



What businesses need: A complete transformation of their **security architecture, not more** security tools

by Santiago Gao
Senior Cybersecurity Solution Architect

Introduction

As part of the Orange Cyberdefense team in APAC, I've had the honour of supporting security transformation plans for companies within Australia and New Zealand and seeing how the solutions have helped to proactively mitigate attacks and beef up their defences in this current threat landscape. More often than not, companies are also caught in the challenge between deploying the right and adequate mix of security tools to safeguard their systems and applications and recouping their ROI from the investments.

As threats continuing evolving and become increasingly sophisticated, the journey of a company's cybersecurity posture too evolves; here's my perspective on what it takes to break it down for customers in empowering them to take the leap with a trusted vendor – in adopting a future-proof solution that promises resilience, agility, and scalability of their businesses.

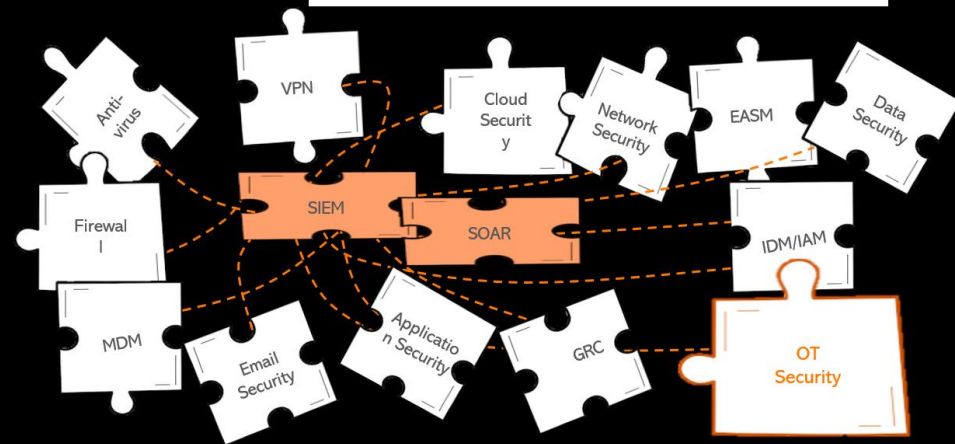


**I) How is the current solution
landscape built and challenges
that companies are facing**



Why Need Transfer?

A Complicated Legacy Cybersecurity Architecture



For Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs), they face an expanding array of security challenges, which include, but are not limited to, Cloud Security, Network Security, Data Protection, Identity and Access Management (IAM), External Attack Surface Management (EASM), Governance, Risk, and Compliance (GRC), Security Orchestration, Automation, and Response (SOAR), and User and Entity Behavior Analytics (UEBA). Additionally, there is an increasing focus on Operational Technology (OT) and Internet of Things (IoT) security, especially in industries like mining, utilities, energy, and manufacturing, where securing critical infrastructure is paramount.

For companies, the foremost gaps are (next page):

Over the years, many companies have layered various cybersecurity tools to protect their systems and data. This typically starts with an antivirus software, firewalls, and VPNs for remote access, before moving into Mobile Device Management (MDM), email security, and application protection tools as needs started growing. Once these foundational security tools are in place, businesses often implement a Security Information and Event Management (SIEM) platform. SIEM systems help aggregate logs and alerts from various sources across the IT infrastructure, including cybersecurity products, operating systems (such as Windows), servers, network devices, and cloud environments. The purpose is to create a centralized platform for monitoring and analysing security events, forming the basis of an organization's core security architecture.

However, this basic setup is no longer sufficient in the face of evolving threats. As both hacking techniques and technology continue to advance, companies must increase their cybersecurity investments. The protection of confidential business data, privacy, and the prevention of cyber breaches and incidents require more sophisticated security measures.

Overlapping Investments:

Companies often invest in redundant or unnecessary security capabilities, leading to inefficiencies and wasted resources.

Critical Gaps:

Missing essential security features can leave organizations vulnerable to emerging threats, especially as existing security products become outdated or insufficient.

Evolving Threats and Legacy Systems:

As hacking techniques evolve, many legacy security products struggle to keep up with new attack methods, creating vulnerabilities in the system.

Complicated Architecture:

Security infrastructures can become overly complex, making it difficult to manage and maintain.

Poor Integration:

Lack of seamless integration between different security solutions and systems increases operational complexity and reduces overall effectiveness.

High Costs and Efforts:

Significant resources are spent on troubleshooting, integration, and managing multiple suppliers, adding to the overall cost of security operations.

Manual Efforts:

Heavy reliance on manual processes rather than automation increases workloads, slows response times, and leaves room for human error.

Scalability Constraints:

Integrating new sites, branch offices, or cloud environments can be challenging, limiting the organization's ability to scale its security infrastructure effectively.



**II) The cybersecurity architecture
has transformed – from
perimeter to distributed security**

The IT and Security landscape has undergone a profound transformation over the past decade, driven by technological advancements and changing work dynamics. This evolution can be understood through several key phases, outlined below:



a) Traditional architecture

In this model, organizations relied heavily on a centralized data center. It featured a clear demarcation between:

- **Intranet:** The secure internal network where employees accessed resources.
- **DMZ (Demilitarized Zone):** A buffer zone for external-facing services, providing an additional layer of security.
- **Internet:** The external network, often with limited security measures.

This structure was designed for a workforce that primarily operated within the confines of the corporate network.

b) Enterprise boundary shift

As organizations began to adopt cloud services and support remote work, the enterprise boundary underwent a significant transformation. The cloud emerged as the new data center, while the internet became the primary network for accessing resources. This shift expanded the enterprise boundary, necessitating new security paradigms to protect data and applications that are no longer confined to a single location.

c) Increased attack surface

The explosion of data, devices, and locations has dramatically increased the attack surface for organizations. With employees accessing resources from various devices and locations, the potential for security breaches has escalated. This necessitates a more integrated security approach that can protect sensitive information across multiple platforms and environments.

d) Work is not a place

The shift in work culture is evident, with employees now able to work from anywhere using any device. This flexibility requires robust security measures that adapt to diverse access points, ensuring that organizations can maintain productivity while safeguarding their data.

The shift from traditional, datacentre-centric IT architectures to a modern, distributed environment—where users, devices, and data reside everywhere—has rendered legacy security models increasingly obsolete. Traditional security frameworks, often perimeter-based and reliant on centralized controls, struggle to effectively protect dynamic, cloud-first, and remote-work environments.

It's a timely call for a complete security solution transformation towards the **Secure Access Service Edge (SASE)** architecture. By integrating networking and security into a unified, cloud-delivered service, SASE brings security closer to users and data regardless of location. and provides consistent, scalable, and identity-driven protection. This transformation is essential to meet the demands of a borderless digital enterprise, ensuring secure access, improved performance, and reduced complexity in a world where work can happen anywhere, anytime.

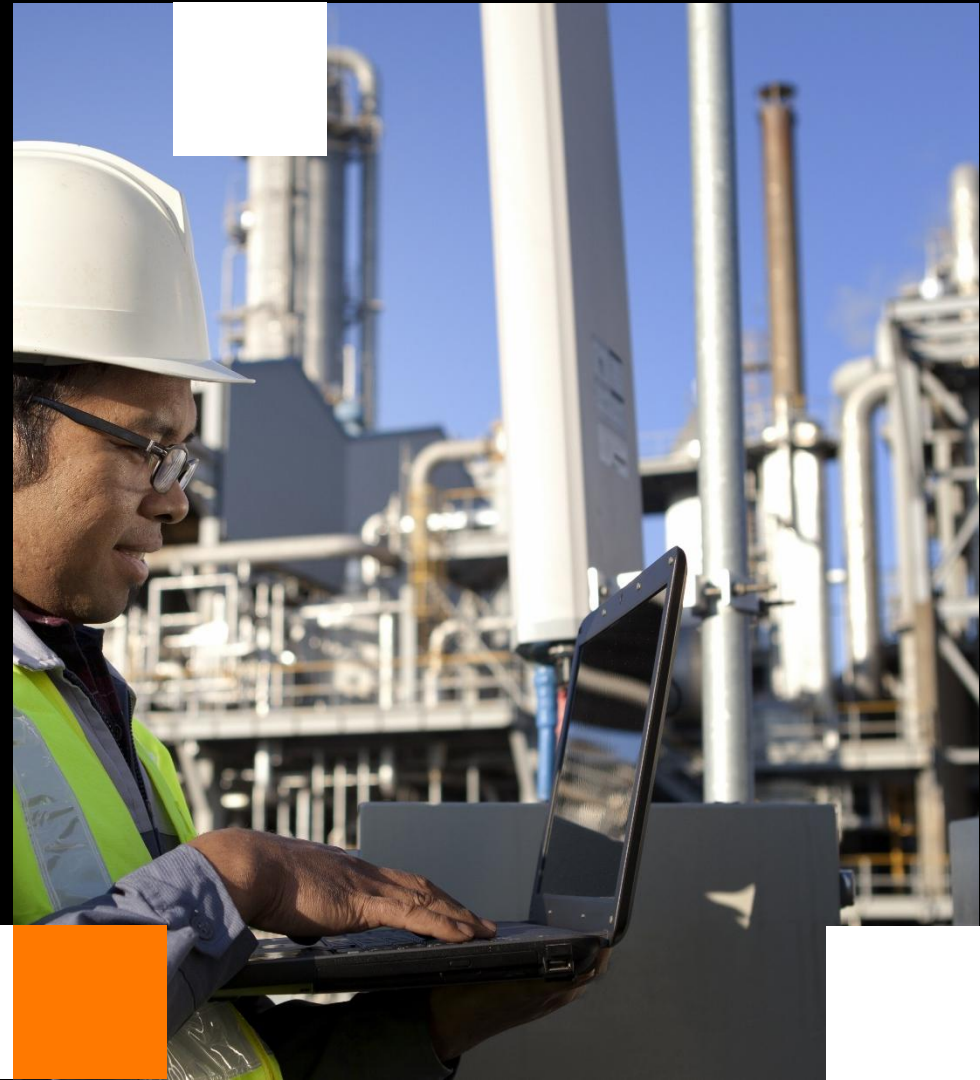


III) What is SASE, its key components and benefits



Secure Access Service Edge (SASE) is a transformative network architecture that converges wide-area networking (WAN) capabilities with comprehensive security functions into a single cloud-based service model. This approach enables organizations to provide secure, reliable access to applications and data from any location, accommodating the growing trend of remote work and the increasing reliance on cloud services.

The primary use case for SASE is to facilitate secure and efficient access to cloud applications and services for remote and mobile users. As organizations shift towards digital transformation, SASE addresses the challenges of traditional network security models, which often struggle to protect distributed workforces and cloud environments. By leveraging SASE, businesses can ensure that users have secure access to necessary resources, regardless of their physical location, while maintaining optimal performance and user experience.



Key components of SASE

SD-WAN

Optimizes network performance and connectivity across distributed locations, enhancing user experience.

Firewall-as-a-service (FWaaS)

Delivers advanced threat protection and traffic filtering in a cloud-based model, ensuring robust security.

Zero Trust Network Access (ZTNA)

Grants access based on user identity and device posture, enforcing strict security measures regardless of location.

Cloud Access Security Broker

Provides visibility and control over cloud applications, enforcing security policies and monitoring user activity.

Secure Web Gateway

Protects users from web-based threats and enforces security policies for safe Internet access.

Data Loss Prevention

Monitors and protects sensitive data from unauthorized access and potential breaches.

Identity and access management

Manages user identities and access rights, ensuring only authorized users can access specific resources.

Edge Computing and Distributed Architecture

Supports processing data closer to the source, improving response times and reducing latency.

The future of SASE: Incorporating AI/ML, 5G and Edge Computing in a cohesive narrative

The evolution of SASE is shaped by the convergence of AI/ML, 5G, and edge computing—enabling a secure, adaptive, and high-performance architecture for modern enterprises. This next-generation SASE will deliver smarter threat defence, seamless connectivity, and real-time decision-making across a globally distributed environment.

AI and ML: Intelligence at the core

- **Enhanced Threat Detection:** Detect previously unknown threats such as zero-day attacks, by identifying patterns and anomalies in real time.
- **Behavioural Analytics:** Continuous monitoring of user and device behaviour will enable baseline profiling, helping flag deviations that signal risk or compromise.
- **Automated Policy Enforcement:** Policies will become self-adaptive, adjusting dynamically based on risk context, threat signals, or network conditions—without human intervention.
- **Network Traffic Optimization:** Intelligently prioritizes and routes traffic, ensuring critical applications receive the performance they need, while conserving bandwidth for lower-priority services

5G: The connectivity backbone

- **Ultra-Low Latency and High Bandwidth:** 5G will supercharge performance for users and applications, making real-time access and processing across geographies seamless.
- **Distributed Architecture for Scalability:** SASE will operate closer to the user, allowing consistent security enforcement and data handling across multiple global regions.
- **Edge Synergy:** Coupled with edge computing, 5G enables localized decision-making—accelerating response times and minimizing backhaul to centralized infrastructure

Edge Computing: Localized intelligence and control

- **Faster, More Efficient Processing:** By shifting data processing closer to the source, edge computing reduces latency and bandwidth usage.
- **Security at the Edge:** Threat detection and enforcement can happen on-device or on-site, enabling granular control even in remote or offline environments.
- **Real-Time Analytics:** Edge-enabled insights support immediate responses to security events, improving incident containment and reducing dwell time

In a nutshell, this is the future of SASE:



The background of the slide is a blurred photograph of a modern office environment. In the foreground, a person's hands are visible holding a tablet. In the background, another person is seated at a table with a laptop. The scene is brightly lit, suggesting a window nearby. The text is overlaid on a black rectangular area in the upper left portion of the image.

IV) The future of security architecture and challenges with implementing SASE

According to Gartner, by **2026, 45%** of enterprises are expected to adopt Managed SASE Services¹, often accompanied by varying degrees of consulting services. Notably, most SASE technology vendors lack a legacy in delivering managed services.

SASE is projected to be among the top three technologies implemented by 2025, with:

- **70%** of enterprises globally currently subscribing to some form of managed security services². This high adoption rate is largely driven by a skills gap in managing numerous security vendor components.

The SASE market is anticipated to grow at a compound annual growth rate (CAGR) of:

- **36%**, reaching nearly \$15 billion by 2025³.

Sources:

- 1) [Why Cato Networks' MSASE Gives Channel Partners Vendor Power | Cyber Magazine](#)
- 2) [What's Changed: 2023 Gartner Magic Quadrant for SSE](#)
- 3) [SASE market](#)

The Benefits of SASE for Enterprises

- **Seamless and Flexible Security:** Customize your security experience to adapt to emerging threats effectively.
- **Comprehensive Security Coverage:** Leverage cutting-edge technology to ensure full security capability, while avoiding overlaps and mitigating gaps.
- **Cost Reduction:** Minimize expenses related to duplicated investments, critical incident troubleshooting, integration, and supplier management.
- **Enhanced Threat Detection and Response:** Integrate with SIEM and SOAR platforms for consolidated data, improving advanced threat detection and response across both IT and OT environments.
- **Innovative Solutions:** Achieve improved scalability for easier integration of new sites or branch offices.

Key challenges in implementing SASE

While SASE offers a transformative approach to secure connectivity, its successful implementation comes with several critical challenges that organizations must navigate:



Integration with legacy systems

Many enterprises operate with entrenched legacy infrastructure—such as traditional firewalls, VPNs, and remote access tools—that were not built for the cloud-native, distributed model which SASE supports. Seamlessly integrating these components without disrupting business operations requires thoughtful planning, migration strategies, and often, custom engineering.



Cost and ROI justification

Transitioning to SASE often involves significant upfront investment in both technology and operational change. Building a strong business case—demonstrating clear return on investment (ROI), cost savings from decommissioned legacy systems, and long-term security benefits—is essential to gain executive buy-in.




Vendor selection complexity

The SASE market is still maturing, with a wide range of vendors offering overlapping yet distinct capabilities in networking, security, and cloud delivery. Choosing the right partner—or combination of partners—requires deep technical evaluation, future-proofing considerations, and alignment with both security and IT operations.



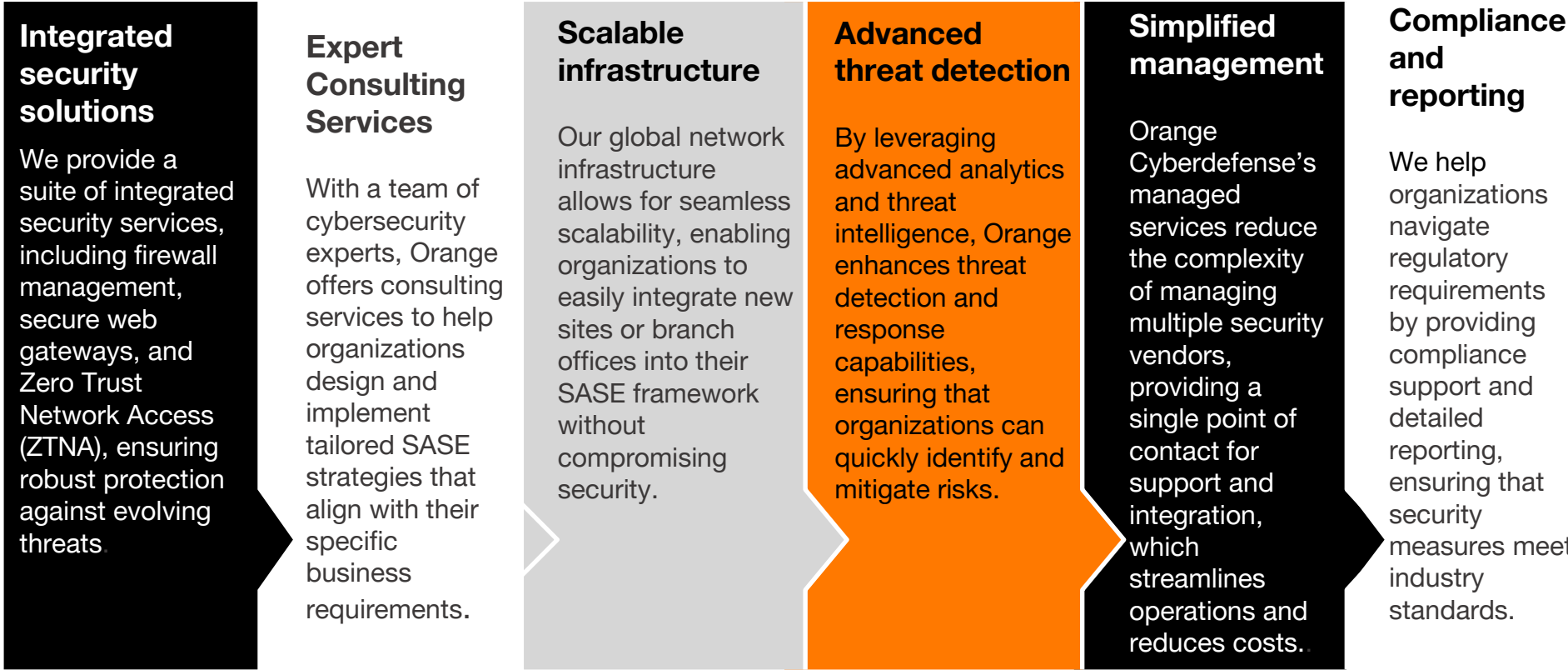
Deployment strategy

SASE is not a one-size-fits-all rollout. Organizations must decide between a "big bang" transformation or a phased, modular deployment. This requires a tailored implementation roadmap based on business priorities, existing architecture, user locations, and risk tolerance. Poor planning in this area can lead to service disruption or fragmented security posture.



**V) How can Orange
Cyberdefense help you with
SASE?**

Orange Cyberdefense offers comprehensive solutions to support organizations in their transition to SASE, ensuring managed secure access that meets modern security and connectivity needs:



Conclusion

Implementing SASE is as much a strategic transformation as it is a technical one—requiring careful planning, investment justification, and alignment across legacy and modern systems to realize its full potential.

As there isn't a one-size-fit-all solution for companies given the different pain points and complexities with their existing infrastructure, SASE's customization strength is clearly an upper hand for companies that know how to leverage it to their advantage and prefer a long-term consistency with performance and security delivery, than having to upgrade to new security features each time.

By partnering with Orange Cyberdefense, organizations can effectively implement SASE, achieving a secure, flexible, and scalable network environment that supports their digital transformation goals.

To learn more, visit [Orange Cyberdefense - Build a safer digital society](#)



Reach out to us today!



Contact person:

Santiago Gao

Senior Cybersecurity Solution Architect
Orange Cyberdefense, APAC

Email:

santiago.gao@orange.com



Thank You!



Cyberdefense