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 cloud environment. Unfortunately, that is not the world we live in, but the transition doesn’t have to be complicated once you have the right partner.

The magic of a smooth transition is a SASE architecture 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, security, and at a pace that is best for your business.

**1. UNIFIED POLICY MANAGEMENT**
Manage security anywhere and everywhere, on-premises and in the cloud, from the cloud within a single UI.
Unified Policy Management maximizes your user experience with policies that follow users, devices, and applications wherever they go.

**2. FLEXIBLE AND EFFECTIVE PROTECTION WITHOUT COMPLICATED RULE SETS**
Protect against unknown and unknown threats, even if they are encrypted.
A cloud-based service that performs static and dynamic detection makes it so that the signatures and analysis are updated in real-time. No one should be forcing you to move to a SASE architecture before you are ready.

**3. RESILIENT AND SCALABLE**
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 so never negatively impacts the user experience.

**4. SINGLE SOURCE OF IDENTITY**
Leverage existing investments, an on-premise to business critical cloud security services.
Your SASE provider must empower you to choose the infrastructure that best fits your business and ensure you leverage your existing investments.

**5. DYNAMIC USER SEGMENTATION**
Consistently segments users and applications without having to duplicate and shadow rules.
Consistent security policies must follow users, devices, and applications without having to duplicate or recreate rule sets.

**6. SINGLE SOURCE OF IDENTITY**
The magic of a smooth transition to a SASE architecture 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, security, and at a pace that is best for your business.

**7. SINGLE STACK ARCHITECTURE WITH A SINGLE POLICY MANAGEMENT UI**
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 on-ramp attacker, 3rd party access, further reducing the attack surface on the edge.

**8. 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, ransomware, botnets, and DNS tunneling. They must be able to orchestrate, provision, and manage policy services across your network.

**9. BONUS POINTS: SECURITY ASSURANCE**
Make policy rules change confidently and ensure policy changes are effective.
Whether it’s a rule for a traditional firewall policy or policy delivered as a service, they must be placed in proper order so they’re effective. Your SASE provider must help you define roles in secure policy sets and automatically surface rules that are ineffective.

**10. TRANSITION SMOOTHLY TO A CLOUD-DELIVERED SECURITY ARCHITECTURE**
No one should be forcing you to move to a SASE architecture before you are ready.
Transition to a cloud-delivered security architecture at your own pace within the same management UI with unified policy and intuitive orchestration, provision, and manage policy services whenever those services are located.

Every SASE Journey is unique to you and your organization, but ultimately it is your choice how you go about the design, build, and deployment of this new approach to security. The essential elements are whether the service follows users, devices, and applications wherever they go.