Building specific of zero trust architecture in hybrid infrastructures*

Roman Syrotynskyi[1,*,†], Ivan Tyshyk[1,†], and Alona Desiatko[2,†]

[1] *Lviv Polytechnic National University, Information Security Department, 12 Stepan Bandera str., 79000 Lviv, Ukraine*
[2] *State University of Trade and Economics, 19 Kyoto str., 02156 Kyiv, Ukraine*

Abstract

The popularity of hybrid infrastructures is growing rapidly. The reason is the ability to combine the advantages of local computing resources such as control, cost-effectiveness, compliance with regulatory requirements with the scalability, flexibility and high availability of cloud technologies. In such conditions, there is a need to provide a unified approach to information security that can cover both types of environments. Zero Trust Architecture (ZTA) is considered a modern and effective model that allows achieving a high level of access control, minimizing the risks of security breaches and ensuring the protection of critical resources regardless of their location. However, building ZTA in hybrid environments is accompanied by a number of challenges due to the heterogeneity of technologies, the lack of unified management tools, varying degrees of control over infrastructure components and the complexity of implementing unified authentication, authorization and monitoring policies. The article examines the key differences between the same type of local and hybrid infrastructures, in particular from the point of view of building a zero trust architecture. The specifics of integrating elements of local and cloud environments, which often have different mechanisms for user identification, session management, event logging, and access policy enforcement, are analyzed. A number of important architectural components and technologies are proposed that form the stack of components necessary for implementing ZTA in a hybrid environment. An analysis of the challenges of implementing Zero Trust architecture in a hybrid network infrastructure is also described. Taking into account the identified features, a phased plan for migrating hybrid infrastructures to Zero Trust architecture has been formed, which includes assessment and planning, architecture development, decision selection, and other important steps.

Keywords

Zero Trust Architecture, hybrid network environment, LAN, Cloud Infrastructure, Integration, compliance, microsegmentation, identity

1. Introduction

A hybrid network environment in enterprise IT is an integrated network architecture that combines on-premises data centers with cloud infrastructure (AWS, Microsoft Azure, Google Cloud, etc.). This model allows companies to store mission-critical applications and sensitive data in on-premises data centers, while leveraging the scalability, flexibility, and cost-effectiveness of cloud services [1–3].

A hybrid network enables seamless communication between on-premises and cloud applications, allowing enterprises to optimize performance, security, and resource allocation, as well as guarantee business continuity [4–6].

An example of a hybrid network environment in an enterprise infrastructure would be the Enterprise Data Center + AWS Cloud infrastructure. A large enterprise uses an on-premises data center to store databases, legacy applications, and mission-critical workloads, while AWS cloud resources use for scalable web applications, AI analytics, and backup storage. For example, a

[*] *CPITS-II 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2025, Kyiv, Ukraine*
[*] Corresponding author.
[†] These authors contributed equally.

roman.m.syrotynskyi@lpnu.ua (R. Syrotynskyi); ivan.y.tyshyk@lpnu.ua (I. Tyshyk); desyatko@gmail.com (A. Desiatko)
0009-0002-6280-3290 (R. Syrotynskyi); 0000-0003-1465-5342 (I. Tyshyk); 0000-0003-2860-2188 (A. Desiatko)

financial company stores customer transaction data in an on-premises center for regulatory compliance, while using AWS for big data analytics and AI fraud verification [1].

Another option for implementing a hybrid infrastructure is to implement Microsoft Azure Hybrid Cloud for enterprise IT. In this case, on-premises Active Directory (AD) integrates with Azure Active Directory (AAD) to provide single sign-on (SSO), identity management, and secure access to cloud services. An example is an international company that uses on-premises AD to authenticate employees, and also integrates Microsoft 365, Azure Virtual Desktop, and cloud storage for remote access of employees [7, 8].

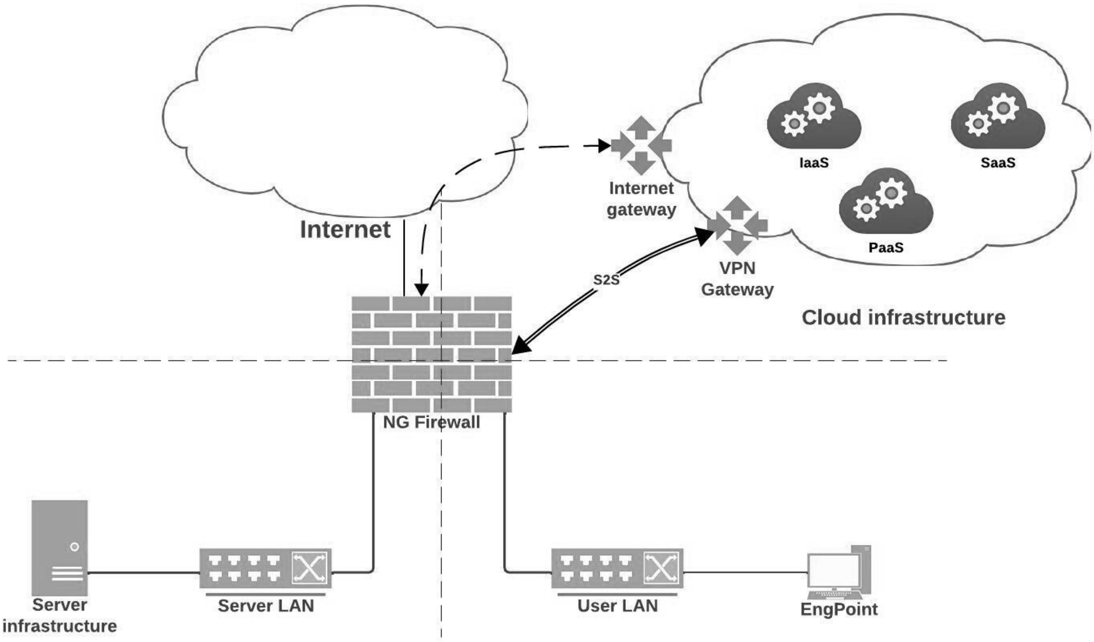

Figure 1: Example of hybrid infrastructure

2. Differences between traditional and hybrid architectures

Hybrid Information technology architecture combines the specifics of on-premises and cloud architectures which translates into certain aspects that differ from both on-premises and cloud options. Traditional on-premise architecture provides a high level of control and security, but limit scalability and flexibility. The main characteristics of hybrid infrastructure are significantly different from homogeneous ones. Their research was conducted based on published materials, researches and own experience. The results are listed in Table 1.

Table 1
Main differences of on-premise and hybrid infrastructures

Aspect	On-premise architecture	Hybrid architecture
Infrastructure	Fully on-premises infrastructure with dedicated servers, network equipment, and private data centers	Combination of on-premises data centers and cloud services (AWS, Azure, Google Cloud).
Scalability	Limited by physical resources; Expansion requires significant investment.	High scalability; Cloud resources can be quickly scaled up or down as needed.
Flexibility	Rigid infrastructure with a fixed	Flexible and adaptable;

	allocation of resources.	Workloads can be distributed between on-premises and cloud resources.
Cost structure	High capital expenditure (CapEx) on equipment, maintenance and IT personnel.	Reduced CapEx; operating cost model (OpEx) for cloud services.
Security	Perimeter security model; relies on firewalls and VPNs to protect the internal network.	Zero Trust model; Constant authentication and access control between on-premises and cloud resources.
Performance and latency	Low latency for on-premises applications because all resources are physically connected.	Performance may vary depending on the network connection, but CDN and edge computing in the cloud reduce latency.
Reliability and fault tolerance	Requires separate disaster recovery (DR) and backup solutions.	Built-in high availability with cloud-based DR solutions and automatic failover.
Maintenance and management	Requires manual updates, patches, and monitoring by the internal IT team.	Cloud providers perform automated updates, monitoring, and maintenance.
Deployment Speed	Slow deployment; Setting up new servers and networks takes time.	Fast deployment; Cloud resources can be connected in a few minutes.
Networking	Uses traditional LAN/WAN architectures, often requires leased communication channels for remote access.	Uses SD-WAN, VPN, Direct Connect, and cloud peering connections to integrate on-premises and cloud infrastructure.
Areas of application	The best option for companies that need full control over the infrastructure (e.g. banks, government agencies, legacy applications).	The best option for businesses that need scalability, remote work, and cloud computing (e.g., SaaS companies, e-commerce).

Thus, hybrid IT architectures make it possible to get the benefits of both on-premises and cloud environments at the same time, however, since hybrid architecture is essentially a symbiosis of on-premises and cloud, it is not without challenges that are characteristic of hybrid environments, such as complexity, security boundaries, data flow management, integration issues, and others.

3. Zero Trust Architecture main principles and it’s value in hybrid infrastructures

Zero Trust Architecture (ZTA) is a modern cybersecurity concept that eliminates the concept of default trust in networks. Unlike traditional security models that rely on perimeter protection, ZTA assumes that no user, device, or network segment can be trusted by default—regardless of their location or prior authentication [9]. Instead, each access request is constantly confirmed, and permissions are granted only within the required minimum [10–12].

ZTA is based on the principle of “never trust, always verify”, i.e. access control decisions are made based on rigorous identity checks, device security assessments, and contextual risk analysis [13]. This approach guarantees dynamic adaptation of security policies to changing threats.

The core of the zero trust architecture is its basic principles, in addition to the principle of “never trust, always verify”, these include the following:

The principle of Least Privilege. This principle ensures that users, applications and devices are given the minimum level of access necessary to perform their tasks. This reduces the attack surface and limits the potential consequences of compromise [14]. Compliance with the principle should be carried out in all access control mechanisms, both in terms of granting administrative access and in the management of network access by means of firewalls, etc. and the assignment of network traffic can be added using certain techniques and tools to minimize the necessary privileges. These include the following:

- Granular Access Control: ZTA applies role-based (RBAC) and attribute (ABAC) access control to restrict user rights.
- “just-in-time” access: Temporary permissions are granted only for the necessary time to complete the task.
- Device and location restrictions: Access policies take into account device security and risk factors such as geolocation.

Assumed Breach approach. This principle of “hacking assumption” is based on the fact that the network can already be compromised. Therefore, the organization not only protects itself from external attacks, but also prepares for potential threats from the inside [15]. Ensuring the resilience of the infrastructure to the compromise of some part of it is carried out through the implementation of architectural measures and tools that ensure localization, detection and response to future incidents.

- Microsegmentation: Splitting the network into isolated zones prevents lateral movement of attackers [16].
- Continuous monitoring: Using behavioral analytics to detect abnormal activity.
- Incident preparedness: Automated threat response mechanisms such as Endpoint Detection and Response (EDR) help to quickly eliminate compromise [17].

The Principle of Explicit Verification. Zero Trust requires constant authentication and authorization of each access request, even if the user or device has already been verified previously [18]. Ensuring access verification is carried out by next-generation firewalls using additional information that is collected and transmitted to make a decision on granting network access. Technologies that can be used:

- Multi-Factor Authentication (MFA): Uses multiple identification factors, such as biometrics and hardware tokens.
- Checking the status of the device: Before granting access, the system checks that the device meets security standards.
- Adaptive access: Access policies change dynamically based on behavioral analysis and risk levels [19, 20].

The value of zero trust in securing hybrid environments. Hybrid environments combining on-premises data centers and cloud services pose complex security challenges because they involve a variety of access points and multi-domain systems. ZTA is essential to protect them because:

- Reduces security risks in the cloud: Guarantees the security of AWS, Azure, and Google Cloud, through strict access control and encryption mechanisms [21, 22].

- Ensures remote work security: With the Bring Your Own Device (BYOD) model and hybrid workplaces, ZTA provides continuous authentication [13].
- Minimizes risks from insider attacks: With the assumption of compromise, ZTA prevents unauthorized access even from internal users [23].

4. Typical features of hybrid network architecture within the Zero Trust concept

Hybrid network architectures operating on the principles of the Zero Trust Framework (ZTF) inherit security mechanisms from both on-premises and cloud environments. Their essence and method of implementation are similar to those used in non-hybrid environments. For example, the principle of Least Privilege Access (LPA). ZTF implements strict access control based on role-based (RBAC) and attribute (ABAC) policies to minimize access rights of users, devices, and applications [13]. This prevents attackers from moving laterally in the event of a network compromise.

Multi-factor authentication (MFA) and identity verification. Constant authentication using MFA, biometrics, or hardware tokens ensures that no entity is trusted by default.

Another fundamental security mechanism in ZTA is micro-segmentation. Micro-segmentation is necessary to isolate network resources. Its security value lies in dividing the network into isolated segments, which limits the spread of attacks and reduces the impact of compromise [24]. This works on both cloud and local networks. What different infrastructures have in common is the need for continuous monitoring and behavioral analytics. Real-time monitoring and AI threat analysis allow you to adapt to variable attacks. And automated response mechanisms block suspicious devices and accounts [25].

Most of the security mechanisms used in building a zero-trust architecture are common in on-premises infrastructures, cloud environments, as well as their hybrid combinations. However, in a zero-trust architecture, there are unique challenges and solutions that are unique to hybrid environments, due to the specifics of such infrastructure and additional complexities arising from the combination of different systems and the need for unified management. Such features specific to hybrid architectures include the following:

Integration of Hybrid Identity and Access Management (IAM). Since hybrid environments must authenticate users in on-premises and cloud services, this leads to identity fragmentation. Fragmented identity creates the need to solve the problem of integration and unification of identity management tools. An example of a solution is using Federated Identity Management (FIM) to combine on-premises Active Directory (AD) with Azure AD, AWS IAM, or Google Cloud Identity [13]. To meet the requirements of Zero Trust verification, it is advisable to use Single Sign-On (SSO), which applies to all hybrid resources. One of the options of federated identity management might be ADFS based implementation. Example ofADFS integrated authentication process is described in Figure 2. It includes 6 major steps:

1. User login to authentication portal
2. User authenticated
3. Receive SAML response SAML
4. Post the SAML response to sign-in
5. Receive temp credentials
6. Redirect to AWS Console

In this implementation scenario SAML (Security Assertion Markup Language) is used to authenticate users in local AD Identity store using ADFS 3.0 solution during connection to AWS cloud. Such approaches are required to solve the problem of integration and unification of identity management tools in hybrid infrastructures.

SD-WAN & Direct Cloud Peering (SD-WAN & Direct Cloud Peering) is another example of a security mechanism unique to hybrid infrastructures. Traditional VPN-based security models struggle to provide dynamic security in hybrid cloud connections. Lack of flexibility, compatibility and performance do not allow them to be used effectively between different platforms. Potential solutions could be Software-Defined WAN (SD-WAN) integration to create encrypted tunnels between on-premises infrastructure and cloud services [26], as well as private communication channels (AWS Direct Connect, Azure ExpressRoute), which provide low latency and high security between on-premises and cloud systems.

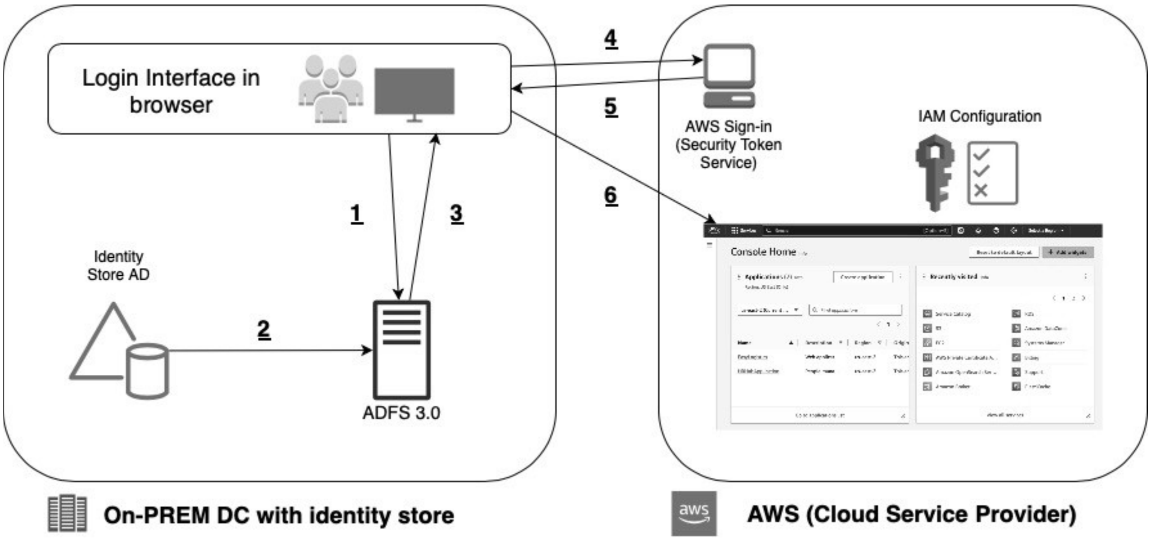
Login Interface in browser
4
5
6
1
3
2
AWS Sign-in (Security Token Service)
IAM Configuration
Identity Store AD
ADFS 3.0
Console Home
On-PREM DC with identity store
aws
AWS (Cloud Service Provider)

Figure 2: ADFS Integrated Authentication Process

Data flow management and encryption in a hybrid environment. A task that, like the previous ones, requires certain solutions that are not found outside of hybrid infrastructures built on a zero-trust architecture. We are talking about hybrid networks that require unified encryption standards when transferring data between on-premises and cloud infrastructure. Current research and recommendations suggest the use of end-to-end encryption (E2EE) using TLS 1.3 and AES-256 for all hybrid data streams [24]. To control the movement of confidential data through local storage and cloud services, it is recommended to use Cloud Access Security Brokers (CASB).

Threat detection and automated response in a hybrid network. The difficulty lies in the fact that hybrid architectures increase the attack surface, which makes centralized defense difficult. Many of the already existing approaches and tools are not flexible enough and do not fully cover the need for analytics and response in different environments at the same time. Zero Trust-based security orchestration, which can detect and isolate potential threats in the cloud and on-premises infrastructure in real-time, can help with the solution [27]. And the use of SIEM systems will allow integrating event logs from on-premises and cloud resources, providing automated response to threats [13].

The need to comply with safety standards and policies in hybrid environments. According to regulatory requirements, hybrid architectures must provide uniform regulatory compliance for on-premises and cloud environments. Thus, common rules must be followed by different infrastructures built on different platforms. Zero Trust Policy Automation can help with the arrangement of rules that must comply with security standards. The use of the Tool will allow the management and maintenance of uniform rules for PCI-DSS, NIST, GDPR, HIPAA, and other standards that may be necessary.

5. Architectural Components and Technologies

Building a Zero Trust Architecture (ZTA) in hybrid environments that combine on-premises and cloud infrastructures involves several critical architectural components and technologies that ensure both security and operational efficiency.

Identity and Access Management (IAM): IAM is a fundamental component of ZTA that enforces identity verification and policy-based access control. Technologies such as Single Sign-On (SSO), Multi-Factor Authentication (MFA), and identity federation (e.g., SAML, OAuth, OpenID Connect) provide secure, identity-centric access management in hybrid environments. Centralized identity providers (IdPs) such as Azure Active Directory, Okta, or Ping Identity ensure consistent identity governance and seamless integration.

Policy Enforcement Point (PEP): PEPs dynamically apply access decisions defined by policy engines. This includes network firewalls, gateways, software-defined perimeter (SDP) solutions, and microsegmentation technologies. Solutions such as VMware NSX, Cisco ACI, Palo Alto Prisma, AWS Security Groups, Azure Network Security Groups, or Cloudflare Access enforce resource access in both on-premises and cloud environments.

Policy Decision Point (PDP): PDPs evaluate access requests based on identity, context, resource sensitivity, and predefined security policies. Technologies implementing PDPs include Zero Trust policy engines (e.g., OPA—Open Policy Agent), centralized policy management platforms, and identity-aware proxies (IAPs) offered by major cloud providers.

Microsegmentation and Network Isolation: Fine-grained network isolation technologies, such as VMware NSX, Cisco ACI, or cloud-native network segmentation services (AWS VPC, Azure VNets, GCP VPC), limit lateral movement and reduce the attack surface. Microsegmentation strengthens the ZTA model by enabling precise, context-aware control of communications between resources.

Continuous Monitoring and Visibility: Tools for continuous monitoring and visibility—including Security Information and Event Management (SIEM) systems such as Splunk, Azure Sentinel, Elastic Stack, Cloud Security Posture Management (CSPM) platforms, and endpoint detection and response (EDR/XDR) solutions—provide real-time threat detection, analytics, and auditing essential to maintaining trust.

Secure Connectivity and Encryption: Encrypted communication through VPNs (IPsec, WireGuard), TLS/SSL, and dedicated cloud connectivity services (AWS Direct Connect, Azure ExpressRoute, Google Cloud Interconnect) ensures confidentiality and integrity of data exchanged between on-premises and cloud infrastructures.

Automation and Orchestration: Infrastructure-as-Code (IaC) and automation tools such as Terraform, Ansible, Chef, Puppet, or Kubernetes enable consistent deployment, enforcement, and scaling of Zero Trust policies across hybrid infrastructures.

Together, these integrated components and technologies form an identity-driven security stack that dynamically enforces Zero Trust principles in complex hybrid infrastructures. Their effectiveness depends not only on individual functional capabilities but also on their ability to operate as a unified system with consistent policy logic based on identity, access context, and continuous risk analysis.

6. Implementing Zero Trust Architecture in Hybrid Network Infrastructure challenges

The implementation and operation of Zero Trust Architecture (ZTA) in hybrid IT infrastructures that integrate cloud services and on-premises resources poses significant challenges related to network architecture and network access management. These challenges arise primarily due to the complexity and diversity of hybrid environments, which require comprehensive strategies to ensure effective security implementation.

One of the main architectural challenges is the inherent complexity of hybrid network topologies. Traditional on-premises infrastructures are often rigid and static, if compare with dynamic, highly flexible nature of cloud platforms. This inconsistency creates significant barriers to the development of uniform, consistent network designs and the application of consistent security policies in both environments. In addition, legacy infrastructure often lacks built-in compatibility with modern zero-trust principles, requiring large-scale upgrades or even replacements to support features such as micro-segmentation and dynamic policy enforcement.

Microsegmentation itself, a fundamental principle of ZTA, creates another notable difficulty. Creating accurate micro-segments in mixed cloud and on-premises environments requires detailed planning and advanced technical capabilities. The diversity and distributed nature of resources further increase efforts needed to maintain segmentation boundaries and consistent policy application. This complexity can affect performance, such as increasing latency, due to the constant monitoring and verification of real-time network traffic flows, which can negatively impact the user experience and responsiveness of applications.

An important prerequisite for successful ZTA is to achieve unified visibility of all network resources. Hybrid environments typically suffer from fragmented monitoring systems and isolated logging solutions, making it difficult to try to gain a consistent understanding of network activities and threats. Without integrated visibility, it becomes significantly more difficult to detect potential security incidents or anomalous behavior and respond to them quickly.

When it comes to network access management, centralized identity and access management (IAM) is especially problematic in hybrid setups. Maintaining consistent, unified IAM policies becomes complex when identities and access controls span on-premises Active Directory services, multiple cloud IAM providers, and various third-party solutions. This complexity often leads to policy fragmentation, inconsistencies, and potential security vulnerabilities as the management of authentication, authorization, and user roles across heterogeneous platforms becomes more demanding.

Continuous identity verification—the cornerstone of the Zero Trust approach—also poses significant operational challenges. Implementing real-time persistent authentication and trust verification requires sophisticated technical tools and can be resource-intensive, especially when legacy systems are involved. Additionally, balancing strict security measures, such as always-on authentication and granular access control, with convenience and performance for users remains an ongoing challenge.

Further complicating the issue is the compatibility between suppliers' solutions. Organizations often rely on products from multiple vendors, including firewalls, Zero Trust Network Access (ZTNA) solutions, cloud access security brokers (CASBs), and software-defined wide area networks (SD-WANs). Integrating these diverse solutions into a consistent Zero Trust strategy requires careful vendor selection and significant integration efforts to avoid creating gaps or inconsistencies in security policies.

Compliance and regulatory requirements add another layer of complexity. Consistently adhering to stringent regulatory requirements and compliance standards across cloud and on-premises environments requires meticulous attention to policy development, enforcement, and audit readiness.

Finally, the human factor should not be underestimated. The shift to zero trust from traditional perimeter-based security marks a fundamental cultural shift. Organizational resistance, skills gaps among IT staff, and the need for intensive training and education make it even more difficult to successfully implement and operate ZTA in hybrid network environments. Thus, effective implementation requires not only technical solutions, but also significant investments in organizational alignment, communication and continuous learning.

Addressing these interconnected challenges requires thoughtful planning, careful architecture design, strategic vendor selection, and ongoing cross-functional collaboration to ensure the successful implementation and sustainability of the zero-trust architecture in hybrid IT infrastructures.

Implementing Zero Trust Architecture (ZTA) in hybrid networks that combine on-premises data centers and cloud services creates unique challenges. The reason is mainly the increased diversity of infrastructure elements of different origins, as well as the need for their integration and shared management in compliance with the principles of zero trust. The following are key problems and effective solutions supported by research.

Building a hybrid infrastructure for enterprise needs makes it possible to take advantage of different platforms and formats, but the opposite side of the coin is the need to support a wider number of technologies, as well as new challenges that manifest themselves when migrating to ZTA—zero trust architecture. Migration to ZTA in a hybrid environment is more complex than in traditional on-premises infrastructure. However the successful implementation of ZTA in hybrid infrastructure ensures sustainable security, scalability, and control over today's digital risks.

7. Hybrid infrastructure migration to Zero Trust Architecture recommendations

Migrating a hybrid infrastructure to a Zero Trust Architecture (ZTA) is not a one-time event but a structured and iterative transformation. This process requires careful preparation, gradual implementation, and continuous optimization to ensure that both on-premises and cloud environments remain secure and operationally efficient. Each stage of migration builds upon the previous one, addressing organizational, technological, and human factors. A clear roadmap helps to minimize risks, avoid common pitfalls, and ensure alignment with business goals. Figure 3 represent sequence of main stories in process of migration of infrastructure. The following migration plan outlines the key stages, providing a practical framework for enterprises seeking to modernize their security posture.

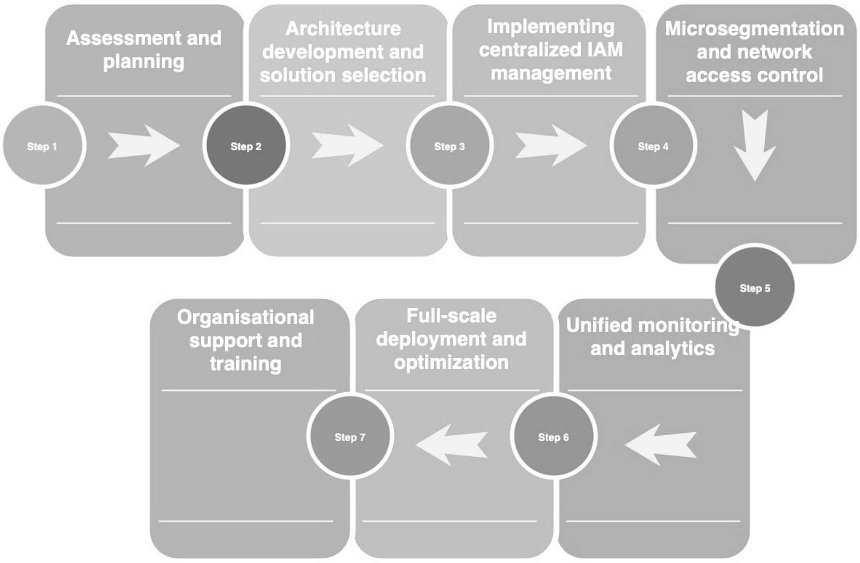
Assessment and planning
Architecture development and solution selection
Implementing centralized IAM management
Microsegmentation and network access control
Step 1
Step 2
Step 3
Step 4
Step 5
Unified monitoring and analytics
Full-scale deployment and optimization
Organisational support and training
Step 6
Step 7

Figure 3: Migration sequence of hybrid infrastructure to ZTA

Stage 1: Assessment and planning

At this stage, it is necessary to conduct a full assessment of the existing IT infrastructure, including hardware and software resources, identities, applications, as well as data flows in both on-premises and cloud environments. It is important to determine the current state of cybersecurity, identify existing gaps, and clarify compliance requirements (compliance with regulatory standards).

The next step is to formulate clear security goals that align with the business objectives and principles of the Zero Trust architecture. It is important to form a step-by-step roadmap, identifying priority resources and applications with the highest risks.

It is also necessary to provide management support and agree on an action plan between IT, security and compliance departments. This involves regular communication about the expected benefits and necessary changes in the organization's culture.

Stage 2: Architecture development and solution selection

In the second stage, a Zero Trust reference architecture should be created, which will provide unified approaches to cybersecurity in a hybrid environment. It should take into account the integration of on-premises and cloud resources, include centralized identity management (IAM), micro-segmentation, and network access policies.

Next, you need to evaluate the solutions available on the market, such as Zero Trust Network Access (ZTNA), Cloud Service Access Protection Brokers (CASBs), IAM solutions, and micro-segmentation tools. It is important to test these solutions as part of Proof of Concept projects, verifying that they meet security, performance, and infrastructure compatibility requirements.

Phase 3: Implementation of Centralized Identity Management (IAM)

This stage involves the creation of a single IAM system that integrates on-premises services (for example, Active Directory) with cloud solutions (Azure AD, Okta, AWS IAM). It is important to implement multi-factor authentication (MFA), single sign-on (SSO), and Conditional Access.

The use of tools for continuous identity verification and adaptive authentication will help implement the principle of continuous access control based on the analysis of user behavior risks. It is also necessary to regularly audit access policies, avoiding fragmentation and ensuring relevance.

Stage 4: Micro-segmentation and access control at the network level.

Conduct a gradual micro-segmentation of the network, starting with the most critical applications and services. This will allow you to create isolated network segments, managing them using software-defined networks (SDN).Traditional perimeter firewall rules should be gradually replaced by access policies at the application and service level, providing dynamic access control to resources. While it is important to make identity management and monitoring unified, it is proposed to make access control at the network level distributed, this approach will provide several advantages, namely:

- Systemic risk reduction: Disruption in one segment or environment is less likely to immediately affect others, providing resilience.
- Increased fault tolerance and fault tolerance: Distributed systems can more effectively isolate and contain threats, preventing massive failures.
- Advanced Protection: Distributed architecture is inherently consistent with the principles of multi-layered security.
- simplification and reduction of the cost of ZTA implementation due to the absence of the need to develop integration solutions

Stage 5: Unified security monitoring and analytics system

At this stage, a centralized monitoring system is created, covering both cloud and on-premises infrastructures. Logging systems should be integrated, as well as solutions such as SIEM (Security Event Monitoring), SOAR (Incident Response Automation), and User Behavior Analytics (UBA). In addition, incident response procedures must be implemented and continuously improved by conducting training simulations for the team on a regular basis.

Stage 6: Full-scale deployment and optimization.

Gradually scale the implementation of the Zero Trust architecture to other resources, services, and users according to the initially developed plan. It is important to constantly analyze the effectiveness of the policies in place, improving them in accordance with changes in the environment and threats. Regularly review and update the architecture to meet new technologies, regulatory requirements, and business needs.

Stage 7: Organizational support and training of staff

It is equally important to conduct regular trainings for IT staff and users, which will help create an understanding of the principles of Zero Trust and teach them how to apply them in practice.

It is necessary to organize systematic information work aimed at changing the corporate culture regarding security, as well as to constantly maintain cross-functional cooperation.

Implementation using the proposed milestones will allow organizations to move to a Zero Trust model in a structured manner, ensure consistent improvements in cybersecurity, and achieve the necessary flexibility and resilience of their hybrid IT infrastructure.

8. Conclusions

Implementing Zero Trust Architecture (ZTA) in hybrid network environments that combine on-premises infrastructure and cloud services is significantly different from classic scenarios using only on-premises or exclusively cloud infrastructure. Hybrid solutions are characterized by a significantly higher complexity of the network architecture, which arises from the need to combine legacy, rigid systems with flexible and dynamic cloud resources. In such conditions, it is much more difficult to provide single visibility, centralized identity management, and consistent access control. Unlike classic architectures, hybrid networks require continuous access verification and real-time monitoring require much more powerful and integrated tools than when using homogeneous environments. Additional difficulties arise from the need to ensure compatibility of solutions from different manufacturers and compliance with regulatory requirements specific to different platforms.

Hybrid environments are also characterized by higher operating costs and a more difficult balance between high security and user performance. Thus, the successful implementation of ZTA in hybrid infrastructures largely depends on careful architectural planning, strategic selection of compatible technologies, and effective organizational support, which makes it more resource-intensive compared to classic scenarios.

The study accomplished next tasks:

- identified key differences between traditional and hybrid architectures
- specified features of hybrid network architectures within the Zero Trust concept
- investigated possible architectural components and technologies
- formed hybrid infrastructure migration to ZTA recommendations

Prospects for further research may include studying the issues of network access control in zero-trust architecture and possible resolutions development.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] A. Teykhrib, Data Transmission in Hybrid Distributed Environment, Int. J. Electr. Comput. Eng., 6 (2016) 2989–2993. doi:10.11591/ijece.v6i6.12129

[2] O. Vakhula, I. Opirskyy, O. Mykhaylova, Research on Security Challenges in Cloud Environments and Solutions based on the “Security-as-Code” Approach, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, 2023, 55–69.

[3] V. Susukailo, I. Opirsky, O. Yaremko, Methodology of ISMS Establishment against Modern Cybersecurity Threats, in: Lect. Notes Electr. Eng., Springer, Cham, 2021, 257–271. doi:10.1007/978-3-030-92435-5_15

[4] A. Liakopoulos, A. Hanemann, A. Sevasti, Point-to-Point Services in Hybrid Networks: Technologies and Performance Metrics, in: Int. Conf. Netw. Serv. (ICNS 2007), 2007, 11–11. doi:10.1109/ICNS.2007.96

[5] O. Milov, et al., Development of Methodology for Modeling the Interaction of Antagonistic Agents in Cybersecurity Systems, East.-Eur. J. Enterp. Technol., 2.9(98) (2019) 56–66. doi:10.15587/1729-4061.2019.164730

[6] S. Vasylyshyn, et al., A Model of Decoy System based on Dynamic Attributes for Cybercrime Investigation, East.-Eur. J. Enterp. Technol., 1.9(121) (2023) 6–20. doi:10.15587/1729-4061.2023.273363

[7] C. Tchepnda, H. Moustafa, H. Labiod, Hybrid Wireless Networks: Applications, Architectures and New Perspectives, in: 3rd Annu. IEEE Commun. Soc. Sensor Ad Hoc Commun. Netw., 3 (2006) 848–853. doi:10.1109/SAHCN.2006.288571

[8] I. Opirskyy, et al., Modern Methods of Ensuring Information Protection in Cybersecurity Systems using Artificial Intelligence and Blockchain Technology, O. Harasymchuk (Ed.), Technology Center PC, Kharkiv, 2025. doi:10.15587/978-617-8360-12-2

[9] P. Petriv, I. Opirskyy, N. Mazur, Modern Technologies of Decentralized Databases, Authentication, and Authorization Methods, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 60–71.

[10] O. Prydybaylo, Zero Trust Architecture Logical Components and Implementation Approaches, Connectivity, 2024. doi:10.31673/2412-9070.2024.030711

[11] P. Skladannyi, et al., Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 97–106.

[12] R. Syrotynskyi, et al., Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture, in: Cyber Security and Data Protection, vol. 3800 (2024) 97–105.

[13] M. Hasan, Enhancing Enterprise Security with Zero Trust Architecture, arXiv preprint, 2024. doi:10.48550/arXiv.2410.18291

[14] J. Singh, Zenith Armor: Advancing Security with Zero Trust Measures, Int. J. Sci. Res. Eng. Manag. (2024). doi:10.55041/ijsrem31326

[15] T. Bashir, Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks, J. Comput. Sci. Technol. Stud. (2024). doi:10.32996/jcsts.2024.6.4.8

[16] O. Prydybailo, Zero Trust Architecture: The Basics Organization Principles, Connectivity (2022). doi:10.31673/2412-9070.2022.051620

[17] B. Lund, et al., Zero Trust Cybersecurity: Procedures and Considerations in Context, Encyclopedia, 4(4) (2024) 99. doi:10.3390/encyclopedia4040099

[18] P. Bansal, Zero Trust Security: Is It Optional?, Int. J. Innov. Sci. Res. Technol. (IJISRT) (2024). doi:10.38124/ijisrt/ijisrt24sep1521

[19] D. Shevchuk, O. Harasymchuk, A. Partyka, N. Korshun, Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, 2023, 217–225.

[20] M. Hussain, et al., Federated Zero Trust Architecture using Artificial Intelligence, IEEE Wirel. Commun., 31 (2024) 30–35. doi:10.1109/MWC.001.2300405

[21] Y. Martseniuk, A. Partyka, O. Harasymchuk, N. Korshun, Automated Conformity Verification Concept for Cloud Security, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 25–37.

[22] P. Nutalapati, Zero Trust Architecture in Cloud-based Fintech Applications, J. Artif. Intell. Cloud Comput. (2023). doi:10.47363/jaicc/2023(2)e152

[23] S. Teerakanok, T. Uehara, A. Inomata, Migrating to Zero Trust Architecture: Reviews and Challenges, Secur. Commun. Netw., 2021 (2021) 9947347:1–9947347:10. doi:10.1155/2021/9947347

[24] P. Dhiman, et al., A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model, Sensors, 24 (2024) 1328. doi:10.3390/s24041328

[25] C. Yang, et al., Research on the Application of Zero Trust Framework in the Design of Power System Network Architecture, Proc. SPIE 13073 (2024) 130731F. doi:10.1117/12.3026713

[26] S. Sarkar, et al., Security of Zero Trust Networks in Cloud Computing: A Comparative Review, Sustainability, 14 (2022) 11213. doi:10.3390/su141811213

[27] M. Khan, Zero Trust Architecture: Redefining Network Security Paradigms in the Digital Age, World J. Adv. Res. Rev., 19(3) (2023). doi:10.30574/wjarr.2023.19.3.1785