# Your journey to SASE

## Delivering security everywhere on the Secure Access Service Edge path

orange™ Business Services

paloalto® NETWORKS

# Executive summary

**Enterprise IT requirements are broad and ambitious. Most are looking for greater flexibility, an enhanced user experience, organizational optimization, and the ability to manage an increasingly distributed workforce. You have probably heard that Secure Access Service Edge (SASE) promises to deliver all this. What you probably don't realize is that you are actually on the SASE journey already.**

Most enterprises are in the early phase of the SASE transformation. As we advance, all enterprises that have adopted SD-WAN to deliver cloud-based services will need to take SASE onboard. However, it is essential to note that SASE is about buying into a methodology, not a platform. It is about taking small steps to the big vision and starting with the biggest challenge, such as remote access and adding the stepping stones to SASE.

In this paper, Orange Business Services teams up with Palo Alto Networks to reflect on what SASE brings to enterprises and how they can accelerate their SASE journey through this partnership. We also examine how enterprises can implement a proactive SASE strategy that targets individual business outcomes, identifying dependencies and priorities to aid in driving success.

Read on to learn how to take advantage of SASE for your organization.

**60%** **By 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access, up from 10% in 2020.[1]**

## Contents

# Why SASE

**Cloud-first is fast becoming the norm for enterprises, and processing is moving away from the data center to the edge of the network for some workloads but not necessarily for all, requiring integration of cloud-first with workloads that don't necessarily lend themselves to cloud migration. Users need immediate, uninterrupted access to data and applications wherever they are working. The big challenge in this increasingly dynamic and expanding environment is keeping it all secure.**

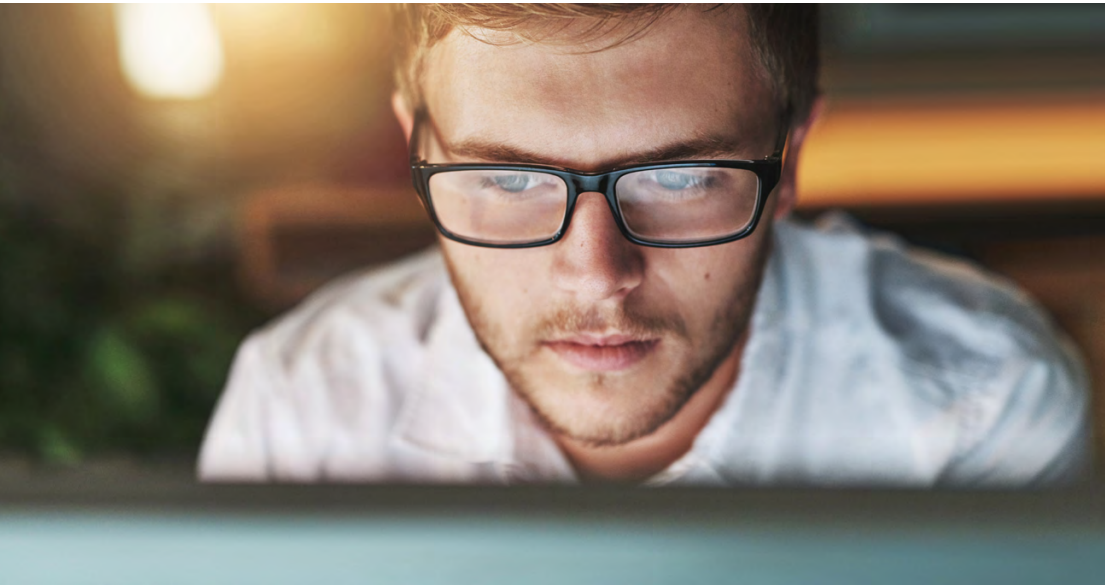
Can SASE provide the answer? An emerging cloud-oriented cybersecurity & network strategy converges network and security services to protect users, applications, and data. A SASE architecture identifies users and devices, applies consistent policy-based security, and delivers secure access to the appropriate application or data.

Fundamentally, SASE combines Software-defined Wide Area Network (SD-WAN) capabilities with a set of prescriptive security strategies oriented around securing assets, significantly as cloud and "as-a-service" technology accelerates. This security approach delivers network and security services at the underlay and overlay level as a single service, reducing complexity. It converges best-of-breed security and SD-WAN capabilities to provide an exceptional user experience while reducing security risks.

# Navigating the journey to SASE

**As enterprises migrate to the cloud, they quickly realize that network infrastructure and security can no longer operate in silos. Many organizations have started on their SASE journey but are sometimes unaware of exactly where they are in the process. This begins by addressing their challenges of digital transformation, edge computing, and a mobile workforce.**

SASE isn't a single product that can be purchased. At its highest level, deploying a SASE architecture is built around the concept of enabling secure connectivity and access to resources from the edge. To work efficiently, all the components in the SASE model of connectivity, networking, and security need to seamlessly integrate as part of a centrally managed system.

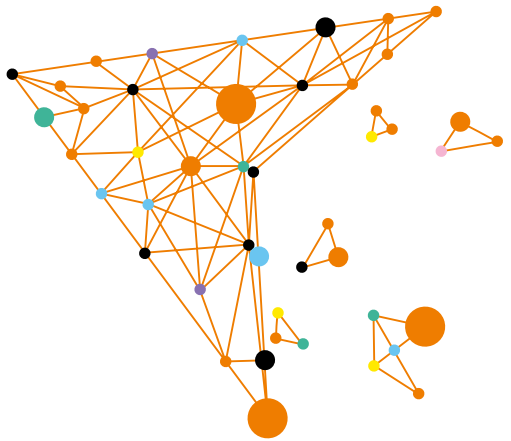


## There is no cookie-cutter answer to SASE

The road to SASE is far from straightforward. Every enterprise has its starting point, which requires thought, flexibility, and customization.

The SASE journey provides enhanced flexibility and data protection, reduced complexity, and increased performance – providing gains in productivity and profitability. Instead of buying and managing multiple point products, a single platform will significantly increase IT resources efficiencies and offer the enterprise greater agility by bringing network and security into a single pane of glass.

**By 2023, to deliver flexible, cost-effective, scalable bandwidth, 30% of enterprise locations will have only internet WAN connectivity, compared with approximately 15% in 2020.[2]**



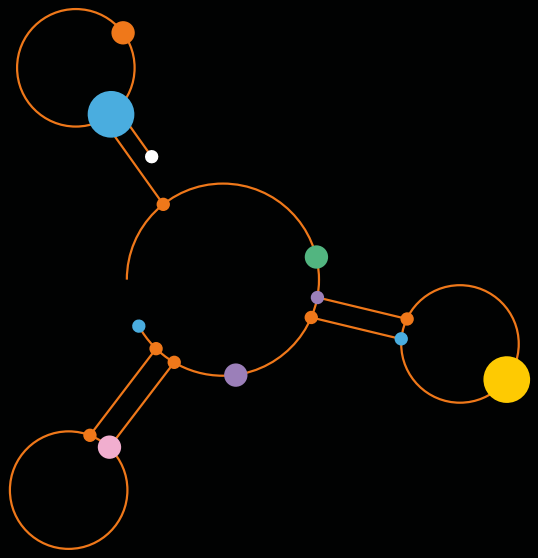
# Enabling Zero Trust

Zero Trust Network Access (ZTNA) is an essential component in the SASE architecture, critical in delivering end-to-end security. ZTNA is designed to enforce a Zero Trust policy built around the concept of “never trust, always verify”. In essence, the trust level is set at “zero”. Full content inspection integrated into SASE offers better security and visibility into the network.

The necessity to support agile digital business transformation undertakings with a zero-trust security posture while managing complexity is crucial for SASE adoption.[3]

Together SASE and ZTNA can significantly improve your overall security posture by:

- Bringing secure scalability to a multi-tenant cloud-native platform
- Greater granularity in terms of network visibility and policy control
- Security without performance degradation
- Providing secure anytime anyplace working without impacting productivity



**60%** **By 2023, together with SASE and ZTNA, 60% of enterprises will phase out their VPNs in favor of ZTNA based solutions.[4]**

# SASE supports digital business

**With the explosion of digital business, networks are becoming increasingly distributed and virtualized. SASE can help you deliver cloud and other applications to end-users securely.**

Digital transformation and accelerated cloud adoption have changed the enterprise network. More users work remotely, and more sensitive data is held in the cloud and outside the traditional enterprise perimeter. Having this access to the enterprise from anywhere is another contributing factor driving SASE adoption.

The significant advantage of the SASE architecture is that it packages technologies delivered as a service to embed security into the network for anytime, anywhere access. This helps to make the delivery of cloud services safer and smoother. It can apply consistent security policies for all users and assets regardless of location, whether in data centers, the cloud, or as SaaS – without any degradation to performance.

**"The vast majority of enterprise SASE adoption will occur over several years, prioritizing areas of greatest opportunity in efficiency gains, eliminating complexity and redundant vendors, and risk reduction through adopting a zero-trust secure posture."** [5]

**Neil McDonald, distinguished VP analyst, Gartner.**

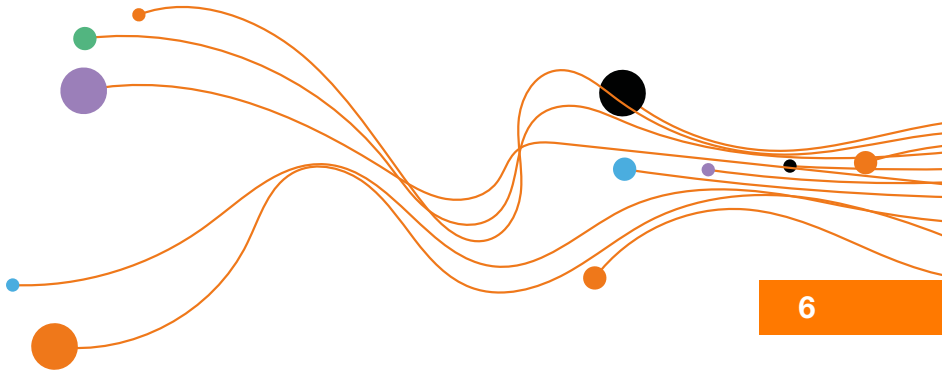
## A transformational process

A SASE infrastructure strategy cannot be achieved overnight. It is a transformational process that will replace legacy VPNs, hardware firewalls, and DDoS protection appliances over time.

SASE provides a set of capabilities that can be introduced at your own pace, allowing you to adopt services that are right for your business cases. They typically include SD-WAN, secure web gateways (SWG), Cloud Access Security Brokers (CASB), next-generation firewalls, and ZTNA. A SASE architecture can co-exist with your current networking and security portfolio until assets reach the end of life or retire.

According to Gartner, SASE adoption will be partly driven by network and network security solution refresh cycles and MPLS offload programs designed to make cloud traffic more efficient[6]. Here, direct-to-internet connections can be used to offload traffic destined for the Web if required. Some enterprises, however, have policies that restrict this.

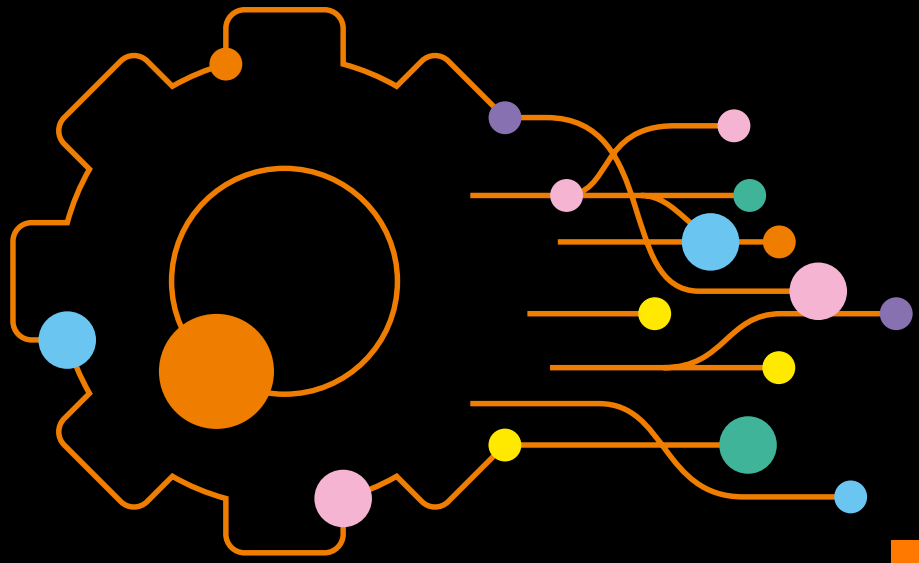
If you haven't already looked at SASE, now is the time to create an overarching strategy for replacing legacy estate with a converged SASE model. This is essential to effectively manage costs, complexity, and the demands of supporting business in a dynamic environment moving forward.



## Strategic business benefits of SASE

As remote working continues to become the norm and a cloud-first approach grows, SASE also brings the following strategic benefits to your business:

- Converges networking and security capabilities into a single cloud delivered service, managed from a single console, reducing costs and complexity
- Applies least privilege network access utilizing ZTNA, enhancing the security posture
- Consistent security policy enforcement reduces resource requirements, freeing up teams to focus on revenue-generating projects
- Utilizing identity and context-aware policies delivers a more dynamic and granular approach to security – allowing you to open your virtual doors to business partners while mitigating risk
- Cloud management enables enterprises to quickly deploy and scale services without additional devices or hardware connections
- Ensures corporate and regulatory security no matter where or when employees are logging on
- Bringing secure scalability to a multi-tenant cloud-native platform
- Greater granularity in terms of network visibility and policy control
- Security without performance degradation
- Providing secure anytime anyplace working without impacting productivity



# Strategic steps to replacing your legacy estate

**A transformation to a SASE architecture takes time. Investments in hardware and software contracts may not yet be ready for replacement.**

To further complicate the picture, many large enterprises have separate network security and network operations teams that operate in silos. Gartner suggests creating unified teams responsible for access engineering to unify networks and network policies across the entire organization in the same way platform engineering works with DevOps.

However, many enterprises have started their SASE journey (whether they know it or not) and may not have assessed where they are in their security and network roadmaps against SASE as a reference architecture. A critical first step for continuing your SASE journey is selecting a trusted partner. They can assist in technology evaluation, establishing proof of value, or what adaptations you may need to make to integrate specific SASE components. This can help you build your security and network roadmaps.

In addition, while many vendors are advertising SASE solutions, they don't all offer the necessary SASE capabilities. You should measure your requirements against best-of-breed offerings until the market matures and gaps are closed.

**By 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access, up from 10% in 2020.[8]**

Gartner[7] goes as far as setting out a three to five-year plan for SASE transformation encompassing secure access approaches for users, branches, edge locations, and distributed applications. Suggested changes include:

- **VPN:** Replace network-level VPN access with zero trust access. In addition, adopt cloud-based ZTNA to supplement legacy VPN access for higher-risk scenarios such as unmanaged device access.
- **Demilitarized Zone (DMZ):** begin phasing out DMZ-based services for named user access.
- **Start replacing physical SWG, CASB, and VPN appliances** with a move to the cloud when refresh opportunities arise.
- **Deploy Firewall as a Service (FWaaS)** which moves firewall functionality away from the traditional network perimeter to the cloud.

## Robust migration roadmap

It is important to reiterate that SASE isn't a case of switch on and go. It requires a strategic migration roadmap covering branch, edge, campus, headquarters, and remote access requirements. The migration plan should be consistently re-visited as the SASE market matures.

Using a single vendor for network security as a service and consolidating technology stacks reduces cost and complexity. No two SASE journeys are the same, however. Every enterprise will need to prepare differently and plan for different outcomes.

One thing SASE does for all enterprises is to align processes and streamline complicated networks and security operations. This allows you to redesign network policies and create a model that enables secure business in the cloud.

# The Orange approach to SASE

**The SASE model may take several years to achieve effectively. This requires a well-thought-out long-term SASE strategy and identifying short-term SASE consolidation tactics.**

Not all enterprises have the skills, resources, or time to research, build, design, and deploy a SASE model. Here at Orange Business Services, we can put your enterprise ahead of the SASE curve, allowing you to make network and network security changes with minimal disruption – while capitalizing on business benefits.

We can provide an initial SASE assessment in three parts:

1. Where are you against the SASE model?
2. Where do you want to go? What are your aspirations? What parts of SASE are clear adoption targets? How does your current security policy work within a SASE model?
3. How can we get you there? In other words, how Orange can help you establish your customized SASE roadmap.

We can plan the SASE journey according to your specific requirements, taking over the migration and managing the risk if required. This is a crucial differentiator when it comes to our SASE offering.

SASE requires a change in IT culture to adopt integrated networking and security teams. This is an area that is often overlooked. But, if teams can't move out of working in silos and share control, your SASE journey will hit some difficult hurdles. We can help ensure your SASE journey drives performance and overall organizational health.

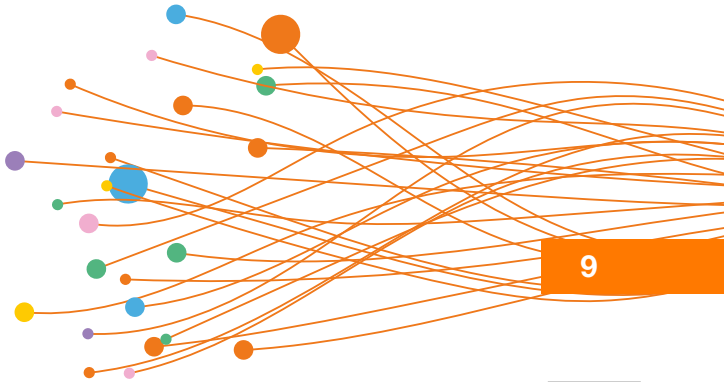
## A unique SASE offering with Palo Alto Networks

Not all SASE offerings are equal. What differentiates our approach is that it is built on Prisma® SASE, one of the industry's most complete SASE solution from Palo Alto Networks. Together with Orange Business Services managed services, it delivers consistent network access and security services to all types of applications through a common, unified framework.

Orange Business Services and Palo Alto Networks bring the interoperability, consultancy, support, migration skills, and flexible management and consumption models that enterprises are demanding to achieve their SASE goals.

This comprehensive SASE offering provides:

- Convergence without compromise: best of breed security and SD-WAN natively integrated.
- Best in class security: consistent security across all apps, regardless of location.
- Exceptional user experience with end-to-end visibility and insights across both mobile and branch users.



# Why Orange

**SASE is a broad-ranging, multi-disciplinary project with many moving parts. This is why it is vital to work with a trusted partner that understands SASE and can effectively unite security with your network infrastructure.**

At Orange Business Services, we deliver integrated SASE services while leveraging our extended ecosystem of best-of-breed technology partners. Taking advantage of integrations between ZTNA, CASB, cloud SWG, cloud VPN, FWaaS, SD-WAN, and other heterogeneous technologies will be crucial in realizing the full benefits of a SASE strategy.

With a continuing skills drought, you can also tap into our global team of IT and security professionals, skilled in network optimization, knowledgeable about new and emerging technologies, and familiar with regulatory and compliance measures.

Our cloud, security, and connectivity experts across the globe can help you on your SASE journey. They can support you end-to-end, allowing you to scope out an effective SASE strategy.

- **8,900 experts in managing your digital transformation**
- **18 Security Operations Centers (SOCs) around the globe**
- **2,500 security practitioners at a time when the employment market for cybersecurity has negative unemployment**
- **Edge-to-cloud expertise ensures security, performance, and cost optimization for your network**
- **160 counties with local sales and support**
- **Our team of experts provides operational excellence combined with solid tools to create a rich API catalog to enhance any co-management model**
- **MSI capabilities offer simplicity and streamlined management of multiple service providers**

To find out more about our SASE offer with Palo Alto Networks,
**https://www.orange-business.com/en/partners/palo-alto-networks-prisma-sase-specialized-partner**



orange™ Business Services

Sources:
1. Gartner 2021 roadmap for strategic SASE convergence.
2. Gartner 2021 roadmap for SASE convergence
3. Gartner 2021 roadmap for SASE convergence
4. Gartner Zero trust architecture and solutions 2020
5. Gartner 2021 strategic roadmap for SASE convergence
6. Gartner: e Service Access Secure the Into Converge Security and Edge WAN as Win to How: Trends Market July 2019
7. Gartner 2021 roadmap for strategic SASE convergence
8. Gartner 2021 roadmap for strategic SASE convergence

paloalto® NETWORKS