



# Implementing Zero Trust Architecture for Identities and Endpoints with Microsoft tools

Jani Kujo

Master's thesis

May 2023

Information and Communication Technology

Master's Degree Programme in Information Technology, Cyber Security

**Jani Kujo**

### **Implementing Zero Trust Architecture for Identities and Endpoints**

Jyväskylä: Jamk University of Applied Sciences, May 2023, 85 pages.

Master's Degree Programme in Information Technology, Cyber Security, Master's Thesis

Permission for open access publication: Yes

Language of publication: English

### **Abstract**

For past couple of years, it's been a trend for employees for working from home. This is mostly because of covid but other factors also play a part. This change from perimeter work from offices and organization facilities has brought up new issues in the everchanging cyber landscape. The exposure of identities and endpoints are growing, and organizations are more vulnerable.

This research describes efficient methods that helps organizations to protect from cyber attacks against identities and endpoints with Zero Trust Architecture and discusses possibilities to develop overall cyber strategy.

The results show that with the right policies and setting organizations are able to deflect certain types of attacks and threats and that the security posture can be uplifted with relatively small changes. In this research this is demonstrated with use cases of threats and by creating example policies to protect with.

The findings in this research are that the protection mechanisms of identities and endpoints are currently inadequate against very big attack vector and organizations should take this into consideration.

### **Keywords/tags (subjects)**

Cybersecurity, Zero Trust, Identity, Endpoint

### **Miscellaneous (Confidential information)**

Work is public. It does not contain any confidential information.

Jani Kujo

### Zero Trust Arkkitehtuurin implementointi identiteeteille ja päätelaitteille

Jyväskylä: Jyväskylän Ammattikorkeakoulu, Toukokuu 2023, 85 sivua.

Master's Degree Programme in Information Technology, Cyber Security, YAMK Opinnäytetyö

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: English

### Abstract

Viimeisten vuosien aikana on ollut trendinä, että työntekijät tekevät etätöitä kotoa käsin. Tämä johtuu pääasiassa koronasta, mutta tähän vaikuttava myös muut tekijät. Muutos perinteisestä toimistossa ja organisaatioiden tiloissa tapahtuvasta työstä on tuonut uusia haasteita jatkuvasti muuttuvassa kybermaailmassa. Identiteettien ja päätelaitteiden altistuminen kasvaa ja organisaatiot ovat haavoittuvaisempia.

Tässä tutkimuksessa esitellään tehokkaita menetelmiä, joiden avulla organisaatiot voivat suojautua kyberhyökkäyksiltä jotka kohdistuvat identiteettejä ja päätelaitteita kohtaan, Zero Trust -arkkitehtuurin avulla, tutkimus myös esittelee mahdollisuuksia kehittää kokonaisvaltaista kyberstrategiaa.

Tulokset osoittavat, että oikeiden politiikkojen ja asetusten avulla organisaatiot voivat torjua tiettyjä hyökkäystyyppisiä ja uhkia, ja kyberturvan tasoa voidaan parantaa suhteellisen pienillä muutoksilla. Tässä tutkimuksessa tämä osoitetaan esimerkki uhka skenaarioilla sekä luomalla esimerkki politiikkoja, jolla näitä vastaan voidaan suojautua.

Tämän tutkimuksen löydökset osoittavat, että identiteettien ja päätelaitteiden suojausmekanismit ovat tällä hetkellä puutteellisia erittäin suurta hyökkäysvektoria vastaan ja organisaatioiden tulisi ottaa tämä huomioon.

### Avainsanat (asiasanat)

Kyberturva, Zero Trust, identiteetti, päätelaite

### Muut tiedot (salassa pidettävät liitteet)

Työ on julkinen, eikä sisällä miltään osin salattavaa materiaalia

## Contents

<b>1</b>	<b>Introduction .....</b>	<b>9</b>
<b>2</b>	<b>Research methodology .....</b>	<b>10</b>
2.1	Research Questions.....	10
2.2	Research methods.....	10
2.3	Research Ethics.....	10
<b>3</b>	<b>Cybersecurity in general.....</b>	<b>11</b>
3.1	Threat actors .....	11
3.1.1	State sponsored actors .....	12
3.1.2	Hacktivist.....	12
3.1.3	Insider threats.....	13
3.1.4	Script Kiddies .....	13
3.1.5	Cyber Criminals .....	13
3.2	Common attack techniques .....	14
3.2.1	Malware based attacks .....	15
3.2.2	Denial of service attack.....	15
3.2.3	Phishing.....	16
3.2.4	Social engineering.....	16
3.2.5	Zero-day exploits .....	16
3.3	Common issues within organizations .....	17
3.3.1	User awarness.....	17
3.3.2	User and Endpoint protection .....	17
3.3.3	Misconfiguration.....	17
3.3.4	Privileges.....	18
3.3.5	Vulnerability management .....	18
3.4	Administrative Cyber Security.....	19
3.5	Administrative security measurements .....	20
3.5.1	Risk Assesment .....	20
3.5.2	Employee Awarness.....	20
3.5.3	Incident Response.....	21
3.6	Technical Cyber Security .....	22
3.6.1	Endpoint security .....	22
3.6.2	Identity security .....	24
3.6.3	Network security.....	25
3.6.4	Physical security.....	26

3.6.5	Application Security .....	27
3.6.6	Data Security.....	28
<b>4</b>	<b>Zero Trust .....</b>	<b>28</b>
4.1	Formation of Zero Trust .....	28
4.2	Tenets of Zero Trust .....	30
4.3	Microsoft’s implementation of Zero Trust.....	32
4.3.1	Identity.....	34
4.3.2	Endpoints .....	35
4.3.3	Applications .....	35
4.3.4	Network .....	36
4.3.5	Company Data .....	37
4.3.6	Infrastructure.....	38
4.3.7	Visibility, Automation Orchestration .....	39
4.4	Environment.....	39
4.5	Assets.....	40
4.6	Identities.....	40
4.7	Baseline settings.....	41
<b>5</b>	<b>Heading towards Zero Trust Architecture .....</b>	<b>42</b>
5.1	Planning Zero Trust Architecture .....	42
5.2	Implementing Zero Trust Architecture .....	43
5.3	Conditional access.....	50
5.3.1	Building Common Zero Trust compliant Conditional Access policies .....	51
5.4	Compliance policies.....	57
5.4.1	Building Common Zero Trust compliant Compliance policies.....	58
<b>6</b>	<b>Use cases .....</b>	<b>62</b>
6.1	Brute Forcing or leaked credentials .....	62
6.2	Passing conditional access policy with stolen credentials .....	65
<b>7</b>	<b>Security baseline and posture .....</b>	<b>68</b>
7.1	Security Baseline .....	69
7.2	Security Posture .....	70
7.3	Microsoft 365 Defender Security score .....	70
7.3.1	Identity score .....	73
7.3.2	Data Score.....	73
7.3.3	Device score.....	74
7.3.4	Apps score.....	74

7.3.5	Recommended actions .....	75
<b>8</b>	<b>Discussion.....</b>	<b>76</b>
8.1	Changing cyber landscape.....	76
8.2	Hardship of Zero Trust .....	78
<b>9</b>	<b>Conclusions .....</b>	<b>78</b>
	<b>References .....</b>	<b>81</b>

## Figures

Figure 1:	Zero Trust Timeline .....	30
Figure 2	Overview Of Zero Trust Architecture.....	33
Figure 3	Zero Trust layers.....	34
Figure 4	Licenses used in the research .....	40
Figure 5	Overall architecture of Zero Trust for RaMP.....	44
Figure 6	Custom banned password list.....	46
Figure 7	M365 Defender & Microsoft Intune connection .....	49
Figure 8	Overview of Conditional access .....	51
Figure 9:	Conditonal access policy - Block clients that don't support modern authentication..	52
Figure 10:	Conditonal access policy - Require MFA when sign-in risk level is Low-High.....	53
Figure 11	Conditonal access policy - High risk user password change .....	54
Figure 12	Conditonal access policy - Require approved apps and app protection .....	55
Figure 13	Conditonal access policy - Block Exchange ActiveSync on all devices .....	55
Figure 14	Conditonal access policy - Require compliant PCs and mobile devices .....	56
Figure 15	Conditonal access policy - Always require MFA .....	57
Figure 16	Windows 10 and later compliance policy .....	59
Figure 17	Android Compliance policy .....	60
Figure 18	iOS Compliance policy .....	61
Figure 19	Successful Azure sign-in for Mark Mountain .....	62
Figure 20	MFA challenge for Chris .....	63
Figure 21	Login failure.....	63
Figure 22	Applied Contitional Access policies on sign-in event.....	64
Figure 23	Alert of Risky sign-in activity .....	64
Figure 24	Increased user risk .....	65
Figure 25	Forced password change .....	65
Figure 26	Add work account .....	66

Figure 27 Marks new device .....	66
Figure 28 Successful login to Azure portal .....	67
Figure 29 Passed compliance policy .....	67
Figure 30 Default Secure Score .....	71
Figure 31 Secure Score After Policy deployment.....	72
Figure 32 Identity security score improvements .....	73
Figure 33 Microsoft 365 Security recommendation for identities .....	75
Figure 34 Microsoft 365 Security recommendation for endpoints .....	76

## Acronyms

AI	Artificial Intelligence
API	Application programming interface
BYOD	Bring Your Own Device
C&C	Command and Control
CIS	Center for Internet Security
CSF	Cybersecurity Framework
DDoS	Distributed Denial of Service
DoS	Denial of Service
EDR	Endpoint detection and response
IOT	Internet of things
JIT	Just-In-Time
JEA	Just-Enough-Access
MFA	Multifactor Authentication
MS	Microsoft
NIST	National Institute of Standards and Technology
RaMP	Rapid Modernization Plan
SaaS	Software as a Service
TPM	Trusted Platform Module
VM	Virtual Machine
ZT	Zero Trust
ZTA	Zero Trust Architecture



# 1 Introduction

This thesis brings forth the process on building Zero Trust architecture (ZTA) in a modern Microsoft based environment and provides real-life use cases to demonstrate how this Zero Trust improves the capabilities to protect against attacks.

Lack of previous research emphasizes the importance of this study. There are not that many previous studies of this topic that deals with Zero Trust in Microsoft ecosystem as it is fairly recently emerged to the cyber security field, even though the concept of Zero Trust has been for a while now. This research will go through in practice, how it improves security posture of organizations and how to proceed towards Zero Trust security strategy.

In the theoretical part we go through cyber landscape that organizations face these days, we'll discuss about threat actors, attack types, common issues organizations have and fundamentals of administrative and technical cyber security. Theoretical part also covers brief history of Zero Trust and how Microsoft implements Zero Trust Architecture on their ecosystem.

In the technical part we go through on how to plan and build Zero Trust architecture, where to start and what is needed to achieve Zero Trust Compliancy. We will go through this with real-life examples in a test environment built for this research, we'll simulate attacks that organizations usually have to endure. Research also discusses about how overall security level can be measured and improved. Lastly, we will discuss the advantages, challenges and what can be accomplished with Zero Trust Architecture, and which were the results and conclusions of this research.

It is notable that anything in this research can't be stated as absolute truth since Cyber Security field is constantly changing as technology evolves. Everything presented in the research is relying on the information that is present this day.

## **2 Research methodology**

### **2.1 Research Questions**

The main research question on this thesis is defined to answer to following question:

“how does Microsoft Zero Trust architecture enhance one’s capability to protect against cyber-attacks?”

Secondary research question is:

“how does the Zero Trust Architecture improve security posture and how can we measure it?”

As a part of these research questions research was tasked to study about “how does Zero Trust Architecture protect against Brute forcing and leaked credentials?” The answer to this question also serves technical perspective on secondary research question.

### **2.2 Research methods**

This thesis aims to provide intermediate information about Zero Trust Architecture, planning and implementation, the end goal and protection capabilities.

The research has been approached from the perspective of constructive case study, where the central construction has been: “How to mitigate threats and reduce attack surface that involves the regular users”

Research also takes semi quantitative analysis perspective about security posture analysis.

### **2.3 Research Ethics**

This study adheres to ethical research principles and guidelines.

It is important to ensure that any software used in research is properly licensed. This is ensured by obtaining a license for development purposes.

Research is conducted in an ethical manner, with no intentional harm or damage being inflicted on any parties. Also, it is important to respect the privacy and autonomy of others, and to only conduct research within your own environment or with the explicit consent of others.

Plagiarism or the act of intentionally claiming someone else's work as your own, is a major violation of ethics. It is important to properly give credit to the original creators and cite all sources correctly of any source material that is used in this research.

It is also important to evaluate thoroughly the credibility and liability of any sources used in this research. This may involve verifying the expertise of the authors, the reliability of the publication, and the relevance of the information in the research. It is also important to ensure that your research is grounded in established theories and concepts in your field of study.

### **3 Cybersecurity in general**

In this chapter we introduce the different types of malicious actors and the attack vectors that these malicious actors usually try to exploit for financial gain or to gain access to organizations and cause harm, we also go through administrative and technical aspects of cyber security and introduce the fundamentals of cyber security from both viewpoints.

From technical perspective we go through multiple different layers of cyber security ecosystem, introducing different layers where security measurements can and should be implemented.

From the aspect of administrative cyber security, we'll discuss about how it regulates and controls the overall security posture and security measures such as processes and policies, emphasizing that technical security goes hand-in-hand with the administrative cyber security as the controls and security measures are ruled by the administrative level and implemented with technical tools.

#### **3.1 Threat actors**

It is important to know the types and motivations of the attackers since there is many faces of threat actors, basically there is few different types of threat actors, state sponsored actors, hacktivists, insider threats, script kiddies, cyberterrorist, and cyber criminals.

As stated in CrowdStrike's GLOBAL THREAT REPORT from year 2023 It is important to know your adversaries, meaning that organizations should invest in threat intelligence to gain visibility and knowledge about the threat actors who may be targeting you and for what reasons.

Motivations of the threat actors can be equivocal, including nationwide espionage, political or social reasons, causing havoc or financial gain by stealing and selling organization data to third parties such as competitors, nations or other cybercriminal gangs, financial gain also can be acquired by extortion the organization with ransomware. Encyclopædia Britannica. (n.d.).

### **3.1.1 State sponsored actors**

State sponsored actors are individuals who sometimes work in groups. These are funded and supported with technical assistance from a nation-state to advance that nation's particular interests to conduct cyberattacks against other countries, organizations, or individuals. They usually have access to advanced technologies and resources that are not typically available to public. RAND Corporation. (2021).

State sponsored actors work for different motivations, such as espionage, political influence, sabotage, or disruption of critical infrastructure. They often work in coordination with other entities of their represented government, such as intelligence agencies.

### **3.1.2 Hactivist**

Hactivists are individuals or groups that mostly work for "the greater good", causes that they believe that they are in the right side. The motivations are usually political, economic, or social such as embarrassing celebrities, or to highlight current global events, such as human right issues, and provoke organizations to address its vulnerabilities or misdoings, and lastly harassing entities whose ideologies are contradicting their views. IT Pro. (2018, April 23)

Most common ways that hactivist influence on their matter is to cause havoc with Distributed Denial of Service (DDoS) type of attack or try to steal and publicize sensitive information. RAND Corporation. (2021).

### **3.1.3 Insider threats**

Insider threats as threat actors are individuals inside an organization who has user privileges to its resources, systems, or data. These individuals may include employees, contractors, partners, or vendors. Insider threats can cause intentionally or unintentionally, misuse or abuse with their privileges to harm the organization.

Insider threats attack types include multiple shapes, such as theft, sabotage, fraud, espionage, or data breaches, and can cause significant financial, reputational, or operational damage to the organization. Examples of insider threats may include employees stealing sensitive data, IT administrators abusing their privileges, or contractors installing malware on the company's systems. Logically Secure Ltd. (2018, January 17).

For organizations, it is crucial to implement a comprehensive and forward-thinking strategy towards to insider threat management that addresses not only technical and operational controls but also human factors such as employee morale, job satisfaction.

### **3.1.4 Script Kiddies**

Script kiddies are individuals who lack hacking skills and knowledge but use pre-built tools provided on the internet such as automated hacking tools, scripts and exploits to launch attacks against computer systems and networks. According to TechTarget "Script kiddies are typically motivated by simple, personal reasons, to have fun, create chaos, seek attention or take revenge" TechTarget. (n.d.). or to prove their skills to their likeminded entities.

Script kiddies typically do not have any specific target or motive and may randomly scan the internet for vulnerable systems to exploit and launch attacks against the found vulnerabilities.

### **3.1.5 Cyber Criminals**

Individuals or groups who engage in illegal activities are known as cyber criminals, these threat actors operate over the internet with modern technology to commit crimes against individuals, organizations, or governments Cybercriminals are motivated by financial gain. RAND Corporation. (2021). Encyclopædia Britannica. (n.d.).

Cyber crimes can be segregated to own individual categories depending on the techniques and tactics being used.

Cyber espionage is stealing sensitive information, such as information about organizations financial status, its future plans and future developments, as well as government secrets, for political or financial gain.

Identity theft is an act of illegally acquiring an individual's personal info, like their address, name, social security number, and financial details like credit card number or banking information, with the intent to perpetrate fraudulent activities or other unlawful acts using the stolen data. Norwich University Online. (n.d.).

Cyber extortion is used as threatening to publish sensitive content or information of the target, if the target does not play along with the extortionist, it could launch cyberattacks unless requested payment is completed, this attack method is generally known as ransomware attack.

Financial fraud is using technology to commit deceitful activities, like phishing scams, credit card fraud, or money laundering.

Cyber terrorism is using technology to cause physical or psychological harm to individuals or governments, such as by disrupting critical infrastructure or launching cyber attacks against nationally important targets, such as intelligence agencies or federal police. RAND Corporation. (2021).

### **3.2 Common attack techniques**

In this chapter we'll go through the most common attack tactics and techniques that threat actors use against organizations in hope of financial gain, influence or havoc and harm. To understand common attack techniques, it is appropriate to mention Mitre ATT&CK.

Mitre ATT&CK is a "globally-accessible knowledge base of adversary tactics and techniques based on real-world observations". knowledge base is created and maintained by the MITRE Corpora-

tion. It provides a structured framework for understanding, organizing, and communicating information about the known tactics and techniques that threat actors use to compromise systems, networks, and data. Tactics represent the overall goal of an attacker, while techniques describe the specific methods used to achieve that goal. MITRE Corporation. (n.d.)

Moreover, many security vendors are using Mitre ATT&CK mapping within their products to help organizations to understand threats they are undergoing and what are the most uses techniques and tactics against them.

### **3.2.1 Malware based attacks**

Malware meaning Malicious Software is a program, code or script that is designed to cause any kind of harm in the destination. Malware is the most used type of an attack, this is mostly because due to the fact that malware is an umbrella term that describes any malicious program or code Malwarebytes. (n.d.). Such as ransomware, spyware, adware, worms, trojans, exploits, keyloggers etc. Threat actors typically spread malwares via malicious files from websites or emails.

CrowdStrike. (n.d.). Hub International. (2022, January 18)

### **3.2.2 Denial of service attack**

A Denial-of-Service (DoS) attacks targets to disrupt or disable the normal functioning of a computer network, application, system, or website by flooding it with traffic, requests, or data. This overloads the system, making it incapable of respond to requests that are sent to the system, and therefore denying access to authorized users.

DoS attacks can be carried out by a single attacker using a single device or through a coordinated effort involving multiple devices commonly referred as botnet, this attack method that uses multiple devices is known as a distributed denial-of-service (DDoS) attack, which is more likely to be used since this attack method is harder to stop because the harmful traffic comes from various sources.

### **3.2.3 Phishing**

Phishing is a type of cyberattack that uses communication technology such as email, SMS, phone, or social media to fool the users to send sensitive or personal information, such as banking information, credit card numbers, or login credentials. Depending on the stolen information, threat actors may use this information for financial gain or as a part of a larger attack scheme.

In a typical attack that uses phishing method, a threat actor sends a deceptive email that seems to originate from a legitimate source, such as insurance company, and requests the email recipient to access a website link and enter their login credentials in a counterfeit website. CrowdStrike. (n.d.).

### **3.2.4 Social engineering**

Social engineering is an attack technique used by threat actors to influence individuals into giving confidential information or to execute actions that could pose a threat to security of a network or system within the organization or in private life. Social engineering attacks exploit human psychology, rather than relying on technical weaknesses.

Social engineering is used in many different attack schemes, such as pretexting, phishing emails and baiting.

The effectiveness of social engineering attacks comes from their ability to take advantage of the vulnerabilities inherent in human nature, such as trust, fear, curiosity, or ignorance. These types of attacks are also more harder to detect by the security software and systems since the attacks does not exploit technical weaknesses.

### **3.2.5 Zero-day exploits**

Zero-day exploits refers to a newly discovered vulnerability in software or hardware that are not yet recognized by the vendor or manufacturer, nor its developers and these vulnerabilities do not have any available patches or updates to fix them. Logically Secure Ltd. (2018, January 17). Threat actors can leverage zero-day vulnerabilities to gain unauthorized access to systems, snatch sensitive data, or cause harm or system disruption.



Zero-day exploits are highly valuable to threat actors because they can bypass existing security measures and detection systems, allowing them to carry out attacks without being detected. Once a zero-day exploit is discovered, attackers can use it to compromise multiple systems until a patch is released. Norton. (n.d.)

### **3.3 Common issues within organizations**

The common issues that organizations may have, and which are used directly or indirectly in attacks are presented in this chapter. Security teams are facing formidable challenges in today's threat landscape, as risks are widespread and threat actors are continuously evolving their tactics and techniques.

#### **3.3.1 User awareness**

User awareness training is critical to arrange in constant manner, training should include security training and practical testing, such as phishing email campaigns, fundamentals of attack vectors and threat actors and day to day procedures on when and where to report anomalies.

#### **3.3.2 User and Endpoint protection**

Lack of user and endpoint related security measures, such as absence of endpoint protection, and Endpoint Detection and Response (EDR) systems, poor security measures on email handling, which allows malicious email through and bad password hygiene and policies, which allows weak passwords, reusing of passwords, and absence of secure password vault.

#### **3.3.3 Misconfiguration**

Misconfigurations may happen due to lack of visibility and understanding of systems and software, unqualified employees among other reasons, these misconfigurations may allow threat actors to infiltrate into the systems and exploit them.

Typical misconfigurations are weak or default passwords, unpatched or obsolete software which are not updated automatically or under influence of update procedures, misconfigured firewalls

that allow unnecessary ports and protocols through, improper access control that could allow unauthorized access that leads to data breaches, unsecured cloud services, including storage, databases, or Application programming interface (API), can lead to unauthorized access, data exposure, or worst case scenario complete takeover of cloud based systems. BrightSec. (2021, February 22).

#### **3.3.4 Privileges**

Many security incidents are related to user privileges either that regular users have administrator privileges to their local endpoints, which allows threat actors to arbitrarily run malicious actions on the endpoint if it's breached or that administrator privileges are too broad, meaning that same administrative account can be used to access all the assets in the organization, including high risk devices such as domain controllers and databases.

#### **3.3.5 Vulnerability management**

Outdated operating systems and other software, may include vulnerabilities that threat actors could exploit to gain privileged access, move laterally, steal data, or disrupt services. If these systems are easily accessed by for example directly from the internet it is most likely that these vulnerabilities are targeted. To minimize the vulnerabilities organizations should conduct vulnerability scanning across the environment and have patch management processes set, also all obsolete systems should be replaced with up-to-date equipment.

With continuously performed vulnerability and network scanning organizations can address security gaps previously mentioned such as default password misconfigurations, outdated systems, vulnerable software versions as well as rogue devices that organizations are not aware of, these devices may be unpatched containing vulnerabilities and weaknesses and possibly are out of reach of the security personnel.

### 3.4 Administrative Cyber Security

Administrative cybersecurity utilizes a framework of policies, procedures, and practices that organizations adopt to secure their ecosystem against potential cyber threats. It involves the management of people, processes, and technology to ensure the confidentiality, integrity, and availability of data. Firewall Times. (n.d.).

These frameworks are developed for organizations to implement effective administrative cybersecurity controls. The most common frameworks in use are introduced below.

National Institute of Standards and Technology (NIST) is a framework that serves as a comprehensive guide for organizations to effectively govern and mitigate cybersecurity risks. NIST framework approaches risk reduction in five stages including Identify, Protect, Detect, Respond, and Recover.

ISO 27001 framework is a widely acknowledged standard that presents a structured methodology for managing confidential information. It consists of a large variety of controls that organizations can implement to protect their ecosystem. International Organization for Standardization. (2013)

CIS Controls, developed by the Center for Internet Security (CIS), furnish organizations with a prioritized list of cybersecurity measures to secure against prevalent cyber threats. Center for Internet Security. (n.d.).

Administrative cybersecurity controls can be categorized into three distinct groups, technical controls, physical controls, and administrative controls. The focus of administrative controls is on the people and processes involved in the management and operation of information systems. International Conference on Information. (2016).

Overall, administrative cybersecurity should be important aspect in organization's overall cybersecurity strategy, as implementation of effective administrative controls is essential in mitigating against cyber threats.

## **3.5 Administrative security measurements**

### **3.5.1 Risk Assessment**

Risk Assessment should always be considered when planning on cyber security. Organizations should conduct risk assessments to identify probable threats and vulnerabilities in their infrastructure. This involves identifying potential attack vectors and the probability of an attack that is executed successfully, as well as the impact potential of such an attack. Risk Assessment should also consider the potential cost of an attack and related to Risk Assessment organizations should conduct business continuity plan for worst case scenarios.

Risk assessments should be conducted each time something changes on the environment, for example if new technologies intended to be implemented. The scope of risk assessments is vast, and the depth may vary depending on the use case, but carefully prepared risk assessment template built in accordance with good processes is the key feature so it can be implemented in use no matter how vast the scope is. Hyperproof. (n.d.).

### **3.5.2 Employee Awareness**

Employee training is essential for maintaining understanding of overall cyber security and how cyber security is treated in the organization, employee awareness also should empathize that cyber security is everyone's concern as it's said that "Cybersecurity is as strong as it weakest link", meaning that in many security breaches the weakest link is the human, which causes the incident directly or indirectly.

Employees should be trained on the best practices of network, endpoint, identity and physical security. Teaching the employees about attack vector and the tools and procedures to protect against attacks is essential. Employees should be aware of malicious actors' tactics and techniques against them, like social engineering, brute forcing, and phishing attacks. Also, it is crucial to teach how to recognize any attack attempts against the employee or the organization. They should also be trained to acknowledge of the potential risks of using public Wi-Fi, downloading attachments from unknown sources, how to manage passwords safely, risks of phishing emails meaning not clicking on suspicious links and other risk factors inside and outside the company network.

What comes to physical security, employees should be trained such as not sharing their access credentials, always report suspicious activities, and following security protocols when accessing physical facilities. Additionally, regarding to any aspect of cyber security employees should be made aware of the potential risks of using personal devices for work-related activities.

### **3.5.3 Incident Response**

It is necessary for organizations to create a well-defined incident response plan to properly respond and react to any security related anomalies. The plan should encompass guidelines for detecting and reporting an anomaly, incident, or breach, isolating affected assets, and restoring normal operations. IBM. (n.d.).

For each incident there should be a procedure about how the matter should be dealt with, formal incident response plan should cover following steps.

Initial Response phase, Identify the anomaly and its scope, notify the incident response team or whoever is responsible of incident handling, secure the affected systems or devices.

Investigation phase, conduct a detailed investigation of the incident and identify the root cause of the incident and collect required evidence for forensic analysis. It is also important to determine if the incident is real or false.

Containment phase, Isolate the infected appliance to minimize further damage and to stop the incident from spreading. Implement temporary fixes to reduce the incident impact. Review security controls and implement additional measures if necessary.

Analysis phase, analyze the evidence collected during the investigation. Assess the scope of the incident and its impact on the organization. Identify the vulnerabilities that led to the incident.

Remediation phase, develop a plan to remediate the incident and prevent future incidents. Implement permanent fixes to address the vulnerabilities identified during the analysis. After an incident, it is advisable to conduct a comprehensive review to extract insights, identify areas for improvement, and enhance the incident response plan.

Recovery phase, restore infected systems to their previous state before the incident, verify that the systems are not malfunctioning and are safe to use.

Reporting phase, document the incident and the response actions. Notify appropriate parties, such as customers, partners, shareholders, and official authority, if required by law or regulation. Share the lessons learned and the implemented improvements to the incident response plan.

### **3.6 Technical Cyber Security**

Technical cybersecurity refers to the use of technology to protect an organization's ecosystem against cyber threats. It includes the implementation of hardware, software, and network-related controls to prevent unauthorized access, detect and respond to cyberattacks, and ensure the confidentiality, integrity, and availability of data. Varonis. (n.d.).

Technical cybersecurity controls can be implemented at various layers within an organization's ecosystem. In this research we'll discuss about following layers, identity layer, Network layer, Endpoint layer, Application layer, and Data layer.

Overall, the layers where protection is implemented can differ within each organization depending on the needs, resources, and the specific threats they face. The implementation of effective technical cybersecurity controls at each layer is crucial to the organization's overall security posture and should be complemented by administrative and physical controls to provide a holistic approach to cybersecurity. CISO Portal. (n.d.).

#### **3.6.1 Endpoint security**

Endpoint layer security refers to the process of securing the endpoint devices, including laptops, desktops, smartphones, and tablets, that are linked to the organization's network. The aim is to

protect these devices from various types of cyber threats such as malware, viruses, spyware, among other types of attacks that may compromise sensitive data. In this chapter we go through some key points to focus on when it comes to endpoint security for organizations.

Anti-Malware Protection should cover all endpoint devices, these devices should be protected with an effective anti-malware solution that detect and prevent malware from infecting the device. IBM. (n.d.). The solution should include real-time monitoring and threat intelligence capabilities. In addition to traditional malware protection organizations should extend the protection with EDR software to gain better visibility and means to mitigate threats. Fortinet. (n.d.).

Application firewall protects the device from unauthorized network access and malicious traffic. Properly configured firewall should block all incoming traffic except for those that are required for business purposes.

Patch management is crucial to regularly deploying updates for software and firmware on endpoint devices to maintain the security of the devices. Unpatched software causes vulnerabilities and malicious actors can in some circumstances exploit these vulnerabilities. Organizations should have a formal patch management process to assure that all devices are kept up to date with the latest available software and firmware versions.

Endpoint devices should be fully encrypted to secure the confidentiality and integrity of data saved in the disk of the device. Full-disk encryption is recommended to protect data at rest. Encryption is also essential against theft or loss of endpoint device as it prevents the access to the data saved in the endpoint's disk.

Access to endpoint devices should be limited to authorized personnel. Organizations should implement strong password policies, MFA, and if feasible access control policies that are role-based to ensure that only authorized personnel can access the devices.

Mobile Device Management (MDM) solution should be implemented to allow centralized management for mobile devices that are used in the organization's ecosystem. The MDM solution should

include features such as remote wipe, device tracking, and application control to secure the device and the data it contains.

### **3.6.2 Identity security**

In Identity security layer the measures are taken to protect an organization's digital identities and the personal information of its employees and customers from unauthorized access, abuse, or theft. Here are some key points to focus on when it comes to identity security for organizations. SailPoint. (n.d.).

Identity and Access Management (IAM) should be used for managing identities and their permissions to resources within an organization. It involves identifying users, authenticating their identity, and regarding users roles and responsibilities authorizing their permissions to systems, applications and other organizations resources. Implementing IAM solution is essential for identity security.

Passwords are a primary means of authentication for most organizations, therefore password policies should require strong passwords, password expiration, and MFA whenever possible. MFA appends additional security control by requesting users to prove their identity with an additional authentication method like biometric, SMS verification, or hardware token.

Privileged Access Management (PAM) is a solution that can monitor, control and restricts permissions to sensitive systems and data to personnel that are authorized to view the content in question. It involves managing and monitoring privileged accounts and providing just-in-time access when needed.

Organizations should constantly monitor and regularly audit their identity and access management systems to ensure that wanted controls are met and that there are no security gaps. They should also monitor user activity and access logs for any signs of suspicious activity.

In summary, it's important to secure organization's digital identities and personal information from unauthorized access, theft, or misuse. By focusing on identity and access management, password policies, privileged access management, training and awareness, auditing and monitoring,



organizations have a better chance to protect their digital identities and minimize the likeliness of identity-related cyber attack.

### **3.6.3 Network security**

Network security layer focuses to the practice of protecting organizations networks from unwanted access, theft, damage, or misuse. It involves implementing controls and procedures to prevent threats such as cyber attacks, viruses, and malware, and also secure the confidentiality, integrity, and availability of data transmitted over the network. In this chapter we go through some key points that are the backbone in network security for organizations.

Organizations should implement encryption technologies like SSL and TLS to secure data in transit and at rest encryption for sensitive data stored on servers and other storage devices. With data encryption organizations are converting data into a format that can only accessed with decryption key.

An approach to limit the propagation of a possible breach is through network segmentation, which are measures to divide the network to smaller network divisions. By segmenting the organizations networks, it's possible to restrict access for critical resources, make lateral movement harder, reduce the impact of a potential attack, and simplify network management.

Patch Management meaning regularly updating software and firmware on network devices is critical for maintaining the security of the network. Organizations should have a formal patch management process to make sure that all network devices are running the latest software and firmware versions.

Network protection appliances such Web Application Firewall (WAF) and Intrusion Prevention system (IPS) are effective to detect and protect against attacks. IBM. (n.d.). With WAF Organizations are able to reduce and block malicious traffic such as cross site scripting and SQL injections into their public services and applications. IPS on a network layer helps to monitor, detect, and protect against anomalies in the network traffic with IPS it's possible to protect against multiple different threats within the company's network. Cloudflare. (n.d.).

### 3.6.4 Physical security

Physical security layer is often forgotten when considering cyber security, it refers to the actions implemented to protect an organization's people, property, and physical assets from unauthorized access, theft, damage, or exploitation. In the context of cybersecurity, physical security should be part in an overall security strategy of an organization because it provides the first line of defense against physical attacks that can lead to cybersecurity breaches. In this chapter we go through basics of physical security for organizations to consider in the context of cybersecurity. CSO Online. (n.d.).

Access to an organization's physical facilities, including factories, headquarters, branch offices, stores and other locations which are used and connected to the company infrastructure should be limited to authorized personnel. To control the access there is vast variety of measures that can include keycards, biometric authentication, or security personnel at entrances.

Organizations should install monitoring and surveillance systems to detect and prevent unauthorized access to their physical facilities. This can include video surveillance, motion sensors, and intrusion detection systems. These systems can alert security personnel or trigger alarms if they detect unauthorized access.

Physical barriers could be applied to complicate unauthorized access to an organization's physical facilities. This can include security gates, fences, and walls. Barriers created difficulties for potential attackers trying to breach an organization's physical assets.

Environmental controls are important to physical assets within an organizations facilities from damage. This can include measures such as temperature and humidity control to protect sensitive equipment or backup power systems to prevent service disruptions.

In summary, physical layer is a important part of the organization's cyber security strategy. By focusing on access control, monitoring and surveillance, physical barriers, environmental controls, employee awareness, and incident response, organizations can provide better protection their physical assets from potential threats and prevent physical attacks that can lead to cybersecurity breaches.

### 3.6.5 Application Security

The application security layer is an essential component of technical cybersecurity, as it involves protecting software applications from cyber threats that can exploit vulnerabilities within the code or design of the application. This layer focuses on implementing measures to ensure that applications are developed securely and that vulnerabilities are identified and remediated.

To implement effective application security measures, technical cybersecurity controls can be deployed at various points within an organization's software development lifecycle.

Developers should be trained for coding practices that are secure to ensure that applications are developed with security focused mindset to prevent misconfigurations in the software that allows malicious actors easily to abuse the software.

Vulnerability or penetration testing should be done to recognize potential security risks or weaknesses within applications and mitigate these before malicious actors are able to exploit them. For the penetration or vulnerability testing it should consider the software as well as the host system that provides the platform for the software.

Applications and their corresponding Application Programming Interfaces (APIs) should be developed with built-in authentication and access control mechanisms to limit access to confidential data or critical functions.

Input validation and output encoding should be addressed to prevent attackers from exploiting common vulnerabilities such as injection attacks.

Regular patching of applications should be conducted to prevent exploitation of known vulnerabilities and decrease the overall risk of exploitation.

### **3.6.6 Data Security**

Data security involves protecting sensitive data from unauthorized access, theft, and exposure. This layer focuses on implementing measures to ensure that data is encrypted, securely stored, and only accessible by authorized users.

To keep the data secured, it is recommended to implement data encryption technologies for both data at rest and data in transit and limit access to sensitive data solely to authorized users or applications.

Organizations should take backups regularly from sensitive data and process of backup recovery should be in place and tested regularly to make sure that data from backups are restored correctly in case of data loss or corruption for example in a case of ransomware or injection attack.

Data classification policies should be implemented to confirm identification and appropriate handling of sensitive data. Data classification should also use to plan access control policies and prevent unauthorized identities to access classified data.

To secure an organization's sensitive data, it is recommended to deploy data loss prevention (DLP) technologies that can actively monitor and prevent data leakage or theft from the organization's systems. This includes cases like insider threats and data leaks.

## **4 Zero Trust**

This chapter provides a deep dive into the Zero Trust concept, including its origins, its definition, and its application through the implementation of Zero Trust Architecture. The chapter clarifies how Zero Trust Architecture builds upon existing security controls and procedures through the integration of additional technical measures to strengthen the organization's security posture.

### **4.1 Formation of Zero Trust**

Zero Trust architecture (ZTA) is a security model that assumes that all devices and users are untrusted by default and requires strict verification before granting access to resources. The concept

of Zero Trust has its roots in the early days of networking, when the perimeter-based security model was prevalent. This model relied on the idea of a network perimeter that was secure and trusted, with all devices and users inside the perimeter being considered trusted and all devices and users outside the perimeter being considered untrusted. National Institute of Standards and Technology. (2020).

In the late 2000s, as the nature of networks and cybersecurity threats evolved, the perimeter-based security model began to be seen as inadequate. The increasing use of cloud services, remote work, and the Internet of Things (IoT) made it more difficult to define a clear perimeter around a network. As a result, the Zero Trust architecture emerged as a way to address these challenges and provide a more robust and flexible approach to security. TechTarget. (2021, June).

The National Institute of Standards and Technology (NIST) had significant role in the development and promotion of the Zero Trust security model. In 2018, NIST released Special Publication 800-207, "Zero Trust Architecture", updated in 2020, which helps organizations to implement a Zero Trust architecture. This publication outlines the fundamentals of Zero Trust, describes the components of a Zero Trust system, and provides recommendations for implementing and maintaining a Zero Trust architecture.

The Zero Trust architecture has been further developed and refined over the years, and it is now seen as a key component of modern cybersecurity strategies. It has been adopted by a wide range of organizations in different sectors, and it is commonly noted as enhancing protection against modern threats like advanced persistent threats (APTs), insider threats, and ransomware attacks.

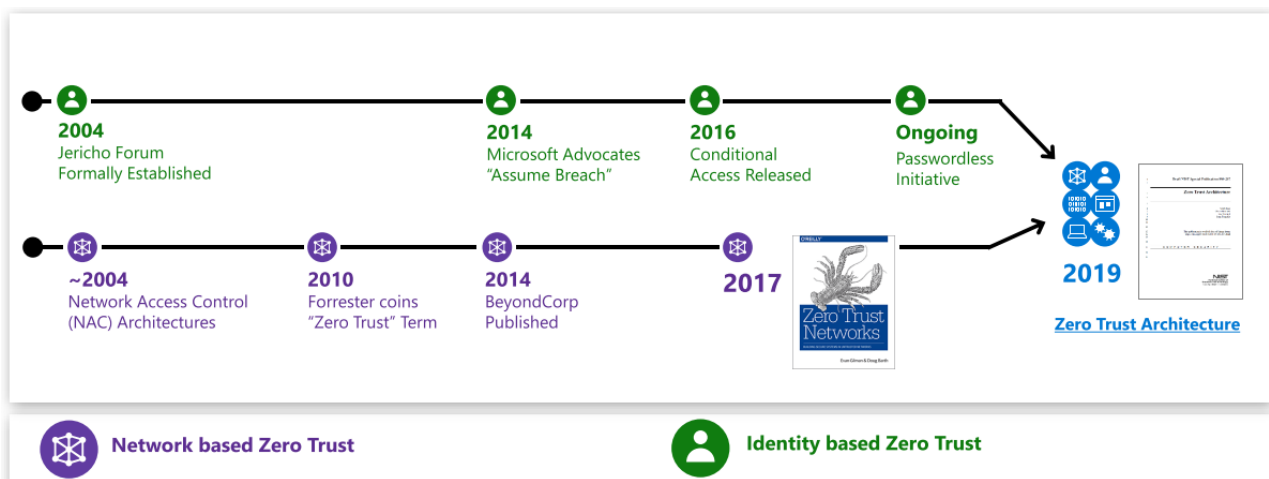


Figure 1: Zero Trust Timeline. Microsoft. (2022). Microsoft Security Virtual Training Day: Zero Trust.

## 4.2 Tenets of Zero Trust

The Tenets of Zero Trust are a set of principles that guide the design and implementation of a Zero Trust security model it is notable that the tenets are not technology agnostic. National Institute of Standards and Technology. (2020) According to the NIST Special Publication 800-207, the Tenets of Zero Trust are as follows:

### **1. All data sources and computing services are considered resources.**

A network can consist of various device classes, including small footprint devices that send data, SaaS, systems for sending instructions, and more. Personal devices may also be classified as resources if they can access enterprise-owned resources.

### **2. All communication is secured regardless of network location.**

Location does not imply trust, even for assets located on enterprise-owned network infrastructure. Access requests from such devices must meet the same security requirements as those from any other non-enterprise-owned network. Trust should not be granted automatically based on network infrastructure. Communication should always be secure, protect confidentiality and integrity, and provide source authentication.

### **3. Access to individual enterprise resources is granted on a per-session basis.**

Access is granted based on trust evaluation and with minimum privileges required. This may not require recent authentication before each transaction. Access to one resource does not automatically grant access to others.

### **4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.**

Organizations implement zero trust by defining their resources, members, and their access needs.

Client identity includes user accounts, attributes, or artifacts to authenticate automated tasks. Asset state includes device characteristics, time/date of request, previous behavior, and installed credentials. Policy is the set of access rules based on these attributes and environmental factors like requestor network location and time. These policies are based on business needs and acceptable risk levels. Least privilege principles are applied to restrict resource visibility and accessibility based on the sensitivity of the resource/data.

**5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.**

Assets are not automatically trusted in a ZTA. The enterprise must evaluate the security posture of assets before granting resource access. A continuous monitoring system should be implemented to detect vulnerabilities and apply patches/fixes. Devices that are not managed by the enterprise or have known vulnerabilities may be denied access to enterprise resources. Personally owned devices may also have restricted access to certain resources. A monitoring and reporting system is essential for maintaining the security of enterprise resources.

**6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.**

In ZTA, access, threat assessment, adaptation, and trust evaluation are constant cycles. An enterprise implementing ZTA requires ICAM and asset management systems and may use MFA. Continuous monitoring with reauthentication and reauthorization occurs throughout user transactions, as defined by policy for security, availability, usability, and cost-efficiency.

**7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.**

An enterprise should collect and analyze data on asset security, network traffic, and access requests to enhance policy creation and enforcement. This data can also provide context for access requests.

As of the present day, a multitude of service providers have incorporated their distinct implementations of the Zero Trust framework in their software and services. Prominently, Cisco has integrated Duo, Trend Micro offers Zero Trust Secure Access, and Microsoft highlights its Zero Trust Architecture on Azure and Microsoft 365 platforms, which is the primary focus of this research.

### 4.3 Microsoft's implementation of Zero Trust

Zero Trust is a security strategy that emphasizes a holistic approach to designing the infrastructure and its components. It is not a product or service, but rather a guiding principle that informs a range of individual security principles. At its core, Zero Trust operates under the fundamental principle of "never trust, always verify," which underscores the need for continuous security checks and verifications throughout the system. Microsoft's Zero Trust principles Microsoft. (n.d.) is as follows:

*Verify explicitly*

*"Always authenticate and authorize based on all available data points."*

*Use least privilege access*

*"Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection."*

*Assume breach*

*" - Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses."*



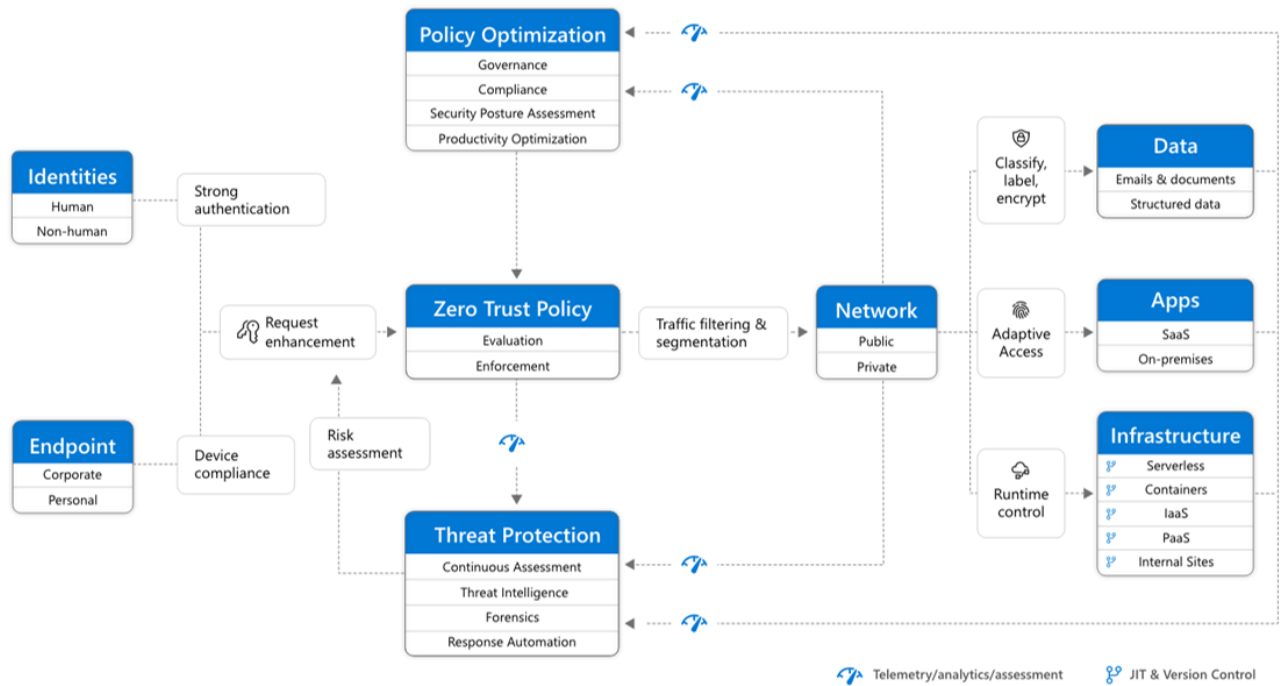


Figure 2 Overview Of Zero Trust Architecture

Microsoft. (n.d.). Zero Trust security model. [Diagram]. Microsoft 365.

<https://learn.microsoft.com/en-us/microsoft-365/media/zero-trust/zero-trust-architecture.png?view=o365-worldwide#lightbox>

Microsoft has implemented ZTA as a means of secure six crucial layers within modern organizations ecosystem. These layers encompass a range of entities, including Identity, Endpoints, Applications, Networks, Data, and Infrastructure. In the following chapters, we will delve deeper into these entities, exploring their significance and how ZTA can enhance their level of protection.

This research focuses on Endpoint and Identity security by following the Zero Trust principles and implementing Zero Trust policies and controls to these layers in the Zero Trust Architecture. Other layers are out of scope and are only presented in theoretical part of this research.

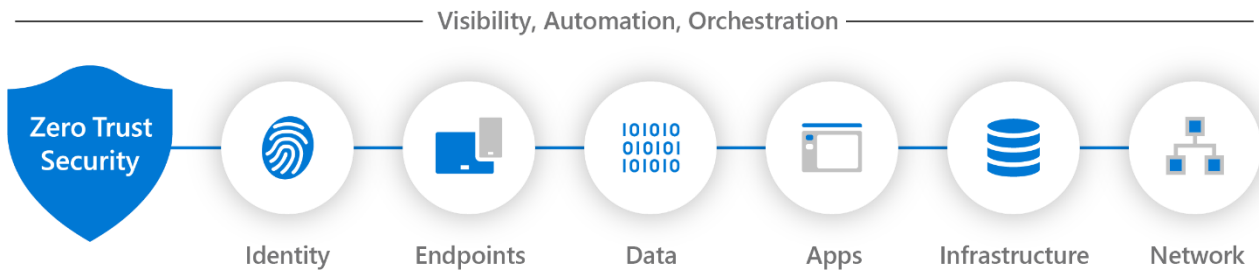


Figure 3 Zero Trust layers Microsoft. (n.d.). Diagram: Zero Trust security elements.

### 4.3.1 Identity

Identity refers to the unique characteristics that distinguish an individual or a device in a network. In a Zero Trust security architecture, identity is a crucial part of granting access to the company's resources and confirming the authenticity of devices and users.

In a Zero Trust architecture, all users, devices, and resources are held as untrusted by default. Access to company resources is permitted if the required conditions are fulfilled that are enforced through authentication and authorization processes. These processes check the authenticity of the user or device requesting access and determine whether they are authorized to access the requested resources.

Identity verification can be based on multiple conditions, such as username and password, biometric authentication, or device attributes. The goal of identity verification is to make certain that only approved devices and users are granted access to an organization's network and its assets. Identity is continuously verified and re-verified as users and devices move back and forth between company's network and access different resources. Continuous verification is an effective measure to mitigate security risks by preventing unauthorized access and minimizing the occurrence of security-related incidents like data breaches and leaks. Microsoft. (n.d.)

In a Zero Trust security architecture, identity serves as a critical component by validating the legitimacy of users and devices and managing resource accessibility.

### 4.3.2 Endpoints

Endpoints refer to the devices that connect to the company network, such as laptops, smartphones, tablets, and servers. In a Zero Trust security model, endpoints are in determining access to resources and enforcing security policies. Microsoft. (n.d.)

In a Zero Trust architecture, all endpoints are treated as untrusted by default and are continuously verified to ensure that they are secure and compliant with security policies. The constant verification process helps to decrease the likelihood of unauthorized access and minimize the risk of security breaches.

Zero Trust architecture policies may force requirements for endpoint devices to ensure their security and compliance. These requirements may contain various measures, including presence of antivirus software, EDR system, software firewalls, and up-to-date operating system.

In addition to securing the endpoints themselves, a Zero Trust architecture also involves securing the communication between endpoints and the network. This can be accomplished by implementing techniques such as blocking legacy protocols, adding encryption to communication channels, and with virtual private networks (VPN).

Overall, endpoints are in a key role in the ZTA, as they are the entry points through which users access the network and its resources. Ensuring the security and compliance of endpoints is essential for maintaining the security of the entire network.

### 4.3.3 Applications

To fully leverage the advantages of cloud apps and services, organizations should seek a delicate harmony between providing access and maintaining control to secure vital data obtained through applications and APIs. Microsoft. (n.d.)

The Zero Trust model for application facilitates organizations with six security measures to secure apps and the data moving in, out and within the application.

Monitor cloud app activities and data with APIs, use cloud app APIs to prevent threats and anomalies as they occur in organization environment with real-time monitoring and alerting.

Discover and control shadow IT usage, Identify app usage patterns, assess risk levels, prevent data leaks, and limit access to regulated data.

Protect sensitive information with policies: Create policies to automatically protect sensitive information and activities, including access, activity, anomaly detection, app discovery, file policy, cloud discovery anomaly detection, and session policies.

Deploy adaptive access and session controls, ensure that applications use least-privileged access and if session risk changes dynamically adapt and restrict access to prevent leaks and breaches as soon as incident is ongoing.

Strengthen protection against cyber threats, use tools like UEBA, anomaly detection, malware protection, OAuth app protection, incident investigation, and remediation to target security anomalies and protect against threats.

Defender for Cloud Apps helps on evaluation of the security posture and compliance level in the public cloud platforms, this is essential to enhance the security posture for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) services.

#### **4.3.4 Network**

The Zero Trust model has three primary objectives in securing networks. Be prepared to handle attacks before they occur, minimize the scope and speed of any damage that does occur, and enhance the difficulty of compromising your cloud presence.

Basic networking principles also applies in Zero Trust Network architecture, this contains traffic Encryption, network segmentation, constant monitoring, real-time threat protection and analytics. Microsoft. (n.d.)

Encrypting network data between entity communication so the threat actors are unable to monitor or catch credentials passed on the network.

Segment the network, create segments of subnets with unique access rights, this greatly prevents potential lateral movement, meaning that if a malicious actor gains access to company network it will be less likely to access multiple resources and causing vast amount of harm.

Monitor network traffic from anomalies, such as connections to C&C server, connections from non-typical geographical locations based on these conditions raise flags/alerts/mitigate and possible malicious URL and DNS queries.

Real-time threat protection and analytics, stop harmful files passed around the network, prevent connection towards harmful websites and servers.

#### **4.3.5 Company Data**

Data classification and labeling are important steps in protecting company data. Organizations should classify data based on its sensitivity and apply appropriate security controls to protect it. Data labeling can help identify sensitive data and ensure that it is handled appropriately.

Information protection involves implementing access controls and encryption to protect sensitive data. It also includes monitoring and auditing data usage to ensure compliance with policies and regulations.

DLP is a crucial aspect of information security. DLP policies are to monitor data usage, data leakage and prevent unauthorized data access, theft, or loss.

Insider risk management involves identifying and mitigating risks posed by insiders, such as employees or contractors. This can include implementing controls to decline unauthorized access, monitoring and auditing user activity, and training employees on security best practices.

Data governance encompasses the development and implementation of comprehensive policies and procedures to effectively manage data across its entire lifecycle. Effective data governance requires establishing clear data ownership and roles, defining data retention policies, and implementing robust controls to ensure regulatory compliance throughout the data lifecycle.

Overall, protecting data, it requires a comprehensive approach that includes data classification, information protection, DLP, insider risk management, and data governance. Organizations should identify and classify their data with the help of automation, implement appropriate security controls, and continuously monitor their data for potential security incidents.

#### **4.3.6 Infrastructure**

The infrastructure layer comprises a range of critical components, including servers, databases, and other computing resources that support an organization's operations.

Microsoft's ZTA approach to the infrastructure layer involves implementing a range of security controls and best practices. Before moving into Zero Trust infrastructure must fulfill a certain baseline, including access control, data encryption, network flow restrictions, security team visibility, monitoring, anti-malware, and vulnerability scanning, in compliance with organizational guidelines. Microsoft. (n.d.)

Zero Trust implementation requires undertaking several tasks, including monitoring workloads for anomalous activity, assigning a consistent application identity to each workload, employing Just-In-Time access for human users, blocking unapproved deployments, facilitating granular visibility and access control, and segmenting user and resource access for each workload. These tasks are fundamental to establish a robust Zero Trust framework that strengthens an organization's security posture on infrastructure layer.

### **4.3.7 Visibility, Automation Orchestration**

Microsoft's Zero Trust framework incorporates visibility, automation, and orchestration capabilities to enhance security. These capabilities enable real-time monitoring of security events, automated responses to detected threats, and streamlined management of security policies and access controls. Microsoft. (n.d.)

The implementation of a comprehensive Zero Trust framework across identities, endpoints, data, apps, infrastructure, and network increases visibility and provides better data for trust decisions. However, this also increases the number of security incidents that need to be addressed, potentially leading to alert fatigue and missed critical alerts. To better defend against threats and validate trust, an integrated capability is needed to manage the influx of data generated by each area. This capability should include the ability to detect, investigate, respond, hunt, assess vulnerabilities, and provide threat analytics, with a focus on preventing or blocking events across all layers.

## **4.4 Environment**

To create a suitable environment for testing and building Zero Trust Architecture, this research leveraged an Azure tenant with an E5 license for developers and a trial period of Microsoft Defender for Endpoints. These licenses enabled the research to fully implement a Zero Trust compliant environment. To evaluate the efficiency of Zero Trust, two virtual Windows 10 desktops were created and joined to Azure Active Directory and Intune, along with few Azure AD users. These virtual machines and users were subjected to security, compliance, and conditional access policies,

demonstrating the efficacy of the Zero Trust architecture.

### Products from Microsoft and others (2)



Product name ↑	
<input type="checkbox"/>	 Microsoft 365 E5 Developer (ilman Windowsia ja puhelinneuvotteluja), kokeiluversio
<input type="checkbox"/>	 Microsoft Defender for Endpoint P2 Web Trial

Figure 4 Licenses used in the research

## 4.5 Assets

For the purpose of this thesis, two virtual desktops have been created on my personal computer using the VirtualBox software. These desktops have been designated with the names "Chris-PC" and "Mark-PC", which are reflective of their assigned users. Both virtual machines run the Windows 10 22H2 version and have identical settings, configurations, and installations. Additionally, devices have been enrolled to Intune, which has been specifically set up for the purpose of this research.

## 4.6 Identities

For the purpose of this thesis, two high-level target identities have been created: Chris Candy and Mark Mountain. Chris Candy is designated as the CISO, while Mark Mountain is designated as the CIO.

These identities have been used to evaluate the policies and overall level of security within the research. The identities have been configured to use Conditional Access policies, which are presented in detail in Chapter 6. In Chapter 7, the same identities have been used to demonstrate the behavior of Zero Trust policies when targeted by various types of attacks.



## 4.7 Baseline settings

Before organizations should pursue Zero Trust compliance the basic security level of the tenant should be implemented, to reach certain level of maturity. This research does not go that deeply into the basic configurations that should be done to the tenant before appending the Zero Trust architecture, but similar settings presented here are covered in chapter 5 where the conditional access and compliance policy are built. Some of basic settings that should be implement are briefly introduced below.

Password policies help to enforce strong password requirements, such as minimum length, complexity, and expiration time, to prevent unauthorized access and minimize the risk of password-related attacks such as password spraying and brute-force attacks.

MFA policies requires users to authenticate using two or more factors, which could include a password or a verification code, in order to gain systems and other resources. This helps to prevent unauthorized access, even in a such case where the user's password is leaked to the threat actor.

Conditional access policies allow organizations to define access controls based on specific conditions, such as the user's location, device type, or risk level. This helps to ensure that users are accessing resources and data from trusted devices and locations, mitigating the risk of unauthorized access.

Device compliance policies allow organizations to effectively manage and secure devices that access resources and data within Azure AD and Microsoft 365. This includes enforcing policies such as device encryption, screen lock, and device health checks to ensure that devices meet the organization's security requirements.

Later on, this research we will discuss more about the baseline benchmark tools that you can use to implement Basic and advanced security settings to your environment.

In this research the baseline security settings were kept minimal, and the focus was on Zero Trust related policies to see the how these policies enhance the level of security alone.

## 5 Heading towards Zero Trust Architecture

When an organization's environment maturity level is considered adequate, it can begin the process of transitioning towards Zero Trust Architecture. However, like any major process, a thorough and comprehensive plan should be developed before implementation. In this chapter, we will discuss the planning phase of this process, including choosing an appropriate deployment plan and outlining the key steps involved in the implementation phase.

### 5.1 Planning Zero Trust Architecture

The Microsoft Zero Trust architecture is very vast and there are multiple layers where Zero Trust controls can be implemented as previously mentioned, these layers include Identity, Endpoints, Applications, Networks, Data, and Infrastructure. The focus in this research is the identity and endpoints, other layers are only discussed, and are left out from the implementation phase.

In Microsoft Zero Trust architecture there is also multiple different deployment plans on how you can start implementing controls to approach Zero Trust compliance, organizations should consider factors such as company size, time and resources to choose the correct plan for their path. This research follows Zero Trust Rapid Modernization Plan (RaMP). This plan allows us to rapidly adopt Zero Trust principles to our Identities and Endpoints, also the RaMP covers Apps and Networks but are out of scope from this research. Microsoft. (n.d.)

It is important to know your infrastructure and plan the depth of Zero Trust Architecture organization is able to implement. Some organizations may not have all the components present in their environment, so some rules and policies cannot be implemented, or it would not be unnecessary, also it should be considered that organization may not have the required licenses to implement all the capabilities of Zero Trust so thorough planning phase should be done before moving on to implementation phase.

## 5.2 Implementing Zero Trust Architecture

When the plans are done and the organization is ready to move towards implementing the Zero Trust Architecture, prudence is necessary to maintain, so you don't lock out yourself from the environment, don't break anything and cause harm to users or endpoints and always have a plan to move backwards if anything breaks. Zero Trust Controls should always be tested in small scale before implementing to full scale in production.

In this chapter of research, we go through what needs to be implanted to be Zero Trust compliant with the RaMP among with Microsoft's recommended conditional access policies. We will implement Conditional Access, Compliance policies and other user and security policies to our environment and see how these policies are built, how the policies affects and behaves and how the security maturity is risen.

RaMP provides checklist type of approach which allows you easily move forward step by step to reach the end goal of Zero Trust compliance. Checklists includes top level tasks which are done inside Azure AD and Intune with Compliance policies, Conditional access policies, device configuration policies and other administrative settings. Deployment tasks are listed below with explanatory about how the task is fulfilled and how the setting is implemented to this research also if the setting is out of scope it is mentioned. Microsoft. (n.d.)

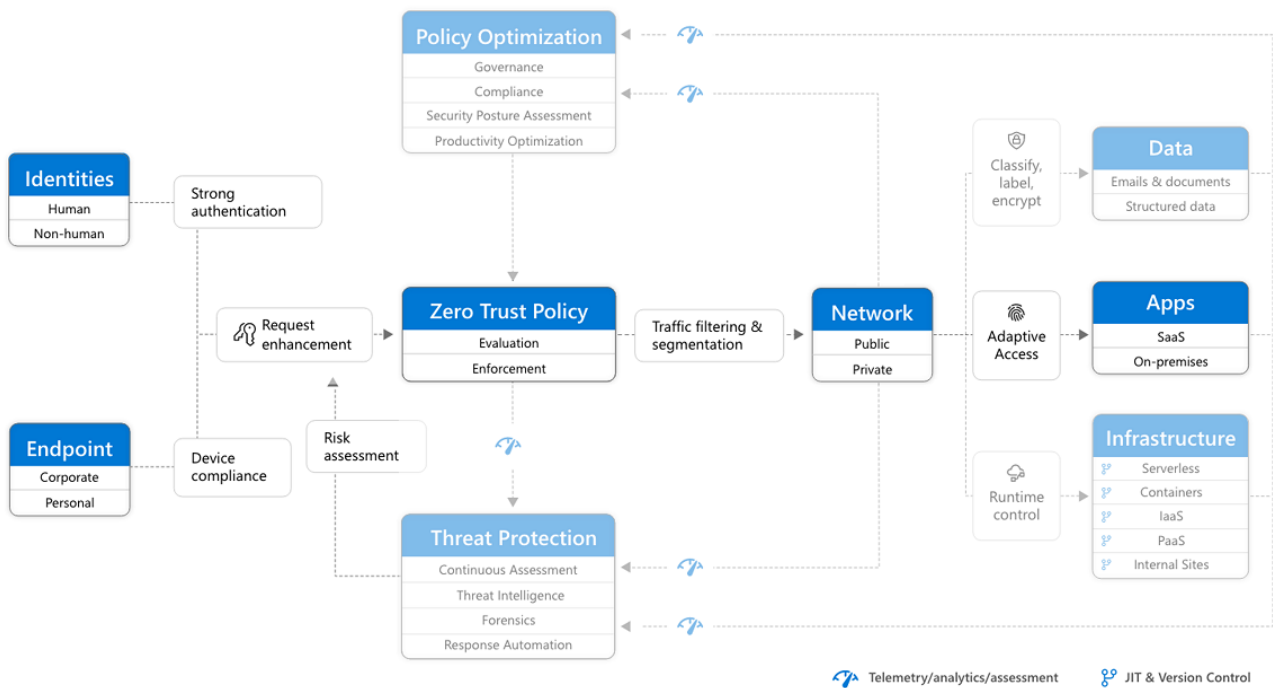


Figure 5 Overall architecture of Zero Trust for RaMP. Microsoft. (n.d.). User Access Productivity Overview.

### RaMP Checklist for privileged Identities

1. Deploy secured privileged access to protect administrative user accounts.
2. Deploy Azure AD Privileged Identity Management (PIM) for a time-bound, just-in-time approval process for the use of privileged user accounts.

Privileged identities we're left out from this research, so these task are not part of this research

### RaMP Checklist for regular user Identities

1. Enable self-service password reset (SSPR), which gives you credential reset capabilities.

This setting allows users to reset their own password, which reduces the workload on IT personnel and allows them to focus other tasks. This also improves the level of security by disallowing unauthorized access to user accounts.

In this research this setting is enabled, this is done from Azure Active Directory from “password reset” menu, by selecting group where all the tenant users is located.

## 2. Enable Multi-Factor Authentication (MFA) and select appropriate methods for MFA

MFA adds an extra layer of security to the authentication process by requiring users to provide additional proof of their identity this additional info, such as verification code delivered via text message, phone call or with authenticator application, in addition to their password.

This is implemented to the identities used on this research, both are using SMS as a default MFA method, Mark is also eligible for Microsoft authenticator App.

## 3. Enable combined User Registration for your directory to allow users to register for SSPR and MFA in one step

This allows users to register themselves for SSPR and MFA in one step, which makes it easier for users to set up and use these security features, without the need of IT personnel to set it up. In this research this setting is turned on.

## 4. Configure a Conditional Access policy to require MFA registration.

This is a security setting that forces MFA registration for identities in conditional access policy, with this we can improve the level of security and protect against leaked passwords, phishing, and other password related threats.

In this research this is done with below as we build the conditional access policy in chapter 6.

## 5. Enable user and sign-in risk-based policies to protect user access to resources.

These policies use machine learning to analyze user behavior and detect signs of risk or suspicious activity, if the endpoint or identity is determined as a risk it can be prevented to access resources this helps prevent unauthorized access.

In this research this is done with below as we build the conditional access policy in chapter 6.

6. Detect and block known weak passwords and their variants and block additional weak terms specific to your organization.

This setting is blocking commonly used weak passwords such as “password123” or “1234567”, as well as words that are referring to your organization name, username, or the combination of these factors. This helps organizations to protect against password related attacks.

In this research the setting is implemented with device compliance settings and forcing custom banned password list from the Azure AD password protection settings.

Custom banned password list ⓘ

```
Company  
password  
password123  
january  
february
```

Figure 6 Custom banned password list

7. Deploy Microsoft Defender for Identity and review and mitigate any open alerts (in parallel with your security operations).

This is a security solution that provides advanced threat detection and remediation capabilities for your organization's identity infrastructure. Reviewing and mitigating any open alerts helps your identity infrastructure ensure its security and protect against threats.

In this research the sensor is out of scope since the sensor is designed to be installed on domain controllers and there are only workstations in the fleet of the test environment.

## 8. Deploy passwordless credentials.

Passwords are a major attack vector. Malicious actors use attacks such as social engineering and phishing to compromise passwords. A passwordless authentication solution mitigates efficiently against these types of attacks.

With Passwordless authentication there are multiple different offerings for identities to provide authentication, such as Microsoft authentication app, Security keys or Windows Hello. From these companies you can choose a suitable option for their use.

Microsoft Authenticator app can turn any iOS or Android mobile phone into a passwordless credential, from the app you can provide authentication to the identity.

FIDO2 compliant security keys are useful for identities which are used from shared machines, or in situations where use of phones is limited, and for high privilege identities.

Windows Hello for Business is the best for users on their dedicated Windows endpoints, identities can provide biometric authentication such as fingerprint, facial recognition or a pin code.

This is not implemented on this research. As we are using passwords on the identities and one angle in this research is to break in with leaked or brute forced passwords.

## RaMP Checklist for Endpoints

### 1. Register devices with Azure AD.

All the devices that are used to access company resources should be registered to Azure AD and should have unique identity, in this way company has full visibility and control on the devices that are used on their environment. If device is not registered to Azure AD the Zero Trust architecture cannot be implemented.

In this research the workstations in test environment are enrolled to Azure AD and Intune

### 2. Enroll devices and create configuration profiles.

Enrolling devices and creating configuration profiles is an essential step in modernizing endpoints and ensuring that they are properly configured and secured. To enroll devices, you will need to have a MDM solution in place, such as Microsoft Intune. Intune allows you to enroll devices from various platforms, including Windows, macOS, iOS, and Android. Once devices are enrolled, you can manage the endpoints from centralized management and apply configuration policies to ensure that they meet your organization's security and compliance requirements.

In this research we will be using Microsoft Intune to enroll by this we can maximize the control and level of security by forcing all necessary compliance and conditional policies among other security settings to the devices.

### 3. Connect Defender for Endpoint to Intune (in parallel with your security operations).

It is recommended to integrate Microsoft Defender for Endpoint to Intune, this allows companies to determine device risk levels which is used on in the compliance



and conditional access policies, it also allows automatically implement Microsoft Defender to endpoints to protect against malware, spyware and other possible threats and unwanted objects.

In this research this setting is fully implemented. To turn on the setting you can follow these directions, turn on “Microsoft intune connection” from the Microsoft 365 Defender menu, go to Settings → Advanced Features → turn switch to “On” position on the “Microsoft intune connection” setting

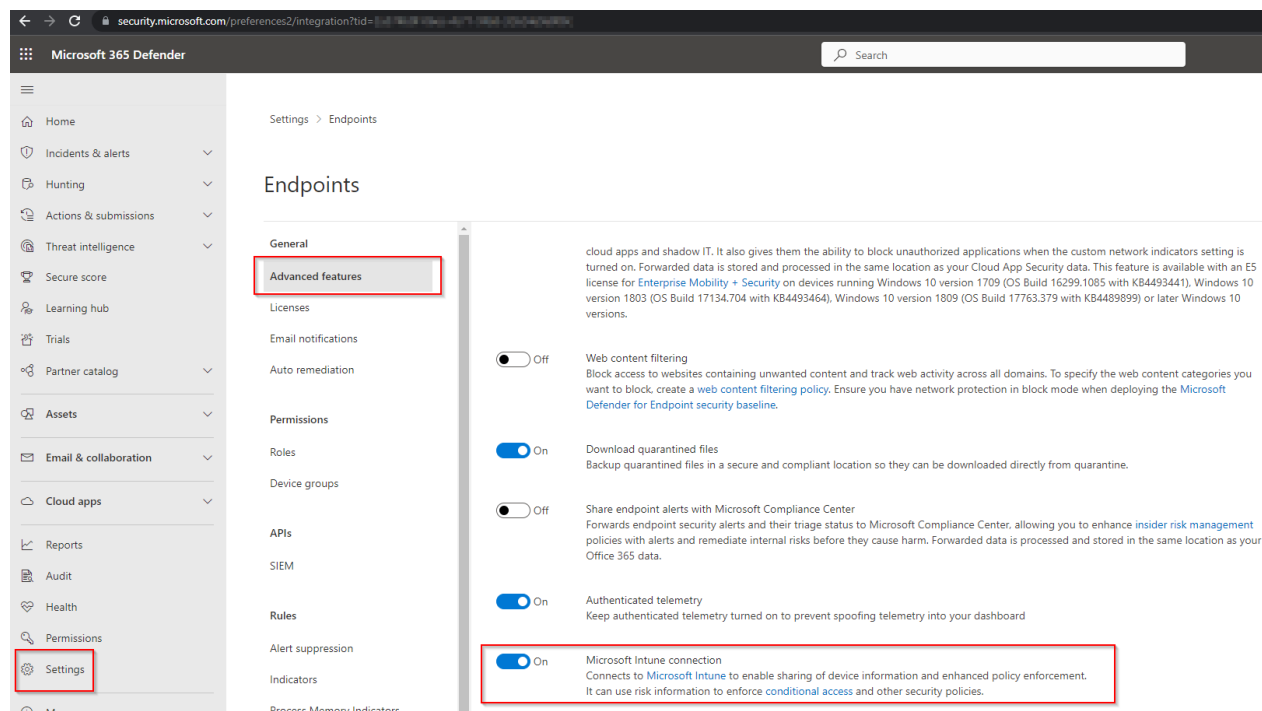


Figure 7 M365 Defender & Microsoft Intune connection

#### 4. Monitor device compliance and risk for Conditional Access.

This is done by forcing Compliance policy to the endpoint which is connected to the company network that monitors the computer that all the wanted compliance requirements are met. If these conditions are not met, device will be marked as non-compliant and conditional access will prevent the access to the company resources and data from the endpoint.

In this research this is implemented, Device compliance policies are in place and the conditional access will prevent the access if compliance requirements are not fulfilled.

#### 5. Implement Microsoft Information Protection and integrate with Conditional Access policies.

This is done with sensitivity labels to categorize and protect company data within Teams, Sharepoint etc. In this research this is out of scope.

### 5.3 Conditional access

Microsoft's Conditional Access is a feature built-in Azure Active Directory (AAD) and Intune, it allows an organization to enforce access policies based on required conditions or criteria. These conditions can include factors such as user identity, device state, geographical location, or the sensitivity of the resource being accessed. With conditional access policies, an organization is able to control which resources are accessed, by whom, under what circumstances, and from what location. Microsoft. (n.d.)

Conditional Access is the centre component of Zero Trust architecture, by integrating Conditional Access with Zero Trust architecture, organizations can create a security framework that enforces strict access controls and ensures that only authorized users, devices, and applications can access sensitive resources. This is achieved by setting up conditional access policies that require identities and endpoints to meet specific criteria before they are granted access to a resource.

As an example, an organization could set up a conditional access policy that requires all users to authenticate using multi-factor authentication, when accessing company resources from unknown network. It's also possible to set the policy to require that the user's device is enrolled in the organization's Intune system and has the latest security updates installed.

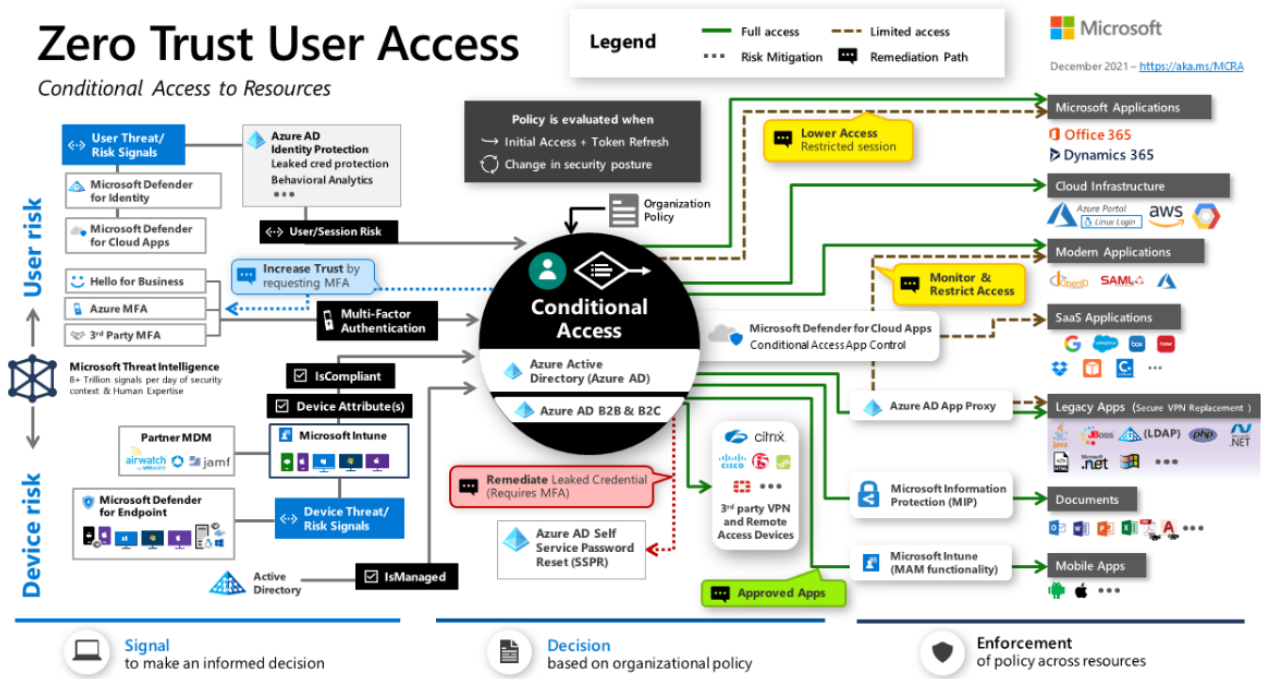


Figure 8 Overview of Conditional access. Microsoft. (n.d.). User Access. Azure Architecture Center.

**5.3.1 Building Common Zero Trust compliant Conditional Access policies**

In this chapter we go through the settings that are necessary for Zero Trust compliant Conditional access policy. The settings provided here is the current recommendations from Microsoft, these policies are implemented in the research test environment to provide insight on how the Zero Trust architecture is built. The recommendations append some settings that are required in the RaMP checklist. Microsoft. (n.d.)

We will go through setting by setting and give you the necessary info on why this should be implemented and how the setting improves the overall level of security.

Block clients that don't support modern authentication, Figure 9 – This blocks legacy authentication protocols, that does not support modern authentication methods like MFA, for example these legacy authentication protocols are used by Microsoft Office 2013 or older Office versions and applications that uses mail protocols like POP, IMAP, and SMTP AUTH and many more.

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
Block legacy Authentication ✓

Assignments  
Users ⓘ  
[All users included and specific users excluded](#)

Cloud apps or actions ⓘ  
[All cloud apps](#)

Conditions ⓘ  
1 condition selected

Access controls  
Grant ⓘ  
[Block access](#)

Session ⓘ  
0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ  
Not configured

Sign-in risk ⓘ  
Not configured

Device platforms ⓘ  
Not configured

Locations ⓘ  
Not configured

Client apps ⓘ  
2 included

Filter for devices ⓘ  
Not configured

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ  
Yes No

Select the client apps this policy will apply to

Modern authentication clients

Browser

Mobile apps and desktop clients

Legacy authentication clients

Exchange ActiveSync clients

Other clients ⓘ

Figure 9: Conditional access policy - Block clients that don't support modern authentication

Require MFA when sign-in risk is low, medium, or high, Figure 10 - This Conditional access policy requires the user to provide MFA when the sign-in risk is determined as low, medium, or high by the Azure AD Identity Protection sign-in risk detection module. The low sign-in risk may cause some unwanted complexity to user experience, so it should be considered that is the risk and reward ratio fulfilled.

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
 ✓

Assignments

Users   
[All users included and specific users excluded](#)

Cloud apps or actions   
[All cloud apps](#)

Conditions   
 1 condition selected

Access controls

Grant   
 1 control selected

Session   
 0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk   
 Not configured

Sign-in risk   
 3 included

Device platforms   
 Not configured

Locations   
 Not configured

Client apps   
 Not configured

Filter for devices   
 Not configured

Control user access to respond to specific sign-in risk levels. [Learn more](#)

Configure

Sign-in risk level is generated based on all real-time risk detections.

Select the sign-in risk level this policy will apply to

High  
 Medium  
 Low  
 No risk

Figure 10: Conditional access policy - Require MFA when sign-in risk level is Low-High

High risk users must change password, Figure 11 – This Conditional access policy requires the user to provide MFA and change password when the sign-in risk is high by the Azure AD Identity Protection sign-in risk detection module.

The screenshot shows the configuration page for a Conditional Access policy named "High risk users PWD change". The page is divided into several sections:

- Header:** "High risk users PWD change" with a menu icon. Below it, "Conditional Access policy" and actions: "Delete" and "View policy information (Preview)".
- Description:** "Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)"
- Name:** A text box containing "High risk users PWD change".
- Assignments:**
  - Users:** "All users included and specific users excluded"
  - Cloud apps or actions:** "All cloud apps"
  - Conditions:** "1 condition selected"
  - Access controls:** "Grant" (1 control selected)
  - Session:** "Sign-in frequency - Every time"
- Control access enforcement:**
  - Radio buttons for "Block access" and "Grant access" (selected).
  - Checkboxes for:
    - Require multifactor authentication (checked)
    - Require authentication strength (Preview) (unchecked)
    - Require device to be marked as compliant (unchecked)
    - Require Hybrid Azure AD joined device (unchecked)
    - Require approved client app (unchecked) with link "See list of approved client apps"
    - Require app protection policy (unchecked) with link "See list of policy protected client apps"
    - Require password change (checked)
- Warning:** A yellow box with a warning icon stating: "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Figure 11 Conditional access policy - High risk user password change

Require approved apps and app protection policies with mobile devices – This Conditional access policy is a combination of two policies.

First policy in Figure 12 requires that apps used by the client are approved by the organization administrator or the application meets the app protection policy conditions, these conditions are set by the organization administrator and can include for example could require support for MFA, and data encryption.

Second policy in figure 13 prevents mobile devices the use of basic authentication in Exchange ActiveSync when connecting to Exchange Online.

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
Require approved apps or app protection ✓

Assignments

Users ⓘ  
[All users included and specific users excluded](#)

Cloud apps or actions ⓘ  
[All cloud apps](#)

Conditions ⓘ  
1 condition selected

Access controls

Grant ⓘ  
2 controls selected

Session ⓘ  
0 controls selected

Control access enforcement to block or grant access. [Learn more](#)

Block access  
 Grant access

Require multifactor authentication ⓘ  
 Require authentication strength (Preview) ⓘ  
 Require device to be marked as compliant ⓘ  
 Require Hybrid Azure AD joined device ⓘ  
 Require approved client app ⓘ  
[See list of approved client apps](#)  
 Require app protection policy ⓘ  
[See list of policy protected client apps](#)  
 Require password change ⓘ

For multiple controls

Require all the selected controls  
 Require one of the selected controls

Figure 12 Conditional access policy - Require approved apps and app protection

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
Block Exchange ActiveSync on all devices ✓

Assignments

Users ⓘ  
[All users included and specific users excluded](#)

Cloud apps or actions ⓘ  
1 app included

Conditions ⓘ  
1 condition selected

Access controls

Grant ⓘ  
1 control selected

Session ⓘ  
0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ  
Not configured

Sign-in risk ⓘ  
Not configured

Device platforms ⓘ  
Not configured

Locations ⓘ  
Not configured

Client apps ⓘ  
1 included

Filter for devices ⓘ  
Not configured

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ  
 Yes  No

Select the client apps this policy will apply to

Modern authentication clients

Browser  
 Mobile apps and desktop clients

Legacy authentication clients

Exchange ActiveSync clients  
 Other clients ⓘ

Figure 13 Conditional access policy - Block Exchange ActiveSync on all devices

Require compliant PCs and mobile devices, figure 14 – This conditional access policy required the device used to access company resources to fulfil the compliance settings which set in the Compliance policy. When the Compliance Policy is fulfilled the device is set as compliant and with this conditional access policy access is granted.

The screenshot shows the configuration for a Conditional Access policy named "Require compliant devices". The policy is set to "Grant access". Under the "Require device to be marked as compliant" option, several settings are listed, including "Require multifactor authentication", "Require authentication strength (Preview)", "Require Hybrid Azure AD joined device", "Require approved client app", "Require app protection policy", and "Require password change". A warning message states: "Don't lock yourself out! Make sure that your device is compliant. Learn more".

**Conditional Access policy**

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

**Name \***  
Require compliant devices ✓

**Assignments**

**Users** ⓘ  
[All users included and specific users excluded](#)

**Cloud apps or actions** ⓘ  
[All cloud apps](#)

**Conditions** ⓘ  
[0 conditions selected](#)

**Access controls**

**Grant** ⓘ  
[1 control selected](#)

**Session** ⓘ  
[0 controls selected](#)

**Control access enforcement to block or grant access.** [Learn more](#)

Block access

Grant access

Require multifactor authentication ⓘ

Require authentication strength (Preview) ⓘ

Require device to be marked as compliant ⓘ

**⚠ Don't lock yourself out! Make sure that your device is compliant.** [Learn more](#)

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ  
[See list of approved client apps](#)

Require app protection policy ⓘ  
[See list of policy protected client apps](#)

Require password change ⓘ

Figure 14 Conditional access policy - Require compliant PCs and mobile devices

Always require MFA, figure 15 – Some users may be required to perform MFA authentication every time organization resources, or specific cloud application are accessed, these are used in special cases for example if the user is accessing data which is considered confidential or otherwise sensitive.



Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Always require MFA -For Sensitive Content ✓

Assignments

Users ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

[1 condition selected](#)

Access controls

Grant ⓘ

[1 control selected](#)

Session ⓘ

[0 controls selected](#)

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multifactor authentication ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require authentication strength (Preview) ⓘ

Multifactor authentic... ▾

ℹ To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Azure AD tenants for external users. Authentication strengths will only configure second factor authentication for external users. [Learn more](#)

Require device to be marked as compliant ⓘ

Figure 15 Conditional access policy - Always require MFA

## 5.4 Compliance policies

Microsoft Device Compliance Policy feature is built-in feature within Intune, It can enhance the protection of organizational data by enforcing certain user and device requirements.

The Compliance Policy is closely entangled with Microsoft's Zero Trust architecture, Implementing compliance policies, organizations can create a security framework that enforces strict data protection and risk management policies. This is achieved by setting up compliance policies that are applied to all devices and users attempting to access sensitive resources. Microsoft. (n.d.)

As an example, an organization might set up a compliance policy that requires endpoint to fulfil certain conditions such as operating system version, device locking policies, presence of antivirus and disk encryption. By enforcing these policies, the organization can reduce the risk of data breaches and ensure compliance with industry-specific regulations, as well as append conditional access with compliance policy requirements.

#### **5.4.1 Building Common Zero Trust compliant Compliance policies**

Define device compliance policies should be created for each platform used in the company infrastructure, including Windows Devices, Android devices and iOS devices. Each compliance policy contains different security levels and

Enrollment and compliance policy for Windows 10 and Later, figure 16 – Compliance policy should verify that endpoints are secured correctly and as the organization requirements for system security is fulfilled, The Compliance policy should include settings at least about Disk encryption, OS version, Anti malware software settings, if these conditions are not matched, the device is set as non-compliant and its access is prohibited to company resources as its non-compliant so conditional access prevents it. Microsoft. (n.d.)

**Basics** [Edit](#)

Name	Windows 10 and later Compliance policy
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

**Compliance settings** [Edit](#)

## Device Health

Require BitLocker	Require
Require Secure Boot to be enabled on the device	Require
Require code integrity	Require

## Device Properties

Minimum OS version	10.0.19045.2486
--------------------	-----------------

## System Security

Require a password to unlock mobile devices	Require
Simple passwords	Block
Minimum password length	6
Maximum minutes of inactivity before password is required	15 minutes
Require password when device returns from idle state (Mobile and Holographic)	Require
Require encryption of data storage on device.	Require
Firewall	Require
Trusted Platform Module (TPM)	Require
Antivirus	Require
Antispyware	Require
Microsoft Defender Antimalware	Require
Microsoft Defender Antimalware minimum version	4.18.2301.6
Microsoft Defender Antimalware security intelligence up-to-date	Require
Real-time protection	Require

## Microsoft Defender for Endpoint

Require the device to be at or under the machine risk score:	Medium
--	--------

Figure 16 Windows 10 and later compliance policy

Enrolment and compliance policy for Android, figure 17 - There is multiple different enrolment types for Android operating system, so you must choose the correct compliance policy for your enrolment type, if multiple Android enrolment types are confronted, you can create compliance policy for each enrolment type. In this case we create compliance policy for "Android Enterprise -

Fully managed, dedicated, and corporate-owned work profile” -devices. Compliance policy settings should require latest operating system version and security patch level, use of a complicated password, device encryption and block rooted devices, if these requirements are not fulfilled, the device should be set as non-compliant and therefore prevented to access company data and services by the conditional access policy. Microsoft. (n.d.)

### Fully managed, dedicated, and corporate-owned work profile ...

Android Enterprise

✓ Basics
✓ Compliance settings
✓ Actions for noncompliance
✓ Assignments
5 Review + create

**Summary**

**Basics**

Name	Android Fully managed Compliance Policy
Description	--
Platform	Android Enterprise
Profile type	Fully managed, dedicated, and corporate-owned work profile

**Compliance settings**

**Microsoft Defender for Endpoint**

Require the device to be at or under the machine risk score:	Clear
--	-------

**Device Health**

Require the device to be at or under the Device Threat Level	Secured
SafetyNet device attestation	Check basic integrity & certified devices

**Device Properties**

Minimum OS version	11.0
Minimum security patch level	2023-01-01

**System Security**

Require a password to unlock mobile devices	Require
Required password type	Alphanumeric with symbols
Minimum password length	8
Number of characters required	1
Number of lowercase characters required	1
Number of uppercase characters required	1
Number of non-letter characters required	1
Number of numeric characters required	1
Number of symbol characters required	1
Maximum minutes of inactivity before password is required	1 minute
Number of days until password expires	365
Number of passwords required before user can reuse a password	5
Require encryption of data storage on device.	Require
Intune app runtime integrity	Require

**Actions for noncompliance**

Action	Schedule	Message template	Additional recipients (via ...
Mark device noncompliant	Immediately		

Figure 17 Android Compliance policy

Enrollment and compliance policy for iOS/iPadOS, figure 18 – Compliance policy for iOS should verify that iOS devices are secured to fulfil company requirements, the compliance policy should include need for latest operating system version, use of a complicated password and block jailbroken devices, if these circumstances are not met, the device should be marked as non-compliant and therefore prevent the access to company data and services by the conditional access policy. Microsoft. (n.d.)

**iOS compliance policy** ...  
iOS/iPadOS

✔ Basics
✔ Compliance settings
✔ Actions for noncompliance
✔ Assignments
4 Review + create

**Summary**

**Basics**

Name	iOS Compliance policy
Description	--
Platform	iOS/iPadOS
Profile type	iOS compliance policy

**Compliance settings**

**Device Health**

Jailbroken devices	Block
Require the device to be at or under the Device Threat Level	Secured

**Device Properties**

Minimum OS version	12.5.7
--------------------	--------

**Microsoft Defender for Endpoint**

Require the device to be at or under the machine risk score:	Low
--	-----

**System Security**

Require a password to unlock mobile devices	Require
Simple passwords	Block
Minimum password length	6
Required password type	Alphanumeric
Number of non-alphanumeric characters in password	1
Maximum minutes after screen lock before password is required	1 minute
Maximum minutes of inactivity until screen locks	1 minute
Password expiration (days)	365
Number of previous passwords to prevent reuse	5

**Actions for noncompliance**

Action	Schedule	Message template	Additional recipients (via ...)
Mark device noncompliant	Immediately		

Figure 18 iOS Compliance policy

## 6 Use cases

In this chapter we will demonstrate few use case scenarios that may happen against organizations, we will go through the normal usage of enrolled devices and designated user logins, then what happens when threat actor gains access to the user account via Brute force or if the user credentials are leaked lastly we'll try to go around for all the security measures with stolen credentials including MFA.

In a theory the previously implemented Zero Trust policies should protect against these attack types.

### 6.1 Brute Forcing or leaked credentials

In a normal sign-in event from Chris's computer or from Marks computer the designated users are able to access <https://portal.azure.com> -website without any issues and as they are using trusted devices and sign-in nor user risk is not increased MFA is not challenged as shown in figure 19.

Policy Name	Grant Controls	Session Controls	Result
Require compliant devices	Require compliant device		Success
Block legacy Authentication	Block		Not Applied
Sign-in risk-based MFA	Require multifactor authentica...		Not Applied
High risk users PWD change	Multifactor authentication and...	Sign-in frequency	Not Applied
Always require MFA - for Sams...	Require compliant device		Not Applied

Figure 19 Successful Azure sign-in for Mark Mountain

But what happens if the user credential is used from another location, we can get through the login by entering the user account and in this case the stolen password (in this case it does not matter whether it's leaked or brute forced), we are challenged by MFA as in Figure 20, because the sign-in risk is increased. If we can get past MFA challenge, we are in a situation as in Figure 21, we are unable to login since our device does not meet the compliance requirements. In figure 22 is shown the Applied conditional access policies to this sign-in event and we can see that the Sign-in risk based MFA policy is applied and successfully passed, but the two policies are in failure, since both require the device that passes compliance requirements.

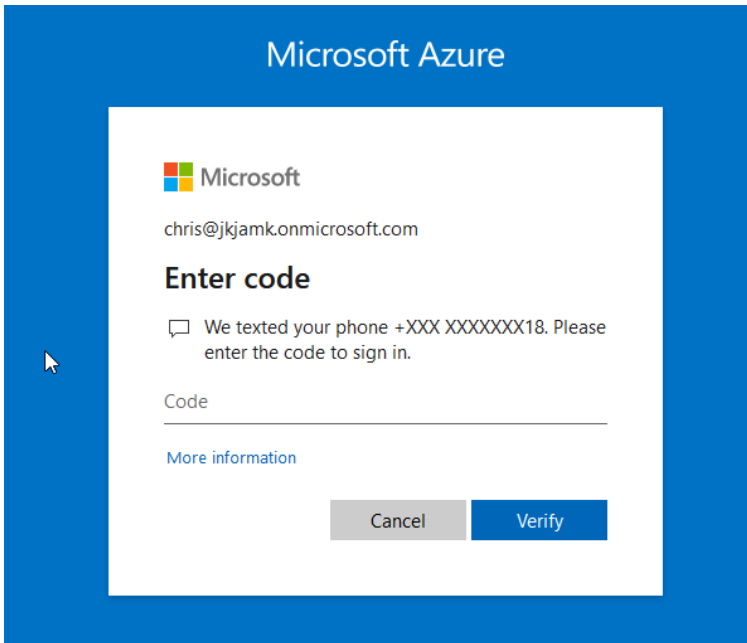


Figure 20 MFA challenge for Chris

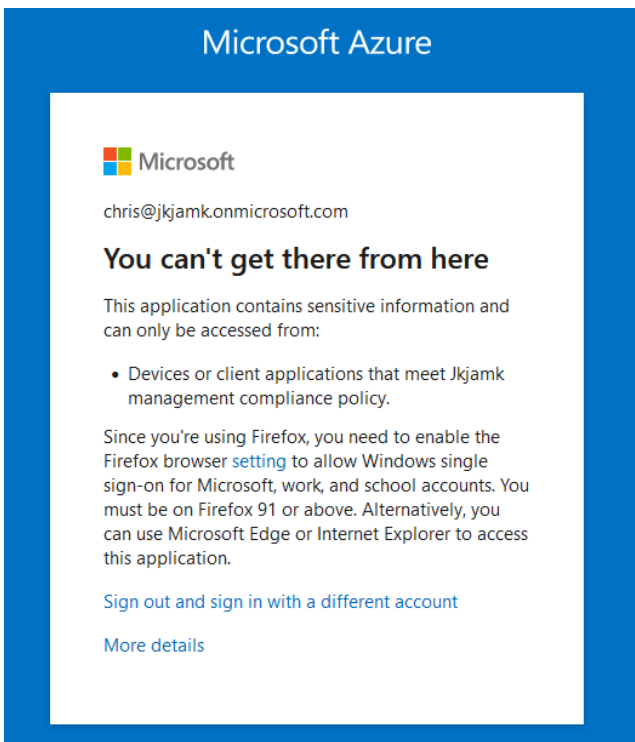


Figure 21 Login failure

## Activity Details: Sign-ins

Basic info	Location	Device info	Authentication Details	<u>Conditional Access</u>	Report-only
Search					
Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓		
Sign-in risk-based MFA	Require multifactor authentica...		Success		
Require compliant devices	Require compliant device		Failure		
Always require MFA -For Sensi...	Require compliant device, Req...		Failure		
Block legacy Authentication	Block		Not Applied		
High risk users PWD change	Multifactor authentication and...	Sign-in frequency	Not Applied		
Require approved apps or app...	Require approved app		Not Applied		
Block Exchange ActiveSync on ...	Require app protection policy		Not Applied		
User risk level high or medium	Multifactor authentication and...	Sign-in frequency	Not Applied		

Figure 22 Applied Conditional Access policies on sign-in event

Addition to this when the account is brute forced from unusual location in this case Chris's user account was tried to break in with brute force from Los Angeles via VPN. We can see few things happening in the Microsoft 365 Security centre. First, we can see that the security centre has raised an alert because of unusual sign-in activity, figure 23.

The screenshot shows a security alert titled "Anonymous IP address involving one user". The alert is categorized as "Anonymous IP address" and is marked as "New". The incident graph shows a node for "91.219.212.86". The "What happened" section includes a timeline entry: "Attempted to sign-in from IP address 91.219.212.86" on 4/26/2023 at 9:25:04 PM. The details for this event are: IP address: 91.219.212.86, Sign-in location: Los Angeles, California, US, and Sign-in request ID: c951a58a-c47f-4c58-8db7-03e707752600.

Figure 23 Alert of Risky sign-in activity



Second finding is that Chris's user risk is now increased as in Figure 24. Due to this, Chris is forced to change password on next login in Figure 25 as the compliance policy forces that if user risk is high or medium, in this research the rule was changed from high to cover also medium user risk.

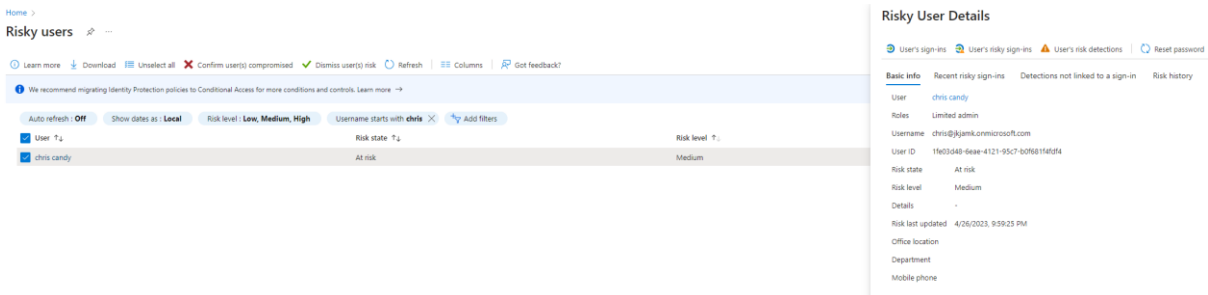


Figure 24 Increased user risk

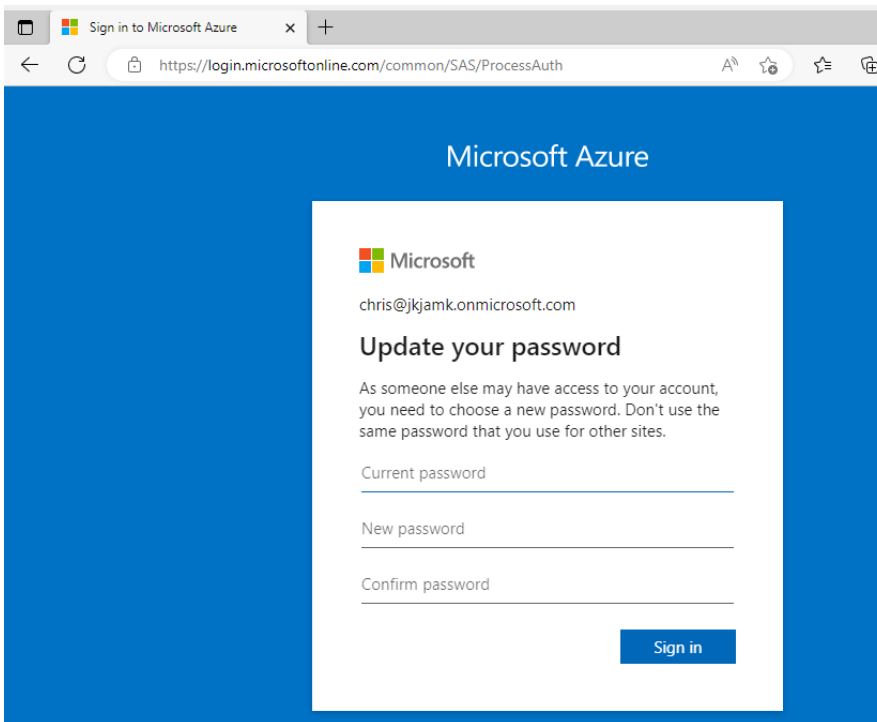


Figure 25 Forced password change

## 6.2 Passing conditional access policy with stolen credentials

In this next case I wanted to demonstrate how can we bypass the conditional access policy, with fully stolen credentials including MFA. For this we need to setup another windows 10 machine

After the machine is setup, and we have acquired the credentials we login to the machine with local account then we add the stolen credentials as a work account and enroll the machine to Intune, this requires MFA challenge to pass. Due to enrolment, the device is forced compliance policies, conditional access policies, and configuration profiles such as setting a PIN code to the device.

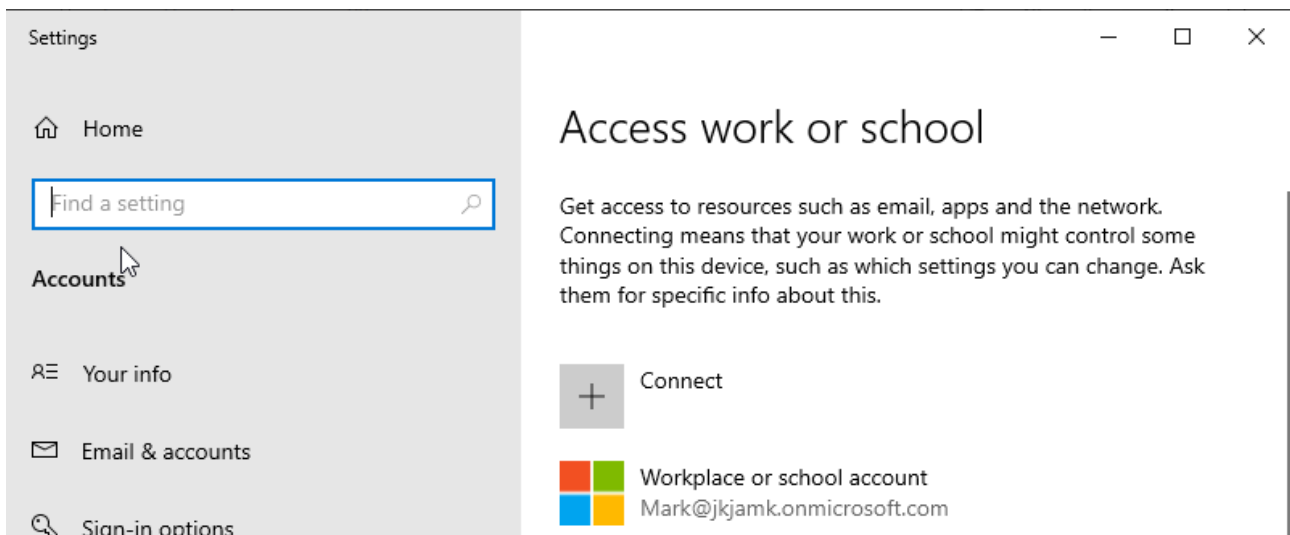


Figure 26 Add work account

After the enrolment we can see that Mark's device is changed in Intune as in Figure 27. Until the device does not fulfil the compliance requirements, we can't access any company data. In this demonstration we are missing Bitlocker and operating system version is not up to date.

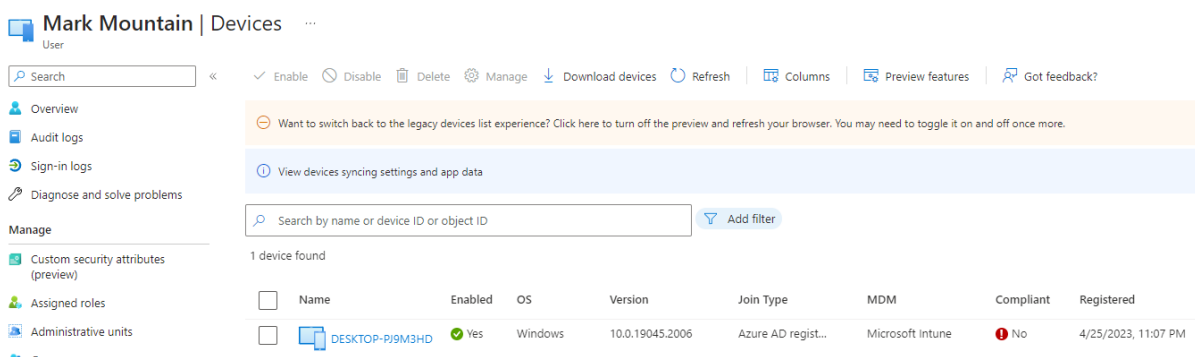


Figure 27 Marks new device

After updates and setting up bitlocker we can access <https://portal.azure.com> as in Figure 28 and we can see from AAD sign-in logs that the login event passes compliance policies.

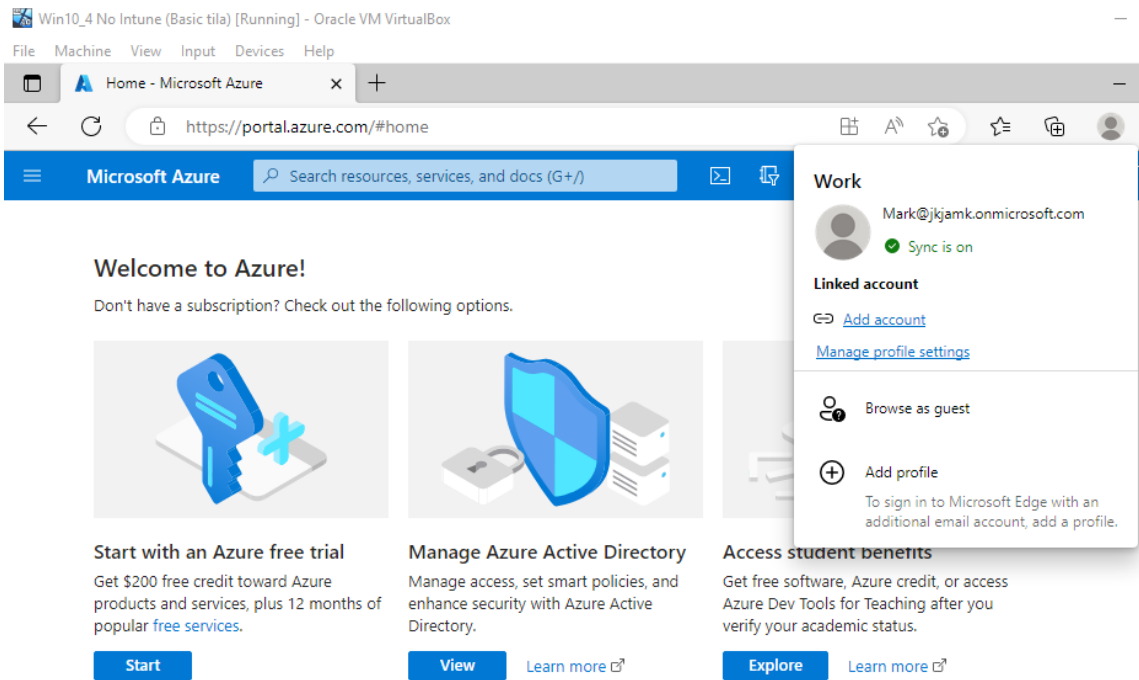


Figure 28 Successful login to Azure portal

## Activity Details: Sign-ins

Policy Name	Grant Controls	Session Controls	Result
<a href="#">Require compliant devices</a>	Require compliant device		Success
<a href="#">Block legacy Authentication</a>	Block		Not Applied
<a href="#">Sign-in risk-based MFA</a>	Require multifactor authentica...		Not Applied
<a href="#">High risk users PWD change</a>	Multifactor authentication and...	Sign-in frequency	Not Applied
<a href="#">Always require MFA -For Sensi...</a>	Require compliant device		Not Applied
<a href="#">Require approved apps or app...</a>	Require approved app		Not Applied
<a href="#">Block Exchange ActiveSync on ...</a>	Require app protection policy		Not Applied
<a href="#">User risk level high or medium</a>	Multifactor authentication and...	Sign-in frequency	Not Applied

A sign-in can also be interrupted (e.g. blocked, multifactor authentication challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

Figure 29 Passed compliance policy

This scenario is very unlikely to happen due to the MFA requirement, and it can be prevented with simple enrollment restriction settings from Intune, to prevent user enroll personal devices to the Intune portal.

Home > Devices | Enrollment device platform restrictions > Prevent personal device enrollment

## Prevent personal device enrollment | Properties

Search

Changes saved.

Overview

Manage

Properties

**Basics** Edit

Name	Prevent personal device enrollment
Description	--
Platform	Windows

**Platform settings** Edit

MDM	Allow
Min Version	--
Max Version	--
Personally owned devices	Block

In summary, the implemented Zero trust policies efficiently debunked all malicious login attempts and even in a case where MFA is successfully challenged, the access is denied by compliance requirement.

## 7 Security baseline and posture

In this chapter we go through how we can measure level of security and how the security posture is uplifted after the Zero Trust controls are implemented. We'll also discuss about the security baseline and how that can be improved, built and measured by using 3rd party tools.

## 7.1 Security Baseline

There are multiple useful baseline benchmarks that could be used to build a security baseline, for example there is Center for Internet Security (CIS) benchmark, National Institute of Standards and Technology (NIST) benchmark, and Microsoft cloud security benchmark (MCSB) among many else. MCSB is a combination of CIS, NIST, PCI controls. MCSB covers security controls for Network security, Identity management, Privileged Access, Data protection, Asset management, Logging and threat detection, Incident response, Posture and vulnerability management, Endpoint security, Backup and recovery, DevOps Security and Governance & Strategy which are in some part in a scope of Microsoft ZTA. Center for Internet Security. (n.d.).

There exist numerous third-party tools that utilize and visualize these benchmark settings within an organization's ecosystem, enabling rapid implementation of selected benchmarks and their associated configurations.

It is up to organization to implement the baseline suitable for their environment considering industry and regional regulation and legislation, for many you do not have to implement the benchmarks up to the hilt, and you can choose settings that are feasible to your environment.

It is also important to remember that the level of security is constantly changing, and new threat vectors (more sophisticated malware, new vulnerabilities are found and much more) emerge from time to time, so security settings should be reviewed constantly. For example it would be great practice to develop a year clock to maintain the security posture, this year clock should include tasks that should be done repeatedly, for example every 6 months, these repeated tasks could be for example following:

Reviewing security settings on identities, endpoints and other services.

Validate for example incident response, disaster recovery plans, meaning that you practice scenarios, which could happen in real-life to illustrate, if you are attacked with ransomware, how do you mitigate from that or if a malicious threat actor is able to acquire admin account to your tenant via phishing, how you can detect and mitigate from that.

In this research we didn't build baseline security, the Azure tenant security level is left "as is", so the default security settings are only implemented, except the settings that are mentioned on the

RaMP checklist and some configurations that are required to build the Zero Trust compliant Conditional access and Compliance requirement policies.

We had to build few configuration profiles to the Intune management for Microsoft Defender and Bitlocker. With the configuration profiles Microsoft Defender was rolled on the devices with some additional settings such as ransomware protection, Endpoint detection and response (EDR) and spyware protection. For bitlocker we've modified the it to be allowed without TPM, as well as the device compliance settings had to be modified regarding TPM requirement, since the virtual machines does not have TPM the requirement had to be changed to "not configured"

## **7.2 Security Posture**

In this chapter we'll go through the level of security of the Azure and M365 tenant. We'll dive into the Secure score from Microsoft 365 Defender portal which indicates the effectiveness of configured security policies, conditional access policies, and compliance requirements.

## **7.3 Microsoft 365 Defender Security score**

Below in Figure 30 is the default secure score from the Microsoft 365 Defender portal, this score is the default level when the tenant is set up. Device score is not visible at this point since there is no

relevance to it due to the fact that there is no enrolled endpoints nor Microsoft Defender licenses are not assigned to any entity.

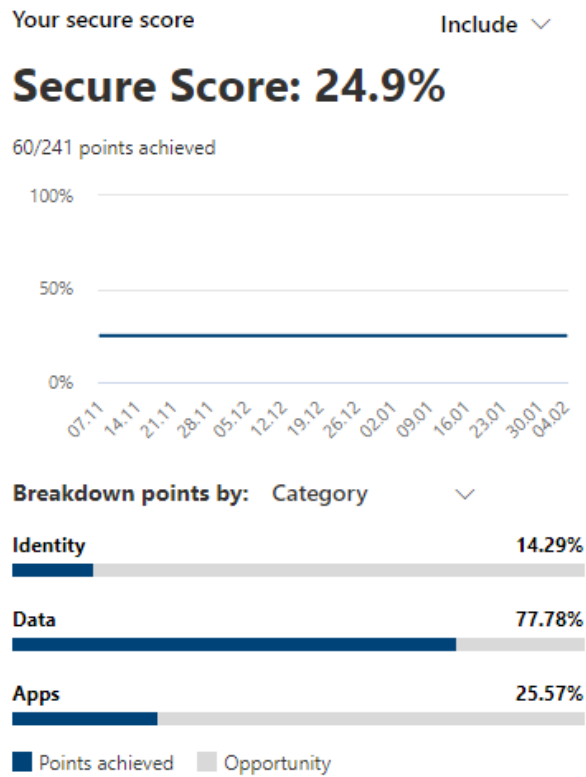


Figure 30 Default Secure Score

## Secure Score: 43.83%

425.6/971 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 04/28

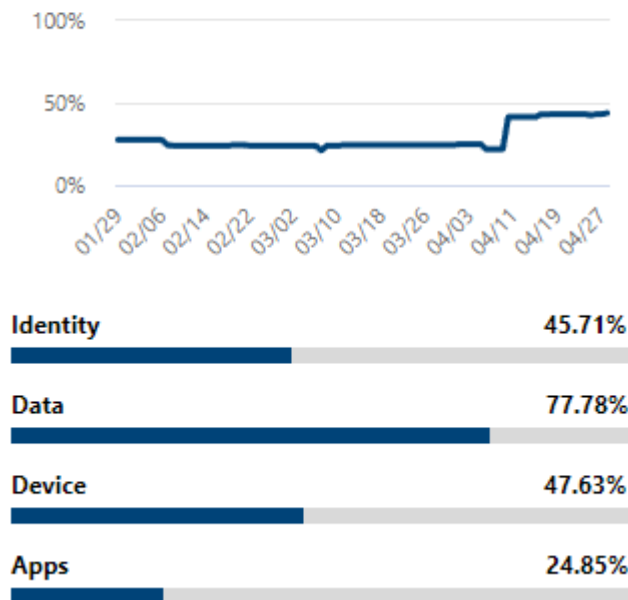


Figure 31 Secure Score After Policy deployment

Above in figure 31 is the Security score after implementing the Zero Trust compliant Conditional access policies and compliance requirements for endpoints which were presented on the chapter 6. From the Microsoft 365 Defender portal we can see that the security score has been clearly improved but there is still much space for improvement.

As the baseline configurations from this tenant are missing, we can clearly point out that Zero Trust Controls alone does not provide the desired level of security. Next, we'll dig deeper what has been increased or decreased on each category from the implementation of the settings. Also, we'll discuss on why some settings does not seem to be fully implemented. Lastly the recommended actions are reviewed and discussed.



Also, it is notable that the score is actively moving back and forth, since the score value of settings is changing, and new settings and controls are implemented by Microsoft. In addition the Secure score takes time to update, so there is sometimes days of delay until the security score is changed.

### 7.3.1 Identity score

As this research focuses on the identities and their security it is positive to notice that the identity score has been significantly improved. The base security score was only 14,29%, after implementing the Conditional access policies that are linked to the identities and their security settings the security score is dazzling 45,71%.

Activity	Resulting points
0.40 points gained for <a href="#">Enable policy to block legacy authentication</a> because 1 fewer users are affected	6.4/8
0.90 points regressed for <a href="#">Ensure all users can complete multifactor authentication</a> because 3 more users are affected	3.6/9
1.00 points gained by completing <a href="#">Enable self-service password reset</a> . Great work!	1/1
0.35 points gained for <a href="#">Protect all users with a sign-in risk policy</a> because 1 fewer users are affected	5.6/7
6.00 points gained for <a href="#">Enable policy to block legacy authentication</a> because 1 fewer users are affected	6/8
4.50 points gained for <a href="#">Ensure all users can complete multifactor authentication</a> because 2 fewer users are affected	4.5/9
5.25 points gained for <a href="#">Protect all users with a sign-in risk policy</a> because 1 fewer users are affected	5.25/7

Figure 32 Identity security score improvements

On Figure 32 we can see as the conditional access policies are taken place and improves the level of security from the score viewpoint. Due to the excluding of some users in the tenant from these Conditional access policies causes minor decrease in the results.

### 7.3.2 Data Score

The controls implemented at the identity and endpoint layers did not impact the data score, which is a typical outcome. To enhance the data score, additional measures such as extending Microsoft 365 sensitivity labeling to assets in Microsoft Purview data map, establishing and utilizing auto-

labeling data classification policies, creating Data Loss Prevention (DLP) policies, and publishing M365 sensitivity label data classification policies could be implemented.

This research did not include any controls for the data layer, as it was deemed out of scope. Consequently, no controls were implemented for the data layer.

### 7.3.3 Device score

When the conditional access policies and compliance requirements are set, we can't instantly see improvement on the secure score, even though the endpoints are enrolled to Intune. This happens because the secure score is related to Microsoft Defender, and it is required to be applied and configured to the endpoints. Use of Microsoft Defender also may require additional licenses.

+10.00 points score change because <a href="#">Turn on real-time protection</a> has become relevant	10/10	Device
+10.00 points score change because <a href="#">Turn on Microsoft Defender for Endpoint sensor</a> has beco...	10/10	Device
+10.00 points score change because <a href="#">Turn on Microsoft Defender Firewall</a> has become relevant	10/10	Device
+10.00 points score change because <a href="#">Turn on Microsoft Defender Antivirus</a> has become relevant	10/10	Device
+10.00 points score change because <a href="#">Fix Microsoft Defender for Endpoint sensor data collectio...</a>	10/10	Device
+10.00 points score change because <a href="#">Fix Microsoft Defender for Endpoint impaired communica...</a>	10/10	Device
+10.00 points score change because <a href="#">Enable Microsoft Defender Antivirus scanning of downloa...</a>	10/10	Device

Significant enhancements were observed in the Device Secure score upon the implementation of the recommended zero trust policies as well as outlined in the RaMP and the allocation of eligible licenses to endpoints. Key improvements were achieved by integrating Intune with Microsoft 365 Defender, monitoring device compliance against compliance policies, and addressing any compliance deviations using conditional access measures.

### 7.3.4 Apps score

The Apps (Cloud applications) score has remained stable since no settings regarding applications has been made, this is due to that the Applications are out of the scope of this research. There is

just minor change to the score, and this is due to the normal score value shifting on Microsoft's end.

### 7.3.5 Recommended actions

From each category there is Recommended actions menu, which allows organizations to check the settings that are implemented and improves the score value. More importantly the Recommended actions menu shows settings that are not fully implemented or implemented at all. Which you could use to improve the score value. From each setting that are not implemented, you can check how it would affect the score and open a step-by-step guide. Also notable is that the menu shows if you have already the needed license acquired, since some setting may need extensive licensing model.

In this case the Identity recommendations shown below in figure 33 does not mark some setting as completed, even though the conditional access policy is in place, the reason for this is that the tenant administrator and some other user accounts are excluded from all of the settings.

Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product
1	Require multifactor authentication for administrative roles	+1.03%	0/10	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
2	Protect all users with a user risk policy	+0.72%	0/7	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
3	Ensure all users can complete multifactor authentication	+0.93%	3.6/9	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
4	Do not allow users to grant consent to unreliable applications	+0.41%	0/4	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
5	Enable policy to block legacy authentication	+0.82%	6.4/8	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
6	Protect all users with a sign-in risk policy	+0.72%	5.6/7	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
7	Designate more than one global admin	+0.1%	0/1	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
8	Do not expire passwords	+0.82%	8/8	<input checked="" type="checkbox"/> Completed	No	Yes	Identity	Azure Active Directory
9	Enable self-service password reset	+0.1%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Identity	Azure Active Directory
10	Use least privileged administrative roles	+0.1%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Identity	Azure Active Directory

Figure 33 Microsoft 365 Security recommendation for identities

The research revealed a broad range of device recommendations, with numerous critical settings still requiring attention. Overall, there were 57 recommendations that could be implemented to enhance device security. The top 10 recommendations, listed below in figure 34 in order of their impact on score, include essential measures that ought to be implemented.

Filters: Category: Device ×

Rank	Recommended action	Score impact ↓	Points achieved	Status	Regressed	Have license?	Category	Product	
▼ To address (57)									
<input type="checkbox"/>	1	Block untrusted and unsigned processes that run from USB	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint
<input type="checkbox"/>	2	Block all Office applications from creating child processes	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint
<input type="checkbox"/>	3	Block JavaScript or VBScript from launching downloaded executable content	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint
<input type="checkbox"/>	4	Block Office applications from injecting code into other processes	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint
<input type="checkbox"/>	5	Block executable content from email client and webmail	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint
<input type="checkbox"/>	6	Block Adobe Reader from creating child processes	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint
<input type="checkbox"/>	7	Block Office communication application from creating child processes	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint
<input type="checkbox"/>	8	Block credential stealing from the Windows local security authority subsystem	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint
<input type="checkbox"/>	9	Block process creations originating from PSEXec and WMI commands	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint
<input type="checkbox"/>	10	Block abuse of exploited vulnerable signed drivers	+0.93%	0/9	<input type="radio"/> To address	No	Yes	Device	Defender for Endpoint

Figure 34 Microsoft 365 Security recommendation for endpoints

Despite the presence of essential Zero Trust controls for identities and endpoints, such as denying non-compliant devices, among other security measures, it is evident that the base-level security remains insufficient and is lacking key components. To achieve a higher level of security, it is necessary to implement additional measures to protect the organization.

## 8 Discussion

### 8.1 Changing cyber landscape

It is inevitable to discuss the evolving cybersecurity landscape, with the topic of Zero Trust gaining particular prominence. Since 2020, when the COVID-19 pandemic necessitated a shift from office-based to remote work, significant changes have occurred in the way people work. Even now, in mid-2023, many individuals prefer more flexible work arrangements, such as working from home, hybrid work, or even working from abroad. Consequently, organizations have had to adapt and adopt more modern solutions to facilitate remote work from any location.

Organizations are confronted with numerous challenges in governing identities. The rapid expansion of the application market, combined with a shift towards more flexible work arrangements, including the ability to work remotely from any location, has introduced new obstacles and the persistent availability of personally identifiable information, whether as a result of data leaks, data

breaches, or information that is publicly accessible on a company website, increases companies risks to be targeted with cyber attacks.

Contemporary flexible work arrangements have increased the number of endpoint devices in the organizations ecosystems. In modern organizations, it is common practice to implement Bring Your Own Device (BYOD) policy, allowing users to access company data with personal devices such as personal phone.

The trend towards working from any location presents new challenges in managing endpoints with regard to cybersecurity. Some companies may have hastily implemented modern solutions at the cost of cybersecurity, such as granting users excessive privileges or neglecting to update endpoints regularly. Additionally, endpoints are more vulnerable as they may be used on random networks outside the company network, exposing them to potential attacks.

The current practice of implicitly trusting devices that connect directly to a company's network or via VPN is being replaced by a more proactive approach under modern ZTA. ZTA employs endpoint monitoring and inspection, and policies that require endpoints to meet specific criteria, such as being updated and connected via VPN. Organizations can use ZTA to limit access to company data to endpoints that meet the required criteria.

ZTA offers several methods to mitigate identity and endpoint risks, beginning with verifying all login attempts with conditional access, compliance policies, multi-factor authentication (MFA), single sign-on (SSO), or a combination of these factors. Requests that do not meet these conditions can be denied, such as if the request comes from a non-typical geographical location. Organizations that adopt ZTA and continually monitor identity and endpoint activity can achieve a state in their ecosystem where the risk level is significantly reduced compared to ecosystems that do not follow ZTA.

## 8.2 Hardship of Zero Trust

I believe that Zero Trust has not been actively implemented to companies as it may be considered as hard or complex to implement. This may be because there is a lot of babble about ZTA and it may sound gibberish for many, since Zero Trust is presented either very high-level marketing or technical perspective which means that there is very fancy technical, or marketing terms added to the sales pitch.

In simple terms Zero Trust Architecture is just a security strategy to prevent unauthorized access to company resources. The implementation is always different for everyone since technologies for implementing Zero Trust may vary, the ecosystem of organizations is always different, and the laws and regulations differs on every industry.

Companies that consider moving towards ZTA I would suggest implementing the policies and configurations in small steps to maintain control and not to apply unnecessary complexity which hampers either the work of administrators or the company users or for both.

For technology companies I would personally suggest approaching ZTA with more practical manner and provide simple guidelines with step-by-step guides or implementation paths which could be modified to the target companies needs to apply growth on ZTA market. This is one objective of the research.

## 9 Conclusions

In this research the overall picture of Zero Trust is thoroughly described, and we can safely say that the benefits of Zero Trust are remarkable from the scope studied in this research and the benefits are clearly pointed out on this research, but the Zero Trust Compliant security settings alone does not make organizations completely safe if the baseline is not built well or at all. The path to Zero Trust compliance is feasible if organizations have enough willpower and resources in hand. The use cases provide valid real-life context and are comparable with real-life scenarios which organizations could meet.

This research main question was How does Microsoft Zero Trust architecture enhance one's capability to protect against cyber-attacks? As it quickly turned out the research was needed to delimit to Identities and Endpoints so we would focus this research question about these two factors.

The research question was tackled using a constructive case study approach, which acknowledges that cybersecurity is an ongoing concern for organizations. Specifically, the study aimed to address the issue of the increasing number of cyber attacks and involvement of regular users being targeted as attack vectors and sought to explore ways to minimize their involvement in such attacks.

This research tackles that construction as it provides valid information on how ZTA improves the capabilities to protect against attacks that targets identities. This is demonstrated in chapter 6 where the policies built with Zero Trust Architecture efficiently prevent access from untrusted locations and devices and therefore eliminates one aspect from the user attack vector perspective. The identities and endpoints may still be vulnerable for other attack vectors such as malwares, phishing, and zero-day attacks.

This research was also tasked with demonstrating how ZTA protects against brute-force attacks and cases of leaked credentials as part of the main and secondary research questions. The tests were carefully planned and involved trying different variations of the aforementioned attack scenarios. The results of these tests were successful in demonstrating the effectiveness of ZTA in protecting against these types of attacks.

Secondary research question was how can we measure the effectiveness of Zero Trust? The effectiveness of Zero trust were measured in this research with two ways, by conducting previously mentioned life like attack simulations that organization may have to endure and analyze the results on how does the Zero trust policies implemented behave and protect against these attack simulations, second measurement method was to look into security score provided by Microsoft Defender 365 security center and to see how the score is affected by the Zero Trust controls that were implemented on this research. The Base Security score was checked before any implementations were done and after creating all the necessary policies and settings it was checked again and analyzed on how the controls affected the score.

We can state that it is evident that Zero Trust Architecture provides effective protection against identity-targeted attacks. During the use cases, despite obtaining a multi-factor authentication (MFA) token and successfully completing the MFA challenge, we were unable to exploit user identities. The ZTA policies effectively blocked access to the identities by requiring them to connect from compliant devices through conditional access measures.

The research was also able to prove that the Zero Trust controls improves the security level from secure score perspective and that there is a solid way how we can measure it.

This research does not cover all the layers of Zero Trust in Microsoft M365 and Azure infrastructure, so the final result is not in full scale. The research also fails to prove on how Zero Trust Architecture would improve the level of security on an environment where the baseline is already in place and build with consideration and security focused.

All in all, we can prove by the use cases and analyzing the Microsoft 365 Defender Security level that the Zero Trust Compliant policies does bring controls and compliance requirements that improves the level of security and protection against attacks against identities and endpoints. But without a good baseline the Zero Trust policies does not make you immune to breaches nor cyber attacks.

For future research the focus could be in the missing parts of this research to cover the full scale of Zero Trust Architecture with Microsoft tools. For future you could also research different roll-out plans towards Zero Trust Architecture and also a full scale “migration” to Zero Trust Architecture would be interesting case study. All the up and downs, challenges and victories would be important information for organizations which are planning on moving toward Zero Trust Architecture in their own environments.

Never Trust – Always verify!



## References

BrightSec. (2021, February 22). Security Misconfiguration: Impact, Examples, and Prevention. Retrieved from <https://www.balbix.com/insights/security-misconfiguration-impact-examples-and-prevention/>

BrightSec. (2021, February 4). Security Misconfiguration. Retrieved from <https://brightsec.com/blog/security-misconfiguration/>

Center for Internet Security. (n.d.). CIS Controls. Retrieved from <https://www.cisecurity.org/controls/>

CISO Portal. (n.d.). What are the 7 cybersecurity layers? CISO Portal. <https://www.ciso-portal.com/what-are-the-7-cybersecurity-layers/>

Cloudflare. (n.d.). Web Application Firewall (WAF). Cloudflare. <https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/>

CompTIA. (n.d.). Network security basics: Definition, threats, and solutions. CompTIA. <https://www.comptia.org/content/guides/network-security-basics-definition-threats-and-solutions>

CrowdStrike. (2023). CrowdStrike 2023 Global Threat Report. Retrieved from <https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf>

CrowdStrike. (n.d.). Most Common Types of Cyberattacks. Retrieved from <https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/>

CrowdStrike. (n.d.). Threat Actor. Retrieved from <https://www.crowdstrike.com/cybersecurity-101/threat-actor/>

CSO Online. (n.d.). What is physical security? How to keep your facilities and devices safe from on-site attackers. CSO Online. <https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html>

Encyclopædia Britannica. (n.d.). Cybercrime. Retrieved from <https://www.britannica.com/topic/cybercrime>

Firewall Times. (n.d.). Administrative Security Controls. Retrieved from <https://firewalltimes.com/administrative-security-controls/>

Fortinet. (n.d.). What is endpoint security? Fortinet. <https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security>

Hub International. (2022, January 18). Common Cybersecurity Risks for Businesses. Retrieved from <https://www.hubinternational.com/blog/2022/01/common-cyber-security-risks-for-businesses/>

IBM. (n.d.). Cybersecurity. Retrieved from <https://www.ibm.com/topics/cybersecurity>

IBM. (n.d.). Endpoint security. IBM. <https://www.ibm.com/topics/endpoint-security>

IBM. (n.d.). Incident response. IBM. <https://www.ibm.com/topics/incident-response>

IBM. (n.d.). Network security. IBM. <https://www.ibm.com/topics/network-security>

International Conference on Information. (2016). What Is Defense in Depth and Why Is It Important? Retrieved from <https://ici2016.org/what-is-defense-in-depth-and-why-is-it-important/>

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. Retrieved from <https://www.iso.org/standard/54534.html>

IT Pro. (2018, April 23). What is hacktivism? Retrieved from <https://www.itpro.com/hacking/30203/what-is-hacktivism>

Logically Secure Ltd. (2018, January 17). 11 Common Cyber Attack Methods and How to Prevent Them. Retrieved from <https://www.logicallysecure.com/blog/11-common-cyber-attack-methods/>

Malwarebytes. (n.d.). Malware. Retrieved from <https://www.malwarebytes.com/malware>

McKinsey & Company. (2021, January). The Risk-Based Approach to Cybersecurity. Retrieved from <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity>

Microsoft. (2019, November 11). Zero Trust strategy: What good looks like. Security Blog. Retrieved from <https://www.microsoft.com/en-us/security/blog/2019/11/11/Zero-Trust-strategy-what-good-looks-like/>

Microsoft. (2023, April 24). Stay compliant and protect sensitive data with zero trust security. Microsoft Security Blog. <https://www.microsoft.com/en-us/security/blog/2023/04/24/stay-compliant-and-protect-sensitive-data-with-zero-trust-security/>

Microsoft. (n.d.). Android Enterprise fully managed device settings in Intune. Retrieved from <https://learn.microsoft.com/en-us/mem/intune/enrollment/android-fully-managed-security-settings>

Microsoft. (n.d.). Configure device compliance settings for iOS/iPadOS devices in Microsoft Intune. Learn. Retrieved from <https://learn.microsoft.com/en-us/mem/intune/enrollment/ios-ipados-device-compliance-security-configurations>

Microsoft. (n.d.). Azure Active Directory security baseline. Microsoft Security Compliance Toolkit. Retrieved from <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/aad-security-baseline>

Microsoft. (n.d.). Azure security benchmark. Microsoft Security Compliance Toolkit. Retrieved from <https://learn.microsoft.com/en-us/security/benchmark/azure/overview>

Microsoft. (n.d.). Common Conditional Access policy settings. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-common>

Microsoft. (n.d.). Conditional Access policy to control risk. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk>

Microsoft. (n.d.). Create device compliance policies for Windows devices with Microsoft Intune. Learn. Retrieved from <https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows>

Microsoft. (n.d.). Diagram: Zero Trust security elements. Microsoft. Retrieved from <https://learn.microsoft.com/en-us/security/zero-trust/media/diagram-zero-trust-security-elements.png>.

Microsoft. (n.d.). Identity and access policies for Microsoft 365. Microsoft Learn. <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/identity-access-policies?view=o365-worldwide>

Microsoft. (n.d.). Identity and access policies in Office 365. Learn. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/identity-access-policies?view=o365-worldwide>

Microsoft. (n.d.). Infrastructure deployment. Retrieved from <https://learn.microsoft.com/en-us/security/zero-trust/deploy/infrastructure>

Microsoft. (n.d.). Microsoft Azure PCI DSS Compliance. Microsoft Azure Compliance Offerings. Retrieved from <https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-pci-dss>

Microsoft. (2022). Microsoft Security Virtual Training Day: Zero Trust. Retrieved from [https://info.microsoft.com/WE-ZTF-WBNR-FY22-05May-19-Microsoft-Security-Virtual-Training-Day-Zero-Trust-SRDEM107648\\_LP01-Registration---Form-in-Body.html](https://info.microsoft.com/WE-ZTF-WBNR-FY22-05May-19-Microsoft-Security-Virtual-Training-Day-Zero-Trust-SRDEM107648_LP01-Registration---Form-in-Body.html)

Microsoft. (n.d.). Overview of Conditional Access in Azure Active Directory. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

Microsoft. (n.d.). Security defaults in Azure Active Directory. Learn. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

Microsoft. (n.d.). Security planning for Azure Active Directory roles. Learn. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/roles/security-planning>

Microsoft. (n.d.). Security planning in Azure Active Directory roles. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/active-directory/roles/security-planning>

Microsoft. (n.d.). User Access. Azure Architecture Center. <https://learn.microsoft.com/en-us/azure/architecture/guide/security/user-access>

Microsoft. (n.d.). User access and productivity: Validate trust for users, devices, apps, and network. Retrieved from <https://learn.microsoft.com/en-us/security/zero-trust/user-access-productivity-validate-trust>

Microsoft. (n.d.). User Access Productivity Overview. [Diagram]. Retrieved May 7, 2023, from <https://learn.microsoft.com/en-us/security/zero-trust/media/user-access-productivity-overview/user-access-productivity-validate-trust-users-devices-apps-network.png#lightbox>.

Microsoft. (n.d.). Visibility, automation, and orchestration. Retrieved from <https://learn.microsoft.com/en-us/security/zero-trust/deploy/visibility-automation-orchestration>

Microsoft. (n.d.). Zero Trust overview. Retrieved from <https://docs.microsoft.com/en-us/security/Zero Trust/Zero Trust-overview>

Microsoft. (n.d.). Zero Trust Ramp Overview. Microsoft Security. <https://learn.microsoft.com/en-us/security/Zero%20Trust/Zero%20Trust-ramp-overview>

Microsoft. (n.d.). Zero Trust security model fundamentals. Microsoft. <https://learn.microsoft.com/en-us/azure/security/fundamentals/zero-trust>

Microsoft. (n.d.). Zero Trust security model. Retrieved from <https://learn.microsoft.com/en-us/azure/security/fundamentals/Zero Trust>

Microsoft. (n.d.). Zero trust: Ramp overview. Retrieved from <https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview>

MITRE Corporation. (n.d.). ATT&CK. Retrieved from <https://attack.mitre.org/>

National Institute of Standards and Technology. (2020). Zero Trust Architecture. Retrieved from <https://www.nist.gov/publications/zero-trust-architecture>

National Institute of Standards and Technology. (2020). Zero Trust Architecture. (NIST Special Publication 800-207). Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

National Institute of Standards and Technology. (n.d.). Cybersecurity Framework - Five Functions. Retrieved from <https://www.nist.gov/cyberframework/online-learning/five-functions>

Norton. (n.d.). How do zero-day vulnerabilities work? Retrieved from <https://us.norton.com/blog/emerging-threats/how-do-zero-day-vulnerabilities-work#>

Norwich University Online. (n.d.). Types of Cybercrime. Retrieved from <https://online.norwich.edu/academic-programs/resources/types-of-cyber-crime>

Palo Alto Networks. (n.d.). Intrusion Prevention System (IPS). Palo Alto Networks. <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>

RAND Corporation. (2021). Cybersecurity Challenges and Opportunities for the Department of Homeland Security: Remarks to the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, Committee on Homeland

Security, U.S. House of Representatives. Retrieved from [https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND\\_CT490.pdf](https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf)

S&P Global. (2021). SASE, ZTNA, and XDR: Three security trends catalyzed by the impact of 2020. Retrieved from <https://www.spglobal.com/marketintelligence/en/news-insights/research/sase-ztna-and-xdr-three-security-trends-catalyzed-by-the-impact-of-2020>

SailPoint. (n.d.). What is identity security? SailPoint. <https://www.sailpoint.com/identity-library/what-is-identity-security/>

TechTarget. (2021, June). History and evolution of zero trust security. Retrieved from <https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security>

TechTarget. (n.d.). Script kiddie (script kiddies). Retrieved from <https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie>

Varonis. (n.d.). What Is a Security Policy? Retrieved from <https://www.varonis.com/blog/what-is-a-security-policy>