accenture

The convergence of network and security is here: It's called SASE.

As enterprises have transformed over the last several years to consume more cloud-based services and moved out of the data centers, their connectivity and security have become ever more important. Perimeter-based network access solutions were designed in a different time, for a different problem. That's why today—with most data, applications, and devices outside the walls of the enterprise—security teams are struggling to maintain control...and it's only getting harder. Fortunately, Secure Access Service Edge (SASE) has arrived to take advantage of the convergence of network and security.

It's time to change the way we do security

The way companies access their data has changed, but network security has not kept pace with the challenges of this approach. Network security previously relied on perimeter-based network access solutions, which were adequate when enterprise data and applications were hosted in physical on-premise data centers. Today, however, as more and more organizations have transformed to consume more cloud-based services and moved out of these data centers, enterprise security teams are struggling to maintain control and address the accelerating threat landscape.

Costs of data breaches continue to escalate. In fact, the global average cost of data breaches reached an all-time high of $4.35 million in 2022 compared with $4.24 million in 2021, according to a new IBM Security report.[1] About 60 percent of the affected organizations raised product and services prices due to these data breaches.

Additionally, the drive for more efficient business models and enhanced user experiences requires new approaches to secure remote access, without regard for where the user is in relation to the data in today's hyper-connected world. After two-plus years of widespread remote work, companies are still struggling with secure remote access because many employees, across organizations and industries, prefer—or even demand—hybrid schedules.

And because traditional security solutions were not designed with the cloud in mind, network infrastructure became needlessly complex, resulting in increased administrative costs and incomplete protection solutions. That's why, with the boundaries of enterprise networks weakening at an alarming rate, company infrastructure must be built by design to encompass data and endpoints that exist within and outside of the business.

50% by 2025

Enterprise wireless endpoints using networking services that deliver additional capabilities beyond communication, up from < 15%

(Realizing Value from Next-Generation Wireless; Gartner, October 2022)

80% by 2025

Enterprises adopting a strategy to unify web, cloud services and private application access using a SASE/SSE architecture, up from 20%

(Market Guide for Single-Vendor SASE; Gartner, September 2022)

75%

Enterprises pursuing security vendor consolidation, up from 29%

(Top Trends in Cybersecurity—Survey Analysis: Cybersecurity Platform Consolidation, February 2023)

[1] Cost of a data breach 2022; IBM

Organizations are shifting to SASE

Why are organizations making such a rapid shift to SASE? One primary reason is that cybersecurity today, where both users and data are everywhere, must be cloud-based. The game-changing SASE solution combines both networking and security into a single cloud-based service model with consistent security policies, which can be applied globally for a seamless experience no matter where users, applications or devices are located. SASE enables companies to provide secure and performant access, effectively addressing modern cyber threats that enterprises continually face.

Although traditional security models have assumed internal traffic is safe, enterprise wireless endpoints using networking services other than corporate communication have more than tripled.[2] Most modern application development is now taking place on cloud platforms using microservices and cloud functions, and a majority of enterprises are adopting strategies to unify web, cloud services and private application access using SASE/SSE (Secure Service Edge) architecture.

Cybersecurity today, where both users and data are everywhere, must be cloud-based.

[2] Realizing Value from Next-Generation Wireless; Gartner, September 2022

SASE core capabilities and functional layers

The SASE core provides the main security building blocks, which include:

- **Zero trust network access** (ZTNA) for secure remote access based on dynamic access control policies to applications, data and services
- **Secure web gateway** (SWG) solution for traffic and content inspection, as well as URL filtering, to protect against a multitude of web-based threats such as phishing and ransomware
- **Firewall as a service** (FWaaS) for a cloud based next generation firewall (NGFW) to protect infrastructure across on premise, software as a service (Saas) products and various cloud service providers
- **Cloud access security broker** (CASB) that spans security across SaaS, platform as a service (PaaS), infrastructure as a service (IaaS) and on-premise data centers,strengthening security postures to protect against data leakage, shadow IT and unauthorized resource access
- **Domain name system** (DNS) security that limits access to potential malicious domains, such as Command and Controls

The SASE external protection layer provides an optimized level of protection to secure access to applications exposed on the internet. These protection building blocks include web application and API protection (WAAP) with web application firewall (WAF), application programming interface (API) management, distributed denial of service (DDOS) mitigation and anti-bot/content delivery network (CDN).

The SASE connectivity capability provides network software-defined wide area network (SD-WAN) integration to facilitate operations, and, importantly, inspect and control network traffic for site-to-site connectivity.

SASE automation and orchestration capabilities provide building blocks with built-in native threat intelligence management capabilities to enhance dynamic detection and response that continually evaluate destinations for malicious activity.

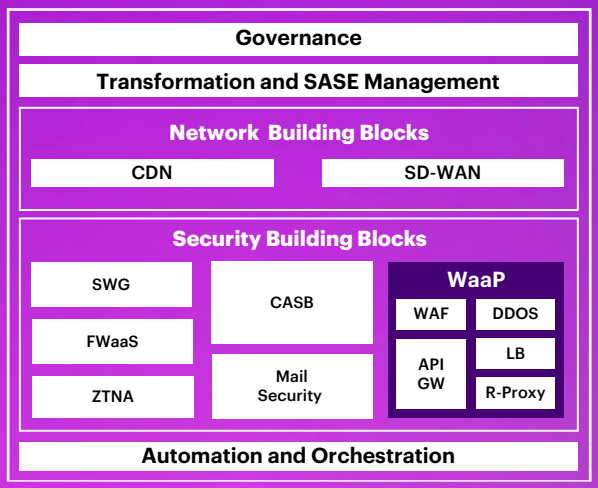


Figure 1: Network and security building blocks are the core components of SASE, while functional layers help operationalize SASE.

The value of SASE is achievable for any enterprise or industry

As an emerging architectural framework, SASE is a component that enables a secure-by-design network. And because technology is rapidly moving from data center-centric network security to identity based, adaptive secure network access, SASE bridges this security gap. Successful implementation employs a comprehensive approach to integrating domains such as identity, cloud, security, infrastructure, network, governance and operations. Additionally, SASE applies zero trust—"never trust, always explicitly verify"—authentication to users, devices and applications. Zero trust is the crucial comprehensive data-centric cyber security strategy for modern threat defense.

By integrating zero trust and SASE efforts into a single initiative, companies increase scalability, reduce complexity, increase automation and strengthen secure access capabilities, as well as manage their organizations' overall security postures. Further, the integration of network and security capabilities help optimize operations of an organization's security tools.

Successful implementation employs a comprehensive approach to integrating domains.

Why enterprises need SASE

Technical debt:
Organizations can consolidate technology solutions, converging network and security solutions to reduce costs while also improving security.

Distributed workforce:
Enabling organizations to consistently provide secure access for a distributed workforce has moved from a "good-to-have" to a "need-to-have" solution. By leveraging SASE, cloud-delivered security drives significant short- and long-term value for modern workforce trends.

Network security at scale:
Every security leader must consider scalable security solutions that grow with the organization (or shrink with economic downturns).

User experience:
Providing direct access to SaaS applications, for example, and leveraging massively scalable networks with ultra-low latency ensures the best digital experience for end users.

Mergers and acquisitions:
M&A activity introduces additional risk vulnerability, so the potential for security related incidents increases. SASE accelerates collaboration and secure connectivity between disparate organizations who may have different levels of security maturity.

Third-party access:
Third-party companies often receive privileged network access that can leave organizations open to unknown threats. SASE enables secure access to specific identified systems and applications with real-time visibility, enforcing the principle of least privileged access.

Enhanced data protection:
The traditional need for VPN connectivity to a data center is going away—as SaaS and cloud-based applications become the standard, organizations must leverage a cloud-first solution to provide traffic inspection and enhanced data protection, including data discovery and identification of shadow IT.

SASE is more than a set-and-forget solution

SASE is a convergence of security and networking capabilities organizations can leverage as a unified platform that enables security and networking functions and, potentially, new business models. SASE alone, however, is not a "magic bullet" for modernizing operating models, and organizations that perceive their SASE security needs as a "set-and-forget" solution must now recognize that achieving zero trust is a journey unique to each enterprise.

Organizations must consider how SASE can complement existing security solutions and, more importantly, meet their company business objectives. Although SASE provides a comprehensive security solution, SASE does not replace other security solutions such as endpoint detection and response (EDR) or security information and event management (SIEM).

For this convergence of capabilities into a single SASE platform to be successful, network and security services must be modernized. For most organizations, this modernization looks like:

- A revised and updated operating model for both network and security where roles and responsibilities are clearly understood
- Essential integration with other security domains such as security operations
- Governance controls updated to support and sustain network and security services

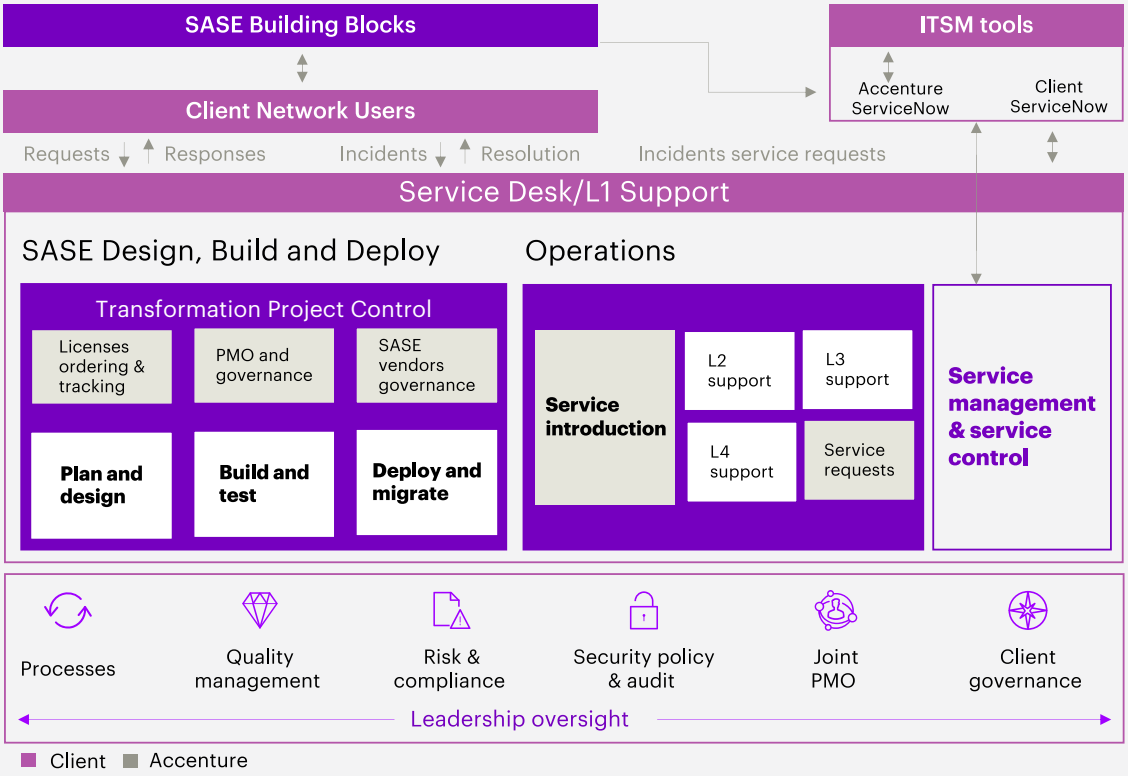


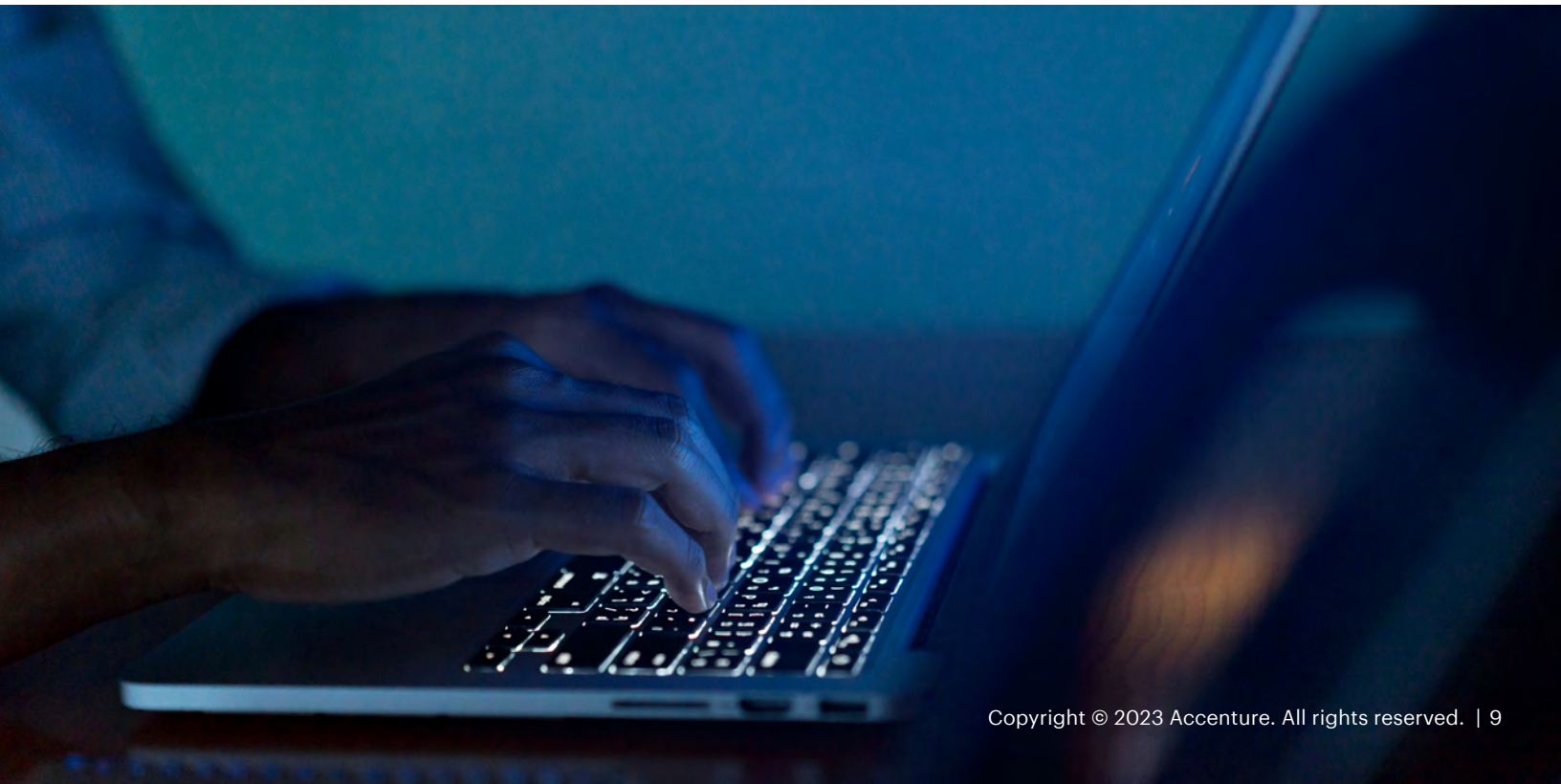
Figure 2: The Accenture modern SASE operating model

Ultimately, SASE is a foundational capability for an enterprise along its transformative journey to achieving zero trust. A modern SASE solution, then, combines the capabilities of always-on VPN, CASB, SD-WAN and FWaaS delivered through a cloud hosted platform. And, as with any enterprise-related technology, maximizing return will require appropriate preparation, collaboration and architectural alignment to address factors such as continuous operation, maintenance, updates, and adoption of new features and capabilities as they become available, such as the addition of cloud wide-area network (WAN).

Businesses must assess goals and needs before implementing SASE

Organizations must carefully assess their goals and needs before implementing SASE, considering their geographies, regulatory environments and existing network and security solutions, as well as architecture and application requirements and operations. For example, an underestimation of the complexity of SASE implementation directly correlates with a lack of operational readiness. That's why organizations need to start with small steps, one after the other, for successful transformation, rather than attempting multiple giant leaps at one time.

Plus, too often, with traditional security tools, it is left to the organization itself to "stitch" various security tools, together, with the goal of achieving control and visibility. Further, due the variety of security tools and vendors in an organization's tech stack, enabling orchestration and automation of incident response can become a challenge. By adopting SASE, businesses can facilitate and accelerate adoption of a holistic security platform that enforces security policies consistently across various personas while seamlessly integrating with the security operations team for visibility and automated response.



Roles, responsibilities and user experience

User experience has not always been considered a security requirement. However, improving user experience is a key business requirement for attracting and retaining talent, especially in the current work-from-anywhere environment. In fact, over the recent three to five years, user experience has become a critical success measure for delivery of security projects. SASE facilitates effective access to daily applications, enhancing the user experience.

Additionally, when an organization's security operations are siloed—that is, with limited collaboration across functional areas and inadequate understanding of risks, criticality of the data and/or applications running across the network—this situation creates a business and technical misalignment. A zero-trust approach enabled by SASE allows the security controls to adapt to the context of a connection. For example, a senior vice president of mergers and acquisitions has different read-and-write access to sensitive information depending on their connection location—in office versus at a coffee shop. The trust score is re-evaluated constantly, and the security controls adapt dynamically to the change of network connection. For businesses to realize maximum value from their investment in SASE, collaboration across the various security domains is crucial.

Governance, risk and compliance (GRC) controls

GRC controls are critical to the long-term success of SASE and the larger zero-trust journey. Such initiatives often stall because the controls don't support and enable forward-thinking technology or initiatives. Further, some organizations operate without adequate GRC controls—if written at all—that require effort to modernize. In many cases, business leaders may not even allocate budget and resources to implement SASE and zero-trust GRC. Organizations today, though, need to ensure that GRC is part of the conversation. When determining plans and strategies, businesses must review their GRC controls to identify what needs to be deprecated, modernized or net-new creation in support of successfully adopting SASE across their organizations.

SASE facilitates effective access to daily applications, enhancing the user experience.

SASE is not the end of the network security journey

SASE is not the end of the network security journey, but rather a step toward new emerging trends. Current technology shifts to SASE can help an organization move away from a static environment and set the foundation for adaptive controls and automation that further protect the data and mature the overall security environment.

When such modernized transformation brings essential components together—much as an orchestra brings finely tuned instruments together—the result is a harmonious outcome. If one section is off beat, out of tune or plays a wrong note, however, the effect is felt by the entire symphony! Zero trust and SASE must harmonize in the same way. Thus, when core domains such as identity, device, network, application, data and security operations function well together, the quality of the symphony reverberates throughout the organization as well-defined, integrated and mature security capabilities.

Accenture accelerates value with SASE

SASE truly is a journey, not a weekend deployment in an approved change window or a race to deploy an agent to an endpoint. Our expertise in zero-trust domains such as identity, device, network, application, data and security operations enables us to conduct these symphonies—in essence, providing quality end-to-end service lifecycle capabilities to support clients at all points of their SASE journeys.

Zero trust is the symphony and SASE is its most important instrument.

Contacts

Rex Thexton
Senior Managing Director, Accenture Security, Security Technology Officer

Martin Glowik
Managing Director, Accenture Security, Cyber Mesh, Zero Trust and Secure Edge Lead

For more information, please contact us at zerotrust.security@accenture.com

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities. Visit us at www.accenture.com.

Accenture Security *is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us* ***@AccentureSecure*** *on Twitter,* ***LinkedIn*** *or visit us at* ***accenture.com/security****.*