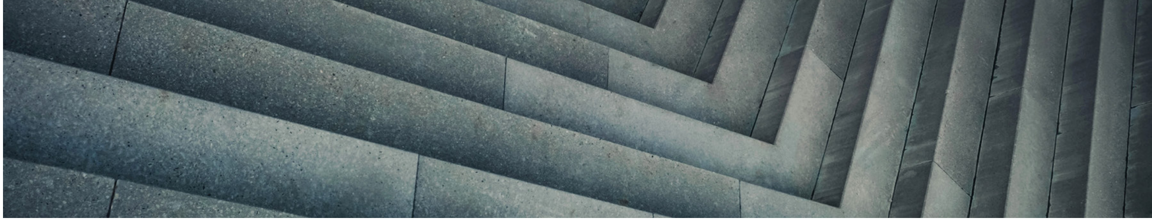
S&P Global
Market Intelligence
Business Impact Brief



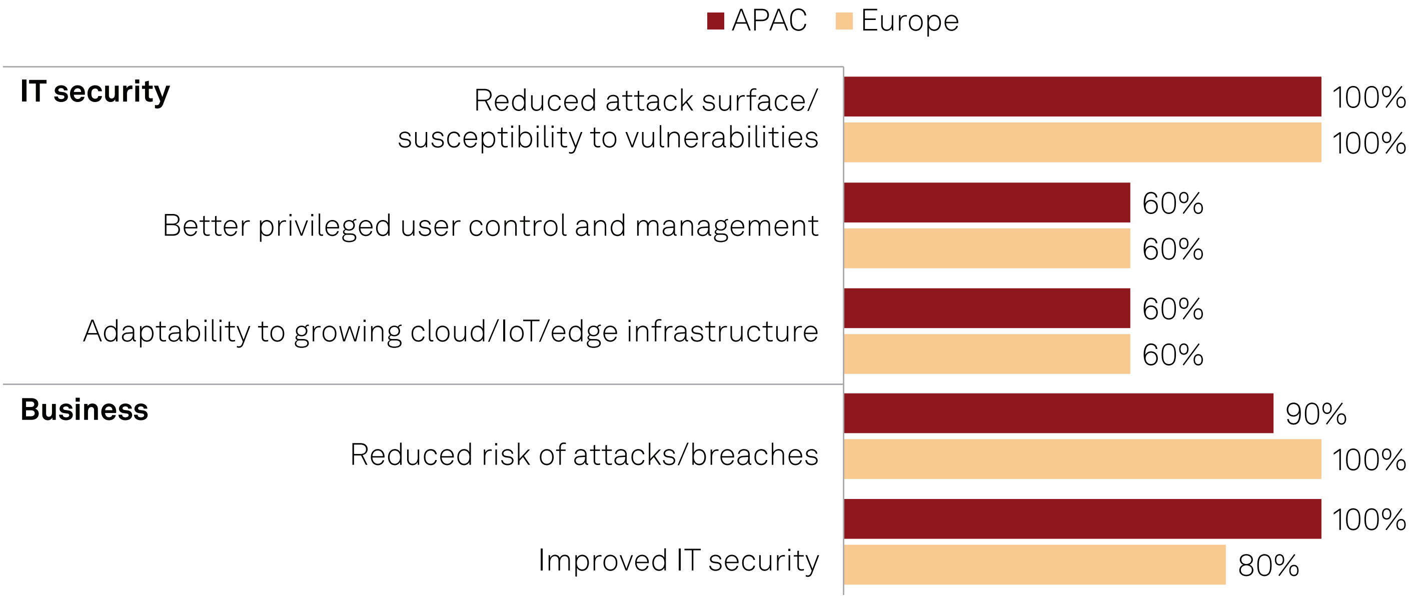
Secure Access Service Edge Provides Key Business and IT Benefits

The Take

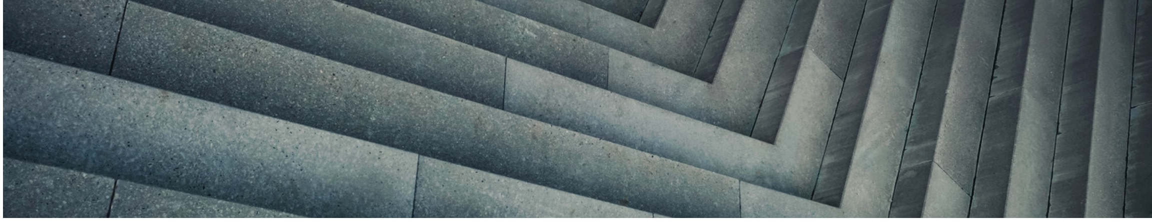
Digital transformation, shifting work patterns, continued growth in the use of cloud-based services and the emergence of technologies such as edge computing and artificial intelligence are straining legacy perimeter-based security models. Secure access service edge (SASE) based on zero-trust principles provides a set of converged remote access and identity controls delivered as a suite of cloud-native services, including secure web gateway, firewall as a service, cloud access security broker and software-defined WAN. SASE emerged in 2019, and already, more than 20 vendors offer SASE platforms, and adoption rates grow every year.

S&P Global Market Intelligence conducted a custom SASE research project in late 2022 and early 2023 focused on determining key SASE decision-making criteria, areas of benefit, deployment models and roadblocks/lessons learned for respondents in Europe and Asia-Pacific. This report focuses on the top five SASE areas of benefit expressed by the 20-person virtual executive discussion board (APAC=10; Europe=10). Note that user benefits, while important, did not appear in the top rankings for either region, which prioritised IT security and business benefits over user benefits. This could be due to bias from the perspective of study participants, which were primarily IT and security practitioners whose focus is more on technical and business concerns.

Top areas of SASE benefit



Q. Top areas of SASE benefit.
Base: All virtual executive discussion board respondents (n=20; APAC=10, Europe=10).
Source: S&P Global Market Intelligence custom SASE study, March 2023.



Business impact

The study shows that organisations involved in SASE deployments have already benefitted or expect to benefit substantially from the technology. Unsurprisingly, the benefits from each of the cited areas tend to overlap. For example, reducing the attack surface and susceptibility to vulnerabilities (No. 1, listed as an IT security benefit) also reduces the risk of attacks and breaches, which is the top business benefit, No. 2 in the overall ranking.

IT security: reduced attack surface and lower susceptibility to vulnerabilities. SASE provides advantages by reducing attack surfaces and lowering an organisation's susceptibility to vulnerabilities. This includes benefits derived from highly scalable, zero-trust-based, cloud-native security controls that limit access at the user and device/entity level rather than traditional perimeter-based controls. SASE's identity-based controls limit access to authorised entities, helping to prevent lateral network movement by attackers. SASE helps ensure secure communications with identity-based controls combined with micro-segmentation and enforced trust levels.

IT security: better privileged user control and management. Privileged access management is a key concern of many organisations today. Privileged users have access to the "keys to the kingdom," so it is not surprising that their identities are highly targeted by attackers whose goal is to use their credentials to gain access to the organisation and then use their elevated trust levels to expand the attack. A key SASE benefit is streamlined and centralised role-based access control (RBAC). RBAC combined with zero-trust network access ensures that privileged users have access only to specific resources required by their roles, limiting potential damage from breaches utilising privileged credentials. SASE also supports "just in time" access, providing temporary, time-limited access to critical resources.

IT security: adaptability to growing cloud/IoT/edge infrastructure. SASE's architecture, which is designed to enforce security policies at the service edge, is well suited to cloud, IoT and edge use cases. It also ensures secure cloud-to-edge connectivity through secure tunnels between cloud, IoT and edge devices, data centres and offices while improving remote device connectivity through reductions in network latency. SASE incorporates IoT security capabilities such as device authentication, encryption and policy-based access controls, enabling secure IoT devices and data.

Business: reduced risk of attacks/breaches. From a business perspective, attacks and breaches are risky and expensive to remediate. Naturally, business leaders are interested in reducing and avoiding risk — a board-level concern in most organisations today. Most study participants indicated that it was not necessary to build a substantial SASE business case prior to deployment because decision-makers had a clear understanding of its value in helping ensure successful digital transformation projects.

Business: improved IT security. SASE's cloud-native architecture enables higher levels of scalability and resilience compared with traditional on-premises approaches. Security updates and threat intelligence can be applied and updated more quickly than with traditional tools, improving the platform's overall security and analytics currency. SASE's centralised architecture is simpler to manage and more streamlined than legacy approaches, so it requires fewer devices and personnel, reducing the attack surface while simplifying management.

Looking ahead

SASE is clearly here to stay. Cloud-native security management coupled with support for zero-trust network architectures and centralised policy management across security and networking domains reduces overall risk, simplifies network management and pushes policy enforcement to the edge while supporting greater scalability and resilience. SASE is a significant step in the right direction given today's increasingly complex IT estates that rely on cloud, edge and IoT.

We commissioned this research to help companies cut through all the noise and get a true picture of both the good and the bad. Understanding both the obstacles businesses are facing and the benefits that can be achieved through SASE enables us to evolve the services that we offer. Our highly experienced network security consultants can support you throughout the journey, including to help determine your strategic approach and target operating model, as well as providing ongoing proactive management. We can help you de-risk adoption and realise greater benefits, faster.

EMEA whitepaper APAC whitepaper