iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VI **Month of publication:** June 2024

DOI: https://doi.org/10.22214/ijraset.2024.62457

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

Emerging Trends in Cloud Security: Zero Trust and SASE

Amarnath Ragula
Archer Daniels Midland, USA

Abstract: ***A lot has changed in the world of IT since cloud computing came along. Now, businesses can use shared tools and services whenever they need to. The old security models that were based on perimeters no longer work to protect cloud settings. This change has also made businesses more vulnerable in new ways. This article talks about two new security trends in the cloud: zero trust and secure access service edge (SASE). The idea behind zero trust security is that you shouldn't trust anyone or anything by default. Based on the principle of least privilege, every request for entry has to be checked out and given the go-ahead. SASE, on the other hand, is a cloud-based architecture that combines WAN and network security features to make it easy and safe to access cloud services. The article tells the truth about these technologies and how they will grow. It also talks about what they can do for businesses and how they will affect their security.***

Keywords: Zero Trust, Secure Access Service Edge (SASE), Cloud Security, Cyber Threats, Network Architecture

I. INTRODUCTION

Cloud computing has changed the way IT works by letting businesses use shared tools and services whenever they need to. A new study by Gartner says that end users will spend $591.8 billion on public cloud services around the world in 2023, which is 20.7% more than they did in 2022 [1]. The following table shows how spending on public cloud services is expected to rise from 2021 to 2023:

Year	Public Cloud Services (in billions)	Growth Rate
2021	$396	23.1%
2022	$490.3	23.8%
2023	$591.8	20.7%

Table 1: Worldwide Public Cloud Services End-User Spending Forecast (in billions) [1]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

Cloud services are becoming very popular because they have many benefits, such as being able to grow as needed and being cost-effective. Companies can quickly get the tools they need and only pay for what they use. This cuts down on capital costs and makes development and deployment more flexible [2]. In addition, cloud computing lets businesses use cutting-edge technologies like AI, machine learning, and big data analytics without having to spend a lot of money upfront [3].

But as cloud technologies grow in popularity, they also bring new security risks for companies. It's no longer possible to protect cloud environments with security models that are based on perimeters and believe that internal networks can be trusted but not external networks [4]. Some companies are concerned about the safety of their cloud-based data [5]. The Cloud Security Alliance (CSA) did a study that showed this. The main cloud security concerns that companies have brought up are shown in the table below:

Cloud Security Concern	Percentage of Organizations
Data Loss and Leakage	69%
Data Privacy and Confidentiality	66%
Accidental exposure of credentials	52%
Insider threat	50%
Insecure interfaces and APIs	48%

Table 2: Top Cloud Security Concerns [5]

These concerns about security are not unfounded. It was found in the 2022 Thales Data Threat Report that 45% of businesses have had a data breach in the cloud in the last 12 months [6]. IBM Security [7] also says that the average cost of a data breach will go up to $4.35 million in 2022.

Two new ideas that are becoming more common are Zero Trust and Secure Access Service Edge (SASE). These ideas are meant to help with these issues. If you want to be safe, zero trust means you shouldn't trust any person or device by default, no matter where they are or what network they're on [8]. WAN and network security features work together in SASE, which is a cloud-based architecture that makes it safe and quick to reach cloud resources [9].

In the next few years, Zero Trust and SASE are likely to become much more popular. A study by MarketsandMarkets says that the Zero Trust security market will grow at a CAGR of 19.9%, going from $15.6 billion in 2020 to $38.6 billion by 2025 [10]. Another market that will grow quickly is the SASE market, which will go from $2.2 billion in 2020 to $10.9 billion by 2025, or a CAGR of 37.4% [11].

Year	Zero Trust Security Market Size (In billions)	SASE Market Size (In billions)
2020	$15.6	$2.2
2025	$38.6	$10.9
CAGR	19.9%	37.4%

Table 3: Projected Growth of Zero Trust Security and SASE Markets [10,11]

The fast rise of Zero Trust and SASE is caused by several things. Traditional security methods aren't working anymore because cyber risks are getting smarter and more complicated, and attacks can reach more places now that more people work from home and use the cloud [12]. As companies get used to having workers in different places, safe remote access has also become very important [13]. In addition, the rules are changing. New data protection laws and business standards require more stringent security measures [14].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

Because cyber threats are getting smarter and more people are using cloud computing, companies need to adopt new security ideas like Zero Trust and SASE. Businesses can make their security better, lower their risk of data hacks, and give their workers safe ways to work from home by following these new trends.

II. ZERO TRUST

According to the zero trust theory, one shouldn't trust any person or device by default, no matter where they are or what network they're on [15]. Each access request is instead carefully examined and granted based on the idea of least privilege. In the Zero Trust model, there are three key ideas: clearly verify, use least privilege access, and assume breach [16]. Businesses can make it harder for hackers to get into their systems and increase the safety of their data by implementing Zero Trust.

Zero Trust is what the National Institute of Standards and Technology (NIST) calls "evolving cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources" [17]. As explained by NIST, the main ideas behind Zero Trust are:

1) All sources of data and computer services are thought of as resources.
2) No matter where the network is located, all information is safe.
3) Each session gives the user access to a different set of enterprise tools.
4) Dynamic policy decides who can access resources based on things like the client's name, the application, and the asset being requested, as well as other behavioral factors.
5) The company keeps an eye on and rates the safety and purity of all its owned and linked assets.
6) Authentication and authorization for all resources are dynamic and must be strictly followed before entry is granted.
7) The company gathers as much data as it can about its current assets, network infrastructure, and contacts, which it then uses to boost its security [17].

A study by the National Institute of Standards and Technology (NIST) found that companies that used Zero Trust principles had 50% fewer security issues than companies that used traditional security models based on perimeters [18]. A study of 250 companies from different fields found that after they switched to Zero Trust, the average number of security events per year dropped from 28 to 14. The line below shows how many security events happened before and after Zero Trust was put in place:

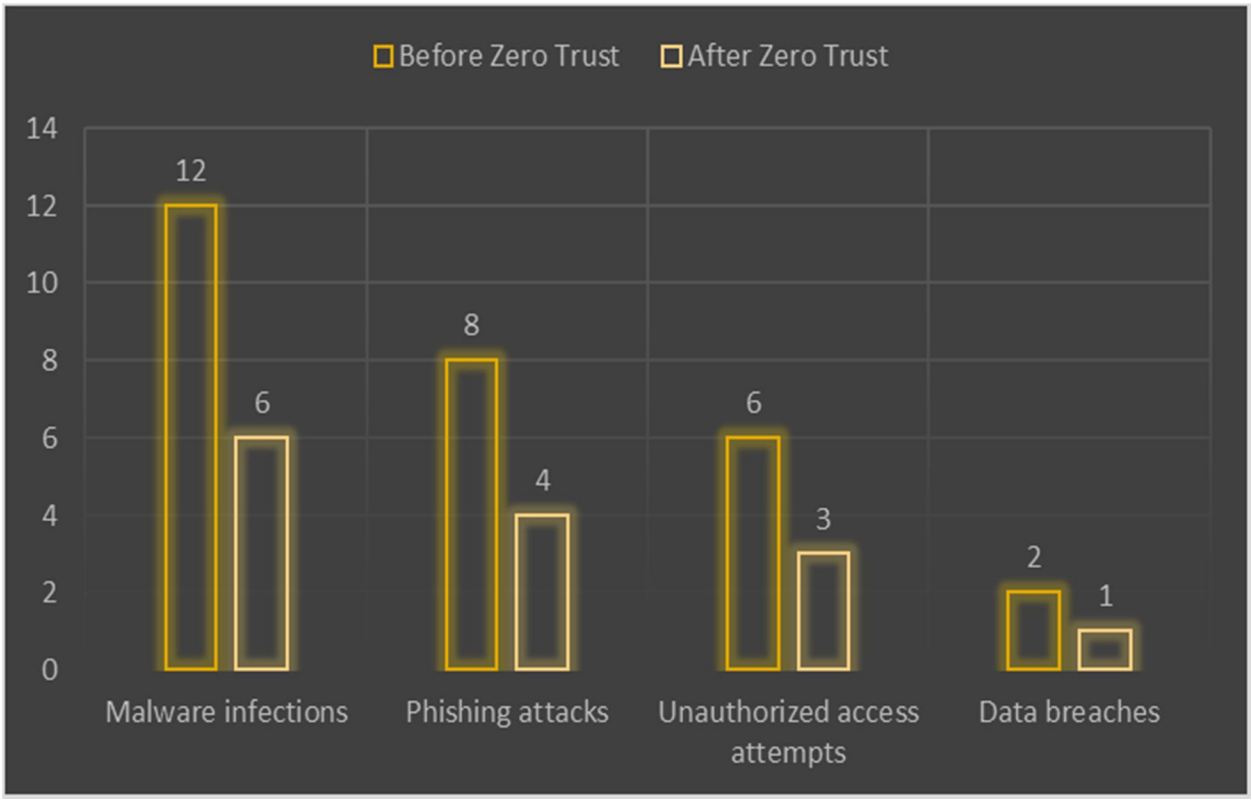


Fig. 1: Average Number of Security Incidents per Year Before and After Zero Trust Adoption [18]

It was also shown in the study how important it is for Zero Trust settings to always be tracking and evaluating risk in real-time. As part of their Zero Trust strategy, companies that used ongoing tracking and risk assessment had 30% fewer security incidents than companies that didn't [18]. How tracking and evaluating risks all the time have changed the number of security events is shown in the table below:

Zero Trust Implementation	Average Security Incidents per Year
Without continuous monitoring	14
With continuous monitoring	10
Percentage reduction	30%

Table 4: Impact of Continuous Monitoring and Risk Assessment on Security Incidents [18]

The Cloud Security Alliance (CSA) also did a study [19] that showed 61% of companies plan to use Zero Trust in the next 12 months. Based on the vote, these were the best things about Zero Trust:

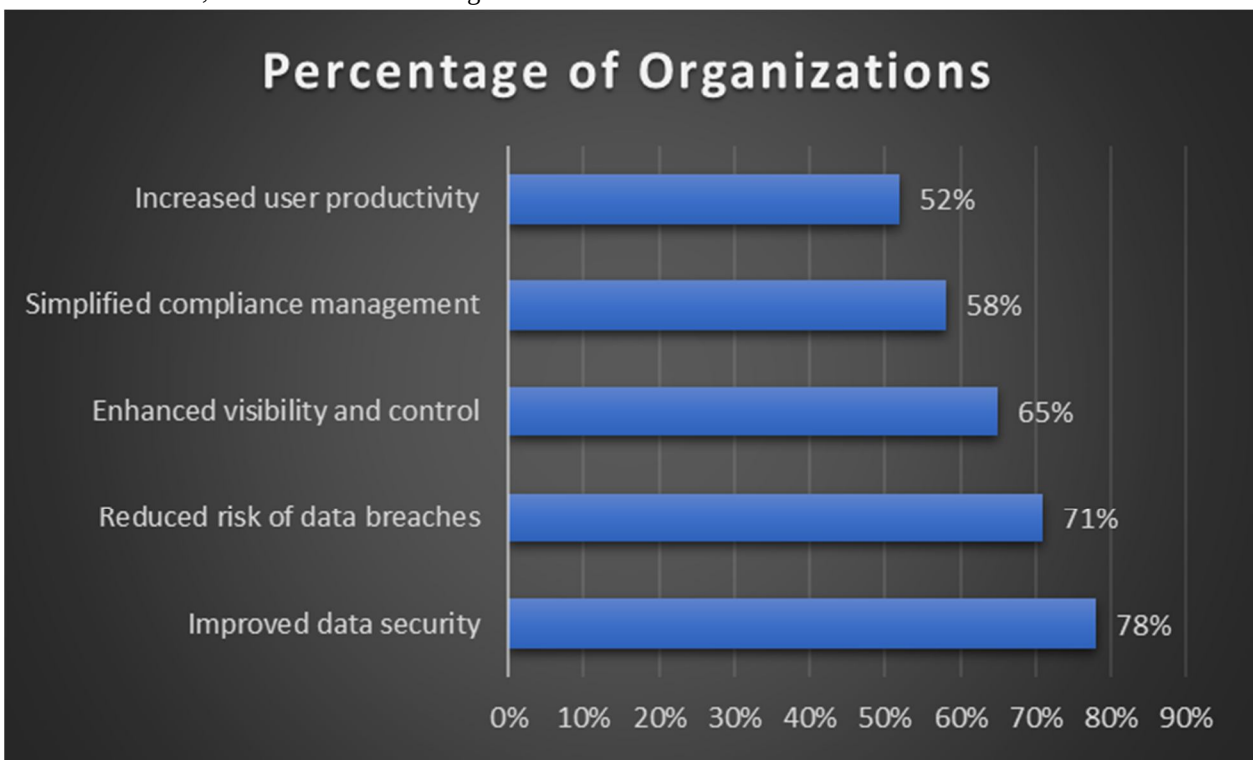


Fig. 2: Organizations' Perceived Top Benefits of Zero Trust [19]

To use Zero Trust, a company must completely change how it thinks about and handles security. The Zero Trust principles are put into action by a mix of technologies, methods, and rules that work together [20]. The following are some important parts of a Zero Trust architecture:

a) Multifactor authentication (MFA): It is a way to make sure that a person is who they say they are by using more than one method, like passwords, biometrics, or hardware tokens.
b) Identity and Access Management (IAM): It is the process of managing users' identities and their rights to access resources based on the concept of least privilege.
c) Microsegmentation: Breaking the network up into smaller, separate pieces to stop people from moving laterally and make a breach less dangerous.
d) Continuous Monitoring and Risk Assessment: Always keeping an eye on user behavior, gadget health, and network traffic to spot strange things and evaluate risk in real time.

e) Secure Access: Using technologies like Virtual Private Networks (VPNs) or Zero Trust Network Access (ZTNA), secure access means giving users safe, authorized access to resources no matter where they are or what device they're using.

f) Encryption: Using strong encryption methods to protect data while it is at rest and while it is being sent [20].

To reach Zero Trust, you need to carefully plan your steps, carry them out, and keep making them better. First, businesses should look at their current security, figure out what data and assets are most important, and set their Zero Trust goals and plan [21]. Then, they should decide which Zero Trust controls to put in place first based on risk and business effect, starting with the most important assets and use cases [22].

To make sure the Zero Trust rules work and to adapt to new threats and business needs [23], they must also be constantly tested, monitored, and improved. Key performance indicators (KPIs) and metrics should be set up by organizations to track the success of their Zero Trust efforts and show stakeholders the return on investment (ROI) [24].

Businesses will likely use Zero Trust a lot more in the next few years as they learn how well it protects their current IT systems. If businesses follow the Zero Trust principles, they can make a more thorough and adaptable security system that can keep their data and assets safe even as online threats change.

III. SECURE ACCESS SERVICE EDGE (SASE)

SASE is a cloud-based architecture that combines WAN and network security features to make it easy and safe to use cloud services [25]. Some of the security services that SASE offers through the cloud are Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), and Firewall-as-a-Service (FWaaS). These are all held together on a single platform.

Dell'Oro Group says the SASE market will grow at a rate of 116% per year from 2020 to 2025, reaching $5.1 billion by that year [26]. The table below shows how much the SASE market is likely to grow.

Year	SASE Market Size (in billions)
2020	$0.8
2021	$1.7
2022	$2.8
2023	$3.7
2024	$4.5
2025	$5.1

Table 5: Projected Growth of the SASE Market [26]

SASE has many perks, such as making management easier, increasing performance, and making security stronger. Based on a survey by Gartner [27], 40% of companies will have adopted or will adopt SASE by the end of 2024. The study also found the main reasons why people use SASE:

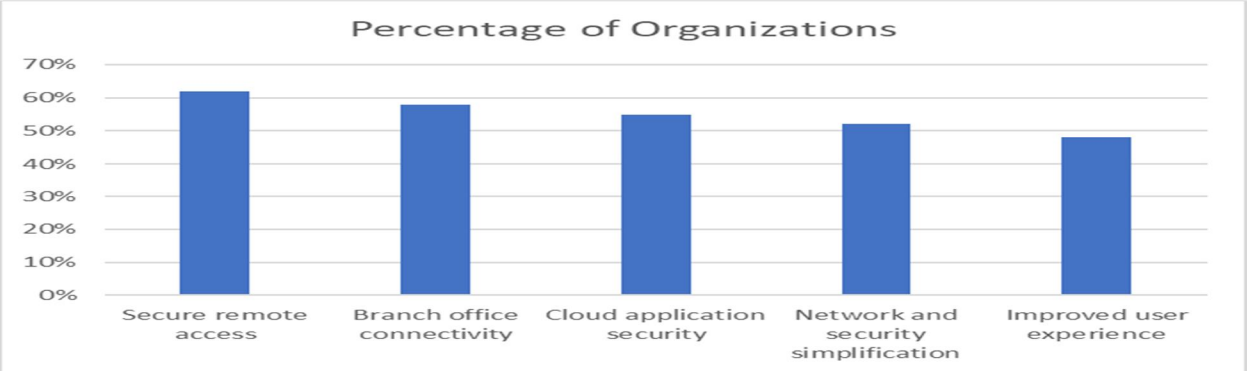


Fig. 3: Top Drivers for SASE Adoption [27]

According to Gartner, The Most Important Parts of a Sase Design Are [28]

1) Software-defined wide area networking, or SD-WAN, connects people, devices, and apps in a way that is based on policies and changes over time.
2) Zero Trust Network Access (ZTNA) lets users safely connect to apps based on their name, the situation, and the rules, without leaving the network open.
3) A cloud access security broker (CASB) makes sure that cloud services and data follow security rules. These rules include controlling access, keeping data safe, and stopping threats.
4) SWG protects users from web-based risks like malware, phishing, and content that isn't supposed to be there.
5) FWaaS, or firewall-as-a-service, is a way to get next-generation firewall features like application control, intrusion protection, and threat intelligence through the cloud.
6) Cloud Security Posture Management (CSPM) is the process of constantly checking for and fixing mistakes and compliance risks in cloud settings [28].

By using SASE, businesses can make sure that internet users and branch offices can easily and safely get to cloud resources. There was a case study by Palo Alto Networks [29] about a global manufacturing company that showed how SASE could help them. This is what the company, which has 10,000 employees in 50 places, got from SASE:

- 70% less difficult to set up and protect a network
- The application works 50% better now.
- Setting up new branch offices 80% faster
- By 60%, security events related to online access went down.

Forrester also found in a study that putting SASE into place can give businesses a 139% return on their investment (ROI) over three years [30]. The report also talked about the following affects that could be tracked:

- $2.5 million saved on IT costs
- $1.8 million in increased user productivity
- Higher levels of security: $1.2 million
- $0.8 million for easier compliance handling

Putting SASE into place needs a plan that fits with the business goals and IT roadmap of the company. Some important things to think about when adopting SASE are [31]:

- The present network and security architecture is being looked at to find holes and chances for SASE integration.
- Defining the SASE use cases and standards based on what the company needs, like working from home, moving to the cloud, or connecting branches.
- Looking at SASE providers and solutions based on what they can do, how well they work, how much space they take up, and how easy they are to connect to other systems.
- Plan to roll out SASE in stages, starting with the most important use cases and working your way up to all people, devices, and apps.
- Setting up rules, steps, and measurements to control and keep an eye on the SASE implementation and find out how well it's working and the return on investment (ROI).
- Giving users and managers training and help to make sure that SASE features are adopted smoothly and are used to their fullest [31].

Businesses will likely use SASE more as they learn how it can make their network and security plans easier while still letting them quickly and easily access cloud resources. SASE can help companies make their networks and security better, give users a better experience, and lower the costs of doing business the old way.

IV. CONCLUSION

With more companies moving to the cloud, Zero Trust and SASE will be needed more and more to make sure that cloud systems are safe. Cyber threats are getting smarter, so businesses need safer remote access and easier ways to set up their networks and protection. For businesses to make their protection better, these new trends are a must.

Businesses can make it much harder for hackers to get into their systems and get data stolen by following Zero Trust principles and using SASE. This also makes it easier for employees to access cloud resources safely.

Zero Trust offers a complete and flexible security system that constantly checks and allows entry based on a real-time assessment of risk. One other option is SASE, which offers a unified network and security through the cloud. This lets you access cloud resources safely and efficiently from anywhere.

A number of research and case studies have shown that using Zero Trust and SASE has big and measurable benefits. It's possible for businesses to cut down on security events by at least 50%, speed up the deployment of branch offices by 80%, and get a 139% return on investment (ROI) over three years.

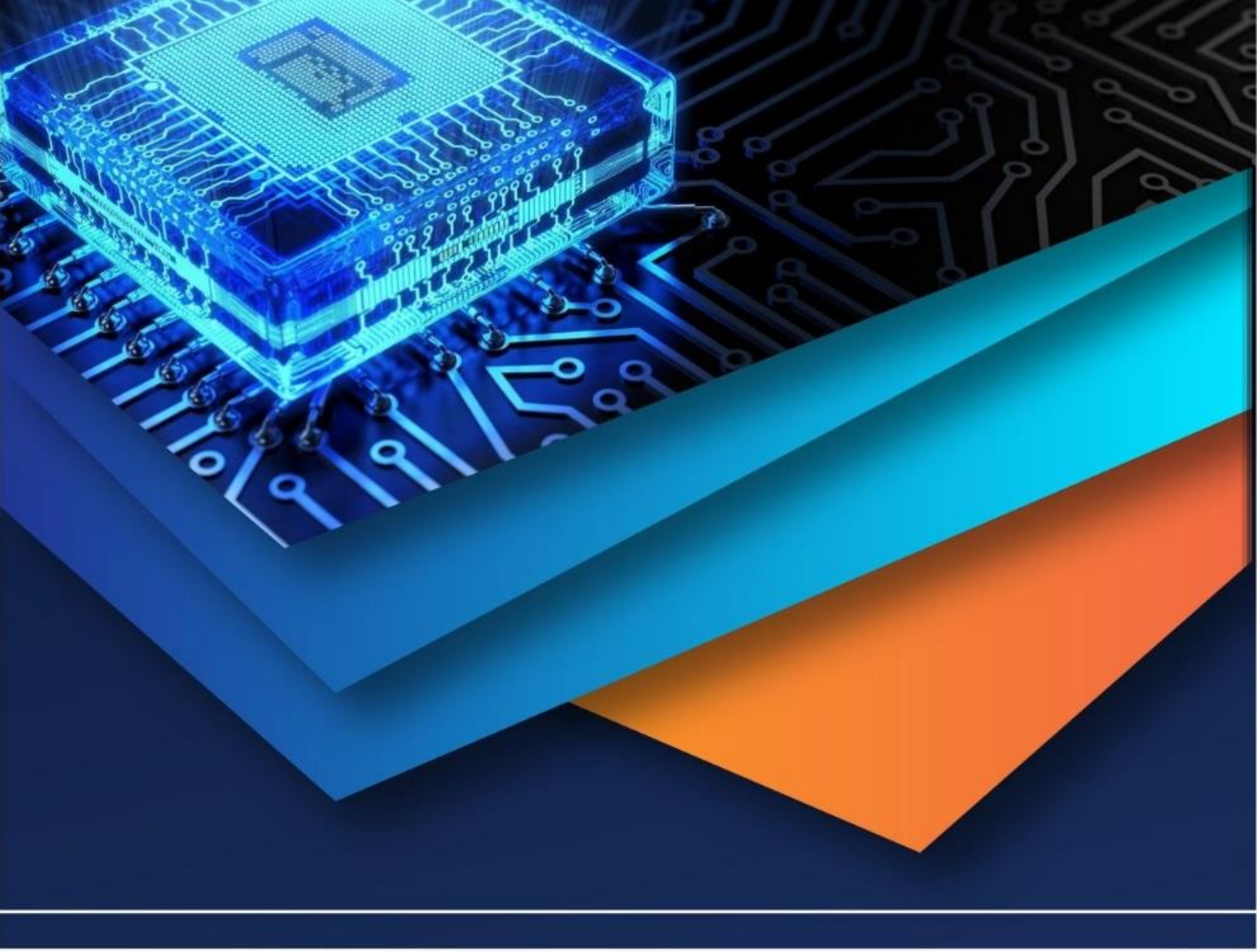
But putting Zero Trust and SASE into place isn't a one-time thing; it's a journey that needs constant dedication, investment, and improvement. Adopting Zero Trust and SASE should be seen by companies as a strategy project that fits with their overall business goals and risk management plans. They should also work with reputable service and vendor providers who can give them the knowledge, help, and solutions they need to be successful on this trip.

Zero Trust and SASE will become more important for organizations to protect their assets and enable their digital transformation as the use of cloud computing continues to grow and cyber threats continue to change. By embracing these new trends, organizations can build a more resilient, agile, and secure foundation for their future growth and success.

REFERENCES

[1] Gartner, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 20.7% in 2023," 2023. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-20-percent-in-2023. [Accessed: May 10, 2024].
[2] M. Armbrust, et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, 2010.
[3] S. Marston, et al., "Cloud computing — The business perspective," Decision Support Systems, vol. 51, no. 1, pp. 176-189, 2011.
[4] J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, 2010.
[5] Cloud Security Alliance, "Top Threats to Cloud Computing: The Egregious 11," 2020. [Online]. Available: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/. [Accessed: May 10, 2024].
[6] Thales, "2022 Thales Data Threat Report," 2022. [Online]. Available: https://cpl.thalesgroup.com/data-threat-report. [Accessed: May 10, 2024].
[7] IBM Security, "Cost of a Data Breach Report 2022," 2022. [Online]. Available: https://www.ibm.com/reports/data-breach. [Accessed: May 10, 2024].
[8] NIST, "Zero Trust Architecture," NIST Special Publication 800-207, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. [Accessed: May 10, 2024].
[9] Gartner, "The Future of Network Security Is in the Cloud," 2019. [Online]. Available: https://www.gartner.com/en/documents/3957717/the-future-of-network-security-is-in-the-cloud. [Accessed: May 10, 2024].
[10] MarketsandMarkets, "Zero Trust Security Market by Solution Type (Data Security, Endpoint Security, API Security, Security Analytics, Security Policy Management), Deployment Type, Authentication Type, Organization Size, Vertical, and Region - Global Forecast to 2025," 2020. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/zero-trust-security-market-2782835.html. [Accessed: May 10, 2024].
[11] MarketsandMarkets, "Secure Access Service Edge (SASE) Market by Offering (Network as a Service and Security as a Service), Organization Size, Vertical (BFSI, IT & Telecom, Healthcare, and Manufacturing), and Region - Global Forecast to 2025," 2020. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/secure-access-service-edge-market-220190440.html. [Accessed: May 10, 2024].
[12] Verizon, "2022 Data Breach Investigations Report," 2022. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/. [Accessed: May 10, 2024].
[13] Gartner, "Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021," 2021. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2021-06-22-gartner-forecasts-51-percent-of-global-knowledge-workers-will-be-remote-by-2021. [Accessed: May 10, 2024].
[14] Deloitte, "The future of cyber survey 2021," 2021. [Online]. Available: https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html. [Accessed: May 10, 2024].
[15] [NIST, "Zero Trust Architecture," NIST Special Publication 800-207, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. [Accessed: May 10, 2024].
[16] Forrester, "The Zero Trust eXtended (ZTX) Ecosystem," 2018. [Online]. Available: https://www.forrester.com/report/The+Zero+Trust+eXtended+ZTX+Ecosystem/-/E-RES137210. [Accessed: May 10, 2024].
[17] NIST, "Zero Trust Architecture," NIST Special Publication 800-207, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. [Accessed: May 10, 2024].
[18] NIST, "Implementing a Zero Trust Architecture," NIST Cybersecurity White Paper, 2021. [Online]. Available: https://www.nist.gov/publications/implementing-zero-trust-architecture. [Accessed: May 10, 2024].
[19] Cloud Security Alliance, "Zero Trust Adoption Report," 2022. [Online]. Available: https://cloudsecurityalliance.org/artifacts/zero-trust-adoption-report/. [Accessed: May 10, 2024].
[20] Microsoft, "Zero Trust Maturity Model," 2020. [Online]. Available: https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model. [Accessed: May 10, 2024].
[21] Palo Alto Networks, "The Ultimate Guide to Zero Trust," 2021. [Online]. Available: https://www.paloaltonetworks.com/resources/guides/the-ultimate-guide-to-zero-trust. [Accessed: May 10, 2024].
[22] Okta, "The Eight-Step Guide to Implementing Zero Trust," 2021. [Online]. Available: https://www.okta.com/resources/whitepaper-the-eight-step-guide-to-implementing-zero-trust/. [Accessed: May 10, 2024].

[23] Google Cloud, "BeyondCorp: The Complete Guide to Zero Trust Security," 2021. [Online]. Available: https://cloud.google.com/beyondcorp. [Accessed: May 10, 2024].
[24] Zscaler, "The Definitive Guide to Zero Trust Security," 2021. [Online]. Available: https://www.zscaler.com/resources/ebooks/definitive-guide-to-zero-trust-security.pdf. [Accessed: May 10, 2024].
[25] Gartner, "The Future of Network Security Is in the Cloud," 2019. [Online]. Available: https://www.gartner.com/en/documents/3957717/the-future-of-network-security-is-in-the-cloud. [Accessed: May 10, 2024].
[26] Dell'Oro Group, "SASE Market to Reach $5.1 Billion by 2025, According to Dell'Oro Group," 2021. [Online]. Available: https://www.delloro.com/news/sase-market-to-reach-5-1-billion-by-2025-according-to-delloro-group/. [Accessed: May 10, 2024].
[27] Gartner, "Gartner Survey Reveals 40% of Organizations Have Adopted or Plan to Adopt SASE by 2024," 2022. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2022-06-15-gartner-survey-reveals-40-percent-of-organizations-have-adopted-or-plan-to-adopt-sase-by-2024. [Accessed: May 10, 2024].
[28] Gartner, "The Future of Network Security Is in the Cloud," 2019. [Online]. Available: https://www.gartner.com/en/documents/3957717/the-future-of-network-security-is-in-the-cloud. [Accessed: May 10, 2024].
[29] [29] Palo Alto Networks, "Global Manufacturing Company Achieves Secure Cloud Transformation with SASE," 2023. [Online]. Available: https://www.paloaltonetworks.com/resources/case-studies/global-manufacturing-company-achieves-secure-cloud-transformation-with-sase. [Accessed: May 10, 2024].
[30] Forrester, "The Total Economic Impact of Palo Alto Networks Prisma Access," 2021. [Online]. Available: https://www.paloaltonetworks.com/resources/whitepapers/total-economic-impact-of-prisma-access. [Accessed: May 10, 2024].
[31] Cisco, "SASE for Dummies," 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/sase-for-dummies.html. [Accessed: May 10, 2024].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY