2023 SASE TRENDS REPORT:

Beating Expectations on Security While Easing IT Ops

SPONSORED CONTENT

CIO

COMCAST BUSINESS

Powering Possibilities™

New research from *CIO* and Comcast Business reveals that network security and remote connectivity have replaced cloud security and innovation as the top challenges driving interest in adoption of secure-access-service-edge (SASE) solutions. Based on a survey of 257 IT decision-makers, the research also finds that SASE is exceeding expectations in critical areas, including IT operations, user experience, and remote work connectivity.

The operational benefits of SASE are especially noteworthy, as they may help alleviate persistent cybersecurity staffing challenges experienced by 80% of the survey respondents. Those decision-makers also indicated that they are dealing with the need to adopt more robust cybersecurity measures to secure data, networks, and cloud environments because of hybrid and remote work. The survey finds a strong preference for working with a managed services provider (MSP) for SASE deployment and ongoing management.

As in a similar survey conducted a year earlier by *CIO*, Comcast Business, and Fortinet, SD-WAN is deemed to be the most important capability organizations expect in their SASE solutions. This year, though, zero-trust network access (ZTNA) almost doubled in importance from the previous year, drawing nearly even with cloud access security brokers (CASBs) as the next-most-important capability.

45%

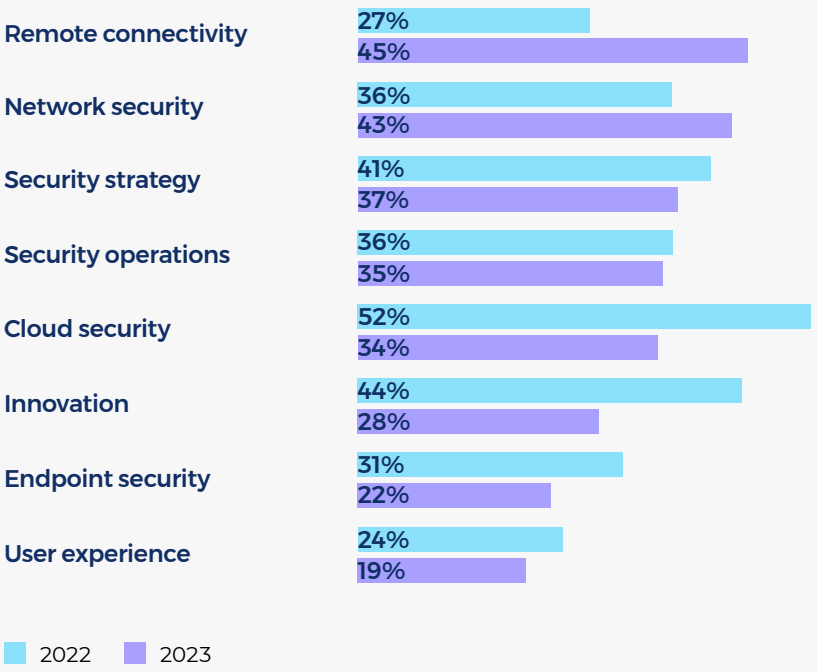
say remote connectivity is top driver of SASE adoption

SASE Delivers on Key IT Priorities

SASE is a category originally defined by Gartner as a framework that delivers converged network and security-as-a-service capabilities, including SD-WAN, CASB, and ZTNA as well as secure web gateways (SWGs) and next-generation firewalls (SGFWs). The *CIO*/Comcast survey finds that network and security convergence is top of mind as extremely or very important for 94% of those surveyed in 2023. Convergence is a priority because it supports key business needs — effective end user security, remote work, and cloud security — and SASE offers a path to this convergence.

The factors driving that convergence appear to be shifting, however. The top challenge by far (cited by 59% of the respondents) that decision-makers were seeking to address with SASE in 2022 was cloud security, reflecting the ongoing and often challenging migration from traditional data-center-based applications and workloads. In 2023 that dropped to 34%, overtaken by remote connectivity (45%) and network security (43%).

Figure 1: Challenges Driving SASE Investment



What appears to be predominantly driving that shift is the realization that remote work is here to stay and that related security concerns persist. With remote workers needing access to key IT assets and the ability to collaborate with teams virtually, IT is grappling with growing cybersecurity complexity and threats. In fact, 76% of those surveyed said hybrid work has caused them to adopt more robust cybersecurity measures to secure data, networks, and cloud environments. But they are doing so in the face of persistent staffing and hiring challenges, according to 80% of the 2023 survey participants.

SASE Benefits Beating Expectations

Security, always a top-of-mind issue, continues to resonate as a justification for SASE investment, with 73% saying the top measure of success for SASE will be improvement in the areas of security and compliance. Almost as many, 71%, will also measure success based on improved network and application performance.

Among those who have not yet implemented SASE, the most anticipated business benefits are improved security and compliance (47%) and improved security performance (46%). They also anticipate that SASE will improve overall IT operations (44%).

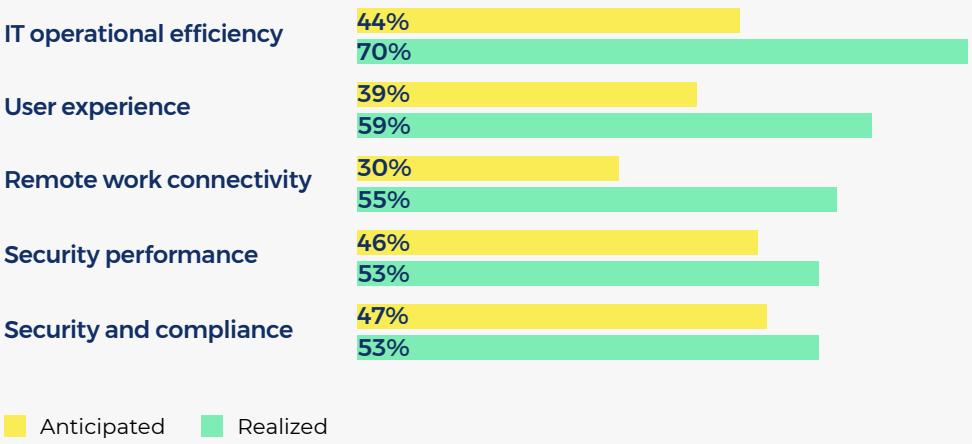
Actual results for organizations that have already implemented SASE show that 53% have realized those security benefits. However, IT operational improvements have been gained by an eye-popping 70%, illustrating that improving security creates even greater benefits than anticipated in overall

IT operations, with greater efficiency and productivity. That's likely due to enhanced abilities to deploy equipment, software, and policies more easily with centralized network and security management for onsite or remote workers.

"SASE provides a framework in which network and security teams are forced to work more closely to accomplish the goal of high application performance that doesn't compromise the security and integrity of the connectivity they are providing," says Trevor Parks, senior director, security solutions, at Masergy.

With SASE, says Parks, "organizations are realizing they can avoid business-stopping threats more reliably than ever before. When these technologies are combined and they're working together, it's much more cost-effective from the perspective of operating expenses and technology investment."

Figure 2: Anticipated vs. Realized SASE Benefits



Other key benefits identified by SASE implementers include improved user experience through more reliable network and cloud app performance as well as improved performance and uptime for remote workers.

IT decision-makers want to be sure that their SASE solutions have flexibility to deploy security technology in the cloud or on-premises, incorporate a 24/7 security operations center, and integrate well with existing security technologies, all factors that were deemed more critical in 2023 than in the 2022 survey. But they are also keen on extended detection and response, endpoint security protections, and advanced analytics, among other features and services.

SASE Implementation: Challenges and Strategies

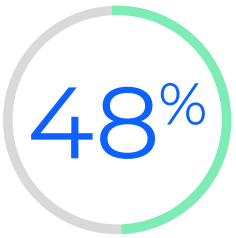
Although SASE adoption offers clear benefits, organizations reveal some key hurdles to fully realizing the required convergence of systems and teams. Less than half of the respondents indicated that they've completed their journey in key areas such as building cross-functional teams, implementing security controls, and incorporating cybersecurity in network design — and, perhaps most critically, only 31% have fully implemented common operating procedures — indicating that much work remains.

The survey findings also show that having the right people to take on the challenge of implementing and managing SASE may be what success hinges on. What most impedes SASE adoption is the issue of providing the IT expertise, best practices, and necessary training, according to 48% of the 2023 survey respondents.

"Many organizations are not very security-mature, those skills are not easily obtained, and it takes years to really get good at it," says Parks. "Some companies have bought multiple network and security solutions, and they may not have the skills needed to successfully manage them all."

Other top challenges organizations are dealing with include converging the internal network and security operations and teams (41%) and supporting network security operations, which notably includes staffing.

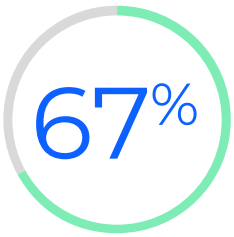
The 2023 survey illustrates that companies are increasingly inclined to partner with MSPs for deployment of their SASE solutions, bridging the internal lack of skills via increased reliance on dedicated and skilled teams those MSPs have built up in recent years. The number of those electing to use internal resources in combination with MSPs for SASE implementation increased to 67%, up from 48% a year earlier, as the number of those relying only on internal resources declined to 22% — a 14% drop from the previous year.



say lack of expertise, best practices and training are biggest challenges to SASE adoption

Parks says the growing impetus to utilize MSPs for SASE solutions for most companies comes down to resource management and practicality. “Many companies may not have dedicated security teams and rely on IT staff that aren’t well skilled in security,” he asserts. “A smart way to achieve the level of security they want without actually going out and hiring a whole security team is through managed security services.”

Cautioning that “not all SASE solutions are created equal,” Parks urges organizations to avoid “one-size-fits-all solutions” and instead seek out tools and service providers able to maximize value by customizing implementations to fit individual customers’ business challenges.



are implementing SASE with a combination of internal resources and MSPs

Many Priorities to Address

Differences between the 2022 and 2023 surveys demonstrate the evolution of security priorities, as organizations’ business needs shift and IT teams adjust. IT decision-makers must juggle multiple cybersecurity priorities, and the SASE framework reflects industry efforts to resolve many of those issues.

The growth in remote and hybrid work has accelerated the adoption of SASE tools and services as decision-makers strive to meet their organizations’ needs in that regard with greater security effectiveness, converge security and network staffs and their technology stacks, and overcome ever-present staff shortages that impinge on their ability to recognize and respond to threats.

Engaging with established network and security providers with MSP offerings may represent the best opportunity for many organizations to find the best-possible partners able to help them effectively address an imposing combination of challenges.

Learn about global secure networking from Comcast Business, including solutions that meet the key tenets of the SASE model.