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 8, August 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|

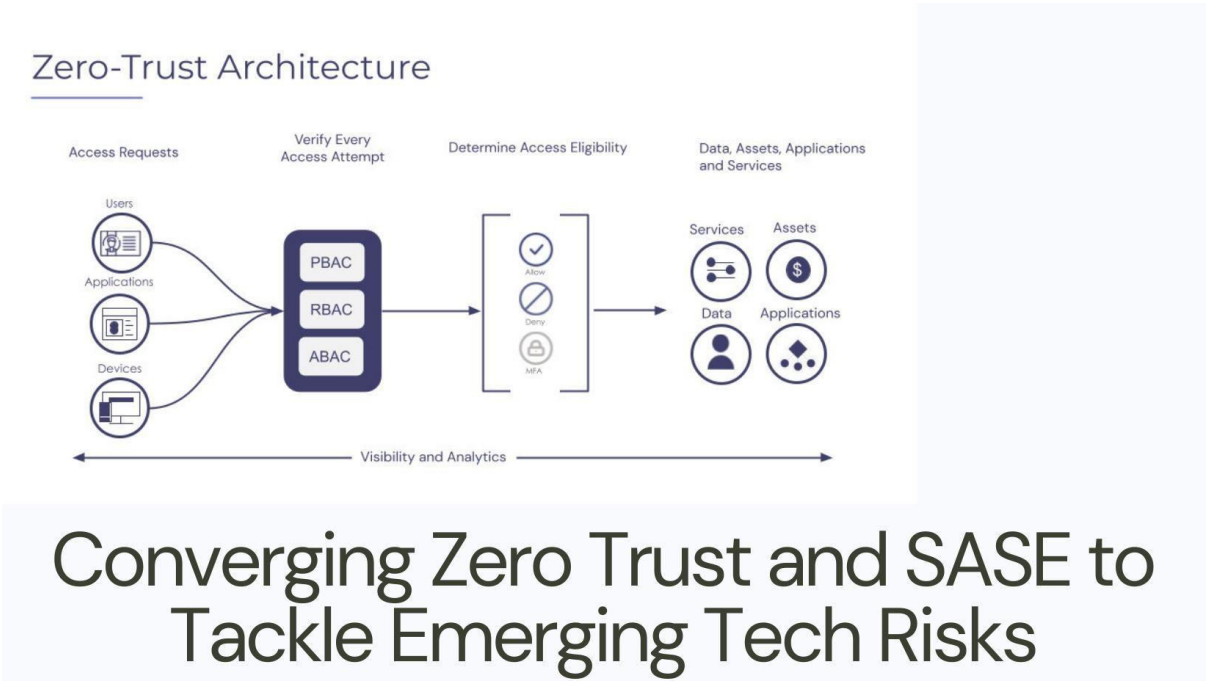
Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

Converging Zero Trust and SASE to Tackle Emerging Tech Risks

Nithin Varam

Palo Alto Networks, USA



Converging Zero Trust and SASE to Tackle Emerging Tech Risks

ABSTRACT: The widespread adoption of cloud services and the rise of remote work have made traditional perimeter based security models increasingly ineffective. Enterprises are looking for a more flexible, scale and user centric approach to securing internet access. SASE and Zero Trust offer a compelling solution to this challenge by leveraging their architecture synergies: SASE combines multiple security and networking functions to single, cloud delivered service and Zero Trust operates on the principle of "never trust, always verify. By leveraging these two frameworks, Enterprises can enhance their security postures while enabling their distributed workforce productivity. While enterprises adopt their frameworks, they must also be cognizant of the emerging risks posed by the new technologies, such as Generative AI and Quantum computing, becoming a tool for sophisticated cyber attacks. In conclusion, while the convergence of SASE and Zero Trust provides a comprehensive approach to secure internet access in the modern enterprise, modern day enterprises must proactively address the risk of advanced technologies by implementing strong security measures.

KEYWORDS: Zero Trust Architecture, SASE (Secure Access Service Edge), Cloud Security, Emerging Cyber Threats, Generative AI & Quantum Computing Risks

I. INTRODUCTION

Providing consistent and pertinent access control for remote users and cloud resources is a challenge for traditional network security models that rely on fixed network boundaries [1]. Perimeter based architectures use demilitarized zones and firewalls to isolate internal corporate networks from external environments. The traditional network security used intrusion prevention systems, VPN gateways, and on-premises firewalls to create a fortified perimeter around

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 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

corporate environments. Distributed apps and cloud adoption, however, dissolve this rigid boundary. The idea of a safe network perimeter that divides areas into trusted and untrusted areas is becoming less and less relevant. In addition,

- Hybrid work environments: With employees alternating between working from home and the office, it is crucial to ensure consistent performance and security regardless of the user's location. This requires a flexible and adaptable network infrastructure that can accommodate the needs of a distributed workforce.
- Cloud Adoption: As more applications migrate to the cloud, the risk of data exposure increases due to data transfer beyond the traditional enterprise perimeter. This necessitates the implementation of robust security measures that can protect data both within and outside the organization's network.
- New Technological Advancements: The emergence of newer technologies, such as Generative AI and Quantum computing, has the potential to further accelerate and increase the sophistication of already rapidly evolving cyber threats. Organizations must stay vigilant and proactively adapt their security strategies to counter these advanced threats and protect their assets.

II. EVOLUTION FROM PERIMETER-BASED SECURITY

Cyber threats change quickly, and modern computing environments are getting more complicated with hybrid work arrangements, cloud adoption, and new technologies like generative AI and quantum computing. These changes have shown where traditional security architectures fall short. This has led to the development of new security frameworks, such as Secure Access Service Edge (SASE) and Zero Trust, which have emerged as promising solutions to address these challenges by providing consistent performance and security across distributed workforces, protecting data within and outside the organization's network, and enabling proactive adaptation to counter advanced threats.

The core principle of Zero Trust, "never trust, always verify," eliminates the traditional notion of a trusted network perimeter, recognizing that threats can originate from both internal and external sources. Complementing Zero Trust, SASE offers a cloud-native architecture that converges networking and security functions, enabling secure connectivity across diverse environments.

While enabling direct access to cloud and internet platforms can greatly increase productivity, it also increases the attack surface. According to the Verizon 2023 Data Breach Investigations Report [12], 74% of all breaches include the human element, with people being involved either via privilege misuse, use of stolen credentials, or social engineering. While zero trust is generally attributed to the ZTNA pillar of SASE, this study explores it in terms of internet access. SWG and CASB pillars for SASE typically cover internet access. The study looks at how the architectural synergies of these frameworks can make it easier to use security-enhancing features like threat prevention and data protection to help secure distributed workforce access to the internet.

III. ZERO TRUST AND SASE

Zero Trust

In 2010, analyst John Kindervag of Forrester Research developed the notion of Zero Trust. Zero Trust is an information security model that denies access to applications and data by default. To stop threats, you should only let people into networks and workloads when you follow rules that are based on constant, contextual, risk-based checks of users and the devices they use [23].

NIST Special Publication 800-207 states that the following are the fundamentals of the Zero Trust model:

- Resources provisioned within or outside of an organization's network are all data sources and services.
- Any communication, regardless of where it is on the network, is secure.
- Policy enforcement provides per-session access to specific enterprise resources.
- To guarantee least-privileged access, policies specify the means of communication between different components [2].

SASE

Gartner created the term SASE (pronounced "sassy") to support the distributed workforce in 2019 to describe the convergence of network security and connectivity capabilities provided as a cloud service. SASE is a single, integrated solution that combines the capabilities of zero-trust network access (ZTNA), firewalls, cloud access security brokers

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 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

(CASB), secure web gateways (SWG), and SD-WAN. Cloud-based access permits direct access from branches and mobile devices, maintaining policy consistency regardless of location or network type.

Industry analysts have highlighted how the SASE and Zero Trust frameworks address distinct but related facets of security for contemporary enterprises. While SASE concentrates on safeguarding access to external apps, analysts claim that SASE answers "how to enable secure access everywhere." In contrast, Zero Trust provides an answer to "who should access what resources?" Instead of only centralized security stacks, SASE offers globally distributed access policy enforcement points close to users. Context-aware access based on user, device, app, location, and network environment is possible when combining SASE and Zero Trust.

Furthermore, SASE requires a software-defined coordination layer to manage user identities and devices and enforce fine-grained segmentation as it combines networking and security capabilities in the cloud. The Zero Trust identity governance principles enable SASE to transition from an IP-based legacy access model to a user-centric one.

Aspect	Zero Trust	SASE
Goal	To prevent unauthorized access, contain breaches, and limit attackers' lateral movement by enforcing least-privilege access	To provide secure and optimized access to applications and services anywhere, with consistent policy enforcement and user experience
Key Principles	1. Never trust; always verify 2. Assume breach 3. Least privilege access	1. Identity-driven 2. Cloud-native 3. Supports all edges 4. Globally distribute
Components	Not a specific technology, but incorporates concepts like MFA, micro-segmentation, continuous monitoring, encryption, etc.	Combines SD-WAN, SWG, CASB, FWaaS, and ZTNA into a unified cloud platform with centralized policy control

Table 1: Key principles of Zero Trust and SASE model

IV. ENABLING SECURE INTERNET ACCESS WITH SASE AND ZERO TRUST

Balancing security and productivity

The essence of a secure enterprise is protecting critical assets without impeding business velocity or workforce efficiency. Security actions that impede user productivity led to frustrated end users resorting to risky workarounds that undermined security.

Methods that balance security and better user experience include just-in-time access and providing context-based access instead of rigid blanket policies.

Modern-day CASBs are very flexible and provide granular access controls based on the risk of cloud applications. Instead of allowing or blocking access, enterprises can control the access based on the user's function in the cloud application. Similarly, SWG can categorize and filter the websites based on their content and risk. The measured approach enables enterprises to securely adopt SaaS and provide access to internet resources while maintaining productivity.

Ensuring the user's permissions are context- and risk-based and monitoring their activities to adjust policies as needed ensures that users don’t have overly permissive access while not impacting their work. Automatically adjusting the policy based on the SOAR workflows, which leverage user behavior analytics, and MIRTE ATT&CK framework tactics, further helps in containing the threats without burdening the end users.

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 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

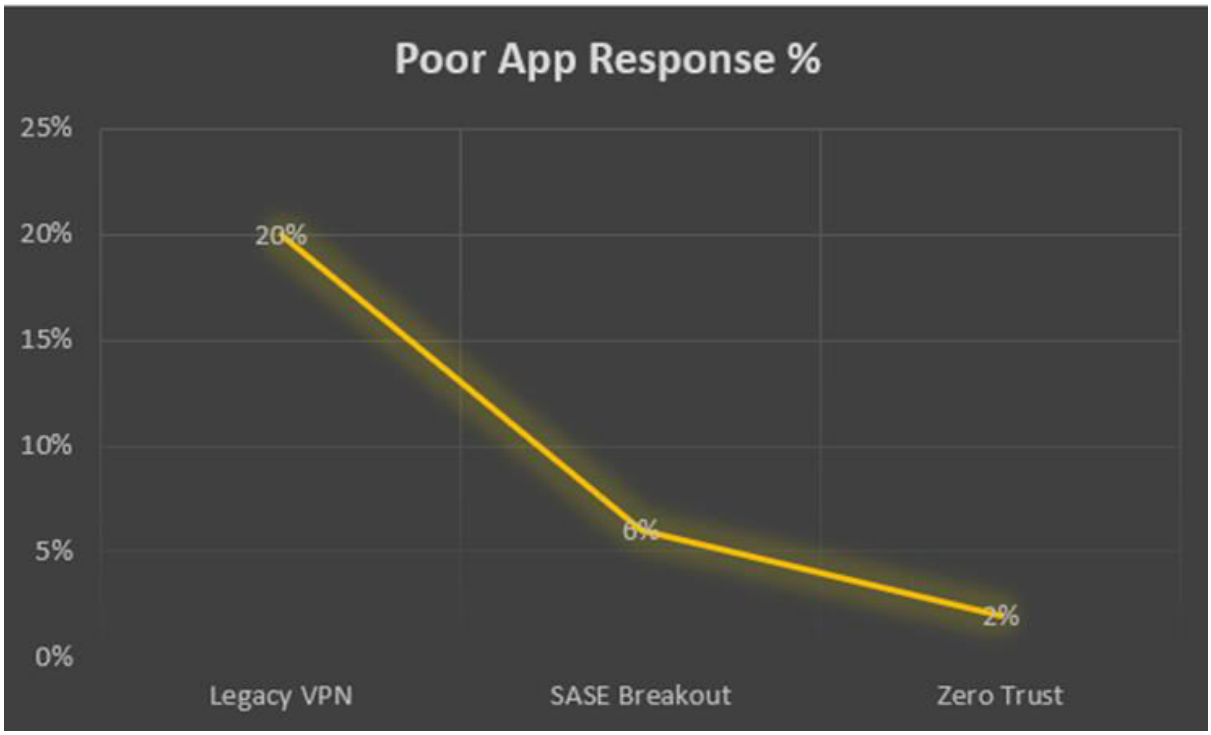


Fig. 1: Access Model: Boost in Productivity [3]

V. BEST-IN-CLASS SECURITY

Continuous verification and context-aware access controls

Thanks to the integrated SASE stack running on Zero Trust, context-aware policy enforcement is possible with distributed yet unified policy engines. This helps the modern digital enterprise find a balance between security and productivity. The SASE architecture's distributed but unified design makes enforcing context-based, coherent access policies closer to user endpoints possible. Granular segmentation schemes driven by user identity, device posture, application sensitivity, and network trust levels make it possible to implement risk-appropriate controls. Under Zero Trust principles, SASE components must constantly verify users and devices before granting access.

Making context-aware, risk-appropriate access policy decisions is made possible for SASE POPs by integrating identity and device metadata from Zero Trust engines. POPs use SAML and OAuth standards for interoperability to combine cloud security features like CASB with SD-WAN capabilities [3]. Policy decisions are risk-appropriate based on user, device, and anomaly profiles and device metadata integrated from Zero Trust engines. Because POPs have integrated traffic inspection capabilities that adjust based on trust levels, they can dynamically block, isolate, or limit access. The real-time correlation of access requests with threat intelligence feeds enables dynamic policy fine-tuning that is responsive to new vulnerabilities.

Integrating controls like data loss prevention and user-entity behavior analytics makes it possible to provide data-centric protection that complies with current compliance requirements. Contextual policy checks on accessed applications, content sensitivity, anomaly patterns, and integration with threat feeds all help to improve real-time risk analysis of access requests.

Cloud-delivered protection against online threats

SASE services improve threat protection for distributed enterprises by moving secure web gateways, firewalls, remote access VPNs, and other network security appliances to the cloud. The globally dispersed yet unified security stack that is closer to user endpoints makes consistent policy enforcement and cutting-edge threat prevention possible regardless of location. Cloud-based secure web gateways shield all web traffic from malware and phishing attempts while offering

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 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

real-time website profiling. Protective controls on SaaS usage are also possible thanks to the native integration of cloud access security brokers. Embeded zero-trust network access with context-aware policies prevents lateral threat movement.

ML-based user and entity behavioral analytics (UEBA) and context-aware micro-segmentation make it possible to enforce policies tailored to the level of risk. Automated response playbooks are activated to contain advanced threats and to respond to breaches of the risk threshold.

Data Protection

As applications move to cloud, data is being stored accessed, and shared from more places than ever. As a result, enterprises struggle more than ever to protect their data and prevent data breaches. Data Protection is a key component of SASE and Zero Trust frameworks. Sensitive data must be identified, classified, and secured across all environments, from endpoint to cloud, irrespective of whether the data is at rest, in use or in motion. Data Loss Prevention (DLP) must be leveraged as part of the SASE framework to ensure end-to-end data security. Modern-day DLP uses Optical character recognition (OCR), Exact data match (EDM) fingerprinting, and indexed document matching (IDM) to accurately identify the data across all document types, including images, sensitive records, and high-value documents. Enterprises should establish data governance frameworks to meet regulatory requirements such as GDPR as well as mitigate security risks.

Optimizing the User Experience

The SASE model hosts security controls distributed globally via points of presence (POPs) at the network's edge and closer to the user. The POPs provide local breakouts closest to the user edge rather than backhauling traffic over MPLS or VPNs through regional hubs. This ensures faster and more direct access to applications and data, thus reducing latency and enhancing overall performance for users. No matter whether users are at the office or home, they receive the same level of performance.

SASE's dynamic and adaptive security policy enables the Zero Trust framework's continuous verification for all access, thereby balancing security without hindering productivity. By incorporating risk thresholds for stepping up access validation, it is possible to reduce the number of excessive authentication requests.

Furthermore, by converging multiple security and networking functions into a unified cloud service, SASE offers organizations consistent security and streamlined user experience.

VI. OVERCOMING OPERATIONAL CHALLENGES

Consolidation of networking and security in the cloud

Simplifying the process of switching to SASE can help businesses reduce costs, improve security, and maintain business continuity.

Key steps include:

1. Consolidating legacy network and security hardware into cloud-hosted virtual instances
2. Integrating threat intelligence, analytics, and response workflows into a single management interface
3. Implementing a gradual rollout that prioritizes high-risk users and specific applications
4. Upgrading bandwidth and connectivity to manage growing volumes of encrypted traffic
5. Linking SASE components with current identity systems for consistency
6. Educating end users on improved authentication protocols before going live
7. Encouraging collaborative security efforts through open feedback loops

By following these steps, businesses can successfully transition to SASE while minimizing disruption and ensuring a balance between productivity and protection.

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 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

Fig. 2: Advancing Threat Protection [5]

Addressing common implementation challenges

To integrate Zero Trust controls into the SASE architecture, priorities must be coordinated among multiple internal teams. A central office with cross-department leads on staff is responsible for directing the change management protocols, phased rollout strategy, and roadmap. This incremental approach minimizes risks, identifies issues, and validates resilience measures, enabling organizations to build more robust and fault-tolerant systems.

A phased rollout strategy can contain prepare, pilot, validate, and scale phases. Using current access patterns, the Prepare phase involves evaluating the current legacy application and data environment in terms of criticality, compliance requirements, and end-user profiles. This offers information for creating a business case and a deployment strategy that is optimized for lowering cyber risk. Infrastructure upgrades for connectivity must take increasing traffic volumes into consideration.

Phased deployment that serves as value-proof without interfering with other systems is the main focus of the active phase. To test real-world viability, start with non-sensitive applications and restrict locations and user groups. Continue to optimize access policies based on feedback to avoid process gaps or productivity losses.

Leveraging lessons from earlier phases, the Propel phase transitions into an organization-wide rollout while keeping adequate fallback plans in place. Maintaining continuity before decommissioning legacy hardware entails gradually transferring bandwidth from legacy tools into the integrated SASE stack. Secure transformations are maintained through routine cyber resilience testing. Proactively communicating improved access validation protocols and transparency regarding monitoring practices helps to allay employee adoption concerns.

VII. PREPARING FOR EMERGING THREATS WITH ZERO TRUST AND SASE

As zero trust and SASE initiatives take priority over enterprise cyber security initiatives, it is important to look towards the future and plan for emerging risks from advanced technologies. According to a recent survey by Gartner, 60% of organizations are expected to have adopted zero trust as their primary security model by 2025 [13]. The complexity of contemporary IT infrastructures and the increasing sophistication of cyber threats are what are driving the shift toward zero trust and SASE.

One of the primary emerging threats is the rise of quantum computing, which has the potential to break traditional encryption methods [14]. As quantum computers become more powerful, organizations must adopt post-quantum cryptography to maintain the security of their sensitive data [15]. Another significant threat is the proliferation of Internet of Things (IoT) devices, which often lack robust security features and can serve as entry points for attackers

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 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

[16]. By 2025, it is estimated that there will be over 75 billion IoT devices worldwide [17], making it crucial for organizations to implement strong authentication and access control measures.

Artificial intelligence (AI) and machine learning (ML) also present both opportunities and challenges for cyber security. While AI and ML can be leveraged to detect and respond to threats more efficiently [18], they can also be used by attackers to create more sophisticated and harder-to-detect malware [19]. Organizations must stay vigilant and continually update their AI-based security systems to keep pace with evolving threats.

To address these emerging risks, organizations should adopt a comprehensive zero-trust and SASE strategy that encompasses all aspects of their IT infrastructure [20]. This includes implementing strong multi-factor authentication, microsegmentation, and continuous monitoring and analytics [21]. By adopting a proactive and adaptive approach to cyber security, organizations can better protect themselves against future threats and maintain the confidentiality, integrity, and availability of their critical assets [22].

Quantum Computing: Breaking Encryption

Within the next 5–10 years, quantum computing could pose a major threat to current encryption methods [6]. Most of the existing widely used public-key cryptography algorithms, such as RSA, may be at risk, making much of today's encryption vulnerable. While quantum computer are not powerful enough to break encryption, bad actors could be storing encrypted data now to decrypt later once quantum computing advances. Enterprises need to start preparing by adopting post-quantum cryptography algorithms

SASE architectures should incorporate PQC, QKD, and FHE into future-proof encryption so that quantum-related risks can be mitigated. As part of the SASE transition, enterprises should invest in transitioning to post-quantum cryptography (PQC) algorithms that are resistant to quantum attacks.

Enterprise should implement quantum key distribution (QKD), which uses quantum mechanics to securely distribute encryption keys. Further, they should utilize fully homomorphic encryption (FHE), which allows computation on encrypted data without ever decrypting it.

Also, regulatory guidelines from GDPR and CCPA are pushing for stronger encryption to secure the user's privacy and data. Enterprises should find the right balance to have selective policy-based decryption as part of the SASE rollout so that they can meet the regulatory requirements to secure user privacy while decrypting traffic for security risks.

AI-Powered Phishing and Social Engineering

Artificial intelligence is making it much more sophisticated and harder to detect phishing emails and social engineering attacks. AI language models can write phishing emails with perfect grammar and spelling, personalized to the victim, and scaled up massively. Since the release of ChatGPT, malicious AI-generated phishing emails have increased by over 1200% [7].

Enterprises should implement AI-powered phishing detection and also further train employees about Social Engineering and phishing. During SASE implementation, enterprises should integrate with cloud email security, sandboxing, and CASB functionality. They should deploy AI-powered email security that can detect new and AI-powered phishing attempts.

To effectively combat the growing threat of AI-generated phishing attacks, enterprises must adopt a multi-faceted approach that includes both technological solutions and employee training. Implementing SASE architectures that integrate cloud email security, sandboxing, and Cloud Access Security Broker (CASB) functionality will provide a thorough defense against sophisticated phishing attempts. Additionally, deploying AI-powered email security solutions capable of detecting novel and linguistically complex phishing attempts and continuously updating these models to keep pace with evolving attacker techniques is crucial. Furthermore, conducting regular phishing awareness training for employees, with a strong emphasis on the fact that AI can create extremely authentic-looking emails, is essential to educate them on how to recognize and report suspicious emails, even if they appear to be genuine. By combining cutting-edge technology with ongoing employee education, enterprises can significantly reduce their risk of falling victim to AI-generated phishing attacks and protect their sensitive data and systems.

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 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

AI Model Theft and Manipulation

Artificial Intelligence (AI) models face various security risks, including theft through network attacks, social engineering, or vulnerability exploitation [6]. Attackers can also manipulate AI systems using techniques such as data poisoning, evasion attacks, and privacy abuse [7]. Additionally, "prompt injection" attacks pose a threat by manipulating AI outputs [8].

To mitigate these risks, enterprises should take the following steps:

1. Insist on code provenance and Software Bill of Materials (SBOM) to ensure the integrity of the AI/ML supply chain [8].
2. Implement robust access controls and network segmentation to prevent unauthorized access to AI models and training data.
3. Regularly test AI systems for vulnerabilities and monitor for attempts to manipulate model behavior [9].

By adopting these security measures, organizations can better protect their AI models and data from theft, manipulation, and abuse, ensuring the reliability and trustworthiness of their AI-powered applications.

Identity and Access Management (IAM) and Multi-Factor Authentication (MFA) Risks

Multi-factor authentication (MFA) has long been considered the gold standard for securing user accounts, but emerging threats like reverse proxy tools (e.g., EvilProxy) are capable of bypassing MFA by intercepting codes and cookies, as demonstrated in recent breaches at Uber and Okta [10]. With the increasing adoption of cloud services, identity has become the new security perimeter. However, identity and access management (IAM) systems face various risks, including excessive permissions, misconfigurations, privilege escalation, and compliance challenges. The 2022 Trends in Securing Identities Report by IDSA revealed that 84% of organizations experienced an identity-related breach [11].

To strengthen identity systems within SASE architectures, organizations should implement the following measures:

1. Adopt phishing-resistant MFA methods, such as security keys and passwordless authentication using FIDO2 or certificate-based authentication.
2. Implement granular access policies that incorporate user/device identity, location, and behavior.
3. Automate offboarding and de-provisioning of unused accounts to minimize the attack surface.
4. Employ privileged access management for administrative accounts to prevent unauthorized access.
5. Continuously monitor for signs of compromised credentials and evaluate MFA logs to detect potential compromises.

By integrating these security measures into their SASE architectures, organizations can better protect their identity systems and mitigate the risks associated with emerging threats.

VIII. CONCLUSION

In summary, combining the concepts of cloud-native SASE architecture with Zero Trust architecture offers a thorough method of securing enterprise access in the contemporary, digitally-driven business environment.

The Zero Trust philosophy of identity-centric "never trust, always verify" access, along with SASE's globally distributed cloud security stack, redefines the corporate boundary to workforce identity, whereas legacy network security depends on brittle perimeters. Instead of giving out one-time network grants, continuous authorization of users, devices, and environments is built into the workflows for data and application access. This makes context and risk-aware protection much better.

The consolidated networking and security-as-a-service capabilities of SASE enable uniform enforcement of context-aware security policies, regardless of user location. SASE and Zero Trust provide strong defenses against cyber threats. SASE, with integrated CASB, SWG, threat prevention, and data security, removes the need for point products and provides consistent security. By striking a balance between user experience and security, SASE ensures that stronger security controls, as advised by Zero Trust, don't negatively impact the user experience.

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 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

As we move forward, we'll need to stay aware of the risks posed by new technologies like Generative AI and Quantum computing and plan to mitigate them. By staying informed, investing in the latest security solutions, and creating a culture where everyone takes cybersecurity seriously, we can build a safer digital future for all.

REFERENCES

[1] S. Srinivasan, K. Sarukesi, P. Rodrigues, M. S. Manoj, and P. Revathy, "State-of-the-art cloud computing security taxonomies: A classification of security challenges in the present cloud computing environment," in Proc. International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2012, pp. 470-476, doi: 10.1145/2345396.2345474.
[2] NIST 2021: https://csrc.nist.gov/publications/detail/sp/800-207/final
[3] Abdulmalik Alwarafy, Khaled A. Al-Thelaya, Mohamed Abdallah, and Jens Schneider, "A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things," IEEE Access, vol. 9, pp. 76092-76115, 2021, https://ieeexplore.ieee.org/document/9163078.
[4] A. Abuhussein, F. Alsubaei, S. Shiva, and F. T. Sheldon, "Evaluating Security and Privacy in Cloud Services," in Proc. IEEE International Conference on Smart Cloud (SmartCloud), 2020, pp. 134-139, https://ieeexplore.ieee.org/document/7552089.
[5] S. Sengupta, V. Kaulgud, and V. S. Sharma, "Cloud Computing Security--Trends and Research Directions," in Proc. IEEE World Congress on Services, 2011, pp. 524-531, https://ieeexplore.ieee.org/document/6012787.
[6] "Quantum Computing and its Impact on Cryptography." Cryptomathic, https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography. Accessed 19 May 2024.
[7] "AI like ChatGPT is creating huge increase in malicious phishing email." CNBC, 28 November 2023, https://www.cnbc.com/2023/11/28/ai-like-chatgpt-is-creating-huge-increase-in-malicious-phishing-email.html. Accessed 19 May 2024.
[8] "How Generative AI is Creating New Cybersecurity Threats at Scale." Comcast Business, https://business.comcast.com/community/browse-all/details/how-ai-is-generating-new-cybersecurity-threats-at-scale. Accessed 19 May 2024.
[9] Oprea, Alina. "NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems | NIST." National Institute of Standards and Technology, 4 January 2024, https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems. Accessed 19 May 2024.
[10] Mukherjee, Anupama. "Is MFA As Secure As It Used To Be?" Threat Intelligence, 4 October 2023, https://www.threatintelligence.com/blog/mfa. Accessed 19 May 2024.
[11] Zimmerman, Eric. "2022 Trends in Securing Digital Identities." Identity Defined Security Alliance, https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/. Accessed 20 May 2024.
[12] 2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket." Verizon, 6 June 2023, https://www.verizon.com/about/news/2023-data-breach-investigations-report. Accessed 20 May 2024.
[13] Gartner. (2021). Gartner Predicts 60% of Enterprises Will Have Adopted Zero Trust as Their Primary Security Model by 2025. Gartner. https://www.gartner.com/en/newsroom/press-releases/2021-03-09-gartner-predicts-60-percent-of-enterprises-will-have
[14] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012-1236. https://doi.org/10.1364/AOP.361502
[15] National Institute of Standards and Technology. (2020). Post-Quantum Cryptography. NIST. https://csrc.nist.gov/Projects/post-quantum-cryptography
[16] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), 2702-2733. https://doi.org/10.1109/COMST.2019.2910750
[17] Statista. (2021). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. Statista. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
[18] Berman, D., Buczak, A., Chavis, J., & Corbett, C. (2019). A Survey of Deep Learning Methods for Cyber Security. Information, 10(4), 122. https://doi.org/10.3390/info10040122
[19] Kaloudi, N., & Li, J. (2020). The AI-Based Cyber Threat Landscape: A Survey. ACM Computing Surveys, 53(1), 1-34. https://doi.org/10.1145/3372823
[20] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

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 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308145|

[21] Gartner. (2020). The Future of Network Security Is in the Cloud. Gartner. https://www.gartner.com/en/documents/3982949/the-future-of-network-security-is-in-the-cloud

[22] Kumar, R., & Goyal, R. (2020). A framework for sustainable cybersecurity ecosystem. Journal of Information Security and Applications, 54, 102559. https://doi.org/10.1016/j.jisa.2020.102559

[23] Homles,D., & Burn, J (2022), The Definition Of Modern Zero Trust, https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/

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