the bicycle all over again, then it would be wise to use recommendations from known cyber frameworks like NIST or ISO 27000.

The goal of this thesis is to develop an implementation guide for private businesses, who allow Bring Your Own Devices. These devices are owned by employees but have access to company's sensitive information. In 2016 Daniel A. Arregui, Sean B. Maynard and Atig Ahmand presented a research paper "Mitigating BYOD Information Security Risks", which gives a good overview of risks, that business owners face while allowing BYOD inside their organization. They have categorized risks into 3 main groups: 1) Risks from user behaviour; 2) Exposure of different networks; 3) Remote work and training. Within these groups they have analysed and described the most likely appearance of different risks, that might compromise company's information. To mitigate these risks, we use requirements and suggestions from ISO 27001 and ISO 27002 frameworks. ISO 27000 frameworks are widely used and popular among private sector businesses. They have very simple implementation guides and ISO compliant production, or service gives competitive advantages in markets.

The scope of this thesis is to implement ISO 27000 requirements in a medium size private business. That means at least or more than 50 BYOD devices. To ensure, that every device has latest updates, is covered with basic security requirements and has received all policies, we need to centralize and automate these actions. Therefore, we need to implement software for managing mobile devices. In practical portion of this work we will have a closer look at a few top products rated by Gartner and compare their functionality against requirements from ISO 27001 and keep in mind, the selected solution has to be easily managed. Also compare top products to one widely used software, that is not as highly rated but is suitable for price sensitive companies.

Outcome of this work is ISO compliant implementation guide for medium size private sector company with recommendations on how to centrally manage BYOD devices.

2 Background

The scope of this thesis is to find out the best practices, on how to manage and mitigate risks of BYOD in a medium size private company in Estonia. This section gives an overview and a more detailed explanation, why we look at BYOD devices and exclude all other usage types as well as why we are looking only at private sector businesses and benefits of implementing ISO27000 framework.

2.1 The concept of BYOD

Many IT Managers, who have been dealing with mobile devices in terms of business, know these acronyms – BYOD (Bring Your Own Device), CYOD (Choose Your Own Device) and UWYT (Use What You are Told), which can also be divided in two larger groups like COPE (Company Owned/ Personally Enabled) and COBO (Company Owned/ Business Only) (Wired Insider 2018). Which acronym, with its definition, suits better for your organization depends highly of answers to these three main questions:

1) Device. What is it? Who chooses? Who buys, who pays and who is paying for cellular services?
2) Management and support. Who manages, supports and what are the limits?
3) Integration and Applications: how closely integrated and important is the device with everyday workflows? (Wired Insider 2018)

Since in scope of this thesis UWYT are not significant, we compare only CYOD vs BYOD and explain why we choose BYOD.

“Traditionally, when it comes to mobile devices, the employee received their working tools with the words; Use What You are Told (UWYT). IT support then got a pre-determined list of approved devices which the organization controls and has configured for work purposes. Variation in the list of allowed devices is dependent on the role of the employee, where some roles can get much freedom of choice than others. The role-based list approach is a mix of UWYT and CYOD. When moving from UWYT to CYOD the IT-department leave the choice of device completely to the user, but still purchases and controls the device. In this category, there are some variations between level of private use and control. When the organization lets go even more of the control, they let the employee buy the device by themselves, but with money from the organization, if it will be a private or proprietary device may vary. The final step in device freedom is when the organization is completely left outside of the devices and the employees use their own private devices even at work." (Bordin 2016)

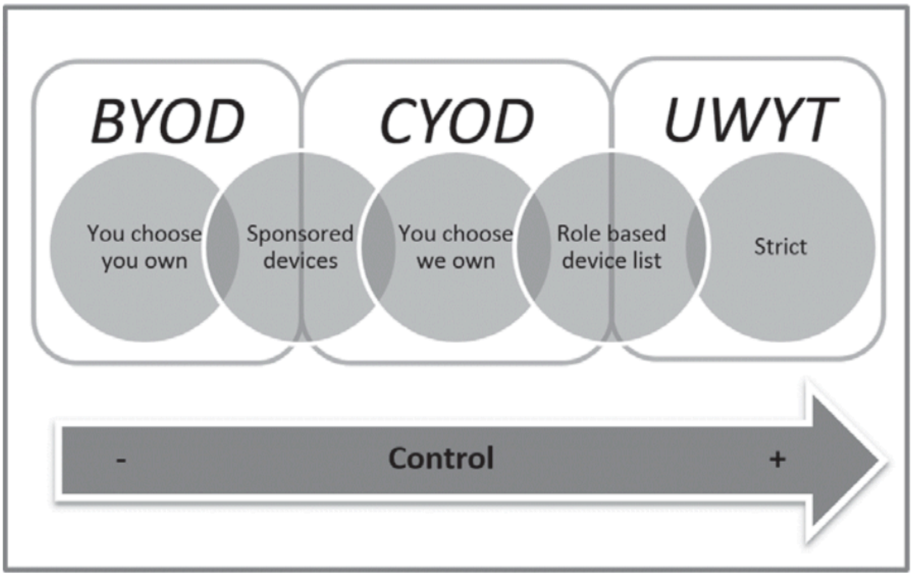


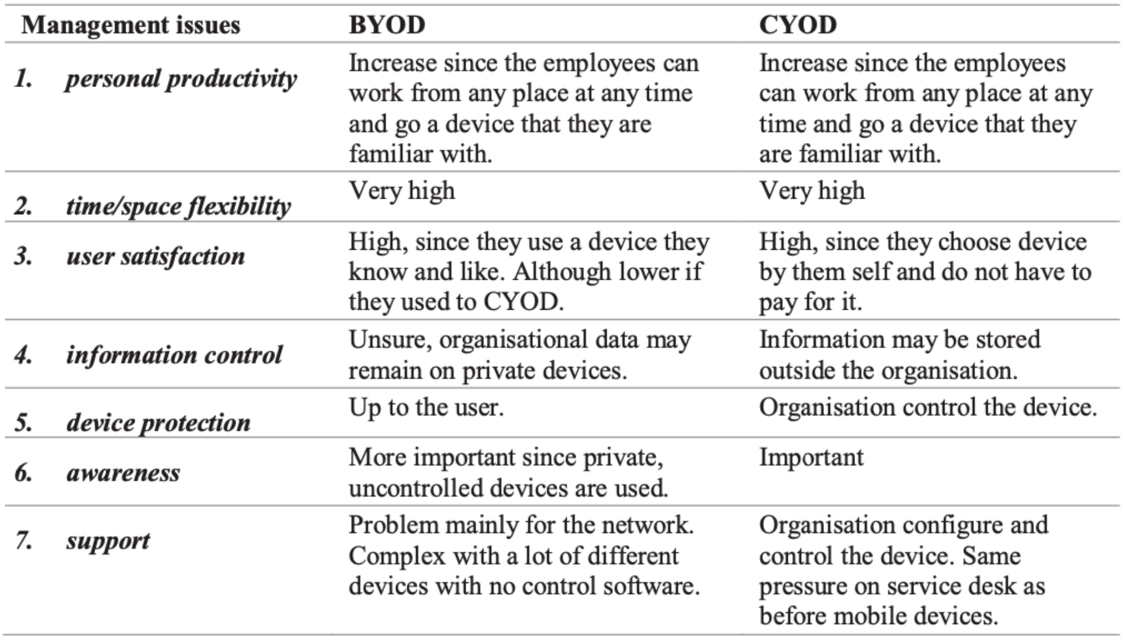
Figure 1. Example of device management strategies (Bordin 2016)

In many ways, BYOD and CYOD are quite similar. The perceived benefits are the same, both solutions provide increased productivity, flexibility, and user satisfaction. (Bordin 2016).

"In both cases users will choose products, that they already know, and which feels comfortable, but from management perspective the differences appear around security aspects. When a device is owned by the organization, they have more control over the device and can apply policies to it. On a privately-owned device, it is up to the user to secure the device and its information. When an employee leaves the organization a CYOD device can be completely erased, but for a BYOD device, it is up to the user to remove all data that belongs to their former employer. If the user allows the employer to use a mobile management tool on their device, the control gap between CYOD and BYOD decreases. Another issue that separates CYOD from BYOD is the possibility of deeper investigation in cases of suspected policy violation. If the device is CYOD the employer can take the device and perform a forensic investigation, if it is BYOD the employer has no right to apprehend the device and cannot carry out the investigation. Furthermore, the workload for the IT-department increases when handling BYOD. With BYOD the user can have more than one device on the network, which requires more network capacity and secondly, more devices require more help from the IT-Support. (Bordin 2016)

In conclusion CYOD are more secure to the company, but costly, since people will probably choose expensive devices. In Europe and also in Estonia BYOD-s are more popular and due to that they are more relevant in our context. (Daniel Alejandro Arregui 2016)

Table 1. Comparison of BYOD and CYOD. (Bordin 2016)



Management issues	BYOD	CYOD
1. personal productivity	Increase since the employees can work from any place at any time and go a device that they are familiar with.	Increase since the employees can work from any place at any time and go a device that they are familiar with.
2. time/space flexibility	Very high	Very high
3. user satisfaction	High, since they use a device they know and like. Although lower if they used to CYOD.	High, since they choose device by them self and do not have to pay for it.
4. information control	Unsure, organisational data may remain on private devices.	Information may be stored outside the organisation.
5. device protection	Up to the user.	Organisation control the device.
6. awareness	More important since private, uncontrolled devices are used.	Important
7. support	Problem mainly for the network. Complex with a lot of different devices with no control software.	Organisation configure and control the device. Same pressure on service desk as before mobile devices.

BYOD are defined very differently, depending of the concept they are used in. In terms of this research we use the definition provided by Gartner (2012) and research work by Arregui, Maynard and Ahmend “Mitigating BYOD Information Security Risks” which states that BYOD can potentially include a large variety of electronic devices including: workstations, mobile communication devices portable storage media (USB memory sticks, memory cards, portable hard drives, floppy disks) and media recorders.
In this research BYOD-s are defined as follows:

- Mobile device or tablet
- The user can do knowledge work with the device.
- It must be owned by the individual and not by the organization.
- The device is portable.
- It is capable of installing third party software applications.
- It can be connected to at least one wireless network interface, a mobile phone network (2G, 3G, 4G), a local area wireless computer network (Wi-Fi) or a personal area network (Bluetooth). (Arregui, D.,2016)

2.2 Small, medium and large companies in Estonia

The European definition of SME (small medium enterprise) follows: "The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro."
(EUR-Lex, Access to European Law)

The Estonian government decided to distinguish between the sizes of business in order grants various benefits. Limited liability companies are categorized into small, medium and large companies in Estonia. Among these, small and medium-sized enterprises, also known as SMEs, will benefit from several incentives offered by the authorities.
(AnsonBaer Nordic OÜ 2020)

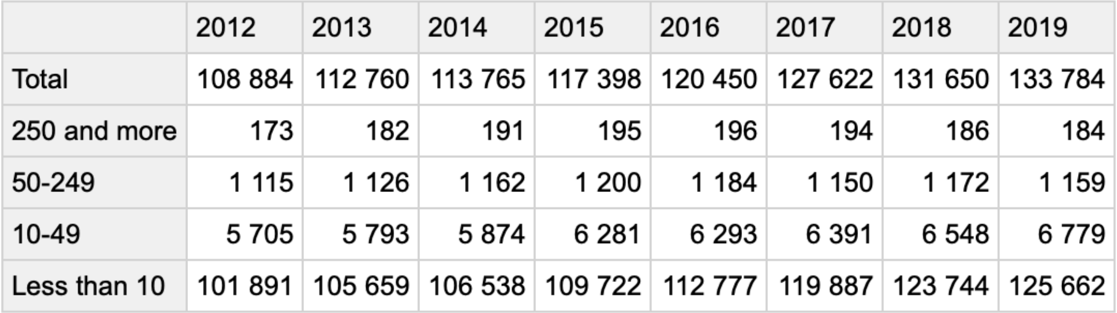
These companies are categorized as:

- micro companies which have assets with a total value of 175,000 euros and an annual income of maximum 50,000 euros;
- small companies which own assets of maximum 4 million euros and annual sales of 8 million euros and an average number of 50 employees
- medium-sized enterprises which have either the value of assets totalling 20 million euros, or 40 million in yearly sales or an average number of 250 workers;
- large companies which enter the same category with medium-sized enterprises, however, they must meet at least two of the three indicators mentioned above.

(AnsonBaer Nordic OÜ 2020)

According to data from Estonia’s Statistics Department, there were 1159 economically active companies registered in 2019.

Table 2. Economically Active Enterprises. (Estonian Statistics Department)



	2012	2013	2014	2015	2016	2017	2018	2019
Total	108 884	112 760	113 765	117 398	120 450	127 622	131 650	133 784
250 and more	173	182	191	195	196	194	186	184
50-249	1 115	1 126	1 162	1 200	1 184	1 150	1 172	1 159
10-49	5 705	5 793	5 874	6 281	6 293	6 391	6 548	6 779
Less than 10	101 891	105 659	106 538	109 722	112 777	119 887	123 744	125 662

In terms of Estonia SME-s play very important roll. According to 2018 statistics, there are about 74% of companies, who are considered as SME and they cover 78% of private sector employment. The minus part is, that SME-s are combination of micro, small and middle size enterprises. In terms of numbers, this means micro and small businesses have only 1-10 and 11-49 employees. Supposedly every employee wants to use only one mobile device for reading business related emails or work with documents. The max number of devices would be 49. This number is quite small. In smaller businesses this is not a problem, because employees are usually working closely, and information exchange is quick. The need for automated management is low to zero. Exceptions are companies, where people travel a lot and therefore the management of devices is difficult or companies, who are working with very sensitive information, for example law offices. Since their field of activity is so different and works policies are not related at all, they need personal approach or tailor-made solutions. For that reason, they fall out of scope of this thesis.

Management software is needed to govern large number of devices at the same time. For example, to push on all mobiles at the same time newest policies and updates. In order for the mobile management platform to work effectively, first is necessary to prepare an elaborated and formed policy for the use of mobile devices.

Perfect company, who finds this thesis useful:
1) has need for mobile management software, that means more than 50 employees;
2) have developed internal policy for mobile device usage;
3) is allowing BYOD;
4) does not have limitation on cloud services;
5) is active only in private sector.

This rises another question- why not large and public sector companies? Public sector has very strict limitations and the scope of the research is to use policy suggestions and implementation guides from ISO 27000 framework family. Also, these organizations have different rules about using outsourced services and usually they are not allowed to use cloud-based platforms. Private sector companies are required to use ISKE cyber security framework. Large enterprises have also strict limitations. Although they could be ISO 27000 compliant, the need for more detailed policies, various alternatives and access to segmented sections of networks leads to a need for tailor-made solutions. These are very expensive, and one solution is not always suitable for all large companies.

2.3 ISO27000 framework and legal issues

Whether a business is relatively small or a huge global corporation, it is vital for them to follow standards to help ensure their business runs smoothly. One of the most common issues a business can face is when it suffers from a lack of information security. Whether it's stolen credit card details, mishandled personal information or even intellectual property, businesses are obliged to protect this sensitive data. To help companies keep their data and information assets secure from threats, it's important to understand security standards such as the ISO 27000 series. (Miller, 2019)

Introduction to ISO27000

Also known as the ISO 27000 Family of Standards, it's a series of information security standards that provide a global framework for information security management practices. They're published and developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission. ISO/IEC 27000:2018 focuses on information technology, security techniques and information security management systems. This particular standard involves an overview and vocabulary used by the ISO27000 series standards and serves as a general introduction to the more common ISO/IEC 27001:2013, also known as ISO 27001. (Jason Miller, BitLyft Cybersecurity, 2019)

Definition of ISO27001

The ISO 27001 standard explains the requirements for an organization's information security management system (ISMS). It enables organizations to prove that they meet regulatory requirements that are related to information security and it demonstrates that the company is committed to protecting sensitive and confidential data. The ISO 27001 standard provides a framework for organizations to use when protecting information. This is often done through the use of different technologies, auditing practices and tests. It also helps to improve staff awareness on ISO 27001 so that internal incidents have a low risk of breaking ISO 27001 standards due to uninformed or untrained staff. (Miller 2019)

ISO 27002 on the other hand is more focused on the individual and provides a code of practice for use by individuals within an organization. In comparison of these two, it is notable that they're structured similarly and that they map to each other. The difference is that the ISO 27001 standard has an organizational focus and details requirements against which an organization's Information Security Management System (ISMS) can be audited. (Kaufman 2014) In this research the scope is limited with only ISO 27001 boundaries.

Teleworking and mobile devices

ISO 27001 defines security measures for mobile devices and describes suggestions for physical devices, but it also states, that mobile devices go under requirements of teleworking.

Teleworking, also known as telecommuting, means working from home or remotely using modern technology and telecommunications to remain in touch with your employer or business. Teleworking allows individuals to work either at home, a local cafe with WiFi, or at a local telework centre for one or more days each week, or full time. (Market Business News 2020)

Teleworking policy includes all portable devices, but we look closer only those, what are required for mobile devices.

Legal issues

Under ISO 27001 Annex A control A.6.2.1, the organization must be able to demonstrate a policy and supporting security controls to reduce the risk posed by mobile or remote devices. As a result of this, it is the organizations responsibility to issue a mobile device policy that should cover the registration/de-registration of mobile devices, physical security requirements, technical security requirements including remote connections, software control, access control and encryption at rest/in-transit. (Alliantist Ltd, 2020)

The mobile device policy should include all of the above topics, stating the businesses requirements for use of mobile devices and when they are appropriate. Company should specify their expectations for topics such as bring your own device (BYOD). BYOD is a hot topic for information security, with many practitioners agreeing that the risks posed by unmanaged, personally owned devices is too great. However, ISO 27001 does not specify whether BYOD is or is not permitted – it simply requires that the organization determines this, issues a policy stating their intentions and monitors compliance with this policy through audit or technical controls. (Alliantist Ltd, 2020)

For example, if the company's policy requires using VPN while reading email, then they have no power to check from BYOD if the user acted accordingly. In cases like this automated management comes in handy giving feedback and more transparency about policy usage. This arises another big problem – how company assures, that they are not collecting info and any personal data from that private device? In Europe there are already many lawsuits, where employees have failed a complaint against their own employer about collecting too much data from their personal devices and have won. That's why it is important to pre agree terms of management platform usage in BYOD-s. Examples and suggestions will be presented in Practical section.

2.4 Mobile Management Software

Mobile Device Management (MDM)

Mobile device management (MDM) includes software that provides the following functions: software distribution, policy management, inventory management, security management, and service management for smartphones and media tablets. MDM functionality is similar to that of PC configuration life cycle management (PCCLM) tools; however, mobile-platform-specific requirements are often part of MDM suites. (Definition by Gartner)

Unified endpoint management (UEM)

Unified endpoint management (UEM) is an approach to securing and controlling desktop computers, laptops, smartphones and tablets in a connected, cohesive manner from a single console. Unified endpoint management typically relies on the mobile management (MDM) application program interfaces (APIs) in desktop and mobile operating systems. (Margaret Rouse 2016)

Mobile Threat Defence (MTD)

When technologies are new, it can take a while before everyone agrees on the same language. Mobile security has gone by many names – Gartner goes for Mobile Threat Defence (MTD), IDC calls it Mobile Threat Management (MTM) while others prefer Mobile Threat Prevention (MTP). Regardless of the exact terminology, these solutions are all concerned with the same thing doing the same thing: securing mobile devices. (Robin Gray, 2018)
In scope of current thesis our MTD products are Lookout, Sophos Mobile, SandBlast.

Future

Future looks bright for the UEM software platforms. Unified Endpoint Management (UEM) which allows the businesses to manage all the endpoints like laptops, mobiles, tablets, PCs, printers and wearables using a single extensive EMM solution.
EMM (enterprise mobility management) is nothing more than the combination of an MDM and MAM (mobile application management) solutions equipped with a secure container that keeps business data secure. An EMM solution in addition to MDM offers Mobile App Management, Mobile Content Management, App Wrapping and Containerization. EMM is a complete package of services which offers complete data security on BYOD and Dedicated Devices (formerly called COSU or Corporate-Owned Single-Use) for enterprises. (April 25,2017, 42gears.com)

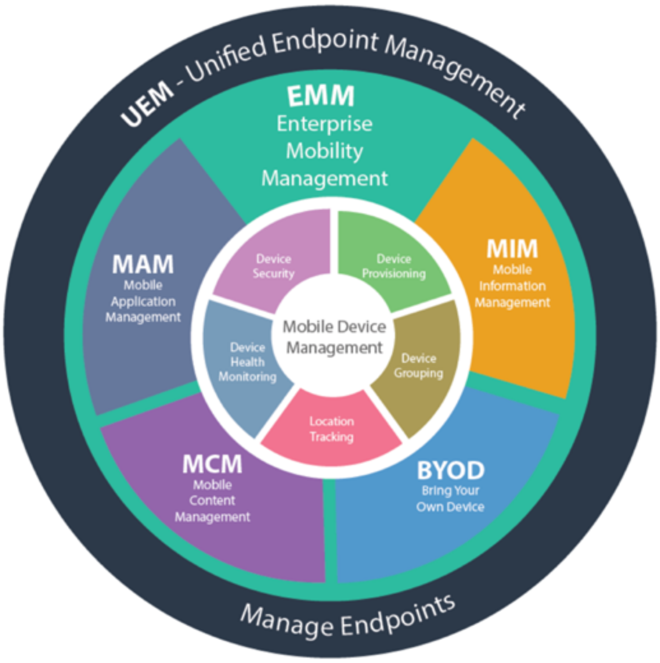


Figure 2. Different Management types. 42gears.com

But what is the result of taking an approach that unites all of your devices? According to Tess Hanna (Best Practices, 24 March 2019) the top three reasons to use UEM in order to figure out why it's a method worth considering.

1. **Improved security.** When using a UEM solution, you have the ability to manage security across devices, rather than the security of mobile devices or desktops separately. These devices are all connected to the organization's backend data, and were most likely deployed at different times, with disparate management systems. At an organization with hundreds of workers, each employee would also have two or three devices, which is overwhelming for the IT department to oversee. Not only that, but the number of endpoints in this situation increases the risk of threats. However, when using UEM, all of those devices across different systems are managed under one security protocol. This is a way to maintain consistency across devices, as well as reduce the overall amount of maintenance your IT team has to perform. With UEM, IT admins have the ability to implement the same set of processes across all devices.

2. **Cost effective.** UEM benefits organizations financially by reducing the number of systems that are licensed or sought each year. In addition to this, replacing multiple existing management solutions for on- and offline equipment with a single solution reduces costs. As well as this, the fact that UEM decreases the cost of management translates to increased administrator productivity and timesaving. Finally, with enhanced and improved security, it is less likely that an organization will suffer a financial loss as a result of a cyber-attack or data breach.

3. **A More Cohesive User Experience.** When IT teams handle managing Bring Your Own Device (BYOD) and Corporate Owned Personally Enabled (COPE) policies, they have to be concerned with the users' reaction to how their different devices will be managed. However, with a UEM solution, the user experience across all levels of the business will be consistent.

Consistency, security, and cost reduction create a solution that is appealing to both businesses and their employees, which is powerful in a market setting. (Tess Hanna (Best Practices, 24 March 2019)

Intune, Workspace ONE, Sophos versus Lookout and CheckPoint SandBlast

Names mentioned in title will not say a lot about their character. According to Gartner, most known and rulers of the software market have been for many years Intune and Workspace One. According to research done by PCMAG in 2017, they predicted top places in leader boards, and they didn't get it wrong. Workspace One and Intune are also known products in Estonian market. Their market advantage is, that they offer full management of different software platforms, for example – Android, macOS, iOS and also different Windows operation systems. Intune and Workspace ONE are defined as UEM (unified endpoint management). UEM-s are good tools for medium size companies because of their ability to manage different OS (operation system) platforms. It is very convenient to manage all devices from one place, UEM combines different functionalities of MDM, MAM and EMM, also being the economical choice. It is cheaper to choose only one software instead of using multiple from multiple vendors. Downside is that UEMs don’t offer you the same granularity as different combinations of MDM-s and MAM-s etc., but in terms of medium size company you don’t need it. MDM and UEM are offering only central management solutions, but they don’t protect devices against malicious organized attacks or malware. Sophos is not highly rated by Gartner, but it offers full mobile protection services, that combines endpoint protection and management. Sophos is defined as UEM, meaning, that it has ability to manage different OS-s. Comparing to Intune and Workspace ONE, Sophos is not that powerful tool, but offers more cheaper alternative for smaller or price sensitive companies.

If the choice is to use Intune or Workspace ONE, then for preventing malicious attacks, impact of phishing campaigns or checking reputations of installed third party software, there is need to use services from Mobile Threat Defence products like Lookout or Sandblast. According to Gartner, these two are top leaders, who offer protection for mobile devices.

In this thesis the focus is on mobile devices and therefore MDM solution could also satisfy the management question, but since the future is in hands of UEM and in some point the policies should be extended to other devices, that are used for remote work, then for medium size would be more cost worthy to choose out the quality UEM product. The combination of UEM and MTD keeps devices monitored and protected 24/7 making life easier for the information security specialist

Intune

In 2017 a technical journalist Prajwal Desai released an article about Microsoft Intune. This article gives a short, but very accurate definition, what Intune is.

“Microsoft Intune is a cloud-based service that lets you manage mobile devices, PCs, and apps. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure. Microsoft Intune solves the network connectivity problem by delivering a reliable and secure service from the Internet, meaning that every user can access it no matter where they are physically located. The good part is Microsoft Intune provides the subscription service with a low cost per user per month. We can start with a single user, then add and remove users as required by our business needs.” („Microsoft Intune overview and its features “Prajwal Desai 2017)

Workspace ONE

VM Ware is one of the know developer, who offers different products for managing Information Technology Assets. Workspace ONE is VM ware's workspace solution. It's a digital workspace platform that delivers and manages any app on any device by integrating access control, application management and multi-platform endpoint management. Workspace ONE is built on the unified endpoint management (Workspace ONE UEM, formerly known as AirWatch) technology and integrates with virtual application delivery (VM ware Horizon) on a common identity framework. The platform enables IT to deliver a digital workspace that includes the devices and apps of the business's choice, without sacrificing the security and control that IT professionals need. (VM Ware documentary, 2020)

Sophos Mobile

Sophos Mobile is a Unified Endpoint Management (UEM) and Mobile Threat Defence (MTD) solution that helps businesses spend less time and effort to manage and secure traditional and mobile endpoints. The only UEM solution that integrates natively with a leading next-gen endpoint security platform, Sophos Mobile manages and secures iOS, Android, Chrome OS, Windows 10 and macOS devices.

Manage and secure corporate-owned or personal Windows 10, macOS, and mobile endpoints in one system to ensure a simpler management strategy, ensuring uniform company security policies and secure access to company assets. For maximum productivity, organizations where BYOD is embraced can apply consistent policies regardless of device type or ownership. And, because everything we do at Sophos is about security, Sophos Mobile will keep business data, users, and their mobile devices protected and secure. (Sophos Mobile documentary, Sophos Ltd 2020)

Lookout

As the leader in mobile security, Lookout continues to innovate and define the market with a platform enabling rapid deployment of advanced protections for millions of users worldwide.

A highly scalable cloud- and mobile-first platform, only the Lookout Security Platform provides a privacy-centric approach that continuously protects users and enterprise data from the latest phishing, application, device, and network threats.

The Lookout Security Platform offers the flexibility of easy-to-use modules for mobile protection, detection, visibility, analysis, response and remediation. (Lookout product overview 2020)

CheckPoint SandBlast

Check Point SandBlast Zero-Day Protection is an innovative solution that stops unknown malware, zero-day and targeted attacks from infiltrating networks. The SandBlast solution is based on new CPU-level exploit detection technology to identify threats earlier, before malware has an opportunity to deploy evasion code. With its unique inspection capabilities, SandBlast delivers the highest catch rate for threats, and cannot be bypassed using evasion techniques.

SandBlast also includes the Threat Extraction capability, allowing practical protection by proactively reconstructing content into safe documents, preventing malware from ever reaching users. With traditional sandboxing products, customers had to make a choice to either delay delivery of files until inspection was complete, or to run in a detection only mode, letting content through while testing was done in parallel. Threat Extraction makes real-world deployment in prevent mode possible by promptly delivering a clean copy of content, and then only delivering the original once it is deemed safe. (2020 Check Point Software Technologies Ltd.)

3 Problem description and theoretical analysis

3.1 Problem description

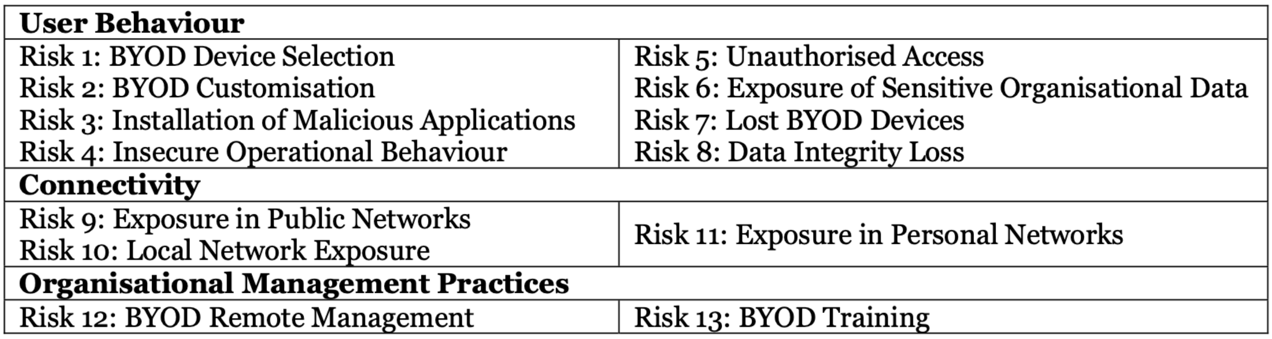
With the rapid increase of mobile devices has also increased its prevalence in businesses, facing the challenge of mitigating risks posed by these devices within the business network. This trend is increased the need for more detailed and deeper protection of data and mobile devices, wherever they are located. For example OWASP has generated top 10 security threats to mobile devices: 1) Improper platform usage; 2) Insecure data storage; 3) insecure communication (http vs https); 4) Insecure authentication; 5) insufficient cryptography; 6) insecure apps, poor code quality (buffer overflow possible); 7) code tampering; 8) hidden backdoors; 9) reverse engineering, binary codes; 10) malware. This sums up most known threats to mobile devices regardless they are fully managed, and company owned or privately-owned devices. Allowing BYODs access company owned information arises the risk of information exposure and data loss. Organizations need effective ways to preserve confidentiality, integrity and availability of sensitive information accessed or manipulated with the rise of personal devices. (Ahmad et al. 2006)

Cappelli et al. (2012) remark that information security incidents can be triggered by former employees, contractors, suppliers and business partners, who may have access to sensitive organizational information using personal devices. Information leakage may cause substantial damage to the organization, including financial loss, operational disruption, damage to the organization reputation and damage to the client's image (Ahmad et al. 2014)

In their research "Mitigating BYOD Information Security Risks" David Arregui and Sean Maynard have analysed and evaluated BYOD information security risks. Comparing their work to OWASP list shows, that their approach is more detailed and gives better picture about different risks.

Table 3 summarizes thirteen BYOD risks from the literature that are associated with allowing BYOD into organizations. Additionally, to identify the most significant risks, they have been grouped into three common areas related to BYOD usage: User behaviour, Connectivity risks, Organizational management practices. (Arregui & Maynard 2016)

Table 3. Synthesis of risks associated with allowing BYOD into the organization. (Arregui & Maynard 2016)



User Behaviour	
Risk 1: BYOD Device Selection	Risk 5: Unauthorised Access
Risk 2: BYOD Customisation	Risk 6: Exposure of Sensitive Organisational Data
Risk 3: Installation of Malicious Applications	Risk 7: Lost BYOD Devices
Risk 4: Insecure Operational Behaviour	Risk 8: Data Integrity Loss
Connectivity	
Risk 9: Exposure in Public Networks Risk 10: Local Network Exposure	Risk 11: Exposure in Personal Networks
Organisational Management Practices	
Risk 12: BYOD Remote Management	Risk 13: BYOD Training

3.2 Theoretical analysis

Based on the risk mitigation theory developed by Arregui and Maynard, that concentrates on finding out risk, that may impact your organization, causing information breach or data loss, we describe in more detail what these risks are and how organization may be affected. In their work, they have identified 13 risks, divided into 3 major categories, that are specifically related to BYOD or mobile devices. The list covers all risks, that may occur due to the absence or insufficient implementation of security policies, level of restrictions and information security knowledge or ignorance of user. Arregui and Maynard worked thru nearly 120 articles to determine the significance and relevance of these risks in today's business environment. These risks are briefly described and at the end of each description there is a recommendation on how to reduce or eliminate this risk. As these are direct conclusions from the research of Arregui and Maynard, they are presented here unchanged.

User Behaviour Risks

Majority of risks evaluated by Arregui and Maynard are caused by users and their behaviour.

1. BYOD Device Selection

- Users choice of device - Users can choose from many mobile device platforms (eg. Apple’s iOS, Android, and Windows Mobile).
- Operating system- Each platform has a unique security model, with strengths and weaknesses to counter security incidents. To illustrate this, Android’s open structure is customizable by the user which makes it more susceptible to attacks than other mobile systems. Whereas, Apple’s iOS security prevents the use of mobile device management (MDM) because of security restrictions in the operating system

Organizations need to evaluate the security risks for each BYOD platform before initiating a BYOD program. They should define the benefits and disadvantages of particular platforms and establish strategies to counter security incidents that may arise. This information should be conveyed to users. (Arregui & Maynard 2016)

2. BYOD Customization

- Disable vendors restrictions - "Jailbreaking", "root", and “unlock” are three popular procedures that users may execute on personal devices to remove vendors’ configuration restrictions,
- Third-party software - Enables users to install third-party applications unavailable on official vendor stores or unlock carrier-locked devices
- Admin rights - Insecure applications on jailbroken devices run with administrator privileges with considerable control over device sensors and applications

Subsequently, it is critical for organizations to define whether or not the use of "jailbreaking" or "root" devices is permitted as a BYOD. (Arregui & Maynard 2016)

3. Installation of malicious Applications

- Phone customization privileges - Users customise their devices according to their preferences and needs, using application markets, like Apple Store and Google Play, to browse and install applications.
- Granted permission for apps - During installation process users grant permissions, like allowing push notifications or location-based services, putting aside security considerations because of the benefits that will be received. For example, a free game application will be installed on the same device as a highly trusted banking application.
- User are not aware of malicious apps - Users are unable to recognise which applications have malicious functionality. The free application may be a malicious one that can sniff, modify, or steal inter-application messages and, therefore, compromise organisational information security Those applications affect the information security of the organisation, generate problems for data privacy, and affect organisations and customers' reputations. (Ketel and Shumate 2015)

It is critical for organisations to control which applications can be installed on BYOD in order to protect the information security of the organisation. (Arregui & Maynard 2016)

4. Insecure operational behaviour

- Users insecure behaviour - While using BYODs allowing viruses and other malware infections to proliferate; exposing the organisation to information security incidents.
- Malware - Is software created to disrupt the normal operation of other software, gather personal information, or access personal computer devices. In the same way that it impacts personal computers, malware is affecting mobile devices.

Organisations must encourage the installation of anti-virus software on BYODs in order to prevent the proliferation of malware infection from BYODs. (Arregui & Maynard 2016)

5. Unauthorized Access

- Unauthorized access - How users handle BYODs may allow unauthorised access to organisation information by third parties, exposing organisations to information security incidents
- Family sharing - According to a survey by Botdefender, 30% of BYOD users share their personal devices with relatives and friends, 40% do not have a save screen mechanism, and only 9% employ a biometric authentication mechanism to secure access to the device (Donovan 2014).
- Awareness of security risk - BYOD users do not realise the security risks that may arise from unauthorised access to their devices by third parties.

Cappelli et al. (2012) suggest that the use of password-protected screen savers, along with good password practices (enforcing password robustness, changing passwords periodically etc.) is essential to decrease information security incidents. This reduces the likelihood of unauthorised users' accessing sensitive information storage on devices and use of organisation applications. (Arregui & Maynard 2016)

6. Exposure of sensitive organizational data

- Exposure - BYOD provides not only a wider range of endpoints where the employees can access organisational resources, but also allows distribution of sensitive information without authorisation, exposing data confidentiality.
- Data control - Once data is on a mobile device, control is difficult
- Sensitive information - Such as customer data, is generally restricted to a few users in the organisation, however, with personal devices, that information can be easily copied
- Unintentional information exposure - Employees sometimes intentionally bypass organisational security, when they need an electronic enterprise resource to complete a task. This action is considered to be non- malicious misuse of organisational resources. For these reasons, organisations should establish the services and electronic resources that are allowed to access mobile devices

The organisation must consider the BYOD risks and determine the services and application that will be accessible from personal devices such as e-mail, calendars, contacts and electronic documents. (Arregui & Maynard 2016)

7. Lost BYOD devices

- Lost device - The device could be lost or stolen. Theft and loss of mobile devices exposes the confidentiality of organisational information (e.g. emails, business documents and financial information), in addition to personal information.

Ketel and Shumate (2015) suggest that organisations need to implement technology tools able to remotely wipe or lock devices to protect sensitive organisational information. (Arregui & Maynard 2016)

8. Data Integrity Loss

- Erase or editing - In the normal operation of personal devices, users may accidentally modify or eliminate sensitive organisational information (Dong et al. 2015; Miller et al. 2012). As users employ BYOD for both personal and business purposes, both environments need to coexist harmoniously in the same device without adversely affecting each other (Wang et al. 2014).

Therefore, the security procedures to prevent the accidental modification or elimination of sensitive organisational information are required. For instance: to prohibit downloading of organisational information into personal devices; backing up and performing changes of control of documents; or using a virtualisation technique to separate organisational space from personal space in personal devices. (Arregui & Maynard 2016)

BYOD Risks from Connectivity Procedures

9. Exposure in public networks

- Public networks - Employees want to remain connected with organisational electronic resources with their BYOD devices even outside the organisation. Example: public networks, such as Wi-Fi hotspots, which are usually free and are common in public places such as restaurants and airports making them extremely attractive. Wi-Fi hotspots are susceptible to a man-in-the-middle attacks and eavesdropping, causing compromises in the integrity and confidentiality of information.

Organisations can mitigate this risk by connecting through public networks employing encryption of the communication with a virtual private network (VPN) (Ketel and Shumate 2015). (Arregui & Maynard 2016)

10. Local Network exposure

- Allowing BYOD in LAN - When an employee bypasses BYOD security controls through connecting to a local area network inside an organisation, internal attacks are difficult to prevent since they occur in the local area network (LAN) of the organisation using a valid user profile.
- Access control - Mobile devices and devices that do not meet the security conditions should be denied access. Antivirus software, mobile operating systems, and security configuration settings - consider while granting access to their internal network.

Moreover, Verizon's study suggests that organisations not only need to control employee-owned device access, but also review their users' privileges to access sensitive data with their devices. (Arregui & Maynard 2016)

11. Exposure in personal networks

- Unprotected home networks - The information security of the organisation could be exposed when BYOD users connect their devices to a personal area network.
- Bluetooth - The most popular personal area network is one employing Bluetooth Technology (BT). BT device may be a threat not only to the user, but to the organisation as Bluetooth attacks can introduce security vulnerabilities into the business. These include eavesdropping, message modification and resource misappropriation.

Podhradsky et al. (2012) suggest that the following security procedures may be adopted to reduce the likelihood of a Bluetooth incident: disable BT functionality if it is not used, change default device names, do not use the owner's name as part of the device name, and change default pairing passkeys. (Arregui & Maynard 2016)

BYOD risks from Organizational Management

12. BYOD Remote Management

- Device monitoring- Establish BYOD policies, and also need to ensure that employee-owned devices comply with these policies. Challenge for organisations is to manage remotely both a large quantity and numerous models of personal devices.
- Mobile Device Management (MDM) - Is a primary information security tool for organisations to manage employee-owned devices. MDM permits organisations to monitor, manage, secure, and apply security policies on employee-owned mobile devices.
- Network Access Control (NAC) - Controls the users that are allowed to access what sort of data.

Employing MDM and NAC allows the following functionality: device enrolment into the network (e.g. connection, device registration, user), device operation (e.g. profile configuration, certificates, accounts) and monitoring (e.g. policies, alerts, rules). (Arregui & Maynard 2016)

13. BYOD Training

- Low awareness of cyber security threats - Users, without appropriate information security knowledge, may perform insecure behaviour and social learning may contribute to this insecure behaviour.
- Training - Organisations provide information security training sessions to their employees. Employees must know exactly what the organisation expects from them while they are working with their devices.

The guidelines must include: safe device operation (e.g. establish lock codes or passcodes, avoid lending the device to third parties); networks allowed to access (e.g. hotspots are prohibited, a VPN connection needs to be established); measures to store organisational information (e.g. information must be encrypted, do not upload information to the cloud); and protocols to follow in case the device is lost or stolen (e.g. report immediately to the organisation). (Arregui & Maynard 2016)

3.3 Mitigating BYOD risks

Arregui and Maynard's risks description and assessment has given great overview, what are organization facing in term of BYOD. According to their theory and suggested solutions we can start to work out action plan for risk mitigation. In some points they have been too strict. Since employees are using their private devices, organization have to keep that in mind and to ensure, that they don't manage or collect information from parts of the mobile devices, that is not consisting organization information. In terms of legal issues and privacy it is always best approach to allow more then to restrict. Restricting freedom to use private device may lead to serious legal arguments and its always the company's problem to prove, that they have not collected more information than its needed for information protection.

Arregui and Maynard have divided risk into three groups – User Behaviour, Connectivity and Organizational management practices. This is also a great hint where to start creating your own action plan and keep the same order. It is very important to collect as much info in preplanning stadium and then move on to risk management due to user's behaviour. Notice, that in network exposure part there is VPN requirement. Definition by Cisco - VPN is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

Before we can conduct VPN connectivity and profiles it is very important to be aware if all devices, that are planning to use it and evaluate the status of devices (devices have to be known, clean of malware and know OS type and applications) and users knowledge how to use VPN and what might be the consequences of misuse. We cannot allow unknown and unauthorized devices to inside network.
In the third part - Organizational management practices- the focus is more on how to implement preconfigured security polices and how to maintain the pre-agreed level of security. For better overview and easier management, it is highly recommended to use some central management platform and for keeping the level of cyber hygiene high, then constant and ongoing education plan for users is a must.

The outcome of Arregui and Maynard's research is presented below has table. In their paper the solutions for handling the risks are more descripted, but in our table, it is shown in action, what needs to be done to eliminate or reduce this risk. Later on, we can compare this action plan to ISO27000 requirements and from there we get full list of policies we need to implement to get ISO certified, but keep in mind to keep it simple to maintain user's freedom of using their devices. Also, we can start testing our chosen MDM and UEM platforms, are they capable of handling and maintaining these requirements or not.

Table 4. BYOD risks and solutions proposals

Numb	Risk type	Solutions
1	BYOD Device Selection	Plan your work; Evaluate current state of BYOD; Detect OS platform; Evaluate benefits and disadvantages of different OS platforms; Be prepared to answer users' questions; Develop strategy to counter security incident; Communicate this info to users;
2	BYOD Customization	Define the use of "jailbreaking" or "root" devices is permitted as a BYOD;
3	Installation of malicious Applications	Applications - control, evaluation good or bad, prevent malicious;
4	Insecure operational behaviour	Installation of anti-virus software on BYODs in order to prevent the proliferation of malware infection from BYODs.
5	Unauthorized Access	Password-policy: combination, numbers, biometrical; Change password periodically; Info storage and third-party Access;
6	Exposure of sensitive organizational data	Accessible from personal devices such as e-mail, calendars, contacts and electronic documents.
7	Lost BYOD devices	Implement technology tools able to remotely wipe or lock devices.
8	Data Integrity Loss	To prohibit downloading of organisational information into personal devices; Backing up and performing changes of control of documents or using a virtualisation technique to separate

		organisational space from personal space in personal devices;
9	Exposure in public networks	Organisations can mitigate this risk by connecting through public networks employing encryption of the communication with a virtual private network (VPN)
10	Local Network exposure	Access Control – know your devices, keep them secure, know; who is using your Network; review user privileges;
11	Exposure in personal networks	reduce the likelihood of a Bluetooth incident: disable BT functionality if it is not used, change default device names, do not use the owner's name as part of the device name, and change default pairing passkeys.
12	BYOD Remote Management	Employing MDM and NAC allows the following functionality: device enrolment into the network (e.g. connection, device registration, user), device operation (e.g. profile configuration, certificates, accounts) and monitoring (e.g. policies, alerts, rules).
13	BYOD Training	The guidelines must include: safe device operation (e.g. establish lock codes or passcodes, avoid lending the device to third parties); networks allowed to access (e.g. hotspots are prohibited, a VPN connection needs to be established); measures to store organisational information (e.g encrypted information, do not upload information to the cloud); and protocols to follow in case the device is lost or stolen (e.g. report immediately to the organisation).

3.4 Mobile device protection requirements from ISO27001 standard

ISO27001 standard is suitable for middle sized companies, because it defines very clearly, what needs to be done, by who, what way and how to monitor it. Many companies prefer it to our local standard ISKE, because it’s not that granular and leaves more opportunities to do things “their own way”. ISO27001 states that implementing their system specifies the requirements for establishing, implementing, maintaining and continually improving and information security management system within context of the organization.
Mobile protection in ISO is divided into parts: 1) physical device and its protection 2) Teleworking (working remotely, flexible work, virtual working)

Mobile device policy

- Registration of mobile devices
- Requirement for physical protection
- Restrictions of software installation
- Restriction of connection to information services
- Access controls
- Description of the problem
- Cryptographic techniques
- Malware protection
- Remote disabling, erasure or lockout
- Backups
- Usage of webservices and web apps

Care should be taken if using devices in public areas, meeting rooms and other unprotected areas. Avoid unauthorized access – cryptographic techniques (MFA, token), enforces secret authentication – passwords. Mobile device should also be physically protected, in case of losing it or against directed attacks. When used also for private purposes, then should separate business related apps from private and accessing business related information only if user is authorized to see it. Train personnel to acknowledge threats to use public Wi-Fi networks and overall information exposure in other networks.

Teleworking

Through this policy, an organization can establish the rules for the implementation of safeguards to protect information accessed, processed, or stored outside the organization, such as:

- who may telework (e.g., IT staff, sellers, managers on travel, etc.)
- which services are available for teleworkers (e.g., development environment, invoicing systems, etc.)
- which information can be accessed through telework (e.g., performance dashboards, list of customers, etc.);
- Which access controls shall be applied before access to information and resources is granted (e.g., password, two-factor authentication, use of VPN on communication channels, etc.);
- How devices and remote sites should be configured, protected, and used (e.g., devices with cryptography, no use of shared rooms to work, information backup, etc.)
- Can private devices access remotely, in what terms?
- Virus protection and firewall requirements

It’s important to remember that while the ISO 27000 series of standards is already well-defined, it’s a constantly evolving standard that will continue to be updated as new technologies and threats appear. By adopting these new standards and always ensuring that you’re up to date with ISO 27000 regardless of your chosen industry, you’ll always be able to protect your organization’s most sensitive data and build trust with both employees and customers. (Miller 2019)

In following chapters, we will conduct analysis and practical testing, on how different management platforms are handle all of these requirements.

4 Practical analysis

Previous chapters show analysed work about areas, that need to protection, risk assessment and also introduction about the possible solutions. In practical section should give answers, how we going to find the result. The goal of this research is to find out which UEM vendors offer most convenient software for managing BYOD-s and mitigating risk of information security breaches. The final solution should give overview of UEM platform, that does not overload device, does not collect private information outside the scope of organizational information, is easy to use and is not the most expensive offer in the market. Goal is not to find the cheapest vendors, because nowadays organization evaluate their information very highly and therefore it is important to keep your focus on quality and well know reputation. Since UEM-s alone cannot provide the protections level of mobile devices, that is required by ISO27001, then there is need to implement protection against malicious activities. Products chosen to test scope are the market leading vendors.

4.1 Methodology

Purpose of the practical research is to test out mobile management possibilities and see if they meet ISO 27001 requirements. There are a lot of vendors, who offer similar service. To narrow the scope focus was set on only highly ranked ones. Gartner is advisory and research company, who collect data and creates statistical data about different products. They have ranked all MDM and UEM and gathered users' feedback. For this research only the top leaders were chosen, who have been in top 3 at least 3 years in a row. Testing criteria was worked out based on information analysis from ISO 27000 materials and from different previous researches, who were handling security risk problems caused by BYOD-s. To find out, how UEM work on private mobile devices, an experiment was performed. Test group was combined by 7 different mobile phones with different operating systems. The choice was done by popularity in Estonia. This thesis will build a case study of well-known UEM vendors in combination with MTD. UEM-s are not capable to full fill all ISO requirements and cannot help mitigating risks, that are related to malicious behaviour or attacks. Therefore, we need to combine them with protective software, like MTD, that can prevent impact of phishing attack, remove malware infections and predict zero-day attacks. It is important to test how UEM-s and protective software can work together in one device. According to test plan the goal is to go deeply into UEM and MTD performance and functionality capabilities, impact on mobile devices, analyse how they collect and store user's data, are they easy to use for the administrators and can defend device against different malicious behaviour.

4.2 Theoretical input

From research done by Arregui and Maynard an action list can be generated to present consistency with ISO27001. Solution we are looking has to mitigate known risks, light weight to mobile devices, almost seamless for the user and easily manageable for IT staff. Let's compare this list to requirements from ISO framework.

Table 5. 13 known risks vs ISO requirements

No	Risk mitigation action list	ISO requirements
1.	Plan your work; Evaluate current state of BYOD; Detect OS platform; Evaluate benefits and disadvantages of different OS platforms; Be prepared to answer user questions; Develop strategy to counter security incident; Communicate this info to users;	Registration of mobile devices; Description of the problem
2.	Define the use of "jailbreaking" or "root" devices is permitted as a BYOD;	Restrictions of software installation
3.	Applications - control, evaluation good or bad, prevent malicious;	Requirement for physical protection

4.	Installation of anti-virus software on BYODs in order to prevent the proliferation of malware infection from BYODs.	Malware protection
5.	Password-policy: combination, numbers, biometrical; Change password periodically; Info storage and third party Access;	Access controls
6.	Accessible from personal devices such as e-mail, calendars, contacts and electronic documents.	Restriction of connection to information services
7.	Implement technology tools able to remotely wipe or lock devices.	Remote disabling, erasure or lockout
8.	To prohibit downloading of organisational information into personal devices; Backing up and performing changes of control of documents or using a virtualisation technique to separate organisational space from personal space in personal devices;	Cryptographic techniques
9.	Organisations can mitigate this risk by connecting through public networks employing encryption of the communication with a virtual private network (VPN)	Usage of webservices and web apps
10.	Access Control – know your devices, keep them secure, know; who is using your Network; review user privileges;	Access controls Backups
11.	reduce the likelihood of a Bluetooth incident: disable BT functionality if it is not used, change default device names, do not use the owner’s name as part of the device name, and change default pairing passkeys. default device names, do not use	Malware protection

	the owner’s name as part of the device name, and change default pairing passkeys.	
12.	Employing MDM and NAC allows the following functionality: device enrolment into the network (e.g. connection, device registration, user), device operation (e.g. profile configuration, certificates, accounts) and monitoring (e.g. policies, alerts, rules).	Registration of mobile devices;
13.	The guidelines must include: safe device operation (e.g. establish lock codes or passcodes, avoid lending the device to third parties); networks allowed to access (e.g. hotspots are prohibited, a VPN connection needs to be established); measures to store organisational information (e.g. information must be encrypted, do not upload information to the cloud); and protocols to follow in case the device is lost or stolen (e.g. report immediately to the organisation).	Continuous training Cyber Hygiene

In terms of BYOD it would be reasonable to keep the selected solution light and simple as possible, because if it’s very complicated and somehow overloading the device performance, then users simply don’t want to use it. Since its their private device, then organization are not able to force them as well. Then there would be two outcomes – 1) organization have to provide mobile devices themselves and take full control of them or 2) users are not allowed to read email or any organization related information from their mobile devices. Both options are not acceptable. Additional expenses for providing new phones are not satisfiable nor is access restriction for users. In company’s interest are, that user keep their freedom to move around and still be in contact with work related information. Quick change of information is one of the key factors of running successful business. The goal is not restricting user’s freedom in their own devices, but to offer secure solution, enable distance working and find a solution, that both parties can benefit. Keywords are well organized planning, user and device friendly, minimum restrictions and requirements, private info remains private, ISO complaint.

BYOD Policy

Table 6. ISO compliant policy for BYOD-s

Devices	1) List of devices 2) Device OS and version 3) Admin or root rights, jailbroken or not
Physical protection and access	3) If possible, MFA 4) At least 6 figure passcode 5) Password for applications, where are signed in with company's account or security container for those applications. Periodic change required
Restrictions of software installation	6) Allow downloads only for devices, that are registered into know devices list 7) Other downloads are not restricted *
Restriction of connection to information services	8) allow inside network only known BYOD-s by the known device list 9) allow VPN possibility 10) not to restrict public WIFI access* 11) train personnel to understand security risk of public networks and how to protect themselves
Remote disabling, erasure or lockout	12) If password for applications is entered 5 times incorrectly, then WIPE 13) If password for security container is entered incorrectly 5 times, then WIPE 14) If device is lost or stolen, then WIPE

Cryptographic techniques	15) If device gets in to third hands or gets stolen, then cryptographic measures have to keep information secure – secure password, cannot make a copy, cannot read information from external device
Malware protection	16) Virus protection is mandatory
Backups	17) Backups from BYOD are not allowed* 18) For users it's not allowed to keep copies or backup information outside applications allowed by organization or in other private devices, that are not listed in known device list
Usage of webservices and web apps	18) Web Apps and services in internal LAN are only reachable if VPN connection is up

* Organization accept the risks and consequences for user convenience

It is not possible to activate BYOD policy for all devices at once and also monitor if policy is received. As suggested in risk mitigation work, we need to implement MDM solution. Next chapters will present more comprehensive overview and test results of UEM and MTD.

4.3 Research and testing

Relying on already analysed data strict bullet points can be created and write down criteria, what we are looking for in MDM platform. Keywords are light weight, don't want to use or collect more data as needed for IS (information security), keep it simple as possible with less restrictions, but at same time be sure, that company related information is secure. Don't want third party access, don't accept the risk of malware or cyber-attacks and in case of losing the device, it is important to perform remotely wipe action. Taking account, the requirements from risk mitigation suggestions and ISO 27001, the test plan was conducted, that will help to get familiar with the software, before we make a decision which one to choose. Many answers can be found from products white papers, but the performance and data collecting questions get answers only by testing out software in real time.

Test group and devices

There are a lot of operating systems for mobile phones. Some of them are open source, for example Android, and some of them are closed. Open source platforms can be used on different devices like Nokia, Samsung, LG etc. Android is the most popular platform used today, because of its capability to work on different mobile devices. Second popular is iOS. Closed platforms are used only in combination with certain device, like iPhone and iOS. Both are Apple products and always used together, no other software is used on iPhones and also iOS is not used on other mobile phones. One of the popular ones are also Windows OS and Blackberry OS, not so widely recognized, but in top 10 of mobile operating systems. From the history not so while ago, some might still remember Nokia Symbian OS. At some point Nokia phones were market leaders and they were one of the first, who enabled web browsing in mobile phones and created similar product as today we call smartphones.

By the statistics, people in Estonia prefer iOS and Android devices. By the results from March 2020 60,86% prefers Android based devices, most popular ones are Samsung, Huawei, Xiaomi, OnePlus and Sony. 33,59% prefer iOS and Apple iPhone, which makes it the most popular choice ahead of Samsung, who loses only by 2 percent. (StatCounter 2020)

For testing purposed different Android and iOS based phones are chosen. Since Android and iOS is preferred by almost 94% of Estonians mobile device owners, there is no need to test others. To get wider range and more different mobile devices I managed to convince to participate 3 other persons in this test. It is not best practise to test on devices, that are in real life usage and any error could paralyze the usability and reduce device value. It is strongly recommended to use test devices, that can be compromised, and no one has to accept damage. From another perspective, the goal is to find best solution to BYOD-s, then this testing environment is as real as it gets. Imitates real life situation and justifies the current choice.

Table 7. Test group devices and system versions

No	Device	Model	Op sys	Version	Last update	Comments
1.	LG	G4	Android 8	8.1.0 Oreo	5.12.2017	Android 8 is the latest and up to date version for this phone. Cannot be updated on 9 or 10
2.	iPhone	8	iOS 13	13.3	10.12.2019	latest version was 13.3.1, purpose is not to update this phone, to see how MDM-s react on it
3.	Samsung	S10	Android 10 Enterprise Knox	10.1	29.01.2020	Up to date phone
4.	iPhone	XS	iOS 13	13.4	24.03.2020	Up to date phone
5.	Nokia	8 Scirocco	Android 9 Enterprise	9.1	01.03.2020	Up to date phone
6.	Samsung	S9 Plus	Android 10	10.1	28.01.2020	Stable version, not latest
7.	Samsung	Galaxy S8	Android 9	Pie	31.11.2019	Old phone with old version

It is notable, that not all devices are up to date. The purpose is to keep them that way and see, what the UEM-s and MTD-s think about it. Based on previous research and theoretical input an action plan was created for testing purposes. Please look at LISA-1to find out test criteria.

Test results

Test group was composed of seven different devices with different versions of operation systems - 2 of them iPhones and 5 Android based mobile phones. Not all of them were up to date and the plan was to test UEM-s on them as they were to simulate problems and difficulties that might occur when trying to manage BYOD-s.

For better understanding we chose different Android platforms. Comparing to iOS, that has only one version of operating system and keeps developing it, then Android has many. Starting from Android 1 to 10 and right now even the 11th version is in development. For that reason, only 2 iPhones were included – the purpose was to test on old version and the latest. To get more visibility from Android different types like 8, 9 and 10 were included. They all have different functionality. Test with Android 8 failed because it does not share out API and therefore not manageable by MDM. API function is only enabled with Android Enterprise. If can be enabled by using company owned G Suite account or Google Play Store. LG G4 phone is a good example of a problem, that might occur, when trying to manage BYOD. The phone was released in 2015, quite old model, but is widely used today. It supports only Android 8 and due to lack of technical competence it is not possible to upgrade it to Android 9 or 10. Android Enterprise feature is not support on Android 8. Fortunately, it is not the most popular phone, but similar legacy type phones are still in use and this makes it a problem, because Android 8 does not share API and therefore unmanaged by any UEM, EMM, MDM or MAM. User preferences are different and not all people care about getting the latest and newest phones. It would be really hard from company's side to explain the need for new phone, alternative and empathic behaviour would be to offer new phone by company's expenses. In this case, the phone would be categorized as COPE not BYOD anymore.

For Android phones another feature to think consider. It is called Samsung Knox. Samsung is one of the most exemplary developer of Android. Over the years they have improved the usability of the platform and invested a lot in security features achieving the market leading position and Android users first choice. Knox is built native work profile, that helps for the user to isolate work related apps and private info. Many MDM can handle Knox and take over the management rights, but not all. It is important to find out which phones are equipped before choosing management solution, can save time and workhours.

For better overview and comparison, the test results are presented as one table in APPENDIX-1. More descriptive comments about test objects are in following section.

Workspace one

Through the times Workspace One has had many different names, but always on the top of Gartner's table and still keeping its place. Top ranks are justified for this software, because it offers many possibilities for customization, integration and reporting. Suitable for large companies because of its capability to vert granular with settings and also because it is compliable with different cyber security frameworks (NIST, ISKE, ISO).

Although it has UEM capability, the product can be used only for EMM or MDM purposes. Minus is that it needs administration rights to manage BYOD and by accepting this request user gives access to all data in their mobile devices. It can manage the device only when container is installed. Any extra component is a problem for BYOD-s and test result showed the fact, that system administrator can collect and see data outside of container. Good news is, that it is not doing it by the default, but with some configuration change it is possible for some nosy person to get around. Also, plus for the product is the possibility to create custom privacy policy and require user acceptance before sharing out administrator privileges. It prevents legal questions, that may occur, when employee is leaving from the organization.

From configuration side it has no problems. As mentioned earlier you can go very granular and when comparing the capability with our policy needs, then it meets expectations. Workspace One is available for on-prem installation or cloud base usage. The admin console is quite complex and needs training to get started. Since there are some many configuration possibilities basic training is required, because some configuration tips you just need to know to get expected result. That info or best practices cannot be learned by your own from white paper or forums, it does not exist. Only from vendor training program.

Since compatibility to share out Syslog, API and JSON format, it is possible to integrate with different other systems. For example, it is possible to manage info and carry out incident response from all known SIEM platforms.

Workspace One does not have the functionality of MTD, but integration with different MTD vendors are possible. Vendors in our scope – Sophos Mobile, Sandblast and Lookout are all usable with Workspace One.

WIPE possibility tests with Android worked well, left no traces and all information, from admins view and phone view, was removed. But there was error with both iPhones. After WIPE the admin view showed, that all information was removed from device, but it left extra menu page, that was required for creating container space and where organization apps were installed. After WIPE the page was empty, but not accessible for the user and it was not possible to remove it. That is a big minus if considering BYODs. It is good, that before testing we backuped all devices in test group and were able to restore original state. Therefore, do not consider it suitable for BYOD-s.

Intune

Intune has been top rated UEM solution for many years and now, when its part of the O365 licensing system, then it is growing popularity even more. Microsoft is changing licensing model and terms very frequently. Intune used to be part of O365 E3 license, that was more expensive, but since 1st of April this year, Microsoft renamed products, added user limitations and changed pricing plan. Old O365 cloud services are now divided into 2 large sectors M365 and O365. If plan is to continue with O365, then access to Intune will be lost and moving to M365 business will require more investment. Last Year Microsoft changed their licensing principals at least 3 times, which makes financial planning very difficult. At some point some companies found, that the products don't work anymore and were asking higher level licenses. That is a big downside and does not add much creditability to Microsoft side.

Intune is UEM, but can be used as EMM, MDM or MAM. It is only cloud based and therefore does not require any installation work. Admin console is ready to use with default settings after first login. The configuration range and customization possibilities are wide and offer same granularity as Workspace One. Comparing to Workspace One the configurations possibilities and admin console are more logical, but still needs many system administrator workhours to customize it and create policies, but Microsoft offers a lot of free support opportunities and trainings.

Integrations with other systems are possible. You can use Azure monitor with event hubs to stream logs to SIEM solution. Splunk, Qradar and Sumo logic are supported. Also compliable with different cyber security frameworks (NIST, ISKE, ISO). Does not have built in MTD functionality yet (according to latest news someday integration with Windows Defender will be made) but has the capability to integrate with our selected MTD vendors.

Big plus for Intune is its capability to manage Microsoft apps. Private sector companies are using lot of Microsoft products and their cloud services. In many cases, when considering information management, we only need a plan to manage Microsoft services and apps. Intune does not require admin level access or build a container in BYOD devices to manage apps and is still capable to manage other requirement like access control. Intune can be used only as MAM and it has a wide functionality to perform all required actions by the BYOD policy, that was worked out earlier. Also, it does not collect or see personal information, that makes Intune very lightweight, user friendly and definitely suitable for BYOD-s.

Sophos Mobile

Sophos Mobile is unique combination of UEM functionality and MTD. Sophos is highly rated for their effort of virus protection functionality, that is called Intercept X. It has deep learning capability; it is using artificial intelligence for known and unknown malware and does not only relay on signatures. Protects against ransomware attacks, malicious traffic, credential deft, exploit prevention, EDR (endpoint detection and response) and incident response.

To test out its functionality, we used EICAR program. The European Institute for EICAR developed the EICAR antimalware test file. The EICAR test file is a legitimate DOS program that is detected as malware by antivirus software. It is considered to be safest way for malware testing and does not harm the device. When the test file runs successfully (if it is not detected and blocked), it prints the message "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!". (EICAR, 2006) Intercept X performed without fault deleted the file and share information to the admin console.
While the MTD side is excellent, the MDM part is not. Fortunately, it is possible to use MDM functionality and MTD separately. MDM installation failed many of times, for both Android and Apple devices. Sophos Mobile requires administration rights and container installation before it can start managing the phone. Container installations is quite a pain. It offers quick container installation for BYOD-s, but after many hours spent with support, it turned out it does not work. Fortunately, Sophos Mobile offers alternative. Due to integration possibilities with other MDMs and SIEM solution, it is possible to use Intercept X with other vendors and drop out the whole native MDM part.

Functionality and policy enforcements work the same way as MDM installation. Support says that Their product works better with Apple devices, because iOS operating system is more stable and does not offer that variety as Android, but the results showed, it didn’t work well on both systems. Especially poor quality was for Samsung with Knox. The Sophos container installations went in conflict with Samsung Workplace and Sophos installation failed but didn’t give any error messages. From admins view it showed, that the installation is complete and connection between phone and admin console is established, but when testing connectivity, then test failed and it was not possible to push policies. Support couldn’t help either. Recommend using Intercept X functionality without MDM.

CheckPoint SandBlast

SandBlast is very powerful tool. It is considered as MTD, but additionally offers the base functionality of MDM. The functionality is CPU based and it can detect exploits and malware before they are opened or activated. Comparing with Sophos Intercept X the working principle and structure is the same. Very happy with the performance and was able to detect all of the tests we preformed, including EICAR. Has unique Behavioural Risk Engine and CheckPoint threat Cloud to run recourse intensive analysis in cloud environment. Admin console is a bit complex and needs preparation before starting using. Fortunately, information is easy to find, forums and whitepaper gives answers to many questions without need to evolve support.

Plus is that SandBlast is capable to integrate with different MDM (both Workspace One and Intune) and SIEM platforms, but minus, in terms of BYOD, is it needs security container to manage the device. It gains full access and can collect private information. Therefore, not really suitable for BYOD-s.

Lookout

Lookout is a cloud based MTD solution. The admin console is preconfigured and ready to use after first login. Since the admin console does not offer any customization possibilities, does not offer any MDM functionality and individual profile creation, then it does not need highly trained IT personnel to manage it. Comparing to SandBlast and Sophos Intercept X, it does not use some next generation AI (artificial intelligence) self-learning method, but uniquely compares data with information they are seeing from other customers. They are monitoring more than 185 million devices all over the world and have very wide knowledge about IS. Lookout uses collected data only for analysing purposes, it does not store data and in fact – Lookout is database free. After analysing the info comparing it to already known data and creating new rules, it forgets it immediately. That also goes for admin console. If admin access passcodes are forgotten, then there are no recovery options. All profile gets deleted and have to start to build your console from the scratch. Mainly it means only connecting mobile phones to new profile, because the console itself is not very customizable.

Performed also EICAR test. File was recognized and deleted. The information didn’t appear in admin console and that’s a minus, because admins need to collect info for analysing purposes - employee cyber hygiene maturity, statistics, for evaluating the need and scope of next cyber hygiene training. Otherwise have no complaints and for user this program is almost seamless. Definitely a good tool for BYOD-s.

4.4 Summary and implementation recommendations

After testing MDM and MTD vendors with different mobile devices and compared these results with our theoretical analysis and action plan, it can be concluded, that most impressive products in terms of BYOD were Intune, Sophos Intercept X and Lookout. Considering the requirement stated for user friendly approach and ease of use for system manager, then it is most reasonable to choose Intune in cooperation with Lookout. Sophos Intercept X showed some impressive results and the technology behind it is exemplary, but test results showed, when scanning the device performance issues were caused and therefore the best choice is Lookout.

Since the scope is only monitor mobile devices it would be reasonable to use Intune as MAM. The goal is to protect our own information according requirements sated by ISO27001 framework and make it as easy as possible for the user to understand the need and for administrator to manage it. That way there is no need to deal with legal issues and privacy compliance. Only these apps will be installed, that are allowed to use with access requirements and network policy. When employee leaves organization, then it is possible easily perform WIPE without harming the device or its operating system. Example policy for Intune, which is suitable for BYOD and is ISO compliant, is added to this work in APPENDIX-2.

Implementation guidance

After completing previous steps like theoretical preparation, practical analysis and preconfiguring Intune, the next step would be installation process. Behind every successful process, there is a procedure. Good procedure is always well described, ongoing and unambiguous. ISO 27000 has suggestions about implementation process that is very efficient – "Plan, Do, Check, Action (PDCA)" Plan. In phase PLAN, there is only one activity called "establish ISMS (information security management system)". In phase DO, there exist two activities, called "Implement and operate the ISMS". In phase CHECK, there are two activities called "monitor and review ISMS". In ACT phase, two activities called "maintain and improve" are involved. (Xiaobo Zhu, Yunqian Zhu, 2019)

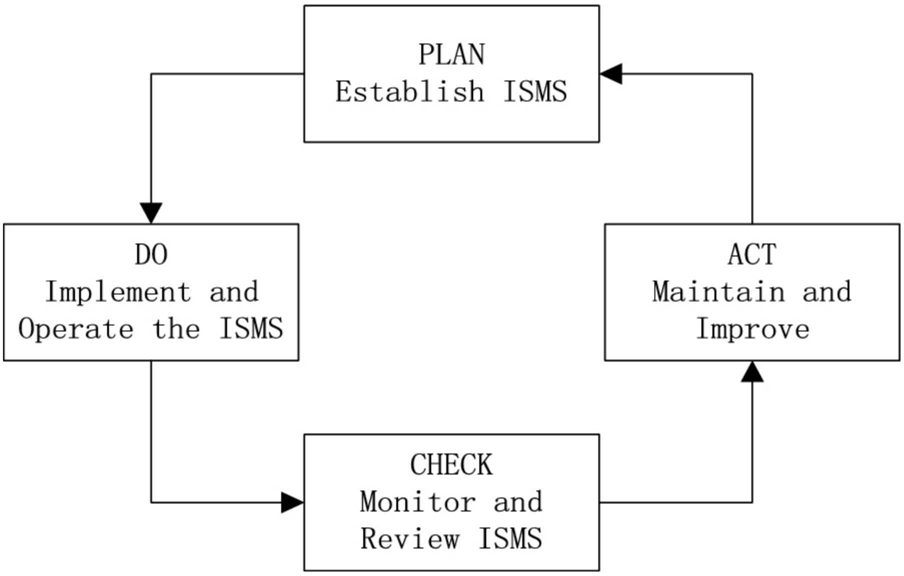


Figure 3. PDCA process (Xiaobo Zhu, Yunqian Zhu, 2019)

PDCA is also a good process to implement for incident response procedure. Where the ongoing process improving is very important for incident detection, pattern development, finding solution, patching and analyse what went well, what bad and what to do better next time. In terms of protecting BYOD devices against known risks and keeping mind ISO requirements our PDCA will look like this.

PLAN

- Create a work plan
- Map down all Mobile devices, operating systems, versions
- Evaluate benefits and disadvantages of different OS platforms
- Develop strategy for incident response
- Communicate the need of this work to employees
- Test before going in live

DO

- Create network plan and access permits
- Segment your information

- Analyse risks
- Implement MDM and MTD
- Activate policies

CHECK

- Monitor devices, incidents and react
- Monitor systems, network (Update and backup procedures)
- Redundancy plan

ACT

- Report
- Analyse results
- Training
- Improve procedures

5 Conclusion

When started working on this subject I was convinced, that the problem is acute in today's modern world and in future the even more important. That time I was only thinking about business related inputs, but could have not predicted, that in three months we face world crisis and distance working will become matter of economic survival.

Today, there is no question, do we need teleworking solutions or not. Working from distance is new normality standard. With the increased need to work form distance, the risk of information loss has also doubled. According to reports, that are published by RIA every year, the risk of data loss or getting hacked increases 25-50%. In light of pandemic crisis, the number is even higher, and focus is turned from enterprise attacks to individuals, who are more vulnerable working from home, isolated from secure company's network and all cyber security measures are not reachable.

In these circumstances many companies have permitted to use personal devices for working purposes. That means using BYOD-s gets more popular, but also the risk of losing data or important information also increases. By the statistics almost 90% hacked accounts didn't have MFA activated, but according to latest news even 2-step authentication does not keep your information safe. Well planned phishing campaigns and malicious attachments/links have always been on top places, when talking about examples of successful incidents, but now more sophisticated methods are taking over and focus is on mobile devices, instant messaging platforms and authenticator apps. If we are thinking on businesses, who have 50 employees or more, in terms of Estonia Middle Sized enterprise, then the need of automated supervision, data control and device management is mandatory. It would be unthinkable for IT teams to handle such a big group of devices one by one.

Essence of BYOD requires more individual approach and since they are owned by employees and contain their private information, then it is very important to keep in mind privacy policies and user rights to prevent further legal issues. It is highly recommended to communicate in detail, how the process will work and what are the benefits for the user. Raising the common knowledge about data protections principles and risk awareness, can lead to thought-out behaviour and actions by the employees, that is also a big part of risk mitigation.

Even in times of crisis we cannot underestimate the importance of prework. All action must be driven from planning. If planning and prework is done perfectly, then it saves a lot of time in the following sections of work. In this research we have proved that the organizations need common understanding of security risks when bringing BYOD into network and allowing to access business related information. Since the technical environment is evolving fast then the need for continuous development plan is highly recommended. When implementing a known security framework like ISO27000 it is ensured, that procedures are up to date and will help to keep the level of information security.

Outcome of this work is ISO compliant implementation guide for medium size private sector company with recommendation how to centrally manage BYOD devices. Goal is to save a lot of time, that is needed for data collecting and analysation and man-hours for the organization to test out different solution and practises. This thesis gives overview about all major sectors and problems IT managers might face while working out the BYOD policy. The final solution is tested and proved to mitigate standard risks and ISO requirements for teleworking. The evaluation was done keeping in mind not to restrict user freedom and not to collect user data more, that it is needed for IS (information security).

The research concentrates on overall knowledge about security risks in terms of BYOD-s and working out IS (information security) procedure, that is also ISO compliant. The goal is to point out and find solution to weaknesses and possible problems, what might occur, when trying to monitor privately owned devices. This paper does not consider the need or business drives of specific industry and field. That might be one of the future topics and opportunities to continue this work.

References

1. 42gears.com, 2017 “What’s the difference between MDM, EMM, UEM?” https://www.42gears.com/blog/difference-between-mdm-emm-uem/ 27.04.2020
2. Ahmad, A., Bosua, R., and Scheepers, R. 2014. "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective,"
3. Ahmad, A., Ruighaver, A.B., and Teo, W.T. 2006. "An Information-Centric Approach to Data Security in Organizations,"
4. Ahmand, Atig; Arregui, Daniel; Maynard, Sean; 2016 “Mitigating BYOD Information Security Risks” https://minerva-access.unimelb.edu.au/handle/11343/56627 27.04.2020
5. Alliantist Ltd, 2020 “ISO27001 Annex A.6, 2016” https://www.isms.online/iso-27001/annex-a-6-organisation-information-security/ 27.04.2020
6. AnsonBaer Nordic OÜ, 2020 https://ansonbaer.com 27.04.2020
7. Armando, A., Costa, G., Verderame, L., and Merlo, A. 2014. "Securing the "Bring Your Own Device" Paradigm,"
8. Arregui, D., Maynard, S. 2016 “Mitigating BYOD Information Security Risks”
9. Bordin, Martin 2016 “Mobile Device Strategy”
10. Cappelli, D., Moore, A., and Trzeciak, R. 2012. „The Cert Guide to Insider Threats : How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)“
11. Check Point Software Technologies Ltd., 2020 “Introducing Check point SandBlast Zero-Day Protection” https://blog.checkpoint.com/2015/09/02/introducing-check-point-sandblast-zero-day-protection/ 27.04.2020
12. Dong, Y., Mao, J., Guan, H., Li, J., and Chen, Y. 2015. "A Virtualization Solution for Byod with Dynamic Platform Context Switching,"
13. Donovan, F. 2014. "Employees Fail to Take Basic Steps to Secure Byod Devices, Data,"
14. EICAR, 2006 https://www.eicar.org/?page_id=3950 29.04.2020
15. Estonia’s Statistics Department, 2020 https://www.stat.ee/68772 27.04.2020
16. EUR-Lex , Access to European Law, Eur-Lex EU recommendation 2003/36 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361 27.04.2020
17. Gajar, Ghosh, A., and Rai. 2013. "Bring Your Own Device (Byod)- Security Risks and Mitigating Strategies,"
18. Gartner Glossary, Information Security, Definition by Gartner https://www.gartner.com/en/information-technology/glossary/bring-your-own-device-byod 27.04.2020
19. Goldsborough, R. 2011. "Wi-Fi Convenience Comes with Risks."
20. Gray, Robin, 2018 “What is Mobile threat Defence (MTD)?” https://www.wandera.com/what-is-mobile-threat-defense-mtd/ 27.04.2020
21. Haataja, K.M.J. 2008. "Further Classification of Bluetooth-Enabled Ad-Hoc Networks Depending on a Risk Analysis within Each Classified Group,"
22. Kang, D., Oh, J., and Im, C. 2015. "Context Based Smart Access Control on Byod Environments,"
23. Kaspersky. 2013. "One in Every Six Users Suffer Loss or Theft of Mobile Devices." Kaspersky Lab.

24. Kaufman, Lucas, 2014, Information security Stack exchange https://security.stackexchange.com/questions/76066/what-is-the-difference-between-iso-27001-and-iso-27002 27.04.2020
25. Ketel, M., and Shumate, T. 2015. "Bring Your Own Device: Security Technologies,"
26. Kramer, S., and Bradfield, J.C. 2010. "A General Definition of Malware,"
27. Kwikcert, 2019, “Mobile Device and Teleworking Policy” https://kwikcert.com/iso-27001-mobile-device-teleworking-policy/ 27.04.2020
28. Lawrence, D., and Riley, M. 2014. "A Fresh Reason Not to Jailbreak Your Iphone."
29. Leavitt, N. 2013. "Today's Mobile Security Requires a New Approach,"
30. Lookout Ltd,2020 “Lookout whitepaper” https://www.lookout.com/insights 27.04.2020
31. Market Business News, 2020 “What is teleworking? Definition and meaning” https://marketbusinessnews.com/financial-glossary/teleworking-definition-meaning/ 27.04.2020
32. Miller, Jason, 2019 Bitlyft https://www.bitlyft.com/what-is-iso-27000/ 27.04.2020
33. Nasim, R. 2012. "Security Threats Analysis in Bluetooth-Enabled Mobile Devices,"
34. Podhradsky, A.L., Casey, C., and Ceretti, P. 2012. "Managing Bluetooth Risks in the Workplace,"
35. Potts, M. 2012. "The State of Information Security,"
36. Prajwal, Desai 2017 „Microsoft Intune overview and its features “ https://www.prajwaldesai.com/microsoft-intune-overview-and-its-features/ 27.04.2020
37. Rouse, Margaret, 2016 “Unified Endpoint Management” https://searchenterprisedesktop.techtarget.com/definition/unified-endpoint-management-UEM 27.04.2020
38. Ruighaver, A.B., Maynard, S.B., and Warren, M. 2010. "Ethical Decision Making: Improving the Quality of Acceptable Use Policies,“
39. Schulze, H. 2014. "Byod & Mobile Security Report."
40. Sophos Ltd, 2020 “Sophos Mobile documentary” https://www.sophos.com/en-us/products/mobile-control.aspx 27.04.2020
41. Souppaya, M., and Kent, K.A. 2012. "Guidelines for Managing and Securing Mobile Devices in the Enterprise: Recommendations of the National Institute of Standards and Technology,"
42. Spencer, L. 2015. "16 Million Mobile Devices Hit by Malware in 2014: Alcatel-Lucent," in: ZDNet. www.zdnet.com.
43. StatCounter, 2020 “Global Statistics, Mobile Vendro Market Share Estonia” https://gs.statcounter.com/vendor-market-share/mobile/estonia 27.04.2020
44. Tess, Hanna, 2019 “Top three Reasons to use UEM” https://solutionsreview.com/mobile-device-management/top-three-reasons-to-use-uem/ 27.04.2020
45. Tu, Z., Turel, O., Yuan, Y., and Archer, N. 2015. "Learning to Cope with Information Security Risks Regarding Mobile Device Loss or Theft: An Empirical Examination,"
46. Vishal, G., Deepak, S., and Lovekesh, D. 2013. "An Approach to Implement Bring Your Own Device (Byod) Securely,"

47. VM Ware, 2020 “Workspace One whitepaper” https://techzone.vmware.com/resource/what-workspace-one#section2 27.04.2020
48. Wang, Y., Wei, J., and Vangury, K. 2014. "Bring Your Own Device Security Issues and Challenges,"
49. Wired Insider 2018, „BYOD, CYOD, COPE, COBO — What Do They Really Mean?“ https://www.wired.com/brandlab/2018/06/byod-cyod-cope-cobo-really-mean/ 28.04.2020
50. Wood, A. 2013. "Byod in the Financial Sector: The Pros and Cons for End Users and the Business,"
51. Xiaobo Zhu, Yunqian Zhu, 2019 „Extension of ISO/IEC27001 to Mobile Devices Security Management”

Appendix 1 – Practical Analysis

No	Service	Workspace One	Intune	Sophos Mobile	Sandblast	Lookout
1	Cloud based	Yes	Yes - hosted in azure	Yes	Yes	Yes
2	On-prem	Yes	No	No	No	No
3	Security Container	Yes	No	Yes - does not work good with Samsung Knox	No	No
4	Full Control	Yes	Yes - for fully managed devices. No - for MAM devices	Yes	No	No
5	MAM, EMM, MDM, UEM	Full UEM, MDM and MAM part can be used in scope of mobile devices	Intune is full MDM solution and has MAM capabilities	Has UEM functionality, can be used only for mobile devices, includes MTD	MTD - Mobile threat defence app	MTD - Mobile threat defence app
6	Admin console	Yes – On-prem,	Yes - Azure portal or Microsoft Endpoint Manager Admin centre	Yes- cloud based	Yes - Cloud based and check point hosted	Yes, cloud based
7	Install requirements (on VM?, how much space)	VM, physical machine	-	-	-	-
8	Suitable for Androids	Yes	Yes	Yes, except Samsung Knox	Yes	Yes

9	Suitable for iPhones	Yes -full control, No - BYOD	Yes	Yes	Yes	Yes
10	Own database?	Yes, on-prem	Yes- in Azure cloud	Yes	Yes - in cloud	No, no database
11	Stores user data?	Yes	Yes	Yes	Yes	No
12	Stores admin data?	Yes	Yes	Yes	-	No
13	Create custom privacy policy, notification, accept from device, data is stored)	Can create custom privacy policy, before installation user has to accept it, it is stored in database for later usage or view	Only default privacy policy	No	Yes - Can choose what data will be sent to check point cloud	No
14	Grace period	Yes	Yes	Yes	-	-
15	Admin console security (level of security, hardening opportunities)	Role based, AD, MFA	Role based access with Azure AD, MFA capabilities.	Role based access, MFA	Role based access model, MFA capabilities	Role based access model, MFA capabilities
16	SIEM integration	integrates with your SIEM tools by sending event logs using Syslog	You can use Azure monitor with event hubs to stream logs to SIEM solution. Splunk, Qradar and Sumo logic	API and Syslog format for SIEM integration	ArcSight, Splunk	ArcSight, Splunk, Qradar
17	Integration with MDM, UEM, EMM? (question only for MTD products)	-	-	Yes, with both - Intune and Workspace One	Yes, Intune	Yes, but with configuration help from vendors side

18	How light weight is this program to devices (overloads processor, seamless behaviour or causing any performance issues?)	Light weight	Light weight	Light weight	When scanning, then you feel a light performance loss, other ways seamless.	Does not cause any performance issues, seamless. If reading email from web applications, then blocks attachments, if using mail reading apps, then not.
19	ACCESS CONTROL					
20	MFA activisation on mobile devices	Yes, can be requested from admin console	Support Microsoft Authenticator and SMS option	Yes, can be requested from admin console	No	No
21	Device monitoring (health check, op sys check, version check, update/upgrade from distance)	Yes, updates can be pushed from admin console	Monitoring device compliance, OS version, last check-in. Force Update available for win10 and iOS devices.	Yes, device monitoring, forced updates, version check, OS check	Yes - Health check for apps, network and OS. No remote upgrade for apps/OS	Yes - Health check for apps, network and OS. Same as Sandblast
22	Password control for the mobile device (number, figures, biometric, no of digits)	Yes, if fully managed, no if MAM mode. For BYOD-s - if admin access is granted then yes	Yes - for fully managed devices. No - for MAM devices	Yes, can restrict which method has to be used and requirements for password	No	No
23	Periodic password change	Yes	Yes - for MAM only applies to app pin	Yes	No	No

24	Password control for container or apps	Yes	Yes - supported for policy managed app (30+ apps, office365 apps mostly), can be applied to LOB (line-of-business apps)	Yes	No	No
25	WIPE possibility (if password is entered incorrectly, if device is lost)	Yes, container wipe, full wipe, app wipe	Yes - Wipe corporate data on MAM, full wipe for fully enrolled devices	Yes, container wipe, full wipe, app wipe	No	No
26	Application control (downloads available only recognized phones, restrict sign in, other limits)	YES, all limitations are possible for BYOD or full control	Yes - full control for fully managed devices. MAM devices support only policy managed apps (30+ apps, office365 apps mostly)	Yes, if full mode, no if BYOD	No	No
27	Cryptography (is any used, what type, only for containers? is it possible to secure apps?)	Yes, Bitlocker and FileVault. 256-bit AES for iOS/Android	Yes - 256-bit AES for iOS/Android (FIPS 140-2 validated). For MacOS it uses FileVault (XTS-AES-128 encryption with a 256-bit key). For windows 10 Bitlocker	Vendor says yes, but it is not described	No	No

28	Is it possible to export data using external tools?	-	-	-	-	-
29	User Behaviour					
30	Copy/ Paste control	Yes, by policies	Yes - for policy managed apps in MAM	Only in full control	No	No
31	OWA restrictions	Yes, can be integrated with AD	No - OWA restriction are applied on exchange admin centre or with Azure AD conditional access rules	No	No	No
32	Backup control	Yes, restrict only corporate data or in full control all data	Yes - restrict corporate data backup to Android/iOS backup services	No	No	No
33	Network					
34	VPN possibility	Yes	Yes	Requires additional app	Yes	Safe browsing vpn is a product, that adds extra layer of network protection while web browsing. It is not VPN
35	WIFI access control	Yes	Yes	Yes	No	No
36	Bluetooth control	Yes	Yes - only for fully managed devices	No	No	No

37	Virus Protection					
38	Admin console (access, layout, dashboards, MFA access, security hardening)	Yes, can be integrated with different MTD vendors	Yes- if integrated to windows defender ATP (need E5 license)	Has both MDM and MTD capability, can be used individually	Yes - Admin console use role-based access model and can use MFA	Yes- role based access, MFA
39	Device real-time monitoring	No	No	Yes	Yes	Yes
40	Alerts to admin console	Yes, all alerts can be managed from admin console	Yes - (MTD can alert Intune console if integrated)	Yes	Yes - Also can integrate and send notifications to other MDM solutions	Yes and no, not all data is shown in admin console
41	Incident response possibility (disconnect network access, run full-scan, get sample)	YES	No	Yes, full scan in full control mode, network restrictions	Yes - Conditional access to block access to corporate resources when device is at risk	No
42	Compliance check (root rights, op sys check, version check)	Yes	Yes	Yes	Yes	Yes
43	User notification	Yes	Yes	Yes, but could be better	Yes	Not always if something is blocked
44	Network connection monitoring	no	no	no	Yes	yes

45	Web filtering URL check	yes	Yes - only for fully managed devices with Managed browser (Edge)	Yes	Yes - whitelist and blacklist. Also has On-device network protection	Yes
46	Man-in-the-Middle detect	no	No	Yes	Yes	Yes
47	Sandbox	no	No	yes	Yes - App sandboxing done in cloud	Yes
48	Email Phishing detection	no	No	Yes	Yes - On-device network protection	Yes
49	SMS Phishing	no	No	Yes	Yes - On-device network protection	Yes
50	Application check	no	No	Yes	Yes - Check Point's unique Behavioural Risk Engine (BRE) runs applications in a cloud-based environment to scan for threats.	Yes

51	Your comments	Pros: Very granular product, suitable for large companies, who have lots of different devices. On-prem possibility. Works well with Android and iPhone. Cons: After wipe, left empty hidden slot to iPhone. This cannot be deleted or accessed by user. Not good for BYOD. Hard to start using by your own, requires training by vendor, many things user just needs to know	Pros: easy integration with other Microsoft products, easy to use/manage admin portal. Missing Mobile Threat defence (MTD) solution. Cons: Needs lots of admin hours to set up. Microsoft changes policies and prices very frequently, there’s a risk, that one day some feature may not work because or that or need different licensing	Pros: If using in full control mode, then no problems. Cloud base admin console is easily managed, no installations needed, ready to start using after first login. Price is very low. Can be used as MDM or MTD or both. Cons: Does not work with Samsung Knox, installations fails, MTD functionality is better, than MDM. Not all features work as said in whitepaper. Admin needs consistent help from support.	Pros: It can be integrated to variety MDM solutions. Has unique Behavioural Risk Engine and Checkpoint threat Cloud to run resource intensive analysis in cloud environment. Cons: For iOS it needs management profile to be installed on device (also applies to BYOD). Admin portal is advanced and that can be bit complex to use.	Pros: Very light weight, does not have database, does not store any user data. Is very cheap and very popular. Cons: Admin does not see all info in console, if some document or app is blocked. Blocks attachments if using web browsers for email reading. Setting up network restriction profile fails and does not work as promised in whitepaper.

Appendix 2 – Example MAM policy

Answer – not selected

Answer – as is, not activated

Answer – Selected

iOS app protection policy

Data protection rules

- Backup Org data to iCloud/iTunes/Android backup service - Allow/**Block**
- Send Org data to other apps - **Policy managed apps/**All apps/None
    - Select apps to exempt - **None selected**
    - Save copies of Org data - **Block/**Allow "Save as" option
    - Allow users to save copies to selected services (**OneDrive for Business, SharePoint** and Local Storage)
- Receive data from other apps - Policy managed apps/**All apps/**None
- Restrict cut, copy and paste between other apps - Blocked/Policy managed apps/**Policy managed apps with paste in**/Any app
    - Cut and copy character limit for any app - **0**
- Third party keyboards - **Allow/**Block
    - Select keyboards to approve

- Encrypt Org data - **Require**/Not required (256-bit AES encryption)
    - Encrypt Org data on enrolled devices - **Require**/Not Required
- Sync app with native contacts app **-** Block/**Allow**
- Printing Org data **- Block**/Allow

- Restrict web content transfer with other apps (specify how web content http/https links are opened from policy-managed apps)
    - **Any app**
    - **Intune Managed Browser**
    - **Microsoft edge**
    - **Unmanaged browser**
- Org data notifications - Block/**Block Org data**/Allow/ Any app

Access requirements

- PIN for access **- Require**/Not Required
    - PIN type - **Numeric/**Passcode
    - Simple PIN - **Block/**Allow
    - Select minimum PIN length - "Value" - **6**
    - Touch ID instead of PIN for access (iOS 8+) - **Allow/**Block
        - Override fingerprint with PIN after timeout - Require/**Not Required**
        - Face ID instead of PIN for access (iOS 11+) - **Allow**/Block

    - Select number of previous PIN values to maintain **- 5**
    - PIN reset after number of days - Yes/**No**
        - Number of days
    - App PIN when device PIN is set - **Require/**Not Required
- Work or school account credentials for access - Require/**Not Required**
- Recheck the access requirements after minutes of inactivity - **"Value in minutes" - 15**

Conditional Launch

- Max PIN attempts - value in mins **" 5 "** - action **"Reset PIN**/Wipe data**"**
- Offline grace period - value in mins **" 720 " Block access(minutes)/**Wipe Data (Days)
- Offline grace period - value in days **" 90 "** Block access(minutes)/**Wipe Data (Days)**
- Jailbroken/rooted devices - **Block access**/Wipe data
- Min OS version - **Warn**/Block access/Wipe data -13.0
- Min app version - **Warn/Block access/Wipe data**
- Min patch version - **Warn/Block access/Wipe data**
- Device manufacturers - **Allow specified (block non-specified) / Allow specified (Wipe non-specified)**
- SafetyNet device attestation - **Warn/Block access/Wipe data**
- Require threat scan on apps - **Warn/Block access (This setting in particular ensures that Google's Verify Apps scan is turned on for end user devices.)**

- Min Company portal version - **Warn/Block access/Wipe data**
- Max allowed device threat level - **Block access/Wipe data**

Android app protection policy

Data protection rules

- Backup Org data to iCloud/iTunes/Android backup service - Allow/**Block**
- Send Org data to other apps - **Policy managed apps/**All apps/None
    - Select apps to exempt - **None selected**
    - Save copies of Org data - **Block/**Allow "Save as" option
    - Allow users to save copies to selected services (**OneDrive for Business, SharePoint and Local Storage**)
- Receive data from other apps - Policy managed apps/**All apps/**None
- Restrict cut, copy and paste between other apps - Blocked/**Policy managed apps**/Policy managed apps with paste in/Any app
    - Cut and copy character limit for any app - **0**
- Third party keyboards - **Allow/**Block
    - Select keyboards to approve
- Encrypt Org data - **Require/**Not required (256-bit AES encryption)

    - Encrypt Org data on enrolled devices - **Require/Not Required**
- Sync app with native contacts app **- Block/Allow**
- Printing Org data **- Block/Allow**
- Restrict web content transfer with other apps (specify how web content http/https links are opened from policy-managed apps)
    - **Any app**
    - **Intune Managed Browser**
    - **Microsoft edge**
    - **Unmanaged browser**
- Org data notifications - Block/**Block Org data/**Allow/ Any app

Access requirements

- PIN for access - **Require**/Not Required
    - PIN type - **Numeric**/Passcode
    - Simple PIN - **Block/**Allow
    - Select minimum PIN length - "Value" - **6**
    - Touch ID instead of PIN for access (iOS 8+) - **Allow/**Block
        - Override fingerprint with PIN after timeout - Require/**Not Required**
        - Face ID instead of PIN for access (iOS 11+) - **Allow**/Block
    - Select number of previous PIN values to maintain **- 5**
    - PIN reset after number of days - Yes/**No**

        - Number of days
    - App PIN when device PIN is set - **Require**/Not Required
- Work or school account credentials for access - Require/**Not Required**
- Recheck the access requirements after minutes of inactivity - **"Value in minutes" - 15**

Conditional Launch

- Max PIN attempts - value in mins **" 5 "** - action **"Reset PIN**/Wipe data**"**
- Offline grace period - value in mins **" 720 " Block access (minutes)/**Wipe Data (Days)
- Offline grace period - value in days **" 90 "** Block access (minutes)/**Wipe Data (Days)**
- Jailbroken/rooted devices - **Block access/**Wipe data
- Min OS version - **Warn**/Block access/Wipe data **–8.0**
- Min app version - **Warn/Block access/Wipe data**
- Min patch version - **Warn/Block access/Wipe data**
- Device manufacturers - **Allow specified (block non-specified) / Allow specified (Wipe non-specified)**
- SafetyNet device attestation - **Warn/Block access/Wipe data**
- Require threat scan on apps - **Warn/Block access (This setting in particular ensures that Google's Verify Apps scan is turned on for end user devices.)**
- Min Company portal version - **Warn/Block access/Wipe data**
- Max allowed device threat level - **Block access/Wipe data**