Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 01, April, 2025
Website: usajournals.org

ZERO TRUST ARCHITECTURE IN MODERN ORGANIZATIONS

Alisher Serikbayev,
IT Expert, USA

Abstract:
With cyber threats becoming more complex and remote work becoming more common, traditional security models are becoming obsolete. This article examines the architecture of Zero Trust (ZTA), considering its key components: continuous verification, least privilege, and micro-segmentation . Based on current research up to 2025 and practical cases, the article examines the role of AI/ML and cloud solutions in strengthening ZTA. It concludes with recommendations for the phased implementation of this architecture in the enterprise environment.

Keywords: Zero Trust Architecture , cybersecurity , information security, AI/ML in security, Zero Trust Network Access (ZTNA), cloud security, digital transformation.

Introduction

The scientific novelty of this work lies in conducting a comprehensive analysis of key components and modern trends in the development of Zero architecture Trust (ZTA). The study places special emphasis on the integration of advanced technologies such as artificial intelligence, machine learning, cloud solutions and Zero Trust Network Access (ZTNA). Based on the systematization of empirical cases of leading organizations, the work allows us to identify the practical effects of ZTA implementation and formulate specific recommendations.

In the context of digital transformation, which is characterized by the widespread introduction of cloud technologies, the expansion of remote work and the growth of cyberattacks, modern companies face significant challenges in the field of information security. Traditional security models based on the concept of a strictly defined perimeter and a priori trust in internal networks are losing their

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 01, April, 2025
Website: usajournals.org

relevance and effectiveness in the context of hybrid and distributed IT infrastructures.

In response to these challenges, the concept of Zero architecture is actively developing Trust (ZTA). ZTA is based on the fundamental principle of «nobody and nothing can be trusted by default», requiring constant authentication, authorization, and verification of every attempt to access corporate resources [1]. This approach allows for significant minimization of risks from both external and internal threats through enhanced access control, micro-segmentation of network infrastructure, and widespread use of multi-factor authentication.

American research and consulting company specializing in information technology markets «Gartner» regularly publishes research on security and Zero Trust. Thus, according to one of its reports, organizations that have implemented the principles of Zero Trust, demonstrate a reduction in the number of successful cyber-attacks and a reduction in response time to incidents, which in turn increases the overall resilience of business processes [2]. In addition, a study by Forrester , one of the leading researchers in the information technology markets, focuses on the fact that the transition to ZTA helps optimize access management and simplifies compliance with regulatory requirements in the field of personal data protection [3].

This study is devoted to the analysis of modern trends in the development of Zero architecture Trust and study of practical experience of its implementation in organizations of various industries. Particular attention is paid to consideration of key components of ZTA, including continuous verification, the principle of least privilege, micro-segmentation, as well as the role of artificial intelligence and cloud technologies in strengthening protective mechanisms.

The underlying principles and components of ZTA are described in a guide from the National Institute of Standards and Technology. This document focuses on continuous authentication, micro-segmentation, and privilege minimization as fundamental elements of the architecture. This publication serves as a starting point for developing and implementing Zero Trust in organizations around the world.

Modern research highlights the growing role of artificial intelligence and machine learning (AI/ML) in automating threat detection processes and dynamic access

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 01, April, 2025
Website: usajournals.org

control. In an article published in the journal Nanotechnology Perceptions » on the use of AI for anomaly detection in Zero Networks Trust describes how AI improves the efficiency of detecting anomalies in network traffic and speeds up incident response, thereby strengthening the resilience of security systems [4].

Analytical reports confirm the practical demand for ZTA. According to Gartner , more than 80% of large companies have either already implemented or are planning to implement multi-factor authentication (MFA) and Zero Trust Network Access (ZTNA) as key components of their strategies. Forrester highlights ZTNA as an effective alternative to traditional VPNs, reducing the attack surface and simplifying access management.

The ZTA concept is closely linked to the development of cloud solutions and Secure architecture Access Service Edge (SASE). The research by MarketsandMarkets highlights that these areas provide organizations with flexible, scalable, and integrated tools to protect hybrid IT infrastructures. Thus, the literature review points to the comprehensive nature of the implementation of Zero Trust, which combines technical, organizational and analytical approaches to ensure security in an ever-changing cyber landscape.

Zero architecture Trust (ZTA) is influenced by modern technological trends that expand the capabilities of corporate systems protection and facilitate adaptation to new challenges in the field of information security.

1. Integration of artificial intelligence and machine learning (AI/ML). AI/ML technologies play a key role in automating the processes of detecting anomalies and potential threats in real time. The authors of the article «AI Integration in Zero Trust Security Architecture: A Technical Overview» writes that «integration of artificial intelligence into the architecture of Zero Trust enables complex user behavior analysis, processing an average of 1.7 million behavioral data points per second with 99.94% accuracy in detecting anomalies. This significantly reduces false positives and improves «access control accuracy» [5]. For example, Microsoft uses artificial intelligence capabilities in its Azure solution. Sentinel, which enables automatic detection of suspicious activity and response to threats within the framework of Zero Trust strategies. According to Microsoft , this reduces incident detection time by 60% [6].

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 01, April, 2025
Website: usajournals.org

2. Identity- centric approach. Modern ZTA implementations shift the focus to enhanced authentication of users and devices. This includes mandatory use of multi-factor authentication (MFA) and biometric verification methods. According to the Gartner report (2024), more than 80% of organizations already integrate advanced identity mechanisms into their Zero Trust, which emphasizes the importance of this area [7]. Thus, the company «Google» in its corporate network has implemented multi-factor authentication and biometric verification of users, which has reduced the number of successful phishing attacks by 99.9% [8].

3. Zero Trust Network Access (ZTNA) how to VPN alternative . ZTNA technology offers a more granular approach to providing access to corporate resources, operating at the level of individual applications rather than the entire network. A study by Forrester found that switching to ZTNA helps reduce the attack surface, limiting the potential for lateral threat propagation, and simplifies access management. The American company Okta has implemented the ZTNA solution to provide secure access to corporate applications, which has made it possible to replace traditional VPNs and reduce the risks of internal threat proliferation [9].

4. Integration with cloud architectures and SASE. Convergence of ZTA with Secure architecture Access Service Edge (SASE) allows you to combine network and security functions in a single cloud service. This ensures high scalability and flexibility of the security system. According to the forecasts of the well-known research company «MarketsandMarkets», the SASE and Zero market Trust will demonstrate a compound annual growth rate (CAGR) of more than 25% over the next five years, confirming the strategic importance of this integration for the future of information security [10]. For example, the American multinational company Cisco has implemented the SASE platform in the infrastructure of several large banks, which ensured flexible security when scaling cloud resources and remote access, increasing productivity and reducing system downtime [11].

Systematization of modern trends in the development of Zero architecture Trust (ZTA) suggests that each plays an important role in developing effective and adaptive cybersecurity strategies .

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 01, April, 2025
Website: usajournals.org

Table 1 - Key modern trends in the development of Zero Trust

No.	Trend	Description
1	AI/ML Integration	Automatically detect and respond to threats based on behavior
2	Identity -centered approach	Enhanced Authentication, MFA, Biometrics
3	Zero Trust Network Access (ZTNA)	Access to resources at the application level, reducing the attack surface
4	Cloud architectures and SASE	Combine security and networking in the cloud for scalability

These areas provide organizations with the ability to not only minimize risks, but also quickly respond to constantly evolving threats .

In our research, we have systematized the main components of the Zero architecture Trust (ZTA) in Table 2. Each of these elements plays an important role in ensuring comprehensive protection of corporate information systems, helping to minimize the risks associated with unauthorized access and cyberattacks.

Table 2 - Key Components of Zero Trust Architecture (ZTA)

Component	Description
Identification and authentication	Continuous verification of user and device identity, including MFA and biometrics
Minimum privileges	Providing access only to necessary resources for a strictly limited period
Network microsegmentation	Separating the network into isolated segments to limit the spread of threats
Continuous Behavior Monitoring and Analysis (UEBA)	Using systems to detect anomalies and analyze user behavior

All ZTA components are interconnected and functionally complement each other. Thus, reliable access control is ensured by strict identification and authentication of users and devices. The principle of least privileges limits access rights to resources exclusively to those that are necessary for performing specific tasks. Microsegmentation of the network infrastructure serves to localize potential threats, effectively preventing their horizontal spread. In turn, continuous monitoring and analysis of user and entity behavior (UEBA) allow for timely detection of anomalies and prompt response to suspicious activity.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 01, April, 2025
Website: usajournals.org

In the course of our research into modern approaches and analysis of practical experience in implementing Zero architecture Trust (ZTA) formulated key findings and developed recommendations for its successful implementation.

Key Findings:

1. The principle of «trusting no one and nothing by default» is a highly effective strategy for minimizing the risks of unauthorized access and reducing the potential damage from cyber attacks.
2. The integration of artificial intelligence (AI) and machine learning (ML) technologies increases the adaptability of security systems, allowing automation of threat detection and response processes in real time.
3. Multi-Factor Authentication (MFA) and Zero Trust Network Access (ZTNA) are becoming recognized standards in modern cybersecurity, providing reliable and flexible access control.
4. Cloud solutions and Secure architecture Access Service Edge (SASE) provides the necessary scalability and flexibility, which is especially important for organizations with a distributed IT infrastructure.
5. Successful implementation of ZTA requires not only technical measures, but also a comprehensive approach, including staff training and changes in corporate culture.

We have developed practical recommendations for the successful implementation of Zero architecture Trust , indicated in Table 3.

Table 3 – Practical recommendations for implementing Zero Trust

	Recommendation	Description
1	IT Infrastructure Assessment	Analysis of assets, vulnerabilities and access paths
2	Multi-Factor Authentication (MFA)	Implementation of enhanced identity verification methods
3	Using AI/ML	Automate Threat Detection and Response
4	Transition to ZTNA	Replacing VPN with Flexible Access Control Solutions
5	Integration of cloud solutions and SASE	Ensuring scalability and flexibility of infrastructure
6	Training and safety culture	Formation of awareness and responsible behavior of employees

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 01, April, 2025
Website: usajournals.org

Therefore, the Zero architecture Trust (ZTA) is a modern approach to cybersecurity that rejects traditional trust in an internal network. Instead, it is based on the principle of «trust no one by default». Key elements of ZTA include continuous verification of all users and devices, least privilege access, and network micro-segmentation to contain threats. The evolution of ZTA is supported by the integration of artificial intelligence (AI) and the transition to Zero Trust Network Access (ZTNA) - This architecture improves organizations' resilience to cyberattacks and simplifies security management in today's hybrid IT environments.

References

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology, 2020. URL: https :// nvlpubs . nist . gov / nistpubs / SpecialPublications / NIST . SP .800-207. pdf (access date: 12.08.2025)
2. Gartner. Market Guide for Zero Trust Network Access. 2024. URL: https://www.gartner.com/en/documents/3987952 (accessed: 12.08.2025) .
3. Forrester. The Rise of Zero Trust. 2023. URL: https://go.forrester.com/blogs/the-rise-of-zero-trust/ (accessed: 12.08.2025).
4. Sandhu K., Reddy SG, Hegde RS, Venkataramanan S., Joy M., Ahmed M., Mark M., Gudala L., Shaik M., VSS Srinivas, Hamade MA AI-Powered Anomaly Detection in Zero Trust Environments: A Comprehensive Review of Methods and Evaluation // Nanotechnology Perceptions. 2024. T. 20, Special. issue S16. URL: https://www.researchgate.net/publication/389634535_AI-Powered_Anomaly_Detection_in_Zero_Trust_Environments_A_Comprehensive_Review_of_Methods_and_Evaluation (accessed: 12.08.2025).
5. Gadkari BR AI Integration in Zero Trust Security Architecture: A Technical Overview // International Research Journal of Modernization in Engineering Technology and Science. 2025. T. 7, No. 2. DOI: 10.56726/IRJMETS67329.
6. Microsoft Azure Sentinel. URL: https://azure.microsoft.com/en-us/services/azure-sentinel/ (date accessed : 12.08.2025).
7. Gartner. Market Guide for Zero Trust Network Access. 2025. URL : https://www.gartner.com/en/documents/4239265 (accessed: 12.08.2025) .

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 01, April, 2025
Website: usajournals.org

8. Google Security Blog. Enforcing MFA for all employees. 2021. URL : https :// security . googleblog . com /2021/04/ enforcing - mfa - for - all - employees . html (accessed: 12.08.2025).
9. Okta . Zero Trust Solutions. URL: https :// www . okta . com / solutions / zero - trust / (date accessed : 12.08.2025).
10. MarketsandMarkets . Secure Access Service Edge (SASE) Market Report. 2023. URL : https :// www . marketsandmarkets . com / Market - Reports / secure - access - service - edge - sase - market -297602097. html (access date: 08/12/2025)
11. Cisco . Secure Access Service Edge (SASE). 2023. URL: https://www.cisco.com/c/en/us/solutions/enterprise-networks/sase.html (accessed: 12.08.2025) .