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 private and secure cloud environment. Unfortunately, that is not the world we live in, but the transition doesn’t have to be complicated or time-consuming. The magic of a smooth transition is a SASE architecture start 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 all within a single UI.

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

**2. SECURE AND SCALABLE**
Scale for physical and virtual 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.

**3. 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 rule sets.

**4. SINGLE SOURCE OF IDENTITY**
Solely 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.

**5. 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 help you optimally orchestrate, provision, and manage policy services head-on 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, they must be placed in proper order so they’re effective. Your SASE provider must help you fit them so users of these rule sets and automatically surface duplicate and shadowed rules before they’re committed.

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 wizards. Easily and effectively orchestrate, provision, and manage policy services whenever those services are located.

Juniper Networks software-defined security architecture is head-on and stops attacks in your environment on-premises and in the cloud and must be delivered as-a-service.

Do the research and find a SASE provider who is located in your region.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: +415.599.6100
Fax: +415.599.6170
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.791

Copyright 2022 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or recreate rule sets.

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.

**6. SINGLE SOURCE OF IDENTITY**
Solely 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.

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 fit them so users of these rule sets and automatically surface duplicate and shadowed rules before they’re committed.

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, they must be placed in proper order so they’re effective. Your SASE provider must help you fit them so users of these rule sets and automatically surface duplicate and shadowed rules before they’re committed.

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 wizards. Easily and effectively orchestrate, provision, and manage policy services whenever those services are located.

Every SASE journey will be unique to you and your organization, but ultimately it’s in your choice how you go about the design, build, and modern transformation. The new SASE architecture is head-on and stops attacks in your environment on-premises and in the cloud and must be delivered as-a-service.

**8. DYNAMIC USER SEGMENTATION**
Incorporate follow-the-user policies and provides automated access control based on risk through granular policy, blocking down illegitimate access as an attack vector. Addresses 3rd party access, further reducing the attack surface at the edge.

**9. TARGETED SECURITY EFFORT**
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 help you optimally orchestrate, provision, and manage policy services head-on and stop attacks in your environment on-premises and in the cloud and must be delivered as-a-service.

**10. TRANSITION RISKLESSLY 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 wizards. Easily and effectively orchestrate, provision, and manage policy services whenever those services are located.

DISTRIBUTED WORKFORCE
Incorporate follow-the-user policies and provides automated access control based on risk through granular policy, blocking down illegitimate access as an attack vector. Addresses 3rd party access, further reducing the attack surface at the edge.

**3. 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 rule sets.

**5. 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 help you optimally orchestrate, provision, and manage policy services head-on and stop attacks in your environment on-premises and in the cloud and must be delivered as-a-service.

**7. TARGETED SECURITY EFFORT**
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 help you optimally orchestrate, provision, and manage policy services head-on and stop attacks in your environment on-premises and in the cloud and must be delivered as-a-service.

**9. TARGETED SECURITY EFFORT**
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 help you optimally orchestrate, provision, and manage policy services head-on and stop attacks in your environment on-premises and in the cloud and must be delivered as-a-service.

**10. TRANSITION RISKLESSLY 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 wizards. Easily and effectively orchestrate, provision, and manage policy services whenever those services are located.

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, they must be placed in proper order so they’re effective. Your SASE provider must help you fit them so users of these rule sets and automatically surface duplicate and shadowed rules before they’re committed.

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 wizards. Easily and effectively orchestrate, provision, and manage policy services whenever those services are located.