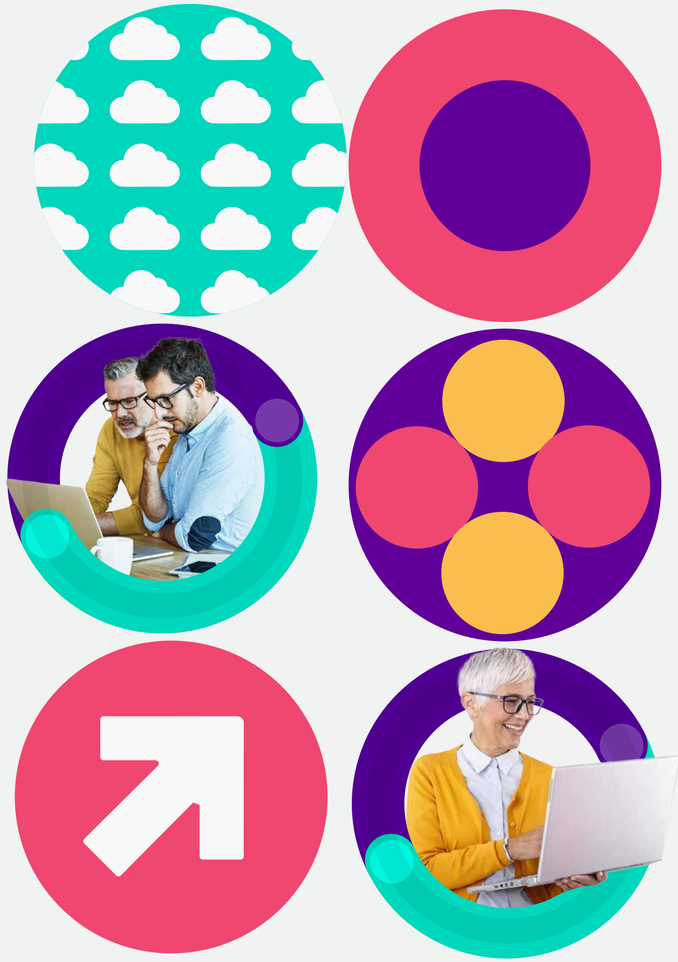
colt

Secure beyond borders:

A guide to **SASE** implementation



Nowadays, networks know no bounds. Employees work remotely and critical systems reside in the cloud, so there's no longer a defined edge to your network. This flexible approach is steadily becoming the new normal for enterprise architecture, but what do business leaders need to consider when looking towards the limitless edge of their cloud-based enterprise?

These digitally distant assets can come under fire from cyber-attacks, and suffer from siloed support limitations: if an employee working remotely cannot access core business systems or a cybercriminal gains access to your network, solving these issues from a distance can cause headaches for CIOs. How does the business apply risk management across widely distributed assets, balancing robust security, governance and compliance with performant application and data availability to run the day-to-day business?

Given that protecting their estate is a top priority for CIOs, IT decision-makers and business owners, each architecture comes with differing risks and controls; the logical answer must be to control all access to every business resource using one converged network and security solution. Though there isn't a one-size-fits-all fix, building digital infrastructure that combines reliable access, robust security and remote support in the form of SD WAN with SASE means you can protect access to business assets and provide the required performance for all users of your modern boundary-free business.

SD WAN and SASE: at a glance

Secure access service edge (SASE) describes how an architecture provides both a flexible and programmable wide area network (WAN) and cloud-based security controls within the same system. This model benefits from cloud-based computing to control data and communications but has comprehensive protection built into the system itself rather than having separate security systems ‘bolted-on’ in different parts of the organisation, as you might see in a traditional configuration.

Software-defined wide area networks (SD WAN) are recognised as the best approach for businesses spread across geographically disparate locations. The technology simplifies network management by separating it from the hardware that traditionally hosted it, allowing for cost-saving changes that get the most out of dynamic end-to-end performance protection via cloud-based platforms.

Cloud security is then added to complete the SASE model, often referred to as ‘SSE’. Security service edge (SSE) describes a collection of security technologies, controls and capabilities that provide pervasive modern security policies, such as Zero Trust, to govern and protect user access to both corporate resources and third-party systems, such as websites, apps and APIs.

A (for access) = your network

SSE + A = SASE

Security service edge

SASE = A flexible and programmable wide area network (WAN) that features cloud-based security controls within the same system

With such a variety of options available to accelerate your digital transformation comes a broad scope of considerations: security, legislation and hybrid workforces, to name but a few. We sat down with Colt's Security Product Manager, Mark Bales, who describes how to navigate these solutions in this seven-minute video.

SASE & SSE: What do they mean for me?"

All these technologies evolve network protection, compared to legacy systems like firewalls. Back when networks were hosted on-site, moat-like security strategies could safeguard businesses effectively, but a business with no boundaries needs a lot more.

You'll find that certain vendors specialise in a particular segment of digital infrastructure: some offer award-winning security solutions, others pride themselves on being network specialists, while some provide a full 'ground to the cloud', all-in-one SASE package.

As businesses grow in tandem with network, so too do the options available for IT managers on how they evolve their digital infrastructure. The key thing to consider is whether to go for a single-vendor SASE solution where the whole of your stack comes from one supplier; or whether to take the best technology from multiple vendors and create a truly 'best-in-breed' solution for your business.

It was impossible to escape the topic of AI in 2023 and in our 2023 Intelligent Infrastructure Report, we found that 47% of IT decision-makers had already adopted AI in some form. SASE is the perfect foundation to build artificial intelligence into your business; if you've decided to embrace the potential of this industry-changing technology, consider how your future digital infrastructure plans might be able to support implementation.

The future of SASE

According to Gartner®, “The SASE market is forecast to grow from $7 billion in 2022 to $25 billion by 2027 (a compound annual growth rate of 29.4%). The market also has a fast-growing number of new competitors. Technology general managers must focus on building compelling SASE offerings and expanding in regional markets.”*

According to us, this means that the opportunities for businesses to adopt a SASE solution, either from one or multiple vendors, are only set to increase. Businesses can rely on digital infrastructure companies to help guide them through this process, knowing that their experience will aid their decision on who can provide the ideal solution.

*Gartner, Market Opportunity Map: Secure Access Service Edge, Worldwide by By Evan Zeng, Neil MacDonald, Naresh Singh, 6 November 2023

Option One: Streamline with a single vendor

The benefits

Adopting a SASE solution with a single vendor includes all of the necessary features in one streamlined package. Normally the choice of businesses with tighter budgets and those with fewer systems, the single-vendor option means you can cut straight to the upgrades SASE provides without having to delve too deeply into the nuts and bolts of a more in-depth configuration.

Bundling your SASE together from a single vendor lowers the level of investment required. Because each layer of your network comes from one source, a more cost-effective solution can normally be arranged. This also avoids incompatibility issues that a multi-vendor solution could produce; your stack comes from the same place, meaning everything is configured to work together seamlessly.

Having a single point of contact for your SASE network means that all queries or concerns can be directed at a dedicated team, simplifying the billing, troubleshooting and maintenance process. The same goes on your end, too: IT teams won't have to worry about lengthier resolution times as all issues can be directed at your sole vendor.

Single-vendor solutions reduce network complexity, saving on bandwidth consumption. Having your infrastructure managed by one supplier means that they're usually in a single location, which reduces traffic having to travel further. Shorter connections improve security, increase reliability and reduce latency, all of which will benefit your network's functionality.

What to consider

While simplicity is appealing, it does mean you're forced to compromise on a 'best in breed' option in the market. A single vendor might lack in a certain area, meaning your business might have to upgrade if its needs change over time, producing continued investment in the long run.

A unique deal with a single vendor simplifies processes but usually results in a longer term of contract, effectively locking you in. Changing suppliers is also a complex process, so being sure your business doesn't need the flexibility a shorter SLA affords bears consideration before signing on the dotted line.

If your single vendor suffers an outage for any reason, the issue could result in downtime on your end too. You'll need to assess what might happen if your vendor goes down and how your business will handle it.

Single-vendor strategy in action

The most direct path to digital transformation, single-vendor SASE is for:

Option Two: Build flexibility into your network with multi-vendor SASE

The benefits

For a truly best-in-breed approach, a multi-vendor SASE infrastructure will give you the most comprehensive, feature-rich solution. For businesses with bigger budgets, being able to pick and choose the highest-ranking product or solution means you'll be maximising your stack's potential. You might choose SSE from one vendor and network access from the other, resulting in a configuration that's built to last with a 'tailored fit'.

SASE deployments mean that the network team and the security team need to agree on the features available in their area of responsibility. Adopting multiple vendors reduces the likelihood of either team having to compromise on deployment: an advantage over a single-vendor strategy that normally comes with a higher maturity level.

Multi-vendor solutions are far easier to reconfigure over time: if you find that one portion of your network isn't performing to the fullest of its potential, or a new security posture is difficult to deploy via a given vendor's security offerings, the opportunity to swap to a new supplier or product is far more likely.

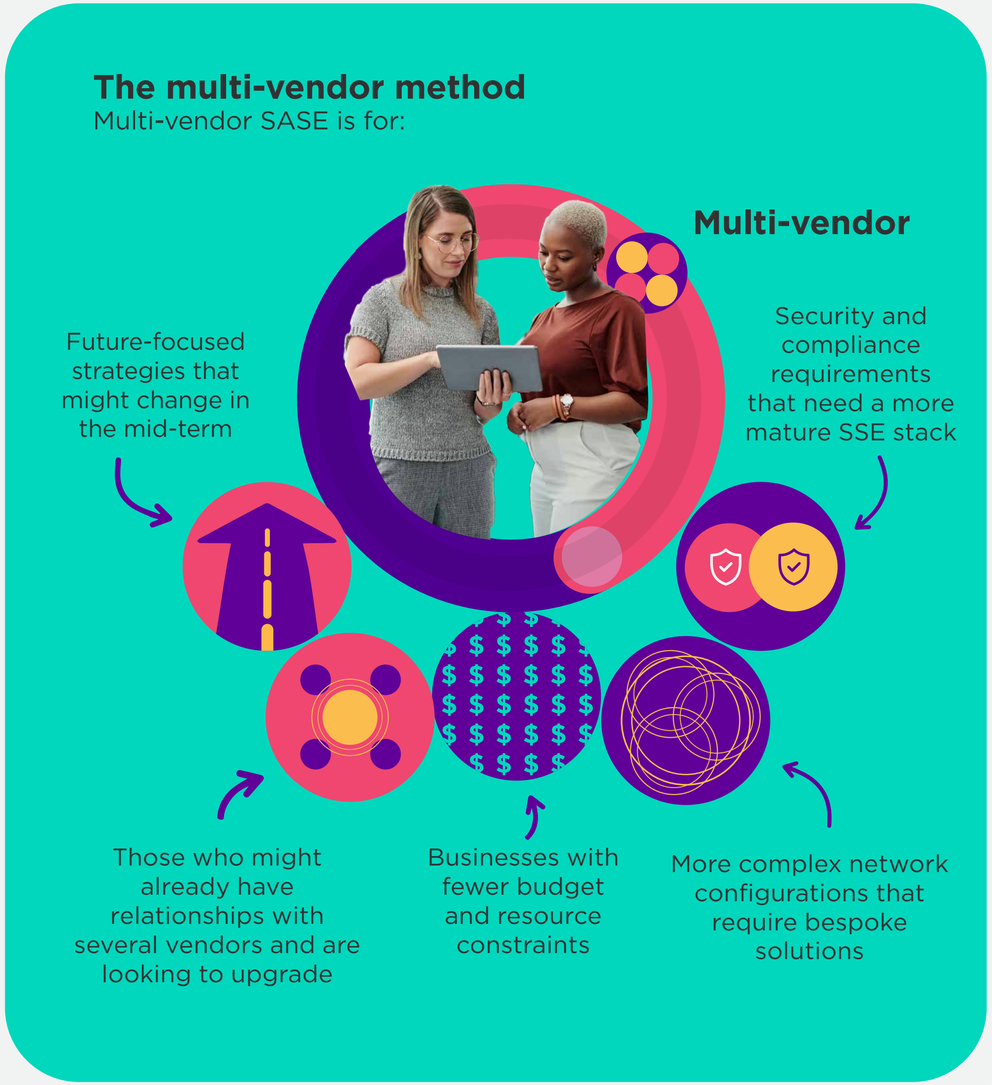
If there's downtime in one of the layers of your network configuration, it doesn't bring down the whole infrastructure; multi-vendor SASE improves redundancy and day-to-day productivity. An isolated issue wouldn't compromise the whole of your business, so for example, a network outage wouldn't jeopardise your security posture.

What to consider

Multi-vendor SASE is the pinnacle of digital infrastructure, but it does mean your IT teams or chosen supplier will need the knowledge and expertise to handle what could potentially be a complex combination of moving parts. Compatibility between vendors will need to be carefully planned, as they are not usually designed with third parties in mind: equipping engineers with the necessary skills to competently manage your infrastructure is a critical requirement.

Likewise, interoperability between multiple vendors means updates and advancements in technology have to come in tandem, lest incompatibility creeps in. You'll need to make sure you're kept up to date on all product updates among all of your vendors so that one portion of your SASE set-up doesn't hinder the others.

You'll be operating on some of the leading network technology on the market, but with it comes a greater level of management: multiple vendors require multiple portals, SLAs and billing requirements. Fortunately, single service providers such as Colt specialise in managing these relationships and integrations on your behalf, so you can concentrate on business as usual and leave the operational tasks to them.



Beyond your border

Depending on the needs of your business and where you are on your digital transformation journey dictate what solution might be best for you. Are you taking your first steps towards evolving your digital infrastructure, or do you already have a high-performing network but need additional security to solve new-age considerations?

If you're after an efficient solution to support your growing business, the single-vendor approach is most suitable. The components you decide to adopt are designed to interoperate, and as your solution is coming from one source, the cost savings would benefit your business's future growth.

If you're already setting the pace and have fewer overhead limitations, selecting the 'best in breed' approach by choosing which suppliers will provide each stack of your infrastructure means the multi-vendor strategy is ideal for you.

Whichever route you decide to go down, having a single service provider guide you along the journey will help you navigate the hurdles of adoption. There are several factors to consider, such as the increasingly demanding regulatory compliance now facing businesses. Service providers specialise in planning the first phase of a SASE project, so you're set up for success from day one.

Why Colt? Access a borderless network

We choose to work with a select choice of vendors because we know that they provide the best-in-class solutions for network potential. Their expertise, matched with our thirty years' experience putting the power of the digital universe in the hands of our customers wherever, however and whenever they want, means whatever your plans are for transformation, we can help you.

Our expert team of solutions engineers, cybersecurity experts and network specialists can guide you through your options, helping you decide which direction to take on your digital transformation journey. Each business is unique, as are its requirements, and helping you navigate your options is what our experts do best.

We can help support your IT team in effectively adopting a new network configuration, guiding them towards effective in-house management of your infrastructure. Having a network that isn't performance-optimised will not fulfil its fullest potential; we make sure that your business is making the most out of some of the industry's most effective technology.

Want to find out more?

Book an Innovation Workshop and speak directly to one of our team about how we can help you secure your network and keep making extraordinary connections.