Zero-Day Attacks and Zero Trust Architecture: A Critical Comparative Review

Hussein Ali Ismael[1]
[1] Department of Computer Science, College of Science, University of Diyala, 32001, Iraq.
Al-Shaibani@uodiyala.edu.iq

Abstract

Because zero-day attacks take advantage of undiscovered, undeclared, or unpatched vulnerabilities before trustworthy signatures, patches, or mitigation rules become available, they continue to be one of the most significant concerns in contemporary cybersecurity. Simultaneously, cloud, remote work, Internet of Things, and hybrid enterprise environments are becoming more and more inadequate for conventional perimeter-based security methods. Zero Trust Architecture is a security paradigm that substitutes policy-based access control, least privilege, micro-segmentation, and continuous verification for implicit trust. This study uses an IMRaD-based framework backed by an Evidence and Reliability Protocol and a PRISMA-informed approach to critically compare zero-day attacks with Zero Trust Architecture. Zero-day detection, machine learning-based intrusion detection, benchmark datasets, Zero Trust principles, migration issues, and cyber-resilience tactics are all included in this review. The results show that because Zero Trust does not eliminate unknown vulnerabilities, it cannot completely prevent zero-day exploitation. On the other hand, it can lessen the attack surface, restrict lateral movement, limit privilege escalation, increase visibility, and lessen the consequences of a compromise. Key gaps are also identified by the review, such as the lack of standardized benchmarks for assessing Zero Trust's efficacy against zero-day attack chains, fragmented Zero Trust implementation models, poor integration between anomaly detection and policy enforcement, and limited real-world validation. Adaptive Zero Trust architectures that incorporate explainable intrusion detection, dynamic risk assessment, Moving Target Defense, and human-in-the-loop decision support should be the main emphasis of future study.

Keywords: Zero-day attacks, Zero Trust Architecture, intrusion detection systems, anomaly detection, cyber resilience, micro-segmentation, PRISMA; critical review.

1. Introduction

The goal of a zero-day attack is to take advantage of a vulnerability that has not been discovered or patched by the vendor or security software. The attacks generally exploit unknown, undisclosed, or unpatched vulnerabilities before security software or the vendor can create a reliable signature, patch, or mitigation rule. Zero days are different from known attacks because they may not have a known behaviour in the data sets or in the signature repository of an IDS. Though machine learning and deep learning have advanced the field of anomaly-based detection, the accurate detection of completely new attacks is an open and challenging research challenge, according to recent reviews [1] and [2].

The challenges of zero-day defense are exacerbated by the evolution of the modern digital environment. Enterprise systems no longer have to be restricted to internal networks with a distinct boundary. Rather, they're relying on cloud services, remote networks, bring your own device approaches, software-defined networks, IoT devices, and distributed workloads. The changes remove some of the traditional assumptions about the perimeter of networks; traditionally, internal users or devices were assumed to be trusted after crossing the network boundary [3] and [4].

Zero Trust Architecture (ZTA), which shifts the emphasis of security from trust to ongoing verification—based on identity and context—was created to address these flaws. Fundamentally, Zero Trust holds that no user, device, program, or network segment should be trusted until it has been demonstrated to be so. Everything should be assumed to be untrusted, even if it is inside the organization's network boundaries, according to the fundamental idea of Zero Trust. Instead, access should be granted in accordance with explicit verification, least privilege, policy enforcement,

device posture, and ongoing monitoring. [3] and [5].

But the connection between Zero Trust Architecture and zero-day attacks is something that needs to be examined. Zero Trust is not a "perfect" zero-day prevention solution as it does not eliminate unknown vulnerabilities or bugs in software or hardware systems. The benefit of it is primarily to minimize the attack surface, restrict access, limit lateral movement, gain some visibility, and minimize the consequences of compromise once it has occurred. Thus, Zero Trust is considered a resilience-based security architecture instead of vulnerability discovery, vulnerability patching, or anomaly detection [4] and [6].

The majority of the research on zero-day attack detection and zero-trust architecture is conducted as separate fields of study in the literature currently in publication. Anomaly detection, machine learning, deep learning, transfer learning, and intrusion datasets are typically the topics of research on zero-day attacks. Nonetheless, identity, access control, micro-segmentation, policy enforcement, continuous authentication, and architectural migration are the main topics of the Zero Trust investigations. Due to this division, there has not been much study done on how Zero Trust controls react to the particular lifespan, vectors, and post-exploitation behaviors of zero-day attacks [1] [2] [4] and [6].

This study addresses a critical comparative analysis of zero-day attacks and Zero Trust Architecture to close this gap. The assessment looks at how zero-day attacks can get beyond conventional security measures, evaluates how Zero Trust reduces exposure and post-compromise harm, and identifies situations in which Zero Trust is insufficient to defend against an unknown threat. The PRISMA technique and IMRaD structure of the study enable the clear identification, screening, and synthesis of literature. Additionally, during the review, an Evidence and Reliability Protocol is employed to distinguish confirmed facts from analytical interpretations, assumptions, and limits [7] and [8].

Contributions of This Review: The main contributions of this review are summarized as follows:

1. Zero-day attacks and Zero Trust Architecture are two connected but conceptually different cybersecurity domains that are critically synthesized in this review.
2. It creates a comparison mapping between the defensive capabilities of Zero Trust controls and the features of zero-day attacks, such as unknown exploitation, stealth, privilege escalation, persistence, and lateral movement.
3. It makes clear that Zero Trust Architecture should be viewed as a resilience-oriented structure that can decrease post-compromise effect, limit lateral movement, and reduce attack surface rather than as a comprehensive preventative strategy against zero-day exploitation.
4. In order to identify confirmed findings, analytical interpretations, assumptions, and limits in the reviewed literature, it combines an Evidence and Reliability Protocol with a PRISMA-informed review technique.
5. It combines an Evidence and Reliability Protocol with a PRISMA-informed review technique to identify validated results, analytical interpretations, presumptions, and limits in the examined literature.

Organization of the Paper. An IMRaD-based review framework is used to structure the rest of this paper. The review technique, which includes the PRISMA-based search strategy, inclusion and exclusion criteria, evidence reliability protocol, and data synthesis approach, is presented in Section 2. The primary findings of the review are presented in Section 3, along with a taxonomy of zero-day attacks, a comparison mapping between zero-day threats and Zero Trust controls, and an overview of the chosen literature. By examining Zero Trust's advantages, disadvantages, research gaps, and potential future approaches with regard to zero-day threats, Section 4 critically examines the results. The work is finally concluded in Section 5, which summarizes the key conclusions and outlines the implications for cybersecurity architects, practitioners, and researchers.

2. Technical Background and Related Work

2.1 Zero-Day Attacks: Concept and Detection Challenges

Zero-day attacks are defined by Ahmad et al. [1] as cyberattacks that take advantage of vulnerabilities that are not yet known to vendors, defenders, or security technologies. They contend that the lack of trustworthy signatures, patches, or mitigation policies during the initial attack window is the primary threat posed by such attacks. Similarly, because novel attacks might not match previously labeled samples, known attack characteristics, or signature repositories, Guo [2] describes zero-day detection as an ongoing cybersecurity challenge. Because delayed detection might result in privilege escalation, persistence, lateral movement, or data exfiltration, zero-day attacks are especially risky in business, cloud, IoT, and industrial settings.

Because anomaly-based intrusion detection focuses on deviations from usual activity, Buczak and Guven [9] argue that it is better suited for unknown threats than signature-based detection. In their evaluation of intrusion detection methods, Khraisat et al. [10] demonstrate that when attack patterns are novel, changing, or underrepresented in training datasets, conventional IDS algorithms continue to have limitations. While Sarhan et al. [13] contend that zero-shot learning can assist in assessing how detection models react to undiscovered attack classes, Liu and Lang [11] further highlight machine learning and deep learning as crucial avenues for intrusion detection. Nevertheless, class imbalance, feature representation, dataset quality, and the challenge of verifying models against genuinely unseen threats continue to limit these methods.

2.2 Zero Trust Architecture: Concept and Security Principles

Zero Trust Architecture is a cybersecurity concept that states that no user, device, task, or network segment should be trusted by default, according to Rose et al. [3]. They stress that explicit verification, least privilege, device posture, and ongoing policy enforcement—rather than network location—should be the basis for access decisions. In response to the shortcomings of perimeter-based security, especially in cloud computing, remote work, bring-your-own-device environments, and distributed enterprise systems, He et al. [4] introduce Zero Trust.

According to Kang et al. [5], identity verification, policy-based access control, least privilege, and ongoing monitoring are the fundamental tenets of zero trust. In their critical analysis, Fernández and Brazhuk [6] contend that Zero Trust Architecture should not be viewed as a comprehensive security solution since it is unable to eliminate software flaws or stop all possible exploitation scenarios. Zero Trust is further described by Syed et al. [22] as a multi-layered architecture strategy that integrates identification, device posture, network segmentation, application access control, and ongoing monitoring. Therefore, rather than being a comprehensive defense against zero-day exploitation, Zero Trust should be seen as a containment and cyber-resilience architecture.

2.3 Related Work on Zero-Day Detection

In their investigation of deep learning methods for detecting zero-day attacks, Hindy et al. [12] demonstrate how autoencoder-based models can help identify anomalous network behavior. A zero-shot machine learning approach is put forth by Sarhan et al. [13] to assess how intrusion detection systems react to unknown attack classes. Using transferable generative adversarial networks based on deep autoencoders, Kim et al. [14] investigate zero-day malware detection and propose that generative models could enhance the detection of malware types that have never been observed before. The potential of transfer learning to enhance generalization beyond known attack classes is highlighted by Sameera and Shashi's [15] deep transductive transfer learning system for zero-day attack detection.

These investigations show encouraging detection skills, but they also highlight persistent drawbacks. Many machine learning-based zero-day detection models are tested under controlled dataset settings, which might not accurately reflect attack chains in the real world, according to Guo [2]. Additionally, Sarhan et al. [13] stress that assessment design and dataset realism have a significant impact on performance against unknown attack types. According to Xi [30], machine learning models in

cybersecurity may also be susceptible to idea drift, evasion, and hostile manipulation. Therefore, rather than being a completely deterministic classification problem, zero-day detection should be viewed as a probabilistic and risk-based approach.

2.4 Related Work on Zero Trust Architecture

A thorough overview of Zero Trust Architecture is given by Syed et al. [22], who address its tenets, elements, implementation specifications, and security issues. The concept of "never trust, always verify" needs to be converted into effective governance, policy management, and technology controls, according to Buck et al.'s analysis of the state of the art and research gaps in Zero Trust [23]. The difficulties of switching from outdated perimeter-based models to Zero Trust Architecture are covered by Teerakanok et al. [24], including organizational preparedness, system compatibility, and policy complexity. Phiayura and Teerakanok [26] emphasize the necessity of organized implementation stages and offer a thorough framework for Zero Trust migration.

Additional research focuses on domain-specific implementation, cost-effectiveness, and maturity. The cost-effectiveness of Zero Trust Architecture for corporate security is examined by Adahman et al. [28], who recommend that adoption choices take into account both financial and technical limitations. Yeoh et al. [29] provide a framework for evaluating Zero Trust cybersecurity maturity and identify key success indicators. According to this research, adopting Zero Trust is an organizational change that involves identity governance, policy maturity, asset visibility, monitoring capabilities, and operational readiness in addition to being a technical process.

2.5 Critical Research Gap

The detection of zero-day attacks using anomaly detection, machine learning, deep learning, and associated intrusion detection approaches is the primary emphasis of Ahmad et al. [1] and Guo [2]. Syed et al. [22] and Teerakanok et al. [24], on the other hand, mainly concentrate on Zero Trust concepts, implementation models, segmentation, identity verification, access control, and migration problems. This suggests that zero-day detection and zero-trust architecture are frequently researched independently.

Nevertheless, little study specifically looks at the relationship between Zero Trust measures and the lifecycle of zero-day attacks, particularly after the first exploitation. By critically analyzing how Zero Trust can lower exposure, limit post-exploitation mobility, enhance monitoring, and fortify cyber resilience, this analysis fills that gap. This article assesses where Zero Trust offers strong, partial, or limited defensive utility against zero-day threats rather than whether Zero Trust can completely avoid zero-day attacks. This viewpoint offers a contrast between zero-day attacks and zero-trust controls that is more grounded in reality and can be supported academically [3], [6], and [29].

3 Methodology

3.1 Review Design

An IMRaD-based framework modified for review articles was used to design this study as a critical comparative review. With a focus on detection, mitigation, containment, and cyber resilience, it synthesizes and critically evaluates the available data on zero-day attacks and Zero Trust Architecture instead of testing a novel detection model [1], [2]. In order to facilitate transparent literature selection, screening, eligibility evaluation, and synthesis, the review also takes a PRISMA-informed approach. PRISMA 2020 was utilized as a reporting guide rather than a meta-analysis framework because the selected research ranged in scope, technique, datasets, architectures, and evaluation measures [7], [8]. The PRISMA-based study selection flow is shown in Figure 1, and the given n values indicate that the search and screening procedure has been completed.

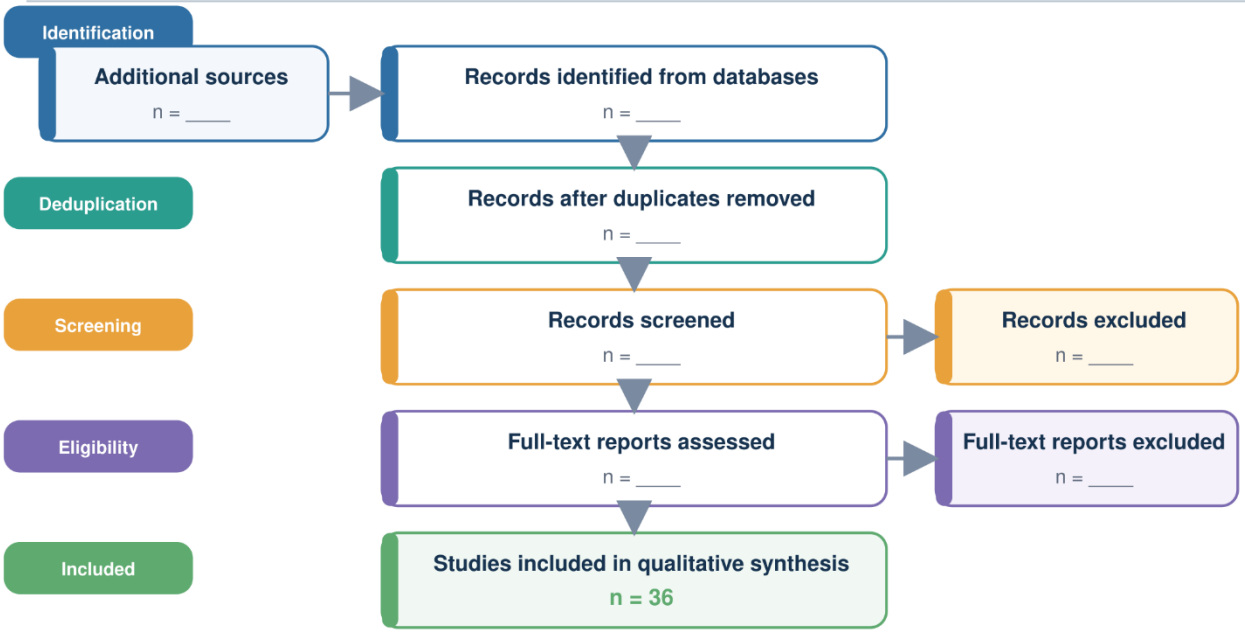


Figure 1. PRISMA 2020 Study Selection Flow Diagram.

3.2 PRISMA-Based Search Strategy

The literature search was designed into two primary research areas: detection of zero-day attacks and Zero Trust Architecture. The search terms were grouped into three clusters. The first cluster was about zero-day threats, like "zero-day attack," "unknown attack detection," "zero-day vulnerability," "zero-day malware," and "zero-day intrusion detection." The second cluster was centered on defensive and analytical strategies, which included the concepts of "machine learning," "deep learning," "anomaly detection," "intrusion detection system," "transfer learning," and "cyber resilience." The third cluster was related to Zero Trust, employing such terms as Zero Trust Architecture, Zero Trust security, least privilege, continuous authentication, micro-segmentation, and policy enforcement [1], [2], [3], and.[4]

Major academic databases and publisher platforms like Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Wiley Online Library, and MDPI will be searched. Consideration was also given to standards and official technical documents when these documents offer definitions or architectural guidance that is fundamental to the understanding of the selected architecture, such as the NIST Special Publication 800-207, Zero Trust Architecture [3]. To ensure relevance of the results to the review questions, publication quality, the clarity of the methodology, and the bibliographic information, such as the DOI (where available), the search results were screened.

3.3 Inclusion and Exclusion Criteria

Only pertinent and academically sound studies that can be used are included due to the formulation of the inclusion criteria. Zero-day attack detection, unknown attack detection, anomaly-based intrusion detection, machine learning, deep learning for cybersecurity, zero trust architecture, zero trust implementation, access control, micro-segmentation, and cyber-resilience strategy were among the focus areas of studies that were included. Priority was given to peer-reviewed journal articles, systematic reviews, excellent conference papers, official standards, and technical guides released within the last ten years (2016–2026).

Educational study was excluded if it had nothing to do with cybersecurity, if the methodology was unclear, if there was insufficient bibliographic information, if it was more opinion than technical or scholarly support, or if it simply mentioned zero trust or zero-day attacks in passing. A non-peer-reviewed source was only utilized when it was an

official standard, technical framework, or authoritative institutional guidance. The source was used cautiously and without question regarding the review's concepts when DOI data were unavailable [3] and [7].

3.4 Evidence and Reliability Protocol

The review employs an Evidence and Reliability Protocol in order to ensure academic reliability while synthesizing. Factual statements are based only on information that has been referenced in the reviewed literature, standards, or documented technical evidence. Second, interpretations are explicit, that is, they are analytical conclusions based on the comparison of several sources and not the result of a single case study. Third, any assumptions are only used if they are needed for conceptual comparison and, when used, are assumed to be an interpretation and not a proven statement. Fourth, limits are clearly identified when evidence is inadequate, incomplete, data set dependent, or not validated in real-world contexts. This protocol is especially significant because it is a space where exaggerated claims tend to abound, both in the area of zero-day attack detection and Zero Trust implementation. For instance, the machine learning detection technology might achieve high accuracy on a benchmark data set but not necessarily on a real data set with a new, unknown attack (zero day). In a similar fashion, Zero Trust Architecture can decrease attack surface and lateral movement but does not necessarily eradicate unknown vulnerabilities or prevent exploitation altogether [1], [2], [4], and [6].

3.5 Data Extraction and Synthesis

The selected studies were analyzed by five categories: Study focus, Cybersecurity domain, Method or architecture, Main findings, and Reported limitations. The following are noted for the zero-day attack studies: Detection method, type of dataset, learning approach, evaluation measures, and capability to deal with unseen and unknown attacks. Architectural principles, identity and access control mechanisms, policy enforcement, micro-segmentation, continuous monitoring, and implementation challenges were all considered for Zero Trust studies.

The synthesis was based on a narrative and comparative method. The selected literature was divided thematically, and that is the first step. Second, a taxonomy of the problems of zero-day attack vectors and detection was set up. Third, Zero Trust principles were compared to the zero-day attack stages to determine the extent to which Zero Trust is useful for defense. Lastly, a critical interpretation of the findings was carried out to reveal the gaps in the research and future directions. This is not an antagonism of the two models, but rather an interaction of them in the current defense of the cyber world, which is the target of the paper.

Table 1. Review protocol summary.

Component	Description
Review type	Critical comparative review
Reporting guide	PRISMA 2020-informed approach
Structure	IMRaD adapted for review articles
Main topic	Zero-day attacks and Zero Trust Architecture
Search focus	Zero-day detection, unknown attacks, anomaly detection, Zero Trust, cyber resilience
Main databases	Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Wiley, MDPI
Inclusion focus	Peer-reviewed studies, systematic reviews, technical standards, and architecture-focused works
Exclusion focus	Irrelevant, weakly documented, non-technical, or unsupported sources
Synthesis method	Narrative, thematic, and comparative synthesis
Reliability rule	Facts, interpretations, assumptions, and limitations are separated clearly.

Table 1. Review databases, search terms, publication years, inclusion and exclusion criteria, document kinds, and screening choices should all be reported. It connects the paper with PRISMA logic and enhances methodological transparency.

4 Results of Literature

4.1 Overview of the Selected Literature

According to the studied literature, machine learning-based cybersecurity, anomaly detection, and intrusion detection systems are strongly related to zero-day attack research. Signature-based intrusion detection systems (IDSs) are successful against known attacks but remain poor against unexpected or changing threats, as demonstrated by Buczak and Guven [9] and Khraisat et al. [10]. Because they detect anomalies from typical activity rather than depending solely on predetermined signatures, anomaly-based and learning-based approaches are therefore more pertinent to zero-day detection.

Machine learning and deep learning are key methods for modeling complicated network traffic and identifying suspicious patterns, according to Liu and Lang [11] and Hindy et al. [12]. However, due to dataset bias, class imbalance, obsolete traffic, and limited representation of undiscovered attacks, high accuracy on benchmark datasets does not always imply real-world zero-day resilience. Transfer learning, zero-shot learning, autoencoders, and generative models can enhance generalization beyond known attack classes, as demonstrated by Sarhan et al. [13], Kim et al. [14], and Sameera and Shashi [15]. However, their effectiveness still depends on feature quality, training diversity, model robustness, and realistic evaluation.

Malware, ransomware, IoT, and IIoT systems are also highlighted in the literature as significant zero-day study topics. While ToN-IoT and Edge-IIoT set investigations demonstrate that heterogeneous devices, low resources, weak patching cycles, and various protocols enhance zero-day exposure in IoT and industrial environments [20], [21], Zahoora et al. [16] highlight the challenge of identifying unknown ransomware variants. Although benchmark datasets like CICIDS2017, UNSW-NB15, ToN-IoT, and Edge-IIoTset are still helpful for assessment, they should be interpreted with caution because simulated or lab-generated traffic might not accurately reflect real enterprise networks, adaptive attackers, or evolving zero-day attack chains [17]–[21].

Table 2. Summary of key literature categories.

Ref.	Literature category	Main focus	Relevance to this review
[9], [10]	IDS surveys	Anomaly-based and signature-based detection	explains why unidentified attacks are a challenge for typical IDS.
[11], [12]	ML/DL intrusion detection	Learning-based detection models	backs up the conversation on automated zero-day detection
[13], [14], [15]	Zero-day-specific detection	Transfer learning, zero-shot learning, and generative models	allows zero-day detection analysis directly.
[16]	Zero-day ransomware	Unknown ransomware variants	displays domain-specific difficulties with zero-day detection
[17]-[21]	Benchmark datasets	CICIDS2017, UNSW-NB15, ToN-IoT, Edge-IIoTset	supports the debate of dataset reliability and evaluation

Figure 2. should differentiate between constraints, interpretations, facts, and assumptions. It can also specify the priorities for technical reports, systematic reviews, peer-reviewed publications, and standards. This avoids drawing unwarranted conclusions and bolsters the paper's reliability claim.

4.2 Taxonomy of Zero-Day Attacks

After reading the literature, there are four categories of zero-day attacks; these categories are based on exploited asset, attack behavior, detection difficulty, and the post-exploitation objective. Vulnerability Level: Zero-day attacks are attacks for which the vulnerability is unknown to the defender, or has not been patched by the vendor. Behavioral signs could include malware

execution, network intrusion, privilege escalation, ransomware activity, web exploitation, or lateral movement. This diversity complicates any one defensive solution for detecting zero-day attacks, as well as complicates the development of an effective defense [1] and [2]. The threats that are known as zero-day can be categorized as follows: network-based attacks, zero-day malware, ransomware, IoT/IIoT attacks, or post-exploitation behavior (refer to Figure 2).

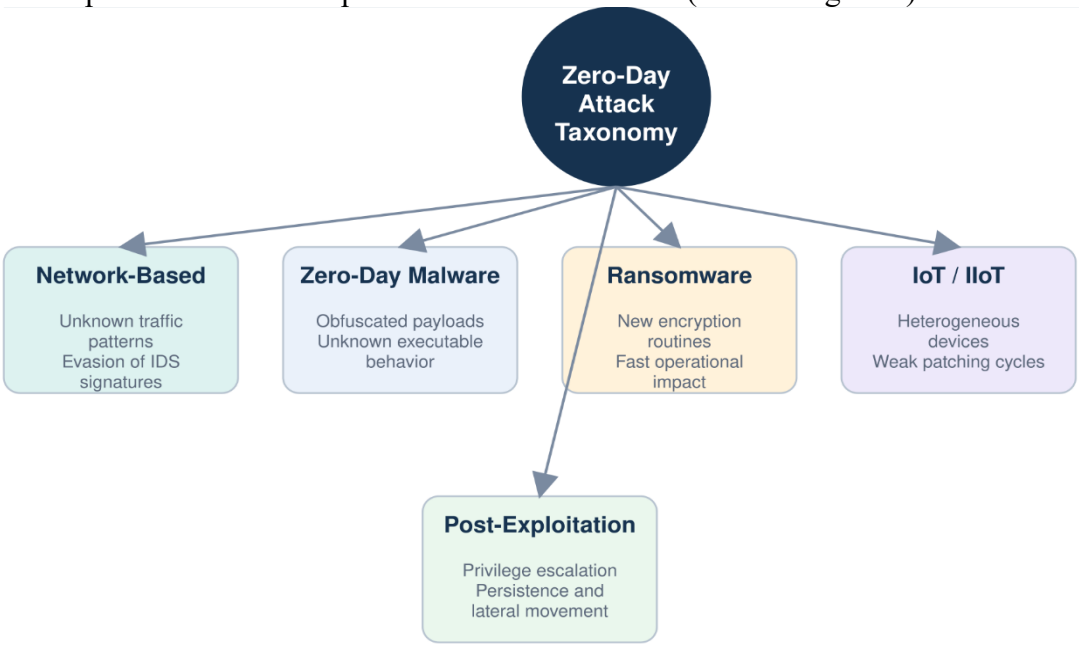


Figure 2. Taxonomy of Zero-Day Attack Categories.

A first category includes network-based zero-day attacks, in which hostile traffic tries to evade intrusion detection systems by employing patterns that have never been detected before. Because the malicious activity may not match known signatures or previously identified attack classes, these attacks provide a challenge to traditional IDS approaches. Deep learning models and anomaly-based intrusion detection systems are frequently suggested for this category, although they are still susceptible to false positives and poor generalization when the training data does not accurately reflect the diversity of actual attacks [9], [10], and [12].

A second category includes ransomware and zero-day malware. In this instance, the attack might use altered payloads, obfuscation, unknown code, or behavioral modifications intended to evade endpoint detection and antivirus software. Learning-based approaches can enhance the detection of unseen variants, according to research on transferred generative adversarial networks and deep autoencoder-based ransomware detection [14], but they still need careful validation against realistic unseen samples and robust feature extraction [16].

A third category includes IoT and IIoT zero-day attacks. Because IoT systems frequently include diverse devices, constrained computational resources, vulnerable firmware, poor authentication, and delayed patching, these threats are especially dangerous. Because they contain current IoT and IIoT traffic patterns, datasets like ToN-IoT and Edge-IIoTset are helpful for researching these scenarios. Nevertheless, the operational complexity of actual industrial contexts cannot be adequately captured by laboratory datasets [20] and [21].

A fourth category includes post-exploitation zero-day behaviors, including lateral movement, persistence, privilege escalation, and credential misuse. These actions are particularly pertinent to Zero Trust Architecture since, although it might not stop the initial exploitation of an unidentified vulnerability, Zero Trust can limit the attacker's freedom of movement within the compromised environment. From the standpoint of cyber-resilience, it is crucial to compare zero-day

assaults with zero-trust restrictions [3], [4], and [22].

Table 3. Taxonomy of zero-day attack categories.

Category	Typical target	Main detection challenge	Relevant defensive focus
Network-based zero-day attacks	Network traffic and services	Unknown traffic patterns and lack of signatures	IDS, behavioral tracking, and anomaly detection
Zero-day malware	Endpoints and files	Obfuscation, unknown payloads, adversarial modification	Behavior analysis, sandboxing, and endpoint detection
Zero-day ransomware	Filesystems and enterprise assets	New encryption behavior and unseen variants	Early anomaly detection, backup isolation, and access control
IoT/IIoT zero-day attacks	Industrial systems, sensors, and smart devices	Device diversity and few resources	Device posture monitoring, segmentation, and lightweight IDS
Post-exploitation behavior	Internal services, identities, and privileges	Misuse that appears legitimate after compromise	After a compromise, legitimate-looking abuse

Table 3 should contrast machine learning, deep learning, transfer learning, zero-shot learning, anomaly detection, signature-based detection, and ransomware-specific detection. Evidence quality, dataset reliance, explainability, adversarial robustness, and false positives should all be highlighted.

4.3 Zero Trust Architecture Pillars

The Zero Trust Architecture relies on the principle that trust should not be assumed just because of the location of the network, the owner of the device, or the fact that they have internal access. Rather, any access to the system should be specifically authorized before it is made. All Zero Trust literature reviewed consistently recognizes the following elements as critical for Zero Trust implementation: identity verification, least privilege, continuous monitoring, policy enforcement, and segmentation. Figure 3 is a summary of Zero Trust Architecture, which is a layered security model that covers identity, device, network, application/workload, and data controls. Shared mechanisms are depicted as cross-cutting functions or mechanisms, rather than individual tools, such as the policy engine, policy enforcement point, continuous monitoring, risk scoring, and logging.

Figure 3. Layered Zero Trust Architecture Model.

The first pillar is on the identity front. One of the cornerstones of a Zero Trust approach is that users, devices, services, and workloads need to be authenticated and authorized to access enterprise resources. Especially important for zero-day attacks: if there are compromised credentials or an endpoint, attackers can seem to be legitimate. Routine identity verification and context-based access control help mitigate the risk of free rein once identity has been compromised [22], [5], and [3].

The second pillar is least privilege access. Therein, Zero Trust reduces the amount of access subjects can have to a specific task. The principle is crucial in the case of a zero-day attack because, no matter what unknown vulnerability is used to attack the system, the attacker can have access to other systems or other sensitive assets. Yet, the implementation of least privilege is closely related to the correct design of the policies, the proper classification of assets, and regular review of access [4] and [24].

Micro-segmentation is the third pillar. Instead, Zero Trust views the internal network as not being a trusted zone and breaks up infrastructure into smaller logical segments that are controlled in the communication between each segment. Micro-segmentation can be important to prevent post-exploitation zero-day activities as it can minimize the attacker's ability to spread laterally between compromised systems and minimize the lateral move [22], [24]

Continuous monitoring and risk-based evaluation are the fourth pillar. Unlike traditional authentication schemes, Zero Trust is not simply an onetime action, but continually assesses user activity, device posture, network activity, and policy adherence. This is significant as zero-day attacks might not be discovered at the initial exploitation phase, but later in the post-exploitation phase, the usage of continuous monitoring and anomaly detection [5] and [23] may be used to detect suspicious activity.

The fifth pillar is the enforcement of policies and architectural maturity. Zero Trust is not a product, but a policy-based approach that involves multiple policy engines, policy enforcement points, identity providers, endpoint controls, logs, and organizational governance. The migration to Zero Trust is mentioned in several studies as a complex, costly, and organization-readiness, legacy-system-compatibility, and maturity-dependent process [26], [28], and [29].

Table 4. Zero Trust pillars and their relevance to zero-day defense.

Zero Trust pillar	Main function	Relevance to zero-day threats	Key limitation
Identity verification	Verifies the identification of the user, device, and workload	decreases the abuse of compromised identities	Strong IAM and MFA are necessary.
Least privilege	restricts access to the bare minimum of permissions needed	minimizes identity theft	Requires accurate policy design
Micro-segmentation	creates regulated zones for infrastructure.	Limits lateral movement	depends on having a strong MFA and IAM.
Continuous monitoring	tracks posture and behavior over time	identifies questionable post-exploitation behavior	May generate false positives
Policy enforcement	Applies access decisions consistently	identifies questionable post-exploitation activity	detects questionable behavior after exploitation

Zero-day attack stages should be mapped to Zero Trust controls like conditional access, least privilege, micro-segmentation, device posture assessment, logging, and policy enforcement in Table 4. Additionally, it should assign a restricted, partial, medium, high, or context-dependent rating to the projected defensive value.

4.4 Comparative Mapping Between Zero-Day Threats and Zero Trust Controls

Comparing Zero-day attacks and Zero Trust Architecture reveals that they're on different layers of cybersecurity. A zero-day attack is an attack that uses a vulnerability in software, hardware, configuration, or logic that is not known to the software/hardware manufacturer. Zero Trust doesn't solve the problems of discovering and eliminating these vulnerabilities. On the other hand, it is used to diminish the attacker's opportunities before exploitation and the attacker's freedom after the exploitation [1], [3][6].

In the pre-exploitation phase, Zero Trust can help to limit exposure by implementing least privilege, obscurity for services, device posture validation, and access restrictions to sensitive resources. But it can't guarantee that there may not be some vulnerability in the system that it has not discovered or that it cannot be exploited. So, Zero Trust needs to be supplemented by the other security pillars of vulnerability management, secure development, threat intelligence, and attack surface reduction [3], [4], and [24].

Exploitation is the halfway point of the life cycle. Zero Trust offers only partial protection. Zero Trust controls can't stop an attack that takes advantage of an unknown vulnerability in an approved application or trusted endpoint. However, additional layers of strong authentication, conditional access, and device posture checks may limit the number of potential targets available for exploitation, and may make it more difficult to exploit them [22] and [27].

As the post-exploitation phase approaches, Zero Trust proves to be more useful. After gaining access to a system, the attackers will try to escalate privileges, steal credentials, persist, and move laterally. Micro-segmentation, least privilege, session monitoring, and adaptive policy enforcement are all components of Zero Trust controls that could limit the attacker's ability to spread its control throughout the environment [3], [22], and [23].

Zero Trust, viewed from a critical perspective, should be considered as a containment & resilience strategy and not a zero-day prevention strategy. The effectiveness depends on the level of maturity of implementation, quality of the access policies, connection with monitoring systems, and ability to react dynamically to abnormal behaviour. If not, Zero Trust will be a disjointed defense system and not a unified one [26], [28], and [29].

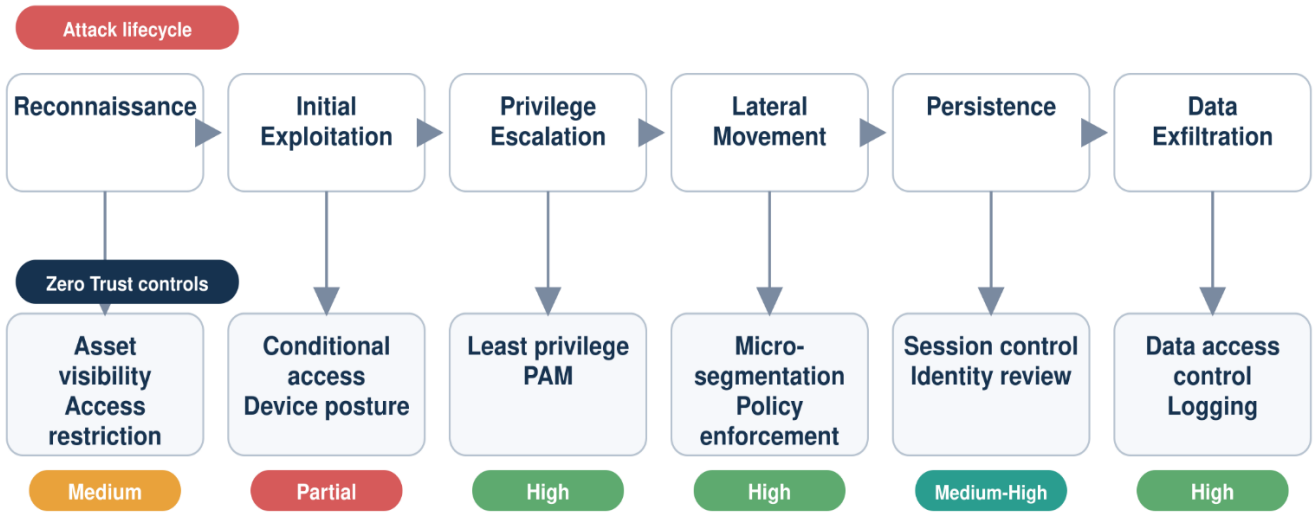
Table 5. Comparative mapping of zero-day attack stages and Zero Trust controls.

Zero-day attack stage	Attacker objective	Relevant Zero Trust controls	Defensive value
Reconnaissance	Identify exposed services and weak targets	Asset visibility, service hiding, and access restrictions	Medium
Initial exploitation	Exploit an unknown vulnerability	Device posture, conditional access, application access control	Partial
Privilege escalation	Increase permissions	Least privilege, privileged access management, and continuous authorization	High
Lateral movement	Move across internal systems	Micro-segmentation, policy enforcement, and network monitoring	High
Persistence	Maintain long-term access	Behavioral monitoring, session control, identity review	Medium to high

Data exfiltration	Extract sensitive information	Data access control, segmentation, logging, anomaly detection	High

Common steps of zero-day attacks are mapped to pertinent Zero Trust controls in Figure 4. It demonstrates how Zero Trust has a minimal direct impact on the existence of an unknown vulnerability, a partial impact during initial exploitation, and a stronger defensive value during persistence, lateral movement, privilege escalation, and data exfiltration. The mapping backs up the review's main comparative conclusion: Zero Trust can lessen the reachability, mobility, persistence, and effect of zero-day attacks but does not completely eradicate them.

Figure 4. Zero-Day Attack Lifecycle Mapped to Zero Trust Controls.



4.5 Summary of Key Findings

The literature reviewed corroborates five main findings. First, it is hard to detect zero-day attacks as they are based on flaws that are not known to the security world (or not observed by the malicious party) and can be different from the known signatures and/or labeled datasets. Anomaly detection, transfer learning, and zero-shot learning are important yet incomplete research directions as discussed [1], [2], and [13]

On the other hand, machine learning and deep learning techniques can enhance the ability to detect suspicious or new types of hacking, but their effectiveness relies on the quality of the datasets, the representation of the features, a realistic assessment, and the ability to withstand new attacks. A high accuracy on benchmark datasets does not mean that it is zero-day resistant to real-world attacks [11], [12], and [17-21].

Thirdly, the ROI of Zero Trust Architecture is greater after an attack than it is during an attack. It is particularly beneficial for restricting users' lateral travel, minimizing any unnecessary privileges, and making it easier to monitor it across users, devices, applications, and network segments [3], [22], and [24].

Lastly, Zero Trust is not a substitute for vulnerability management, patching, secure software development, or intrusion detection. Instead, it adds to these practices by mitigating implicit trust and the impact on operations if successful exploitation is to occur [4], [6], and [23].

Fifth, there is a limited integration between zero-day detection and Zero Trust enforcement systems. Adaptive Zero Trust architectures that adapt to novel attack behavior through anomaly detection, behavioral analysis, and risk scoring should be explored in the future [13], [22], and [29].

5 Discussion

5.1 Critical Interpretation of the Findings

The results show that zero-day attacks and Zero Trust Architecture solve different aspects of the cybersecurity issue. While Zero-day attacks bring uncertainty at vulnerability and behavior levels, Zero Trust brings uncertainty down at the identity, access, segmentation, and policy enforcement levels. So, the Zero Trust association with them is not opposition, but a layered association as a form of defensive relationship, during which Zero Trust minimizes the impact of a zero-day breach, yet it does not stop it [1], [3], and [6].

One of the major interpretations is that no single mechanism can be the basis of zero-day defense. Signature-based detection is not sufficient since zero-day attacks have no signature; machine learning-based detection also relies on the quality of the training data, realistic evaluation, and robustness to unseen behavior. Likewise, Zero Trust also demands to have correct policy configuration, reliable identity infrastructure, and continual monitoring [2], [11], and [22].

5.2 Strengths of Zero Trust Against Zero-Day Attacks

The most powerful times to leverage Zero Trust are after initial compromise. Typically, if a zero-day vulnerability is exploited, the attacker tries to upgrade privileges, steal credentials, move laterally, or gain access to sensitive information. The use of zero-trust controls like least privilege, micro-segmentation, and continuous authorization can help constrain these post-exploitation activities and decrease the blast radius [3], [22], and [24]

Another advantage is that the concept of network location trust evolves to that of context-aware access. The attacker in a traditional perimeter model can gain access to a lot of things when they compromise an endpoint inside the network. In Zero Trust environments, identities, devices, resources, and policies are continually assessed when granting access. Even if the first entry point is breached, unauthorized expansion is more difficult, if not impossible [5], [23], and [29].

Another benefit of Zero Trust is that it enhances visibility. Continuous monitoring, logging, and policy enforcement can produce signals that can be used to aid in anomaly detection and incident response. This is particularly crucial, as a zero-day attack could not be identified at the time of the exploit, but then suspicious post-exploitation activities might be captured via abnormal access patterns, unexpected device posture, or unusual east-west traffic[12], [23], and [31].

The point at which the initial compromise has happened is when Zero Trust is at its strongest. Upon successful exploitation of such a zero-day vulnerability, the attacker typically tries to elevate their access to systems, steal their credentials, move laterally, or attempt access to sensitive information. These post-exploitation activities can be curtailed by zero trust controls like least privilege, micro-segmentation, and continuous authorization, which can minimize the blast radius [3], [22], and [24].

Another advantage is that the concept of network location trust evolves to that of context-aware access. Traditional perimeter models have a problem with end-user compromise, giving the attacker 'jack the jackpot' access. In Zero Trust environments, identities, devices, resources, and policies are continually assessed when granting access. This is more difficult to carry out, even if an initial entry route is gained through authorization [5], [23], and [29].

Another benefit of Zero Trust is that it enhances visibility. Signals created from continuous monitoring, logging, and policy enforcement can be used to aid in anomaly detection and incident response. This is crucial because zero-day attacks can occur, but they might not be detected at the time of the exploit, but may be detected by abnormal access patterns, unusual device posture, or unexpected east-west traffic [12], [23], [31].

5.3 Limitations of Zero Trust Architecture

While there are a number of benefits to Zero Trust, it has its drawbacks. First, it doesn't eliminate any unknown vulnerabilities in software, firmware, cloud services, or applications. While Zero Trust can deny access to an authorization app if there is a zero-day vulnerability found in it, there is no guarantee that it will not be exploited [3] and [6]

Secondly, implementing Zero Trust is complicated. It needs to be based on good identity management, correct asset inventories, policy engines, monitoring systems, segmentation strategies, and governance within organizations.

However, if not properly deployed, Zero Trust can lead to operational issues, rather than security gains. It is particularly high in the organizations that have legacy systems, a lack of complete visibility, and poor Policy management [24], [26], and [28].

Thirdly, compromised identities and misconfigurations of policies can compromise Zero Trust. If risk-based monitoring and adaptive controls are not configured properly, malicious activities can still be allowed to take place on the system, even when using valid credentials and/or exploiting a trusted service account. Therefore, Zero Trust needs to be used in conjunction with behavioral analytics, privileged access management, and periodic policy validation[22] and [29].

Fourth, the capability of AI-based zero-day detection is also limited. Adversarial manipulation, data poisoning, concept drift, and evasion are all potential weaknesses of machine learning models. This implies that it is important to carefully include AI in the Zero Trust decision-making process as faulty or controlled detection signals can result in false trust decisions and/or false alarms [30], [31].

5.4 Research Gaps

The first big research gap is the absence of a common set of metrics to measure the effectiveness of Zero Trust when it comes to zero-day attacks. There are existing datasets like CICIDS2017 (Cyber Security for Industrial Internet of Things), UNSW-NB15, ToN-IoT, and Edge-IIoTset that can be used for the evaluation of an IDS, but none of them measure the impact of Zero Trust controls over lateral movement, privilege escalation, or data exfiltration after a Zero-Day attack [17-21].

The second gap is the real-world limitations of the product. A large number of Zero Trust studies have been conducted at a maturity stage, without considering realistic attack chains, and a myriad of zero-day detection models are tested in controlled environments. Real adversarial evaluation of actual enterprise deployment data and technical simulation should be combined in future work to determine actual defensive value[2], [13], and [16].

The third gap is low levels of linkages between detection and enforcement. Zero-day detection models are capable of generating alerts, and Zero Trust systems make access decisions. But, there is not much research that addresses the dynamics of access policies based on anomaly scores or behavioral signals in real-time, or how the model confidence should change as a function of access. The role of adaptive and risk-aware enforcement is crucial to the future of Zero Trust [13],[22], and [29].

The fourth gap is in terms of explainability. When AI-based detection is utilized to drive access decisions, security analysts must have explanations to interpret why a user, device, or session was marked as risky. High-stakes Zero Trust enforcement might not be a good idea with black-box models, unless they can provide explanations, audits, and validation of their output [31].

5.5 Future Research Directions

Future work needs to be directed towards adaptive zero-trust architectures based on continuous verification and anomaly detection using Artificial Intelligence. Future systems should dynamically modify the level of trust based on identity behavior, the posture of devices, context of the network, and threat intelligence, rather than relying on static policies. This can help Zero Trust to adapt to new and evolving attacks [22], [29], and [31].

Another potential positive direction to go with Moving Target Defense is to combine it with Zero Trust. Moving Target Defense is a technique that alters system configurations, network paths, or attack surfaces to allow a reduction in the attacker's ability to use static reconnaissance. It can be used to add to the uncertainty of attackers and limit access with Zero Trust and potentially improve resilience [32] and [33].

Realistic evaluation frameworks, too, should be researched in the future. Containment time, reduction in lateral movement, policy response latency, false positive cost of operation, and reduction in impact on the post-compromise environment should also be reported along with the accuracy and precision and/or recall of the

classifications. The most accurate indicators of the benefit of Zero Trust to zero-day attacks would be: Finally, it is necessary to create a future explainable and human loop security model. When automated systems limit analysts' access and activate containment, certain trust is required in the Zero Day defense. Explainable intrusion detection and transparent policy reasoning can help boost the analyst's confidence, decrease operational resistance, and enhance the ability to make accountable Zero Trust decisions [31].

Figure 5. It's an interpretative dashboard that overlays the critical findings from the review on the vulnerability, access, exploitation, post-exploitation, and resilience layers. It identifies the gaps, partial, and strong points of Zero Trust in the presence of zero-day threats. It's supposed to keep the engagement from going too far: Zero Trust is supposed to be a containment and resilience model, and zero-day discovery means detection, threat intelligence, secure development, patch governance, and adaptive monitoring.

Figure 5. Critical relationship between zero-day attacks and Zero Trust.

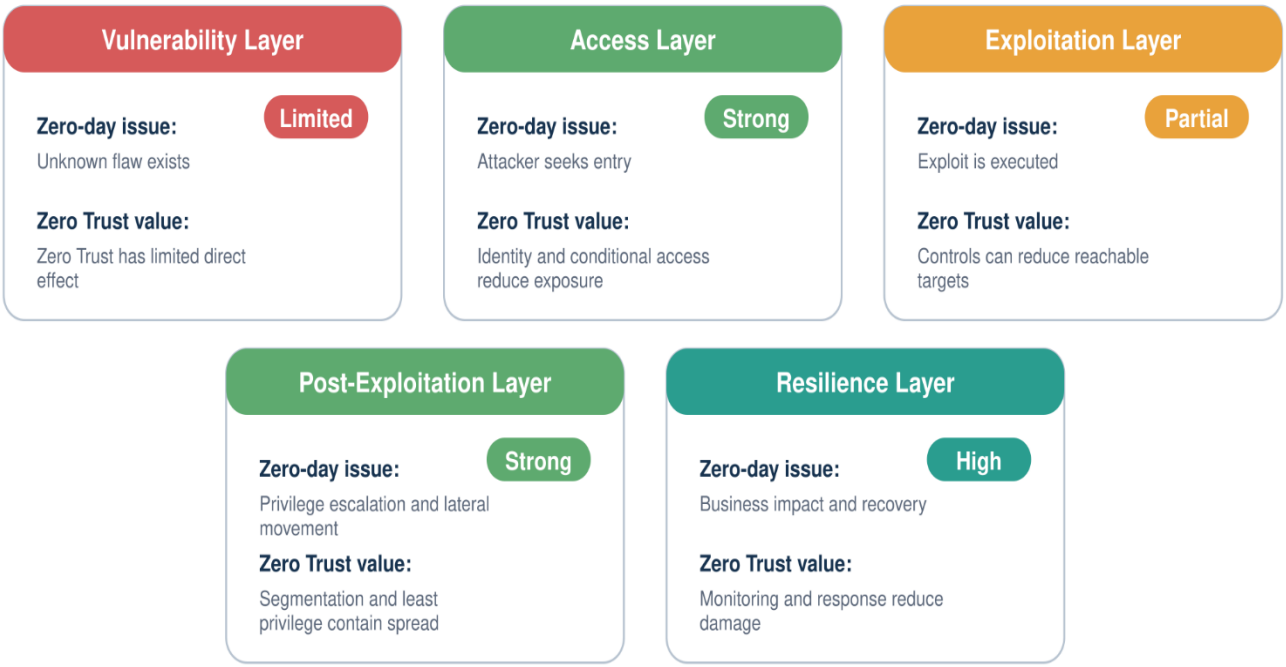


Table 6. Layer-based critical interpretation of Zero Trust value against zero-day threats.

Layer	Zero-day problem	Zero Trust contribution
Vulnerability layer	An unknown flaw exists	Limited direct effect
Access layer	Attacker seeks entry	Strong identity and access control
Exploitation layer	An unknown exploit is executed	Partial protection
Post-exploitation layer	Privilege escalation and lateral movement	Strong containment value
Resilience layer	Business impact and recovery	High value through monitoring and segmentation

The crucial connection between zero-day attack issues and Zero Trust's defensive contribution across five cybersecurity tiers is summarized in Table 6. Because Zero Trust does not eliminate unknown problems, it demonstrates that it has limited direct influence at the vulnerability layer. However, identity control, least privilege, segmentation, monitoring, and response mechanisms can lessen attacker movement and operational damage at the access,

post-exploitation, and resilience layers, when their efensive value rises.

REFERENCES

[1] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "Zero-day attack detection: A systematic literature review," Artificial Intelligence Review, vol. 56, pp. 10733–10811, 2023, doi: 10.1007/s10462-023-10437-z.

[2] Y. Guo, "A review of machine learning-based zero-day attack detection: Challenges and future directions," Computer Communications, vol. 198, pp. 175–185, 2023, doi: 10.1016/j.comcom.2022.11.001.

[3] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, NIST Special Publication 800-207, 2020, doi: 10.6028/NIST.SP.800-207.

[4] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on Zero Trust Architecture: Challenges and future trends," Wireless Communications and Mobile Computing, vol. 2022, Art. no. 6476274, 2022, doi: 10.1155/2022/6476274.

[5] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and application of Zero Trust security: A brief survey," Entropy, vol. 25, no. 12, Art. no. 1595, 2023, doi: 10.3390/e25121595.

[6] E. B. Fernández and A. Brazhuk, "A critical analysis of Zero Trust Architecture," Computer Standards & Interfaces, vol. 89, Art. no. 103832, 2024, doi: 10.1016/j.csi.2024.103832.

[7] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," BMJ, vol. 372, Art. no. n71, 2021, doi: 10.1136/bmj.n71.

[8] M. J. Page et al., "PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews," BMJ, vol. 372, Art. no. n160, 2021, doi: 10.1136/bmj.n160.

[9] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.

[10] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," Cybersecurity, vol. 2, Art. no. 20, 2019, doi: 10.1186/s42400-019-0038-7.

[11] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," Applied Sciences, vol. 9, no. 20, Art. no. 4396, 2019, doi: 10.3390/app9204396.

[12] H. Hindy, R. Atkinson, C. Tachtatzis, J.-N. Colin, E. Bayne, and X. Bellekens, "Utilising deep learning techniques for effective zero-day attack detection," Electronics, vol. 9, no. 10, Art. no. 1684, 2020, doi: 10.3390/electronics9101684.

[13] M. Sarhan, S. Layeghy, M. Gallagher, and M. Portmann, "From zero-shot machine learning to zero-day attack detection," International Journal of Information Security, vol. 22, pp. 947–959, 2023, doi: 10.1007/s10207-023-00676-0.

[14] J.-Y. Kim, S.-J. Bu, and S.-B. Cho, "Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders," Information Sciences, vols. 460–461, pp. 83–102, 2018, doi: 10.1016/j.ins.2018.04.092.

[15] N. Sameera and M. Shashi, "Deep transductive transfer learning framework for zero-day attack detection," ICT Express, vol. 6, no. 4, pp. 361–367, 2020, doi: 10.1016/j.icte.2020.03.003.

[16] U. Zahoora, M. Rajarajan, Z. Pan, and A. Khan, "Zero-day ransomware attack detection using deep contractive autoencoder and voting-based ensemble classifier," Applied Intelligence, vol. 52, pp. 13941–13960, 2022, doi: 10.1007/s10489-022-03244-6.

[17] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. 4th International Conference on Information Systems Security

and Privacy, 2018, pp. 108–116, doi: 10.5220/0006639801080116.

[18] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in Proc. 2015 Military Communications and Information Systems Conference, 2015, doi: 10.1109/MilCIS.2015.7348942.

[19] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," Information Security Journal: A Global Perspective, vol. 25, no. 1–3, pp. 18–31, 2016, doi: 10.1080/19393555.2015.1125974.

[20] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," IEEE Access, vol. 8, pp. 165130–165150, 2020, doi: 10.1109/ACCESS.2020.3022862.

[21] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," IEEE Access, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.

[22] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A comprehensive survey," IEEE Access, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.

[23] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," Computers & Security, vol. 110, Art. no. 102436, 2021, doi: 10.1016/j.cose.2021.102436.

[24] S. Teerakanok, T. Uehara, and A. Inomata, "Migrating to Zero Trust Architecture: Reviews and challenges," Security and Communication Networks, vol. 2021, Art. no. 9947347, 2021, doi: 10.1155/2021/9947347.

[25] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero Trust Architecture for 6G security," IEEE Network, vol. 38, no. 4, pp. 224–232, 2024, doi: 10.1109/MNET.2023.3326356.

[26] P. Phiayura and S. Teerakanok, "A comprehensive framework for migrating to Zero Trust Architecture," IEEE Access, vol. 11, pp. 19487–19511, 2023, doi: 10.1109/ACCESS.2023.3248622.

[27] D. Tyler and T. Viana, "Trust no one? A framework for assisting healthcare organisations in transitioning to a Zero-Trust network architecture," Applied Sciences, vol. 11, no. 16, Art. no. 7499, 2021, doi: 10.3390/app11167499.

[28] Z. Adahman, A. W. Malik, and Z. Anwar, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security," Computers & Security, vol. 122, Art. no. 102911, 2022, doi: 10.1016/j.cose.2022.102911.

[29] W. Yeoh, M. Liu, M. Shore, and F. Jiang, "Zero trust cybersecurity: Critical success factors and a maturity assessment framework," Computers & Security, vol. 133, Art. no. 103412, 2023, doi: 10.1016/j.cose.2023.103412.

[30] B. Xi, "Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges," WIREs Computational Statistics, vol. 12, no. 5, Art. no. e1511, 2020, doi: 10.1002/wics. 1511.

[31] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, "Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities," IEEE Access, vol. 10, pp. 112392–112415, 2022, doi: 10.1109/ACCESS.2022.3216617.

[32] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A survey of moving target defenses for network security," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1909–1941, 2020, doi: 10.1109/COMST.2020.2982955.

[33] J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim,

H. Lim, and F. F. Nelson, “Toward proactive, adaptive defense: A survey on moving target defense,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 709–745, 2020, doi: 10.1109/COMST.2019.2963791.

[34] M. Souppaya, K. Scarfone, and D. Dodson, “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for mitigating the risk of software vulnerabilities,” National Institute of Standards and Technology, NIST Special Publication 800-218, 2022, doi: 10.6028/NIST.SP.800-218.

[35] M. Souppaya and K. Scarfone, “Guide to enterprise patch management planning: Preventive maintenance for technology,” National Institute of Standards and Technology, NIST Special Publication 800-40 Revision 4, 2022, doi: 10.6028/NIST.SP.800-40r4.

[36] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST Cybersecurity White Paper 29, 2024, doi: 10.6028/NIST.CSWP.29.

Hussein Ali Ismael: is currently a Ph.D. student in Computer Science, having started his doctoral studies in 2024. He received his B.Sc. degree from Al-Yarmouk University College in 2015, and his M.Sc. degree in Computer Science from the College of Science, University of Diyala, Iraq in 2020. His research interests focus on advanced topics within computer science and information technology. He can be contacted at
E-mail: al-shaibani@uodiyala.edu.iq .