In a perfect world, transitioning to a SASE architecture would be as easy as pushing a button and moving your entire network architecture into a secure and cloud-environment. Unfortunately, that is not the world we live in, but the transition doesn't have to be complicated either. The magic of a smooth transition is a SASE architecture that starts by finding the right provider for you to help you on your journey. Your SASE provider should begin by helping you leverage your existing investments, lead with experience, and help you transition to cloud-delivered security seamlessly, securely, and at a pace that is best for your business.

**QUICKSTART POLICY MANAGEMENT**

Manage security anywhere and everywhere, on- premises and in the cloud, from the cloud all within a single UI.

Unified Policy Management maximizes user experience with policies that follow users, devices, and applications whenever they go.

**RESILIENCE AND SCALABILITY**

Scale for physical, virtual, and cloud-based security environments easily and effectively.

You need operational simplicity and security at scale that is invisible to the end user and never negatively impacts the user experience.

**CONSISTENT SECURITY FOR YOUR DISTRIBUTED WORKFORCE**

Give your remote workforce secure access to the applications and resources they need to do their job effectively.

Consistent security policies must follow users, devices, and applications without having to duplicate or recreate rules sets.

**SINGLE SOURCE OF IDENTITY**

Seamlessly integrates with any identity solution provider on the market.

Your SASE provider must empower you to choose the identity provider who will best serve your business needs, not the one that best fits theirs.

**UNIFIED POLICY MANAGEMENT**

Do the research and find a SASE provider with proven security effectiveness.

Your SASE provider must show effective threat protection including client-side and server-side exploits, reconnaissance, botnets, and DNS tunneling. They must have the tools to dynamically analyze, flag, and stop attacks in your environment on- premises and in the cloud and must be delivered as a service.

**BONUS POINTS: SECURITY ASSURANCE**

Make policy rule changes confidently and ensure policy changes are effective.

Whether it’s a rule for a traditional firewall policy or policy delivered as a service, your SASE provider must help you implement SASE by meeting you where you are and is with you every step of the way on your journey.

Every SASE Journey starts with you and your organization, but ultimately it’s in your choice how you go about the design, build, and implement this new architecture for your business that defines how your business will live and work in the future. Whichever path you choose, it is critical to have a service provider that can help you get there. Don’t settle for anything less, and start every step of the way on your journey.

- **FINISH strong:** Prepare and protect effectively.
- **FAST AND EFFECTIVE PROTECTION AGAINST ADVANCED THREATS**

Proactively protect against unknown and invisible threats, even if they are encrypted.

Find a cloud-delivered service that performs static and dynamic detection that identifies and eliminates new and emerging threats at all moments of detection.

**SINGLE STACK ARCHITECTURE WITH A SINGLE POLICY FRAMEWORK**

Leverage existing investments, as an on-ramp to business-critical cloud security services.

Create policies once and apply them anywhere and everywhere with unified policy management, including user- and application-based access, IPS, anti-malware, and secure web access within a single policy.

**SUPPORT FLEXIBLE ENVIRONMENTS**

It shouldn’t matter to your SASE provider whether your infrastructure is on-premises, in the cloud, or a combination. They should support it all.

Your SASE provider must help enable your transition to a SASE architecture seamlessly and securely, and at a pace that is best for your business.

**RESILIENCE AND SCALABILITY**

Transition seamlessly to a cloud-delivered security architecture at your own pace within the same management UI with united policy and intuitive deployment wizards. Easily and effectively orchestrate, provision, and manage policy services whenever those services are located.

**DYNAMIC USER SEGMENTATION**

Ensure your users are protected wherever they are. Incorporate follow-the-user policies and provide automated access control based on risk through granular policy, locking down 3rd party access as an attack vector, addressee 3rd party access, further reducing the attack surface at the edge.

**TRANSITION RAPIDLY TO A CLOUD-DELIVERED SECURITY ARCHITECTURE**

No one should be forcing you to move to a SASE architecture before you are ready.

Transition seamlessly to a cloud-delivered security architecture at your own pace within the same management UI with united policy and intuitive deployment wizards. Easily and effectively orchestrate, provision, and manage policy services whenever those services are located.