White Paper

Network and Security Transformation Empowers the Business: Aligning the SASE Road Map to Strategic Organizational Goals

Supported by: Lumen and VMware

Ghassan Abdo Christopher Rodriguez

October 2022

INTRODUCTION

Digital transformation (DX) has provided key business benefits, with most organizations reporting an increase in employee productivity in the range of 25%–49%. However, there is no single threshold to cross with digital transformation. Undoubtedly, more change is coming, as business leaders look to technology to help navigate emerging challenges.

The drawback to DX implementation is that technical and business challenges have emerged as a result. Digital transformation has followed specific use cases and short-term objectives out of necessity. In some cases, this transformation was not optional, as the network perimeter shifted from the corporate office and datacenter to workers' home offices and cloud applications in the short span of a few weeks in 2020. This evolutionary process has introduced a level of complexity that confounds traditional security practices and tooling leading to heightened business risk.

Accelerating Network Transformation with Secure Access Service Edge

Secure access service edge (SASE) is an emerging framework for modernizing network and network security infrastructure in a manner that addresses challenges, both old and new. However, confusion about SASE has become a complicating factor on its own right.

For IT buyers, the key is to understand how to approach network and security transformation in a manner that best enables the business to meet essential strategic goals for optimal customer experience, increasing trust, business agility, resiliency, and robustness.

This IDC White Paper presents a clear overview of SASE beginning with key concepts, benefits, and approaches and including important use cases for reference.

SITUATION OVERVIEW

Networking Trends

Networking is experiencing macro factors that have an impact on network economics, customer experience, and business resiliency improvements. These factors include the following:

- **Proliferation of IoT and growth of global ecommerce moving intelligence and data gathering to the edge.** IoT is a primary example of the need to gather customer or appliance data close to the point of generation to ensure timely response to adverse conditions. Primary use cases include IoT, content management, media applications, and manufacturing.

- **Adoption of multicloud strategies to avoid lock-in and serve the productivity needs of a distributed workforce.** Multicloud and hybrid cloud adoption requires enterprises to implement a multicloud networking strategy to ensure secure and timely access to cloud-hosted data and applications.
- **Increasing role of customer experience as a key beneficiary of DX.** Enterprises are demanding a rich-media experience to address the needs of their customers, especially at the intersection of virtual and physical worlds. This will include interactive and personalized multimedia use cases and the use of AR/VR to enrich customer experience.
- **Emergence of low-latency edge use cases to optimize operations and improve user experience.** These include predictive maintenance support for the manufacturing industry and the use of video-enhanced ecommerce to deliver a more immersive customer experience.

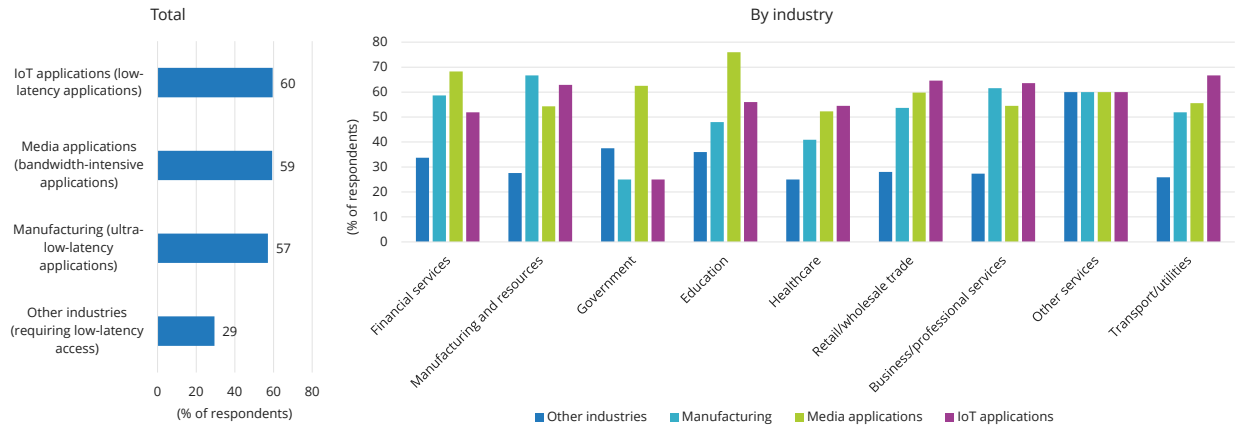
A 2022 IDC survey of U.S. enterprises indicates that IoT, media, and manufacturing are the top use cases for edge services (see Figure 1). These priorities tend to shift depending on the industry as reflected in the same figure.

Implementing a successful DX strategy will require enterprises to put networking transformation at the heart of their strategic decision-making process.

FIGURE 1

Top Use Cases for Edge Services

Q. What are your company's main use cases for edge services?



n = 500

Source: IDC's *Enterprise Communications Survey,* August 2022

In summary, implementing a successful DX strategy will require enterprises to put networking transformation at the heart of their strategic decision-making process.

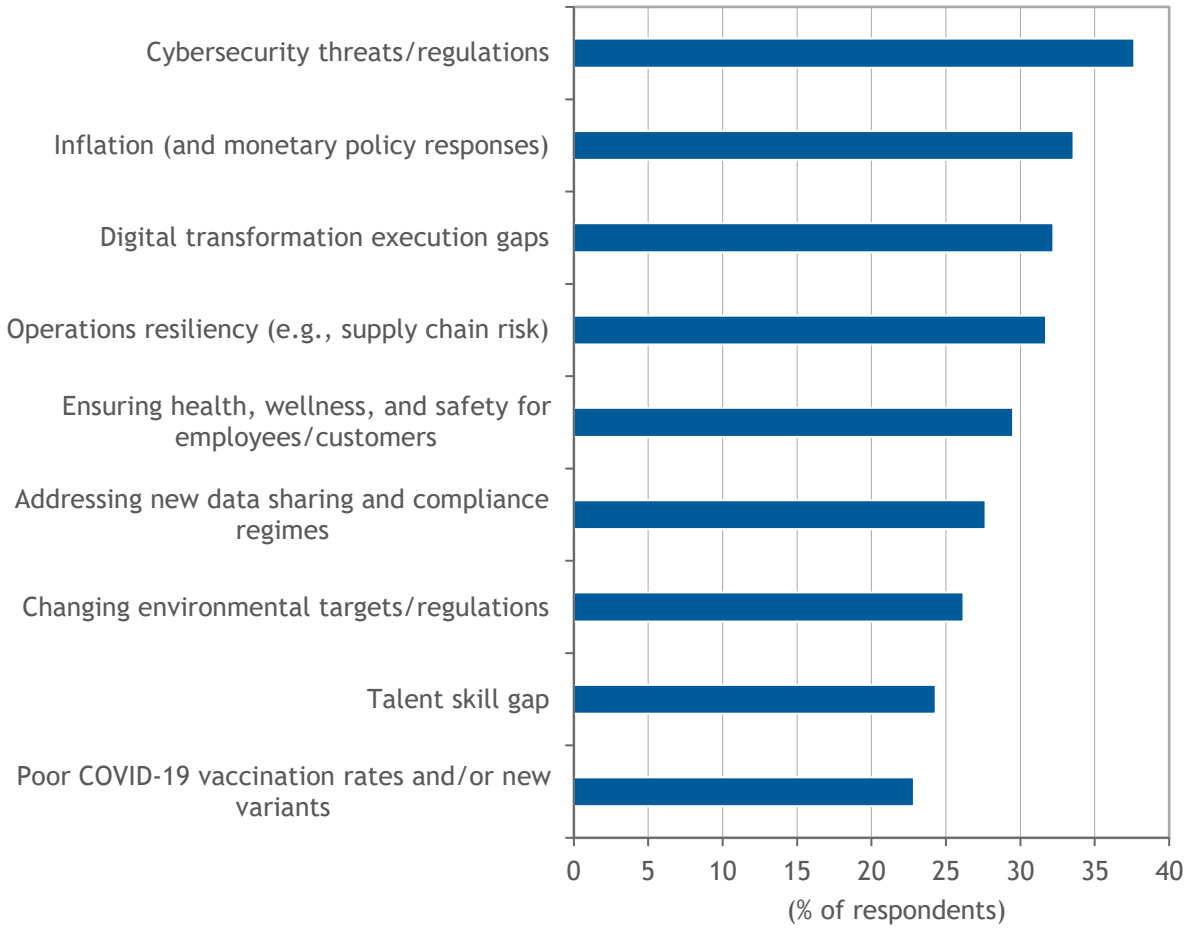
Security Trends

While network transformation projects offer multiple benefits, business leaders are facing a number of challenges as well. IDC research shows that cybersecurity threats and related regulatory requirements are a top-of-mind concerns for business leaders, ahead of even inflation, supply chain challenges, and COVID-19 (see Figure 2).

FIGURE 2

Cybersecurity Risk Is the Top-of-Mind Business Concern

Q. Of the following political, social, and economic risks, which three do you expect will have the greatest impact on your organization's technology investment plans in the next two years?



n = 810

Source: IDC's *Future Enterprise Resiliency and Spending (FERS) Survey, Wave 12,* January 2022

Despite growing concerns about these macro risk factors, businesses are primarily leaning into technology as a means to address challenges, with 42.5% of decision makers planning to increase budgets as the top response, ahead of options such as delayed projects or less expensive alternatives (source: IDC's *FERS Survey, Wave 3,* April 2022, n = 300).

Transformation Requires Enhanced Security

Digital transformation has been beneficial overall but was not without challenges. The network transformation process has unfolded organically, driven by business needs and urgent use cases. For example, the COVID-19 pandemic spurred a drastic increase in VPN usage in order to support the sudden migration of the workforce from in-office work to work-from-home access in March 2020.

Establishing basic access was the first and foremost priority at the time, and security and performance considerations were treated as secondary concerns for refinement at a later date. This unexpected, accelerated network transformation resulted in a high degree of complexity throughout the network and application infrastructure.

Unfortunately, complexity is the enemy of security. Protection gaps have emerged, as point products are required across various environments, including on premises, branch, and various permutations of cloud, leading to inconsistent policies and protections. This disjointed security architecture is vulnerable to evasion tactics and multivector attacks. Given that incomplete security visibility is a challenge, siloed security tools fail to share the insights necessary to prevent data breaches.

Threat actors have noticed and taken advantage of disjointed security efforts, as pernicious threats such as ransomware, advanced persistent threats (APTs), and insider threats have propagated. IDC research shows that ransomware has been a particularly pronounced business problem in 2022. IDC's December 2021 *FERS Survey, Wave 11* (n = 858) illustrates the costs:

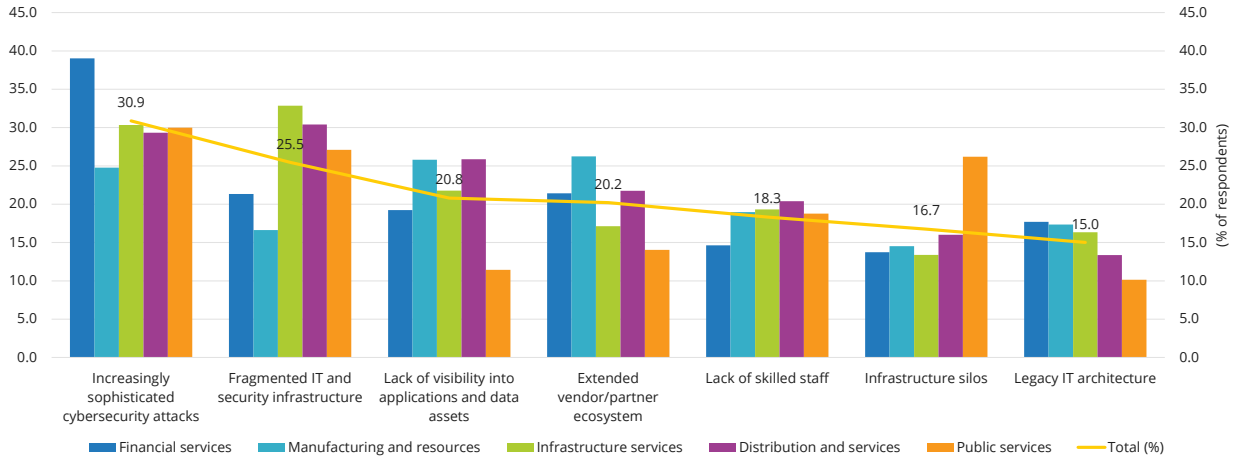
- 44% of organizations experienced ransomware incidents in the previous 12 months.
- 18% of ransomware victims that paid the ransom paid 6 figure sums.
- 24% of survey respondents reported a business disruption lasting at least 1 week.
- 22% of targets also had valuable sensitive or secret data stolen.

Ultimately, this accelerated, aggressive, and often forced transformation process has introduced security challenges including "fragmented IT and security architecture" that inhibit trust, affecting organizations across financial, manufacturing, services, and infrastructure, as shown in Figure 3.

FIGURE 3

Security Challenges Impact the Business via Trust

Q. What are the top challenges inhibiting trust in the organization (internally and externally)?



n = 507

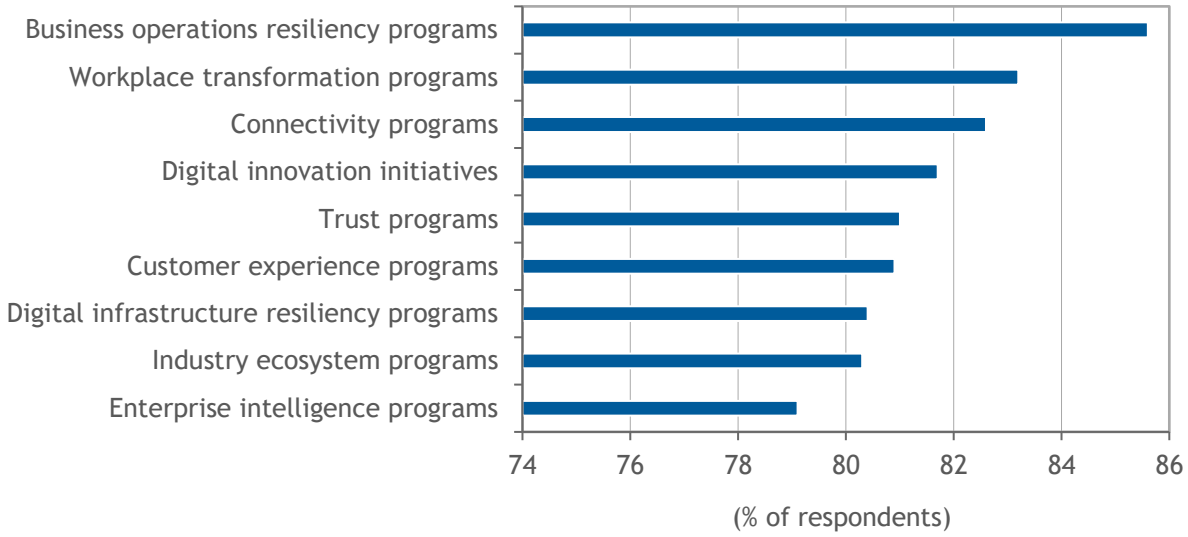
Source: IDC's *Future of Trust Survey,* February 2021

Overall, digital trust is a key ingredient enabling businesses, their customers, and partners to work together. IDC research shows that business leaders are adopting trust programs as a way to adapt to and achieve important objectives (see Figure 4).

FIGURE 4

Leveraging Transformation, Connectivity, and Trust to Navigate Emerging Challenges

Q. As a result of the uncertainties related to geopolitical tensions, inflation, supply chain disruptions, and managing the ongoing COVID-19 pandemic, how much of a priority will investments in the following areas be for the rest of 2022 and 2023?



n = 832

Source: IDC's *Future of Trust Survey,* February 2021

IDC defines trust programs as investments in security, privacy, and compliance technologies to improve the organization's risk posture. Addressing security challenges, threats, and security silos in a unified, coherent approach is an important strategy to improve organizational trust. For example, high-priority strategic practices such as connectivity and workplace transformation programs require adoption of new technologies that may introduce vulnerabilities or require adaptations to security strategies, given their nature. Consider:

- **Connectivity programs** include investments in enterprise network infrastructure, 5G, Wi-Fi, mobile applications, and mobile devices to better connect workforce, operations, and partners. Network security was rated the top connectivity-related challenge facing organizations (50% cited this, according to IDC's July 2021 *Future of Connectedness Survey,* n = 607).
- **Workplace transformation programs** include investments in collaborative workspaces, talent development, and management tools to increase employee experience and productivity. When asked about the top challenges when implementing workplace transformation initiatives, 30% of respondents noted an ongoing struggle between employee flexibility and security requirements (source: IDC's *Future of Work Survey,* March 2020, n = 415).

Emerging Technologies Address Aspects of the Problem

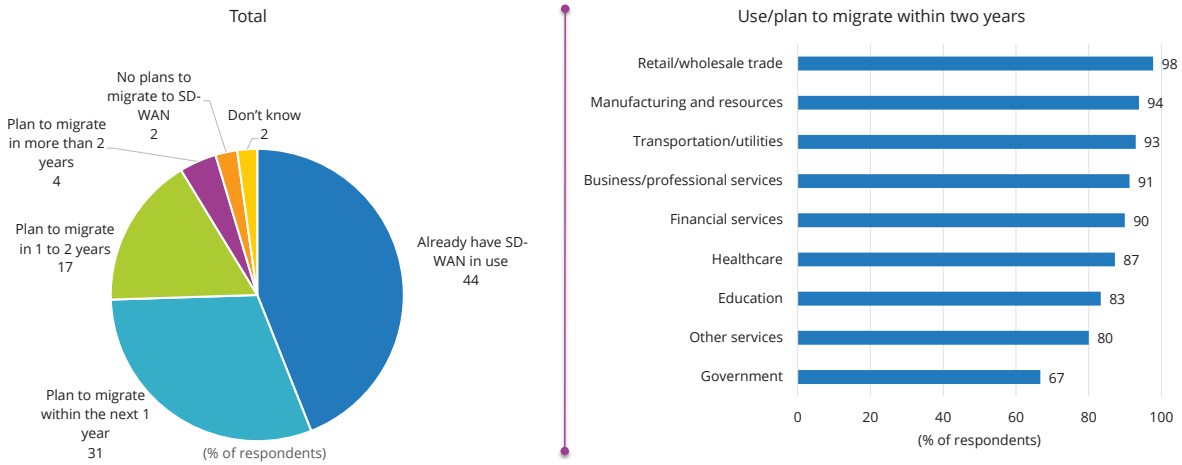
Networking Overview

Recent advances in networking architecture are having positive impact on business resiliency and the ability to deal with increasing and varying traffic demand. At the core of this architecture is the move to separate the control plane from the data plane. Recent surveys indicated continued strong adoption of SD-WAN. 44% of enterprises have already implemented the technology, and 48% of enterprises plan to implement SD-WAN in the next two years (see Figure 5).

FIGURE 5

Enterprise Migration Plans to SD-WAN

Q. Does your company plan to migrate any of your existing WAN/network connections to a SD-WAN alternative?



n = 500

Source: IDC's *Enterprise Communications Survey,* August 2022

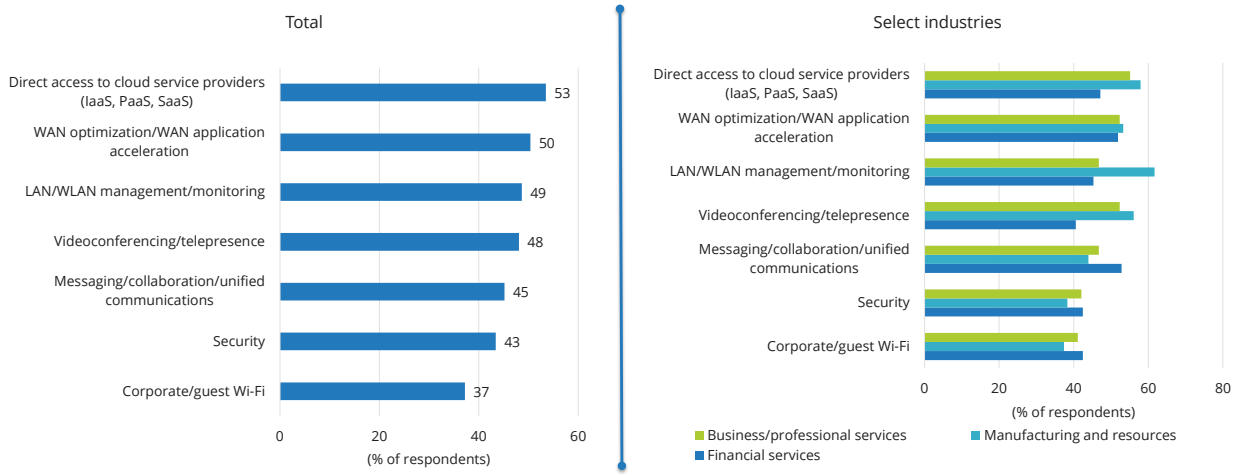
Business agility is critical to certain industries such as retail, manufacturing, and financial services to fend off competition from digitally native competitors and improve operational efficiencies. As enterprises adopt a more distributed hybrid work environment, they seek scalable network solutions that are secure and economically managed.

Enterprises are challenged to optimize multicloud connectivity costs, security, and management of disparate networks. A software-defined architecture with integrated security can help them achieve these goals. An IDC survey highlights that secure direct internet access and dynamic path optimization and application performance are the most valued features of SD-WAN that enterprises want for their particular environment (see Figure 6).

FIGURE 6

Most Valued Features of SD-WAN

Q. Which of the following features of an SD-WAN solution do you think offer the most value for your environment?



n = 500

Source: IDC's *Enterprise Communications Survey,* August 2022

FUTURE OUTLOOK

SASE Overview

While emerging security technologies improve upon existing practices and tooling, their introduction into mainstream security practices has further exacerbated security complexity resulting in siloed approaches. Similarly, while many security technologies are better suited to the technical needs of modern IT environments and practices, they were not designed with networking requirements in mind.

SASE, at its core, is an attempt to address these challenges through integration of key network security technologies, along with important networking functionality, to ensure a unified and performant architecture for secure networking. By definition, SASE integrates key security technologies such as:

- Firewall
- Intrusion prevention systems
- VPN/ZTNA
- Secure web gateway
- Cloud access security broker (CASB)

Optional security technologies include:

- Browser isolation
- Data loss prevention (DLP)
- Web app firewall
- Sandbox-based threat analysis

SASE also requires the integration of key networking functionalities such as SD-WAN, including:

- Centralized management of networking resources
- User-defined policies
- Automated path selection and optimization
- On-premises or cloud-hosted control plane
- Hosting of various virtual network functions (VNFs)
- Fully managed, comanaged, or self-managed deployment

The combination of these core security and networking capabilities makes SASE particularly appealing for organizations with a large WAN, including multiple branch offices. As SASE is a cloud and edge-delivered service, it is also well positioned to support remote workers and IoT.

SASE unites new security tools built on software-based frameworks offering centralized management, cloud-centric user access, and a flexible architecture that is easily maintained and upgraded. These tools include:

- **Zero trust network access (ZTNA):** Protects access to internal resources from anywhere, on any device based on least privilege access permissions, strong authentication, and continuous monitoring
- **Cloud access security broker (CASB):** Provides protection and control of cloud resources (IaaS and SaaS) including threat protection, data protection, and observability
- **Secure web gateway (SWG):** Provides protection of user devices and data while accessing browser-based web resources including unmanaged sites such as YouTube, Consumer Reports, and Advance Auto Parts (Employees may require access to some of these sites for their job [such as Hotels.com and other hospitality and travel sites], more so than others [Netflix or Amazon.com]. But IT organizations are less concerned about policing these online activities and more concerned with securing them.)
- **Next-generation firewall as a service (NGFWaaS):** Supports deeper branch location protection at the perimeter including application protection using deep packet inspection with intrusion detection and prevention (IDS/IPS)
- **Observability, analytics, orchestration, and advanced threat detection:** Adds threat intelligence (XDR), integration with SOAR tools providing bidirectional telemetry collection, security analytics for advanced threat detection, and edge enforcement

Implications for Enterprises

Traditionally, security inspections have been a bottleneck to application performance. Networking teams frequently vetoed investments in new security tools. By addressing the needs of two distinct audiences in a coherent fashion, SASE enables businesses to overcome security and performance limitations that hinder new business use cases.

Benefits to Networking/Delivery

SASE provides many benefits to networking and delivery, including:

- SASE allows for deployment of networking resources on premises, at the service provider edge, or via centralized cloud deployment. This deployment approach optimizes the utilization of network resources based on performance and quality-of-service requirements, thereby reducing overall networking and related costs.
- The SASE commercial model is similar to a cloud consumption model, which is usage based. Moving from a capex to an opex cost model may be attractive to many enterprises.
- Hybrid workforces expect parity in terms of IT experience regardless of access method, whether they are remote, in the office, or on the road. With the ability to define and configure individual policies, SASE can harmonize the employee experience independent of location.
- In today's environment with high dependency on cloud applications, hybrid work environments, and increasing demand for rich media services, it is hard to predict traffic demands. SASE provides flexibility in terms of connectivity choices and can better manage unpredictable changes to traffic patterns.

Security Improvements

There is no "magic pill" in security. SASE converges existing security infrastructure that has largely been disjointed and in recent years has been increasingly ineffective to scalable software services. The benefits include:

- **Centralized management/consistent posture:** SASE provides a unified, coherent secure access point for device, network, and employee access to secure business applications. IT organizations enforce a consistent set of policies and apply the same detection methods across the entirety of the organization, locations, and supporting partners.
- **Increased visibility:** SASE gathers telemetry across multiple network and cloud connections for ingestion into SIEM, SOAR, and XDR platforms. These insights improve the breadth and depth of security understanding and risk mitigation.
- **Elimination of security silos:** Correlation of multiple signals is required to detect advanced threats. SASE delivers unified visibility reducing time to detection, which is a critical factor against ransomware.
- **Edge-based threat prevention:** Edge security ensures that threats are blocked at the point of entry. This ensures a positive user experience for legitimate users. Security decisions are made nearest to the end user, instead of backhauling user traffic to a centralized firewall for inspection.

Recommendations for SASE Adoption

A better understanding of SASE enables IT organizations to adopt a practical road map for adoption that accounts for real-world business considerations. IDC notes strategic recommendations for SASE adopters as discussed in the sections that follow.

Stair-Step Adoption Process Lowers Risk

The early iterations of SASE looked daunting, requiring an all-in-one, turnkey, purely cloud-delivered approach. However, in practice, an all-or-nothing approach escalates risk of project failure. A better option is a graduated, milestone-based approach that can enable a low-risk adoption path. The SASE software-based framework supports this grow-as-you-go approach. The following are potential milestones for consideration:

- **Essential:** SASE should be rolled out to key use cases that are ripe for modernization. For example, VPN-based remote access continues to be a weak link in security practices today and should be upgraded to ZTNA as soon as possible. SASE offers key security practices such as CASB cloud-based SaaS and infrastructure security that go hand in hand with networking practices such as local internet breakout and SD-WAN application-aware routing.
- **Advanced:** SASE architecture can then be extended to more challenging technology areas. IoT and OT security are examples of security practices that must be light touch and low latency. As a result, special considerations may be required.
- **Custom:** 5G, autonomous vehicles, Smart Cities, and other transformational technologies will require specialized security and networking considerations. In some cases, such as smart factories, threat detection and alerting remain important, but automated block may be a nonstarter.

Consideration of Business Requirements

SASE adoptions must account for business objectives and concerns, which are severely hampered by complexity. When survey respondents were asked about the three greatest barriers to achieving their organization's digital infrastructure resiliency goals over the next two years, the top response (38.7%) was "cost and complexity of supporting multiple generations of infrastructure and applications across bare metal, VMs, containers, and public clouds" (source: IDC's *FERS Survey Wave 2,* March 2022, n = 796).

Legacy security architecture is exponentially more complicated, as specialized tools and form factors are required to secure modern networks. The problem is multiplied after years of mergers and acquisitions and changes in vendors. This degree of technical debt is largely considered unsustainable, especially in security where visibility and control gaps are emerging as a result. SASE providers should be able to demonstrate a realistic plan to help customers retire legacy solutions and demonstrate value.

Balancing Performance and Security Needs

Security and performance have long been considered trade-offs based on legacy approaches. In the modern era of hybrid work, diverse devices, and sophisticated use cases, low-latency performance is a foundational requirement. As a result, SASE must provide security while supporting the needs of networking and security teams. SASE providers must demonstrate best-of-breed security without impeding network performance or user productivity.

Improving Security

While there is value in consolidation of several security services and appliances into one unified platform, the value cannot end there. SASE should ultimately improve security, by enabling sharing of threat data and improving observability across all network entry points. Vendors should demonstrate this capability natively, and potentially through expanded ecosystems with security orchestration tools and XDR platforms, with some aspects available now and in upcoming product road maps.

Managed Services

A growing skill shortage is another top concern for business leaders, with 34.5% expressing concern about staffing shortages (source: IDC's *FERS Survey, Wave 3,* April 2022, n = 828). As a result, many organizations are looking for outside assistance with network transformation projects, as well as cybersecurity initiatives. Notably, a "lack of personnel" and "lack of in-house talent" were two of the top 4 reasons for choosing a security services provider (source: IDC's *Global Outsourced Cybersecurity Services Survey,* December 2021, n = 517). This provider approach is particularly relevant for SASE given the previously noted questions raised by convergence of networking and security.

OVERVIEW OF THE LUMEN APPROACH TO SASE

Diverse Technology Partnerships Offer Best-of-Class Options

Lumen has multiple SASE partners. These options allow businesses to select the approach that best suits them, whether an SD-WAN first approach or a best-of-class security focus. Lumen is continuing to expand its partner options for SASE.

Leveraging Lumen's Networking Expertise and Infrastructure

Lumen complements its extensive SASE product offerings with three key differentiators:

- Networking expertise with centralized control and customizable managed services
- Security expertise with a deep bench of capabilities that enable a wholistic security solution
- Service wrapper with options to size the level of support to meet customer needs

Aligning Technology and Business Processes

A key goal of Lumen SASE is to align the technology investment with business processes to maximize business benefits. This alignment process relies on the following capabilities:

- **Lumen Marketplace:** This simplified digital buying experience guides customers through the process so they can purchase the right network and security capabilities for their organization.
- **Multilevel managed service options:** Customers have the option to manage their own SASE solution with basic levels of Lumen support or have Lumen fully manage the deployment, implementation, and ongoing management of their customized SASE product.

Fit Within the Broader Lumen Portfolio

Adaptive Networking for Edge to Cloud Integration

Enterprises are seeking solutions that allow easy integration of applications spanning edge to cloud deployments. Lumen adaptive networking facilitates application access independent of deployment model, on premises, edge, or cloud. A software-defined architecture provides flexibility in terms of on-premises and cloud-based deployment of the control layer. This provides key benefits as follows:

- Pay-per-use services with dynamic cloud connections to public, web, and SaaS applications and infrastructure and bandwidth that instantly scales on demand
- Increased application performance that improves the latency response of time-sensitive applications
- Improved go to market with a flexible service delivery model that allows for quicker application deployment
- Reduced cost through a cloud-based consumption model offering that simplifies deployment with optimized cost in IT time savings and reduced capital investment
- Innovation that provides a competitive advantage using software-driven and edge-enabled infrastructure solutions

Comprehensive Risk Mitigation and Protection

Lumen SASE Solutions further bolsters the company's enterprise security portfolio, which has included key functionality such as DDoS mitigation, threat intelligence, and managed security services:

- **Application protection:** Lumen protects web applications against the rigors of the internet, defending against vulnerabilities, zero-day exploits, malware, bots, and common OWASP Top Ten threats such as SQL injection.
- **DDoS mitigation:** Lumen DDoS mitigation protects against business disruption resulting from DDoS attacks. The solution provides full coverage against all forms of DDoS, including Layer 7 attacks, when combined with Lumen application protection capabilities and global scrubbing centers.
- **Managed security services:** Lumen offers managed SOC and XDR to help offload the burdens of alert triage, investigations, and threat hunting.
- **Threat intelligence:** Black Lotus Labs threat intelligence provides insight into attack trends, emerging threats, and zero-day attacks. This insight is propagated across Lumen security services to provide protection against the myriad of online threats facing businesses today.

CHALLENGES/OPPORTUNITIES

SASE is a lofty concept for which Lumen customers may require an ongoing level of education and hand-holding to achieve. While Lumen is developing strategies to support these types of buyer needs, some misperceptions are bound to linger. The challenge may be inward as well, potentially requiring a steep learning curve to update vast sales teams and partners.

CONCLUSION

Network and security transformation is a strategic imperative that can enable the business to meet key strategic goals. However, the approach to transformation must be grounded in reality. A pragmatic, use case–driven approach to SASE adoption will enable businesses to increase trust, productivity, and customer satisfaction and, ultimately, propel the business forward.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com