Gartner anticipates that 40% of companies will have a SASE strategy by 2024, but there’s a long journey between strategy and reality. Companies should begin preparing now for an architectural and cultural change as broad as SASE.

Indeed, many of them have little choice because the pandemic has forced their hand; they already have to embrace some elements of SASE, such as zero-trust network access in response to the need for remote working. Here are some to-do items for your adoption roadmap.

1. Make the business case
   Begin by making the case for SASE among key decision-makers. This involves both a long-term strategic case along with smaller, more immediate proposals as part of an incremental deployment.

2. Build synergy between security and network teams
   Security and network teams often live in silos, but when designing and deploying the SASE model, they can’t talk often enough. Begin to build synergy between these groups as early as possible to smooth integration work further along the road.

3. Assess the operational and organizational impact on networks and security
   When drawing up a long-term architectural proposal for SASE, design teams must consider the operational impact on their systems.

4. Begin the SD-WAN transformation
   SASE needs a software-defined networking platform for the deployment of edge cloud-based services. This involves moving to an SD-WAN architecture, including the transition from MPLS to internet connections. It is crucial to tackle this stage with software-defined network security services in mind, including a remote access solution in the SD-WAN fabric at an early stage to guarantee consistent security for remote workers.

5. Migrate legacy data center cybersecurity services to the cloud
   With an SD-WAN solution in place, it’s time to plan the move from legacy on-premises security services to cloud-enabled POPs running on the software-defined network. This means transitioning to a cloud security provider.

6. Move security posture and design to zero-trust network access
   Clients should make the migration to cloud-based security services with zero-trust network access in mind. This includes planning for identity-based access to all applications. Build out components including identity and access management and identity life cycle management frameworks that will support the move to identity-based access. Now is also a good point to consider complementary technologies like multi-factor authentication and device-based network access control to protect managed mobile devices accessing corporate applications.

7. Develop an automation framework
   With a software-defined network security fabric in place, clients will be well-positioned to drive new efficiencies into their security infrastructure using automation. Invest in creating and refining a software-defined network and security control plane that will form the basis of a robust and adaptive security operation.

Challenge your peers with info from the white paper!
www.orangecyberdefense.com/global/SASE/