AT&T Business

Edging Towards SASE: Next generation networking, cloud and security

An AT&T Guide

Introduction to SASE

John V. Slamecka,
Region President, EMEA & LATAM,
AT&T Global Business

The global pandemic has delivered a paradigm shift in the relationship between employees and their workplace.

The concept of working from home, or to be more accurate, working remotely, had never been fully tested. Until it had to be, at scale and at speed, as businesses adapted to keep their operations running in the face of global ‘stay at home’ orders.

As workers start to find their way back to the office, there’s a recognition that many will want to retain some of the flexibility offered to them during the COVID-19 pandemic.

Which means businesses have a challenge: where they connect from, how they connect and what they connect with.

This army of remote workers numbering in the millions around the world means there’s a permanent problem to solve. People – your people – are sitting outside of the corporate network using the internet to access resources in the cloud.

The challenge is how to optimise their experience and keep them and the data they use safe.

SD-WAN started the software-defined networking revolution. Now the next logical step is wrapping that networking and security technology together. It’s called SASE (pronounced sassy) and stands for Secure Access Service Edge. The term, coined by leading analyst firm Gartner in 2019, describes architecture that combines wide area network (WAN) technology with comprehensive security functions.

AT&T Business

The next stage of digital transformation

Before COVID-19, the convergence of SD-WAN, security and cloud was several years down the road. Now, the next stage of digital transformation is coming much sooner than many of us in this industry expected it to.

It's not really a case of 'if' with SASE. It's 'when'. And your teams – and customers – still expect a great user experience wherever they are. In this eBook we'll set out the what, why and how of SASE. The when, however, is down to you but we are here and ready to draw on our extensive knowledge of complex, global network implementations to help you make it happen.

What is SASE?

SASE in a nutshell

Simply put, SASE brings SD-WAN and security together in a cloud-based service. And because it's in the cloud, it can be scaled up or down to meet the needs of the business, especially when things need to change fast.

Before COVID-19, a technology shift from traditional connectivity 'pipes', multiple remote data centres, racks, and rooms full of boxes and switches was already underway. It's accelerating and SASE is the way forward.

SASE brings so-called Zero Trust networking, which bases access on user, device, and application, as opposed to location and IP address. Think about it in the context of a large headquarters building. In the old model, everyone who works there likely has an ID badge which gets them through the front door. Some floors or rooms will have additional locks which require additional security clearance.

In the new model all access is denied unless specifically granted, so you only gain access to the necessary offices and rooms. This can limit 'wandering around' by the employee or anyone who compromises the employee badge, or for example finding a confidential document accidently left behind at a printer in a different department.

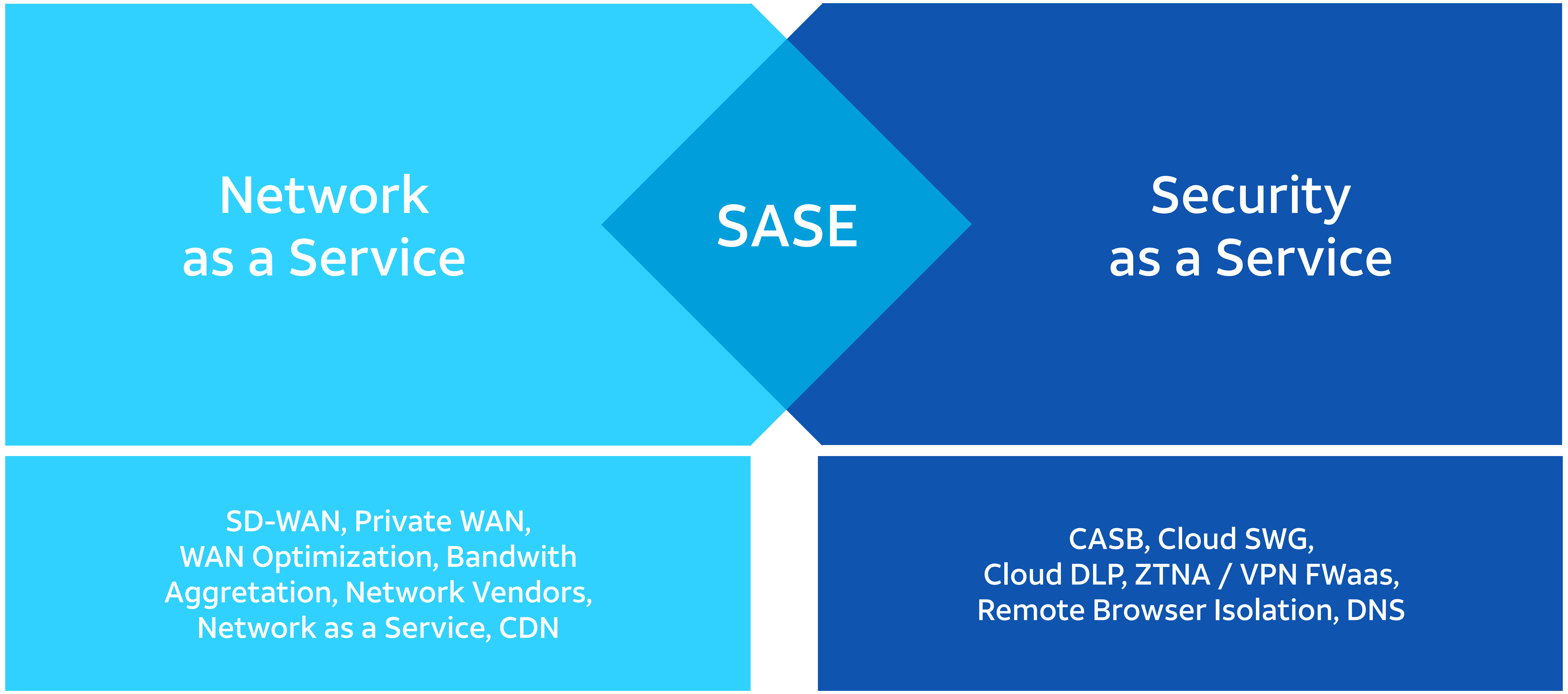
A SASE-enabled wide area network employs the same principles, giving every end point a digital identity and then applying policies which give access to applications and data. Furthermore, in a large enterprise it's probable that there will be a mix of employees, partners, contractors, and customers accessing the network. Zero Trust replaces traditional security – such as the VPN – and due to more granular controls, reduces the risk of potential attacks spreading quickly through the enterprise.

> “At AT&T, we are ready to deploy our expertise and remove complexity from your next stage of digital transformation.”

The result is a consistent, secure experience wherever the end user is located.

Multiple vendors are in the marketplace with SASE solutions. Choosing the right architecture which meets the needs of the business is critical, and that means working with a company which has relationships with best-in-class solution providers and can bring everything together at scale across the globe.

At AT&T, we are ready to deploy our expertise and remove complexity from your next stage of digital transformation.



Network as a Service
SASE
Security as a Service
SD-WAN, Private WAN, WAN Optimization, Bandwith Aggretation, Network Vendors, Network as a Service, CDN
CASB, Cloud SWG, Cloud DLP, ZTNA / VPN FWaas, Remote Browser Isolation, DNS

The "Why"

Rupesh Chokshi

Vice President, Product Strategy & Innovation

What is driving the security evolution and subsequent SASE implementation?

Although it was first coined in 2019, industry experts were expecting SASE to be mature enough for implementation at scale by 2022. COVID-19 changed all that. The resulting move to remote working accelerated the business imperative for SASE by at least 18 months. Almost overnight, IT leaders had to deliver reliable, highly-secure connectivity to company networks; cyber threats were mounting and the need for cloud-based applications to support remote working was growing. Fast. In many cases, this meant tearing up the old IT infrastructure playbook and rethinking how to deliver truly hybrid work options. Enter SASE.

With hybrid as the new normal. It seems unlikely we will ever go back to the way things were. The flexibility afforded is far too compelling for businesses – and their employees – to revert to a solely office-based approach. But this approach is not without its challenges.

Different locations, devices and networks create gaps in the IT ecosystem. This compromises visibility and protection. Data is no longer confined to the corporate data centre – a critical concern for many. Traditionally, this would force enterprises to bolt on layers of disconnected tools to close the widening opportunity gap for attack.

Enter Zero Trust. No-one gets access, data, or connectivity unless the controls put in place says they can. Everyone is the enemy, and the battle plan is set up accordingly.

Remote working has also amplified the move away from controlled on-premises, customized business functions within a walled garden. The next-generation cloud-based global ecosystem needs a secure architecture to underpin and support collaboration beyond company boundaries – a multi-cloud strategy.

“Enter Zero Trust. No-one gets access or data unless unless the controls put in place says they can. Everyone is the enemy, and the battle plan is set up accordingly.”

Rupesh Chokshi, Vice President,
Product Strategy & Innovation

A better user experience

SASE's blend of Zero Trust Network Access (ZTNA), SD-WAN and secure web gateway (SWG) can support the needs of a hybrid workforce and their increasingly connected devices outside of the confines of the business. Instead of using many tools and vendors for different solutions, a SASE approach can help IT teams consolidate and manage their networks more securely. This consolidation also results in improved network performance, lower cost and complexity, and a better user experience.

Having a managed security service provider (MSSP) can help relieve the burden of both implementation and the daily operations of connectivity and security products from internal technology teams. Which means they can get on with the day job.

Lessons learned from SD-WAN, SASE history

Is SASE right for you? What we can learn from SD-WAN implementation

When software-defined wide area networking (SD-WAN) emerged in 2016, enterprises realized that at some point they would need to modernize their networks and SD-WAN would be at the forefront of that strategy. But the question was when and how do they start?

When SD-WAN first appeared, one of the top benefits was viewed as cost-savings, followed by a reduction in provisioning time and performance improvements. Today, enterprises find greater value in reaching their desired business outcomes of optimizing IT resources, improving productivity and performance improvements with cloud applications. By embracing a cloud-first strategy with SD-WAN, enterprises have been able to realize:

- Better optimization of their IT personnel with centralized policy administration and network management
- Improved applications performance based on availability and response times
- Ability to optimize and securely connect remote employees to cloud-based applications
- Enhanced security planning with a more granular policy administration
- Greater cost-saving in their WAN expenditures

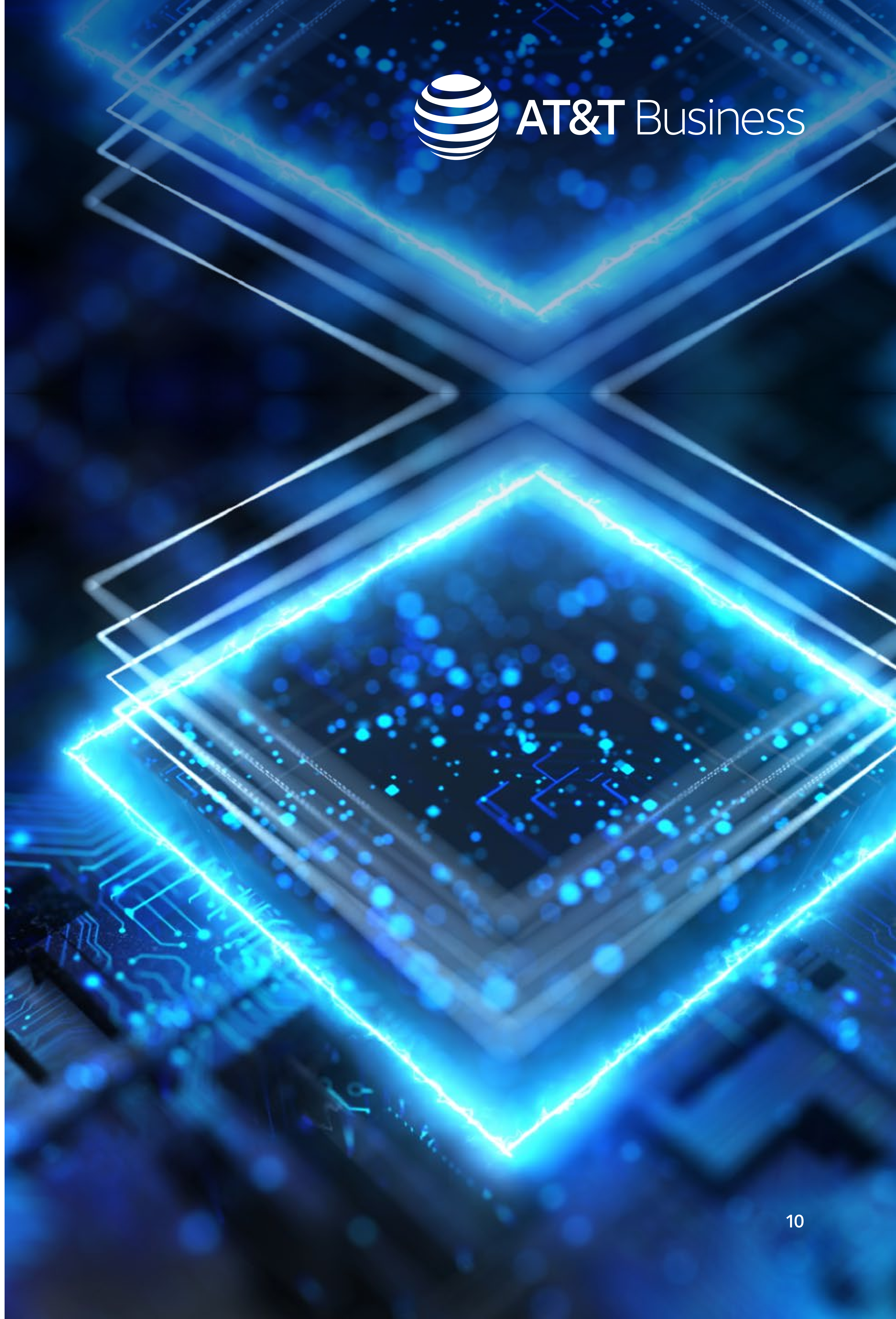
As enterprises are looking to modernize or are in the midst of modernizing their networks with SD-WAN, security has become an increasingly important discussion point and integral part of the plan. The COVID-19 pandemic is forcing many to rethink their digital strategy and accelerate their digital transformation. Today, businesses are looking to support a more remote workforce by solving both their connectivity and growing security requirements to maintain the continuity of their operations and protect an ever-expanding attack plain.

“Another key lesson is the importance of the right service provider to minimize the challenges faced when choosing and deploying SASE solutions.”

Interest in, and the need, for SASE is ever increasing to solve business challenges such as the convergence of connectivity, networking and security to support the growing digital transformation needs of today and in the future.

Lessons learned from the early days of SD-WAN can help ease the adoption of SASE. Many enterprises start with a proof-of-concept (PoC). This allows them to realize the benefits SD-WAN and the security that it can deliver to their enterprise, allowing them to map their deployment and scale it to achieve network transformation goals. As enterprises continue to move through their modernization, they should look to a PoC to help them identify and define their desired business outcomes, and experience how a single stack SASE solution can assist their needs.

Another key lesson is the importance of the right service provider to minimize the challenges faced when choosing and deploying SASE solutions. To overcome operational challenges that can otherwise become overwhelming, businesses should partner with an experienced managed service provider, one that offers a consultative approach, and considers the needs of the business, existing IT resources and the network.



Why is AT&T taking a cloud-first approach?

Jeremy Legg,
Chief Technology Officer,
AT&T Technology Services

It's easy to think the pandemic froze businesses in their tracks, pushing IT transformations to the back burner as everyone struggled just to keep the lights on and key services up and running. But the truth is transformation never stopped, not for our customers and certainly not internally at AT&T.

The cloud has been at the core of our internal transformation over the last 18 months.

At the start of that journey, we only had a handful of applications running in the cloud, with the vast majority operating out of dedicated data centers scattered across the country. With the 5G era upon us and our fiber buildout picking up steam, we knew we needed to upend the legacy IT model that tied us up in never-ending hardware upgrades, patchwork repairs on software platforms that were in some cases decades old, and data center maintenance and operations. That wasn't our core competency and there wasn't time for distractions.

At the same time, those IT systems do power critical platforms and tools we use to support our customers and our network. So turning everything off wasn't an option, either.

We needed to modernize, retire, and transform all at the same time, and the cloud was the answer.

From just that initial handful of cloud apps, we're now up to more than 1,450 apps running in the cloud, with thousands more either retired altogether or moved into a small number of consolidated data centers.

“Our cloud journey has been so successful that we’re adopting that approach in other parts of our business now, too. ”

Jeremy Legg, , Chief Technology Officer,
AT&T Technology Services

We’re faster, nimbler, more aggressive, and able to allocate resources to network deployment while improving customer service.

In fact, our cloud journey has been so successful that we’re adopting that approach in other parts of our business now, too. We recently began migrating our 5G core to Microsoft’s Azure for Operators cloud platform. We’re still deploying and managing our network. That’s what we do. But adopting cloud technologies into the network will help us move faster, manage costs, and meet our customers’ needs.

“Cloud” might sound like a buzzword, but the benefits are real. With the world changing in often unpredictable ways right now, cloud transformation is vital to help businesses focus on what they do best.

Gartner Analyst Perspective

Gartner

Gartner® coined the term SASE back in 2019. It is therefore appropriate that we look at some of the research shared by Gartner experts, and understand the thinking behind those words.

As already outlined in this eBook, the need for Zero Trust security is a core element of any digital transformation roadmap that includes SASE as an option.

According to Gartner, "a mix of legacy perimeter-based security hardware, the use of different vendors for CASB, SWG, ZTNA and SD-WAN functions, and separate organizational structures for networking security and networking have created a complex and unmanageable collection of vendors, agents, consoles and traffic hairpinning."*

From that, it's clear that simplification is a requirement of a successful SASE rollout. Timing is another factor, mapping out the pain points and then dealing with them in a multi-year journey.

Gartner recommends: "Form a joint network and security team to develop a three-to five-year roadmap for SASE transformation covering secure access strategies for users, branches, edge locations and distributed applications,"* whilst also sounding a warning that "vendor hype complicates the understanding of the SASE market."*

To read the Gartner report for additional detail, click the link below:

Gartner Strategic Roadmap for SASE Convergence

*Source: Gartner, 2021 Strategic Roadmap for SASE Convergence, Published March 25, 2021
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Q&A: Challenges to adoption and how they can be overcome

Leon Chang

Director, Strategy and Innovation

Why SASE - how will it benefit my business?

The COVID-19 pandemic prompted a shift to remote and hybrid work. An increase in multi-cloud and Zero Trust adoption and an ongoing skills shortage are contributing to the rise of SASE. In many enterprises, IT teams might utilize multiple tools for each problem. SASE encompasses a range of capabilities including SD-WAN, security, and multi edge compute which can allow enterprises to consolidate those tools. This consolidation results in improved network performance, lower cost and complexity, better user experience and higher security efficacy.

Having an MSSP can help relieve the burden of both implementation and the daily operations of connectivity and security products from internal technology teams, which is especially valuable during a time of skills shortage.

Why should SASE be front of mind for CIOs/CTOs?

Today, with a more dispersed workforce, we need ubiquitous connectivity, and this makes the security of data in transit very important. Things are going to continue to be more interconnected because that's how modernisation, business processes and the flow of information will work.

This increased level of connectivity also comes with an increased degree of risk and cybercriminals look to attack at the point of most vulnerability – which includes remote workers.

Businesses considering a move to the SASE framework are driven by the need to improve user performance and security via Internet access for both on-premises and remote workers. In modern life, this is every business and CIOs are aware of the need for this transition. Each will follow a slightly different path dependent on individual needs, but the trajectory will remain.

> "Each business will follow a slightly different path dependent on individual needs, but the trajectory will remain."
>
> Leon Chang, Director, Strategy and Innovation

Jacco Jurg

Director, Strategy and Innovation

How do I integrate SASE into my networking?

Most of you will adopt more than one technology vendor and a hybrid model in the initial stages, where traditional networking and security systems can handle existing connectivity between data centres and existing sites, leaving SASE to take care of new connections, devices, users, and locations.

What can help is employing an MSSP to focus on specific requirements, which will vary depending on the size, type of industry and plans for future development.

However, the overhead and effort required to deploy a solution like SASE may be more than some organisations are able to undertake.

This is where a strong service provider, with the right networking and security platform, can help by engaging with organisations and designing an approach aligned to their business requirements and needs.

Why should SASE be front of mind for CIOs/CTOs?

Today, with a more dispersed workforce, we need ubiquitous connectivity, and this makes the security of data in transit very important. Things are going to continue to be more interconnected because that's how modernisation, business processes and the flow of information will work.

AT&T's managed security services includes deployment strategy in alignment with the business/network requirements.

When will existing network and security models become obsolete?

Traditionally, companies have deployed multiple products to address their secure remote workforce needs, such as web gateways, next-generation firewalls, secure virtual private networks, cloud access security broker (CASB) solutions, SD-WANs and more. These disparate products come with their own policy management and logging, creating a complexity that increases the administrative cost and can lead to gaps in the overall company's security posture. With organisations demanding uninterrupted, secure access for their users, no matter where they are located, a novel approach to networking and security is needed.

> "What is clear is that we are hurtling towards a centralised future and business models have no choice but to adapt their security models or risk facing very expensive and potentially detrimental risk."
>
> Jacco Jurg, Director,
> Strategy and Innovation

This new approach is the Secure Access Service Edge (SASE). SASE converges software-defined wide area networking (SD-WAN) and security services – firewall as a service (FWaaS), secure web gateway (SWG), CASB, and Zero Trust Network Access (ZTNA) — into a single cloud-delivered service. SASE solves the challenge of delivering consistent, secure access no matter where users, applications or devices live. Because it is a single service, SASE dramatically reduces complexity and cost.

No-one – unless they have a fully functioning crystal ball – can say when current existing models will become obsolete. What is clear is that we are hurtling towards a centralised future and business models have no choice but to adapt their security models or risk facing very expensive and potentially detrimental risk.

Martin Schulze

Director, Strategy and Innovation

Why is Zero Trust important?

The Zero Trust framework was released by Forrester in 2009. A couple of its key tenets are the principle of least privilege and that all traffic should be inspected, regardless of being on network. Some Zero Trust concepts are referenced in SASE, including the idea that access should be based on identity of data, as opposed to location.

Zero Trust assumes that traditional access credentials are no longer sufficient to accurately establish trusted identities for user and application access. Rather, organisations should undertake continuous, risk-informed assessment of those component parts entities with granular security controls to manage, monitor, and enforce access. This solution grants access only to the specific applications users require to complete their job duties, which in turn reduces the number of users that have access to sensitive data.

How is SASE different from any other security service?

Applications are moving out of the data center and into the cloud, more employees are working from remote locations than ever before, and data is being accessed from a wide range of company and personally owned devices. This makes it difficult for network and security administrators to know what applications and data are being accessed by whom, as well as their usage. And what isn't seen is much more difficult to manage and secure.

With SASE, organisations can utilise the power of their network and security as a business enabler. Administrators are empowered to provide users with low-latency access to applications hosted at the data center or in the cloud, and to apply unified security policies virtually anywhere business is conducted.

> "With SASE, organisations can utilise the power of their network and security as a business enabler."
>
> Martin Schulze, Consultant,
> Director, Strategy and Innovation

Future of SASE – Where are we going?

Rupesh Chokshi
Vice President, Product Strategy & Innovation

Transforming industries with SASE

Many organizations were already on their way to modernizing their networks with SD-WAN, but security became an important part of the conversation this year as digital transformation accelerated. Customers have had to solve challenges for both connecting and protecting an expanded remote workforce and an increasing number of remote sites, branches, or pop-up locations. Interest in SASE increased to solve these challenges as connectivity, networking and security converge to support the digital transformation requirements of today – and tomorrow. By 2025, Gartner predicts that at least 60% of enterprises will have explicit strategies and timelines for SASE adoption.

There are many paths to take when deciding how and when to deploy SASE technologies. Building a roadmap of upcoming network and security transformation initiatives and starting the proof of concept (POC) process to qualify SASE solutions early can help set up businesses for increased productivity, fewer risks, and simplified management.

In 2022, SASE will become a real solution for customers. The pandemic proved the need for business agility and many organizations are looking at SASE as providing business continuity and resiliency through network and security virtualization, which allows for faster changes when needed. These changes are transforming industries. Earlier in this eBook, we saw how a medical group struggling with network latency, and reliable remote access and application performance during the pandemic implemented AT&T's Managed SASE solution.

"Retailers benefit from fast deployment of centralised, cloud-based business and security policies, allowing their stores to focus on selling products rather than networking or security management issues."

Rupesh Choski, Vice President,
Product Strategy & Innovation

The solution supported dozens of their new remote clinic locations, an international call center, and thousands of remote employees, enabling the provider to better meet patient demand, and improve network performance and resiliency with centralized security management.

Besides healthcare, other industries benefit from SASE. Financial institutions see improvements in latency between branch connections while maintaining strong security for stringent compliance requirements. Retailers benefit from fast deployment of centralized, cloud-based business and security policies, allowing their stores to focus on selling products rather than networking or security management issues.

AT&T Business

At all stages of their digital transformation

Beyond 2022, with 5G utilization being more widespread, SASE will become more important in pulling together the 'connectivity continuum' of MPLS, broadband, and wireless. As underlay networks evolve, SASE serves as a highly secure, software-defined, and intelligent overlay capable of accommodating customers at all stages of their digital transformation.

References

https://cybersecurity.att.com/resource-center/infographics/protecting-data-in-5g-edge-world
https://www.business-standard.com/article/international/only-30-of-firms-in-us-europe-to-embrace-full-return-to-office-model-121052900353_1.html
https://www.sdxcentral.com/articles/news/att-combats-sase-confusion-as-adoption-surges/2021/09/
https://cybersecurity.att.com/blogs/security-essentials/setting-the-cyberscene-leading-with-a-security-first-mindset
https://about.att.com/story/2021/att_sase_palo_alto_networks.html
https://cybersecurity.att.com/solutions/secure-web-gateway/what-is-a-secure-web-gateway

AT&T Business

Thank you

To learn more, email:
globalmarketing@att.com