UDC 004.8 **doi: 10.26906/SUNZ.2023.2.97-101**

Gennady Golovko, Ivan Taranenko, Oleksiy Kushch

National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

ZERO TRUST: WHY TRADITIONAL SECURITY MODELS NO LONGER WORK

Abstract. In the context of escalating cyber threats and the rapid evolution of digital work environments, traditional security models based on perimeter defense are increasingly proving inadequate. The Zero Trust model introduces a fundamental paradigm shift by eliminating the assumption of trust within corporate networks and instead adopting a continuous verification approach. This article explores the core principles and architectural components of Zero Trust, highlights its operational and strategic advantages over legacy systems, and examines the practical challenges organizations face during implementation. Particular attention is paid to how Zero Trust addresses modern cybersecurity risks such as remote work, cloud infrastructure, insider threats, and the proliferation of mobile and IoT devices. The study also analyzes real-world applications, including Google's BeyondCorp framework, and provides practical recommendations for organizations of various sizes seeking to enhance their security posture. By offering a comparative overview and actionable guidance, this paper contributes to the development of adaptive, scalable, and resilient cybersecurity strategies for enterprises operating in a rapidly changing digital landscape.

Keywords: Zero Trust, cybersecurity, perimeter defense, network security, cloud security, access control, identity verification, digital transformation, remote work, cyber threats.

Introduction

In recent years, the cybersecurity landscape has changed dramatically due to the rapid adoption of cloud services, the rise of remote work, and the increasing sophistication of cyber threats. Traditional security models, which rely heavily on perimeter-based defenses, have become insufficient in protecting modern IT environments. These legacy models operate on the assumption that everything inside the network can be trusted, which has proven to be a critical vulnerability in the age of advanced persistent threats and insider risks.

The concept of Zero Trust, first introduced by analyst John Kindervag in 2010 while at Forrester Research, challenges this outdated assumption by adopting a "never trust, always verify" approach to security. Instead of trusting users or devices by default, Zero Trust continuously evaluates access requests based on identity, context, and risk level, regardless of whether the request originates from inside or outside the network [1].

Organizations such as Google, with its BeyondCorp framework, have successfully implemented Zero Trust principles to protect their infrastructure without relying on traditional VPNs or firewalls. Furthermore, according to the National Institute of Standards and Technology (NIST), Zero Trust is now considered a recommended strategy for reducing the attack surface and increasing organizational resilience.

This article explores the limitations of traditional security models, outlines the core tenets of Zero Trust, and examines its role as a necessary evolution in the face of today's cyber risks

Analysis of Existing Research. The growing interest in Zero Trust security architecture is reflected in numerous recent publications, which examine its core concepts, implementation strategies, and operational benefits. Numerous studies have been dedicated to defining the principles of Zero Trust, its implementation models, and the benefits it brings over traditional perimeter-based security frameworks. Notably, NIST's Special Publication 800-207 provides a comprehensive architectural model and guidance for Zero Trust implementation across different organizational contexts. Similarly, industry reports such as CrowdStrike's Global Threat Report and IBM's Zero Trust Maturity Model examine the evolving threat landscape and advocate for Zero Trust as a strategic response [2].

Many of these works focus on describing Zero Trust's theoretical foundation or reporting on case studies from large enterprises such as Google's BeyondCorp framework. They effectively highlight the vulnerabilities of legacy systems and outline high-level recommendations for Zero Trust adoption. Furthermore, several studies have explored the integration of artificial intelligence (AI) and behavioral analytics to enhance Zero Trust decision-making processes, particularly for anomaly detection and adaptive access control.

However, a critical limitation of these studies is the lack of practical, comparative analyses detailing the specific operational challenges organizations encounter when transitioning from traditional to Zero Trust architectures. Additionally, existing literature often emphasizes enterprise-scale implementations, leaving a research gap in addressing how small and medium-sized enterprises (SMEs) can feasibly adopt Zero Trust principles within resource-constrained environments.

This article addresses these gaps by offering a balanced examination of Zero Trust benefits and real-world implementation challenges, contextualized not only for large corporations but also for medium and small organizations. It provides a practical framework for incremental adoption strategies, tool integration, and policy development, thereby contributing to the operationalization of Zero Trust security models across diverse business environments.

Recent academic works have also expanded the understanding of Zero Trust in specialized domains. Kim et al. (2024) explored the implementation of Zero

© Golovko G., Taranenko I., Kushch O., 2025

Trust principles in defense cybersecurity environments, emphasizing dynamic access control and continuous monitoring [3].

Gambo and Almulhem (2025) conducted a systematic literature review covering the development of Zero Trust architectures from 2016 to 2025, identifying key technological trends and challenges [4].

Additionally, Zanasi et al. (2024) proposed a flexible Zero Trust model tailored for Industrial IoT infrastructures, highlighting the importance of microsegmentation and adaptive access policies in highly heterogeneous environments [5].

Purpose and Objectives of the Study. Based on the analysis of existing research on Zero Trust security models, this study aims to examine the practical implementation of Zero Trust principles in modern IT environments and identify strategies to overcome operational and organizational challenges that arise during this transition. While many prior works provide theoretical foundations or large-scale enterprise case studies, there remains a lack of applied guidance for medium and small organizations adopting Zero Trust under limited resources and legacy infrastructure constraints.

The primary objectives of this study are as follows:

- To analyze the weaknesses of traditional perimeter-based security models in the context of contemporary cyber threats and digital transformation.
- To systematize the core principles and framework components of the Zero Trust model, highlighting their relevance to various organizational environments.
- To investigate real-world Zero Trust implementations, with a focus on both large-scale and resource-constrained organizations.
- To identify the key benefits and operational challenges associated with Zero Trust adoption.
- To propose a practical, incremental implementation approach suitable for different organizational scales, emphasizing operational feasibility and risk mitigation.

By addressing these objectives, the study contributes to closing the existing research gap between theoretical Zero Trust concepts and their real-world operationalization, offering applicable insights for a broader range of enterprises.

Main part

1. The Weaknesses of Traditional Security Models. Traditional cybersecurity strategies are based on perimeter defense, which assumes that everything inside the network is trustworthy, while everything outside is not. This “trust but verify” mindset made sense in an era when organizations operated entirely within on-premise environments. However, in the age of cloud computing and remote work, this model no longer provides sufficient protection.

Modern organizations face a range of threats that traditional models struggle to defend against:

- Remote work has become standard across industries, weakening the internal network concept. VPNs are often overloaded and outdated, failing to provide secure access control for distributed teams (Cisco, 2022);
- Cloud security concerns arise when data is stored and processed across multiple third-party platforms, making traditional firewalls ineffective;
- Insider threats remain a major concern. Once inside the network, attackers (or malicious employees) can move laterally without restriction;
- Digital transformation has introduced more endpoints, devices, and integrations, complicating traditional network security monitoring.

2. The Zero Trust Model: Principles and Framework. Zero Trust is a cybersecurity architecture designed to address the shortcomings of perimeter-based defense. It is built on the idea of "never trust, always verify." Instead of assuming that internal systems and users are safe, it treats every access request — regardless of origin — as potentially malicious until proven otherwise.

The core pillars of Zero Trust are shown in Table 1.

This shift toward **identity verification**, **adaptive access control**, and **visibility** over users and devices allows Zero Trust to secure environments across cloud, hybrid, and on-prem systems [6].

Table 1 – **The core principle of Zero Trust**

Principle	Description
Continuous verification	No user or device is trusted automatically. Identity, device, and context are always checked.
Least privilege access	Users only get access to what they absolutely need — reducing risk exposure.
Micro-segmentation	Networks are broken into zones to minimize damage in case of a breach.
Assume breach	The system is built with the assumption that intrusions will happen — the goal is to contain them.

3. Real-World Application: Google’s BeyondCorp. A leading real-world example of Zero Trust in action is Google's BeyondCorp framework. Launched after a major cyber attack in 2009, BeyondCorp aims to allow employees to work securely from any location without a traditional VPN. Every access request is evaluated based on multiple factors: device posture, user identity, location, time of request, etc (Fig. 1).

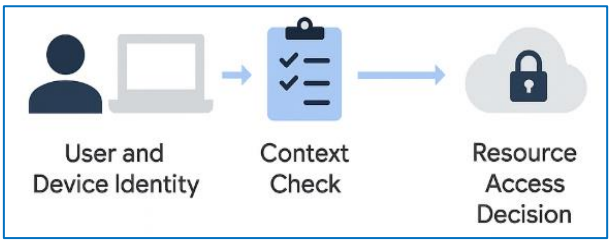

Fig 1. BeyondCorp Access Flow

This model enhances network security by making internal systems less reliant on perimeter defenses. Instead of assuming trust, Zero Trust verifies identity and context every time access is requested [7].

4. Benefits of Zero Trust. The transition to a Zero Trust architecture provides organizations with a robust response to today's dynamic cyber threats. By removing the implicit trust that traditional systems relied upon, Zero Trust significantly reduces the attack surface and increases network security resilience (Table 2) [8].

Key Benefits:

- Minimized impact of breaches: Since access is segmented and tightly controlled, attackers cannot easily move laterally through the network;
- Improved visibility and control: Zero Trust solutions require continuous monitoring of users, devices, and traffic — enhancing situational awareness;
- Stronger cloud security: By applying access policies based on context rather than network location, organizations can more securely adopt cloud services;
- Enhanced compliance: Regulatory frameworks increasingly recommend or mandate Zero Trust elements, especially for protecting identity and access management;
- Support for remote work: Employees can access resources securely from any location or device, without relying on VPNs or centralized infrastructure.

Table 2 – **Key Differences Between Traditional Security and Zero Trust**

Aspect	Traditional Security	Zero Trust Architecture
Trust model	Trust inside, block outside	Trust no one, verify always
Access control	Static, location-based	Dynamic, identity and context-aware
Attack surface	Wide (flat network)	Minimized through segmentation
Cloud and remote support	Limited or dependent on VPN	Built-in and adaptive
Breach response	Reactive, post-incident	Proactive, continuous monitoring
Compliance readiness	Often manual, inconsistent	Auditable, policy-driven

According to recent industry research, organizations implementing Zero Trust experience fewer incidents and lower breach-related costs than those using perimeter-based models. [9]

Improvements after Zero Trust implementation:

- 50% reduction in data breach incidents;
- 2x increase in endpoint visibility;
- 40% improvement in compliance audit readiness;
- Faster detection and isolation of anomalies.

These outcomes make Zero Trust an essential part of digital transformation initiatives, particularly in sectors like finance, healthcare, and government where access control and data integrity are critical.

5. Implementation Challenges. Despite its advantages, implementing Zero Trust is not without obstacles. Organizations often face several technical, cultural, and operational barriers during the transition [10].

Major challenges include:

Legacy infrastructure: Older systems may not support modern identity and policy enforcement mechanisms;

- Organizational resistance: Shifting from a perimeter-focused to an identity-centric mindset can meet opposition from stakeholders used to traditional models;
- Tool and vendor complexity: Integrating different tools for identity verification, device posture, policy engines, and monitoring requires careful planning;
- Cost and resource allocation: The initial investment — both financial and in terms of skilled personnel — may be substantial.

These issues can delay full adoption or lead to partial implementations that fall short of delivering the full benefits of Zero Trust. However, many organizations adopt an incremental approach — starting

with high-risk assets or user groups and expanding gradually.

Tip: Start with an identity and access audit, followed by segmentation and policy definition, to build the foundation of Zero Trust with minimal disruption.

6. Comparative Overview: Traditional vs. Zero Trust Security. As the digital landscape continues to evolve, Zero Trust is expected to become not only a best practice but a fundamental requirement for cybersecurity architectures.

The shift toward decentralized networks, increased remote work, and the proliferation of cloud-based and edge computing systems require a security model that is dynamic, adaptable, and identity-centric.

One of the most promising developments is the integration of artificial intelligence (AI) and machine learning (ML) into Zero Trust frameworks. These technologies enable real-time behavioral analytics, anomaly detection, and automated responses to potential threats. For example, if a user logs in from an unusual location or attempts to access resources outside their normal scope, the system can automatically trigger step-up authentication or deny access entirely

Moreover, the Internet of Things (IoT) presents new security challenges due to the sheer number and heterogeneity of connected devices. Traditional network perimeter controls are insufficient to secure these endpoints. Zero Trust allows for granular policies based on device health, firmware version, and usage patterns, providing enhanced visibility and control over IoT assets [11].

Cloud-native Zero Trust architectures are also becoming a critical focus. As organizations migrate to hybrid and multi-cloud environments, Zero Trust principles ensure that data and applications remain protected across platforms. This includes continuous validation of access requests, encryption of data in motion and at rest, and policy enforcement at every access point.

In the coming years, we are likely to see Zero Trust extended beyond corporate IT to operational technology (OT) and critical infrastructure, where traditional systems were not designed with cybersecurity in mind. Governments and regulatory bodies are already pushing for Zero Trust adoption in these sectors as part of national security strategies

Furthermore, the concept of Zero Trust-as-a-Service (ZTaaS) is emerging, where security vendors provide managed ZT solutions, reducing the burden on in-house teams. This trend is particularly beneficial for small and medium enterprises (SMEs), which may lack the resources to build and maintain complex security infrastructures [12].

In summary, the future of Zero Trust lies in deeper automation, broader adoption across sectors, tighter integration with AI and IoT technologies, and increased regulatory alignment. As organizations strive for resilience in the face of complex cyber threats, Zero Trust will be central to ensuring sustainable and scalable security strategies.

This comparison highlights why Zero Trust is increasingly viewed not just as a cybersecurity improvement, but as a necessity in modern IT environments.

Discussion of Research Results

The analysis of existing scientific publications on Zero Trust models revealed that while previous studies have extensively described the theoretical foundations, core principles, and large-scale enterprise implementations of Zero Trust, they have not sufficiently addressed certain operational aspects and practical challenges organizations face during the transition from traditional perimeter-based models. This study successfully contributes to filling these gaps by:

- Providing a comparative analysis of traditional and Zero Trust security models within the context of modern cyber threats, digital transformation, and remote work environments.
- Systematically structuring the core principles of Zero Trust and relating them to real-world operational needs.
- Highlighting the practical outcomes of a well-documented enterprise-scale implementation (Google's BeyondCorp), offering readers a concrete example of Zero Trust in action.
- Detailing the key benefits organizations can achieve through Zero Trust adoption, including improved visibility, compliance readiness, breach mitigation, and support for distributed workforces.
- Identifying and systematizing the primary technical, cultural, and operational challenges encountered during Zero Trust implementation, which were either omitted or only briefly mentioned in prior works.

Unlike earlier studies that focused mainly on conceptual frameworks or enterprise-level deployments, this paper provides a balanced overview of both strategic advantages and practical obstacles relevant to organizations considering Zero Trust adoption today. By doing so, it expands the applied understanding of Zero Trust and supports informed decision-making for cybersecurity professionals and IT leaders [13].

Conclusion

In an era defined by digital transformation, remote work, and increasingly sophisticated cyber threats, traditional perimeter-based network security approaches are no longer sufficient.

The Zero Trust model emerges as a robust and modern solution that redefines how organizations protect their data, systems, and users. This study not only confirmed the critical weaknesses of traditional security models but also systematized the core principles of Zero Trust, providing a comparative overview of their practical application.

A significant contribution of this research lies in identifying specific operational and organizational challenges associated with Zero Trust implementation — a topic insufficiently addressed in prior studies. By analyzing real-world deployment examples and outlining key benefits, this paper closes existing research gaps and offers applicable insights for organizations of various sizes considering Zero Trust

adoption. Although implementing Zero Trust poses certain difficulties — particularly for organizations with legacy infrastructure — its long-term advantages in terms of resilience, adaptability, and compliance significantly outweigh the transitional challenges. This study emphasizes that Zero Trust should be viewed not merely as a technical solution but as a strategic philosophy aligned with the realities of modern IT environments.

By addressing both conceptual and operational aspects, this research supports informed decision-making for cybersecurity practitioners and provides a foundation for future studies exploring scalable, resource-efficient Zero Trust implementations.

References

1. Forrester Research. The State of Zero Trust Adoption. URL: https://www.forrester.com/zero-trust/
2. CrowdStrike. Global Threat Report. URL: https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2023-global-threat-report/
3. Kim Y., Sohn S.-G., Kim K.T., et al. (2024). Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study. KSII Transactions on Internet and Information Systems, 18(9). DOI: https://doi.org/10.3837/tiis.2024.09.011
4. Gambo M.L., Almulhem A. (2025). Zero Trust Architecture: A Systematic Literature Review. arXiv preprint. DOI: https://doi.org/10.48550/arXiv.2503.11659
5. Zanasi C., Russo S., Colajanni M. (2024). Flexible Zero Trust Architecture for the Cybersecurity of Industrial IoT Infrastructures. Ad Hoc Networks, 157. DOI: https://doi.org/10.1016/j.adhoc.2024.103414
6. NIST. Special Publication 800-207: Zero Trust Architecture. URL: https://doi.org/10.6028/NIST.SP.800-207
7. Google Cloud. BeyondCorp Enterprise Whitepaper. URL: https://cloud.google.com/beyondcorp
8. Cisco. Hybrid Work and VPN Limitations Report. URL: https://www.cisco.com/c/m/en_us/solutions/global-hybrid-work-study.html
9. Verizon. Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/
10. IBM Security. Zero Trust Maturity Model: A Strategic Guide. URL: https://www.ibm.com/zero-trust
11. Gartner. Future of Work Trends: Remote Work and Cybersecurity. URL: https://www.gartner.com/en/information-technology/insights/remote-work-technology
12. Microsoft. Zero Trust Deployment Guidance. URL: https://learn.microsoft.com/en-us/security/zero-trust/
13. Okta. Identity-First Security in a Zero Trust World. URL: https://www.okta.com/zero-trust/

Received (Надійшла) 11.03.2025
Accepted for publication (Прийнята до друку) 21.05.2025

Відомості про авторів / About the Authors

Головко Геннадій В'ячеславович – доцент кафедри комп'ютерних та інформаційних технологій і систем, Національний університет «Полтавська політехніка ім. Ю. Кондратюка», Полтава, Україна;
Gennady Golovko – Associate Professor, Department of Computer and Information Technologies and Systems, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
e-mail: genvgolovko@ukr.net; ORCID Author ID: http://orcid.org/0000-0002-1745-1321;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57195419168.

Тараненко Іван Іванович – студент кафедри комп'ютерних та інформаційних технологій і систем, Національний університет «Полтавська політехніка ім. Ю. Кондратюка», Полтава, Україна;
Ivan Taranenko – student of the Department of Computer and Information Technologies and Systems, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
e-mail: vanyo.taranenko@gmail.com; ORCID Author ID: http://orcid.org/0009-000-4606-6943.

Кущ Олексій Олексійович – аспірант кафедри автоматики, електроніки та телекомунікацій, Національний університет «Полтавська політехніка ім. Ю. Кондратюка», Полтава, Україна;
Kushch Oleksiy – PhD student at the Department of Automation, Electronics and Telecommunications, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
e-mail: alexkusch881@gmail.com; ORCID Author ID: https://orcid.org/0000-0002-7630-6298.

Zero Trust: чому традиційні моделі безпеки більше не працюють

Г. В. Головко, І. І. Тараненко, О. О. Кущ

Анотація. На тлі зростання кіберзагроз і стрімкої трансформації цифрового робочого середовища традиційні моделі безпеки, що базуються на периметровому захисті, дедалі частіше виявляються неефективними. Модель Zero Trust пропонує принципово новий підхід, усуваючи припущення про довіру всередині корпоративних мереж і запроваджуючи концепцію безперервної верифікації. У статті розглянуто основні принципи та архітектурні компоненти Zero Trust, окреслено її стратегічні й операційні переваги порівняно із застарілими системами, а також проаналізовано практичні виклики, що виникають у процесі впровадження. Особливу увагу приділено подоланню сучасних загроз кібербезпеки, таких як віддалена робота, хмарні сервіси, внутрішні загрози та поширення мобільних і IoT-пристроїв. Дослідження містить аналіз реальних прикладів застосування, зокрема фреймворку BeyondCorp від Google, і надає практичні рекомендації для організацій різного масштабу щодо підвищення їхньої кібербезпеки. Запропонований порівняльний огляд і прикладні рекомендації сприяють розробці адаптивних, масштабованих і стійких стратегій кіберзахисту в умовах динамічного цифрового середовища.

Ключові слова: Zero Trust, кібербезпека, периметровий захист, мережна безпека, хмарна безпека, контроль доступу, верифікація особистості, цифрова трансформація, віддалена робота, кіберзагрози.