Journal of Information Systems Engineering and Management
2025, 10(32s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Zero Trust Cybersecurity with AI

Milankumar Rana
Department of Information Technology, University of the cumberlands, Williamsburg, KY 40769, USA.
ORC ID: 0009-0009-1623-0429

ARTICLE INFO

Received: 08 Jan 2025

Revised: 01 Mar 2025

Accepted: 09 Mar 2025

ABSTRACT

Zero Trust Architecture has become the prime asset of any organizations since the data breach and hacking has become normal these days. This paper studies and recommend the solutions for zero trust using Microsoft Copilot and AI driven assistant to improve the existing Identity and access control management and overall security operations. This also deep dive into zero trust mechanism and how it can be more effective for organizations and their own policies [10]. This article investigates how Copilot might help security experts with access control, automate security processes, and provide real-time insight. Examining Copilot's capabilities in line with the Zero Trust basic concept, "Never Trust, Always Verify," this paper Notwithstanding historical challenges to its general acceptability, we wish to demonstrate how artificial intelligence might simplify Zero Trust techniques of application [19].Important areas of research include how Copilot interacts with the current security features in Microsoft 365, how it can be used to improve explicit verification processes, how AI can be used to implement least privileged access, and how Copilot might help discover threats and react to them in the "assume breach" paradigm [10]. This study aims to provide firms with ideas on how to enhance their safety using AI-powered solutions such as Microsoft Copilot by analyzing real-life cases. Within Zero Trust, it zeroes attention on the User Pillar as well as the Automation and Orchestration Pillar. Microsoft's declared end goal (2023) is to use artificial intelligence to help security professionals in their quest of a strong Zero Trust Architecture. They will thus be ready to manage cyberthreats as they develop in an environment driven more by artificial intelligence [18].

Keywords: *Zero Trust Architecture; AI; Microsoft Copilot; Automation; AI Driven; Access Control; Automate Security; threats; orchestration.*

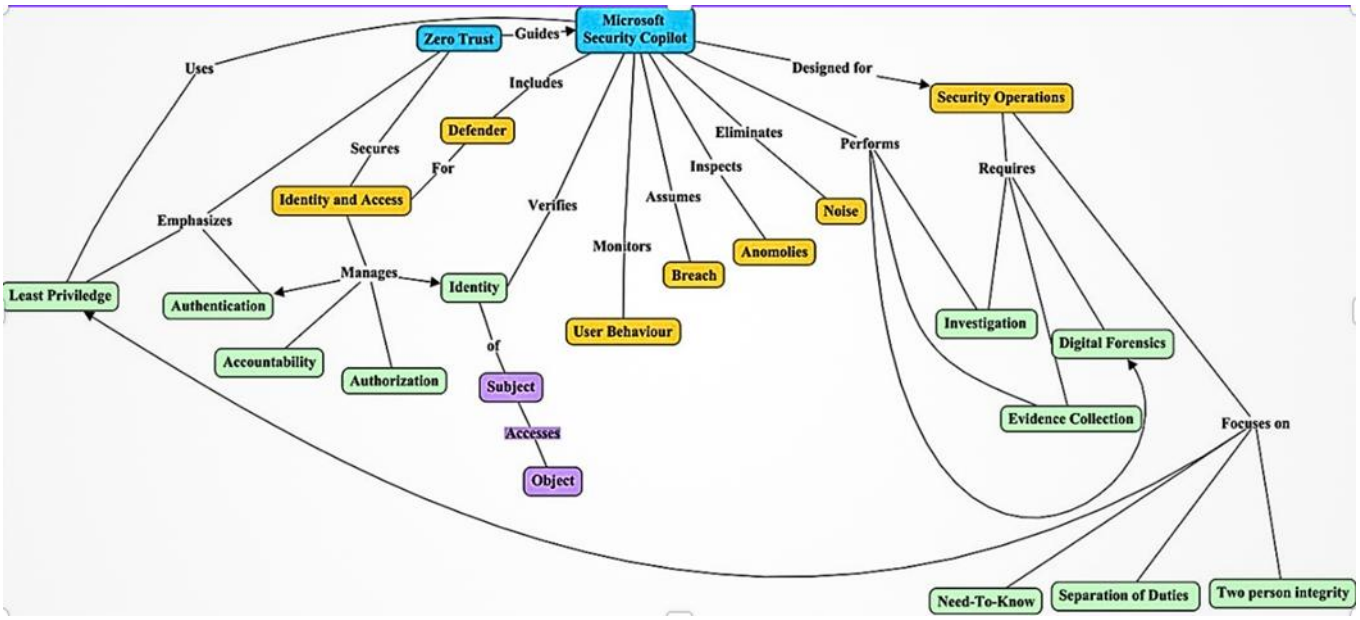
INTRODUCTION

The essence of Zero Trust relies in the statement “Never Trust, Always Verify”. This statement powerfully explains that no user, device or application must be trusted, and its identity must always be verified before allowing a connection. With the shift in dynamics of workplace and the trend of Bring Your Own Device (BYOD) and Remote Work, it becomes imperative to utilize zero trust principles to protect company’s assets. The Zero Trust architecture, despite being a very useful one in current scenario of changing dynamics, has not been widely adopted due to complexities related to its implementation. [5] With the advent of AI the application and implementation of Zero Trust can be made easier with the help of tools like Microsoft Copilot for security. Moreover, with the cyber-attacks increasingly utilizing AI, it only makes sense to employ AI tools to counter and deter these attacks.

Microsoft Copilot can be used to enhance ZTA by integrating Security Operations (SecOps) and Identity Access and Management (IAM) into a cohesive security strategy. It offers a user-friendly interface where administrators can interact with copilot for assistance, automating security workflows and reinforcing access controls. Microsoft copilot aligns with ZTA principles providing a robust mechanism for maintaining secure and efficient operations.

The purpose of this project is to explore how Microsoft Copilot can be used within the ZTA framework to enhance IAM and SecOPs. This practice-oriented study will examine the integration of AI in ZTA emphasizing its role in addressing the modern cybersecurity challenges and its alignment with the User Pillar and Automation and Orchestration Pillar of Zero Trust.

CONCEPT MAP



In previous applications where majority of assets were in the physical perimeter of the organization, traditional cybersecurity defense strategies like Security information and event management (SIEM) were effective in protecting the assets. However, with the changing trend especially after COVID-19, major shift like Work-From-Home scenarios and moving assets from on-premises (On-Prem) facilities to cloud required a shift in cybersecurity practices. Microsoft Security Copilot effectively controls Identity and Access Management by constantly monitoring User Behavior and inspects for any anomalies [17][20]. It speeds up the process by eliminating noise and learning from previous malicious attacks. Following the guiding principles of "Never Trust, Always Verify" and assuming breaches it constantly monitors for attacks. It also performs investigation on request, write Kusto Query Language (KQL) queries to find malicious codes as a part of evidence collection, finds the details of attackers through its database which improves the security operations. Focusing on concepts like Least Privilege, Need-to-Know and Just-in-Time access, tasks related to IAM and SecOps can be automated using Copilot. Separation-of-duties is ensured at the time of setting up the user account and for tasks of high importance Two-person-integrity can also be set up to authenticate the access attempt.

THE PROCESSES OF THE MICROSOFT COPILOT IN ZERO TRUST CYBERSECURITY

Microsoft Copilot for Security now known as Microsoft Security Copilot uses large language models as a base to interact with user and is trained on petabytes worth of data to identify user behavior and enhance cybersecurity by efficient threat handling. It is powered by OpenAI's Chat GPT model to enable natural language conversations and employs Zero Trust Principles as guidelines to integrate Zero Trust Strategy into security operations. The model is being trained on billions of identity transactions and is becoming better every day at identifying threat. With the integration of AI, Microsoft Copilot can now be used to assist junior analyst recognize and counter malicious activities with little training by just prompting the Copilot. It is also capable of providing training and active insights in attacks that take place, isolate the problematic devices, contain the blast radius and stop malicious attacker in their tracks with easy prompts. The core principle of Zero Trust is integrated into its very core i.e., it never trusts but verifies every user, device, application and network. Not only this follows the core guiding principle of Zero Trust but advances its maturity through the User Pillar and ensures Identity and Access Management by monitoring User Behavior.

Microsoft Copilot is built in with Azure and is integrated with Azure Active Directory (Azure AD), Microsoft Defender, and Sentinel which allow for Just-In-Time access, enhances identity verification and supports least privilege strengthening Identity and Access Management. Moreover, it enables security teams to proactively identify threats by analyzing large volumes of security data and recommending appropriate course of action enabling effective Security Operations. It also enhances the Automation and Orchestration Pillar by introducing predictive analytics for threat forecasting.

CASE STUDY

Intesa Sanpaolo, a bank in Italy, uses Microsoft Sentinel security information and event management system to scale elastically to evolving security needs and simplify threat detection. It supports its threat hunters with Microsoft Copilot for Security [16]. The bank faced challenges in strengthening their security posture due to scarcity of cybersecurity talent but with implementation of AI Powered security forefront, the new staff reached maximum efficiency in very short duration. The bank started assessing the Copilot in only in early 2024 and since then have enable junior threat analysts and threat hunters to efficiently utilize Kusto Query Language (KQL) with little to no prior knowledge freeing up Senior Analysts to face more pressing matters. Not only does the query generation through prompts save precious time required for writing the code by using KQL script generator and the script analyzer feature, but it also enables for on job training exposing the malicious patterns used by attackers, increasing analysts' awareness and improving overall quality of analyses.

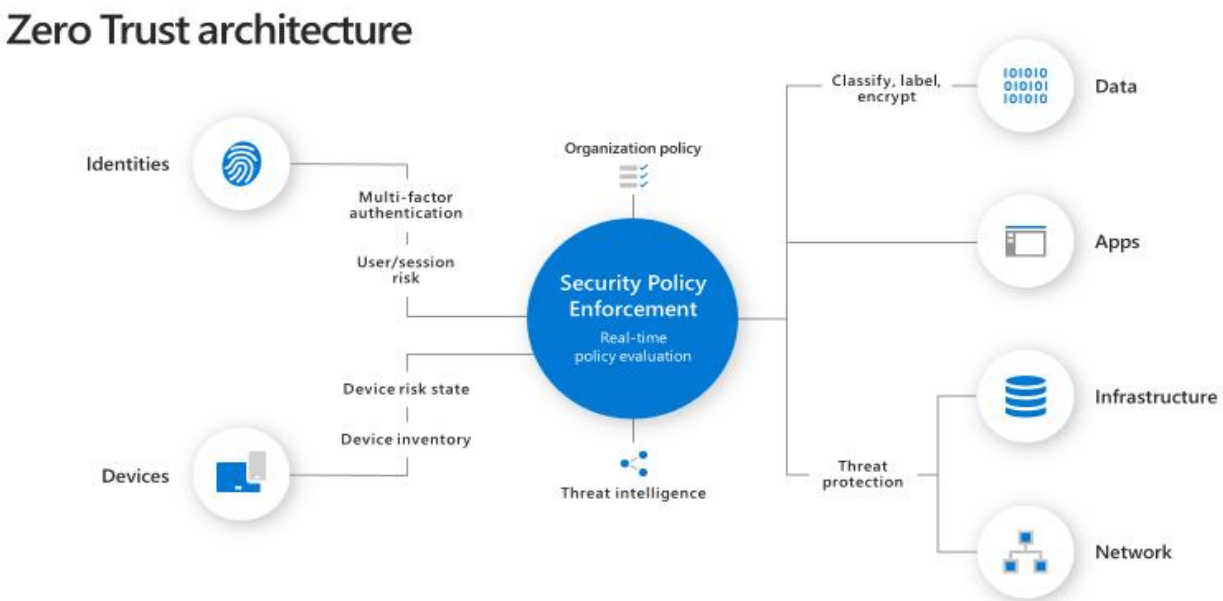
To conclude, this case study proves that in the current situation of changing threat dynamics and limited resources, AI application like Microsoft Copilot proves to be a lifesaver by enabling improved security posture at organizational level. Not to forget this solution is scalable to any level since the security credentials can be assigned and revoked at any time. If we focus on User and Automation and Orchestration Pillars, it enables security professionals to address critical cybersecurity threats like credential threats, insider threats and regulatory challenges at a speed that cannot be compared to its human counterparts.

ADOPTION OF MICROSOFT COPILOT IN ZERO TRUST CYBERSECURITY

ADOPTION AND TARGET AUDIENCE

The Microsoft Copilot in Zero Trust Cybersecurity is integrated at every level i.e., individual level, system level and organizational level since it is integrated with every device and azure cloud services. To utilize security copilot, one must have security permissions from the admin, but it comes integrated with Microsoft security services like sentinel and defender. With it is being used by large organizations that require advanced IAM and SecOps solutions, small and medium organizations to implement Zero Trust principles without requiring significant resources, cloud native businesses to safeguard hybrid and multi-cloud environments, and educational institution and research organizations to secure sensitive intellectual property and ensure compliance with data privacy regulations.

IMAGE: MICROSOFT ZERO TRUST ARCHITECTURE



Microsoft receives telemetry of over 1.5billion PC users and over 1 billion cloud users which accounts to over 630 identity transactions per month. [9] it utilizes these stats to train the models to which over time will become more intelligent in identifying anomalous user behavior and effectively block any malicious actors in their tracks in terms of few hundred milliseconds. This is a profound moment as cyberthreat detection of this level with these timings is not possible by humans and its scalability in terms of any size of system and organization proves its importance. The fact that it can train professionals while making them capable of effective threat management has changed the face of how Zero Trust Strategy can be seamlessly integrated within the security operations with the use of Microsoft Copilot.

BENEFITS, OPPORTUNITIES, COST, AND RISK

Initially it was thought that moving from the existing security measure and adopting zero trust strategy was thought to be costly. Also, IT personnels resisted the change due to fear of user disruption although it would prove to be less costly over the entire lifecycle. [5] But considering the shift in dynamics and utilization of cloud technologies that made users mobile, Zero Trust has grown in popularity. Challenge involves building smart city services that deliver urbanization data. Great service enhances unique customer interactions. This strategy enhanced smart city apps. Big data issues for smart city growth require technology expertise, citizen awareness, administration, data management, and service design.

BENEFITS

The Microsoft Copilot which does not require additional software packages since it is included with services provided by Microsoft for all its cloud users making it easier to implement Zero Trust principles to enhance security. The key benefit of Zero Trust is that it helps reduce the total cost of ownership over the entire lifecycle [4]. The other benefit is that of enhanced security posture even with limited cybersecurity talent and on job training done by the AI. Automation of threat detection and mitigation, anomaly detection, real time access management reduces the risk of data breaches, insider attacks and ransomware attacks. It is user friendly, highly scalable and bring the security of organization in alignment with the regulatory and compliance requirements.

OPPORTUNITIES

Copilot will become widely popular for organizations of all sizes once they realize it can help integrate Zero Trust Strategy in the security framework of their organization even with limited expertise with the help of AI. Integrating Copilot with emerging trends like Blockchain and security in cryptocurrency can enhance the Security strategy by decentralization of IAM.

COST

The current cost listed on the website for using the copilot is $4 per SCU along with the upfront cost of licensing fees, integration with existing systems, and customization expenses. However, one must consider the cost of entire lifecycle from implementation to decommissioning which will reduce cost of ownership. The other costs to consider is the cost of training employees especially effective prompt engineering which can take some time to master.

RISKS

With great benefits comes greater risks. The one challenge that organization will face is the overreliance on the AI. If an unknow bug affects the performance of Copilot, many organizations with limited talent in field of cybersecurity can be left exposed to malicious attacks. The AI models can be subject to poisoning and adversarial attacks which may affect its capabilities to detect threats which can again lead to disastrous outcomes. Then there is always a risk of data breaches due to the utilization of third-party entity, which means Microsoft can gain access to the proprietary data of an organization without the knowledge of the organization raising concerns about data privacy.

PRACTICAL IMPLICATIONS

The companies that utilize the Copilot to enhance the security by integrating the Zero Trust Strategy will experience significant improvement in their cybersecurity resilience. It will also allow better allocation of resources by freeing up the time of experienced senior analyst by providing support to junior analyst in handling threats. The initial cost can be a challenge especially for organizations moving from on-prem to cloud, but in long run it will help reduce the

cost over the entire lifecycle. Repetitive and mundane tasks can be automated freeing the resources for important tasks.

FUTURE TRENDS

The AI like Copilot is constantly evolving and learning from the data that it receives every day. This makes it possible for the AI Model to begin understanding and predicting user behavior through anomaly detection. In future it can even incorporate organization behavior nuances to provide even more precise threat detection and reduce false positives. The other trend is the current reliance on Multifactor authorization and adaptive access policies based on contextual data for Identity and Access Management, however, in future continuous biometric monitoring may be the utilized by integrating Zero Trust IAM to authenticate users.

CONCLUSION

Predicting The integration of Microsoft Copilot into Zero Trust cybersecurity frameworks represents a significant advancement in identity and access management (IAM) and security operations. As organizations face increasingly sophisticated cyber threats, the AI-powered capabilities of Copilot offer a powerful tool to enhance security postures and streamline critical processes.

***Key findings from this study include*:**

1. Enhanced Automation: Copilot's AI algorithms significantly reduce manual workload in IAM tasks, enabling more efficient and accurate identity verification and access control.
2. Improved Threat Detection: The integration of Copilot with security operations centers (SOCs) allows for faster threat identification and response, leveraging machine learning to analyze vast amounts of data in real-time.
3. Adaptive Security: Copilot's ability to learn and adapt to new threats aligns well with the dynamic nature of Zero Trust principles, allowing for continuous improvement in security measures.
4. Challenges in Implementation: While powerful, Copilot requires careful configuration and ongoing management to ensure it aligns with organizational security policies and doesn't introduce new vulnerabilities.
5. Future Potential: As AI technology continues to evolve, Copilot's capabilities in predicting and preventing security incidents are likely to expand, further strengthening Zero Trust architectures.

In conclusion, Microsoft Copilot represents an asset in the implementation of Zero Trust cybersecurity strategies. Its AI-driven approach to IAM and security operations offers organizations a more robust, efficient, and adaptive security posture. However, successful integration requires a thoughtful approach, balancing the benefits of AI automation with the need for human oversight and strategic alignment with broader security objectives.

As cyber threats continue to evolve, the role of AI in cybersecurity will undoubtedly grow. Organizations that effectively leverage tools like Microsoft Copilot within their Zero Trust frameworks will be better positioned to protect their digital assets and maintain resilience in an increasingly complex threat landscape.

REFRENCES

[1] Cloud Security Alliance. (2023, November 17). Guiding principles for implementing zero Trust [Video]. YouTube. https://www.youtube.com/watch?v=_kcAiuTtvJ8
[2] Zurier, S. (2024, January 26). Why has zero trust been stalled for nearly 20 years? SC Media. https://www.scworld.com/research-article/why-has-zero-trust-been-stalled-for-nearly-20-years
[3] Ron Gerber with Angelbeat Seminars. (2023, July 13). Microsoft CoPilot and Zero Trust [Video]. YouTube. https://www.youtube.com/watch?v=zngYsR65UOk
[4] Microsoft Security Copilot | Microsoft Security. (n.d.). https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot#tabs-pill-bar-oca857_tab0
[5] Intesa Sanpaolo accrues big cybersecurity dividends with Microsoft Sentinel, Copilot for Security. (n.d.). Microsoft Customers Stories. https://customers.microsoft.com/en-us/story/1814561247353333768-intesa-sanpaolo-group-microsoft-copilot-for-security-banking-and-capital-markets-en-italy
[6] Naik, S. (2023). Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy.The Eastasouth Journal of Information System and Computer Science, 1(01), 69–87. https://doi.org/10.58812/esiscs.v1i01.452

[7] Vitla, Surendra. 2023. “Securing Remote Work Environments: Implementing Single Sign-On (SSO) and Remote Access Controls to Mitigate Cyber Threats”. Turkish Journal of Computer and Mathematics Education (TURCOMAT) 14 (2):1097-1114. https://doi.org/10.61841/turcomat.v14i2.14968
[8] Bayya, A.K. Advocating Ethical Data Management and Security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) Volume 8, Issue 4 Page Number : 396-417
[9] Yerra, S. (2023). Leveraging Python and machine learning for anomaly detection in order tracking systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://ijsrcseit.com/home/issue/view/article.php?id=CSEIT2311354.
[10] Shah, v. Novel approach for analyzing intraday stock market behavior using stream data analytics
[11] Shah, V., & Sajnani, N. (2020). Multi-class image classification using cnn and tflite. *International Journal of Research in Engineering, Science and Management*, *3*(11), 65-68