EBOOK

SASE and successful digital transformation

EBOOK

SASE and successful digital transformation

wavenet

Contents

Introduction

The way we work has changed, and the tools, platforms and devices we use have also changed.

Many of us are well settled into hybrid or more flexible work patterns by now. And at the very least we expect to be able to work online from lots of different locations.

But has the technology caught up with the reality yet?

In this in-depth report, we'll explore the remaining challenges for technology. And how a secure access service edge (SASE) model could be the ideal solution for businesses now because you can monitor and secure enterprise traffic from a single, cloud-native platform. That means you can protect and defend each and every individual user. Wherever (and however) they're working.

We are one of the UK's leading managed service providers. We've delivered end-to-end IT solutions to over 22,000 UK customers over the past 20 years.

We work together with Cisco to create networking solutions that suit every business, across different sectors. Whether it's future-proofing, system updates or security that you need, we do it all. Wrapped up in one simple gold standard service.

CISCO Partner

It’s a bottle neck

It seems almost ridiculous to talk of ‘traditional’ business networks when we’re discussing technology that was regarded as cutting edge a decade ago, but that’s the world we live in.

Wavenet’s Cisco SASE Product Manager, Darren Sinden, gives us a reminder of just how much things have changed within a short space of time, using his own experience as an example.
“If you look back five or 10 years, I was spending most of my time, apart from when I was on the road meeting customers, sat in one of our offices,” he says.

“I was using a CRM application that was hosted at head office. I was using a Mitel telephone system that was hosted at head office. What else did I use to do my job back then? I was using the Microsoft product suite that was hosted within the company. When I went to see customers, I had a Blackberry with email and not much else.

I couldn’t use a CRM system remotely. I couldn’t really use the laptop outside of the office, certainly not to access any work applications.”

That focus on working largely from the office had a direct impact on the way networks were designed. “If you were the IT director at that time, you have almost all of your users sat on a company site,” says Sinden.

“To do their job, they’re connecting to applications that also sit on another company site or part of the corporate network. Networking at that time was relatively simple. You added a private network that connected all of your branch offices back to head office and your data centre.”

Security was also relatively straightforward because data could almost be physically contained. With most people working on site, “you could put all of your network security and all of your security policies in the centre of your network, because that was where your internet gateway was.

If you were an IT director with a relatively limited team of people, you could manage that internet break out, the firewalls that are associated with it, and all of the security elements associated with it too, because physically they were essentially located in one place.”

“That traditional network approach, just isn’t the right approach anymore,” Sinden says. “It’s got loads of downsides. Primarily, it’s a bottleneck. All of your traffic has to tunnel back to this centralised architecture to then break out to the internet.

“It means that companies are always fighting to catch up because you just chuck in loads of bandwidth in the places it doesn’t need to go. You need to upgrade your circuits continually. You need to upgrade your firewalls and all your other associated network hardware.”

Avoiding those bandwidth bottlenecks and the obvious desire to ensure today’s cloud applications are properly secured are two of the reasons why many companies are embracing secure access service edge (SASE).

SASE connects all your systems and users on the cloud

So it's goodbye to lagging and hello to better security

What is SASE?

It's a cloud-first approach to networking married with a cloud-first approach to security.

Implemented correctly, it's a win-win for both the company and its employees.

Why?

Because the company doesn't end up spending needlessly on bandwidth and networking hardware, while remote working employees aren't left frustrated when applications freeze and they can't do their jobs. IT directors can sleep more easily at night, knowing the correct access and security controls are in place for cloud applications, minimising the risk that sensitive company data is going to leak.

Many aspects of SASE have been around for a while, but bringing all those pieces together reaps real benefits.

It isn't a single product that you can order in one hit. It's a network architecture that combines a number of different technologies. When those building blocks are put in place, not only should your company benefit from enhanced security that is specifically designed to cater for today's widely distributed workforce, but increased network performance too.

Here, then, are the five key components of SASE:

- SD-WAN
- Cloud access security broker
- Secure web gateway
- Cloud-delivered firewall
- Zero trust network access SD-WAN

Let's look at them in more detail...

SD-WAN

(Software-defined wide-area networking)

Crucially, SD-WAN can take advantage of the full gamut of available connectivity – fixed line or mobile – to ensure employees get the application performance they need, whether working from the office, home or on the road.

With SD-WAN, software or virtual appliances are used to apply application-level policies, ensuring the most demanding applications get the bandwidth and security they need.

And that removes one of the big bottlenecks that businesses face on a more 'traditional' networks, where companies extend the network over large distances, physically connecting branch offices with data centres to create secure links for data.

That was fine before the emergence of high-bandwidth/low-latency apps like videoconferencing and VoIP, which now put enormous strain on more traditional WANs and force companies to keep reinvesting to eradicate bandwidth bottlenecks or application performance suffers.

Cloud access security broker/barrier (CASB)

CASB allows a company to enforce its security policies upon cloud applications.

No matter where a person is working, or what device they're using.

The CASB helps an organisation monitor user behaviour and put strict controls on which employees get access to which data, so that staff can't access data that isn't critical to their job function, reducing the risk of data leaks.

The CASB will also monitor which third-party apps have access to company data, allowing the business to quickly shut off any apps that are deemed a security risk, either because they're a known malware threat or may potentially leak sensitive data.

How does the CASB do all of these jobs?
It acts as the intermediary between cloud providers and employees, and spans across software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) environments.

Access to cloud applications has become an essential part of modern productivity, with employees requiring the same access to apps and company data whether they are working from the office, from home or travelling.

Secure web gateway

'A high level of protection, coupled with detailed reporting'

We're putting these two together, because they're both encompassed by solutions such as Cisco's Umbrella SIG technology, which can be bought and configured through our partnership with Cisco.

A secure web gateway minimises the risk of web-based threats wreaking havoc within your organisation. Users can be prevented from downloading certain file types (such as .exe or .iso files) that are regular sources of malware. And any files that are downloaded or uploaded from the company network will be scanned for known malware.

The gateway can massively reduce the risk of data leaks by applying granular controls to specific applications. Users can be blocked from uploading files to Dropbox, for instance, or from uploading attachments to Gmail accounts.

This high level of protection is coupled with detailed reporting, allowing network managers to identify and block threats that might be specific to their organisation.

Cloud-delivered firewall

The cloud-delivered firewall gives the company full control over the type of internet traffic that's permitted across its network. Unwanted traffic can be blocked using IP, port or protocol rules. Plus, there's automated detection and blocking of known vulnerabilities, helping to ensure that the business isn't caught out by existing threats.

Zero trust network access

Trust used to be based on location. If you could get inside a company's building, you could get inside their IT systems.

Trust was traditionally based on location, with access to the network granted if a user was physically inside the company's premises. That model simply doesn't work in today's world, which is why zero trust network access is important.

Zero trust network access helps ensure it's only your employees or contractors who are getting that access and not bad actors.

This is achieved in a variety of ways. Businesses are protected against stolen login credentials with multi-factor authentication, ensuring compromised passwords aren't sufficient to gain access to sensitive data and applications. threats that might be specific to their organisation.

Different risk profiles can also be assigned to different applications. You might decide, for example, that an app explaining the company's benefits scheme has a lower risk profile than one containing customer sales data, thus applying security policies accordingly.

The sheer number of devices being used inside businesses these days is mind-blowing, especially when you take into account employees accessing company data from personal devices. Zero trust access networks can identify devices that pose a security risk and enforce enhanced security policies for those specific devices. Compromised or stolen devices, meanwhile, can be blocked completely.

Combining all these different SASE building blocks might seem like a daunting task, but that's where we and partners such as Cisco can help. Our experts have extensive experience of helping organisations move to a SASE environment that could bring huge benefits to your business.

Get the bandwidth to where it's needed, whilst saving money

Today's critical business applications are bandwidth intensive and require low latency.

Video meetings, online collaboration tools and rich SaaS applications are intolerant of patchy connections. If all of your company's internet traffic is handled by a traditional MPLS WAN – where traffic is fed through a central hub to be inspected by security appliances – cloud application performance will likely suffer. The company will find itself in a bandwidth arms race, furiously adding expensive networking hardware and extra capacity, just so that staff can keep working.

Don't be tempted by the sticking plaster solution. SD-WAN, one of the core SASE components, will not only help you get the bandwidth to where it's needed, but could also save money on IT infrastructure costs.

SD-WAN lets the business leverage all the different types of transport technology – whether that be MPLS, broadband internet or mobile broadband – to provide a secure connection between users and the applications they need to do their jobs.

By dynamically assigning bandwidth and choosing the most appropriate transport method, SD-WAN avoids the need to funnel everything through a central hub. Your staff get the performance they need, without compromising on security.

Out-of-the-box office

Our SD-WAN solutions are powered by Cisco Meraki, making deployment as simple as possible. Out-of-the-box MX appliances can be plugged in almost anywhere, providing an office-like experience for home workers or temporary offices anywhere in the world.

As Sinden, explains:

"There's a range of network devices that are specifically designed for branch offices and home workers. For example, if you've got a branch office with 100 users in there, there'll be two or three devices within the Meraki portfolio that have got the required throughput to cope with that kind of bandwidth.

"If you've got a much smaller site, like a retail site or a construction site, where you probably don't need super-high-performance levels, but you want that box to also provide some switching and wireless access for people working in what is probably quite a small office space, Cisco has a product within the MX range that will do that.

"If you're a home or remote worker and you want to have a little teleworker box the size and shape of a home router, they've got those too. In other words, SD-WAN can have a liberating effect on your business, freeing staff to work wherever best suits them and the organisation."

Get the bandwidth to where it's needed, whilst saving money

Configure-and-go

SASE depends on licenses, not hardware and software. So managing your IT system is simpler - and scalable.

Having staff and appliances dispersed in hundreds or even thousands of different locations might fill an IT director with dread. How will that network be managed? How will it be secured?

The Cisco MX appliances are designed to be zero-touch and 100% cloud managed. Whether staff are sitting at their desks in the company's head office or working out of a home office in their back garden, your IT team will have the exact same visibility and management capability. The MX appliances are even available as virtualised images, meaning they can be deployed in public and private clouds. And all of these appliances – physical or virtual – can be configured from a single dashboard.

"The bit that makes it all happen, ultimately – and this is true of any good SASE solution – is that everything you want to do with that hardware all - of the features that you want to turn on is basically down to what licences you buy," says Sinden.

"It's then about configuring the features within that licence, once, in the cloud dashboard, and then just pushing them out to your entire estate, regardless of whether it's head office, branch office, remote worker, data centre or public cloud environment. You push out that configuration in one go."

SASE helps give IT directors greater control over their entire environment than they've ever had before. And that applies to security too, with IT staff no longer having to fret about whether branch offices have applied the latest updates or having on-site IT staff to apply security patches.

"When security vulnerabilities have been identified, and a software upgrade needs to be applied, you can just find an appropriate time for your network to push that update out," says Sinden. "You do it en masse; it doesn't matter whether you've got five offices or 500 offices."

Get the bandwidth to where it's needed, whilst saving money

Improve efficiency

SASE can deliver office-grade network performance to staff irrespective of their location, improve security and network management, and provide much-needed flexibility for IT staff.

If that's not transformative, we don't know what is.

With the managed services offered by us, businesses don't need to have large teams of IT staff on call around the clock to deal with the latest threats. Our Security Operations Centre (SOC) is highly experienced at dealing with the threats that many different types of organisations face, whether that be ransomware attacks, distributed denial of service (DDoS) or network intrusions. And, of course, when the SOC identifies a new threat attacking one client, it can learn from the method of attack to protect other clients from similar strikes.

And our managed services give companies the flexibility to decide how much of the security and network management functions they want to leave in the hands of their own staff. That flexibility also protects companies from forces outside of their control, such as shortages of trained IT security staff, meaning the business is never left exposed.

Q&A

Darren, tell us why SASE has become so relevant?

"The number of threats there are to a corporate network has exploded in recent years.

SASE is a phrase that Gartner came up with a couple of years ago and it's basically the merging of that cloud-first approach to security with a cloud-first approach to the network.

If you're an IT manager that suddenly needs to put networking equipment, particularly firewalls, in potentially hundreds or thousands of branch offices, homes or devices, you need a way to adequately provision, manage, upgrade, and apply software and security patches from a single place, maybe even remotely."

Why partner with you instead of other providers?

"Connectivity and cyber security are two of the most mature and successful areas of our portfolio. We own and operate a core network providing over 300,000 circuits to our customers. We've been providing solutions as a Cisco Gold Partner for more than 20 years and have been providing managed SD-WAN solutions since 2015.

That gives us a fantastic combination of scale and references, not just in SD-WAN or cyber security, but in both, which as they come together will be increasingly more important. We have partnerships with leading vendors globally and have top-tier accreditations with those vendors. In order to get that, you have to transact a certain amount of business in that particular product line, and you have to train and maintain a certain number of sales, pre-sales, delivery and support engineers within that product line.

In short, you have to know your stuff!

On top of that, we can not only design, deploy and manage the SASE solution but also include other value-added managed services from our networks or Security Operations Centres into a single, all-encompassing service for our customers who want that bit of extra help from a partner. This also frees up their time to focus on driving their business forwards."

Q&A

People often focus on the security benefits when it comes to SASE, but the network performance benefits are huge too, right?

“Security is the prerequisite to let everything else happen. You could build the best, most appropriate network for your business model, but if you can’t secure it, you’re never going to make the most out of it.

The reason that security bit is so important is because it allows you to get away from that old model of having to punt everything back to one place to secure it and then break it out. You don’t just need perimeter network security, but security throughout everything that your organisation touches. And that’s what allows you to have high-performance internet circuits at sites, or for home workers, that just access the applications that they need directly.

SD-WAN comes with additional network- performance features, such as being able to route traffic over different circuits depending on what you want the priority to be. You know what traffic type you want to have priority over others. Email could go out over 4G or a regular broadband connection, for example, but a voice or video call that needs a set amount of bandwidth, both upload and download, you might want to put that on a higher performance circuit. SD-WAN can make those real-time decisions based on the logic that you put into the network design in the first place, to make sure that you’re always using the best available bandwidth from the best available circuit.

What are the benefits of working with a partner such as us when it comes to implementing SASE in your organisation? Why not do it yourself? There are a few reasons, but it comes back to the time and management cost. There is still a lot of time and effort that you need to spend as a network manager, with software updates and security patches coming out all the time. The number of threats to a corporate network has exploded in recent years and will continue to exponentially increase. Frankly, just keeping up with everything, and making sure that when it happens that you’re actually doing something with it, is becoming incredibly difficult. That’s a full-time job for quite a few people for most decent-sized organisations.

How would you typically manage a SASE implementation for a client?

“When we work with a customer, we engage with them in a consultancy pre-sale phase to understand their requirements. As part of that we would then recommend the best-fit design using the breadth of our portfolio.

We would then also deliver that infrastructure for them, both in terms of the configuration of the network in the cloud, but also the physical, going to site – we go and do the site audits, we do the wireless coverage surveys, we do the cabling and install the network hardware as well.

And then, once the installation period is done, we take it on to the service level, where we do all of the break/fix maintenance associated with that hardware. We can also do the associated managed service of both that network infrastructure as well as the security elements. That management layer can vary depending on how much the customer wants to do themselves.

So, it’s an all-encompassing service that is very thorough and covers everything that a customer would expect from a managed service in this particular product set.”

WAVENET.CO.UK

0333 863 3000

Wavenet Limited
One Central Boulevard
Blythe Valley Park
Solihull, West Midlands
B90 8BG

enquiries@wavenet.co.uk

Cloud & Modern Workplace

Mobile & IoT

Contact Centre

Intelligent Connectivity

Unified Comms & Voice

CyberGuard

Business Continuity

wavenet

cisco Partner