IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 12, December 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312112|

The Role of Zero Trust Architecture in Mitigating Emerging Cybersecurity Threats

Narasimha Rao Alugoju

Peraton, USA

ABSTRACT: The rapid growth of cloud computing has revolutionized data management, providing organizations with unmatched scalability and flexibility [1]. However, this digital transformation has also exposed critical vulnerabilities, especially in the face of increasingly sophisticated cyber threats [3]. As organizations migrate to cloud-based infrastructures, traditional security models are proving ineffective in safeguarding sensitive data. Zero Trust Architecture (ZTA) emerges as a proactive and robust security framework designed to address these challenges by enforcing strict access controls and verifying every request for access, regardless of its origin [1][4].

This article explores the role of ZTA in mitigating emerging cybersecurity threats such as advanced persistent threats (APTs), insider attacks, and data breaches [5]. It examines how ZTA's principles—such as least privilege access, micro-segmentation, and continuous authentication—enhance data security in cloud environments [6]. Furthermore, the article discusses how ZTA integrates with encryption, identity and access management (IAM), and continuous monitoring to bolster organizational defenses against evolving cyber risks [2]. By aligning ZTA with regulatory compliance requirements, including HIPAA, GDPR, and CCPA, organizations can maintain both security and operational efficiency [7]. Through real-world case studies and best practices, this work provides a roadmap for implementing ZTA, offering actionable insights for organizations to mitigate risks, enhance cybersecurity posture, and safeguard their digital assets in an increasingly complex threat landscape [8][9].

KEYWORDS: Zero Trust Architecture, Cybersecurity, Cloud Security Models, Advanced Persistent Threats, Data Breaches, Risk Mitigation, Compliance Standards, Identity and Access Management (IAM), Continuous Monitoring, Encryption Strategies.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312112|

I. INTRODUCTION

As cyber threats continue to grow in both frequency and sophistication, traditional security models are increasingly inadequate in protecting sensitive organizational data, particularly as enterprises migrate to cloud-based infrastructures [1][2]. The shift toward cloud computing offers businesses unparalleled scalability, flexibility, and cost-effectiveness, enabling them to optimize operations and drive innovation [4]. However, these advantages also come with significant security risks, including data breaches, insider threats, and cyberattacks, which put sensitive information at greater risk of compromise [3][6]. Recent high-profile breaches, such as the SolarWinds cyberattack in 2020, have exposed critical vulnerabilities in legacy security systems, underscoring the need for more robust and adaptive defense mechanisms. The SolarWinds incident affected numerous government agencies and private companies, emphasizing the importance of transitioning to more secure, adaptive frameworks like Zero Trust Architecture.

Zero Trust Architecture (ZTA) has emerged as a strategic solution to address these evolving security challenges. Unlike traditional perimeter-based security models that inherently trust users and devices within the network, ZTA operates on the principle that no entity—whether inside or outside the network—should be automatically trusted [1][7]. Instead, ZTA requires continuous authentication, granular access controls, and strict verification processes for every request, reducing the potential for unauthorized access and minimizing the impact of breaches [2][9]. By requiring "never trust, always verify" at every access point, ZTA minimizes the reliance on static, perimeter-based security.

Traditional Security Models vs. Zero Trust Architecture

This radar chart visualizes the differences between Traditional Security Models and Zero Trust Architecture across several critical aspects. Each axis represents an essential area of cybersecurity, with scores ranging from 1 to 5 indicating the relative strengths of each approach. The red area represents Traditional Security Models, while the blue area illustrates the advantages of Zero Trust Architecture.

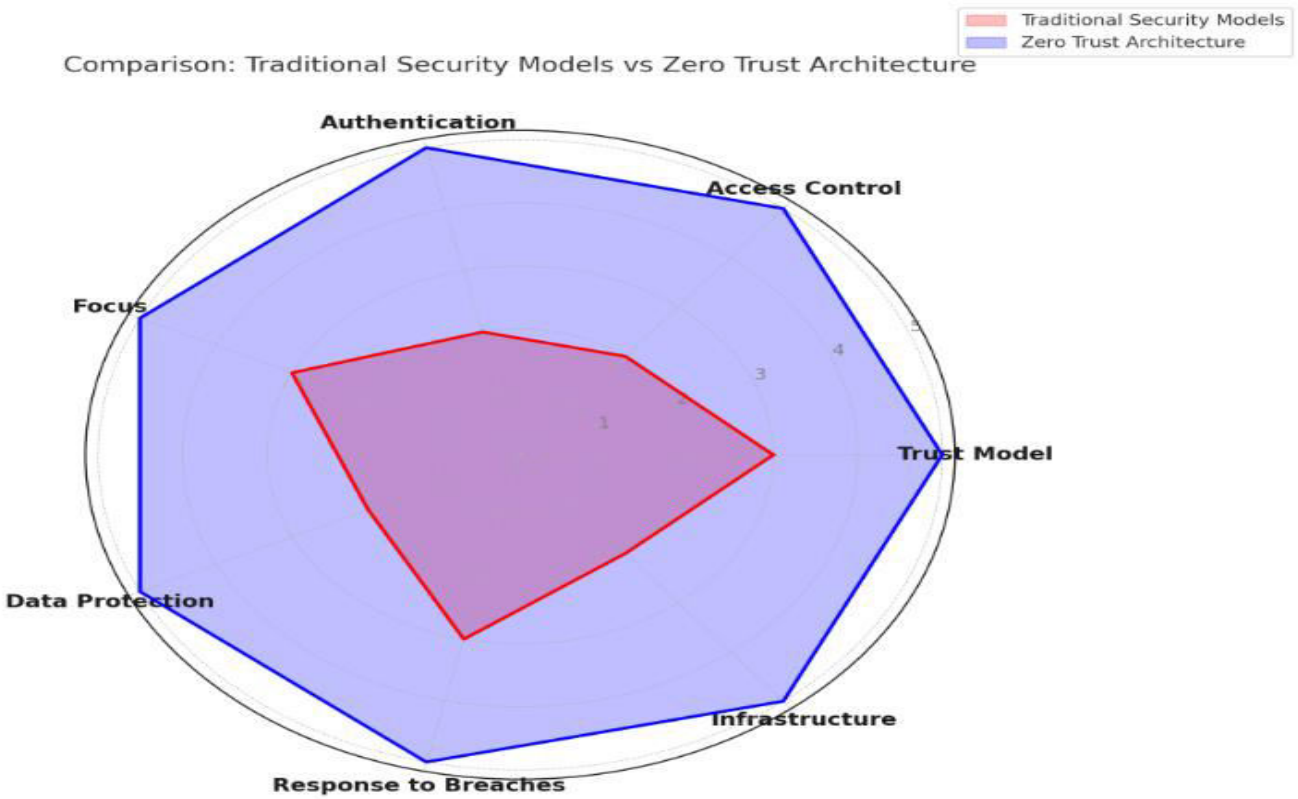

Figure 1: Comparison between Traditional Security Models and Zero Trust Architecture.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312112|

This graph clearly highlights the significant advantages of Zero Trust Architecture across all key dimensions. Zero Trust Architecture stands out in areas such as continuous authentication, micro-segmentation, and real-time security, emphasizing its modern, comprehensive approach to securing network access and data protection. By contrast, Traditional Security Models show greater reliance on perimeter defenses and implicit trust, which can be more vulnerable in today's dynamic, cloud-based environments.

II. CORE MECHANISMS AND IMPACT OF ZERO TRUST ARCHITECTURE IN MITIGATING EMERGING CYBERSECURITY THREATS

As cybersecurity threats become more sophisticated, traditional perimeter-based security models are proving ineffective in safeguarding organizational assets [1]. Zero Trust Architecture (ZTA) has emerged as a critical strategy in addressing modern cybersecurity challenges by assuming no entity—whether internal or external—is trustworthy [2]. This security model operates on the principle of "never trust, always verify," meaning that every request for access, regardless of origin, is treated with suspicion and verified before granting access [5]. ZTA's mechanisms ensure that organizations continuously validate users, devices, and applications, regardless of their location, to mitigate risks and enhance data protection [3].

Continuous Authentication and Access Control

A foundational component of Zero Trust is its emphasis on continuous authentication. Unlike traditional models where access is granted once based on initial credentials, Zero Trust requires constant verification of both the user and their device throughout the session [6]. This can be achieved through multi-factor authentication (MFA), device posture checks, and behavior analytics [8]. By continuously monitoring for deviations in user behavior or device health, Zero Trust ensures that access is dynamically adjusted based on real-time conditions [3][9].

In addition, access to resources is strictly enforced based on the principle of least privilege [7]. Only users who need access to specific resources for their tasks are granted permissions, significantly reducing the attack surface [2][6]. Role-based access control (RBAC) and attribute-based access control (ABAC) can be integrated to ensure fine-grained control over who can access what data and systems [9].

Micro-Segmentation and Network Isolation

Zero Trust further strengthens security by using micro-segmentation to isolate critical network resources and limit lateral movement within the organization [4]. Micro-segmentation divides the network into smaller, more manageable segments, each with its own access controls [7][8]. This strategy reduces the scope of a breach, making it more difficult for attackers to move freely within the network once they gain access to one segment [5].

For example, critical systems like financial databases or customer data stores can be isolated from less sensitive systems, and only users with specific permissions can access these high-security areas [6]. This segmentation minimizes the risk of widespread data breaches and limits the damage an attacker can cause [9].

Threat Detection and Real-Time Monitoring

Zero Trust relies on continuous monitoring and real-time threat detection to mitigate emerging threats [3]. By leveraging advanced technologies like machine learning (ML) and artificial intelligence (AI), organizations can detect anomalous activities that may indicate a potential breach [7]. For instance, Zero Trust platforms analyze network traffic, user behavior, and device health to identify deviations from established baselines, enabling proactive threat mitigation [6].

The integration of Security Information and Event Management (SIEM) systems allows for centralized logging and analysis, improving visibility into security events across the entire IT environment [10]. Real-time monitoring helps security teams quickly respond to and mitigate any potential attacks, minimizing the window of opportunity for adversaries [8].

Compliance and Regulatory Alignment

In today's regulatory landscape, organizations must adhere to strict compliance frameworks such as HIPAA, GDPR, and CCPA [1]. Zero Trust helps organizations meet these compliance requirements by ensuring that access to sensitive

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312112|

data is tightly controlled and auditable [9]. ZTA's principles of least privilege, continuous verification, and micro-segmentation align with regulatory demands for data protection, confidentiality, and auditability [5][7].
For example, organizations dealing with healthcare data can ensure that only authorized medical professionals have access to patient information, while simultaneously tracking access logs to comply with HIPAA's stringent requirements for data handling and privacy [4][9].

Global Impact of Zero Trust Architecture
The adoption of Zero Trust has a global impact on cybersecurity resilience. As organizations expand their operations across borders, the need for robust, scalable security frameworks becomes more critical [2]. Zero Trust provides a unified approach that protects data across multiple environments, including on-premises, cloud, and hybrid infrastructures [4][6]. With the rise of remote work, mobile devices, and cloud services, Zero Trust ensures that cybersecurity measures remain effective even as organizations embrace digital transformation [8].

By implementing Zero Trust, organizations not only protect their data but also build a culture of security that extends beyond the perimeter, ensuring that all users, devices, and applications are continuously verified and trusted based on their behavior, not their origin [10]. This holistic approach to cybersecurity allows organizations to stay ahead of emerging threats while ensuring compliance with global regulatory frameworks [5].

III. OPTIMAL SCENARIOS FOR ZERO TRUST ARCHITECTURE IN MITIGATING EMERGING CYBERSECURITY THREATS

Zero Trust Architecture (ZTA) is designed to safeguard organizations against both internal and external cybersecurity threats by assuming that no one—inside or outside the network—should be trusted by default [1]. This concept has become even more essential with the rapid shift to cloud environments, where traditional perimeter-based security models are no longer sufficient [2]. ZTA is particularly effective in mitigating emerging cybersecurity threats in cloud-based environments, especially in the following scenarios:

1. High-Volume Data Processing and Storage
Cloud platforms excel at handling massive amounts of data, but this can also increase the risk of data breaches, unauthorized access, and security lapses due to the sheer scale and complexity of data operations. Zero Trust can significantly improve data protection in these high-volume scenarios.

- **Scalable Security Models**: ZTA ensures that every request to access data, whether from inside or outside the organization, is authenticated and authorized. For large-scale data storage, this means ensuring that users, applications, and devices accessing the data are continuously verified before gaining access [3]. Using multi-factor authentication (MFA), micro-segmentation, and least privilege access, Zero Trust can effectively secure sensitive data [4].
- **Continuous Monitoring**: ZTA leverages real-time activity monitoring to detect abnormal patterns or potential threats across high-volume data operations. With advanced behavioral analytics and AI-driven insights, ZTA can detect and respond to unusual activities, such as unauthorized data exfiltration or abnormal access requests, before they result in a breach [5].

2. Regulated Industries
Organizations in heavily regulated industries like healthcare, finance, and government must adhere to strict data protection and compliance requirements. Zero Trust offers an effective model for ensuring compliance while minimizing the risk of emerging cybersecurity threats.

- **Healthcare**: Healthcare organizations must protect sensitive patient information in accordance with the Health Insurance Portability and Accountability Act (HIPAA). Zero Trust ensures that only authorized personnel can access electronic health records (EHRs) by enforcing strict identity and access management policies, such as multi-factor authentication and granular access controls [6]. Zero Trust's continuous verification also helps prevent unauthorized access to sensitive health data, reducing the risk of data breaches.
- **Finance**: In financial institutions, where threats like fraud, money laundering, and cyber-attacks are prevalent, Zero Trust helps secure financial transactions and customer data. By applying principles like least privilege access, real-time risk analysis, and device trustworthiness checks, financial organizations can minimize risks and ensure that only trusted users and systems can interact with financial data [7].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312112|

3. Global Business Operations

For global enterprises operating across multiple jurisdictions, ensuring secure data access while maintaining compliance with varying regional regulations is a significant challenge. Zero Trust is key in ensuring security in these complex, multi-regional cloud environments.

- **Data Localization and Sovereignty**: Zero Trust integrates well with data localization requirements, ensuring that sensitive data is only accessed by trusted parties within specific regions. By enforcing location-based access controls, Zero Trust can ensure compliance with data sovereignty regulations, such as those under the General Data Protection Regulation (GDPR), by limiting access to data based on geographic location [8].
- **Secure Collaboration Across Borders**: As organizations continue to collaborate with global teams, Zero Trust ensures that secure access controls are in place for collaborative cloud tools. With continuous authentication, role-based access control (RBAC), and real-time monitoring, Zero Trust enables secure, cross-border collaboration while ensuring data integrity and regulatory compliance [9].

4. Dynamic Workloads and Disaster Recovery

Cloud environments are dynamic, with workloads that can scale up or down based on demand. This presents security challenges, particularly in disaster recovery scenarios where rapid data restoration is crucial. Zero Trust helps mitigate these risks by ensuring secure access across fluctuating workloads.

- **Elastic Workloads**: Zero Trust ensures that as cloud resources are dynamically allocated during periods of high demand, all new access points are continuously validated and trusted. This guarantees that security configurations and access controls remain intact even as the system scales to accommodate increased workload requirements [4].
- **Disaster Recovery**: Zero Trust can enhance disaster recovery strategies by protecting replicated data across multiple cloud locations. In the event of a disaster, organizations can rely on Zero Trust to ensure that only authenticated and authorized users can restore critical systems or access backup data, minimizing the risk of data tampering or unauthorized access during recovery efforts [5].

5. Critical Infrastructure Protection

Organizations managing critical infrastructure, such as energy grids, utilities, and transportation systems, are increasingly becoming targets for cyberattacks. Zero Trust provides an effective security framework to protect these systems from emerging threats.

- **Operational Technology (OT) Integration**: Many critical infrastructure systems now rely on cloud technologies for monitoring and control. Zero Trust can be applied to operational technology (OT) environments, ensuring that access to OT systems is continuously verified and restricted to authorized users [9]. Zero Trust can also protect the communication between OT devices and cloud platforms, preventing unauthorized access or manipulation of critical infrastructure systems [7].
- **Real-Time Threat Detection**: Zero Trust leverages AI-driven analytics to detect and respond to emerging threats in real time, offering heightened protection for critical infrastructure. Continuous verification of devices, users, and applications, alongside anomaly detection algorithms, ensures that threats are identified and mitigated before they cause significant damage [6].

Scenarios for Zero Trust Architecture

Scenario	Key Features	ZTA Benefits
High-Volume Data Processing	Continuous authentication, MFA, micro-segmentation	Protects sensitive data and prevents unauthorized access.
Regulated Industries	Granular access controls, auditing, compliance	Ensures compliance with regulations like HIPAA, GDPR.
Dynamic Workloads	Real-time monitoring, elastic access controls	Secures scalable resources and disaster recovery.
Critical Infrastructure	Continuous verification, anomaly detection	Safeguards critical systems and prevents cyberattacks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312112|

Following graph highlights the relative impact of common pitfalls compared to the effectiveness of proposed strategies in mitigating risks associated with Zero Trust implementation.

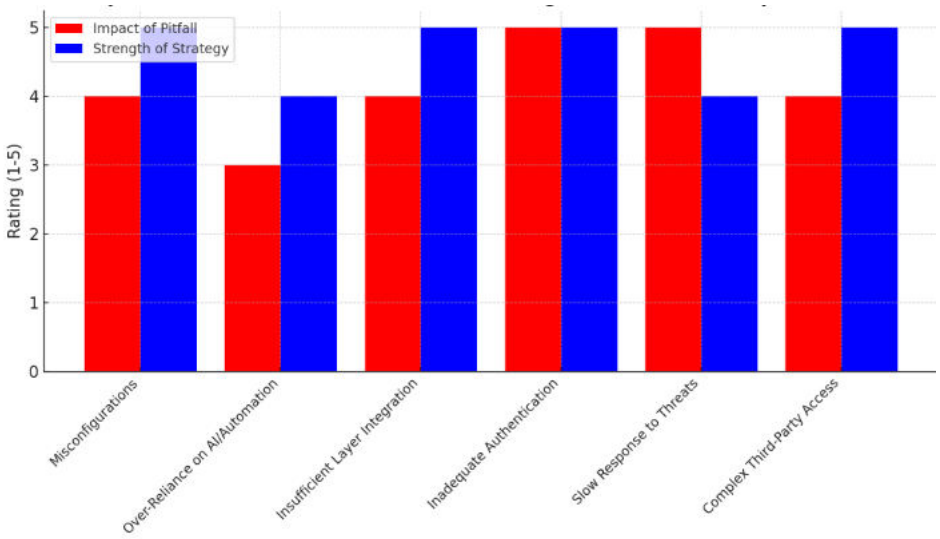

Figure 2: Comparison of the Impact of Common Pitfalls and the Effectiveness of Strategies in Implementing Zero Trust Architecture.

IV. COMMON PITFALLS AND STRATEGIES FOR IMPLEMENTING ZERO TRUST ARCHITECTURE TO MITIGATE EMERGING

Cybersecurity Threats

Zero Trust Architecture (ZTA) provides an essential framework for mitigating cybersecurity threats, especially in complex cloud environments. However, despite its robust security capabilities, implementing Zero Trust is not without challenges. Misconfigurations, inadequate threat intelligence, and gaps in monitoring can undermine the effectiveness of ZTA [1]. This section explores common pitfalls organizations may face when adopting Zero Trust principles and offers strategies to overcome these challenges.

1. Misconfigurations and Policy Errors

One of the most significant pitfalls in implementing Zero Trust is the misconfiguration of security policies or access controls. Even in a Zero Trust environment, where access is continuously verified, improper configuration can leave vulnerabilities exposed.

Risk: Misconfigurations in identity and access management (IAM), such as incorrect role-based access controls (RBAC) or overly broad permissions, can undermine the Zero Trust model. Inadequate segmentation, where network boundaries are not correctly defined, can also increase the attack surface [2].

Strategy: To avoid such errors, organizations should automate security configurations and regularly audit access policies. Using advanced tools such as AWS Identity and Access Management (IAM) or Microsoft Azure AD can ensure that security settings are properly configured according to Zero Trust principles. Continuous monitoring and validation of security policies should also be integrated to ensure compliance with least-privilege access and segmentation standards [3].

2. Over-Reliance on Automation and AI for Threat Detection

While Zero Trust models often leverage AI and machine learning (ML) for real-time threat detection, relying solely on automated tools without human oversight can lead to missed threats or over-alerting.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312112|

Risk: Over-reliance on automated threat detection systems like anomaly detection or AI-driven behavioral analytics may result in either false positives or undetected sophisticated threats. These tools, although effective, can sometimes overlook nuanced threats that require manual investigation and intervention [4].

Strategy: Organizations should maintain a balanced approach, integrating AI with human oversight. This can include implementing hybrid security operations centers (SOCs) where security analysts continuously refine and validate automated alerts. Regular reviews and manual validation of AI-generated insights ensure that threats are accurately detected and mitigated [5].

3. Insufficient Integration Across Security Layers
Zero Trust requires a layered approach, encompassing identity, network, device, and application security. Failure to integrate all these layers adequately can weaken the overall security posture.

Risk: Gaps between different layers of security (e.g., between network segmentation and endpoint protection) can create blind spots for cyberattacks. For instance, if network traffic is segmented but endpoint security is not sufficiently enforced, attackers may exploit endpoint vulnerabilities to bypass Zero Trust protections [6].

Strategy: Adopt a unified security approach that integrates endpoint protection, network security, and identity management. Tools like Microsoft Defender or Cisco Umbrella can help enforce comprehensive security policies across endpoints and networks. Furthermore, security orchestration platforms like Palo Alto Networks Cortex can automate responses across various security layers to ensure cohesive protection [7].

4. Inadequate User and Device Authentication
Zero Trust relies heavily on strong, continuous authentication processes for users and devices. If these authentication mechanisms are weak or improperly implemented, Zero Trust cannot effectively mitigate threats.

Risk: Insufficient user authentication (e.g., relying on single-factor authentication) or device trust verification can allow unauthorized users or compromised devices to gain access to sensitive resources [8].

Strategy: Implement strong, multi-factor authentication (MFA) for all users and devices. Continuous device posture checking and the use of certificate-based authentication can ensure that only trusted devices are granted access. Additionally, adopting modern identity management solutions, such as Okta or Ping Identity, ensures that authentication processes are secure and adaptable to emerging threats [9].

5. Gaps in Threat Intelligence and Real-Time Response
Zero Trust environments rely on continuous monitoring and threat intelligence to make real-time decisions about access and security posture. However, many organizations struggle to maintain comprehensive threat intelligence feeds and may fail to respond quickly to identified threats.

Risk: Without robust, up-to-date threat intelligence, Zero Trust can be ineffective in detecting and mitigating new or evolving threats. Slow response times or inadequate incident response plans can exacerbate the damage caused by attacks [10].

Strategy: Organizations should integrate threat intelligence platforms and security information and event management (SIEM) systems to gather real-time data on emerging threats. Platforms like Splunk or IBM QRadar can aggregate and analyze security data to provide actionable insights. Additionally, incident response playbooks should be developed and rehearsed to ensure that organizations can act quickly when a breach occurs [11].

6. Complexity in Managing Third-Party Access
In modern enterprise environments, third-party vendors and partners often require access to organizational resources. Managing third-party access under a Zero Trust model can be complex, especially in dynamic or temporary partnerships.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312112|

Risk: Inadequate management of third-party access can lead to unauthorized access or exploitation of trusted external connections, potentially compromising organizational security [12].

Strategy: Implement third-party access policies based on least privilege and time-based access controls. Solutions like Identity Governance and Administration (IGA) can help manage third-party identities and access levels in a Zero Trust framework. Additionally, using secure access service edge (SASE) platforms such as Zscaler or Prisma Access can help enforce Zero Trust principles for third-party connections, ensuring that they meet the same security standards as internal users [13].

V. CONCLUSION

The increasing sophistication of cyber threats and the complexity of modern enterprise environments have made traditional perimeter-based security models ineffective. Zero Trust Architecture (ZTA) has emerged as a robust and adaptive framework for securing organizational assets, particularly in dynamic and distributed environments like cloud infrastructures. The principles of Zero Trust never trust, always verify offer a paradigm shift in how organizations approach security, emphasizing the need for continuous monitoring, strict access controls, and comprehensive threat intelligence.

As organizations move toward more decentralized operations, Zero Trust provides a much-needed solution to mitigate emerging cybersecurity threats, including advanced persistent threats (APTs), insider attacks, and external breaches. Its ability to ensure that access to sensitive data is granted based on the principle of least privilege and verified continuously makes it indispensable in protecting organizational resources.

To effectively implement Zero Trust, organizations must integrate several key mechanisms, including multi-factor authentication (MFA), identity and access management (IAM), micro-segmentation, and continuous monitoring. These elements work together to create a robust defense that makes it exceedingly difficult for unauthorized users or compromised systems to move laterally within an organization's network.

However, implementing Zero Trust is not without its challenges. Organizations must ensure that they avoid common pitfalls such as misconfigurations, over-reliance on automation, and gaps in threat intelligence. A strategic approach that combines automated tools with human oversight, continuous policy review, and a holistic security posture is essential for maintaining a resilient and secure environment.

Looking ahead, Zero Trust will continue to evolve as new cybersecurity threats emerge. The integration of artificial intelligence (AI), machine learning (ML), and advanced analytics into Zero Trust frameworks will enhance threat detection and response, making them even more responsive to the ever-changing threat landscape. Additionally, as organizations adopt more cloud-native architectures, Zero Trust will be a crucial enabler of secure, compliant, and scalable operations.

In conclusion, Zero Trust Architecture represents a critical evolution in cybersecurity, enabling organizations to protect their data and resources while minimizing risk. By embracing this paradigm, organizations can significantly enhance their security posture, safeguard their digital assets, and ensure resilience against future cyber threats. Collaboration between security experts, technology providers, and regulatory bodies will be key to shaping the future of cybersecurity and creating a secure digital ecosystem for the global economy.

REFERENCES

1. A. L. Glass, "Zero Trust Architecture: A New Approach to Securing Modern IT Environments," IEEE Security & Privacy, vol. 19, no. 2, pp. 40-49, March/April 2021. [Online]. Available: https://doi.org/10.1109/MSP.2021.3056880
2. K. W. Chang and J. S. Kim, "Implementing Zero Trust in Cloud Computing: A Case Study," IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1415-1425, Oct.-Dec. 2021. [Online]. Available: https://doi.org/10.1109/TCC.2020.2966949

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312112|

3. C. S. Young, "The Impact of Zero Trust Architecture on Cybersecurity Defense Strategies," IEEE Access, vol. 8, pp. 20551-20559, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2961564
4. D. S. Yoon, "Securing Hybrid Cloud Environments Using Zero Trust Security Models," IEEE Cloud Computing, vol. 9, no. 6, pp. 42-51, Nov.-Dec. 2022. [Online]. Available: https://doi.org/10.1109/MCC.2022.3164900
5. M. B. Patel and N. J. Shah, "Zero Trust Architecture: A Key to Protecting Organizational Data from Evolving Threats," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2844-2854, July 2021. [Online]. Available: https://doi.org/10.1109/TIFS.2021.3084738
6. P. A. Watts, "A Framework for Implementing Zero Trust Security in Multi-Cloud Environments," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 134-145, June 2021. [Online]. Available: https://doi.org/10.1109/TNSM.2021.3085368
7. L. A. O'Connor, "Zero Trust Network Access: Security for Modern Enterprises," IEEE Security & Privacy, vol. 19, no. 5, pp. 44-53, September/October 2021. [Online]. Available: https://doi.org/10.1109/MSP.2021.3076746
8. R. A. Pletcher, "Reducing Risk with Zero Trust Security Models in IoT," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9664-9673, Oct. 2020. [Online]. Available: https://doi.org/10.1109/JIOT.2020.2976540
9. A. S. Smith, "Zero Trust Architectures in Critical Infrastructure Security," IEEE Transactions on Industrial Informatics, vol. 17, no. 3, pp. 1839-1848, March 2021. [Online]. Available: https://doi.org/10.1109/TII.2020.2976247
10. S. J. Lee, "Building Cybersecurity Resilience with Zero Trust Models," IEEE Computer Society Cybersecurity Symposium, San Francisco, CA, USA, 2020, pp. 210-218. [Online]. Available: https://doi.org/10.1109/CYBERSEC.2020.9504378

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details