FORTINET

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Consistent Convergence of Networking and Security to Secure the Hybrid Workforce

A DSCI-FORTINET Point of View Paper

August 2023

Objective

As organizations adapt to a new normal in the post-pandemic era, hybrid work is expected to stay. The traditional office-based work structure has been transformed with the blend of remote and in-person work offering flexibility and productivity gains. However, it poses significant challenges for organizations in swiftly establishing robust and scalable access for their remote workforce without introducing complexity or sacrificing end-user performance. Furthermore, users in remote and branch offices require the same level of network performance and security as those in central locations.

IT leaders must develop strategies that protect users, regardless of their location or device, from an array of threats ranging from malware infections to unauthorized access. It has been well acknowledged that the need for secure and reliable connections from home and mobile devices has presented new obstacles for enterprise networking. The emergence of the Secure Access Service Edge (SASE) architecture offers a cloud-based solution that integrates network and security services enabling employees to connect remotely in a fast, scalable, and secure manner.

This paper explores the evolution of Internet and Enterprise Networking in the era of cloud computing. As organizations navigate the future of networking, direct access to cloud services and the convergence of secure edges represent crucial pathways to success in the digital era.

It expands on the shifting network and security landscape, identifies gaps within the existing security infrastructure, and provides a roadmap for organizations to safeguard them in the face of evolving digitalization context. The position paper builds on the following sections:

- Analysis of the pace of rapid digitalization; the challenges for the networking and security teams to secure the hybrid workforce.
- Security perspectives for existing infrastructures and their implications for organizations.
- Comprehending the security paradigms; making sense of WAN transformation and the convergence of networking and security.
- The SASE framework; a unified approach to security [Drivers, Components and Use Cases].
- The Roadmap for SASE adoption; strategies and considerations.

Target Audience

This position paper is tailored for security professionals who are seeking a comprehensive understanding of trends driving the convergence of networking and security. It will equip technical leaders (CISO, CTOs, CIOs) and security teams with knowledge and insights to navigate the challenges and harness the benefits of this transformative shift.

Contents

From Leader's Desk

Modern networks are dynamic and expansive, constantly evolving to support digital acceleration, work from anywhere (WFA) strategies, and top business priorities. Converging networking and security delivers a reliable user experience, improves security, reduces complexities, and enhances efficiency.

SD-WAN proves instrumental in supporting organizations across diverse sectors in their digital acceleration journeys. It enables implementation of stringent controls within data centers and the cloud, establishes secure connectivity across branches, campuses, and manufacturing facilities, and empowers enterprises to address application-steering demands. Furthermore, organizations are making strides by integrating secure remote access through SASE. SD-WAN serves as the unifying force that amalgamates security and networking solutions, streamlining processes, enhancing security effectiveness, and ensuring a reliable user experience across expansive networks in today's digital landscape.

-Vishak Raman, Vice President of Sales, India, SAARC, SEAHK & ANZ at Fortinet

As we witness rapid digitization enabled by a wide range of emerging technologies, fueled by innovation and architectural interventions, and enabled by cloud and mobility, it is critical to examine how workspaces, connectivity, infrastructure, and applications are transforming. Cloud-first strategy, data-enhanced products and services, mobility and device design, open data ecosystem, multiplying third-party interfaces and APIs, and increased transaction volume place the network at the centre of the security discussion. For a secure hybrid workforce, a cutting-edge network is vital. This includes ensuring secure access, safeguarding sensitive data, mitigating threats across diverse endpoints, and enabling secure connectivity regardless of the location or device.

The SASE architectural approach promises to unify security and networking across enterprise, branch, and cloud networks while improving controllability, introducing flexibility, reducing management complexity, and improving user experience. This paper examines the nuances and components involved in this architectural evolution and recommends a roadmap for converging security and networking.

-Vinayak Godse, CEO, Data Security Council of India (DSCI)

Background

1.1 Evolving Digital Landscape

Our world is going through a rapid digital transformation. New technologies, from Augmented Reality (AR) to Artificial Intelligence (AI), are changing the way we live. Driven by agility, connectivity, and availability at its core, it has paved new pathways for businesses to improve performance. In order to address the effects of globalization and the resulting economic forces, organizations have realigned their Information & Communications Technology (ICT) strategic goals to source lower-cost, flexible, reliable and resilient economical solutions/strategies.

1.2 The Rise of Cloud Computing

The emergence of cloud computing has opened new possibilities for delivering content and resources through various service models, such as Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service. This shift marks a departure from the traditional model of “computer as a product” to “computing as a service” supplied to consumers through the internet from the cloud or large-scale data centers. It has also brought a fundamental shift in the way businesses operate, enabling them to access computing resources and services over the internet rather than having to build and maintain their own IT infrastructure. This has led to increased efficiency, scalability, and agility, allowing businesses to respond more quickly to changing market conditions and customer needs.

However, cloud computing is not immune to the challenges posed by the ever-evolving digital world. These challenges include:

- Analysis of the pace of rapid digitalization; the challenges for the networking and security teams to secure the hybrid workforce.
- Securit perspectives for existing infrastructures and their implications for organizations.
- Comprehending the security paradigms; making sense of WAN transformation and the convergence of networking and security.
- The SASE framework; a unified approach to security [drivers, components and use cases].
- The roadmap for SASE adoption; strategies and considerations.

Figure 1: Challenges of the digital landscape

Effective cloud security governance requires a holistic approach that takes into account the entire cloud ecosystem, including the cloud provider, the business, and any third-party vendors or partners. By implementing robust cloud security governance practices, businesses can mitigate the security risks associated with cloud computing and reap the benefits of this transformative technology[1].

1.3 The Rise of Hybrid and Remote Offices

The trend towards remote offices and branch offices is continuing to grow as companies expand and acquire new locations. Secondly, employees returning to the office after the pandemic has caused a shift towards hybrid work models, with many companies embracing branch office solutions to accommodate a more dispersed workforce. This presents a challenge for IT departments, which need to ensure that remote workers and branch office employees are able to access the resources they need securely and reliably.

> “As companies decentralize, a new approach to networking and security is essential to support remote workers and branch offices.”

1 The debate around cloud adoption is multi-faceted. Businesses should consider the advantages, hazards, and impacts of the cloud on their operations. Organizational maturity, cultural aspects, regional legislation, distribution of business portfolio, socio-technical factors such as confidentiality, soaring costs, and control are amongst other elements that needs to be factored in while adopting the cloud.

With the increasing popularity of Direct Internet Access (DIA) links and Virtual Private Networks (VPNs), IT departments are finding new ways to connect remote offices to the main office while maintaining security and data privacy.

Additionally, with the proliferation of cloud-based applications and services, remote workers and branch office employees need reliable and secure access to cloud resources as well. As a result, IT departments are turning to solutions such as Software-Defined WAN (SD-WAN) and Cloud Access Security Brokers (CASBs) to ensure that remote workers and branch offices have the connectivity and security they need to be productive and effective.

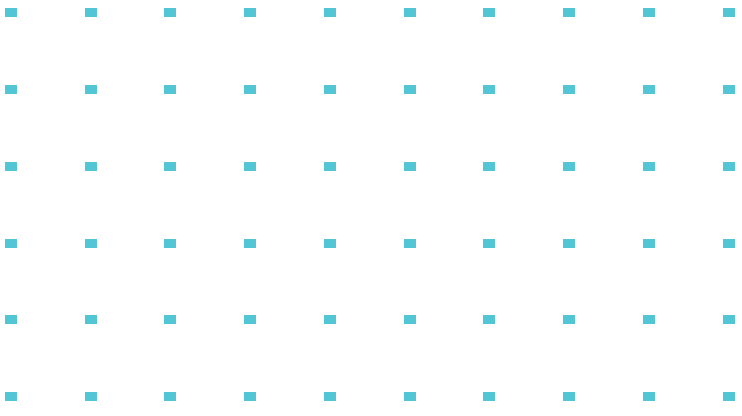
1.4 User Mobility

The prevalence of the culture of BYOD and the utilization of mobile devices for work is fostering work from home environment. Remote work, telecommuting, and workplace flexibility have become a norm where users utilize corporate or personal devices to access the corporate network via a VPN or the internet to perform their job functions.

1.5 Increasing Traffic

Modern-day applications are data-intensive resulting in a significant increase in network traffic. This surge is creating a strain on existing network infrastructure and centralized security processes, resulting in reduced performance, decreased productivity, and poor user experience.

In today's workforce, employees need to access private applications located in a data center or multi-cloud environment. However, these applications may not always be accessible within the confines of an office or branch site, and employees may not have immediate IT assistance. To address this, organizations need to find ways to ensure that employees working from anywhere have consistent and reliable access to corporate resources, while still making use of existing investments.



Grappling with Security & Networking Challenges Cropping in Post-Pandemic Environment

In the post-pandemic phase, where employees prefer a blended remote and office work environment, it is increasingly difficult to align the required security tools and techniques, thus, exposing gaps in the legacy infrastructures. Apart from the aforementioned challenges of digitalisation, complete migration to the cloud for enterprises that are operating with data centres might not be an optimal approach.

Many enterprises have embraced a cloud-first strategy for new systems or implemented certain Software-as-a-Service (SaaS) solutions with success, but many are having trouble realizing the full benefits of migrating the majority of their enterprise systems to the cloud.

Businesses often make the mistake of assuming that simply transferring their IT systems to the cloud is enough to fully benefit from cloud infrastructure. However, the advantages of the cloud cannot be achieved by just "lifting and shifting" traditional applications. In fact, in some cases, this approach can result in more complex, expensive, and inconvenient IT architectures. Here are some reasons why:

- **Legacy systems:** The development of the current business applications was made possible by traditional IT paradigms. Therefore, these applications are often rigid and set up in a small number of data centers for fixed capacity. Migration will not help them to assimilate the dynamic characteristics of the cloud. These systems may be difficult or impossible to migrate to the cloud without significant reengineering, which can be time-consuming and costly.

- **Organizational culture and skills:** Some organizations may not have the culture or skills necessary to manage a complete migration to the cloud. This may be due to factors such as a lack of cloud expertise, resistance to change, or a preference for on-premises systems.

- **Cost considerations:** While cloud computing can be cost-effective for some workloads, it may not be the most cost-effective option for all workloads. Some workloads may be more cost friendly to run on-premises or in a hybrid cloud environment.

- **Latency and network connectivity:** Workloads that require low latency or high network bandwidth, may not be well-suited for a cloud environment, especially if they are geographically dispersed. In such cases, it may be more effective to keep the workload on-premises or in a hybrid cloud environment that combines on premises resources with cloud resources.

  For example, applications that need real-time data processing may require extremely low latency and high bandwidth connections that are difficult to achieve in a cloud environment due to the inherent limitations of the public internet. Similarly, applications that rely on large-scale data analytics or machine learning may require significant computing resources that are better suited for on-premises or hybrid cloud environments. By keeping certain workloads on-premises or in a hybrid cloud environment, organizations can ensure that they have the necessary network connectivity and resources to meet their specific performance requirements, while still leveraging the benefits of cloud-based services for other workloads.

- **Data sovereignty:** Organizations may have concerns about the security of their data in the cloud, especially if they do not have control over the cloud infrastructure. Therefore, preferring to keep it within their data centers.

- **Data privacy and security concerns:** Organizations may have regulatory or compliance requirements that restrict the movement of certain data to the cloud.

The Future of Networking and Security: An Evolutionary Perspective

The trend in networking and security solutions is moving from using various, separate point products to adopting integrated cloud-based networking and security platforms. This change is driven by businesses' growing need for flexibility and control over where and how they deploy these services. They require the ability to secure and manage internet access, regulate cloud application usage, and protect remote users.

3.1 Understanding the Evolution of WAN Transformation

WAN transformation journey is a key instrument to understand the forces driving networking and security transformation.

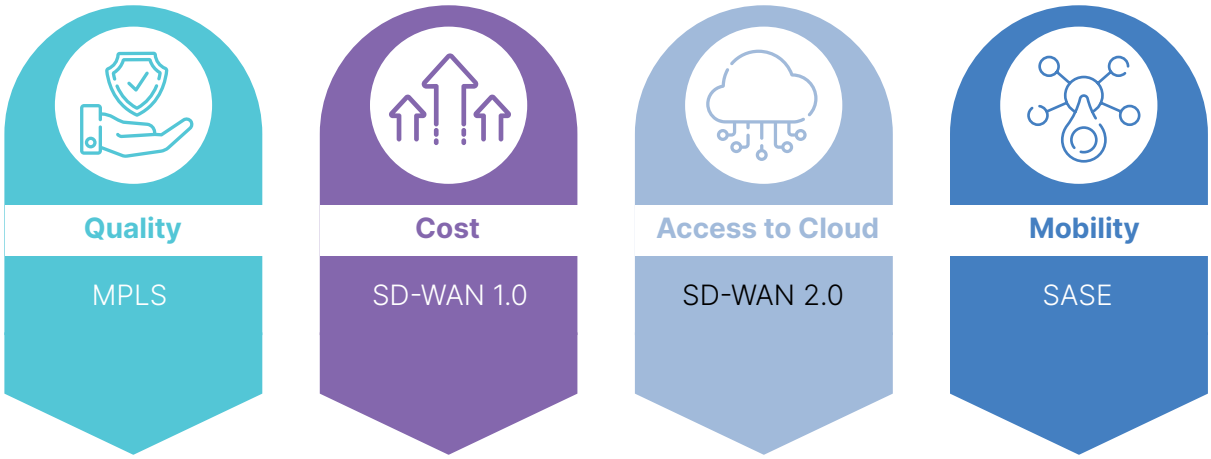


Figure 2: Drivers of WAN transformation

Since 2000, using MPLS has been the de facto approach to building corporate WANs. Yet starting in 2013, a wave of migration to Software-Defined WAN (SD-WAN) began as MPLS was expensive and had limited flexibility. The MPLS networks and broadband internet connections were reused in initial SD-WAN deployments at branch offices of large corporations.

Over time, SD-WAN was successful in increasing network availability and manageability while reducing costs due to dynamic path selection and application visibility. Unfortunately, the early SD-WAN development was constrained by the unpredictable nature of the internet.

The movement of more businesses and applications towards SaaS translates to the wider adoption of the cloud. As a result, the public cloud is now receiving enterprise traffic from headquarters.

Enhancements to enterprise WAN, known as SD-WAN 2.0, were driven by direct cloud access. In order to speed up the adjustments, CSPs either directly connect their networks to ISPs' networks in Internet Exchange Points (IXPs) or give ISPs access to the connections to the closest Point of presence (PoPs). ISPs offer premium connectivity to public clouds that customers can purchase.

Post pandemic, the developments in enterprise WAN are currently being driven by mobility at its core due to the increased number of employees working in hybrid environments. Earlier, VPN was deployed to securely connect to the headquarters. It is based on an out-of-date "hub-and-spoke" architecture that directs traffic from cloud applications back to an on-premises data center for filtering and security checks. The bottlenecks caused by the growing loads of cloud applications users are now experiencing performance issues.

As businesses migrate their data centers to the cloud, sending traffic to a hub site may not be the most cost-effective or efficient option for roaming or branch users needing access to corporate resources in the cloud. Local breakout can be used to directly send traffic from a branch or remote office to the cloud destination, reducing WAN bandwidth usage and improving user experience by lowering latency.

Criticality of SD-WAN

SD-WAN integrates and optimizes traditional WAN technologies such as MPLS and broadband Internet connections. This integration enables businesses to effectively route network traffic to multiple remote branch locations while also providing improved monitoring and management capabilities. In real-time, SD-WAN can monitor network traffic across all available links and dynamically select the best route for each data packet, ensuring optimal performance throughout the network.

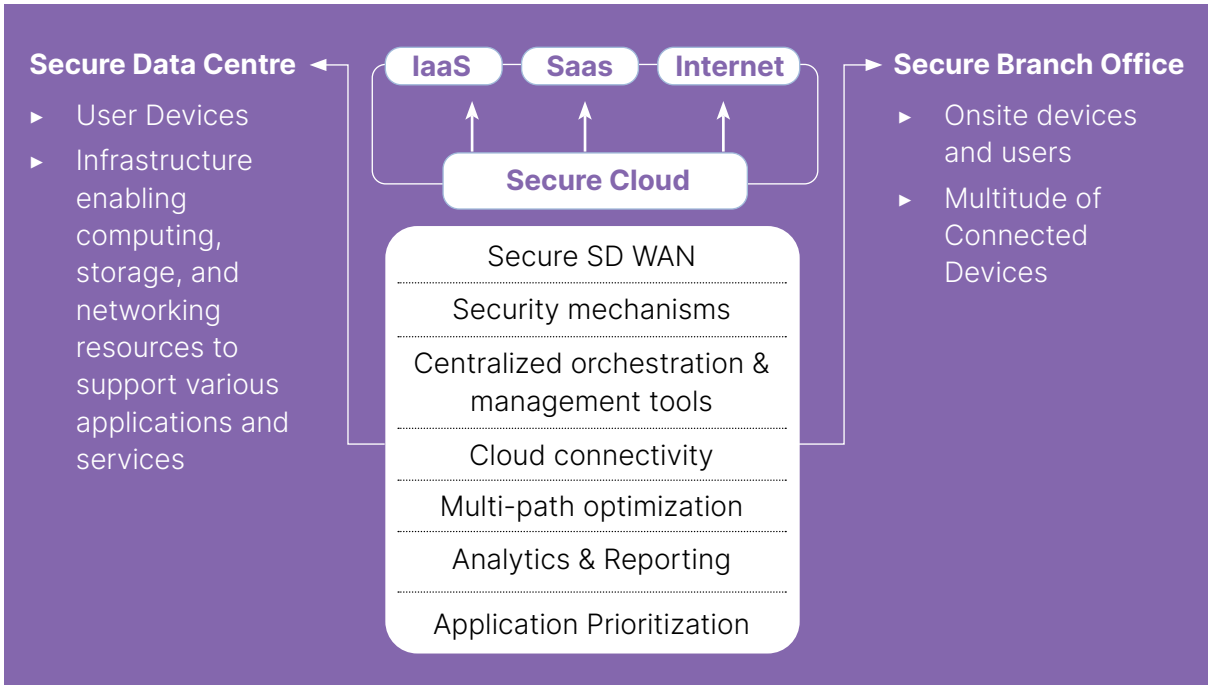


Figure 3: SD WAN as a critical component of SASE to secure Cloud, Data Centre & Branch Edge Network

Zero Trust: "Verify Everything, Trust No-one"

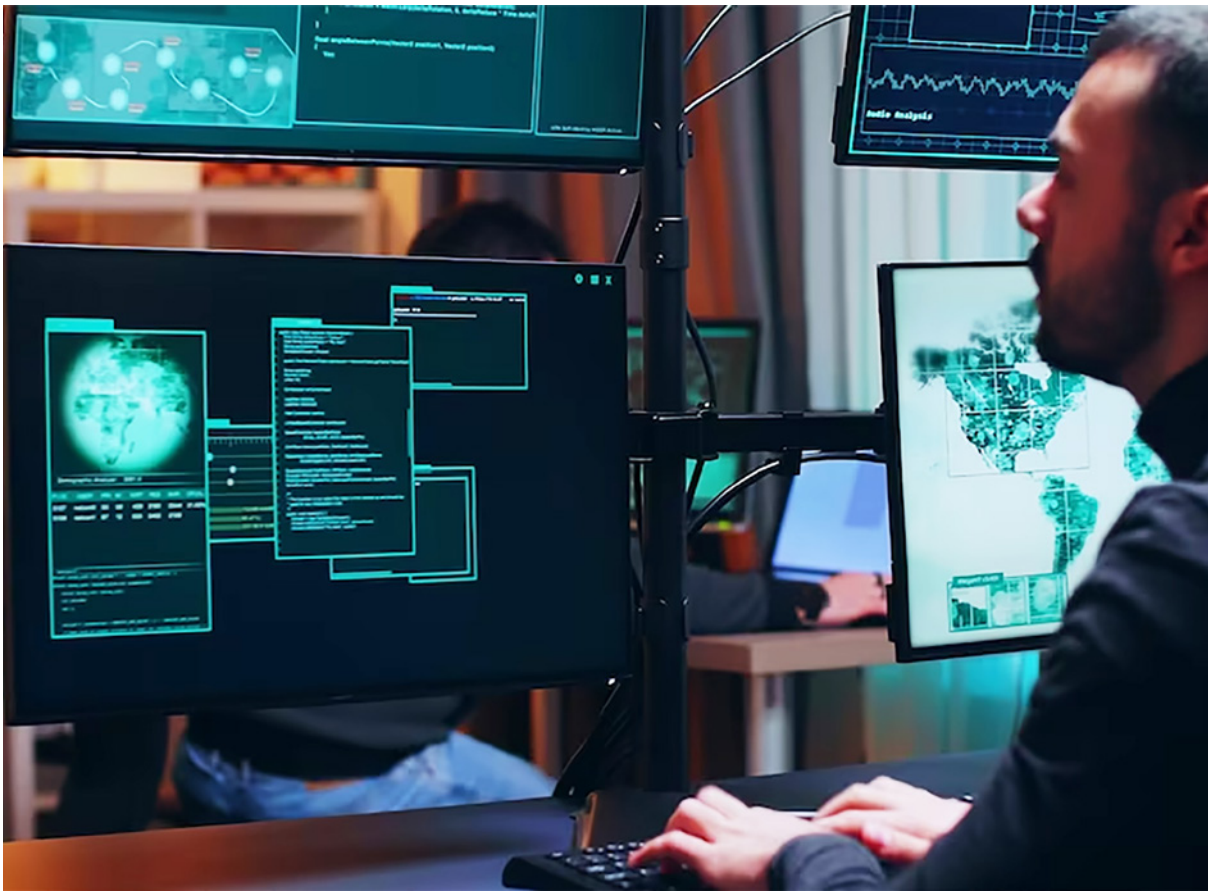
The use of VPN technologies can lead to security issues because they grant users unrestricted access to the entire network, rather than just the applications or resources that they need to complete their tasks. To address this issue, businesses are increasingly adopting Zero Trust (ZT) security architectures to ensure consistent levels of security. This approach is based on two fundamental ideas:

- Providing continuity of access to resources based on identity and not on location.
- Upholding the least privilege concept, i.e., only gives users (or services) access to necessary resources.

The enterprise WAN architecture is transforming into a converged, cloud-native network and security infrastructure due to the growing importance of direct cloud access and mobility. This globally distributed architecture provides speedy cloud access while the Zero Trust (ZT) framework ensures secure connections from any location and device. This architecture is characterized by a cloud-native design that enables dynamic service orchestration and centralized network and security management. The key features of this architecture include:

- Zero Trust framework
- Cloud-native design
- Globally distributed network
- Security-as-a-service at the cloud edge

This unified architecture is known as SASE (coined by Gartner in July 2019) and refers to the convergence of network and security services.



3.2 Convergence of Networking and Security- Addressing Current Risks

> "Protecting the internet today requires an integrated approach to security."

Conventionally, securing a network involved setting up perimeters and monitoring traffic between known devices. However, changing demands have made it necessary for all parts of a network to function as an integrated system. This requires interoperability between dynamic network elements, and protection of transactions, applications, and workflows moving between any devices. The challenge now is to seamlessly couple network connectivity and functionality with security, so that data can move across constantly between moving devices with inspection, encryption, and policy enforcement.

Legacy security tools were designed to defend single defensible boundaries, but today's networks have multiple edges and applications and workflows may span multiple environments in a single transaction. This means that security needs to be applied consistently across LAN, WAN, cloud, and remote user edges, and dynamic connections between these environments must be both reliable and secure. Users of any edge should be able to securely connect to any other edge from any location, no matter what device is being used.

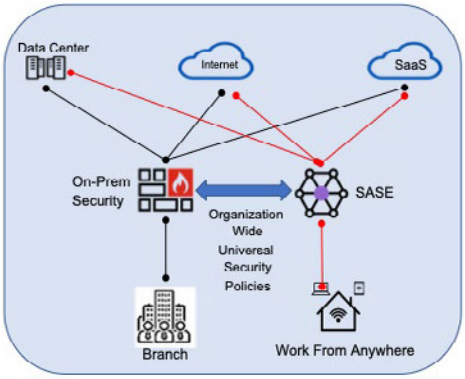


Figure 4: **Securing the hybrid workforce**: On-premises users access resources through on-premises security control and remote users through **SASE** while maintaining organization-wide universal security policies.

It is imperative for IT leaders to put new strategies into place to secure remote workers, protect their business data, and defend against online threats. A security solution that can function natively in any environment is required for hybrid networks to secure all edges consistently, increasing the visibility of threat intelligence across the network and delivering coordinated security enforcement anywhere.

The responsibility to provide consistent, efficient and secure access between users, apps, and locations within an organization falls on the network and security teams to update their tools and procedures to better address these realities. Better network alignment and eventual convergence of networking and security are inevitable.

Combining a digital and physical workforce will help businesses maintain their competitive edge in luring the top talent in a workplace that is becoming more diverse and cost-efficient. Solutions converging towards consolidation and platformization of security is the way forward; a cloud-centric Secure Access Service Edge (SASE) capability offering combined

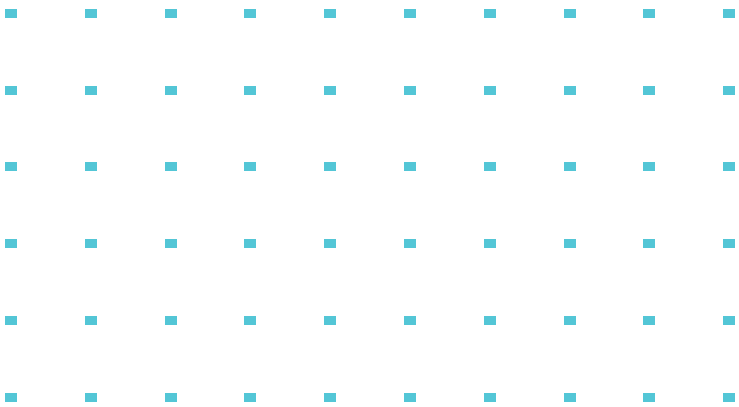
with network edge capabilities such as secured SD-WAN can streamline and enhance the organization's security posture, while also reducing the complexity and cost of managing multiple point solutions from different vendors.

3.3 Secure Networking: Towards Consolidation and Platformization of Security

Traditional networking lacks awareness about content, applications, users, devices, and location, which means organizations need to add security solutions later. It results in various problems such as management complexity, performance bottlenecks, and vulnerabilities. To overcome these issues, a secure networking approach combines networking and security into a single Platform. It improves:

- Network performance and security posture
- Enhances user experience
- Reduces management complexity

Rather than deploying security solutions one at a time, which can increase management complexity and delay response to threats, it is advisable to consolidate point product vendors into a cybersecurity platform. This enables tighter integration, increased automation, and faster and more coordinated response to threats across the network. Consolidating vendors and point solutions into a single platform is one of the trends in the security industry and is closely related to the SASE architecture. Gartner predicts that by 2025 half of all new SD-WAN purchases will be included in a SASE offering provided by a single vendor, which is a significant increase from the current figure of 10% in 2022. This suggests that there will be a growing trend towards incorporating SD-WAN into a more consolidated SASE solution with one-third of new SASE deployments will utilize a single-vendor SASE offering[2].



2 'Single-Vendor SASE', Andrew Lerner, 2022 <https://blogs.gartner.com/andrew-lerner/2022/09/30/single-vendor-sase/>.

3 'Secure Access Service Edge Market Size, Trends, Drivers & Opportunities | MarketsandMarketsTM', MarketsandMarkets <https://www.marketsandmarkets.com/Market-Reports/secure-access-service-edge-market-220384224.html>.

SASE: A Unified Approach

- The SASE market is growing rapidly, with analysts predicting that it will be worth over $11 billion by 2026.
- Simplified management and security is a key reason for organization to adopt SASE.
- 38% of security leaders from a global survey state that they are either actively researching zero trust or have it on their radar.
- By 2025, one-third of new SASE deployments will be based on a single-vendor SASE offering.

In light of the pandemic-induced uncertainties, enterprise networks require agility and scalability, and the need for dynamic secure access puts significant strain on existing networks. As a result, a cloud-based solution that integrates security services is essential.

SASE is a cloud-native platform that connects all edges to a single logical network and delivers network and security services as required. Its four key attributes include:

4.1 Drivers for SASE

The rise of cloud computing, edge computing, and remote work has created a more distributed and complex IT environment that traditional security solutions are not equipped to handle. SASE provides security and networking services from the cloud, which means that traffic does not have to be backhauled to a central data centre for security inspection. This reduces latency and improves network performance, while also providing a more secure and scalable solution. In addition, SASE provides a more holistic approach to security that is better suited to the needs of a distributed workforce. By consolidating networking and security functions into a single cloud-delivered service, SASE makes it easier to manage security policies and controls, while also improving visibility and control over network traffic.

Legacy Systems

Organizations faced challenges with blind spots and remote user traffic inspection. SASE technology offers network services like FWaaS, SWG, DLP, and CASB, providing complete visibility of hybrid network operations. SASE capabilities enable organizations to inspect, manage and secure their entire business network, including data centers, offices, branches, public and private clouds, and mobile users.

Administrative Overload

With the increase of users accessing SaaS applications from multiple devices and locations, there are concerns about nonstandard port usage and violation of company policies. SASE technology can inspect traffic by operation on all ports, reducing administrative burden and offering complete insight into device use.

Cost

SASE technology helps to reduce IT personnel expenses by consolidating safe access facilities from a single vendor. It reduces the number of physical and virtual devices, agents required on the end-user system, and allows enterprises to expand networking and security infrastructure cost-effectively.

Tackling Latency

SASE technology helps to reduce IT personnel expenses by consolidating safe access facilities from a single vendor. It reduces the number of physical and virtual devices, agents required on the end-user system, and allows enterprises to expand networking and security infrastructure cost-effectively.

Control

SASE technology offers easy control as a key advantage. Its single cloud-based manager controls the entire operation, reducing the IT department's workload, even when managing several offices within an enterprise network.

4 'SASE Adoption Motivations Worldwide 2020 | Statista' <https://www.statista.com/statistics/1222865/sase-adoption-motivation-organization/>.

5 'Gartner: Fueling the Future of Business', Gartner <https://www.gartner.com/en>.

Policies Implementation

SASE technology enables each access session to be reviewed, and the same set of policies applied to support the control of content by identifying confidential data, malware, etc.

Ease

With SASE technology, network security experts can concentrate on identifying, regulating, and application access specifications and mapping them to SASE capacities, instead of setting up infrastructure repeatedly. This increases the effectiveness of the network and network security staff.

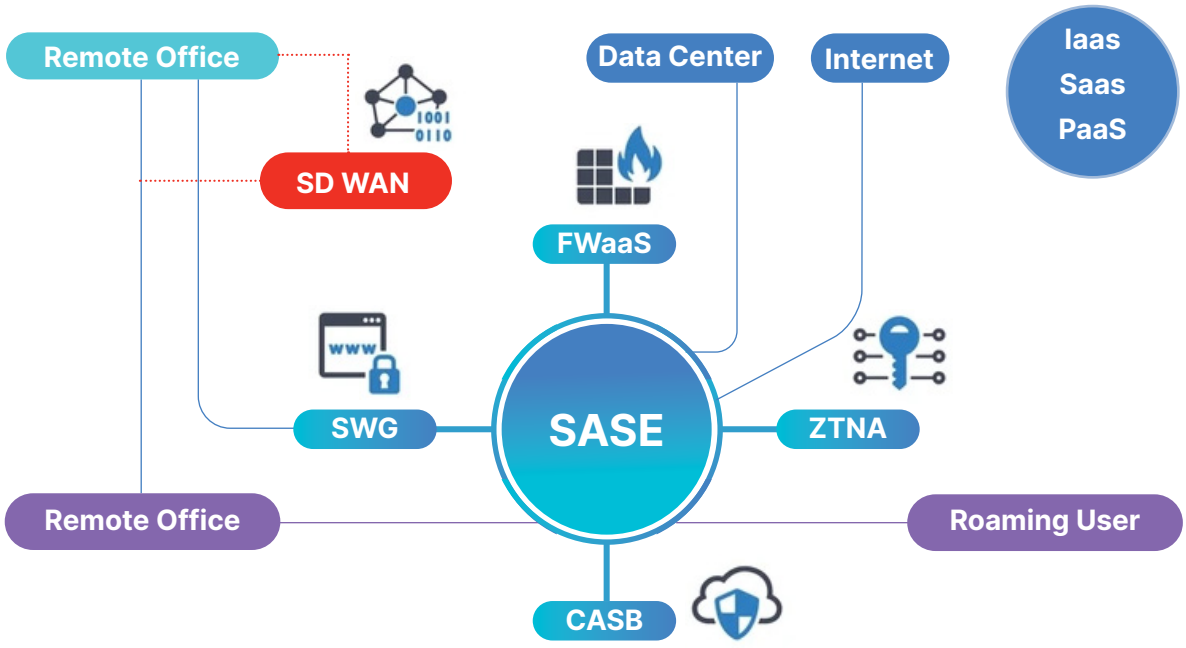
"SASE is needed to address the security challenges created by the increasingly distributed IT environment, where traditional security solutions are no longer effective. By offering a more cloud-native and edge-centric approach to security, SASE provides a scalable, flexible, and comprehensive solution that can adapt to the changing needs of the digital landscape."

4.2 The SASE Architecture

Secure Access Service Edge (SASE) architecture provides more comprehensive and flexible security solutions.

One of the key components of SASE architecture is Software-Defined Wide Area Network (SD-WAN) technology, which directs traffic originating from branch sites for internet or cloud services to SASE security controls. SD-WAN also connects the organization's private data center with branch offices, providing a seamless and secure network infrastructure. However, mobile users who are not connected to SD-WAN still need to be protected. In such cases, these users rely on an agent installed on their device to manage their traffic. This ensures that even mobile users are protected by the SASE security controls.

The SASE cloud consists of several components, including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) Cloud Access Security Broker, (Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS), is designed to detect any malicious traffic to or from branches and roaming users.



4.3 Components of SASE

In contrast to earlier SD-WAN solutions, SASE places greater emphasis on a unified approach to security that simplifies and enhances security solutions consisting of the elements.

Unified management: Managing the above capabilities through a centralized management system lets organizations overcome various challenges related to change control, patch management, outage windows coordination, and policy management. It enables the implementation of consistent policies throughout organizations, regardless of where users are connecting from.

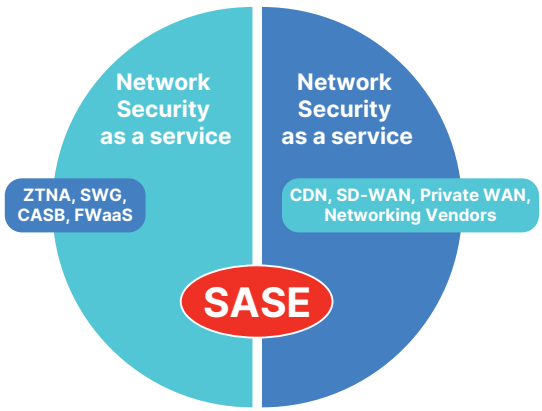


Figure 5: Components of SASE

The components of SASE provide a comprehensive and integrated solution to networking and security challenges faced by modern organizations. The cloud-native architecture, SDP, ZTNA, SWG, FWaaS, and edge computing capabilities work together to create a highly secure and flexible networking environment that can adapt to the changing needs of modern business.

Secure Access Service Edge (SASE) capabilities can be categorized into the following levels:

Basic SASE capabilities

These capabilities include FWaaS, Secure Web Gateway(SWG), Cloud Access Security Broker (CASB), Zero-Trust Network Access (ZTNA), and branch office connectivity.

Advanced SASE capabilities

In addition to the basic capabilities, advanced SASE capabilities include network optimization, SD-WAN, and threat prevention capabilities such as intrusion prevention and detection, sandboxing, and Data Loss Prevention (DLP).

It is important to note that achieving these capabilities require more than simple service function chaining. Service function chaining is a method of combining network functions in a specific order to achieve a desired outcome. However, SASE requires parallel processing to minimize processing latency. Parallel processing involves breaking down a task into smaller sub-tasks that can be processed simultaneously on multiple processors, which can significantly improve performance and reduce latency. This is crucial for SASE, as it involves processing large amounts of data in real-time to provide comprehensive security and performance for remote workers and branch offices accessing internet applications and services.

Core

- SD-WAN, SWG, CASB, ZTNA, FWaaS
- Detect sensitive data/malware
- Rapidly encrypt/decrypt large amounts of data at line speed, at scale
- Constantly assess risk and trust level during sessions

Recommended

- Network sandbox, recursive DNS, RBI, WAAP

Optional

- VPN, Wi-Fi hotspot protection, offline protection

SASE capabilities suggested by Gartner.

4.4 Use cases: Ensuring secure Access with SASE

USE CASE 1 Secure Internet Access

Drivers

- Increase in the remote workforce.
- Users having direct internet access, thus expanding the organization's potential attack surface.

Solution Characteristics

- Ability to ensure user protection irrespective of location.
- Ability to inspect traffic, detect and respond to known and unknown attacks.

SASE Capabilities

- SASE delivers a quality of service; assimilating Secure Web Gateway (SWG) capabilities to monitor and protect data and applications against web-based attack tactics along with other features such as URL filtering, DNS security, antivirus, anti-malware and sandboxing.

USE CASE 2 Secure Private Access

Drivers

- The need for secure connectivity to corporate applications, whether they are deployed in a private data centre or public cloud.

Solution Characteristics

- Integration with SD-WAN and Next-Generation Firewall (NGFW) solutions to offer intelligent steering and dynamic routing capabilities via the SASE Point of Presence (PoP).
- It should ensure an excellent user experience by automatically identifying and securing the shortest path to corporate applications.
- It accomplishes this through a single agent that provides Zero-Trust Network Access (ZTNA), traffic redirection, and endpoint protection.

SASE Capabilities

- SASE provides ZTNA, restricts access to specific locations, protects web-enabled applications from attacks using Web application firewall, and inspects encrypted traffic streams to detect sensitive data loss.

USE CASE 3 Secure SaaS Access

Drivers

- The requirement to provide secure access to applications, devices, users, and workloads, regardless of their location, is crucial for a hybrid workforce that frequently transitions between various environments, including campus, branch, home office, and mobile locations.

Solution Characteristics

- SASE protects mission-critical data and secures cloud-based information with enterprise-grade security whether users are on-premises or off-premises.
- It supports dual-mode CASB with both in-line and API-based capabilities to detect and overcome shadow IT challenges while securing critical data.
- It should provide granular application control to secure sensitive data.
- It should detect and remediate malware in applications across managed and unmanaged devices.

SASE Capabilities

- SASE provides low-latency ZTNA access for cloud users to edge computing resources, obfuscating their IP addresses and establishing an encrypted connection to the cloud with API protection. The SASE provides Firewall-as-a-Service (FWaaS) to protect the edge computing location from inbound attacks.

4.5 Migrating to SASE

It is vital to have a well-defined migration plan when transitioning to SASE. The plan should consider the organization's current IT infrastructure, identify potential risks and challenges, and establish clear timelines and milestones for the migration process. This can help ensure a smooth transition and minimize disruption to the organization's operations.

SASE may not be a one-size-fits-all solution for all organizations, and additional security measures may still be necessary depending on specific industry regulations and compliance requirements. It is important to note that these concerns should not discourage organizations from considering SASE as a viable solution for their networking and security needs. Instead, organizations should carefully evaluate their unique requirements and potential challenges before deciding whether SASE is the right solution for them.

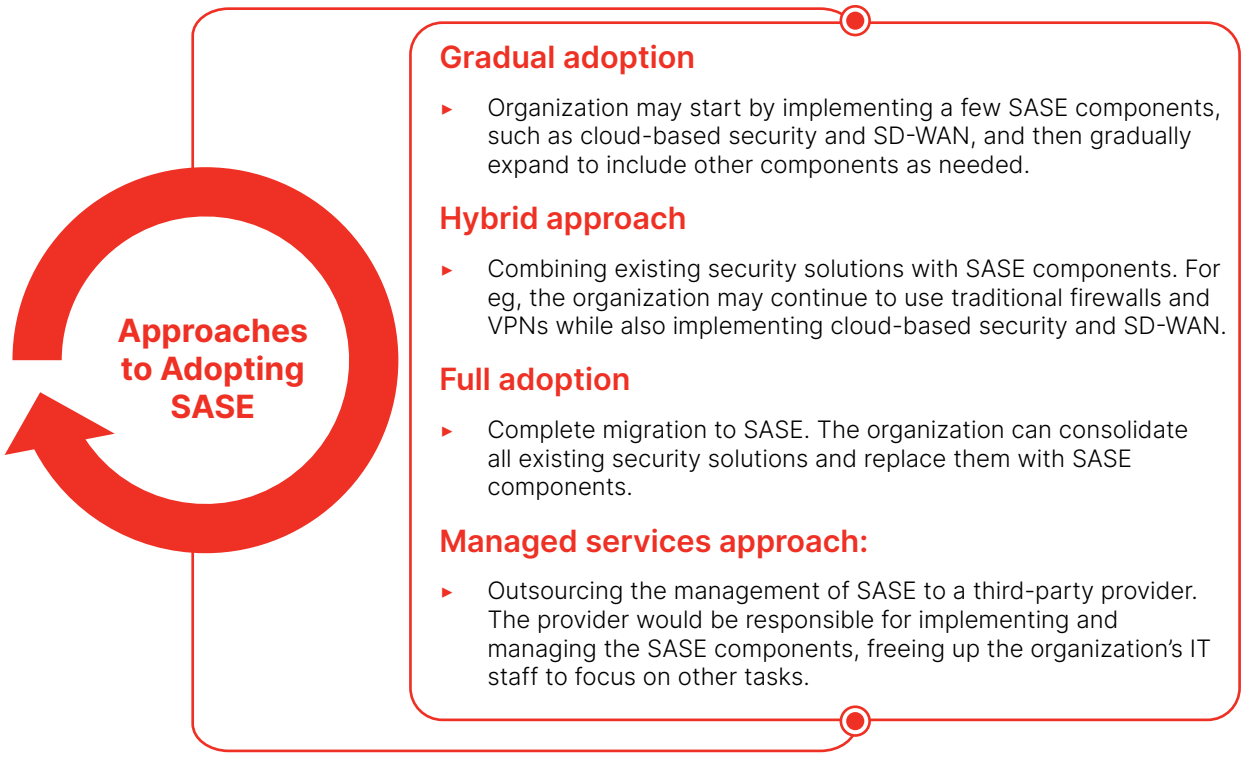


Figure 6: Approaches to adopting SASE.

4.5.1 Roadmap for SASE adoption

Short-term recommendations:

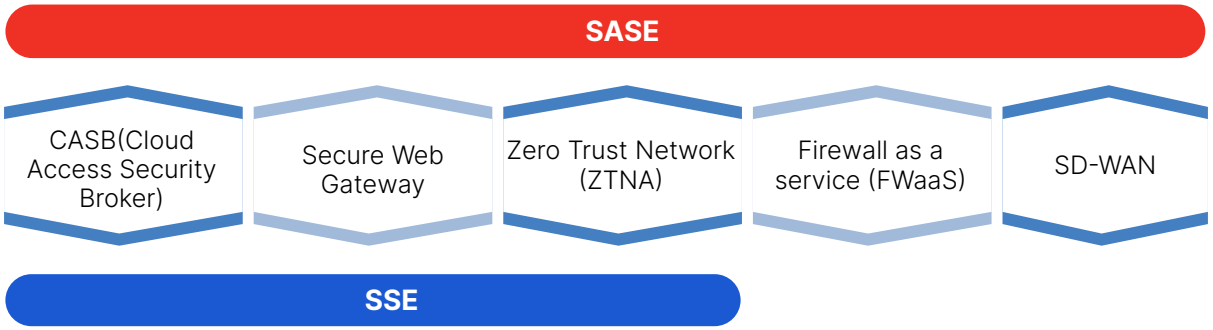
- Use Zero Trust Network Access (ZTNA) to enhance or replace the legacy Virtual Private Network (VPN) for remote users, particularly for high-risk use cases.
- Take stock of devices and contracts to gradually phase out the on-premises perimeter and branch hardware over a period of several years in favor of cloud-based SASE capabilities delivery.
- Simplify and reduce costs by consolidating vendors as secure web gateways, CASBs, and VPN contracts are renewed. Capitalize on a converged market that integrates these security edge services.

Long-term recommendations:

- Consolidate SASE offerings to one or two partnered vendors explicitly.
- Implement ZTNA and authentication mechanisms (e.g. MFA) for all users, including those in the office or branch, regardless of their location.
- Choose SASE offerings that provide control over where inspection occurs, how traffic is routed, what is logged, and where logs are stored to satisfy privacy and compliance requirements.
- Establish a dedicated team of security and networking experts who share responsibility for secure access engineering across on-premises, remote workers, branch offices, and edge locations.
- SASE is a good fit for organizations that have a hybrid workforce and need to secure access to applications, devices, users, and workloads regardless of their location. It is also suitable for organizations that want to simplify their IT infrastructure by consolidating networking and security services from a single vendor.
- Organizations that have a centralized workforce, with most employees working in a single location, may not require the level of flexibility and scalability provided by the SASE framework. Similarly, organizations with a legacy infrastructure that cannot be easily integrated with cloud-based services may not be able to fully leverage the benefits of SASE. Lastly, organizations with strict regulatory requirements or compliance mandates may need to carefully evaluate the impact of SASE on their compliance posture before adopting it.

Overall, the suitability of SASE depends on an organization's specific requirements, goals, and IT infrastructure. It is important to carefully assess the benefits and drawbacks of the SASE framework before deciding whether it is the right approach for your organization.

SASE or SSE?



Secure Service Edge (SSE) and Secure Access Service Edge (SASE) are both cloud-based security models, but they differ in their scope and focus. While SSE primarily aims to secure network access to cloud-based applications and services, SASE provides a more comprehensive approach that covers all aspects of enterprise security.

SSE does not include the network components of SD-WAN and only focuses on optional security components such as DLP sandboxing and network access and control. This makes SSE a suitable solution for organizations that do not require SD-WAN or prefer a best-of-breed approach in choosing an SD-WAN and Cloud delivered security services. Both aim to provide secure work-from-anywhere access without the constraints of a central VPN termination point.

Post-pandemic, where organizations are transitioning back to the office or adopting hybrid approaches, SASE offers a way to enforce consistent security for users, regardless of their location. On the other hand, SSE can be an ideal solution for organizations that are entirely remote.

SASE (Gartner 2019)	SSE(Gartner 2021)
Focus on network and security	Focus on edge Security
Components: CASB, ZTNA, SWG, FWaaS, SD-WAN	Components: CASB, ZTNA, SWG, FWaaS
Suited for organizations requiring secure branch, remote and cloud access	Suited best for complete remote organisations

Conclusion

Networking and Security Convergency is a growing trend that is expected to continue in the future. The adoption of SASE framework is becoming increasingly popular as organizations seek to simplify and consolidate their security and networking infrastructure across branch offices, on premise and cloud providing better visibility and control over security posture, while also improving operational efficiency. However, it is important to note that the convergence of networking and security is not a one-size-fits-all approach, and organizations must evaluate their specific needs and requirements before selecting a solution.

The encapsulate in the figure 7 expands on how security approaches have evolved over time with integration as a bedrock element. The various blocks in the diagram depict the drivers and pillars leading to the phenomena of convergence of networking and security. It also captures the key qualities and outcomes that an organization should be mindful of while choosing a SASE vendor for their business.

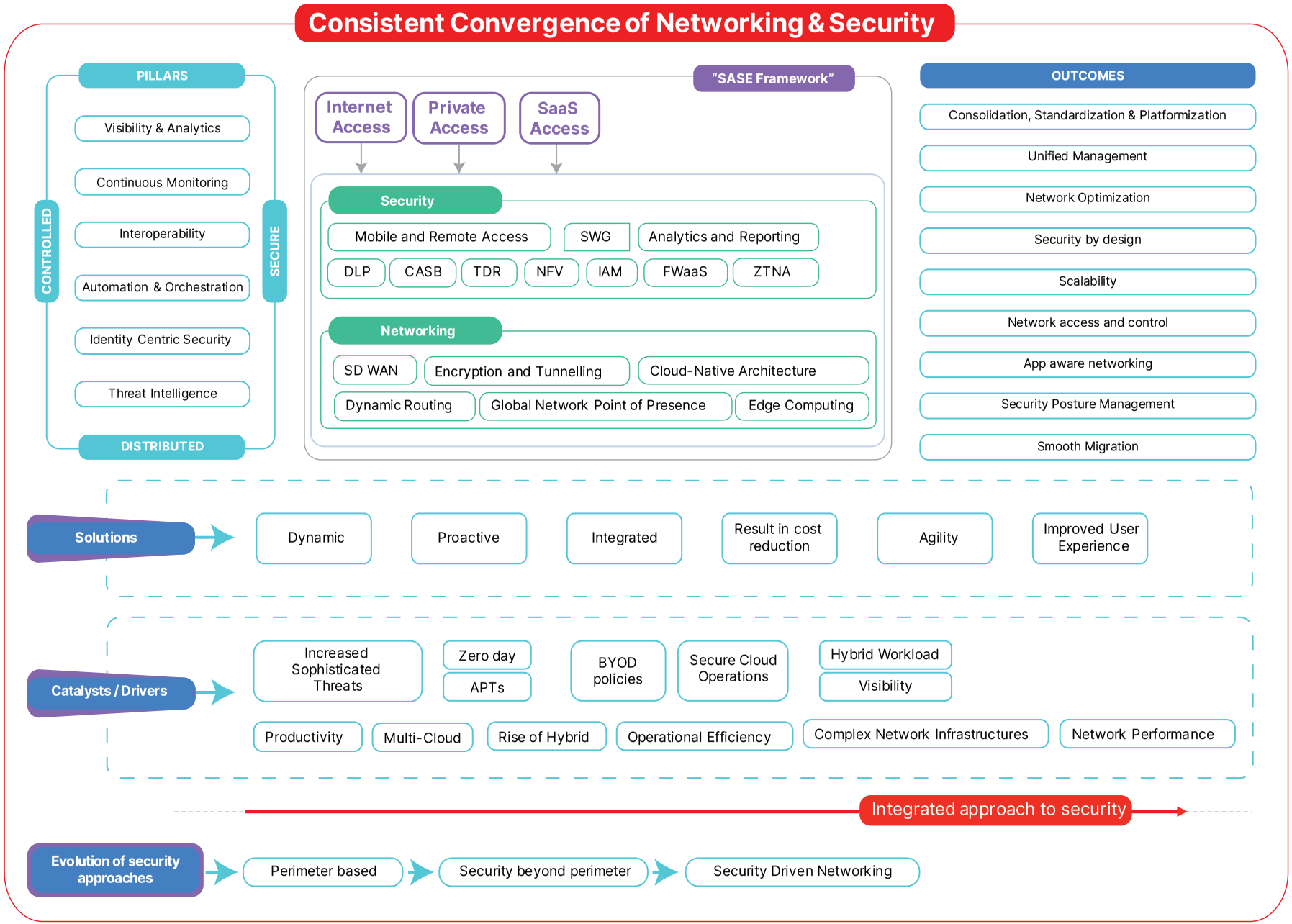


Figure 7: Encapsulate: Convergence of Networking and Security

Appendix

Components of SASE:

- Software-Defined Wide Area Network (SD-WAN): SD-WAN is a technology that provides a virtualized network overlay that allows organizations to use multiple internet connections to create a secure, reliable, and high-performance WAN.
- Cloud Access Security Broker (CASB): CASB is a security solution that provides visibility and control over cloud applications and services, enabling organizations to detect and mitigate security risks.
- Firewall-as-a-Service (FWaaS): FWaaS is a cloud-based firewall solution that provides advanced security features such as intrusion detection and prevention, malware detection, and content filtering.
- Secure Web Gateway (SWG): SWG is a cloud-based security solution that provides web filtering, anti-malware, and data loss prevention capabilities to protect against web-based threats.
- Zero Trust Network Access (ZTNA): ZTNA is a security model that provides access to applications and services based on user identity, device trust, and other contextual factors. SASE leverages ZTNA to provide secure access to applications and services from any location.

References

- 'Gartner: Fueling the Future of Business', Gartner <https://www.gartner.com/en>
- 'SASE Adoption Motivations Worldwide 2020 | Statista' <https://www.statista.com/statistics/1222865/sase-adoption-motivation-organization/>
- 'Secure Access Service Edge Market Size, Trends, Drivers & Opportunities MarketsandMarketsTM', MarketsandMarkets <https://www.marketsandmarkets.com/Market-Reports/secure-access-service-edge-market-220384224.html>
- 'Single-Vendor SASE', Andrew Lerner, 2022 <https://blogs.gartner.com/andrew-lerner/2022/09/30/single-vendor-sase/>

Authors

Data Security Council of India

- Vinayak Godse
  CEO, DSCI
- Aditya Bhatia
  Senior Consultant, DSCI
- Neha Mishra
  Associate, Technical Research, DSCI.

FORTINET

- Michael Joseph
  Senior Director, System Engineering, India & SAARC at Fortinet.

Fortinet is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices, and data everywhere, and today we deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented, and most validated in the industry. The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Learn more at https://www.fortinet.com, the Fortinet Blog, and FortiGuard Labs.

PROMOTING DATA PROTECTION

A nasscom Initiative

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by Nasscom®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in.

DATA SECURITY COUNCIL OF INDIA

Nasscom Campus, Fourth Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

+91-120-4990253 | research@dsci.in | www.dsci.in

DSCI_Connect dsci.connect dsci.connect data-security-council-of-india dscivideo