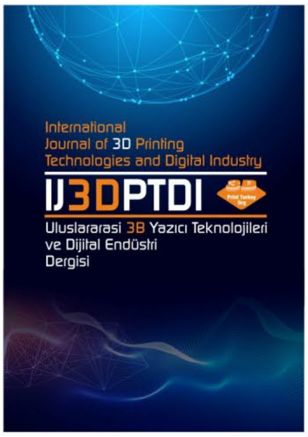
International
Journal of 3D Printing
Technologies and Digital Industry
IJ3DPTDI
Uluslararası 3B Yazıcı Teknolojileri
ve Dijital Endüstri
Dergisi

ULUSLARARASI 3B YAZICI TEKNOLOJİLERİ
VE DİJİTAL ENDÜSTRİ DERGİSİ

INTERNATIONAL JOURNAL OF 3D PRINTING
TECHNOLOGIES AND DIGITAL INDUSTRY

ISSN:2602-3350 (Online)
URL: https://dergipark.org.tr/ij3dptdi

THE ADVANTAGES AND IMPLEMENTATION CHALLENGES WITHIN THE SCOPE OF THE BASIC PRINCIPLES OF TRANSITION TO ZERO TRUST ARCHITECTURE

Yazarlar (Authors): Ahmet Ali SÜZEN*, Osman CEYLAN

Bu makaleye şu şekilde atıfta bulunabilirsiniz (To cite to this article): *Süzen A. A., Ceylan O., "The Advantages and Implementation Challenges Within The Scope of The Basic Principles of Transition to Zero Trust Architecture" Int. J. of 3D Printing Tech. Dig. Ind., 8(3): 416-427, (2024).*

DOI: 10.46519/ij3dptdi.1556319

Araştırma Makale/ Research Article

Erişim Linki: (To link to this article): https://dergipark.org.tr/en/pub/ij3dptdi/archive

THE ADVANTAGES AND IMPLEMENTATION CHALLENGES WITHIN THE SCOPE OF THE BASIC PRINCIPLES OF TRANSITION TO ZERO TRUST ARCHITECTURE

Ahmet Ali SÜZEN[a]*, Osman CEYLAN[b]

[a] Isparta University of Applied Sciences, Faculty of Technology, Computer Engineering Department, TÜRKİYE
[b] Isparta University of Applied Sciences, Uluborlu Vocational School, Department of Computer Technologies, TÜRKİYE

* *Corresponding Author: ahmetsuzen@isparta.edu.tr*

(**Received:** 26.09.2024; **Revised:** 29.10.2024; **Accepted:** 10.11.2024)

ABSTRACT

As the number of people working remotely increases, it is insufficient for organizations to protect the boundaries of their digital networks. To protect these boundaries, organizations need adaptive solutions that perform full authentication, authenticate every access request, and quickly detect and respond to both on- and off-network threats. Within this motivation, zero trust is a next generation security strategy based on the principle of “never trust, always verify”. In this study, the basic principles applied from the transition processes to zero trust architecture are evaluated and the advantages of this architecture to the security scope are examined. At the same time, the challenges that organizations that want to implement zero trust architecture will face in this transition are evaluated. The transition to zero trust architecture requires cumulative serious changes in the IT infrastructure of organizations. Zero trust architecture aims to build a system in which all information assets, users and data flow are constantly labeled as untrustworthy and therefore need to be constantly verified. The successful implementation of the zero-trust approach in organizational structures provides advantages such as dynamic authentication, increased endpoint security and strict control over data flows. However, it is also seen that challenges such as network identity management and data monitoring arise during the transition and implementation of zero trust architecture.

Keywords: Authentication, Cyber Security, Industry 5.0, Network Architecture, Zero Trust.

1. INTRODUCTION

Today, cybersecurity threats are becoming increasingly complex and traditional approaches are not sufficient to ensure the security of organizations' information systems [1]. In the wake of digitalization, threats targeting corporate network systems are increasing in both scope and complexity [2]. Given the rapid developments in the field of information technologies, particularly the proliferation of business models such as cloud computing, the use of mobile devices and remote working, traditional “perimeter-based security” models" are inadequate. These models draw strict boundaries between organizations' internal and external networks, ensuring that all elements within the internal network are secure. However, this traditional approach is not effective enough in today's distributed and dynamic corporate structures and leads to security gaps [3]. The remote working model, which has been widely used especially during and after the pandemic period, has led to the spread of the working model by establishing secure connections to corporate networks from different locations.

Zero Trust Architecture was introduced as a new generation security paradigm. Unlike traditional network security approaches, the Zero Trust model does not assume that any layer of the network is secure and provides verification by independently evaluating each access request sent to the network [4]. The basic principle of this architecture is “never trust, always verify”. The Zero Trust principle views every entity as a potential threat, even within secure boundaries, and is based on the fact that all entities must undergo continuous authentication and authorization processes [5]. The main reason for the emergence of the Zero Trust principle is to minimize security vulnerabilities in companies and thus also to take precautions against internal threats. Especially in today's world, the widespread use of remote companies, the increasing access to services offered by cloud technology and the constant connection of users to corporate networks with various devices mean that the network's cyber attack surfaces are expanding and the number of attacks is increasing. In contrast to traditional security approaches in such architectures, the Zero Trust model aims to implement the principles of least privileged access by continuously checking communications and data traffic between systems.

Zero Trust has a security strategy that offers protection against both insider threats and external threats [4]. This architecture not only authenticates users and systems, but also implements a continuous security monitoring process by evaluating various criteria such as device health, user behavior and environmental factors. In this way, an entity accessing the system can access the system even if it is an authorized user by performing separate authentication for each resource it accesses [6].

Zero Trust Architecture has been introduced as a new generation security paradigm and makes significant contributions to meet the security requirements of Industry 5.0 based on human-machine collaboration [7]. Industry 5.0 aims for humans to play a more active role in a digitalized environment with human-machine interaction. In this case, the impact of Zero Trust Architecture on Industry 5.0 is especially important in terms of human-machine interaction and ensuring data security. Ensuring data security is a very important element in the digitalized structure of institutions. As the digital infrastructure of Industry 5.0 continues to develop, it becomes more vulnerable to cyber threats and becomes the target of attackers [8]. Since Zero Trust Architecture adopts the approach of verifying access every time a user or system requests access, the system's resistance against these threats is increased. This provides a solution to the security needs of Industry 5.0 by ensuring the operational continuity and security of human-machine interaction in terms of data security.

The aim of this study is to assess the requirements and implementation challenges of the transition from traditional approaches to a zero-trust architecture and the impact of this process on organizational structures. In the literature, studies in this area often focus on the conceptual framework of zero trust. However, it appears that the basic principles, advantages and disadvantages, challenges and risk management involved in implementing this architecture are not sufficiently addressed. In this study, the applicability of the basic principles of the Zero Trust architecture, the challenges in the transition process and the benefits of this architecture are explained in detail. The technical and operational challenges faced by organizations currently implementing or planning to implement the Zero Trust Architecture are assessed and recommendations for organizations to successfully manage this process are presented.

2. ZERO TRUST ARCHITECTURE

Traditional network security is usually based on a perimeter-based approach. In the perimeter-based security model, the external and internal boundaries of corporate networks are defined and elements in the internal network are considered secure. This approach is usually supported by tools such as firewalls and gateways [9]. However, the weak point of this model is that attackers can move freely once they infiltrate the internal network. Considering internal computing assets as secure leads to ignoring insider threats in particular. With the proliferation of remote working, cloud-based applications and mobile devices, the expansion of network surfaces makes this traditional model even more vulnerable.

Unlike traditional network security models, Zero Trust Architecture is a security paradigm based on the principle that no entity is considered secure by default and every access request must be authenticated [5-6]. This approach is a comprehensive security strategy that enables organizations to combat insider threats as well as external threats. Zero Trust adopts an approach that can be summarized with the motto "never trust, always verify" and requires continuous monitoring and auditing to minimize security breaches.

It is known as the zero trust model for each user or system to undergo security verification. When a user or system component requests access to a resource, it is evaluated and classified according to access policies. If the request is accepted because of this classification process, the user is classified as "Trusted" and secure access is provided. There are many logical components in the classification process and these logical components constitute the basic components of Zero Trust Architecture. The logical components used to explain the basic components of Zero Trust Architecture and the process of providing secure access in this architecture are given in Figure 1. The components shown in the figure illustrate a security model in which each access request is continuously verified through authentication and security policies [10].

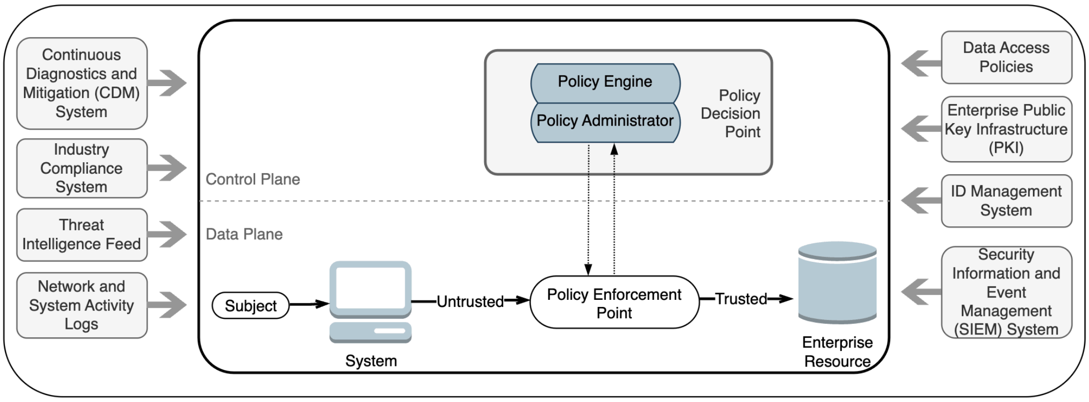

Figure 1. Core Zero Trust Logical Components [10].

2.1. Basic Principles of Zero Trust Architecture

The basic principles of zero trust architecture are based on providing a comprehensive defense against insider threats, not limiting security to threats from outside the network. This approach is based on the idea that security must be continuously verified at every point and at every level. The basic principles of Zero Trust are summarized as follows [8-9].

- **Never Trust, Always Verify:** The basic principle of Zero Trust is that every access request must be verified. This verification is not limited to user identity, but also takes into account factors such as device state, network segment, and even time and place.

- **Least Privileged Access:** Users and applications should only be authorized as much access as they need to perform their tasks. This approach minimizes the potential attack surface and includes strict access policies to limit the impact of breaches.

- **Segmentation and Microsegmentation:** Zero Trust aims to prevent the spread of a potential attack by dividing networks into small segments. Each segment is independently protected and isolated from each other. This method provides an effective defense, especially against insider threats.

- **Continuous Monitoring and Auditing:** Zero trust requires continuous monitoring of every asset on the network and regular auditing of security controls. This process ensures that user behavior is analyzed and anomalous activity is quickly detected.

2.2. NIST SP 800-207 Framework

NIST SP 800-207 is a guide that conceptually defines the Zero Trust Architecture and describes how to implement it. This documentation emphasizes that Zero trust architecture should be considered not only as a technology solution but also as a security strategy. According to NIST SP 800-207, some key components and principles need to be considered for the successful implementation of a Zero trust architecture. These components are integrated into organizational structures to ensure that each access request is evaluated against security risk [10].

These components defined by NIST include;

- Policy Engine (PE),
- Policy Administrator (PA),
- Policy Enforcement Point (PEP)
- Data Feeds (DF) are included.

Before integrating zero trust architecture into an organization, the organization's assets, data and workflows should be determined. This provides information about the current state of an organization's data and network security before the transition to ZTA. The process of transitioning to ZTA is like other security improvements. Implementing the Risk Management Framework (RMF) steps will help an organization reduce security risk and adopt ZTA. The RMF steps involved in implementing ZTA in an organization are shown in Figure 2, including the creation of an initial inventory followed by a regular maintenance and update process. This framework, which includes steps such as the creation of an asset inventory, monitoring, evaluation and feedback, can help continuous improvement to ensure security.

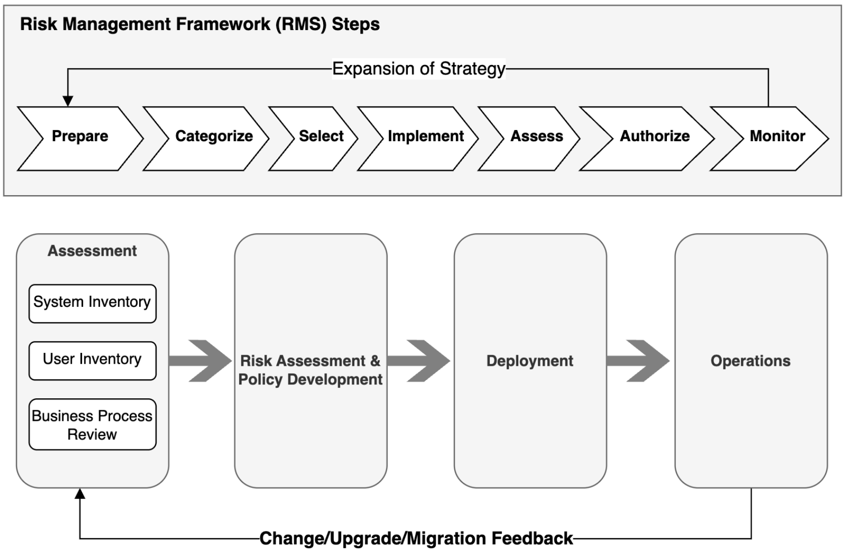

Figure 2. Zero Trust Architecture Deployment Cycle [10].

3. INTEGRATING ZERO TRUST ARCHITECTURE INTO ORGANIZATIONAL STRUCTURES

Applying the Zero Trust architecture to organizational structures is a complex process that requires reassessing and transforming the existing information technology infrastructure. This architecture requires not only technology solutions but also a restructuring of processes, policies and organizational structure. Successful integration of Zero Trust Architecture into enterprise structures makes security a central element, taking into account the dynamic nature of systems and the ever-changing threat landscape [12].

Transitioning to a zero trust architecture in an enterprise is not only possible by upgrading the existing security infrastructure in specific areas, but by a fundamental shift in security strategy. Unlike traditional security approaches, zero trust architecture is based on the principle of not accepting all types of network traffic as secure. Therefore, all assets of the enterprise IT infrastructure (users, devices, networks and applications) should be verified and audited at every point where they interact with each other [13].

The implementation of zero trust architecture in corporate structures requires reviewing the existing security policies of organizations and reorganizing them to comply with this architecture. This process involves not only technical elements, but also human factors and operational business processes. Implementing a zero-trust architecture will require the restructuring of a number of processes such as identity management, access control, endpoint security, data flows and continuous monitoring [13-14].

The transition to a zero trust architecture in the enterprise should be gradual and step-by-step. This transition process usually starts with the implementation of a five-step assessment scope [15].

1. **Assessment of Existing Infrastructure:** Existing systems, network structures and security policies should be comprehensively analyzed and evaluated for compatibility with zero trust architecture.

2. **Identity and Access Management:** Zero trust architecture is based on a security strategy where identity management and access control are at the center. For this reason, it is necessary to optimize the authentication processes of users and devices and to reorganize access authorizations to be least privileged.

3. **Application and Data Security:** While securing data and applications, every data flow and application traffic must be continuously monitored and verified. Micro segmentation and encryption play a key role in this process.

4. **Continuous Monitoring and Threat Detection:** Continuous monitoring and analysis, which is one of the basic principles of Zero Trust Architecture, is a critical element to ensure the security of the corporate structure. All access requests, network traffic and user behavior should be continuously monitored, and abnormal activities should be detected.

5. **Human and Process Factor**: In addition to technological transformation, business processes and the human factor in corporate structures must also be reshaped in accordance with Zero Trust principles. Users must adapt to new access policies and authentication procedures.

The process of integrating zero trust architecture into organizational structures requires not only the purchase of new technologies, but also a change in mindset throughout the organization. A shift from a structure where security is the sole responsibility of IT teams to one where the entire organization actively contributes [16].

For this process to be successful, the following key elements should be considered [17].

- **Gradual Transition:** The transition to Zero Trust Architecture should be implemented gradually, not abruptly. A gradual integration process should be followed before the existing infrastructure and systems are completely replaced.

- **Compatibility with Legacy Systems:** It may not be possible to completely eliminate legacy systems in organizational structures. Therefore, it is important to integrate the Zero Trust Architecture with existing systems in a compatible manner.

- **Risk Management and Challenges:** Risks and challenges that may be encountered in the implementation of Zero Trust Architecture should be carefully evaluated. Organizations should pay attention to ensure business continuity during the transition process and ensure that users experience minimal disruption.

Zero Trust Architecture requires a fundamental change in the security strategies of organizations when implementing it into corporate structures. This process should be treated as a comprehensive transformation process that affects not only technological infrastructure, but also business processes and user habits. The transition to Zero Trust Architecture aims to go beyond traditional security approaches and provide a proactive security model to combat the growing threats in the modern business world [15].

3.1. Process

The implementation of a zero trust architecture in organizational structures requires a well-defined and systematic process. This process consists of a series of steps aimed at continuously assessing and improving the security level of information systems. The Risk Management Framework (RMF) described in NIST SP 800-37 Revision 2 provides the basic methodology for this process. The RMF provides a system lifecycle approach to managing security and privacy risks and is executed through a seven-step process as shown in Table 1 [10]. This methodology ensures that systems are planned, implemented, monitored and updated in a secure manner. Following the RMF steps given in Table 1 in the transition to Zero Trust Architecture is critical to minimize security risks.

Table 1. Process steps and breakdowns offered by RMF in the transition to Zero Trust architecture

Process	Sub Processes
Organizational and System Preparation (PREPARE Step)	Identifying Resources and Roles Defining Security and Privacy Objectives Engagement of Key Stakeholders
System Categorization (CATEGORIZE Step)	Categorization of Systems Determination of Data Sensitivity
Control Selection (SELECT Step)	Selecting Safety Controls Extra Safety Precautions
Control Implementation (IMPLEMENT Step)	Implementation of Selected Controls Structuring Access Policies
Control Assessment (ASSESS Step)	Security Testing and Evaluation Continuous Monitoring and Threat Detection
System Authorization (AUTHORIZE Step)	Authorization Decision Risk Management Decisions
Control Monitoring (MONITOR Step)	Continuous Monitoring and Threat Detection Security Updates

3.2. Prepare

The preparation phase is critical for the successful implementation of the Zero Trust Architecture in organizational structures. This phase includes a comprehensive assessment and planning process at both the organizational and system level. The purpose of the preparation phase is to align existing systems and processes with zero trust principles and to create the necessary infrastructure for the transition [18]. In this phase, the overall security situation of the organization is analyzed as shown in Table 2. In addition, risks are identified and necessary steps are taken to implement the zero trust architecture. Assessment of business processes and systems, at both strategic and operational levels, is essential for the successful integration of zero trust architecture.

Table 2. Process steps and breakdowns of the prepare phase in the transition to zero trust architecture

Process	Sub Processes
Organization and Mission/Business Process Levels	Defining Mission and Security Objectives Review of Business Processes
System Level	Evaluation of System Architecture Review of Existing Security Controls
Risk Analysis	Identifying Threats and Vulnerabilities Prioritization of Risks
Organization and Mission/Business Process Level	Mission Driven Security ZTA Applications Suitable for Business Processes
System Level	Identification of Resources and System Components Selecting Appropriate Safety Measures
Source Categories	Workflow Specific Resources General Infrastructure Resources
Authorization Limit	System Components Connection Security

3.3. Categorize

A critical step in the zero trust architecture planning process is to categorize corporate resources and workflows according to their security requirements. In this process, basic security principles such as confidentiality, integrity and availability are taken into consideration and each resource and workflow is categorized according to certain security levels as given in Table 3. The categorization of resources and workflows is the basis for the effective implementation of a zero trust architecture and helps to determine the security controls to be applied to resources [19].

In this step, resources are categorized into Low, Medium or High levels. These categories indicate what kind of measures should be taken according to the security risk of each resource and determine which level of security will be applied in business processes. This categorization is done to ensure the security of resources and optimize the level of protection against potential threats.

Table 3. Process steps and breakdowns of the categorization phase of the Zero Trust architecture

Process	Sub Processes
Resource Owners and Workflows	Inputs of Resource Owners Analysis of Workflows
System Administrators	Technical Specifications of Sources Evaluation of Existing Security Measures
Categorization of Resources according to Security Levels	Low Moderate High
FIPS 199 and FIPS 200 Standards	Confidentiality Integrity Availability

3.4. Select

Within the Zero Trust Architecture, the select step involves identifying and implementing appropriate security controls to secure systems. This step ensures that the most appropriate security measures are defined for the systems according to the risk levels. Security controls should be tailored to the current threat environment and adapted to the requirements of business processes. In this phase, controls are selected in line with the basic principles of zero trust architecture as shown in Table 4 and the technologies required to enhance the security of business processes are identified. The selection process should be meticulously planned so that the security architecture adapts to the functional requirements and existing infrastructure of the organization [20].

Table 4. Process steps and breakdowns of the select phase in the transition to Zero Trust architecture

Process	Sub Processes
Control Adaptation	Basic Safety Checks Additional Safety Precautions
Control Overlays	Use of coatings Adaptation of coatings
Inputs and Planning	Inputs of Resource Owners Analysis of Business Processes
Continuous Monitoring and Updating	System Monitoring Updates and Security Patches
Additional Resources	Federal CIO Handbook and TIC 3.0 NIST SP 800-53 and 800-53B
Tasks and Inputs	Input from System Administrators NIST SP 800-37 Revision 2

3.5. Apply

Implementing security controls is a critical step for the successful integration of Zero Trust Architecture into organizational structures. The Implement phase involves integrating the security controls and policies identified in the Select step into physical and digital systems. This process provides the technical, organizational and operational steps necessary for the practical deployment of the zero trust architecture (Table 5) [17]. The infrastructure and tools required to manage and monitor systems, users and applications according to zero trust architecture principles come into play at this stage. In the implementation process, security controls are effectively implemented, making a significant contribution to minimizing risks in corporate structures.

Table 5. Process steps and breakdowns of the implement phase in the transition to Zero Trust architecture

Process	Sub Processes
General Approach	Implementation of Selected Controls Least Privileged Access
Future Monitoring and Maintenance	Continuous Monitoring and Updating Monitoring Solutions
Automation and Manual Operations	Automation Manual Operations
Duties and Responsibilities	Managers and Operators Delegation of Tasks

3.6. Evaluate

Once the Zero Trust Architecture has been implemented, it needs to be evaluated regularly to verify that the architecture is continuously improving and achieving its security objectives. The Assess step involves the process of measuring the effectiveness of security controls and collecting the necessary data for improvement [18]. This step tests whether the systems and security policies are suitable for a dynamic zero-trust architecture and ensures that they remain up-to-date and effective in an ever-changing threat environment (Table 6). The Assess process analyzes not only the accuracy and effectiveness of the security controls implemented, but also the impact of these controls on system performance. This step addresses issues such as how to respond to cyber security incidents and how to detect vulnerabilities in systems.

Table 6. Process steps and breakdowns of the Assess phase in the transition to Zero Trust architecture

Process	Sub Processes
Continuous Evaluation	Dynamic Threat Environment Evaluation on System Performance
Two Main Evaluation Processes	Continuous Evaluation of the System Evaluation of the Management Process
Automatic and Manual Controls	Automatic Scanning and Monitoring Manual Evaluation
Active Processes and Tests	Red Team Testing Penetration Tests

3.7. Authorize

Authorization plays a critical role in the final phase of zero trust architecture implementations. This step refers to the formal assessment and authorization of whether a system or application meets security requirements. The authorization process ensures that a system has appropriate security controls in place before moving to the operational phase [19]. In addition, considering the dynamic nature of the zero-trust architecture, security approvals are also required during changes and updates to the systems. This step is a process that maintains the compliance of systems with security objectives through continuous evaluation and the ability to respond to dynamic changes, as shown in Table 7.

Table 7. Process steps and breakdowns of the authorize phase in the transition to Zero Trust architecture

Process	Sub Processes
Dynamic Approach	Evaluation of systems and processes The dynamic nature of zero trust architecture
Changes and Updates	System changes Process updates
Official Approval	Safety assessment Continuous monitoring and improvement

3.8. Monitor

Monitoring is a critical component of a zero trust architecture. It involves continuous monitoring of resources, data flows and systems. Since the zero trust architecture assumes that networks and systems are not always trustworthy, it is necessary to ensure that security controls are active at all times, not just at specific times [20]. As given in Table 8, this step ensures continuous monitoring of the systems to detect new threats and react quickly to potential security breaches. The monitoring process allows early detection of security breaches and creates a rapid defense mechanism against threats. In addition, monitoring data will contribute to the development of future security policies.

Table 8. Process steps and breakdowns of the monitoring phase in the transition to Zero Trust architecture

Process	Sub Processes
Continuous Monitoring of Resources	Continuous monitoring of network traffic Continuous monitoring of endpoint devices
Technology Solutions	Available technology Data analysis and automation
Action Triggering	Reaction to security incidents System improvements
Policy Development	Observations and policy Proactive policy development

4. TRANSITION CHALLENGES AND RISK ASSESSMENTS

While the transition to a zero-trust architecture offers significant advantages for many organizations, it also poses a variety of technical, operational and managerial challenges and risks. The core philosophy of zero trust architecture - “never trust, always verify” - represents a radical departure from traditional security approaches. In this transition, critical areas such as authentication and authorization, endpoint security, protection of data flows, and monitoring of enterprise systems stand out [21]. These challenges require organizations to restructure their workflows and IT infrastructure, update existing security policies, and adopt a new cybersecurity culture. In the following sections, the main challenges and risks in this transition process are discussed and evaluated.

4.1. Principles for Network Identity Management

A zero trust architecture requires all resources, users and devices to go through a dynamic authentication and authorization process before interacting with other entities on the network. In traditional security models, security is typically built at the perimeter of the network, and entities inside the network undergo less stringent controls. However, a zero-trust architecture requires security policies to be applied independently for each entity. In this context, network identity governance is a critical component at the core of a zero trust architecture [22].

- **Dynamic authentication and authorization**: Under a zero trust architecture, each access request must be independently authenticated. This dynamic approach ensures that users, devices and services are continuously authenticated and authorized. In traditional network models, entities are considered trusted once authenticated, whereas in zero trust architecture, each access request is subjected to a separate authentication process. In this way, every access request, even on the internal network, is treated as a threat.

- **Multi-factor authentication (MFA):** Advocates that the authentication process of a zero-trust architecture should not be limited to passwords. In particular, additional security measures such as MFA should be implemented before critical data and systems are accessed. This is an important mechanism that strengthens the security layers of the zero trust architecture and makes the authentication process more secure.

- **Identity management**: Organizations should effectively manage not only user identities but also the identities of all assets (devices, applications, services) on the network. Each asset must be continuously monitored and go through authorization processes. Identity management is a critical element, especially for large organizations that use multiple identity systems within the organization. Integrating authentication and authorization processes into a centralized structure supports the successful implementation of a zero trust architecture.

4.3. Principles on Endpoints

The security of endpoints is of utmost importance for the successful implementation of zero trust architecture. Endpoints are among the areas where security vulnerabilities are most common. Endpoints such as mobile devices, IoT devices, virtual machines and sensors are considered the weak link of the system. Since these devices are part of the network, it is not possible to provide a holistic security without securing each of them [23].

- **All data sources and computing services are considered as resources:** In a zero trust architecture, every device, every data source and every service is considered potentially untrustworthy. All resources, including endpoint devices, should be subject to the system's security policies. This approach requires continuous verification and authorization of endpoints. Organizations should keep these resources under strict security controls and monitor the movement of each resource through the system.

- Integrity and security status of resources: The security of endpoints also depends on keeping these devices protected with up-to-date security patches. Organizations should monitor and assess the security status of all resources they own and use. Each endpoint's configuration status, software version, security updates, etc. should be continuously checked, and security vulnerabilities should be responded to quickly when detected. This process ensures system-wide security of endpoints and increases their resilience against potential threats.

4.4. Principles Applied to Data Flows

An important component of zero trust architecture is to secure data flows. Every data flow that takes place on the network is considered a potential threat under a zero trust architecture. Therefore, data must be secured throughout the transmission process and unauthorized access must be prevented. Zero trust architecture mandates that data should only pass through securely encrypted channels and data integrity should be maintained [15].

- **All communication is secure regardless of network location:** Zero trust architecture considers all data flows as untrustworthy, regardless of whether they are internal or external. Therefore, all communications in the network must be encrypted and carried out over a secure channel. Cryptographic security measures should be used to ensure data integrity and unauthorized access should be blocked immediately.

- **Access to individual corporate resources is granted on a session-by-session basis:** In a zero-trust architecture, each access request is authenticated and authorized on a session-by-session basis. This means that every data transfer and transaction process is evaluated against security policies. Session-based control prevents unauthorized transactions and unauthorized data access.

- **Access to resources is determined by dynamic policies:** A zero-trust architecture does not limit access authorizations to resources to authentication alone. Instead, it determines access authorizations using dynamic policies such as customer identity, application state, service requirements and environmental factors. This dynamic nature allows enterprise security policies to be more fine-tuned and flexible.

- **Data collection and analysis**: A zero trust architecture requires organizations to collect as much information as possible about all entities on the network. The current state of the network, data flows and changes in system components are constantly monitored and analyzed. The collected data is used to improve the security posture of the system and detect potential threats. This process ensures a proactive security approach and increases the effectiveness of the zero trust architecture.

5. CONCLUSION

The transition to a Zero Trust architecture requires a fundamental change in the organizational security structure. However, it offers a more dynamic and comprehensive security strategy compared to traditional security models. The Zero Trust architecture is based on a system where the source, device and user are constantly authenticated and authorized and all data flows inside and outside the network are considered untrusted. The benefits of zero trust architecture include active authentication, increased endpoint security and secure monitoring of data transmissions. In particular, this approach, where potential threats within the system are not even considered trustworthy, allows organizations to develop a proactive defense mechanism against internal and external threats. However, the challenges of implementing a zero trust architecture, such as managing network identity, endpoint security and monitoring data flow, require careful planning and technological investment.

During the transition to a zero trust architecture, organizations should conduct a comprehensive risk assessment, review their existing infrastructure and adapt their security strategies to this structure. A gradual transition and employee training are critical to the efficiency of the transition. In addition, investing in strong technological infrastructures and dynamic security systems will increase the effectiveness of zero trust architecture. As a result, zero-trust architecture allows organizations to build a more flexible and robust security structure against modern cyber threats. If the benefits and challenges that this architecture brings are handled with the right management, it will create a more secure enterprise environment and enable long-term cybersecurity success.

REFERENCES

1. Karabacak, B., "Kritik altyapılara yönelik siber tehditler ve Türkiye için siber güvenlik önerileri," Siber Güvenlik Çalıştayı, Bilgi Güvenliği Derneği, Ankara, Vol. 29, Pages 1-11, 2011.

2. Topcu, N., "Siber güvenlik: tehditler ve çözüm yolları," Cyberpolitik Journal, Vol. 6, Issue 12, Pages 155-181, 2021.

3. Thakur, K., Qiu, M., Gai, K., & Ali, M. L., "An investigation on cyber security threats and security models," IEEE 2nd International Conference on Cyber Security and Cloud Computing, Pages 307-311, November 2015.

4. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X., "A survey on zero trust architecture: Challenges and future trends," Wireless Communications and Mobile Computing, Vol. 2022, Issue 1, Article 6476274, 2022.

5. Bertino, E., "Zero trust architecture: does it help?" IEEE Security & Privacy, Vol. 19, Issue 5, Pages 95-96, 2021.

6. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R., "Zero trust architecture (ZTA): A comprehensive survey," IEEE Access, Vol. 10, Pages 57143-57179, 2022.

7. Czeczot, G., Rojek, I., Mikołajewski, D., & Sangho, B. (2023). AI in IIoT management of cybersecurity for industry 4.0 and industry 5.0 purposes. Electronics, Vol. 12, Issue 18,Pages 3800.

8. Trivedi, C., Bhattacharya, P., Prasad, V. K., Patel, V., Singh, A., Tanwar, S., ... & Sharma, G. (2024). Explainable AI for Industry 5.0: Vision, Architecture, and Potential Directions. IEEE Open Journal of Industry Applications.

9. D'Silva, D., & Ambawade, D. D., "Building a zero trust architecture using kubernetes," 2021 6th International Conference for Convergence in Technology (I2CT), Pages 1-8, April 2021.

10. Stafford, V., "Zero trust architecture," NIST Special Publication, Vol. 800, Issue 207, 2020.

11. Greenwood, D., "Applying the principles of zero-trust architecture to protect sensitive and critical data," Network Security, Vol. 2021, Issue 6, Pages 7-9, 2021.

12. Fernandez, E. B., & Brazhuk, A., "A critical analysis of Zero Trust Architecture (ZTA)," Computer Standards & Interfaces, Vol. 89, Article 103832, 2024.

13. Edo, O. C., Tenebe, T., Etu, E. E., Ayuwu, A., Emakhu, J., & Adebiyi, S., "Zero Trust Architecture: Trend and Impact on Information Security," International Journal of Emerging Technology and Advanced Engineering, Vol. 12, Issue 7, Page 140, 2022.

14. Seaman, J., "Zero trust security strategies and guidelines," in Digital Transformation in Policing: The Promise, Perils and Solutions, Cham: Springer International Publishing, Pages 149-168, 2023.

15. Greenwood, D., "Applying the principles of zero-trust architecture to protect sensitive and critical data," Network Security, Vol. 2021, Issue 6, Pages 7-9, 2021.

16. Edo, O. C., Tenebe, T., Etu, E. E., Ayuwu, A., Emakhu, J., & Adebiyi, S., "Zero Trust Architecture: Trend and Impact on Information Security," International Journal of Emerging Technology and Advanced Engineering, Vol. 12, Issue 7, Page 140, 2022.

17. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X., "A survey on zero trust architecture: Challenges and future trends," Wireless Communications and Mobile Computing, Vol. 2022, Issue 1, Article 6476274, 2022.

18. Ahmadi, S., "Zero trust architecture in cloud networks: Application, challenges and future opportunities," Journal of Engineering Research and Reports, Vol. 26, Issue 2, Pages 215-228, 2024.

19. Qazi, F. A., "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), Pages 111-116, December 2022.

20. Damaraju, A., "Implementing Zero Trust Architecture in Modern Cyber Defense Strategies," Unique Endeavor in Business & Social Sciences, Vol. 3, Issue 1, Pages 173-188, 2024.

21. Alevizos, L., Ta, V. T., & Hashem Eiza, M., "Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review," Security and Privacy, Vol. 5, Issue 1, Article e191, 2022.

22. Gupta, A., Gupta, P., Pandey, U. P., Kushwaha, P., Lohani, B. P., & Bhati, K., "ZTSA: Zero Trust Security Architecture a Comprehensive Survey," 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Pages 378-383, May 2024.

23. Liu, H., Ai, M., Huang, R., Qiu, R., & Li, Y., "Identity authentication for edge devices based on zero-trust architecture," Concurrency and Computation: Practice and Experience, Vol. 34, Issue 23, Article e7198, 2022.