SPOTLIGHT
Sponsored by: NTT DATA

SASE journeys are diverse, but the ideal adoption strategy focuses on a best-in-class, single-vendor solution; involves collaboration between networking and security organizations; and leverages trusted advisors.

A SASE Enterprise Story: The Unity of Security, Network, and Revenue

June 2024

Written by: Ghassan Abdo, Research Vice President, Worldwide Telecom, Virtualization and CDN, and Christopher Rodriguez, Research Director, Security and Trust

Introduction

Digital transformation and cloud adoption are key to enhancing customer experience, generating revenue, and improving productivity. Digital transformation remains a top priority for businesses and continues to disrupt and reshape network environments. Unfortunately, it has also exposed weaknesses in legacy approaches to networking and security that force organizations to decide between accepting increased business risk and adopting business enabling technologies.

Secure access service edge (SASE) was developed to address the limitations of legacy networking and security architecture. SASE promotes the integration of networking and security technologies into a coherent cloud-native and delivered architecture, enabling businesses to implement modern zero trust access frameworks as they digitally transform. SASE enhances customer experience and business use cases with elevated analytics and visibility, simplifies control at scale via an integrated policy and orchestration framework, and can quickly adapt to changes in the network environment, like adding new users or devices allowing for network and security agility and speed.

AT A GLANCE

KEY STATS

- The highest IT investment priority in United States over the next three years is improving WAN and network security, with 50% of enterprises increasing SASE year over year.
- When asked about changes resulting from SASE adoption, 61% of survey respondents described their organizational security posture as "improved" or "drastically improved" and 65% described their network performance as "improved" or "drastically improved" (source: IDC's *SSE/SASE Buyer Adoption Survey,* March 2024).

As a new architecture that integrates software-defined networking (SD-WAN) and security services, SASE promises to accelerate enterprise security network transformation. However, as businesses look to adopt SASE, several questions surface. Where to start with network and security convergence? How to approach SASE, cross-functional stakeholder alignment, and representation? And importantly, how to fund it? By addressing these considerations, businesses can plan for a SASE journey that delivers on the promises of future proofing the network, revenue growth through faster market expansion and product availability, all while maintaining or reducing IT costs and resources.

SASE Adoption Trends

Security Trends Driving Need for SASE

Legacy approaches to network protection rely on perimeter-centric control points and specialized security solutions. A point product approach leads to a complex array of security solutions that operate in disjointed silos. Whether on premises or SaaS based, point products lead to increased management complexity and ensuing security gaps. Labels and policies must be defined and created in each product. Each point product must be integrated with related systems such as identity providers and security information and event management (SIEM) tools. Every new tool added to the security architecture represents a new management console for administrators to learn and operate daily and entails added time and costs to update and maintain. Navigating support channels and procurement processes must also be considered.

These challenges are only amplified as businesses note continued budgetary concerns related to inflation and geopolitical events outside of their control. A skills shortage in the security industry persists due to the difficulty of finding and retaining talent with the requisite skill sets across areas including cloud, network, and security. This skills shortage was a top 3 concern cited by IT decision-makers as reasons for limiting IT investments (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 12*, January 2023).

Essentially, IT organizations are expected to do more with less. These limitations hinder the ability to address emerging threat vectors. Generative AI (GenAI) is the latest emerging technology to raise security concerns, such as usage by cybercriminals when attacking applications, data, and networks, and unintentional exfiltration of sensitive company data and IP by employees or engaging GenAI in harmful actions like generating dangerous code. IDC survey data shows 26.5% of respondents expect security to be the top challenge for GenAI adoption (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 6*, July 2023).

Networking Is Key to SASE Adoption

A recent IDC survey indicated that U.S. enterprises' highest IT investment priority over the next three years is improving WAN and network security, with 50% of enterprises increasing SASE year over year. These indicators underscore the role that SASE plays in improving network agility and guiding enterprises through the complexity of network transformation.

Software-defined networking is essential to managing variable and unpredictable traffic demand. Wide-scale security attacks can alter traffic patterns and potentially cause unforeseen downtime. As an integrated architecture, SASE is more resilient. It is better able to deal with these network anomalies and extract the benefits of software-defined networking.

The key technical benefit is the move toward an integrated orchestration layer for networking and security. SASE can accelerate the move to a uniform orchestration layer that integrates management of networking and security services. An integrated orchestration layer can mitigate a major pain point for enterprises, which is reporting. Enterprises expect reporting to be timely, granular, and relevant to ensure actionable response to anomalies.

In summary, SASE is key to improving network agility, optimizing access to cloud resources, and mitigating the impact of unforeseen traffic anomalies.

The Current SASE Buyer Journey

Consolidation to a single-vendor platform solution is foundational to achieve deep integration, pricing, and ease of adoption. IT buyers expressed an interest in implementing a full SASE solution through one vendor: 62% rated a modern

"single vendor" approach to SASE as important or very important (source: IDC's *SSE/SASE Buyer Adoption Survey*, March 2024). Overall, recent SASE buyers noted improvements in all major categories including network performance, false positives, threat blocking rates, and overall security posture.

A coordinated, strategic approach to SASE adoption is a requisite step to unifying networking and security needs. Security and networking teams typically have differing metrics and goals for a SASE investment. It is important that these organizations work to speak a common language in terms of budgets, KPIs, and project outcomes. IDC survey research shows that these organizations are already collaborating on SASE decision-making: 38% of respondents indicated that these teams collaborate when purchasing SASE. Another 18% of businesses indicated an equal balance of input between networking and security teams for SASE purchases (source: IDC's *SSE/SASE Buyer Adoption Survey*, March 2024).

The pivot to SASE from standalone SD-WAN is motivated by the potential commercial and technical benefits. Commercially, enterprises have traditionally purchased SD-WAN services and supplemented them with point security solutions such as advanced firewall and secure cloud access. SASE removes the friction of managing individual contractual and SLA agreements by bringing them under a single framework. This approach can bring cost benefits and simplify the contractual framework.

When deciding on a SASE solution, organizations are more willing to seek a best-of-breed product than selecting one based on an existing vendor relationship. Furthermore, IDC research confirmed that 29% of SASE buyers noted the value of a trusted managed service provider partner as the overall top factor in their choice of SASE (source: IDC's *SSE/SASE Buyer Adoption Survey*, March 2024).

IDC buyer research shows that SASE journeys are diverse, but the ideal adoption strategy focuses on a best-in-class, single-vendor solution; involves collaboration between networking and security organizations; and leverages trusted advisors in the form of channel partners and service providers.

Benefits of Security and Networking Convergence

SASE Provides Essential Security Improvements

On-premises firewalls and point products can leave gaps in protection and lead to inconsistent policies and security blind spots. A global, service-edge based approach ensures that a unified security stack is present at all network entry points. In short, SASE leverages the power of the following cloud-delivered security services to address the limitations of legacy network security solutions:

- **Zero trust.** Zero trust network access (ZTNA) is a foundational component of SASE. ZTNA is a modernized security technology designed to address the shortcomings of legacy access systems, allowing businesses to enforce zero trust principles such as least privilege access, strong authentication, and continuous monitoring. ZTNA ensures that user access is limited to only the specific, authorized applications and resources required for their job activities, rather than the broad, network-based access offered by VPN.
- **Integrated security services.** The full stack of SASE security functions can be deployed as needed, including firewall as a service (FWaaS), ZTNA, cloud access security broker (CASB), secure web gateway, and data leakage prevention (DLP). IDC notes that SASE is not "all or nothing," and security services may be implemented based on security priorities or other considerations. IDC research shows that most organizations adopt a phased rollout approach to

SASE adoption, focusing on specific security functions first. Similarly, advanced security capabilities such as remote browser isolation (RBI) or sandboxing can be implemented on an as-needed basis.

- **Visibility and monitoring.** Digital transformation reshapes networks from dumb pipes to hyperintelligent supersonic highways, capable of producing vast amounts of data and analytics from devices, users, applications, and locations. The ability to truly understand business risk is directly related to the ability to observe network traffic and proactively identify what's good, bad, important, or critical/business impacting. Network activity generates patterns that cannot be falsified. Continuous monitoring and insights from network communications are key to identifying and mitigating advanced threats and zero-day attacks, including ransomware and insider threats, early in the kill chain.

  SASE provides inline threat prevention as a foundational level of protection, leveraging machine learning to uncover patterns of suspicious activity in network traffic. Integrations with SIEM, extended detection and response (XDR), and other security analytics tools provide network-based insights to security operations center teams for investigations and threat hunting. SASE can be an important source of telemetry data for usage with advanced security analytics solutions when insights from multiple sources are required to identify novel or advanced threats.

- **Future-proof security.** SASE offers a platform for rapid expansion of security architecture as the threat landscape changes. While most organizations start by securing managed users and managed and unmanaged devices via zero trust controls and robust detection capabilities, it is important to next address risks such as "shadow IT" usage of unsanctioned cloud services, support for mobile devices, and Internet of Things discovery and profiling. SASE providers continue to identify new attack surfaces and develop new capabilities to mitigate emerging threat vectors in the modern enterprise networking architecture. For example, SASE vendors have introduced new capabilities such as DLP controls for GenAI use cases in 2024.

SASE Optimizes Networking Performance

Software-defined networking has already driven significant improvements in network performance and optimized use of network resources. SASE will take it a step further by making the right choices of networking and security features that improve resilience and network agility. This is more prominent when SASE is offered as a single-vendor solution. Single-vendor SASE will simplify the deployment, provide better price performance, and ease adoption of secure networking solutions.

SASE creates a new, cross-functional collaborative approach between networking and security decision-makers. This is critical to ensuring that the integrated architecture is well suited to address business needs. While SASE is not the first technology to drive cross-functional collaboration, the business value to be gained by SASE is significant.

The modern digital business is distributed, heterogenous, and dynamic. SASE provides a modernized security architecture for enabling digital transformation, without incurring increased business risk. It can also help organizations make the right trade-offs in terms of deployment models, whether on premises, edge hosted, or cloud hosted. A coordinated approach by networking and security teams can optimize SASE to align with the advantages inherent in these deployment models.

The benefits of SASE are amplified when deployed with assistance from a knowledgeable partner that can aid in the adoption journey as well as day-to-day management. Working with a reliable partner to move security infrastructure to the cloud helps the IT organization to scale as required. Managed SASE services help mitigate other hidden costs of legacy security tools, such as lengthy procurement cycles or difficult update processes. Ideally, a managed SASE will include a

comprehensive stack of integrated security technologies, bolstered by continuous management of the SASE platform, 24 x 7 monitoring, and threat detection. Other SASE-related advisory and assessment services, investigation and threat hunting services, monitoring services, and additional value-adding services help organizations develop robust security strategies that help empower the business through its digital transformation journey.

Considering NTT DATA and Palo Alto Networks

In 2023, NTT DATA and Palo Alto Networks announced a partnership combining integrated services for deployment and management of purpose-built, single-vendor SASE. The offering is a Managed Prisma SASE solution that reduces the number of vendors, tools, and technology stacks needed to support the business, and it combines the strengths of NTT DATA and Palo Alto Networks.

Single-Vendor SASE Offering

Made up of NTT DATA's Managed Network Services (MNS) portfolio and Palo Alto Networks' Prisma SASE, the solution is a comprehensive managed SASE that includes SD-WAN, cloud-delivered security, and enhanced automation and reporting. The end-to-end solution is designed to help enterprises meet current digital transformation challenges and enable more flexible ways of working. The integrated networking and SD-WAN functionality with cloud-delivered security enables customers to secure user access to applications and sensitive data irrespective of location, without compromising on performance and user experience. NTT DATA's platform-driven approach provides advanced AIOps and automation capabilities to help improve operational efficiency and security outcomes. As a fully managed solution, it helps enterprises conserve scarce IT resources and reduce the complexity of managing a global network and security infrastructure, unleashing new capabilities and unlocking new revenue streams.

Those enterprises not currently on a single-vendor SASE path can utilize NTT DATA's wide breadth of technology integration partners for a customized solution that leverages their existing technology environment and investments.

Both NTT DATA and Palo Alto Networks are global providers with expansive vertical expertise, which enables them to provide solution velocity, scalability, consistency, and continuity for enterprises.

About NTT DATA

NTT DATA is a $30 billion provider of IT and business services that combines global reach with local client service in over 80 countries. Its offerings include business and technology consulting, industry and digital solutions, applications development and management, managed edge-to-cloud infrastructure services, network as a service, BPO, systems integration, and global datacenters.

About Palo Alto Networks

Palo Alto Networks provides next-gen cybersecurity to thousands of customers globally, across all sectors. Its best-in-class cybersecurity platforms and services are backed by cutting-edge threat intelligence and strengthened by state-of-the-art automation. Whether delivering products to enable the zero trust enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, Palo Alto Networks is committed to ensuring the safety of its customers.

Challenges

In its pursuit to be a leader in providing managed SASE services, NTT DATA has some challenges to confront. For example, the company faces global and regional competitors, especially in the North America, EMEA, and Asia/Pacific regions. These companies are building up SASE portfolios in collaboration with similar technology vendors. NTT Data's ability to differentiate its offering should go beyond technical features and focus on a full life-cycle approach and global networking assets to help customers with their network transformation journey.

The ongoing evolution of SASE opens the possibility for vendors to expand into specialized or adjacent security practices such as email security or bot detection and control. These are specialized security technologies that are generally outside of Palo Alto Networks' primary area of expertise. Currently, these capabilities lack mainstream acceptance in the definition of SASE but could open the door to increased competition for Palo Alto Networks.

Conclusion

By integrating SD-WAN and security services, SASE promises to accelerate enterprise security network transformation. SASE creates a new, cross-functional collaborative approach between networking and security decision-makers. This is critical to ensuring that the integrated architecture is well suited to address business needs.

SASE promises to accelerate enterprise security network transformation.

The gains from SASE cannot be ignored as it transforms the experience for customers, employees, partners, and vendors. It substantially reduces risk and simplifies control at scale while enabling new paths to revenue by optimizing the integration of experience and security.

About the Analysts

Ghassan Abdo, *Research Vice President, Worldwide Telecom, Virtualization and CDN*

Mr. Abdo, research vice president in the Telecommunications group, covers the evolution of the telco cloud ecosystem as well as the emerging virtualized enterprise networking services. His primary focus areas include service provider SD-WAN and managed services and emerging NFV-based virtual networking services as well as other managed WAN services. In the hosting and cloud segment, Ghassan covers service provider managed hosting services, including hybrid managed private/public cloud services, colocation services, and secure cloud connect and CDN services.

Christopher Rodriguez, *Research Director, Security and Trust*

Christopher Rodriguez is a research director in IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and network infrastructure. IDC's Security and Trust research services to which Chris contributes include network security products and strategies and active application security and fraud.

MESSAGE FROM THE SPONSOR

The integration of NTT DATA's Managed Network Services portfolio with Palo Alto Networks Prisma SASE provides a comprehensive managed Secure Access Service Edge (SASE) solution which includes software-defined wide area network (SD-WAN), secure service edge (SSE), and enhanced automation and reporting. This solution is designed to help enterprises meet digital transformation challenges and enable more flexible ways of working. By integrating networking and SD-WAN functionality with cloud-delivered security, the solution secures user access to applications and data irrespective of location. The platform's advanced AIOps and automation capabilities improve operational efficiency and security outcomes. This fully managed solution reduces the complexity of managing a global network and security infrastructure, conserving IT resources. The solution is highly adaptable and scalable, accommodating changing business needs efficiently. For more information on Managed Network Services with Prisma SASE please visit our website.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com