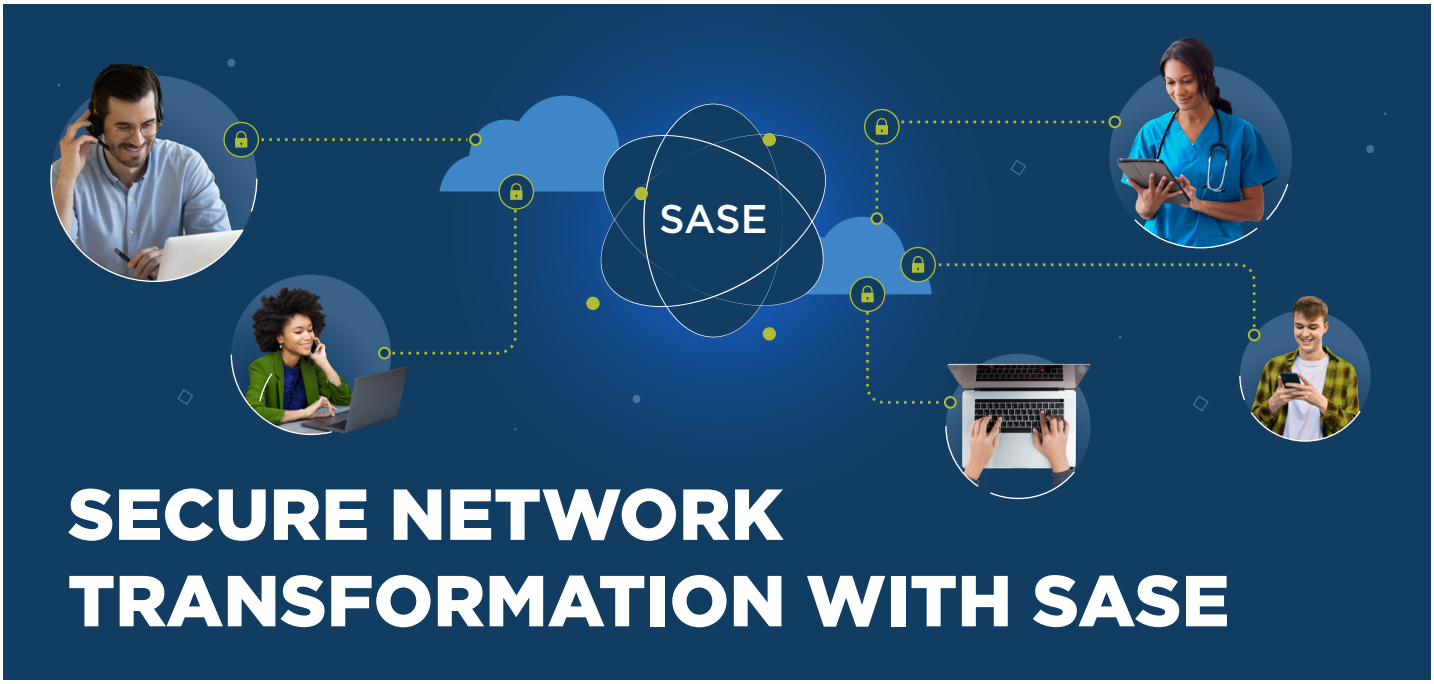


SECURE NETWORK TRANSFORMATION WITH SASE

At a glance

- The network and security challenge facing enterprises
- A clear roadmap for SASE
- The need for a trusted partner with industry expertise

WHEN LEGACY NETWORKS NO LONGER FIT THE BILL

Remote working is now a standard practice of our post-pandemic world, with the modern workforce relying more than ever on resources distributed across data centres and the cloud. Legacy networks are turning 'inside out', and the traditional MPLS-heavy, hub-and-spoke network architecture is under serious review. Not only are enterprises beginning to question the reliability of their traditional MPLS networks; they're looking to new technologies – like SD-WAN – to help deliver the connectivity they need in today's anytime, anywhere world.

What's more, recent network expansion and the proliferation of endpoint devices make enterprises especially vulnerable to cyberattacks. Breaches can happen anywhere, whether it's from an employee device or head office, on a virtual private network (VPN) or the cloud. Chief Information Security Officers (CISOs) are under pressure to adapt rapidly to this changing landscape. In addition, security and network teams need to collaborate effectively to ensure robust threat detection and prevention.

Secure Access Service Edge (SASE) offers the direction and guidance that today's enterprises need. Fusing robust security functions with a truly modern network, it gives users seamless connectivity and access to applications, while also continuously monitoring activities and devices so that data can be secured wherever it is accessed, all without sacrificing user experience.

60%

of enterprises will have explicit strategies and timelines for SASE adoption by 2025[1]

up from **10%**

of enterprises with explicit strategies in 2020[2]

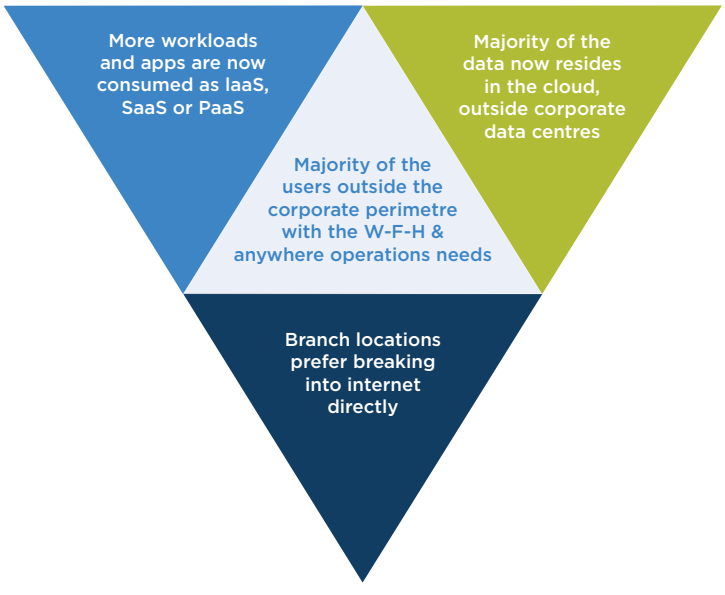
IT ALL STARTED WITH THE EVOLUTION OF CORPORATE NETWORKS

Not long ago, a clear network perimeter used to encompass offices, users and on-premise applications inside a corporate network. The primary role of the IT team was to ensure everyone was securely connected through public and private networks – and this used to be a simple exercise. All it took was putting a firewall at the perimeter to separate the enterprise's resources from the "outside": and the network was secured.

However, today, cloud infrastructure spending has overtaken on-premise spending. And the onset of digital transformation has produced the need for anytime, anywhere access to applications. As a result, the adoption of cloud access and anywhere operations has been so rapid that it has triggered an "inversion" of the network.

Outlining recommendations for successful adoption of SASE, this paper explains how organisations can develop a roadmap for implementing networking and security controls that will deliver real, incremental results in the near term – while laying the foundation for a secure, cloud-first, internet-first IT environment.

Network Inversion



The challenges of legacy architecture

Organisations still backhaul network traffic to data centres for inspection

Channeling network traffic to a central office, only to send it to the cloud and back out again, is commercially and technically inefficient

Network traffic roundtrips add hundreds of milliseconds to every communication, as well as incremental monthly costs for the Multiprotocol Label Switching (MPLS) bandwidth, making a centralized model less viable

An inverted network calls for matching security architecture

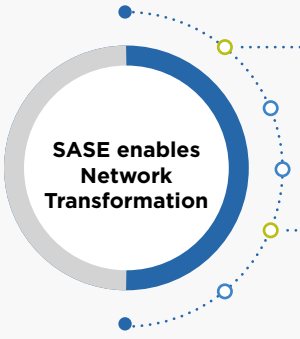
A truly modern network cannot be achieved without the right security controls in place. This is because:

- The distributed nature of enterprise data makes it harder to enforce rigid access rules, bound by the physical or virtual walls of an organisation
- Organisations need to ensure the free movement of data so employees can be productive and customers can transact business whenever and wherever they need. This movement must be enabled only after implementing the right security controls to ensure company data is protected – organisations, for example, must be able to detect whether an employee is downloading commercially sensitive material from the public cloud on their home computer or sharing a revenue forecast from an email with third parties including analysts
- Wherever they are, users need to be protected from attacks to keep data and applications safe

A SUCCESSFUL SASE STRATEGY

We recommend enterprises view SASE as an architectural shift to their network and security controls. Hence implementing SASE is not as simple as buying a ready product. For it to work effectively, SASE needs to be a fully engrained feature of an enterprise's secure network transformation plan, so that users can connect to business resources and applications – securely and efficiently – no matter where they are. The two main principles driving the shift to SASE are:

SASE is an architectural shift



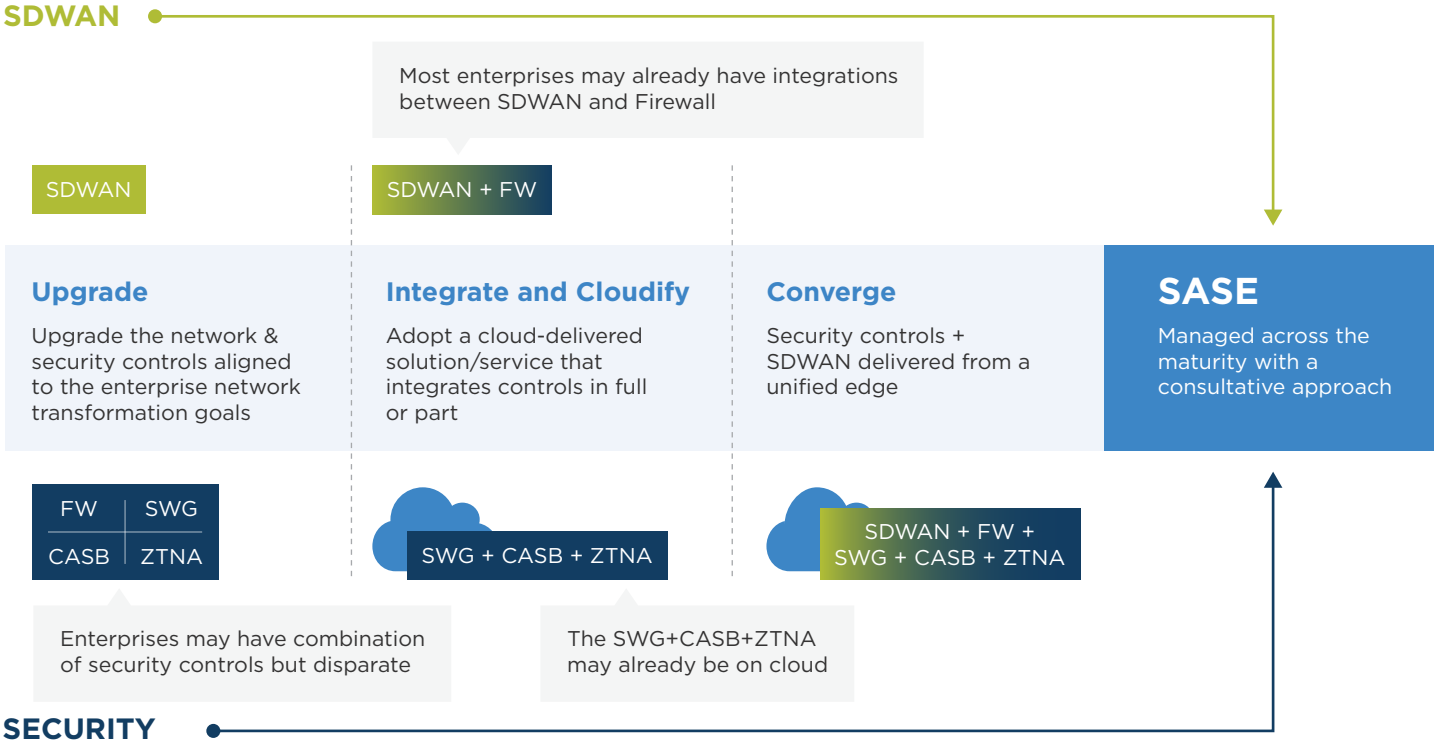
Convergence
the integration or unification of network and security controls

Cloudification
network and security controls delivered on the cloud

The good news is that the foundation of an organisation's SASE architecture can be deployed immediately, and then improved upon in deliberate, incremental steps. Drawing on our deep expertise in this area, Tata Communications has put together a clear roadmap for any enterprise embarking on their SASE journey.

SASE IS AN EVOLUTION, THAN A REVOLUTION

Tata Communications recommends enterprises approach their SASE adoption through **an upgrade, integrate, cloudify and converge approach.**



Phase 1: Upgrade security and network to align with network transformation goals

Organisations are evolving their network transformation with SD-WAN. SD-WAN allows them to gain direct cloud connectivity and optimum user experience with dynamic path selection and policy-based routing based on software-defined policies. This gives enterprises greater control and visibility, as well as choice over private and public networks.

But along with SD-WAN, organisations must upgrade their existing security controls as the hybrid network environment renders legacy security models irrelevant. Visibility and control across an entire network requires robust security tools that enable resistance against breaches and attacks. Organisations in this phase must secure their transformed networks using a multi-layered defence strategy, utilising the latest security controls – including Zero-Trust Network Access (ZTNA), Cloud Access Security Broker (CASB) or Secure Web Gateway (SWG) – to their existing controls, such as perimeter-based firewalls. This will help provide comprehensive protection for people, processes and technology against all cyberthreats.

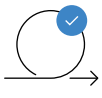
Phase 2: Integrate and cloudify

In this phase organisations should move their network and security controls to the cloud and integrate them in full, or part, to create a unified edge. By integrating these controls, organisations will be able to enjoy comprehensive network security coverage while being able to directly access cloud applications, regardless of location.

Cloud-delivered security solutions apply security at the edge without backhauling traffic to the data centre. This helps the reduction in MPLS costs enabled by using SD-WAN, while also improving user experience through reduced latency. And given that cloud-delivered solutions come as a service, they eliminate the need to deploy hardware, as well as configure, manage, and replace or upgrade these appliances. Organisations can also use security and network policies that are managed centrally, but deployed locally, enabling a distributed security architecture.

Phase 3: Converge

Organisations should be looking to converge the functions of network and security solutions into a converged, global cloud-native service – delivered from a single edge. This will enable a secure network transformation that is adaptive and contributes to evolving digital transformation needs. At this point, organisations will begin to enjoy the following benefits:



Greater business agility – provisioning of new resources and capabilities will be fast and simple. IT will be able to deliver optimized networking and robust security to all locations, applications, and users, regardless of where they are

Reduced management complexity – simplifying the network and security controls by consolidating multiple point products in a single solution will enable organisations to reduce complexity of their IT infrastructure by abstracting upgrades, patches, and maintenance tasks while increasing visibility and ease of management

Cost savings – having a single cloud-native solution will eliminate the need for multiple physical and virtual appliances, which will result in significant cost savings

End-to-end visibility and control – with the "true" convergence of security and networking functions, organisations will be able to manage all features and policies from a single interface, using a common terminology, and gain deep visibility across network and security events across all edges

A MANAGED SERVICES APPROACH CAN ENSURE THE RIGHT SASE STRATEGY

Correct implementation of SASE is absolutely crucial if enterprises are to enjoy the full benefits of SASE. The right SASE partner should be able to:

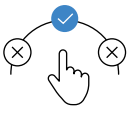
Take single ownership of the complete IT landscape across WAN, SDWAN and security

Craft an effective SASE journey, no matter which phase an organisation is in, with a choice of mature integrated security and network services

Provide an OPEX-based solution which enables a pay-as-you-grow model

Demonstrate experience in integrating and managing security and network controls across multiple vendors through a single pane of glass

Enable automation of routine tasks and processes to save time, while enabling faster detection and response to security threats



Mobilise strong vendor relationships with SASE partners to select and deploy the right solutions much faster

IN CONCLUSION

Whether you want to boost the productivity of your anywhere workforce or allow customers to connect with you round the clock, every step taken towards SASE will bolster the security of your network, data and mission. Tata Communications has the expertise, industry connections and global connectivity to deliver a unique, cost-effective and seamless SASE roadmap to help you take that first step – and ensure you're ready to take on the challenges of a cloud-first, internet-first world.

Source:

1. https://www.gartner.com/en/newsroom/press-releases/2018-12-03-gartner-says-the-future-of-it-infrastructure-is-always-on-always-available-everywhere
2. https://blogs.gartner.com/andrew-lerner/2021/03/26/checking-in-on-sase/

Start your SASE journey with confidence – get in touch with Tata Communications today.

For more information, visit us at **www.tatacommunications.com**

Contact us

© **2021 Tata Communications.** All Rights Reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Limited in certain countries.