SASE: a C-suite priority

How leaders are adopting SASE as an enabler for business differentiation

orange™ Business

Secured by
Orange Cyberdefense

Contents

Executive summary

In today's digital economy, organizations of all sizes face increasing cyber threats that are putting their business ambitions at risk. However, many in the C-suite still delegate responsibility to their network and security teams rather than putting it at the center of their business agenda. For success, they should work closely with their chief information security officer (CISO) and chief information officer (CIO).

The digital economy is a rich target for cyber criminals. According to Orange Cyberdefense's Security Navigator 2024[1], in the first 9 months of 2023, the number of ransomware victims globally increased by 79% – the highest number ever recorded.

One of the reasons for this increase is that cyber criminals are rapidly adopting artificial intelligence (AI). This has driven a significant growth in attack volumes and complexity. Executive sponsorship and an ecosystem approach to security are necessary to counter them.

SASE – the digital business enabler

A secure access service edge (SASE) strategy can help to address these growing concerns head-on. It is a methodology that converges cloud-native security services with networking capabilities. It protects users and gives them the performance they expect wherever they log on, regardless of device. This supports the business needs of a distributed hybrid workforce that uses dispersed resources, for example.

However, despite its importance, SASE is often delegated to IT and cybersecurity teams and remains hidden from the boardroom agenda because it is seen as an IT issue. Typically, security is primarily prioritized on the C-suite agenda in response to a major breach – and by that point, the damage is done.

Without a strategic focus on SASE, there is a risk that organizations will suffer from vendor sprawl and tool bloat. This can make monitoring and incident response slower and much more complex.

In this whitepaper, we look at why the C-suite should address cybersecurity and network operations directly. Executive leadership can help drive the organization's business-wide SASE strategy to deliver a scalable, robust, and, most importantly, secure user-to-cloud experience.

Cybersecurity and network operations: managing business risk

The security threat landscape remains increasingly complex for the C-suite to navigate

New research shows a 30% increase in the number of security incidents detected yearly[2], and the average cost of a data breach continues to rise.

But despite increasingly sophisticated threats, cybersecurity and network operations often don't get considered in the broader business context and what the impact of a breach could have. This frequently leads to missed opportunities to mitigate threats and support overall business expansion.

Managing the business risks created by cyber threats is the responsibility of the entire C-suite. It isn't just a technology issue. While 72% of CEOs in a recent World Economic Forum report[3] have said they are uncomfortable about cybersecurity decisions, these decisions impact every aspect of the business.

To make good cybersecurity decisions it is important to not only address issues from a technical perspective but also to regard them as organizational and strategic priorities. This is why it is so important for leadership to build trusted relationships with CISOs and ensure that the organization takes a holistic approach to dealing with growing cyber threats.

Cybersecurity and networks become a growth enabler

The network should provide the flexibility and performance required to support the business while allowing for a fully integrated security posture. This helps enterprises build trust amongst partners and customers to gain a competitive edge. It also provides a robust foundation for digital transformation, innovation, and differentiated business growth.

Closing the gap between network and cybersecurity complexities and business objectives is essential for a solid overarching strategy. This is where SASE comes in, helping to protect applications and data deployed across multiple clouds and users logging on from any location on any device.

The road to a robust cybersecurity posture

Moving to a cybersecurity approach that focuses on comprehensive protection and anticipation helps focus investment on where it can benefit the business the most and ensure continuity.

Organizations are at different stages of the SASE maturity journey, and what needs to be done depends on where the organization sits on the maturity curve. The ultimate end goal is to create a risk-based approach to cybersecurity, which leverages AI to make faster and better-informed decisions.

Not all business data has the same value; consequently, security measures should not be the same everywhere. The C-suite should focus on prioritizing the network and cybersecurity investments that have the greatest business impact. This will allow businesses to target and pinpoint the biggest threats and allocate budget and resource prioritization accordingly. Simplifying operational complexity reduces data exposure and risk while also delivering cost savings. This can be achieved using a new, better-integrated architecture such as SASE.

Prioritize spending

Many organizations still widely manage cyber risk and network operations in isolation from the rest of the business, resulting in too many vendors and tools, isolated data, and limited risk-based prioritization.

Many organizations are dealing with unmanaged or partially managed risks thanks to skills gaps, vendor-specific silos, scaling challenges, and a lack of business value realization.

A risk-based approach enables C-suite to prioritize security and network transformation spend based on business impact, operational effectiveness, more flexibility, and risk reduction.

Aggregated data ecosystems

A critical first step is to break down any silos between systems and related data, including those from third parties. An aggregated data ecosystem encompassing a data and analytics operating model and robust data governance will give organizations a much more accurate picture of their network and security posture, and risk.

With the number of incidents growing to billions yearly, organizations should also look to contextual AI-augmented analytics incorporating real-time industry operational insights at scale. In other words, consider a protective SASE approach that prioritizes zero trust network access and integrates detection and response capabilities.

In the next section, we outline eight key steps that the C-suite should consider in their move toward risk-based cybersecurity operations.

C-suite actions for successful SASE adoption

Executive involvement is a critical component of an organization's cybersecurity and network strategy, working alongside the CISO and IT teams. We suggest eight actions for the C-suite to take.

Each SASE implementation is unique and designed to target specific business needs. Actions are also dependent on the organization's SASE maturity. As such, the entire C-suite has a role in successfully deploying and maintaining the framework.

The biggest myth to dispel is that SASE is a one-size-fits-all route to solving all security issues. While it is not a silver bullet, it can significantly improve an organization's security posture. Neither is SASE a single product: it is a network-security framework that combines networking and networking security into a coherent cloud service.

Here, we outline eight key actions for the C-suite to consider.

1 Define an enterprise-wide SASE strategy

SASE encompasses multiple solutions under one umbrella and requires a regularly reviewed overarching enterprise-wide strategy to be successful. An action plan can be implemented once the key business risks have been identified. This makes implementation and goals much clearer for the business and technical teams. The speed at which these deployments are made depends on each organization and its SASE roadmap.

From the CIO's stance, zero trust should be non-negotiable through a constant re-evaluation of the given access, not the authentication. Target zero trust network access (ZTNA) to increase flexibility and scalability while reducing the risk of ransomware attacks. ZTNA provides more control and visibility and reduces the attack surface through its strict user authentication service.

From a CFO's perspective, spending on SASE will increase. Over the next five years, the market for SASE will grow at a compound annual growth rate of 29%, reaching over $25 billion by 2027, according to Gartner.[4]

CFOs should work closely with the CISOs and the board to agree on risk appetite thresholds and align the cybersecurity strategy to broader business goals. This includes looking at the cost of advanced security technologies such as AI-based predictive analytics and undertaking a ROI analysis.

2 Embed SASE into the business strategy

A successful SASE implementation needs to be firmly embedded into the business strategy. It requires alignment with business goals and broader organizational strategies such as digital transformation and cloud migration. This will allow businesses to optimize technologies to streamline and modernize operations safely.

For example, SASE can provide a route to AI-augmented productivity and cost savings. It can enable safe, secure usage of Gen AI data use cases, which provides real-tangible business benefit. It simplifies and speeds up the processes for network and security teams monitoring and managing technologies, including network resources and security policies. Cost savings and operational simplification can be achieved from vendor consolidation.

A digital core, cloud-native ecosystem is now a critical business growth enabler. As such, the CEO and the C-suite must link cybersecurity and network investment to the business. This is partly achieved by more closely coupling the SASE and business strategies.

3 Create a robust, secure data mindset

Data today is pivotal to accelerating business. Organizations require a robust data strategy to operate efficiently, innovate, and retain a competitive edge. Connecting the data strategy to the SASE strategy allows for deeper preventative threat insights, quicker threat detection, accelerated containment, and faster remediation.

Quality data is the bedrock of successful AI implementations. An effective data strategy and data analytics operating model are vital to enabling generative AI at scale. Input from the Chief Data & Analytics Officer (CDAO) is pivotal.

CDAOs should pioneer the secure “data at scale” agenda to reach the business outcomes and sustainable differentiation that today’s digital organizations demand.

To achieve this, CDAOs need to evangelize the execution of the SASE data use cases with business owners to build momentum for business value realization and ROI justification. This means delivering improved decision-making, enhanced user experience, and competitive advantage.

4 Adopt a streamlined ecosystem approach

Success demands an ecosystem collaboration approach. CISOs should consider moving away from in-house-only mindsets to tap into external expertise through partnerships and wider ecosystem. This will help achieve the scaling and risk reduction that SASE offers.

Gartner expects 80% of enterprises to have adopted a strategy to unify web,cloud services, and private application access using a SASE or security service edge (SSE) architecture by 2025[5]. However, putting an end-to-end SASE solution in place is challenging regarding tool choice, skills, and management. This is where working with trusted partners comes in.

Enterprises can accelerate SASE adoption at scale by considering existing skill sets, vendors, and the timing of hardware refresh cycles in their strategic roadmap for SASE adoption. A partnership ecosystem allows organizations to draw on skilled external expertise to complement in-house skills and benefit from contextual data analytics for enterprise operations. It also provides a global, broader view across multiple clients to detect issues faster using AI-augmented assets.

SASE co-managed services will become mainstream, driven by the urgency to access AI-augmented platforms and resolve the talent gap.

5 Define specific SASE data use cases and ROI

The C-suite should carefully consider how SASE enables their long and short-term business goals.

CFOs must connect tailored business-led SASE data use cases to a tangible ROI, ensuring future SASE transformation initiatives are tightly linked to business value realization and competitive advantage.

The traditional reactive post-breach or post-non-compliance investments are no longer tenable and fail to deliver shareholder value and future financial goals. CFOs must break the chains of so-called “technical debt” and insist on a tangible ROI within six months on platform SASE data use cases.

SASE ROI will vary from organization to organization. However, the metrics to measure it will be similar in terms of increased security posture and risk reduction, increased business agility and scalability, and cost optimization.

6 Pivot to risk-based cybersecurity and network operations

Full prevention just isn’t possible. Developing a risk-based approach enables the organization to quantify dangers and protect critical business assets.

Start by understanding which assets need protecting. The next step is determining how malicious actors would target your organization and why. Finally, the C-suite must draw up a picture of the organization’s risk appetite. This includes understanding which risks the business faces and what a security breach would cost. This information is paramount in helping to decide where the security budget should be prioritized.

7 Go all in on AI

The C-suite needs to be aware that employees will create unpredictable cyber risks in every organization in the era of AI-augmented analytics and generative AI. Examples include personally identifiable data, bank account details, and application development source code, which can easily be exposed to cyber criminals if not adequately monitored and protected.

C-Suite must be aware that GenAI can make phishing and social engineering attacks more difficult to spot and that attacks could be broadened beyond English-speaking countries.[6] An effective SASE Strategy will enable safe, secure Gen AI data use cases, such as ChatGPT, to be successfully deployed.

Through 2025, generative AI will cause a spike in the cybersecurity resources required to secure it, causing more than a 15% incremental spend on application and data security, according to Gartner[7].

It is crucial to create a framework to understand precisely how AI tools are being incorporated into the business and how they are being used. Insist on measuring SASE outcomes, such as financial performance, to accelerate the cultural shift towards risk-based cybersecurity resiliency.

8 Build AI-driven insights with a platform ecosystem

AI-powered cybercriminals are now attacking with increasing volumes, authenticity, and complexity, which requires an urgent, new approach to cybersecurity and network resilience. CIOs and CISOs can improve their defense by directing the shift away from an insular in-house modus operandi and engaging with co-managed services and trusted partners.

AI and LLM capability are critical in cyber defense initiatives for organizations in the era of augmented analytics and generative AI. They can rapidly analyze zillions of events, identify event types such as malware, and spot malicious behavior patterns. AI-augmented analytics and visualization capability are being achieved through collaboration with ecosystem partners for threat-based insights.

By leveraging the platform ecosystem and associated partnerships, CIOs can help their organizations tap into AI-augmented threat-based insights for their cybersecurity and networking initiatives. This approach is highly efficient at discovering potential threats, for example. AI algorithms are also adept at threat hunting and pinpointing patterns and anomalies that security and network analysts can further investigate.

SASE: a team effort

Getting the most out of SASE requires a rethink regarding networking and security operations. It is essential to invest time to define an overarching SASE strategy with active C-suite sponsorship and close alignment with the business strategy to deliver on ambitions. At the same time, CISOs must work closely with the entire C-suite to align their vision of cybersecurity with business goals. This is very much a team effort.

Enterprises need to be very clear on what they want from SASE before they choose a partner for their journey. They should seek out a SASE framework that can be seamlessly integrated into their networking infrastructure and security architectures to ensure secure and robust connectivity alongside an enhanced user experience.

A fully aligned SASE strategy is imperative to address the AI-augmented threat landscape and enable business differentiation. To ensure your organization is prepared for the future, where AI will bring challenges and opportunities, adopt a rich set of risk-based SASE services that are agnostic from the technology vendor and can deliver business realization within six months.

Customizing the SASE journey to business needs

Selecting technology vendors without a robust SASE strategy will not automatically improve your security posture. SASE is not a one-size-fits-all methodology. Steer clear of short-term mindsets and fragmented technology vendor siloes, and rigid in-house-only operations which drain resources and impact the bottom line. Instead, focus on achieving business value, scaling operations, and harnessing contextual risk-based operations with embedded AI assets.

Few have the talent in-house to get their SASE journey on track rapidly. Partnerships and co-managed services will accelerate plans to address immediate capabilities and scaling. Having said this, SASE does not have to be complex. Visibility on the IT landscape will significantly increase with the right partner and strategy in place, which will help businesses be more resilient.

The threat landscape is continually changing

The threat landscape is complex and forever changing. Standing still or repeating the same procurement and operational historical approaches of the past is placing your business at increasing risk.

The management of cybersecurity and network operations today starts at the top and filters through the organization. Ensuring the C-suite is actively engaged in the SASE journey and committed to seeking rapid business value realization and business differentiation is paramount. The C-suite is responsible for the health and performance of the entire organization, including protecting its users and data.

Why partner with Orange Business and Orange Cyberdefense on your SASE journey

SASE is a multi-disciplinary project framework with many components. This is why working with a trusted network-native cybersecurity partner who understands SASE is vital.

Orange Business and Orange Cyberdefense deliver integrated SASE services while leveraging our extended ecosystem of best-of-breed technology partners. Successfully taking advantage of integrations between ZTNA, CASB, SWG, Firewall as a Service (FWaaS), SD-WAN, and other heterogeneous technologies will be crucial in realizing the full benefits of a SASE strategy. Edge-to-cloud expertise ensures security, performance, and cost optimization for your cybersecurity and network operations.

Our network, cybersecurity, and consulting experts across the globe can help you on your SASE journey from end to end.

- **8,900 experts to help you manage your digital transformation.**
- **18 Security Operations Centers (SOCs) around the world and 14 CyberSOCs**
- **3,000+ security practitioners**
- **A global footprint made up of 160 countries with local sales and support.**

About the author

David Andrew

Senior Partner Consulting
Orange Business

david.andrew@orange.com

David is a Senior Consulting Partner within Orange Business focusing on network-native cybersecurity, cloud strategy, SASE strategy, cloud-native data, and AI transformations.

David leads our business consulting practice across all sectors in the UK, Ireland & Nordics. He works closely with our ISV ecosystem partners and our data-network-cybersecurity experts to lead advisory and digital delivery engagements to the C-suite at our enterprise customers.

David has over 20 years of strategy and technology enabled business transformation experience, providing expertise in cloud native technologies, data strategy, digital business enablement, and IT managed services.

Sources:

1. Orange Cyberdefense: Security Navigator 2024 – https://www.orangecyberdefense.com/global/security-navigator
2. Orange Cyberdefense: Security Navigator 2024 – https://www.orangecyberdefense.com/global/security-navigator
3. World Economic Forum – https://www.weforum.org/agenda/2023/07/3-things-cisos-need-to-know-about-their-ceo-before-the-next-cyberattack-strikes/
4. Gartner: Forecast Analysis: Secure Access Service Edge, Worldwide – https://www.gartner.com/en/documents/4824531
5. Gartner: Forecast Analysis: Secure Access Service Edge, Worldwide – https://www.gartner.com/en/documents/4824531
6. Orange Cyberdefense: Security Navigator 2024 – https://www.orangecyberdefense.com/global/security-navigator
7. Gartner: Top Trends in Cybersecurity for 2024 https://www.gartner.com/doc/reprints?id=1-2G6U1RDP&ct=240109&st=sb