Publication date:
May 2022
Author:
Cindy Whelan

SASE Protects a Changing Workplace Against Dynamic Threat Environments

Commissioned by:

Brought to you by Informa Tech

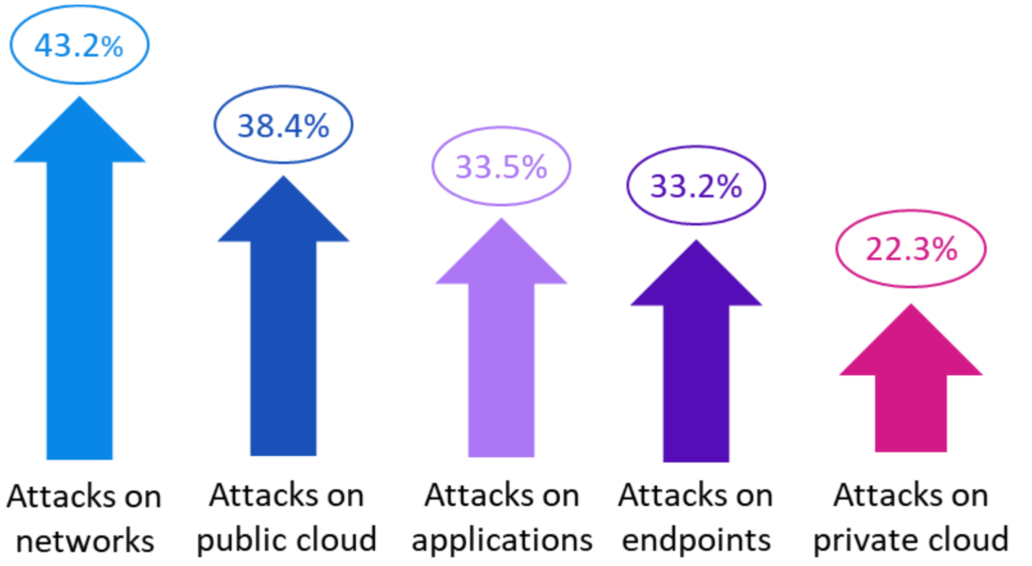
Contents

Summary

Software-defined wide area networking (SD-WAN) proved instrumental to early movers in digital transformation. The solution optimized connectivity budgets without sacrificing network and application performance. SD-WAN let enterprises deploy internet and MPLS based on the needs of each site. Many in the industry believed that connectivity cost savings would be SD-WAN's primary value. It quickly became apparent that the most valued benefit was SD-WAN's inherent security features: the ability to monitor endpoints, manage policies, and protect traffic. Service providers rolling out SD-WAN offers saw the combination of routing and security emerge as a main priority for enterprise adopters. The concept of secure access service edge (SASE) appeared in 2019, integrating network and security functions more tightly to support today's distributed business environments across public cloud, remote workers, and mobile endpoints.

The COVID-19 pandemic raised the stakes for enterprise network security. Home offices, remote work, and the adoption of cloud-based business applications opened new attack surfaces for cybercriminals. Distributed denial-of-service (DDoS) attacks, malware, ransomware, and other criminal and disruptive activity increased during the pandemic. Enterprises surveyed by Omdia cited an increase in security attacks since 2020 across networks, applications, public and private clouds, and fixed and mobile endpoints (**Figure 1**).

Figure 1: Enterprises report increased security incidents between 1Q20 and 2Q21



Notes: n=310; regions: Americas, Asia, Western Europe

© 2022 Omdia

Source: Omdia Cloud & IT Services Survey, August 2021

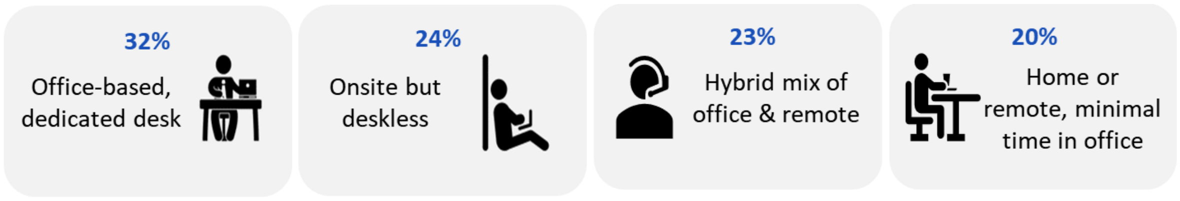
Remote work and cloud applications raise security challenges

One of the major changes wrought by the pandemic is in the workforce model. Full-time and part-time remote work is now a widespread practice. Companies found that some employees are more productive at home. Other workers must be on site. There are cost benefits to these new workforce practices:

- Having fewer employees in an office reduces the need for office space and connectivity, enabling companies to save on facility leases and building operations costs.
- Remote work lets enterprises attract and hire key talent without the need for relocation.
- Flexible workplace models can also improve employee satisfaction and reduce attrition.

Enterprises are crafting workplace policies that give employees options while maintaining business operations (**Figure 2**).

Figure 2: Postpandemic, enterprises expect to support a mix of employee work styles on a permanent basis



Notes: n=1,576; regions: Americas, Asia, Western Europe

© 2022 Omdia

Source: Omdia 2022 IT Enterprise Insights, October 2021

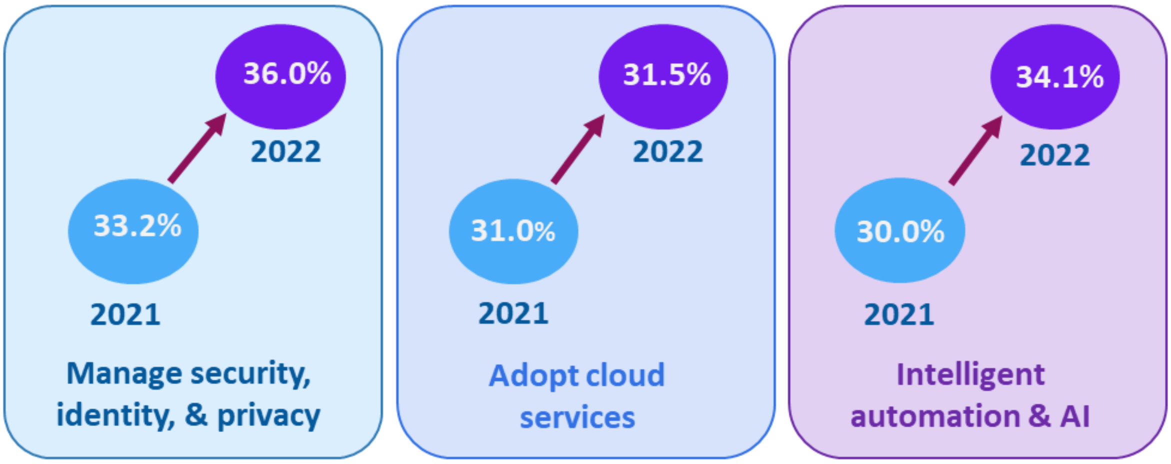
Before the pandemic, enterprises focused their network services on office locations. This static perimeter made it easier for IT and security teams to control applications performance and secure employee activities. By early 2020, companies were migrating from private WAN services and on-premises equipment to software-defined networking and applications delivered “as a service” from public clouds.

Well-defined perimeters were torn down by the outbreak of COVID-19 in 2020. Suddenly IT and security teams needed to connect and secure employees over residential internet services. They needed to migrate business applications and workloads to the cloud so that employees could continue to perform their jobs and maintain business operations.

Disruption and uncertainty led enterprises to reevaluate their business plans. They delayed or revised some IT projects to reduce costs and conserve cash. However, the changes brought about by the pandemic pushed many enterprises to accelerate digital initiatives. Companies invested in supporting their remote workforces, giving them access to the tools they needed to perform their jobs with satisfaction. They kept the business running first, then worked to adapt their security posture to find and close any security holes that bad actors could exploit.

Although lockdowns are less common across the world as the pandemic crisis eases, enterprises are prioritizing how they secure company data and communications in a cloud-based business world, given the expected permanence of the changes to the workplace mix. Results of Omdia's annual IT Enterprise Insight surveys conducted in late 2020 and again in late 2021 highlight an increased focus on security, cloud, and automation (**Figure 3**). For example, 33% of enterprises surveyed in North America and Western Europe in late 2020 noted that they planned an increased focus on managing security, identity, and privacy for 2021. The 2021 survey found that this number increased to 36% as enterprises anticipated the increase in remote workers and cloud adoption in 2022 and beyond. New workforce models and cloud applications mean that security must extend beyond offices and be integrated into every network touch point from branches to remote workers and "road warriors."

Figure 3: Enterprises expect the long-term impact of COVID-19 will be to increase the relative importance of key technology areas



Notes: 2022 n=1,576; 2021 n=1,974; regions: Western Europe and North America

© 2022 Omdia

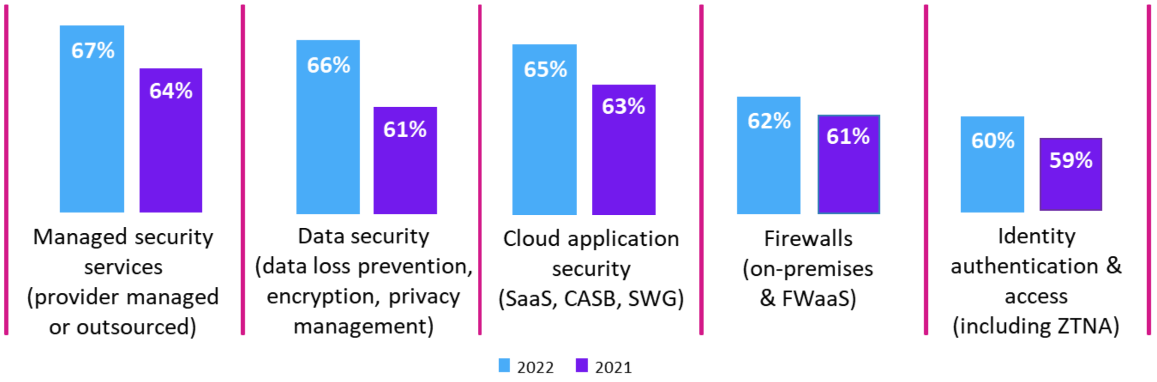
Source: Omdia 2022 IT Enterprise Insights, October 2021; Omdia 2021 IT Enterprise Insights, October 2020

Security plays a prominent role in enterprise technology investment plans

Enterprises were caught off guard by the pandemic and how quickly it affected operations and increased threats to their networks and clouds. The pandemic demonstrated to enterprises that even low-likelihood events must receive more attention when security risks are evaluated. In the future, cybersecurity risk managers will focus more on catastrophic possibilities, regardless of their likelihood, to mitigate the impact of a disaster on the company.

Planned investment increases across most security areas point to enterprise concerns about protecting the company. Key areas of investment growth include traditional security capabilities such as firewalls and an increased focus on protecting data and applications by tightly managing access to network and business applications. When survey results from 2020 and 2021 are compared, 18-month investment plans for enterprises show a steady rise in all areas of security, reflecting a growing concern over ever-increasing security threats (**Figure 4**).

Figure 4: Enterprises are increasing planned investment in key areas in 2022–23



Notes: 2022 n=2,256; 2021 n=2,350; regions: Western Europe and North America

© 2022 Omdia

Source: Omdia 2022 IT Enterprise Insights, October 2021; Omdia 2021 IT Enterprise Insights, October 2020

Managed security services

Enterprises can look to managed security solutions to complement existing in-house capabilities or as a fully outsourced solution. Service providers that can be considered strategic partners have developed a professional services wrapper to deliver services including threat intelligence and monitoring, patch management and software upgrade services, and management and security testing such as audits, threat response, and more to help offload the burden of managing an enterprises' network and security posture.

Data security

A breach that results in the compromise of personal data is a financial and public relations disaster for an enterprise. Data loss prevention, encryption, and privacy management are critical areas for enterprise network and security teams to protect the company and its employees and customers.

Cloud application security

Cloud access security broker (CASB) tools are critical to managing access to cloud applications by remote employees and those in office locations.

Firewalls

Firewalls have a long legacy in network security, sitting between the network and the internet and inspecting traffic to detect and address threats. Firewall as a service (FWaaS) allows enterprises to access these services in a cloud-based model, which can scale more quickly than traditional hardware solutions and can be tailored to meet the specific security needs of the network.

Identity, authentication, access, management

Today identity is the perimeter, and managing identity is essential to protect an enterprise and its business applications. Capabilities such as zero-trust network access (ZTNA) authenticate access to each application rather than granting broad access to corporate resources, whether devices are located inside or outside the corporate network.

Enterprises take diverse paths to securing the network

This desire to take a wider view of risk and potential threats places security at the core of enterprise network investment and digital transformation strategy. SD-WAN is a key piece of enterprise transformation plans because of its flexibility and inherent security. SD-WAN's central policy management lets enterprises connect branch locations with lower-cost services while maintaining visibility and control over site-to-site security policy.

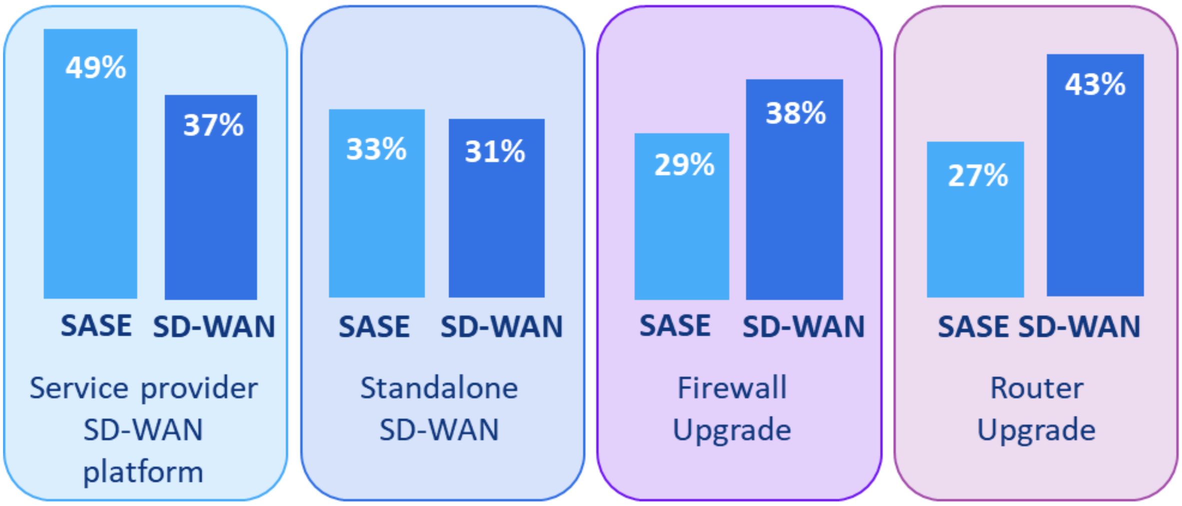
SD-WAN has been widely adopted, but the paths that enterprises are taking in SD-WAN upgrades vary. Enterprise IT leaders must consider many factors when choosing a preferred path. They need to account for existing vendor relationships, in-house expertise, and partner expertise. They need to find a good match for necessary network, security, and management features. They need to think about their current and planned digital applications and network transformation, and how that affects headquarters, branches, cloud migration, and remote workers. There are four SD-WAN paths utilized by enterprises:

- Enterprises may take a network-led SD-WAN approach that leverages an existing router vendor and incorporates new security features for secure SD-WAN.
- Enterprises may opt for a security-led implementation that may be part of a broader security strategy upgrade that leverages an existing firewall vendor, folding in the network for secure SD-WAN.
- Enterprises may opt to partner with a standalone SD-WAN specialist vendor.
- Enterprises may look for a complete integration of network and security, delivered and managed by a single provider. This would embed security more broadly into the network, encompassing SD-WAN and traditional firewall capabilities, with additional tools to protect the business from

malicious web applications and unauthorized user access. This is the product set described for secure access service edge (SASE).

Enterprises that have adopted SD-WAN have primarily looked to router or firewall upgrades, often opting to work with existing vendors to incorporate SD-WAN features into the network. However, enterprises that describe themselves as SASE adopters primarily turn to service providers to supply the solution (**Figure 5**). These service provider partners may already supply the enterprise's network and managed security services and can work with the enterprise to create an integrated solution.

Figure 5: In transforming their network, SD-WAN adopters often rely on firewall and router equipment upgrades; SASE adopters most often turn to service providers



Notes: n=245; regions: Americas, Asia, Western Europe

© 2022 Omdia

Source: Omdia Global Enterprise Network Services Insights, August 2021

SASE is an integrated model for today's complex network environment

Secure access service edge is a new term to describe a network security approach that accounts for increases in remote users and reliance on cloud-based applications. SASE is not its own technology or a service: the term describes a suite of services that combine SD-WAN with other security tools to protect the company from web-based attacks and unauthorized access to the network and applications. The main elements of SASE are described in **Table 1**.

Table 1: SASE elements

Software-defined wide area network (SD-WAN)	Platforms that separate overlay network management from underlying network transport infrastructure. SD-WAN supports dynamic application prioritization and provides enterprises with centralized management and administration.
Next-generation firewall (NGFW)	Firewall solutions that provide a secure gateway between public internet and private enterprise networks including SD-WAN.
Secure web gateway (SWG)	Web application firewall and application/API protection that extend firewall capabilities to protect from web-based threats and to enforce corporate web content policies.
Cloud access security broker (CASB)	Enforces security policies between user and device endpoints and cloud-based applications.
Zero-trust network access (ZTNA)	Also referred to as software-defined perimeter (SDP), it limits access to internal business applications, prohibiting access to any resources that are not explicitly authorized.

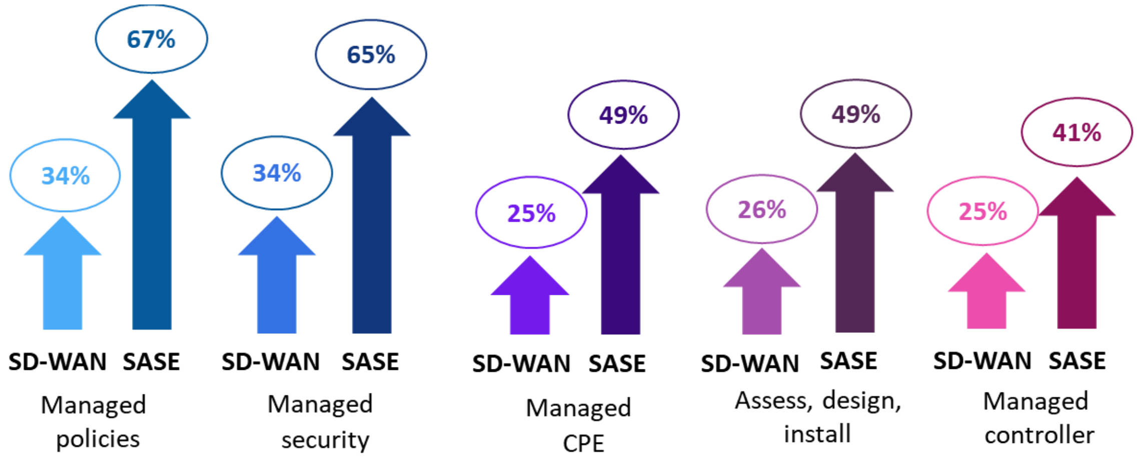
Source: Omdia

Because SASE is a collection of capabilities, each vendor's SASE solution will vary depending on the elements it supports. This inconsistency creates confusion in the market for enterprises. A professional security services company CEO, for example, noted, "Our [large organization] clients are talking about new technologies such as SDN/SD-WAN and SASE, but I do not think they really know what those things mean." Enterprises will find the details of SASE change depending on the vendor making the pitch.

In the early days of SD-WAN, many enterprises opted to handle the implementation themselves, relying on in-house expertise to manage the design, installation, and configuration of the solution. These enterprises quickly found that an SD-WAN implementation was more complex than they had initially believed, and many ultimately turned to a partner for assistance. Taking the next step to integrate more security tools into the network will further increase the complexity of the implementation. Enterprises can turn to managed services partners for help navigating the confusing SASE marketplace and the complexities of SD-WAN and SASE implementations. These partners can help the enterprise identify their security requirements and desired business outcomes, develop a plan to help meet those requirements, and assemble various parties to complete the implementation. Companies in highly regulated industries such as financial services and healthcare will need a partner that can work with their compliance teams to ensure that security practices follow industry requirements.

Enterprise SASE adopters do not just turn to managed services partners more often; they also have deeper partner relationships. SASE adopters more frequently add managed security, policy management, and customer premises equipment (CPE) management than enterprises deploying SD-WAN do (**Figure 6**).

Figure 6: SASE adopters turn to managed services partners to navigate a complex migration



Notes: n=245; regions: Americas, Asia, Western Europe

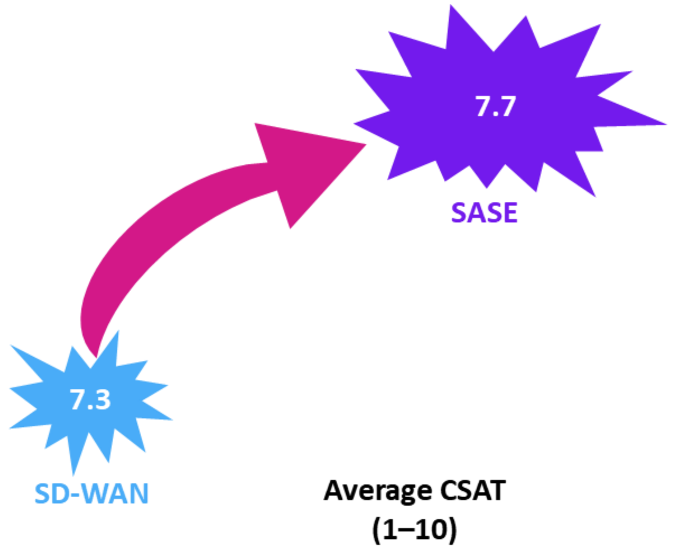
© 2022 Omdia

Source: Omdia Global Enterprise Network Services Insights, August 2021

Enterprise adopters are happy with SASE

Omdia's enterprise surveys consistently find that SD-WAN adopters are happy with their deployment and operating experiences. This holds true in spades for SASE. In its first year of tracking, SASE enterprise adopters already report higher satisfaction and greater net benefits than SD-WAN adopters (**Figure 7**). The enterprise SASE adopter satisfaction ratings are the highest Omdia has recorded for any network transformation service since we launched this series of surveys in 2017.

Figure 7: Enterprises give high marks to their SASE solutions



Notes: n=245; regions: Americas, Asia, Western Europe

© 2022 Omdia

Source: Omdia Global Enterprise Network Services Insights, August 2021

An IT director at a large financial services company described the benefits from its SASE deployment:

Ask me a year from now and I expect to tell you that [SASE] is helping with my supply chain, it is helping with my network capacity, and helping with applications usage. Going on that journey to adopt these technologies will enhance the way we operate; it will make my operating model more efficient and faster. These are the considerations we are bringing into play in our forward-thinking strategy framework. We expect that network and security functions will converge into a single integrated service that works at the cloud level. We are keeping these fundamentals of SASE in place at this point.

Enterprises that work with a partner at the assessment, design, and installation stages also report more positive results. In its enterprise surveys, Omdia consistently finds that IT departments are not permitted to adopt new solutions until security is addressed. Omdia also finds that almost all enterprises undergoing network transformation engage with service partners at some points in their transformation journey. Managed services partners bridge in-house gaps in expertise, starting with security. Omdia's surveys have found that companies that worked with partners for SASE deployments reported high levels of satisfaction, while those companies that opted for a do-it-yourself approach reported a more mediocre experience.

Conclusion

A framework for selecting the best solution to secure your enterprise network

Enterprise perceptions of secure networks are changing. The security built into SD-WAN complemented by cloud-based security is giving way to a more integrated, robust approach that secures all aspects of the enterprise environment: headquarters and branches, data centers, devices, people, and applications. Services under the SASE suite that secure web applications and remote user access are the next logical step in an enterprise's transformation strategy. But as with SD-WAN, this step to SASE is a complex migration. There are several factors that enterprises should keep in mind as they consider SASE:

- **Security solutions must be deployed and managed with the network as part of a broader security strategy.** The network security landscape has changed in the last couple of years. The network perimeter has splintered and become less defined, security attacks have increased, and regulatory compliance requirements governing privacy have grown. Enterprise chief security officers (CSOs) today are tasked with protecting a diverse pool of endpoints in an environment where devices, users, and applications cannot be trusted based on their location or adjacent trusts. Enterprises are protecting the company through a security posture that brings together traditional security tools such as firewalls with newer solutions that secure network access and applications.

- **Integrating network and security requires collaboration across teams.** Historically, network and security have been handled by different teams with different priorities and views. When enterprises relied on private network services connected to secure buildings, this worked. Now that networks are more often internet-based, with employees accessing the company's network and business applications from various locations and devices, integrating network and security is critical. Enterprise IT leaders must find a way to unify these teams to foster information and data sharing to protect the network and the company.

- **Evaluate SASE components and select the most appropriate for your business needs.** The expanded network perimeter and the rise of privacy breaches make enterprises that are subject to stringent regulatory compliance directives vulnerable. For example, businesses in markets such as healthcare, retail, and financial services often rely on remote workers to staff contact centers. These employees access confidential data online and communicate with customers via web chat, text, and telephone. The enterprise needs to identify and implement tools to ensure communications comply with industry regulations.

- **Successful network transformation is a consultative process.** Many enterprises that set out on a DIY SD-WAN journey ultimately find that working with partners leads to greater success. As enterprises take on the complex process of expanding security capabilities, the value of working with a knowledgeable, experienced partner grows. Enterprises understand that a severe compromise can threaten to shut them down and must take the steps necessary to protect their business. Collaboration with a managed services provider gives enterprises the resources to integrate network and security, helping the company achieve its desired business outcomes.

Appendix

Methodology

Materials cited in this white paper are drawn from global quantitative enterprise research surveys conducted by Omdia and from qualitative discussions with enterprise IT leaders.

Author

Cindy Whelan
Practice Leader, Service Provider Enterprise Networks & Wholesale
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decisionmakers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.