Article

Not peer-reviewed version

Analysis of Azure Zero Trust Architecture Implementation for Mid-size Organizations

Vedran Dakic * , Zlatan Moric * , Ana Kapulica , Damir Regvart

Posted Date: 18 July 2024

doi: 10.20944/preprints202407.1454.v1

Keywords: security; cybersecurity; Zero Trust Architecture; ZTA; Azure ZTA; multi-factor authentication; micro-segmentation

Article

Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations

Vedran Dakic *, Zlatan Moric *, Ana Kapulica and Damir Regvart

Department of Operating Systems, Algebra University, 10000 Zagreb, Croatia

* Correspondence: vedran.dakic@algebra.hr (V.D.); zlatan.moric@algebra.hr (Z.M.)

Abstract: The Zero Trust Architecture (ZTA) security system follows the "never trust, always verify" principle. The process constantly verifies users and devices trying to access resources. This paper describes how Microsoft Azure uses ZTA to enforce strict identity verification and access rules across the cloud environment to improve security. Implementation is time-consuming and difficult. Azure's extensive services and customizations require careful design and implementation. Azure administrators struggle to navigate and change configurations due to its complex user interface (UI). Each Azure ecosystem component must meet ZTA criteria. ZTA's comprehensive policy definitions, multi-factor and pass-wordless authentication, and other advanced features are tested in a mid-size business scenario. These configuration changes require a solid grasp of Azure's architecture and Zero Trust. Implementing an Azure ZTA reduces vulnerabilities and restricts authorized users' access to critical resources. Implementation is time-consuming and expensive, requires a significant commitment to changing IT procedures, and can be confusing because the same features are available in multiple places. Azure ZTA has shown great potential for both hybrid and cloud-native companies.

Keywords: security; cybersecurity; Zero Trust Architecture; ZTA; Azure ZTA; multi-factor authentication; micro-segmentation

1. Introduction

ZTA is a cybersecurity architecture emphasizing that no entity, regardless of its location within or outside the network, should be automatically trusted. Instead, every access request must go through authentication, authorization, and continuous validation. As businesses increasingly migrate to cloud platforms like Microsoft Azure, it is essential to establish a ZTA to protect against sophisticated security breaches. However, this transformation is not straightforward. Deploying ZTA in Azure involves a meticulous and complex process requiring deep technical expertise and a thorough understanding of Zero Trust principles and Azure's intricate ecosystem. Azure's intricate user interface exacerbates the challenge, making the navigation and configuration of security settings daunting. Every element, beginning with the establishment of identity management and access restrictions to the installation of network security and the maintenance of continuous surveillance, demands careful planning and precision. Regardless of these challenges, it is crucial to effectively integrate ZTA into Azure to bolster security and safeguard critical assets in an ever-expansive digital landscape.

Previous research explores the application of zero-trust security in intelligent manufacturing, which is essential for safeguarding Industry 4.0 environments [1]. The article highlights several obstacles, including the intricacy of incorporating zero-trust concepts into current legacy systems, rising expenses, and potential effects on productivity. In addition, the authors emphasize the importance of ongoing authentication, live monitoring, and robust security frameworks. They support the need for more research to improve zero-trust architectures specifically designed for IoT and cloud-based manufacturing systems to achieve effortless implementation and heightened security. They propose investigating machine learning (ML) and artificial intelligence (AI) to enhance predictive threat detection and response, highlighting the significance of adaptive security measures. Additionally, the report emphasizes the need to create uniform procedures and foster cooperation among relevant parties to tackle interoperability concerns. This paper highlights the importance of continuous improvements to safeguard innovative industrial systems effectively.

A blockchain framework developed to enhance healthcare data management by bolstering security, privacy, and interoperability was also introduced in 2023 [2]. The authors encountered difficulties achieving a harmonious equilibrium between the openness and secrecy of delicate information, incorporating blockchain protocols into pre-existing healthcare information technology systems, and guaranteeing adherence to rigorous regulatory obligations. Although Hyperledger Fabric has shown notable enhancements in security, crucial areas still require additional research, like scalability, performance concerns, and user adoption. Future endeavors encompass the investigation of sophisticated cryptographic methods, the improvement of blockchain scalability, the execution of real-world pilot studies, and the promotion of collaboration between healthcare practitioners and technology developers to establish standardized protocols. This study emphasizes the significance of employing new strategies to safeguard and efficiently handle confidential healthcare information in an ever-growing digital environment.

Researchers also noted the urgent need to ensure safe remote access in Industrial Internet of Things (IIoT) settings [3]. The authors suggest implementing a zero-trust architecture that prioritizes multi-level authorization, continuous authentication, and strong access control measures to improve security, scalability, and maintainability. Incorporating zero-trust concepts into current IIoT infrastructures posed difficulties, especially in striking a balance between security and operational efficiency and guaranteeing smooth integration with older systems. Notwithstanding these difficulties, the suggested resolution, executed utilizing open-source technology such as Software-Defined Networks (SDN) and Trusted Execution Environments (TEE), exhibited noteworthy enhancements in safeguarding both the network and edge domains. The authors suggest that future research should focus on resolving scalability and performance concerns, enhancing zero-trust implementations, and investigating advanced cryptographic techniques to strengthen security. This study emphasizes the crucial importance of cutting-edge security frameworks in protecting industrial systems from constantly changing cyber threats.

The security environment of the metaverse was also researched [4], highlighting significant concerns and suggesting a ZTA model to address these difficulties. The authors emphasize the intricate interaction among enabling technologies such as AR, VR, and cloud computing, which give rise to distinct security and privacy risks. A vital obstacle noted is balancing, providing engaging user experiences, and implementing strong security measures. The authors encountered challenges when including ZTA into preexisting metaverse frameworks without compromising performance. The study highlights that the existing security solutions frequently prove insufficient to address the dynamic and decentralized characteristics of the metaverse. Potential areas for future research include enhancing ZTA implementations to manage real-time interactions effectively and establishing universally accepted security standards that can be implemented across many metaverse platforms. The writers promote the idea of stakeholders working collaboratively to address these concerns comprehensively.

Previous research also examines a thorough security architecture designed for the banking sector [5]. The system combines ZTA with blockchain technology to tackle cybersecurity issues. The authors highlight the significance of identity and access management, device and network security, and data protection. The challenges involve the delicate equilibrium between security and operational efficiency and guaranteeing a smooth interface with existing systems. The suggested framework utilizes blockchain technology to bolster security safeguards, providing unalterable verification and heightened data integrity. Although the study has potential, it highlights scalability and performance difficulties that additional research needs to address. Future endeavors involve enhancing ZTA implementations, investigating sophisticated cryptographic techniques, and conducting practical pilot studies to verify the framework's efficacy. In addition, the authors promote the idea of financial institutions and technology developers working together to create standardized security procedures and establish best practices.

A new framework that aims to improve security in IoT settings called ZAIB (Zero-Trust and ABAC for IoT using Blockchain) was also introduced [6]. The framework combines a zero-trust architecture with attribute-based access control (ABAC) and blockchain technologies to provide safe device communication. The challenges encompass effectively controlling dynamic access, preserving data integrity, and safeguarding against assaults. The study highlights the significance of ongoing surveillance and flexible security measures. Authors note that future research should prioritize enhancing the scalability and performance of the ZAIB framework, investigating sophisticated cryptographic techniques, and carrying out real-world pilot tests to verify its efficacy. Furthermore, it is imperative to establish uniform protocols and optimal methods to promote the broader implementation of this security framework in diverse IoT applications. The paper emphasizes the urgent requirement for inventive security measures to protect sensitive data in progressively intricate IoT networks.

Researchers investigated integrating zero-trust principles and quantum fingerprinting to improve network security, specifically in countering MAC spoofing [7]. Implementing quantum fingerprinting posed difficulties, such as the intricacy of integration and the need to sustain system performance. The authors stress the importance of ongoing authentication and cryptographic solid techniques. Future research should prioritize enhancing the framework's scalability and performance, investigate advanced cryptographic techniques, and conduct thorough real-world pilot tests to evaluate its usefulness. Furthermore, the study emphasizes the need for established standards and cooperation among industry players to promote the general acceptance of this unique security paradigm. This research highlights the need for advanced technology to create safe and robust networks to combat ever-changing cyber threats.

The complexity of deploying Zero Trust Network Architecture (ZTNA) in cloud environments was also researched [8]. The authors note significant obstacles, such as the need to uphold security while also guaranteeing operational efficiency and seamlessly incorporating with existing systems. The user emphasizes the significance of ongoing surveillance, flexible security measures, and robust data safeguarding. Future research should prioritize the optimization of ZTNA installations, developing improved cryptographic methods, and validating these approaches in real-world scenarios. Furthermore, it is imperative to collaborate across the entire business to establish standardized norms and optimal practices. This evaluation emphasizes the necessity for cutting-edge security solutions to safeguard cloud computing from ever-changing cyber threats. The authors propose that providing advanced training for IT personnel and conducting frequent security audits can bolster the effectiveness of ZTNA installations. In summary, the essay comprehensively examines the possibilities and constraints of ZTNA in cloud computing, providing significant perspectives for future advancements in this domain.

A methodology that enables the seamless integration of AI in Industry 5.0 by employing zero-touch orchestration inside the edge-to-cloud continuum was introduced in 2023 by researchers [9]. The authors stress the importance of smoothly incorporating AI into systems and improving the automation and decision-making procedures. Primary obstacles involve overseeing the entire lifecycle of AI operations and guaranteeing reliable connection between edge and cloud components. Subsequent investigations should delve into sophisticated orchestration strategies, enhancing the deployment of AI models, and conducting real-world validations. The cooperation between industry and academics is essential for developing standardized protocols and optimal practices. The study highlights the capacity of AI to transform Industry 5.0 by implementing inventive, automated, and robust frameworks.

Previous research suggests that ZTA seeks to revolutionize security strategies by shifting away from traditional perimeter defenses and embracing a paradigm that thoroughly authenticates the identity of any person and device attempting to access resources. This strategy is particularly crucial for scenarios that entail geographically distant users and assets hosted in the cloud. ZTA does not rely on implicit trust created based on physical or network locations. Instead, it prioritizes ongoing authentication and verification to guarantee resource access security [10]. Studies highlight the challenges of moving from obsolete systems to ZTA, which necessitate meticulous preparation and the active participation of all essential stakeholders to accomplish a seamless move and improve security posture [11].

Ongoing research indicates that the core technologies of ZTA, such as identity authentication, access control, and trust assessment, are still being developed. Organizations' lack of knowledge about the advantages and disadvantages of ZTA and the complexities involved in implementing it hinders its adoption. Additional inquiry is necessary to address these challenges and develop more sophisticated ZTA solutions [12]. Implementing ZTA has difficulties ensuring robust availability and tamper resistance in policy decision points. These elements are essential for maintaining a strong and secure system [13].

Studies in the field of 6G networks suggest that traditional security frameworks are inadequate for the upcoming generation of networks, demonstrating increased openness and heterogeneity. A cutting-edge software-defined ZTA has been proposed for 6G networks. This architecture offers flexible and scalable security mechanisms, effectively mitigating threats such as Distributed Denial of Service (DDoS) attacks and zero-day exploits. However, unresolved issues still need to be addressed, such as more thorough simulation studies and real-world validations to enhance and optimize ZTA implementations for future networks [14].

Studies on zero trust for applications and network security reveal that globalization, the COVID-19 epidemic, and the shift to cloud services necessitate a departure from traditional security protocols. The study highlights the significance of continuous identity verification and minimizing the delegation of authority to safeguard the security of network systems. A significant finding is that insecure APIs present a considerable threat in zero-trust environments, underscoring the need for enhanced API security policies and awareness [15].

A recent study suggests that using a zero-trust approach in cloud computing efficiently addresses several security concerns, such as internal and external cyber threats and the need for enhanced visibility and automated trust calculations. Comparative assessments of different ZTA models and frameworks demonstrate that while ZTA can significantly improve security, its full implementation requires addressing specific challenges in various domains and integrating new technologies to build robust, trust-based enterprise networks [16].

Previous research has also highlighted the innovative use of ML in implementing ZTA, particularly for calculating trust, which remains a complex and subjective task. ML techniques have shown promise in enhancing security through continuous monitoring and adjusting trust metrics. As a result, this leads to a security framework that is more adaptable and responsive than conventional frameworks [17]. Future investigations should improve machine learning techniques to maximize their accuracy and effectiveness in practical zero-trust architecture implementations.

The rest of this paper is organized as follows. In the next section, we will cover some basic security principles, followed by a section about the specifics of Azure ZTA implementation. We will then move to a ZTA scenario to analyze its capabilities and suitability for mid-size organizations. We will follow up by examining the scenario with some additional best practices and discussing future work and the conclusion.

2. Azure Security Principles

Azure security has a comprehensive and complex toolkit to protect cloud-based resources from various threats. Microsoft Azure provides multiple integrated security features and services to safeguard data, applications, and infrastructure. The following are the fundamental components of Azure security:

- Azure Network Security: The Azure Virtual Network (VNet) is a crucial component that guarantees the separation and division inside the cloud environment. Virtual networks (VNets) can be extended to on-premises locations by establishing secure connections such as virtual private networks (VPNs) and ExpressRoute. Azure offers comprehensive security services, including Azure Sentinel, which uses artificial intelligence and machine learning to detect and mitigate potential security risks [18].

- Azure Active Directory (Azure AD) is crucial for managing identities and controlling access in Identity and Access Management. The platform provides features such as Multi-Factor Authentication (MFA), Conditional Access, and Identity Protection to guarantee the security of user identities and control resource access. Azure AD also enables integration with supplementary identity providers and applications [19].
- Azure IoT Edge and Azure Sphere are purpose-built to bolster the security of Internet of Things (IoT) deployments. Azure Sphere exemplifies the integration of hardware-based security with a tailored Linux-based operating system and a security service to ensure the reliability of devices and safeguard communication [20]. Azure IoT Edge includes built-in security features for deploying and managing IoT devices [21].
- Azure offers various services to protect data during storage and transmission. Azure Key Vault simplifies the administration of encryption keys and confidential information, while Azure SQL Database provides Transparent Data Encryption (TDE) and Always Encrypted features to protect sensitive data [22][23]. Furthermore, Azure's compliance certifications ensure data handling meets rigorous regulatory criteria.
- Azure Security Center provides a comprehensive view of security for all Azure services, offering recommendations and insights to improve security procedures. In addition, it effortlessly integrates with Azure Sentinel to offer enhanced protection against advanced threats and comprehensive monitoring features [24][25]. Azure Defender enhances these capabilities to encompass hybrid and multi-cloud systems, protecting against various threats.
- Azure ensures application security by implementing secure development practices, automated security testing, and runtime protection mechanisms. Azure DevOps includes built-in security features for code repositories, CI/CD pipelines, and artifact storage [26]. Furthermore, Azure Container Registry and Azure Kubernetes Service (AKS) provide functionalities to bolster the security of containerized applications [27].
- Azure offers a comprehensive compliance framework with certifications and attestations such as ISO 27001, GDPR, and HIPAA, guaranteeing compliance and governance. Azure Policy and Blueprints help organizations maintain compliance and governance across cloud environments [28].
- Azure Blockchain Workbench provides a suite of tools for constructing and managing blockchain networks, explicitly focusing on protecting key management and assuring the integrity of transactions. This entails incorporating Azure Key Vault for the secure storage of keys and employing cryptographic techniques to ensure the confidentiality and security of data [29].
- Azure Sentinel is a cloud-based Security Information and Event Management (SIEM) platform that offers advanced capabilities for detecting and mitigating security risks. It employs artificial intelligence to quickly identify and mitigate potential hazards while integrating with various Azure services and third-party solutions to provide a comprehensive security solution [30].

Azure provides a comprehensive security framework encompassing network security, identity management, data protection, threat detection, and compliance measures. By leveraging these technologies and services, enterprises can effectively protect their cloud infrastructures and minimize potential dangers.

3. Azure ZTA

Azure ZTA is a modern cybersecurity framework emphasizing the concept of "never trust, always verify." This architecture shifts away from the traditional security model that depends on defending the boundary to a more extensive and meticulous approach that prioritizes securing individual resources and data streams. Consequently, it enhances organizations' overall security using Azure cloud services [31]. ZTA moves away from exclusively depending on network location for trust and instead requires the authentication of both the user and the device before granting access to resources [32]. This paradigm is crucial for enterprises with remote users and assets in the cloud, making it highly pertinent in the present digital landscape [33]. The basic architecture can be seen in Figure 1:

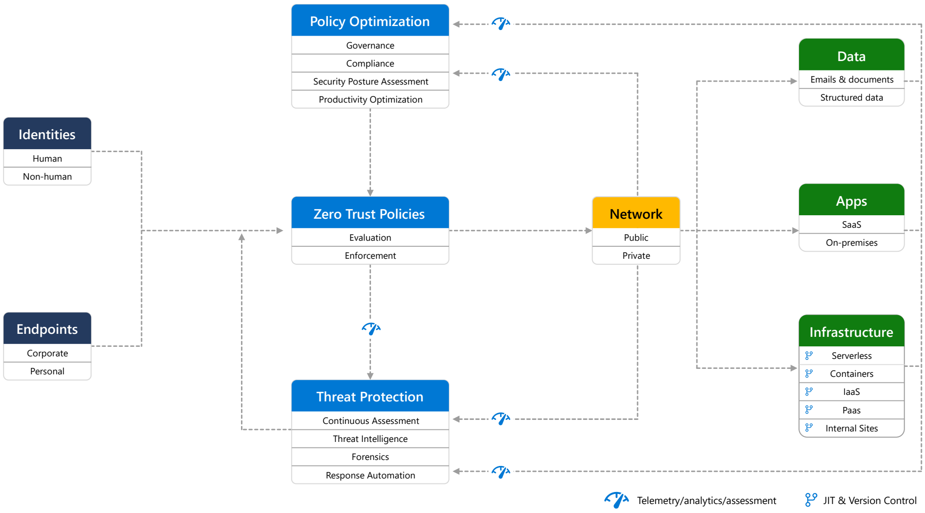


Figure 1. Microsoft Zero Trust adoption framework overview. Available online: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview (accessed on 15.07.2024.).

Implementing ZTA requires significant alterations across the company, demanding a carefully built framework to provide a smooth transition [34]. The main concepts involve continuous verification and permission granting, minimizing vulnerable areas by dividing resources, and granting the least access [35]. Azure's ZTA employs advanced technologies, including micro-segmentation, identity management, and continuous monitoring, to guarantee the security of data and applications [36].

Incorporating ZTA into existing systems poses challenges due to its complex nature and the need for a cultural shift in security procedures [37]. However, studies have highlighted the effectiveness of ZTA in reducing breach risks and enhancing overall security by implementing strict access controls and monitoring [38]. Zero trust systems have shown significant improvements in dealing with cyber threats in cloud environments [39], smart manufacturing [40], and healthcare [41].

Research suggests that ZTA can provide a robust defense against advanced attacks by enforcing stringent access rules and continuously monitoring the system [42]. In addition, the utilization of ZTA in specific domains, such as cyber-physical systems [43] and Kubernetes environments [44], highlights its flexibility [45].

Azure ZTA acts as a resilient security framework that enhances the protection of resources in cloud environments by removing the assumption of trust and enforcing stringent access controls. Implementing it can significantly reduce security vulnerabilities and strengthen the resilience of enterprise systems against cyber threats. In the next section, we'll comprehensively analyze how Azure ZTA can be implemented in a mid-size company migrating to the cloud.

4. Experimental Setup and Study Methodology

We used a test Azure environment with a custom scenario while researching the topic of this paper. Suppose we must implement Azure ZTA in an organization transitioning to a cloud-centric infrastructure. The organization must ensure secure access to resources while managing a distributed workforce. The focus is on identity and access management (IAM) to protect sensitive data and services. The practical implementation involves setting up Microsoft Entra ID for identity management, configuring MFA, Self-Service Password Reset (SSPR), Just-In-Time access (JIT), and passwordless authentication, and enforcing access control. It also requires the implementation of a secure network infrastructure, which involves using Azure Network Security Services. The starting point of the process is an Azure tenant and at least one user with a Global Admin role to introduce the changes needed. The first part of the implementation needs to be done in Entra ID, as the most convenient way to implement ZTA starts with the Conditional Access configuration.

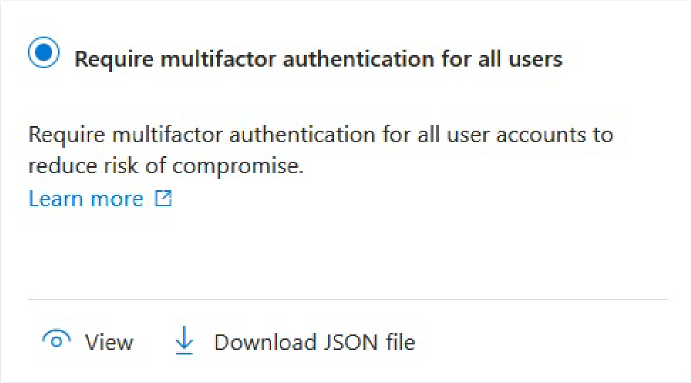
4.1. Azure Conditional Access with MFA and SSPR

Azure Entra ID Conditional Access is crucial to Microsoft's identity and access management service. It helps companies efficiently manage and protect access to their applications and data. Organizations can employ this capability to implement automatic access control decisions based on pre-established regulations. These policies enable administrators to create specific access rules and criteria, ensuring only authorized users can access sensitive information. Conditions may include several elements such as user characteristics, device adherence, geographical location, and amount of danger. Organizations can enhance security by combining several measures, such as implementing multi-factor authentication, restricting access to specific locations, or enforcing device compliance checks. This high level of exact control enhances security by ensuring that access is granted only when specified conditions are met, thereby preventing unauthorized entrance and improving overall security.

For CA to work, we need to meet specific requirements:

- We need to turn off security defaults;
- We need to disable per-user MFA;
- We need a license that supports it (Business Premium, Entra ID P1 or P2).

After we activate the required license, Azure UI takes us to the Microsoft 365 Admin Center, where we get the list of available permits and, if we’re using a trial license, when the trial is valid. We can turn off the security defaults and start configuring Conditional Access Policies there. The first policy that seems to be a reasonable starting point is to enforce MFA for all users. This makes the environment much more secure as we don’t have to rely only on passwords that can be brute forced if not configured correctly. So, after we get to the Home/Default Directory/Conditional Access tab, we can select the following blade from the UI:

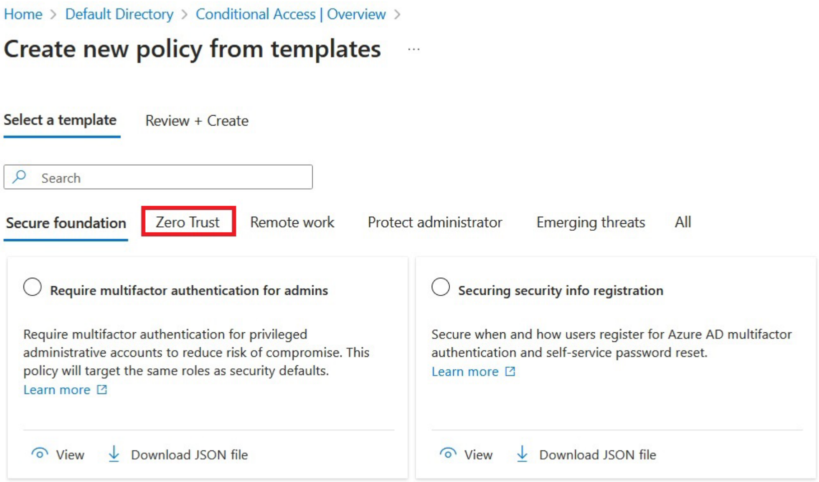


● Require multifactor authentication for all users

Require multifactor authentication for all user accounts to reduce risk of compromise.

Figure 1. Configuring MFA as a mandatory Conditional Access Policy from a template.

There’s a “Zero Trust” tab available here, with a selection of templates to use for ZTA implementation, as we can see in Figure 2:



Home > Default Directory > Conditional Access | Overview >

Create new policy from templates ...

Select a template | Review + Create

Search

Secure foundation | Zero Trust | Remote work | Protect administrator | Emerging threats | All

○ Require multifactor authentication for admins

Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults. Learn more

View | Download JSON file

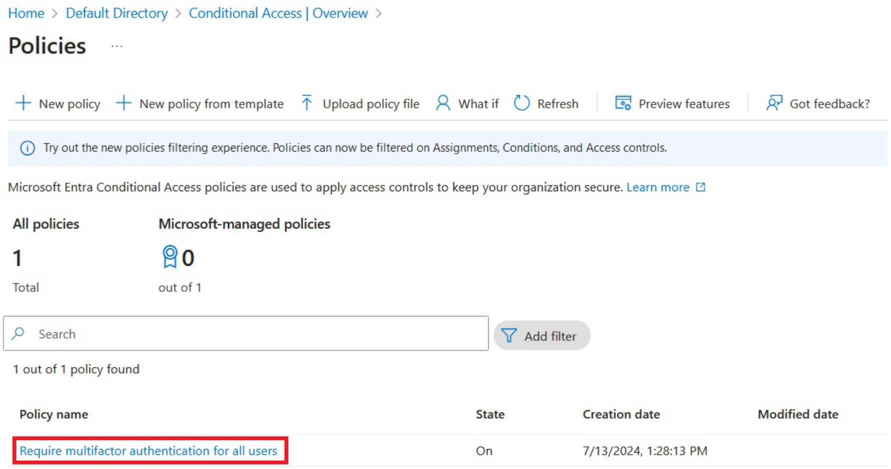
○ Securing security info registration

Secure when and how users register for Azure AD multifactor authentication and self-service password reset. Learn more

View | Download JSON file

Figure 2. There's a selection of Zero Trust templates available for configuration in Conditional Access in Azure.

We can quickly check which Conditional Access Policies are enabled for our tenant, as can be seen in Figure 3:



Home > Default Directory > Conditional Access | Overview >

Policies ...

+ New policy | + New policy from template | Upload policy file | What if | Refresh | Preview features | Got feedback?

Try out the new policies filtering experience. Policies can now be filtered on Assignments, Conditions, and Access controls.

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies: 1 Total

Microsoft-managed policies: 0 out of 1

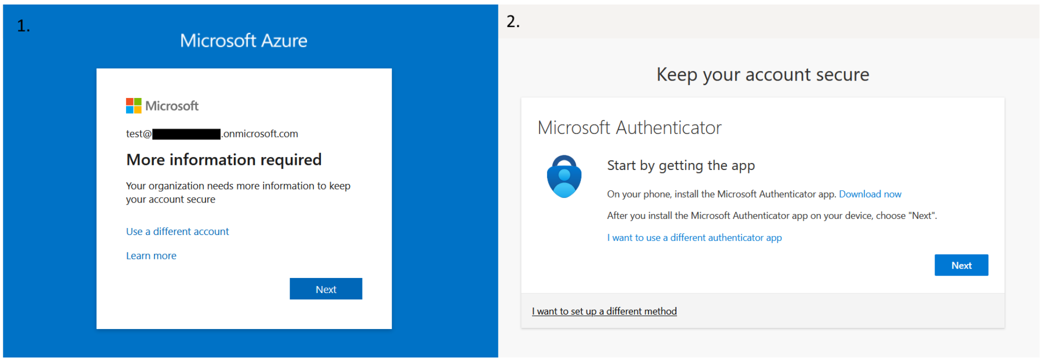
Search | Add filter

1 out of 1 policy found

Policy name	State	Creation date	Modified date
Require multifactor authentication for all users	On	7/13/2024, 1:28:13 PM	

Figure 3. Enabled Central Access Policies.

After enabling this specific Central Access Policy, we will get a familiar message when dealing with MFA on Azure, as we can see in Figure 4:



1.

Microsoft Azure

Microsoft

test@[redacted].onmicrosoft.com

More information required

Your organization needs more information to keep your account secure

Use a different account

Learn more

Next

2.

Keep your account secure

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

Next

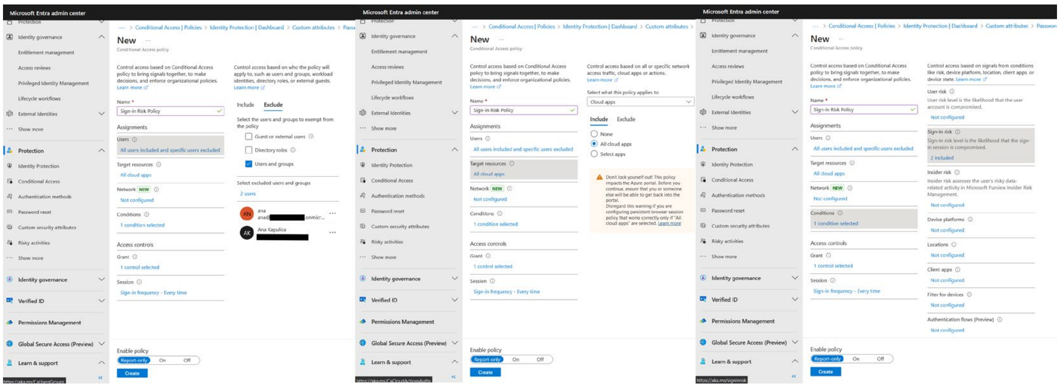
I want to set up a different method

Figure 4. MFA in action – we must install Microsoft Authenticator to log in to our Azure environment.

Now that we have the basic Central Access Policy, we must add additional security measures to follow the ZTA architecture. In this regard, Microsoft recommends implementing additional risk policy configurations to protect our environment, specifically the User and Sign-in risk policies.

User risk policy requires a secure password change if a user's risk level is detected as high. MFA is required before a password change is doable, so we first enforced the MFA policy on all users, as this significantly increased the baseline security level.

The Sign-in risk policy requires MFA if a sign-in risk level is detected as medium or high. This way, the user can prove they are while trying to sign in. It's good practice to have some emergency access or a break-glass account(s) during these implementations so we don't lock ourselves out of our tenant. Let's first configure the Sign-in policy, as we can see in Figure 5:



··· > Conditional Access | Policies > Identity Protection | Dashboard > Custom attributes > Passw

New ···
Conditional Access policy

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

Name *
Sign-in Risk Policy

Assignments
Users: All users included and specific users excluded
Target resources: All cloud apps
Network NEW: Not configured
Conditions: 1 condition selected

Access controls
Grant: 1 control selected
Session: Sign-in frequency - Every time

Enable policy: [✓ Report-only] On Off
Create

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

Include | Exclude

Select the users and groups to exempt from the policy
☐ Guest or external users
☐ Directory roles
☑ Users and groups

Select excluded users and groups
2 users
AN ana
ana@[redacted]onmicr...
AK Ana Kapulica
[redacted]

Control access based on all or specific network access traffic, cloud apps or actions. Learn more

Select what this policy applies to: Cloud apps

Include | Exclude
○ None
● All cloud apps
○ Select apps

Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal.
Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected. Learn more

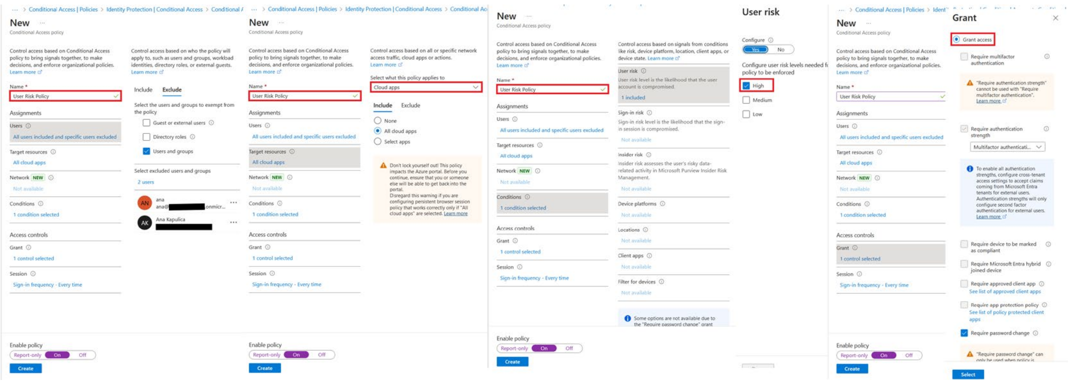
Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk: User risk level is the likelihood that the user account is compromised. Not configured
Sign-in risk: Sign-in risk level is the likelihood that the sign-in session is compromised. 2 included
Insider risk: Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management. Not configured
Device platforms: Not configured
Locations: Not configured
Client apps: Not configured
Filter for devices: Not configured
Authentication flows (Preview): Not configured

Figure 5. Configuration of a sign-in policy.

By having a break-glass account, we can target our policy so we won't lock ourselves out of the environment. Specifically, we want to configure the policy only to affect specific users (in our scenario, test users) and target the policy to resources needing it (for example, cloud applications). In this way, we can use conditions to segment controls based on sign-in risk level and select our specific level (for example, medium and high). The "Grant" part of the policy requires us to choose what the policy grants or blocks if the conditions are met – in our scenario, it grants access to MFA every time a user tries to sign in.

The next step is configuring the User risk policy, as can be seen in Figure 6:



··· > Conditional Access | Policies > Identity Protection | Conditional Access > Conditional A

New ···
Conditional Access policy

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

Name *
User Risk Policy

Assignments
Users: All users included and specific users excluded
Target resources: All cloud apps
Network NEW: Not available
Conditions: 1 condition selected

Access controls
Grant: 1 control selected
Session: Sign-in frequency - Every time

Enable policy: Report-only [✓ On] Off
Create

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

Include | Exclude

Select the users and groups to exempt from the policy
☐ Guest or external users
☐ Directory roles
☑ Users and groups

Select excluded users and groups
2 users
AN ana
ana@[redacted]onmicr...
AK Ana Kapulica
[redacted]

Control access based on all or specific network access traffic, cloud apps or actions. Learn more

Select what this policy applies to: Cloud apps

Include | Exclude
○ None
● All cloud apps
○ Select apps

Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal.
Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected. Learn more

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

User risk: User risk level is the likelihood that the user account is compromised. 1 included
Sign-in risk: Sign-in risk level is the likelihood that the sign-in session is compromised. Not available
Insider risk: Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management. Not available
Device platforms: Not available
Locations: Not available
Client apps: Not available
Filter for devices: Not available

Some options are not available due to the "Require password change" grant

User risk

Configure: [✓ Yes] No

Configure user risk levels needed f policy to be enforced
☑ High
☐ Medium
☐ Low

Grant

● Grant access
☐ Require multifactor authentication

"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more

☑ Require authentication strength
Multifactor authenticati...

To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. Learn more

☐ Require device to be marked as compliant
☐ Require Microsoft Entra hybrid 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

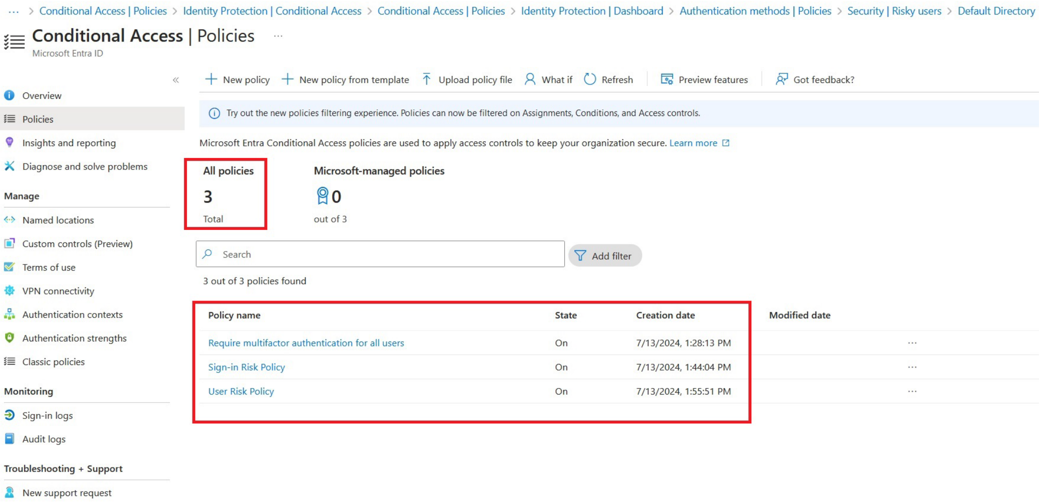
"Require password change" can only be used when policy is

Select

Figure 6. Configuration of a user risk policy.

We can check if the process has finished successfully by checking Conditional Access Policies, as can be seen in Figure 7:

doi:10.20944/preprints202407.1454.v1



Conditional Access | Policies

Try out the new policies filtering experience. Policies can now be filtered on Assignments, Conditions, and Access controls.

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies: 3 Total

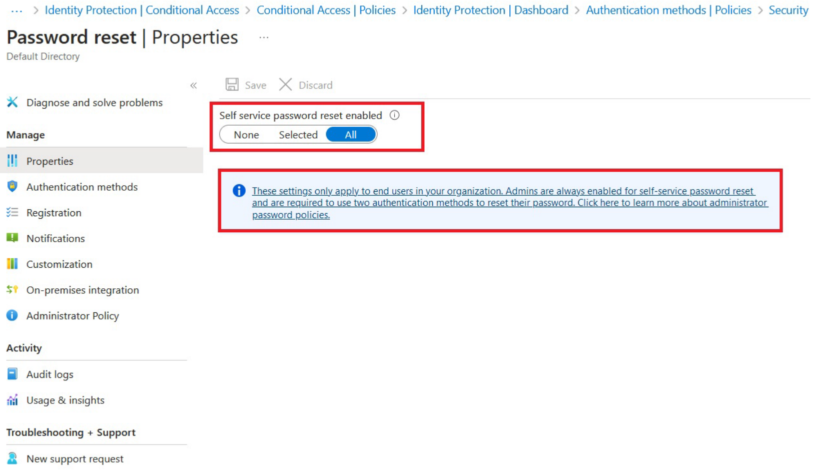
Microsoft-managed policies: 0 out of 3

3 out of 3 policies found

Policy name	State	Creation date	Modified date
Require multifactor authentication for all users	On	7/13/2024, 1:28:13 PM	
Sign-in Risk Policy	On	7/13/2024, 1:44:04 PM	
User Risk Policy	On	7/13/2024, 1:55:51 PM	

Figure 7. Verify whether our Conditional Access Policies have been enabled and configured correctly.

The next logical step in our ZTA process should be to enable SSPR (Self-Service Password Reset). The critical point here is that SSPR can be enabled with MFA, which makes the overall process much more secure. The configuration can be seen in Figure 8:


… > Identity Protection | Conditional Access > Conditional Access | Policies > Identity Protection | Dashboard > Authentication methods | Policies > Security
Default Directory
Diagnose and solve problems
Manage
Properties
Authentication methods
Registration
Notifications
Customization
On-premises integration
Administrator Policy
Activity
Audit logs
Usage & insights
Troubleshooting + Support
New support request
Save
Discard

Password reset | Properties

Self service password reset enabled: None Selected [✓ All]

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

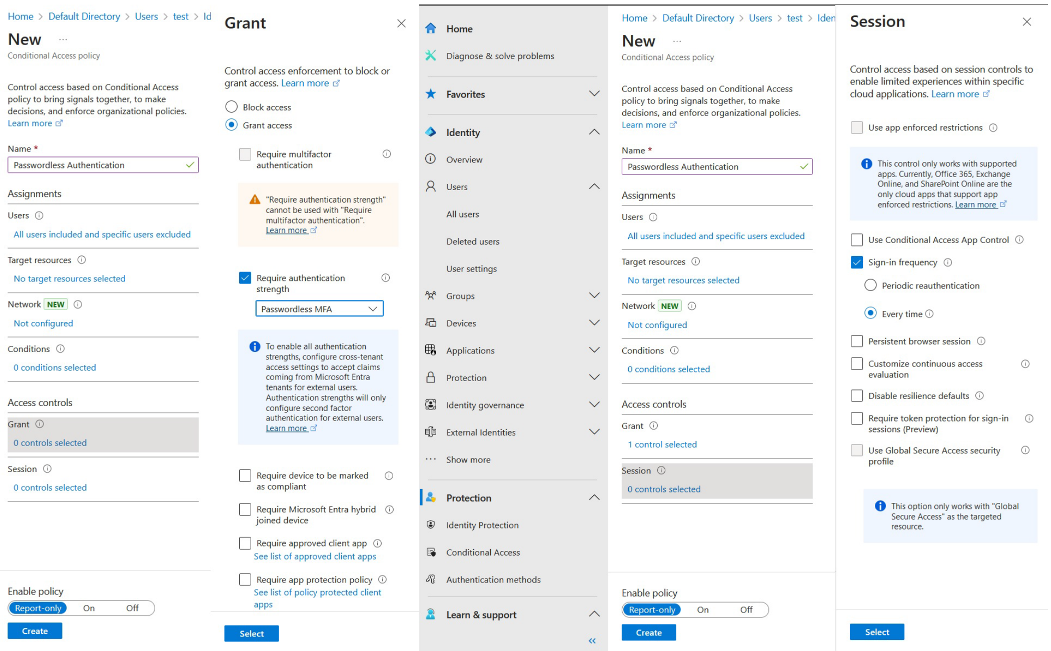
Figure 8. Enabling SSPR with Conditional Access Policies in place.

This will also help reduce helpdesk dependence and allow more user convenience while assisting in the timely resolution of account lockouts without compromising security

4.2. Azure Passwordless Authentication

Let’s now analyze Azure’s passwordless authentication option. By using this capability, we can eliminate vulnerabilities associated with traditional passwords, such as weak passwords, re-using old passwords, and phishing attacks. In ZTA, where continuous verification and strong authentication are important, passwordless methods (like biometrics, hardware tokens, or mobile authenticator apps) ensure that only legitimate users can access resources. This approach reduces the attack surface, enhances user experience with seamless logins, and aligns with Zero Trust principles by requiring multifactor authentication and reducing reliance on potentially compromised credentials.

We will enable passwordless authentication by implementing another conditional access policy, as can be seen in Figure 9:



New ...
Conditional Access policy

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

Name *
Passwordless Authentication

Assignments

Users
All users included and specific users excluded

Target resources
No target resources selected

Network NEW
Not configured

Conditions
0 conditions selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy
Report-only On Off

Grant

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
Passwordless MFA

To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. Learn more

□ Require device to be marked as compliant
□ Require Microsoft Entra hybrid joined device
□ Require approved client app
See list of approved client apps
□ Require app protection policy
See list of policy protected client apps

New ...
Conditional Access policy

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

Name *
Passwordless Authentication

Assignments

Users
All users included and specific users excluded

Target resources
No target resources selected

Network NEW
Not configured

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Enable policy
Report-only On Off

Session

Control access based on session controls to enable limited experiences within specific cloud applications. Learn more

□ Use app enforced restrictions

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more

□ Use Conditional Access App Control
☑ Sign-in frequency
○ Periodic reauthentication
● Every time
□ Persistent browser session
□ Customize continuous access evaluation
□ Disable resilience defaults
□ Require token protection for sign-in sessions (Preview)
□ Use Global Secure Access security profile

This option only works with "Global Secure Access" as the targeted resource.

Figure 9. Setup for Conditional Access Policy for passwordless MFA.

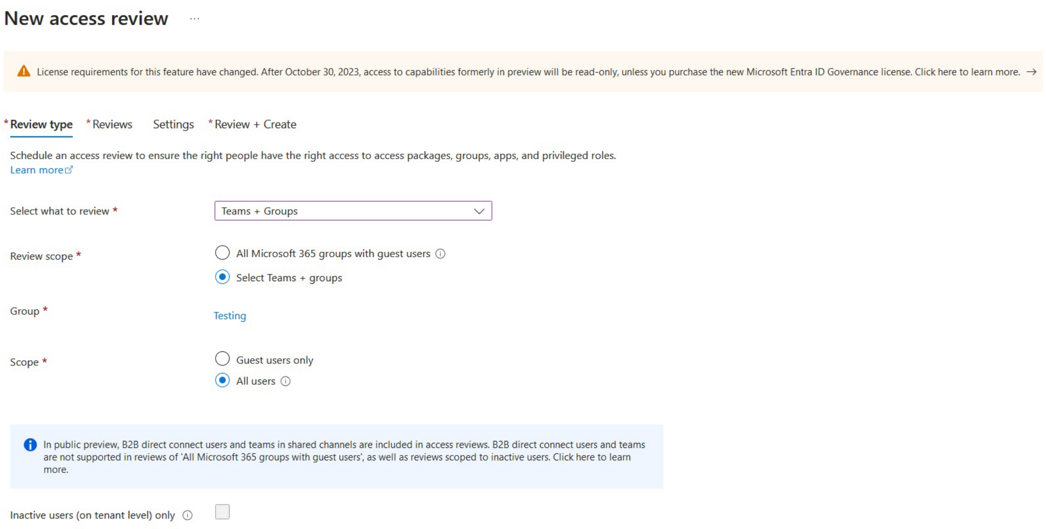
This is a fundamental change in the way we approach authentication in terms of ease of use; if we were to implement the same idea in the private data center, we would be forced to configure multiple services like Active Directory Certificate Services (AD CS), Active Directory Federation Services (AD FS), Microsoft Identity Manager (MIM) or create a hybrid Active Directory (AD) with Entra ID to get access to an equivalent set of features.

4.3. Azure Access Review

Azure access reviews, a Microsoft Entra ID Governance component, enable organizations to effectively oversee and regulate user access to resources. Organizations can guarantee that only authorized users keep access by implementing regular evaluations of group memberships, application access, and role assignments. This approach aids in reducing security risks, ensuring compliance with regulatory standards, and adhering to the principle of least privilege. Automated reviews can be tailored to specific scenarios, such as privileged roles or critical data access, and can be seamlessly incorporated with other Azure AD features to provide a complete identity governance solution.

Access reviews are an essential part of ZTA architecture, as they ensure that users have the appropriate level of access based on their current roles. It also forces us to do regular reviews and validations to help enforce the fundamental "least privilege" principle, reducing the risk of unauthorized access, which further aligns with ZTA's "never trust, always verify" core mantra.

To create an access review, we need an access review scope, for example, a group, as can be seen in Figure 11:



New access review ···

⚠ License requirements for this feature have changed. After October 30, 2023, access to capabilities formerly in preview will be read-only, unless you purchase the new Microsoft Entra ID Governance license. Click here to learn more. →

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles.
Learn more

Select what to review *: Teams + Groups

Review scope *: ○ All Microsoft 365 groups with guest users ⓘ ● Select Teams + groups

Group *: Testing

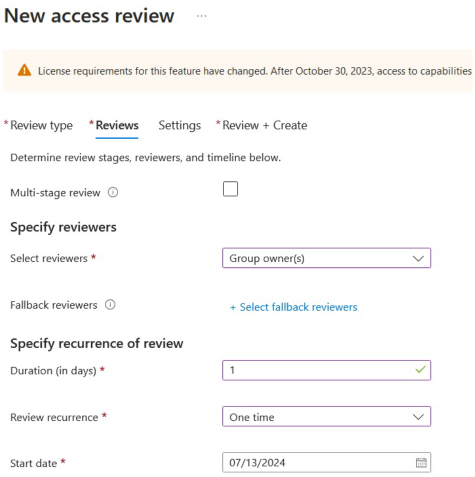
Scope *: ○ Guest users only ● All users ⓘ

ⓘ In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.

Inactive users (on tenant level) only ⓘ □

Figure 10. Creating an Azure access review.

This implementation method ensures that all members of a particular group will be reviewed. The access review wizard asks for some additional settings, like selecting reviewers, people who will have the chance to do the access review, as can be seen in Figure 11:



New access review ···

⚠ License requirements for this feature have changed. After October 30, 2023, access to capabilities

Determine review stages, reviewers, and timeline below.

Multi-stage review ⓘ □

Specify reviewers

Select reviewers *: Group owner(s)

Fallback reviewers ⓘ: + Select fallback reviewers

Specify recurrence of review

Duration (in days) *: 1

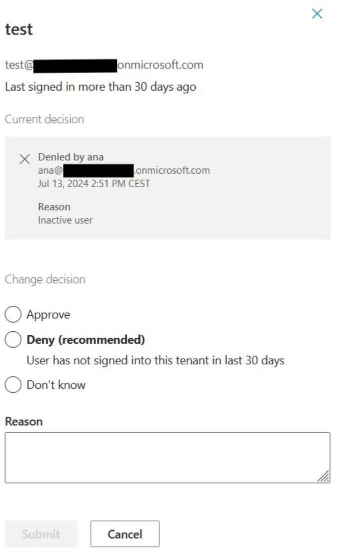
Review recurrence *: One time

Start date *: 07/13/2024

Figure 11. Additional settings for access review.

Based on these settings, the group owner will do the review; it will last for one day and will be a one-time occurrence.

Settings selected in the wizard will configure access review but will not start its implementation. If the reviewer has an email inbox, an email will be there, prompting the start of the review. The other way to begin the review process is from the My Access portal. Let's say we treat the access review process as an attack and want to deny access. We'd select the necessary settings for that in the My Access/Access reviews tab, as demonstrated in Figure 12:



test

test@[redacted]onmicrosoft.com
Last signed in more than 30 days ago

Current decision

Denied by ana
ana@[redacted].onmicrosoft.com
Jul 13, 2024 2:51 PM CEST

Reason
Inactive user

Change decision

○ Approve
○ **Deny (recommended)**
User has not signed into this tenant in last 30 days
○ Don't know

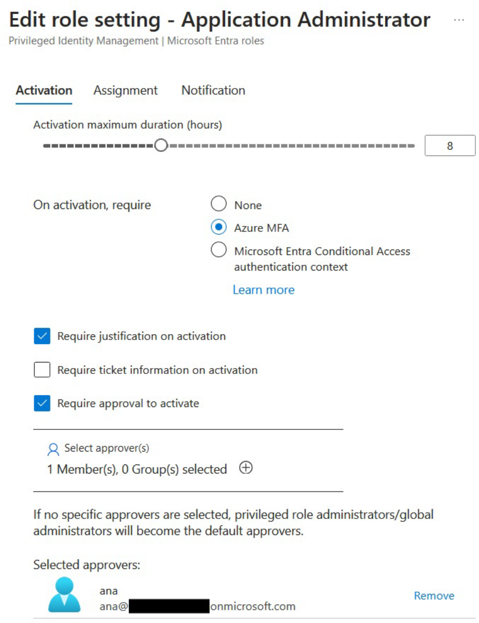
Reason

Figure 12. Wizard for approving or denying access review.

The decision can still be changed after it has been made until the review itself ends. An overview of the entire review process can be seen under the Access review details overview window in the Microsoft Entra admin center.

4.4. JIT Access

Continuing with the Zero Trust Architecture implementation, Just-In-Time (JIT) access is critical in a Zero Trust Architecture because it minimizes the risk of excessive or unused privileges being exploited by attackers. By granting privileged access only when needed and for a limited duration, JIT access ensures that users have the least amount of privilege necessary to perform their tasks. This reduces the potential attack surface and aligns with the Zero Trust principle of "least privilege." Implementing JIT through Azure's Privileged Identity Management (PIM) helps secure administrative tasks, prevent privilege abuse, and maintain continuous verification. Let's prepare one of the Azure roles for JIT access, as seen in Figure 13:



Edit role setting - Application Administrator
Privileged Identity Management | Microsoft Entra roles

Activation maximum duration (hours): 8

On activation, require
○ None
● Azure MFA
○ Microsoft Entra Conditional Access authentication context
Learn more

☑ Require justification on activation
□ Require ticket information on activation
☑ Require approval to activate

Select approver(s)
1 Member(s), 0 Group(s) selected

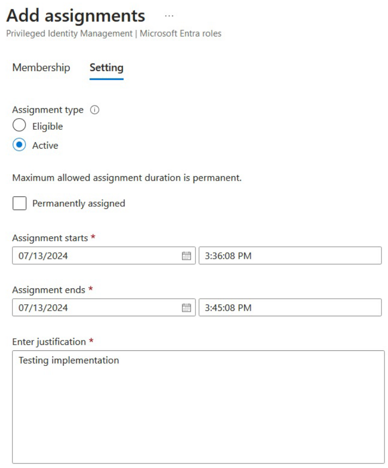
If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers.

Selected approvers:
ana
ana@[redacted]onmicrosoft.com
Remove

Figure 13. Preparing Azure Application Administrator role for JIT.

The maximum duration of the activation has been set to 8 hours; the duration of the activation depends on the organization's needs. We have also checked off the "Require justification on activation" and "Require approval to activate" for extra security.

After configuring some of the settings, we can continue to add the assignment to our test user, as shown in Figure 14:



Add assignments ···
Privileged Identity Management | Microsoft Entra roles

Membership   Setting

Assignment type ⓘ
○ Eligible
● Active

Maximum allowed assignment duration is permanent.

□ Permanently assigned

Assignment starts *
07/13/2024   3:36:08 PM

Assignment ends *
07/13/2024   3:45:08 PM

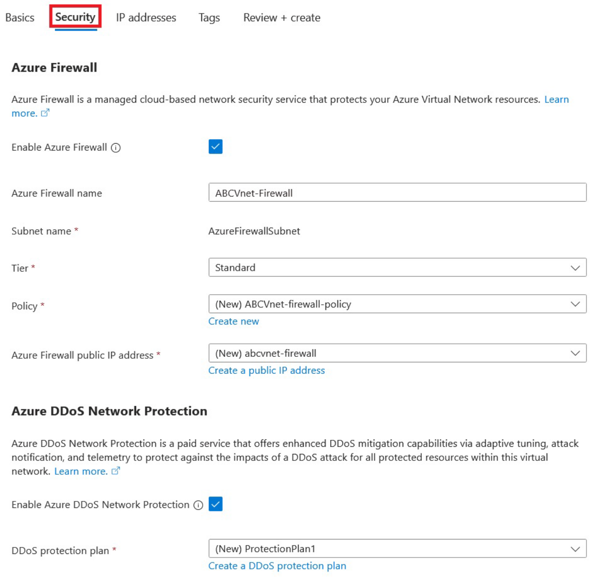
Enter justification *
Testing implementation

Figure 14. After selecting the role for membership, we can add a JIT assignment.

We can view all added assignments through the Assignments tab for the particular role, where we can also remove, update, or extend them.

4.5. Application of Azure ZTA on Azure Networking

Besides achieving Zero Trust in identity management, it is also important to protect network resources. Achieving Zero Trust with network security in Azure is crucial because it ensures comprehensive protection across all layers of your cloud environment. This approach reduces the attack surface and helps prevent breaches by ensuring that every network transaction is authenticated and authorized. We can do this on any existing or new Azure virtual network by going to the "Security" configuration tab, as can be seen in Figure 15:



Basics   Security   IP addresses   Tags   Review + create

Azure Firewall

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. Learn more.

Enable Azure Firewall ⓘ ☑

Azure Firewall name: ABCVnet-Firewall

Subnet name *: AzureFirewallSubnet

Tier *: Standard

Policy *: (New) ABCVnet-firewall-policy
Create new

Azure Firewall public IP address *: (New) abcvnet-firewall
Create a public IP address

Azure DDoS Network Protection

Azure DDoS Network Protection is a paid service that offers enhanced DDoS mitigation capabilities via adaptive tuning, attack notification, and telemetry to protect against the impacts of a DDoS attack for all protected resources within this virtual network. Learn more.

Enable Azure DDoS Network Protection ⓘ ☑

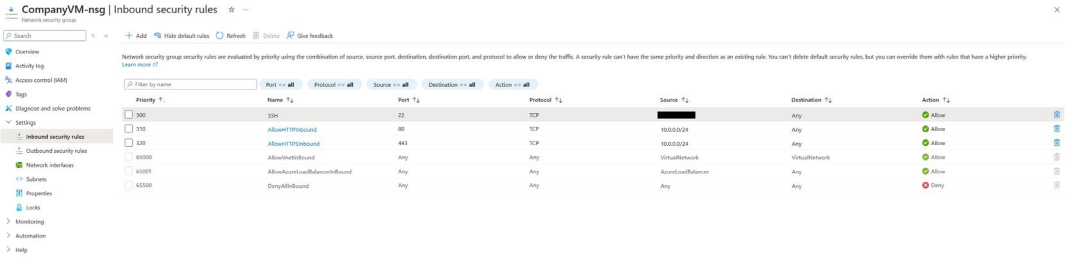
DDoS protection plan *: (New) ProtectionPlan1
Create a DDoS protection plan

Figure 15. Configuring ZTA options for a new Azure virtual network.

doi:10.20944/preprints202407.1454.v1

The "AzureFirewallManagementSubnet" is the subnet used for firewall management traffic. It separates the management plane traffic, such as logging, monitoring, and configuration changes, from the data plane traffic for better security and compliance. Therefore, if we create a Virtual Machine and put it in one of those subnets, it will mix VM workloads with firewall operations, which can compromise network security and the firewall's performance.

After this configuration, we can use an existing or a new VM and associate it with the Azure virtual network created in the previous step. All configured security settings within the virtual network also apply to the virtual machine. One more configuration for its security is left, configuring its network security group on the network interface card level to provide more granular control of inbound and outbound traffic. It ensures that each VM independently manages its network traffic filtering rather than relying on a centralized firewall for all firewalling tasks, which aligns with the context of Zero Trust networks. We can also use this to provision network security group inbound and outbound rules to standardize inbound and outbound firewall rules for any VM, as can be seen in Figure 16 for inbound rules:



Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority.
Learn more

Priority ↑	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
□ 300	SSH	22	TCP	[redacted]	Any	✓ Allow
□ 310	AllowHTTPInbound	80	TCP	10.0.0.0/24	Any	✓ Allow
□ 320	AllowHTTPSInbound	443	TCP	10.0.0.0/24	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Figure 16. Azure NSG inbound rules.

These inbound rules are standard inbound rules. The SSH connections for testing purposes in this demonstration are only allowed from a specific public IP address, and HTTP and HTTPS traffic is allowed from only select subnets. In this scenario, a company subnet could access an internal site hosted on that virtual machine. This ensures no outsider can access the internal network, strengthening the organization's security posture.

5. Analyzing Azure ZTA Implementation and Its Implications

In our implementation, we successfully established a Zero Trust Architecture using Microsoft Azure. This approach demonstrates how a zero-trust model can protect an organization's resources by continuously verifying identities and strictly controlling access, thereby reducing the risk of security breaches in a cloud-centric environment.

We implemented Azure ZTA by employing an extensive array of security measures:

- Multi-factor authentication is a security measure that mandates using multiple verification methods to gain access, minimizing the chances of illegal access.
- Self-Service Password Reset enables users to manage their passwords securely, reducing the need for administrative intervention.
- Passwordless Authentication: Mitigates the risks associated with weak passwords, bolstering security.
- Access Reviews: Consistently validates permissions to conform with the idea of least privilege.
- Just-In-Time Access: Grants temporary authorization to resources, minimizing vulnerability to potential risks.
- Network Security Group: manages traffic within Azure, providing an additional layer of network security.

Implementing ZTA guarantees a strong security position by consistently validating access requests, anticipating possible breaches, and reducing vulnerable areas that attacks can target. ZTA, or Zero Trust Architecture, is an active security approach that safeguards sensitive data, ensures adherence to regulatory requirements, and improves overall resilience. ZTA combines these technologies to create a flexible and responsive security framework that effectively safeguards corporate resources and tightly regulates and monitors access, even in the face of changing threats. By employing a holistic approach, the danger of data breaches and illegal access is greatly diminished, creating a secure and compliant IT environment.

It is essential to consider certain disadvantages. Implementing and configuring a Zero Trust Architecture can be intricate and time-intensive, necessitating a substantial commitment in terms of time and experience. Due to duplicate features in multiple locations, the Azure portal can present challenges, particularly for inexperienced users. However, some of these features may not function as intended, exhibiting either bugs or inconsistent results despite being the same feature but in a different location. Organizations lacking a dedicated IT security team may find disabling security settings and establishing customized policies challenging. In addition, although Azure provides a free trial for many services, utilizing advanced capabilities such as Microsoft Entra ID P2 licensing for an extended period incurs extra expenses, which can be significant for large enterprises.

Another possible drawback is the difficulty level involved in handling and keeping the Zero Trust Architecture. Organizations must ensure their staff receive comprehensive training to manage the new security protocols and tools effectively. This may require continuous training and education to stay updated on the ever-changing security threats and updates to Azure services. Organizations must consider these variables regarding improved security and operational benefits to assess whether this approach aligns with their strategic goals and available resources.

6. Future Work

Five major topics should be researched in the future from the perspective of Azure ZTA implementation: complex micro-segmentation, continuous monitoring and analytics, Data Loss Prevention (DLP), more broad integration of Machine Learning (ML) to help with the deployment process, and Secure Access Service Edge (SASE) implementation. We will strengthen our security position by improving our implementation of ZTA, especially for large-scale organizations.

Micro-segmentation divides the network into smaller, distinct sections to limit the lateral expansion of security vulnerabilities. By employing micro-segmentation, we may create specific security protocols that restrict access to essential assets based on specific criteria, such as user roles, device types, and application contexts. This method enhances the system's resistance to attacks and confines any breaches to a particular location, thus avoiding their spread over the entire network. Furthermore, micro-segmentation improves compliance efforts by ensuring that sensitive data remains inside predefined boundaries. This limits the lateral movement of threats and protects sensitive resources by ensuring that only authorized traffic can flow between segments. Azure Virtual Network (VNet) peering allows secure communication between segments, while Azure Security Center provides continuous monitoring and recommendations for segmentation policies.

Consistent surveillance and analysis are essential for maintaining an up-to-date and efficient security posture. Utilizing software like Microsoft Sentinel may obtain real-time and ongoing knowledge of our environment, allowing us to recognize and deal with developing dangers immediately. Sentinel efficiently integrates multiple data sources to provide comprehensive security analytics and threat intelligence. The system employs machine learning and artificial intelligence to identify anomalies and potential security breaches, enabling proactive threat detection and swift crisis response. Continuous monitoring allows us to swiftly adapt to evolving threats and maintain high security across our system.

DLP solutions protect sensitive data by avoiding unauthorized access and unintentional disclosure of information. By enforcing DLP standards, we may efficiently monitor, detect, and stop the transfer of sensitive information across different devices, networks, and cloud platforms. DLP solutions can monitor and control data flow while enforcing rules prohibiting unlawful data transfer. This ensures that confidential information remains within the organization's control. This capability is crucial for protecting intellectual property and personal information and complying with regulatory requirements like GDPR and HIPAA. This is also an area where ML integration might substantially help when dealing with various regulatory compliance frameworks.

SASE combines network security functionalities with wide-area network (WAN) capabilities to create secure connections among users, systems, and devices. The SASE framework integrates several components to make a unified system, such as secure online gateways, cloud access security brokers, firewall-as-a-service, and zero trust network access. This technique ensures the consistent enforcement of security policies, regardless of the user's geographical location, guaranteeing secure and uninterrupted access to applications and data. SASE enables the shift to a decentralized workforce by offering secure remote access and streamlining the administration of multiple security solutions.

By incorporating these technologies into our Zero Trust Architecture (ZTA), we enhance our ability to detect, reduce, and resolve security vulnerabilities, ensuring a strong and secure environment. The subsequent protocols for executing ZTA will aid us in guaranteeing robust security, protecting confidential data, and complying with evolving regulatory requirements.

7. Conclusions

Utilizing Microsoft Azure to implement a Zero Trust Architecture provides notable security benefits. One of the main advantages is the heightened security provided by implementing MFA for all users. This supplementary level of protection guarantees that simply possessing a password is inadequate for gaining access to the system, diminishing the likelihood of unauthorized entry. By implementing conditional access controls, security is strengthened as security requirements are applied dynamically depending on the risk levels of users and devices. This method facilitates the ongoing surveillance and validation of identities, essential for upholding a strong security stance in a cloud-focused setting.

Another benefit is decreasing vulnerable areas targeted for attacks by implementing passwordless authentication techniques like biometrics, hardware tokens, or mobile authenticator apps. These solutions mitigate the risks commonly associated with standard passwords, including using weak passwords, password reuse, and susceptibility to phishing attempts. In Azure's Privileged Identity Management (PIM), the implementation of Just-In-Time (JIT) access guarantees that users are granted just the essential privileges for the shortest possible duration by the Zero Trust principle of least privilege. By doing this, the likelihood of power misuse is reduced, and the overall security architecture is strengthened.

The implementation also incorporates functionalities that enhance user experience and optimize operational efficiency. Implementing self-service password resets decreases reliance on help desk assistance and empowers users to fix account lockouts quickly, ultimately improving user convenience and productivity. Regular access reviews ensure that permissions are consistently updated to align with users' roles and responsibilities, adhering to the zero-trust principle of ongoing verification.

Author Contributions: Conceptualization, V.D.; Methodology, V.D. and Z.M.; Validation, A.K. and Z.M.; Formal analysis, D.R. and A.K.; Investigation, D.R. and A.K; Resources, D.R.; Writing—original draft, Z.M. and D.R.; Writing—review & editing, V.D.; Supervision, V.D.; Project administration, V.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Paul, B.; Rao, M. Zero-Trust Model for Smart Manufacturing Industry. Applied Sciences 2022, 13, 221. doi: https://doi.org/10.3390/app13010221.
2. Thantharate, P.; Thantharate, A. ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain. BDCC 2023, 7, 165. doi: https://doi.org/10.3390/bdcc7040165.

3. Federici, F.; Martintoni, D.; Senni, V. A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. Electronics 2023, 12, 566. doi: https://doi.org/10.3390/electronics12030566.
4. Gupta, A.; Khan, H.; Nazir, S.; Shafiq, M.; Shabaz, M. Metaverse Security: Issues, Challenges and a Viable ZTA Model. Electronics 2023, 12, 391. doi: https://doi.org/10.3390/electronics12020391.
5. Daah, C.; Qureshi, A.; Awan, I.; Konur, S. Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. Electronics 2024, 13, 865. doi: https://doi.org/10.3390/electronics13050865.
6. Awan, S.M.; Azad, M.A.; Arshad, J.; Waheed, U.; Sharif, T. A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT. Information 2023, 14, 129. doi: https://doi.org/10.3390/info14020129.
7. Zaid, B.; Sayeed, A.; Bala, P.; Alshehri, A.; Alanazi, A.M.; Zubair, S. Toward Secure and Resilient Networks: A Zero-Trust Security Framework with Quantum Fingerprinting for Devices Accessing Network. Mathematics 2023, 11, 2653. doi: https://doi.org/10.3390/math11122653.
8. Sarkar, S.; Choudhary, G.; Shandilya, S.K.; Hussain, A.; Kim, H. Security of Zero Trust Networks in Cloud Computing: A Comparative Review. Sustainability 2022, 14, 11213. doi: https://doi.org/10.3390/su141811213.
9. Alberti, E.; Alvarez-Napagao, S.; Anaya, V.; Barroso, M.; Barrué, C.; Beecks, C.; Bergamasco, L.; Chala, S.A.; Gimenez-Abalos, V.; Graß, A.; et al. AI Lifecycle Zero-Touch Orchestration within the Edge-to-Cloud Continuum for Industry 5.0. Systems 2024, 12, 48. doi: https://doi.org/10.3390/systems12020048.
10. S. Rose, O. Borchert, Stu Mitchell, S. Connelly, "Zero Trust Architecture," 2019, doi: https://doi.org/10.6028/nist.sp.800-207-draft.
11. Songpon Teerakanok, T. Uehara, A. Inomata, "Migrating to Zero Trust Architecture: Reviews and Challenges," Secur. Commun. Networks, 2021, doi: doi: https://doi.org/10.1155/2021/9947347.
12. Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, Xiangjie Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," Wireless Communications and Mobile Computing, 2022, doi: doi: https://doi.org/10.1155/2022/6476274.
13. Po-Han Ho, Hong-Yen Chen, Tsungnan Lin, "Zero Trust Architecture of Token Network," 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), 2023, doi: doi: https://doi.org/10.1109/MetaCom57706.2023.00120.
14. Xu Chen, Wei Feng, Ning Ge, Yan Zhang, "Zero Trust Architecture for 6G Security," ArXiv, 2022, doi: doi: https://doi.org/10.48550/arXiv.2203.07716.
15. Farhan Qazi, "Study of Zero Trust Architecture for Applications and Network Security," 2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), 2022, doi: doi: https://doi.org/10.1109/HONET56683.2022.10019186.
16. Sirshak Sarkar, Gaurav Choudhary, Shishir K. Shandilya, Azath Hussain, Hwankuk Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," Sustainability, 2022, doi: doi: https://doi.org/10.3390/su141811213.
17. Saubhagya Munasinghe, Nuwan Piyarathna, Erandana Wijerathne, Upul Jayasinghe, Suneth Namal, "Machine Learning Based Zero Trust Architecture for Secure Networking," 2023 IEEE 17th International Conference on Industrial and Information Systems (ICIIS), 2023, doi: doi: https://doi.org/10.1109/ICIIS58898.2023.10253610.
18. Copeland, M., & Jacobs, M. (2020). Azure Network Security Configuration. Springer. doi: https://doi.org/10.1007/978-1-4842-6531-4_2.
19. Chilberto, J., Zaal, S., Aroraa, G., & Price, E. (2020). Identity Security with Azure Active Directory. Springer. doi: https://doi.org/10.1007/978-1-4842-5437-0_7.
20. Stiles, D. (2019). The Hardware Security Behind Azure Sphere. IEEE Micro, 39, 20-28. doi: https://doi.org/10.1109/MM.2019.2898633.
21. Jensen, D. (2019). Azure IoT Edge Security. Beginning Azure IoT Edge Computing. doi: https://doi.org/10.1007/978-1-4842-4536-1_8.
22. Ward, B. (2020). Securing Azure SQL. Springer. doi: https://doi.org/10.1007/978-1-4842-5931-3_6.
23. Chaturvedi, C., & Gupta, B. (2020). Cloud Computing Security. Handbook of Research on Intrusion Detection Systems. doi: https://doi.org/10.4018/978-1-7998-2242-4.ch015.
24. De Tender, P., Rendón, D., & Erskine, S. (2019). Azure Sentinel (Preview). Pro Azure Governance and Security. doi: https://doi.org/10.1007/978-1-4842-4910-9_8.
25. Nightingale, E. B. (2019). A View from Industry: Securing IoT with Azure Sphere. Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications. doi: https://doi.org/10.1145/3301293.3302378.
26. Chandrasekara, C., & Herath, P. (2019). Azure DevOps Security Options. Hands-on Azure Boards. doi: https://doi.org/10.1007/978-1-4842-5046-4_8.
27. Ifrah, S. (2020). Secure Your Microsoft Azure Containers. Springer. doi: https://doi.org/10.1007/978-1-4842-5753-1_6.

28. Verma, A., Malla, D., Choudhary, A. K., & Arora, V. (2019). A Detailed Study of Azure Platform & Its Cognitive Services. 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 129-134. doi: https://doi.org/10.1109/COMITCon.2019.8862178.
29. Tanana, D. (2023). Vulnerability Analysis of Azure Blockchain Workbench Key Management System. ArXiv, abs/2301.11569. doi: https://doi.org/10.48550/arXiv.2301.11569.
30. Atlidakis, V., Godefroid, P., & Polishchuk, M. (2020). Checking Security Properties of Cloud Service REST APIs. 2020 IEEE 13th International Conference on Software Testing, Validation and Verification (ICST), 387-397. doi: https://doi.org/10.1109/ICST46399.2020.00046.
31. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2019). Zero Trust Architecture. DOI: https://doi.org/10.6028/nist.sp.800-207-draft.
32. Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and Challenges. Secur. Commun. Networks. DOI: https://doi.org/10.1155/2021/9947347.
33. Rose, S. D. (2021). Planning for a Zero Trust Architecture. DOI: https://doi.org/10.6028/nist.cswp.08042021-draft.
34. Prydybailo, O. B. (2022). Zero trust architecture: the basics organization principles. Connectivity. DOI: https://doi.org/10.31673/2412-9070.2022.051620.
35. Chuan, T., Lv, Y., Qi, Z., Xie, L., & Guo, W. (2020). An Implementation Method of Zero-trust Architecture. Journal of Physics: Conference Series. DOI: https://doi.org/10.1088/1742-6596/1651/1/012010.
36. Ferretti, L., Magnanini, F., Andreolini, M., & Colajanni, M. (2021). Survivable zero trust for cloud computing environments. Comput. Secur. DOI: https://doi.org/10.1016/J.COSE.2021.102419.
37. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. Wireless Communications and Mobile Computing. DOI: https://doi.org/10.1155/2022/6476274.
38. Phiayura, P., & Teerakanok, S. (2023). A Comprehensive Framework for Migrating to Zero Trust Architecture. IEEE Access. DOI: https://doi.org/10.1109/ACCESS.2023.3248622.
39. Edo, O. C., Tenebe, T., Etu, E., Ayuwu, A., Emakhu, J., & Adebiyi, S. (2022). Zero Trust Architecture: Trend and Impact on Information Security. International Journal of Emerging Technology and Advanced Engineering. DOI: https://doi.org/10.46338/ijetae0722_15.
40. Hasan, S., Amundson, I., & Hardin, D. S. (2023). Zero Trust Architecture Patterns for Cyber-Physical Systems. SAE Technical Paper Series. DOI: https://doi.org/10.4271/2023-01-1001.
41. Robinson, P. (2023). Why is zero trust so difficult?. Computer Fraud & Security. DOI: https://doi.org/10.12968/s1361-3723(23)70014-6.
42. Syed, N., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture: A Comprehensive Survey. IEEE Access. DOI: https://doi.org/10.1109/ACCESS.2022.3174679.
43. Paul, B., & Rao, M. (2022). Zero-Trust Model for Smart Manufacturing Industry. Applied Sciences. DOI: https://doi.org/10.3390/app13010221.
44. D'Silva, D., & Ambawade, D. (2021). Building A Zero Trust Architecture Using Kubernetes. 2021 6th International Conference for Convergence in Technology (I2CT). DOI: https://doi.org/10.1109/I2CT51068.2021.9418203.
45. Bertino, E., & Brancik, K. (2021). Services for Zero Trust Architectures - A Research Roadmap. 2021 IEEE International Conference on Web Services (ICWS). DOI: https://doi.org/10.1109/ICWS53863.2021.00016.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.