Navigating network modernization

Map your route to SASE for greater business productivity agility and security

Why network modernization requires Secure Access Service Edge (SASE)

Network modernization and performance have emerged as critical elements in driving excellence for employee and customer experience – not only responding to the radical changes in how we now work, collaborate and make decisions, but also in building confidence in the agility and resilience of every organization.

> Analysts report that **80% of enterprise revenue growth** will soon depend on an organization's digital offerings[1] and cloud is central to this differentiation.

Strategic cloud adoption has accelerated digital transformation but can also increase pressure on network infrastructure, stretching internal capabilities and resources to provide **'any access, from any device, anywhere, at any time'**[2].

New ways of working also require new levels of agility in applying and enforcing security policies for users wherever they are located. Digital transformation demands adaptive access and authentication – with a fundamental shift in controls closer to where they are now needed – typically the end-user and the cloud edge.

> Our research has revealed that **82% of organizations have seen an increase in cybersecurity risk** in the last six months[3].

These network and security imperatives drive a convergence of software-defined wide area networking (SD-WAN) and high-performing security into a strategic, edge-to-cloud service that doesn't increase hardware costs or add complexity – this architecture is called Secure Access Service Edge (SASE).

Our combined experience shows that SASE adoption does not happen overnight or at the flick of a switch. But if deployed effectively, SASE will not only satisfy 'Generation WFH'[4] with office-like resilience and security, but also radically simplify WAN deployment, enable a single point for centralized network management, and provide the right bandwidth provision for every user, device and application.

In this guide, we share our integrated experience of network transformation and cybersecurity advisory to help you define your SASE vision. With practical examples, we explore how to identify the mix of SASE services required to navigate your optimal path from the edge to the cloud.

[1] *Developing the New IT Capabilities for Digital Transformation, IDC*
[2] *2021 Global Managed Services Report, NTT Ltd.*
[3] *2021 Global Managed Services Report, NTT Ltd.*
[4] *Generation 'Work from Home'*

Navigating SASE adoption

1. Defining your security posture – what is your vision for SASE?

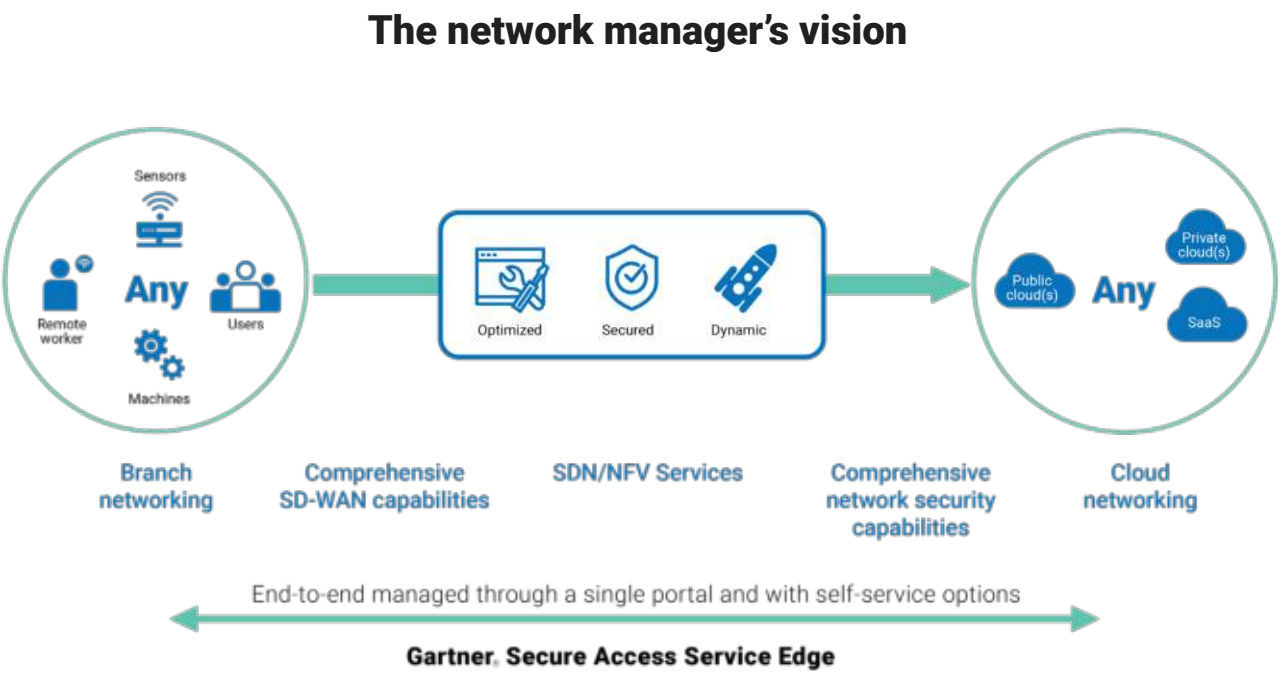


Figure 1: SASE will require more close collaboration between network, application and security specialists than before.

> **'SASE enables companies to operate during times of disruption and provides highly secure, high-performance access to any application, regardless of user location.'**
>
> Gartner 2020 Secure Access Service Edge Forecast, Joe Skorupa and Nat Smith

This statement from Gartner neatly summarizes why so many organizations are exploring SASE on their journey from crisis to recovery. With more users, devices, applications and services — and more data located outside an enterprise than inside — organizations must map a route for their network that provides greater speed, performance and flexibility with new levels of resilience and security.

Although every organization will be travelling a different path, a strategic SASE vision will include:

- A fundamental shift in access controls closer to where they are needed – typically the end-user and the cloud edge
- Drive for reduced complexity – converging security functions into an efficient as-a-service model
- A focus on supporting business agility to react to any internal and external change
- Rigorous simplification of deployment, management and policy enforcement across all environments
- The capabilities and resources to provide seamless, scalable, secure internet and cloud access anytime, anywhere

2. Removing silos – SASE as a secure-by-design intersection for network and cybersecurity

The seismic shifts to the way businesses operate caused by the pandemic, with the rapid shift to remote working and the acceleration of cloud deployment, is putting increasing pressure on the IT and security departments.

Bad actors took the opportunity to exploit the chaos and our research confirms that **nearly five in six organizations (83%) completely re-thought their IT security** to accommodate new ways of working[5].

By thinking about integration at every step, organizations can move closer to secure-by-design operations.

SASE adoption requires a convergence of skills and capabilities, with new levels of collaboration between a range of practitioners – network engineers, application developers and security specialists. For some organizations, this demands a common operating language across IT and security departments for the first time. In addition, strategic stakeholders such as people and access management and compliance leaders become part of the conversation to define advanced policies for data loss prevention (DLP), cloud access security brokers (CASBs) and zero trust network access.

A SASE approach requires integration of multiple security and IT services from an organization's first line of defence, with a DNS layer through a secure web gateway for zero trust – enabling deeper inspection to a cloud-delivered firewall to secure web and non-web traffic.

Many organizations embark on a SASE journey with central management of policy creation and monitoring, increased threat protection and extended security services from the data center to any cloud demanded by the location, user or IoT devices. By combining multiple security functions into a single, cloud-native service, CIOs and CISOs can establish greater central management capability with reduced complexity.

Furthermore, any SASE architecture must be forward-looking and sufficiently agile for business resilience. It needs the ability to scale to meet the traffic and performance demands of further cloud adoption and 5G deployment.

3. More than technology convergence – where SASE delivers and protects business value

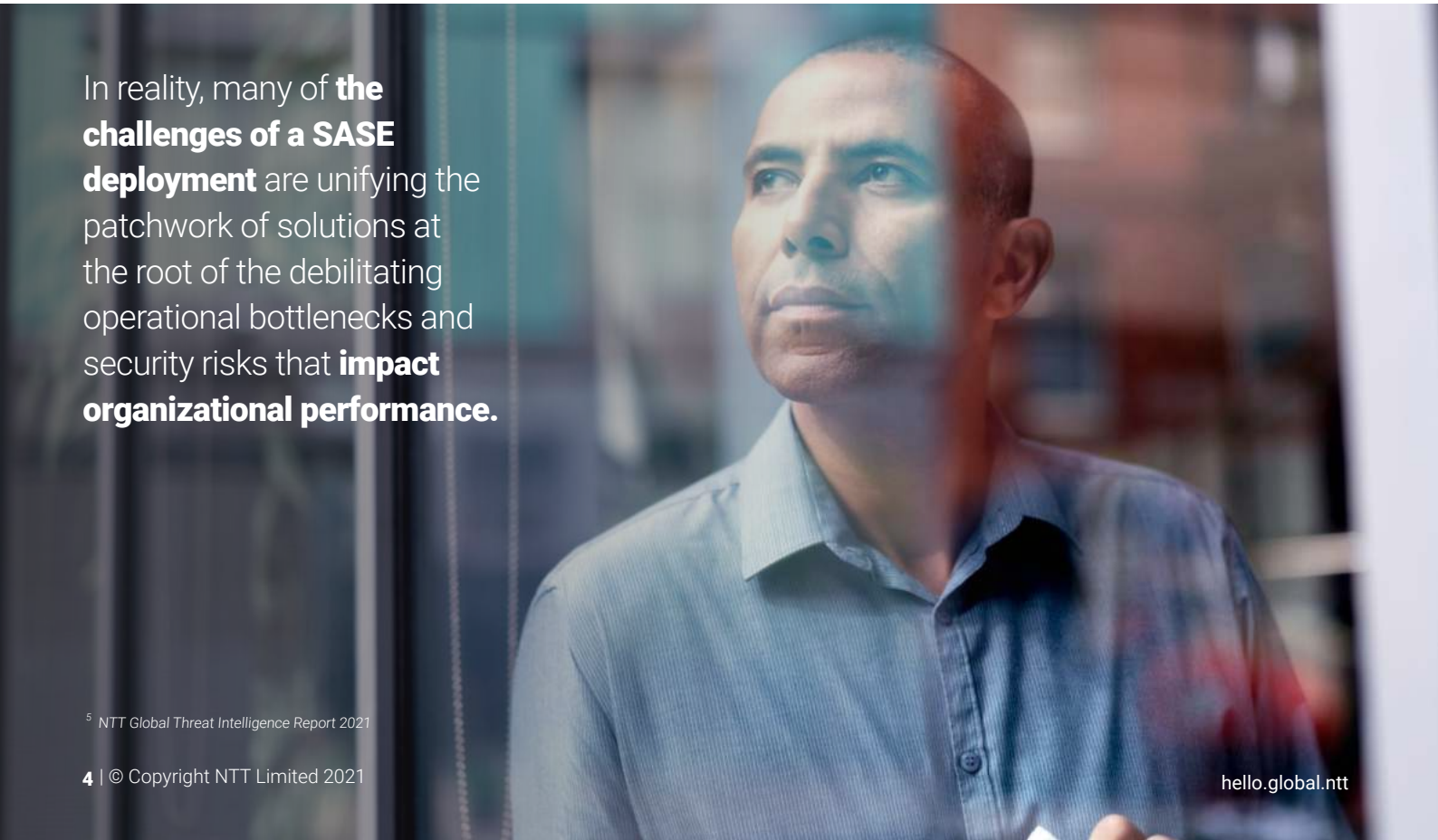
Simplification and security are two driving principles of network modernization. One of the major benefits of this new approach lies in centralized network monitoring and management.

Whether monitoring the center or the edge, convergence cuts costs and increases cross-stack visibility across hybrid environments.

A common framework to analyse users, applications and data will offer a common understanding of any issue and enable faster resolution. The single interface enables far more detailed, consistent analysis and reporting to inform faster decision-making and performance management. **SASE builds on the connectivity benefits of SD-WAN, adding optimized MPLS, internet, and hybrid connectivity, along with integrated security.** It simplifies branch networking by replacing the range of network devices that exist in many organizations with a simple device at the branch that provides access to a wide array of services.

This approach radically reduces the time and effort required for configuration monitoring and troubleshooting of functions such as routing, switching, Wi-Fi, micro-segmentation and application support.

And finally, new applications or services can be deployed much faster. This is not just another argument for automation; rather it is a leap forward in rapid, granular policy definition to meet fast-moving business requirements.



In reality, many of **the challenges of a SASE deployment** are unifying the patchwork of solutions at the root of the debilitating operational bottlenecks and security risks that **impact organizational performance.**

[5] *NTT Global Threat Intelligence Report 2021*

4. Planning the path to effective SASE adoption

The practical questions to ask to map a SASE strategy:

1. Where will we be in five years?
The first point of assessment is to understand potential application shifts in the near and longer term. Applications that are hosted in a data center today may at some point move to the cloud as workloads increase. Applications that were used on-premises may soon be consumed as-a-service. All these potential shifts and the consequent impact must be analysed to inform strategic decision-making.

2. What network performance do you need for the journey?
A detailed analysis of where and how applications are being used and where they may be used in future will highlight the impact on the network; for example, the demand for an increase in bandwidth or a demand for secure cloud connections.

3. Anticipate the direction of traffic flows
Organizations will have greater control if they anticipate not just the type of traffic, but the directional flows as well. A SASE architecture will enable side-to-side communication, end-user to cloud communication, or even a hub-and-spoke environment.

4. Multicloud connectivity as standard
A network modernization design will create a clear framework that includes cloud connections, site-to-site connectivity and user-to-application connectivity.

5. Green light for secure branch networking
Centralizing security into the cloud requires an organization to review the full IT stack of a branch.
Part of the SASE journey is embracing an asset-light concept, which requires an agile managed service to ensure all branches are continuously under control.

6. Go up a security gear
We work with clients to support the migration from on-premises cloud-ready network and security functions to as-a-service, ensuring that organizations can take optimal advantage of intelligent network modernization that is secure by design.

7. No legacy application left on the starting blocks
Nearly every organization has legacy applications that can't be moved to the cloud, or events that are not optimized within the network. Whether in the cloud or on-premises, these must be accommodated as part of your SASE journey and assessed against the long-term business objectives.

8. Regular servicing and pitstops
SASE is an ongoing journey to support rapid business change and growth.
As such, it requires a continuous re-evaluation of the user and application demands and the consequential evolution of a SASE architecture and supporting SASE services. We encourage our clients to continually ask themselves the following questions:

a. Does our network design and performance enable positive business outcomes?

b. Have I considered security controls and policies in every technology decision to ensure our organization is secure by design?

c. What could I change to positively impact business performance?

The ongoing pandemic has emphasized the importance of a secure, high-performing network fabric as a critical asset to support modern business applications. **NTT has been recognized based on our completeness of vision and our ability to execute within the Gartner 2021 Magic Quadrant for Network Services, Global and 2021 Critical Capabilities Report for Network Services, Global.***

Read more at https://hello.global.ntt/insights/2021-gartner-magic-quadrant-for-network-services-global

NTT and Cisco – a trusted partnership

SASE is a sophisticated concept that requires new levels of collaboration between internal and external stakeholders and a bold commitment to breaking down long-established silos of capability and technology ownership. Organizations that are actively mapping and navigating their SASE journey will encounter fewer bumps in the road with the right partners to inform their decision-making and prioritize programs.

For over 28 years, NTT and Cisco have worked together to maximize the potential of the multi or hybrid cloud environments for thousand of clients on every continent.

Through agile, secure-by-design infrastructure and collaboration at every stage of the journey, we help organizations simplify IT complexity and drive innovation to deliver business outcomes. Our shared history, expertise and vision enables us to deliver a unique and trusted approach in designing, deploying and managing SASE architectures.

The NTT and Cisco partnership combines our deep knowledge of network modernization and **evolving cybersecurity risk for a successful SASE deployment.**

No matter where you are on your transformation journey, we can help you to achieve the agility, end-to-end security, improved performance and cost optimization you need from your network.

To find out how to securely achieve your network modernization objectives, visit: **hello.global.ntt/solutions/network-modernization**

Together we do great things