macquarie
TELECOM

Introducing SASE. Security meets the power of AI.

Macquarie Telecom SASE

Pressed for time?
To discover how SASE will make a real difference to your business in less than two minutes, follow the page numbers in the stopwatch icon.

Dying for detail?
To delve into tech that makes SASE the easiest way to keep your network safe wherever your people work, go to the page numbers in the magnifying glass icon.

Contents

Why settle for half a product?

When it comes to choosing a network technology partner, we reckon some traditional suppliers are selling half a product. Even if the technology's adequate, customer service and project management fall short.

We're proud of how we do things differently. Our customer service team is right here in Australia, and our project managers and engineers sit right alongside them, so you're never left fending for yourself.

Of course, there's more to Macquarie Telecom than exceptional service. We challenge the traditional way companies approach networks and security. We introduced SD-WAN to Australia back in 2017 and today, with over 7,000 sites rolled out, our expertise leads the Asia Pacific region.

Now, we're introducing a first-of-its-kind AI-driven SASE solution. It's designed to provide bulletproof, up-to-date protection across your entire environment, no matter where your people work, without compromising their user experience.

Five ways your business will benefit from SASE.

x5

Security

SASE protects your network and users, whether they're in-office or remote, and its cloud-based platform keeps your protection up to date the moment a threat is detected.

3

User experience

Fast, safe access to your business applications with low latency, supported by zero-downtime updates and infinite scalability.

5

Control

Granular control of how apps are used wherever your people do business, through a powerful drag-and-drop interface, reducing the risk presented by shadow IT.

6

Simplicity

Fast problem detection and resolution using AI, paired with efficient network and security deployment, all managed from a single pane of glass.

7

Service

Whether you're onboarding your whole network or trying to solve a simple challenge, you'll be talking to real people based right here in Australia.

8

9

Security

Security breach in session

Security doesn't just belong in the office.

Traditional security is typically appliance-based, living in head offices or data centres. That's made it easy to keep the office environment safe from data breaches and hacks, but has left remote users vulnerable to attacks that can affect the entire corporate network. Macquarie Telecom SASE makes it easy to secure your whole network consistently. It's simple to define policies directly in the dashboard, and then push them out immediately to every device across your network.

Everything controlled from one place.

One of the big challenges for traditional networks has always been keeping security policies up to date across multiple platforms. For example, WAN may have been managed on-site, firewalls through their own interface, and remote SSL policies across a whole fleet of individual devices. It's a disparate approach with no integration.

Doing this is time consuming for your IT team, but perhaps more importantly, it's inherently risky. Because everything needs to be kept up to date independently, inconsistencies can occur across your devices, and it can take weeks or months to update everything across the board. And there's the ongoing need to keep your users and IT teams up to date across each platform, too.

When you bring your security into the Macquarie SASE environment, you can stop worrying about keeping individual platforms and devices synchronised. Instead, every aspect of your network is controlled through a single interface, with just one platform to keep your teams up to speed on.

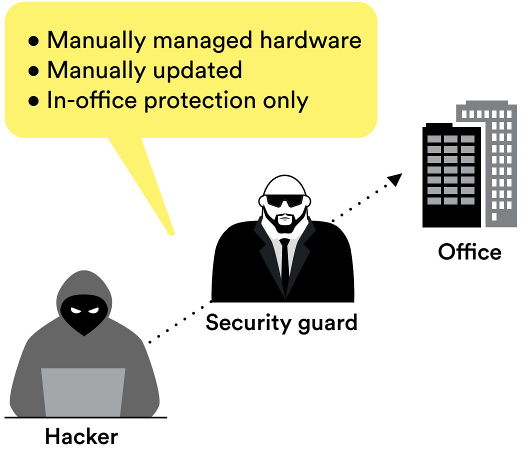
Your whole network, always up to date.

Every day, new security threats emerge globally. Keeping up to date with the latest patches, and rolling them out to every device across your business, is time consuming when urgency is critical. In fact, slow patch rollouts are one of the reasons so many companies fall victim to security breaches.

When you move to SASE, everything's handled in the cloud. And that means speed and scalability with near-zero downtime. With SASE, policies across your entire stack are updated the moment a zero-day threat is identified. Every device, every appliance, is protected from the moment the patch is pushed out. For your IT team, it's the end of laborious manual updates for each piece of hardware at each site, every time a new security threat needs to be plugged. For your business, it means strong, timely defence against attacks that could compromise your data.

When it comes to your security, a partial strategy doesn't cut it.

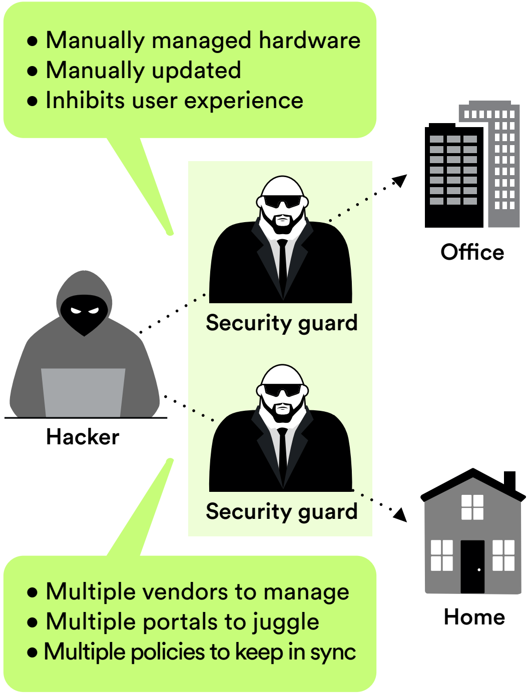
Traditional security



- Manually managed hardware
- Manually updated
- In-office protection only

Traditional security involved a "security guard" (physical firewalls) located on company premises. This provided some protection to devices being used in company buildings, but when people worked at home, their computers and phones were unprotected. And every time an update patch was rolled out, a planned outage was required, impacting productivity.

Reactive strategy

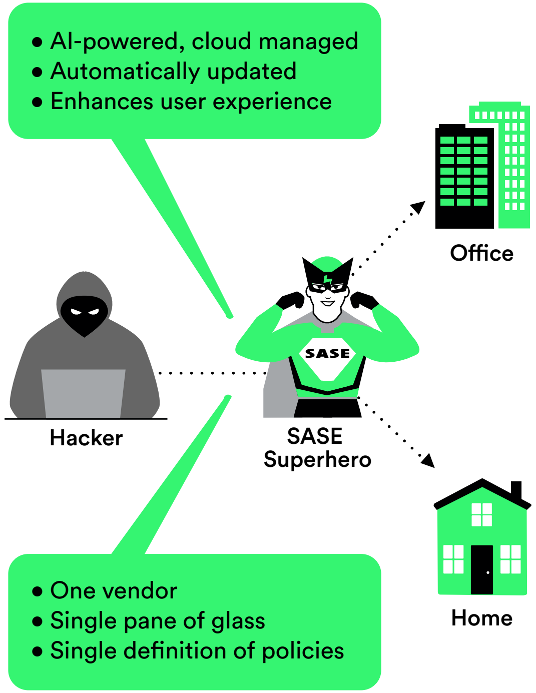


- Manually managed hardware
- Manually updated
- Inhibits user experience

- Multiple vendors to manage
- Multiple portals to juggle
- Multiple policies to keep in sync

When COVID began, we saw a sudden shift to remote working and a wider use of cloud. Companies rolled out a new security guard for remote protection. The problem was, this guard didn't talk to the on-premise guards - which meant manually updating polices, difficulty troubleshooting, and managing different vendors. For the remote user experience, it meant choosing either speed or security, but not both.

Macquarie Telecom SASE



- AI-powered, cloud managed
- Automatically updated
- Enhances user experience

- One vendor
- Single pane of glass
- Single definition of policies

SASE brings the on-premise and remote security guards together, as a SASE Superhero. This means protection for offices and remote workers that's always in sync, controlled by a single pane of glass. Wherever people work, their user experience is the same, and no matter where apps are hosted, everything is fast and secure.

User Experience

Traditional security slows everything down.

Until recently, keeping your remote working environment safe meant compromising on performance.

Appliance-based solutions had to process data packets at your head office or data centre, before sending them on to their destination. Like any detour, this meant everything took longer. And for the end user, it meant the remote work experience didn’t compare favourably with working on the office network.

Smooth performance, wherever you're working.

SASE takes away the long, winding road your data used to take in the name of security.

Instead of hairpinning through physical firewall appliances, all security functionality is processed in the cloud, inline between the user and where their traffic's heading. This means everything travels fast, so there’s minimal latency for remote applications.

Whether you’re running a Zoom call or accessing the company’s central database, the experience is smooth and speedy. And that means your people are less likely to try to bypass your security in their quest for acceptable performance.

Non-cloud applications are protected too.

Of course, it’s not just cloud-based applications that need to perform seamlessly for remote workers.

SASE delivers equally slick performance for any applications you still run in your head office, data centre or hybrid cloud environment. Using multiple SASE POPs and processing locations scattered geographically means there’s no need for hairpinning through a centralised VPN appliance.

Updates don’t need to bring work to a standstill.

With traditional security protection models, a planned outage is required every time an update patch is rolled out. This of course means that productivity across your business takes a hit whenever it's time for a routine security update.

Being cloud-based, SASE works in the background, so there’s no need to bring systems down every time protection is enhanced. Instead, patches are pushed out as soon as they're ready, with no need to hold them back to avoid downtime.

Control over personal apps in a business environment.

These days, people want to use their personal apps on their business devices. Typically, this has inherent risks. Without protection, people can easily transfer confidential business data onto their own cloud-based storage platforms – either intentionally or by mistake.

Of course, you could simply block your people from using any non-business apps. But expectations have moved on, and people want to have some level of access to their own content when they're at work.

SASE changes all of this by making it easy to control app access in a granular way.

Bring shadow IT out from the shadows.

Through our CASB tool, you'll have visibility over shadow IT – applications that aren't approved or deployed by your business, but which end users have chosen to adopt. This means even more control over what can and can't be used in your company environment.

Setting up rules should be drag-and-drop, not a drag.

In our portal, it's easy and quick to build access rules for people or groups.

For example, by setting up a blacklist, you could prevent everyone in your business from posting videos to YouTube, but still give them access to view content. Or you could decide to let people post updates on LinkedIn, but not allow video uploads. And when it comes to cloud storage apps like Dropbox or Google Drive, you can decide that uploading files is allowed, but lock down the option of sharing those files with other people.

The depth of control on offer is amazing. And you don't need to be an expert to set things up exactly as you want them and deploy them at scale. Revolving round a clear GUI, there's minimal training needed, but zero compromise to the depth of control you have over your network.

Control that extends beyond the office walls.

Traditional systems let you choose which apps people use when they're connected to the office network. But once they're working further away, having nuanced control over what they can and can't access has historically been impossible.

SASE's tools give you the same level of control over how your people access their apps – whether they're in the office, or miles away on their own network.

Control

Simplicity

SASE reduces the drain on your resources, whichever way you look at it.

Security doesn't need to be a minefield.

Traditionally, keeping your network secure has been complicated and resource draining. It's usually involved working with multiple vendors, each with their own portal, all mashed together to fulfil different functions of your security strategy.

That's made it a complex environment to deploy, manage, update and fund. SASE brings all your security functions together, and that means significant, measurable benefits for your business.

A single interface makes everything faster.

When you're deploying all your security functionality and remote access through a single interface, everything's easier. First, you'll need less people, and they'll need less time. And second, there's no risk of hitting the roadblocks that often crop up when blending multiple solutions together.

Speedy resolution, less downtime.

When a user on your integrated SASE network hits a bump in the road, resolving their problem is almost always easier and faster.

SASE's intelligent tools make it quick and simple to find the root cause of a problem. And for the user who's experiencing trouble, it drastically reduces downtime.

A measurable difference to your bottom line.

Choosing SASE, the all-in-one solution, inevitably means lower cost to your business. We've packaged everything together so you're not forced to negotiate with multiple vendors for each service. And of course your CAPEX budget can rest easy, with no need to keep your hardware equipment maintained or invest in new devices as your company grows.

With SASE's analytics, you can use quantitative data reflecting things like comparative site performance to make decisions about future IT investment across your sites.

Instead of deploying the same policies multiple times across an array of platforms, an integrated SASE framework means you're only doing it once. And that delivers a measurable reduction in time and cost. The result? Your IT people can give their time to more important activities within your business.

Scalability without the CAPEX investment.

Traditional networks are limited by a fixed number of tunnels, determined by how many hardware devices are running at each site. When a business grows, it has to invest in more hardware and then configure it. The upfront and ongoing costs are high and despite this, protection can be inadequate if the devices aren't kept up to date with the latest patches.

SASE is different. It delivers infinite scalability, which is a must in a security landscape that's constantly evolving. It means you're not only ready for today's threats, but protection is on standby for every new threat that's on the horizon.

From onboarding to management, our service is unmatched.

Service

There's nothing like a real human.

If you're familiar with any old-school telco, you'll know that real service is often replaced by self-service chatbots. We believe that when businesses need help from their telco, they need a real human.

Unmatched experience in secure network rollouts.

Since we launched SD-WAN in Australia in 2017, we've deployed over 7,000 new sites across Australia. In the process, we've migrated over 600 legacy networks over to SD-WAN. When you're moving to the SASE platform, you can expect seamless integration between SASE and SD-WAN.

Project management that's always on the front foot.

At Macquarie, we use tightly integrated systems and thorough automation to provide a managed service that's always on the front foot. This leaves your IT people to focus on more important things like modernising applications or internal projects centred around a better end user experience.

An on-shore team that works together.

In the Macquarie Telecom Hub, our customer service team, and solution architects work together – shoulder-to-shoulder in our Sydney office. They work alongside our certified delivery engineers and domain architects to deploy and manage networks and security services. It's a very different approach to the traditional telcos.

We don’t do SASE by halves.

>42%

Security is in our blood.
Over 42% of Australian Federal
Government data is kept safe
by Macquarie Telecom.

95% of calls are answered in less than one minute, by our call centre right here in Australia.

<1min

19

12

Other telcos have guesswork. We have Kate.

People learn best from people.

We believe that providing incredible online tools to manage your SASE environment is only half the story. Giving you real life training is the other half.

That's why we offer face to face training to anyone in your business, whenever they need it.

Training that puts you ahead from day one.

When you migrate your security platform to Macquarie Telecom SASE, we'll run training sessions to make sure you're ready to fly solo with our network management tools

And if you've chosen us for SASE and SD-WAN together, we'll provide even more specialised training on monitoring, problem diagnosis and trend reporting, along with guidance on using your SD-WAN hardware.

A helping hand, on demand.

We know that the need for training doesn't end once you're on board with us. That's why dedicated training is on hand whenever you need it. Whether you have new starters, existing staff who need to be upskilled, or just need refresher training, Kate and her team will be delighted to help you.

Cloud Web Security.
Protection everywhere.

Real protection that follows you everywhere.

Cloud Web Security takes the security functions of traditional networks and places them in the cloud. But it's far more than a cloud-based replica of traditional security systems.

Recently, two fundamental changes have affected how people do their work. First, we're working in places other than the office more than ever before. And second, the nature and frequency of security breaches have escalated dramatically. Workers no longer sit in the safe, secure environment of an office, where traditional hardware can protect their data.

We've built Cloud Web Security to make it safe for people to work wherever they need to, with powerful, simple to use protection against the barrage of threats facing your company's confidential data.

Protection for people, not devices.

Cloud Web Security is a cloud-based service that gives you granular control over the access and protection profile for every person in your business. Unlike traditional systems, it works at a user level – with protection for up to five devices per user.

Previously, security was controlled at a device level, making it much more time consuming to deploy and update security policies. Back then, if a user replaced their laptop (for example), that new laptop would need to have its own security configuration set up manually on the device.

The move to cloud means that the user's security profile can be pushed down to their new laptop the moment they log on.

Rules that are easy to set. And easy to see.

Our interface is all about simplicity. In our portal, it's easy to set up rules for roles, teams or individuals, by dragging and dropping applications and criteria into black and white lists.

For example, you could limit access to a category of websites across the whole business, or set up a rule for a specific team preventing them from posting video onto a social media platform.

Keeping attackers out and your confidential data in.

Cloud Web Security is always watching the internet traffic right across your network, both in-office and remote. Put simply, it has two jobs: keeping attackers out, and keeping your confidential data in.

So how does CWS keep attackers out? It's simple. With URL filtering, you can block or limit access to any website categories that don't align with your company's internet policy. And content filtering gives you always-on protection against known malicious websites.

When it comes to keeping your critical company data private, data loss prevention (DLP) keeps a close watch for signs of accidental or intentional sharing of data. It does this by defining acceptable user behaviour, and then looking for anything that seems out of the ordinary.

Ready for business as usual. And business as not usual.

Here's a simple example of CWS in an office environment. A user might access Microsoft OneDrive periodically throughout the day, in line with the business' definition of typical behaviour. CWS will take note of this pattern, see that it's business as usual, and allow it.

But let's say the CWS engine notices a user who's uploading large blocks of data into Google Drive (a non-business application). As soon as this atypical behaviour is identified, the system allows your IT administrators to choose how to react to the situation – either by blocking the action immediately or raising a data exposure alarm.

Your users don't always know what's safe. Enter the Content Inspection Engine.

Your business network is only as safe as your users' judgement allows. From time to time, you might find that someone in your business lands on a website containing malicious files, or downloads files unintentionally that are malicious in nature.

That's where our Content Inspection Engine's sandboxing feature comes in. If a file fails a set of standard security checks, it's placed in a separate environment for sandbox inspection. There, it's analysed for malware, and only released to the user if it gets the all-clear.

It's a final layer of security that provides bullet-proof protection against all known and zero-day threats. And at a time when data breaches are on the rise, it's a critical defence layer for every business.

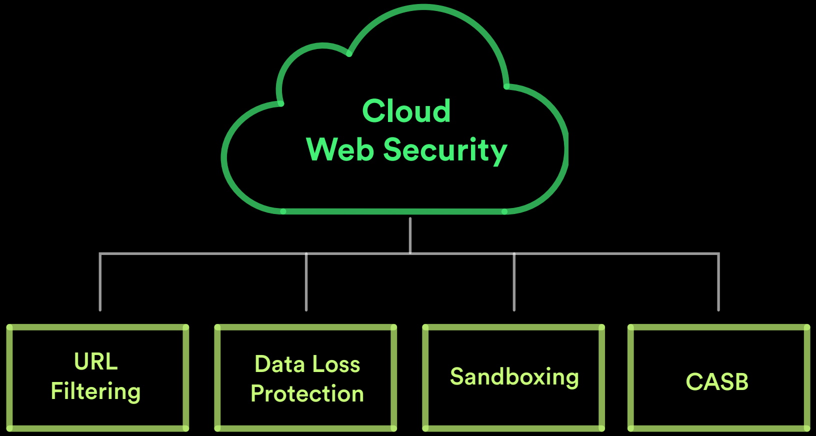
Security patches on time, every time.

These days, network threats emerge fast, and failure to patch them promptly can be catastrophic for your business. In fact, in 2022, the majority of significant incidents responded to by the Australian Cyber Security Centre (ACSC) were due to inadequate patching.

In traditional networks, security patches had to be installed on each appliance (whether it was physical or virtual) to protect against newly-identified threats. Labour intensive? Definitely. Slow? For sure.

Cloud Web Security turns threat patching on its head. As soon as a new threat is discovered globally, we push out a patch to respond to it, within 15 minutes. That means you'll always be confident that the latest patches are live at every site and device in your network, providing up-to-date protection with no negative impact on productivity.

In 2022, the majority of significant incidents responded to by the Australian Cyber Security Centre (ACSC) were due to inadequate patching.



Edge Network Intelligence. The AI-driven security watchdog for your business.

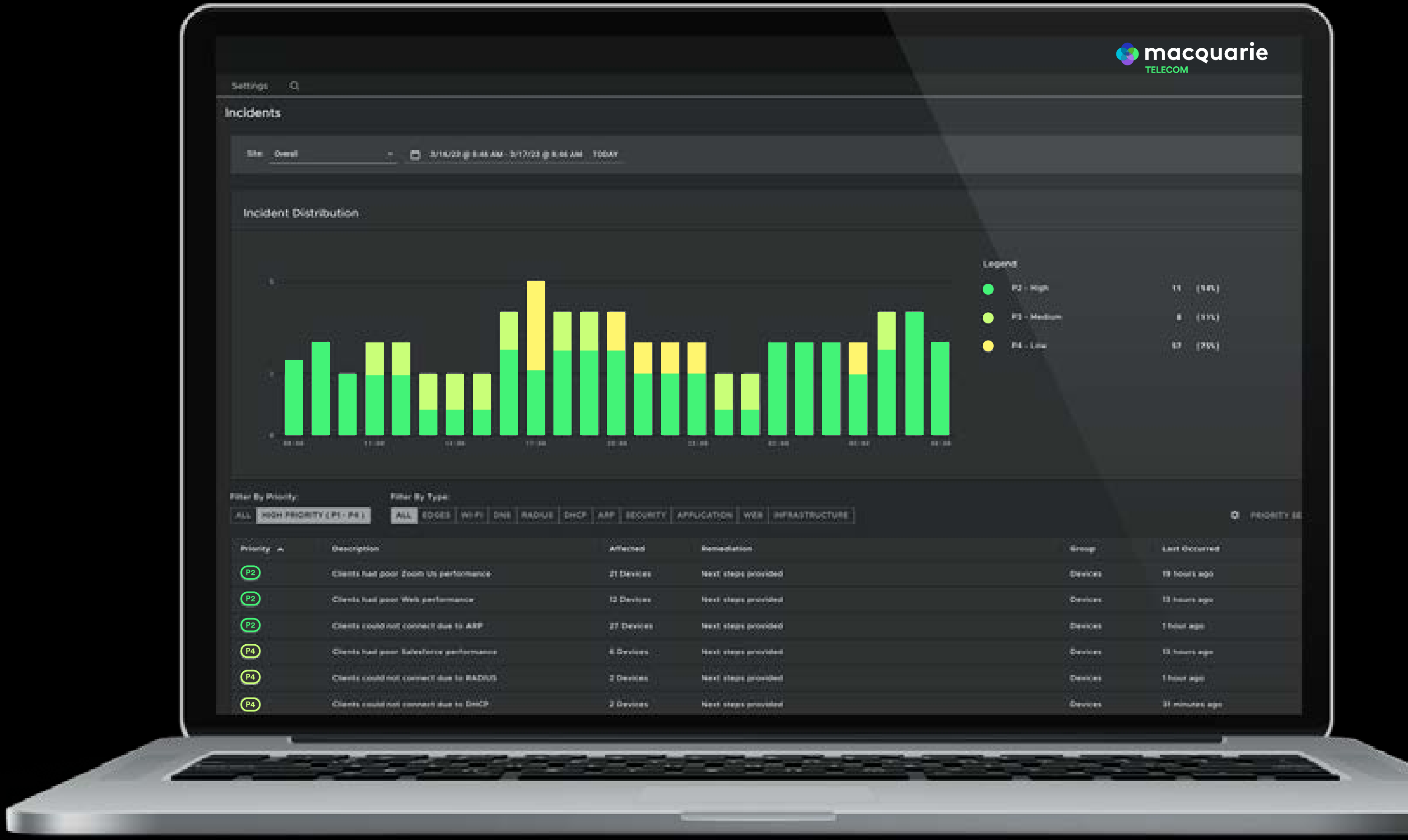
Edge Network Intelligence is an AI-driven system that watches over your entire network, from SD-WAN devices to access points, switches and other IoT equipment you're running.

Whether your workforce is office-based, remote, or a mix of both, ENI keeps an eye out for problems, risks and unexpected behaviours from one end of the network to the other. And being vendor-agnostic, it can work with devices from almost anywhere.

ENI gets to know you, then it gets to work.

Our Edge Network Intelligence platform is incredibly capable at picking up off-trend behaviours within your network. But before it can do that, it has to get to know your whole environment inside out.

After initial deployment, ENI builds a deep profile of what's normal on your network. For example, it'll look at things like how much traffic is going in and out of each site and analyse what type of traffic it is. It's granular enough to get right down to a specific printer, camera or other IoT device sitting in your environment. And once it's built this profile, it's permanently on guard.



Priority	Description	Affected	Remediation	Group	Last Occurred
P2	Clients had poor Zoom Us performance	21 Devices	Next steps provided	Devices	19 hours ago
P2	Clients had poor Web performance	12 Devices	Next steps provided	Devices	13 hours ago
P2	Clients could not connect due to ARP	27 Devices	Next steps provided	Devices	1 hour ago
P4	Clients had poor Salesforce performance	6 Devices	Next steps provided	Devices	13 hours ago
P4	Clients could not connect due to RADIUS	2 Devices	Next steps provided	Devices	1 hour ago
P4	Clients could not connect due to DHCP	2 Devices	Next steps provided	Devices	31 minutes ago

Catch problems before they become... problems.

Identifying issues on your network when they've already impacted your people means lost productivity.

Edge Network Intelligence is always on, ready to detect faults and immediately isolate a problem until you respond to the notification. It has visibility into each user's wireless and wired state, putting your IT team on the front foot with a proactive approach to network management. This means that you can easily sift out noisy complainers from a group of people genuinely experiencing a performance issue.

On a single screen, you can see all your networks, each with a summary performance ranking. If any of them is performing sub-optimally, you can click to drill down for a root cause analysis. When someone complains about a performance issue, actionable data is already available. And that means the time to resolve the problem is significantly reduced.

ENI analyses trends and draws conclusions.

When a group of people are experiencing a problem, ENI immediately pulls together a number of data feeds to profile the situation on a simple summary screen.

Let's say some of your people are having problems accessing your billing system. You'll quickly be able to see key metrics like the percentage of users affected, the number of people that equates to, and a summary of the symptoms they're experiencing.

ENI then provides a clear summary of the potential root cause of the problem, and recommended steps to solve it.

All eyes on everything, all the time.

ENI recognises and creates a baseline of standard performance for all your IoT device. From there, it can provide intelligent warnings about any digital activity that could represent a hacking threat.

For example, let's say your business uses security cameras across all sites. These cameras may not be "smart" devices – they're just camera hardware relaying images to the cloud or signalling to a centralised server. But ENI can intelligently analyse their data, so if one of the cameras suddenly begins sending traffic to an untrusted overseas destination, you can examine this behaviour and remove the device from your network if it's compromising your security.

Macquarie Secure Access.
Cloud or local, your data's safe.

Non-cloud files shouldn't be compromised.

When you choose Macquarie Telecom SASE, you're entering a world where apps and security both benefit from living in the cloud. But there are situations where companies still need to run critical apps from within their own data centres. And we believe that stringent levels of protection should be available to those apps too.

That's why we offer Macquarie Telecom Secure Access. It's an easy way to make sure all your apps – whether they're cloud-based or local – are protected the same way. Remote users can log in from wherever they're working, and their access to the corporate network will be seamless.

Our Orchestrator portal provides centralised enterprise-wide installation and configuration of new SD-WAN sites, with your chosen policies and settings, and offers single-click provisioning of virtual services at the branch, in the cloud, or within your enterprise data centre.

Streamlined management.

Managing Macquarie Telecom Secure Access is all done through the cloud. It's a hosted service, which means there's no need to install and manage remote access concentrators. And as your organisation grows, you won't have to continually scale those concentrators or buy additional internet bandwidth to send VPN traffic through your data centre and back to the SaaS environment.

Speed and simplicity for your users.

No matter where your people work, they'll experience fast and consistent performance with low latency and high resilience. This is because SASE doesn't need to send their data through a VPN concentrator hosted in a distant data centre. For your remote workers, this means a speedy experience that's just like working in the office.

The right access for the right people. And nothing more.

Let's say you have a gardener coming to mow the lawn. You'd want to give them a key to the front gate, but not open the front door to the house. SASE takes the same approach to network access.

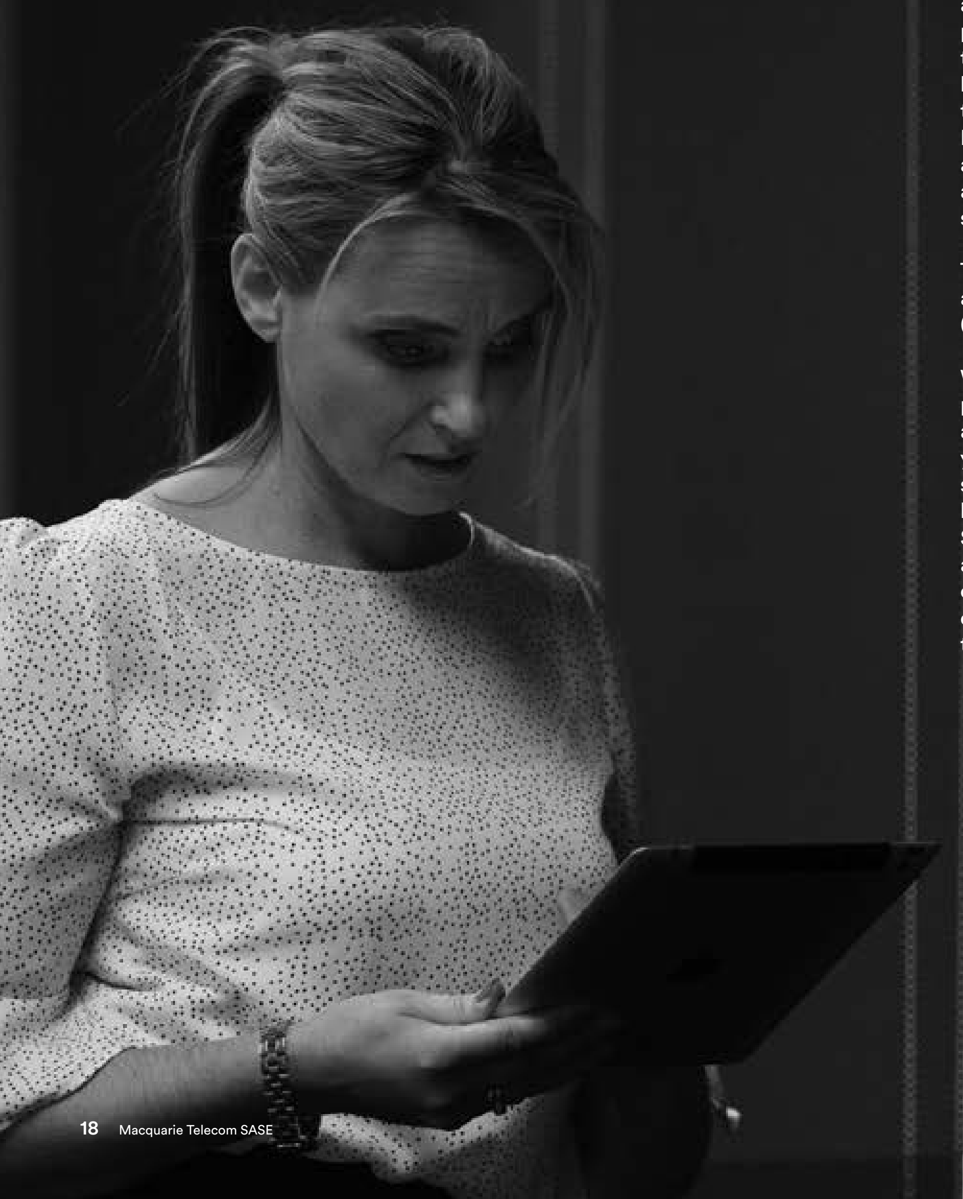
Unlike legacy VPN architectures that conduct one authentication and then give that user ongoing access to the whole network, SASE provides authenticated access only to the resources a specific user needs. We call it Micro-Segmented Access.

Let's take a contractor as an example. Working with your business for a short period of time, you can ensure they only have access to the resources that are critical to their role. How? The SD-WAN client creates a point-to-point connection between that contractor and the specific server they need to access, protecting the wider network from a potential data breach.

SD-WAN client and ENI.

The SD-WAN client on mobile, laptop, desktop, servers can integrate with ENI. So just like the insights ENI provides for your office-based users, you'll get alerts and insights when there's deviation from the normal user experience for remote workers, too.

The great CASB.
Insanely granular SaaS control.



People want choice. Businesses want control.

These days, people use their work devices for work applications, but often run personal applications too. A typical business user might have WhatsApp installed on their phone and use Google Drive on their laptop to access personal files. These applications can all put the safety of your data at risk.

That's where SASE's cloud access secure broker (or CASB) steps in.

Where traditional security policies respond to personal application use with a hard yes or no, CASB is all about supporting real-world usage but keeping everything secure. So instead of blocking personal applications altogether, you can offer your people the right level of access – without jeopardising the security of your business.

It starts with visibility.

So how does CASB set the scene for providing such a deep level of control in a modern environment of increased cloud consumption?

It starts by building a complete profile of all the SaaS applications being run by each user – whether they're business-supported or private. From there, it has a comprehesive picture of each person's app landscape, which it updates constantly.

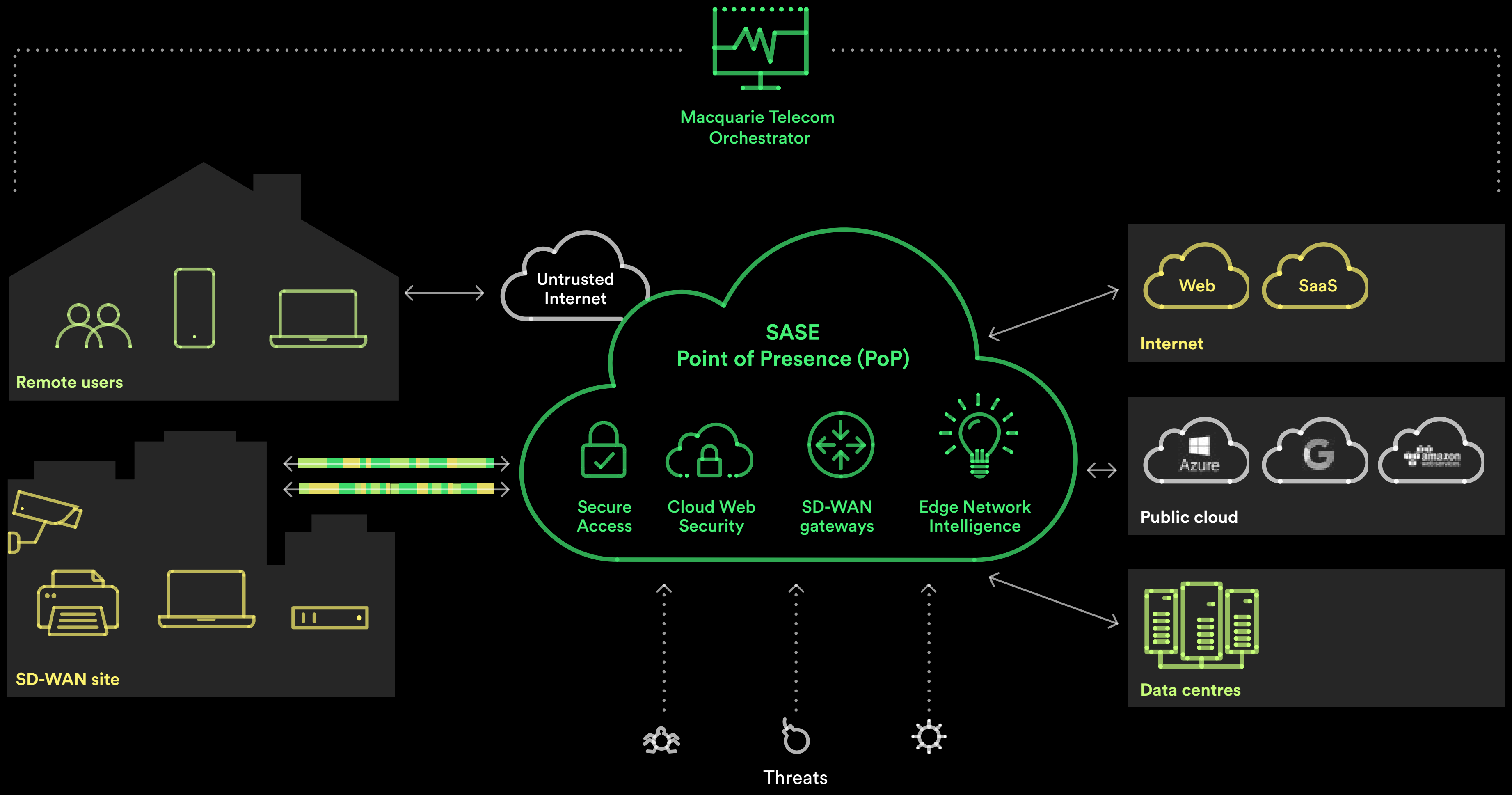
Control down to the last action.

Having built a profile of applications used by each user, CASB lets you make decisions about the features of each app that you'll allow access to. For example, you might decide that most users are permitted to access LinkedIn and may view and like content in their feed, but that they can't post images or video. But you may also decide that a specific team – for example PR and marketing – can have full access as it's an essential platform for their role. Or you might allow YouTube, but only allow people to consume content.

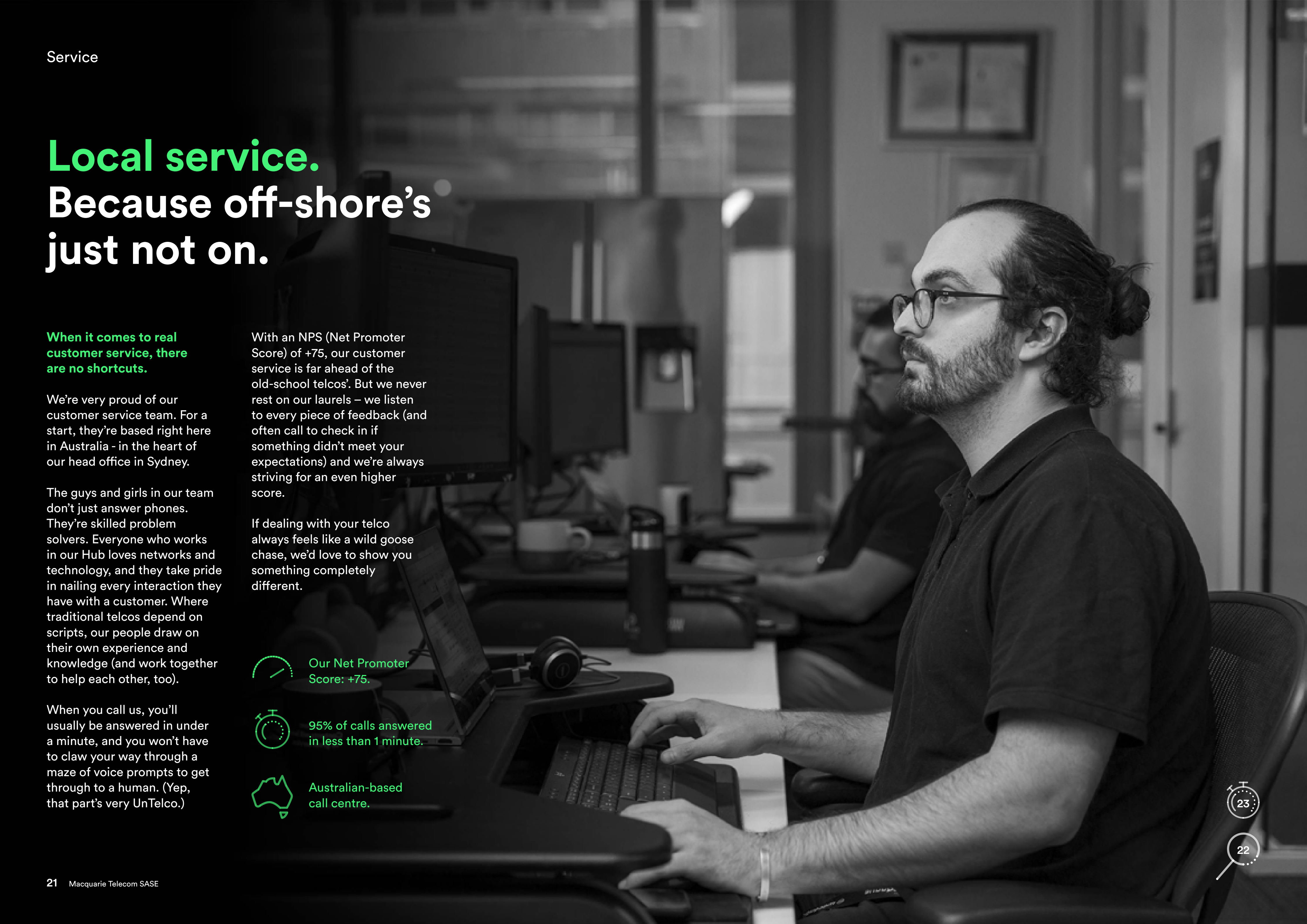
Leaked confidential files, either by intention or in error, are an ongoing risk in every company's security landscape. CASB gives you precise control over the way files and data are handled within applications. For example, you may allow people to install and use Google Drive, but lock down the ability to add files from their computer to Drive. Or you could choose to allow file uploads, but block files from being shared to anyone aside the user themselves.

With CASB, cyber security challenges arising from shadow IT are tackled head-on, without impeding productivity or employee satisfaction.

The anatomy of Macquarie Telecom SASE.



Dealing with your telco shouldn’t feel like a wild goose chase.



Local service. Because off-shore's just not on.

When it comes to real customer service, there are no shortcuts.

We're very proud of our customer service team. For a start, they're based right here in Australia - in the heart of our head office in Sydney.

The guys and girls in our team don't just answer phones. They're skilled problem solvers. Everyone who works in our Hub loves networks and technology, and they take pride in nailing every interaction they have with a customer. Where traditional telcos depend on scripts, our people draw on their own experience and knowledge (and work together to help each other, too).

When you call us, you'll usually be answered in under a minute, and you won't have to claw your way through a maze of voice prompts to get through to a human. (Yep, that part's very UnTelco.)

With an NPS (Net Promoter Score) of +75, our customer service is far ahead of the old-school telcos'. But we never rest on our laurels – we listen to every piece of feedback (and often call to check in if something didn't meet your expectations) and we're always striving for an even higher score.

If dealing with your telco always feels like a wild goose chase, we'd love to show you something completely different.

Our Net Promoter Score: +75.

95% of calls answered in less than 1 minute.

Australian-based call centre.

23

22

We’re all in this (office) together.

Old-school telcos like to shuffle you from A to B. (And then to C, D, and E.)

Traditional telcos often prefer to minimise their customer service investment by outsourcing and offshoring their call centres. This makes things hard for their customers, because different functions are often in completely different locations.

When you’re calling an old-school telco for help, it’s not uncommon (when you finally get through to a human) to be told that your problem will be sent to someone else to solve.

That might mean a ticket is put in a lengthy queue for an engineer elsewhere to read. Or it might mean an email is sent for someone else to call you back… eventually.

More often than not, it’ll be a week or more before you hear back from someone and – with a bit of luck – get your problem sorted out.

All our people work alongside each other, to solve your problems fast.

Here at Macquarie Telecom, you’ll find our customer service people working right beside our network operation centre (NOC) engineers and solution architects.

You’ll also find our certified delivery engineers and domain architects working in the same office as customer service.

What does this mean? When you call us, the person who answers the phone will use their expertise to help solve your problem. But if they need the knowledge or experience of an engineer, they can walk over and solve your problem together.

That means your problem will be solved fast and the right way, the first time. When your critical SASE and SD-WAN networks depend on it, that’s a big deal for your business.

Security isn’t just something we sell. It’s who we are.

We're trusted by the Australian Federal Government.

42% of the Australian Federal Government's data is housed in Macquarie Telecom's data centres.

Over the last fifteen years, we've built and extended our cybersecurity services specifically for Australia's Federal and State government agencies, and we're proud to be trusted with Australia's critical government data.

Our role in protecting Australia against cyber attacks sees us analyse over 7 billion security events annually. We've proactively hunted over 4,000 cyber security use cases, and our team of experts monitors and responds to attacks on Australian Government IT systems every day of the year.

We're proud to bring these credentials to every business we serve with our network, data centre, and cloud security services.

Macquarie Telecom and VMware. An innovative, recognised partnership.

Changing the rules for business networks.

Macquarie Telecom's partnership with VMware dates back to 2017, when we introduced SD-WAN to the Australian market together.

Since then, our partnership has delivered over 550 SD-WAN networks to businesses across Australia.

These days, VMware is recognised as an innovative leader in cloud-based networks. In just over half a decade, years, they've rolled out over 400,000 SD-WAN sites globally, and can also take credit for the world's largest deployment incorporating 18,000 sites collectively.

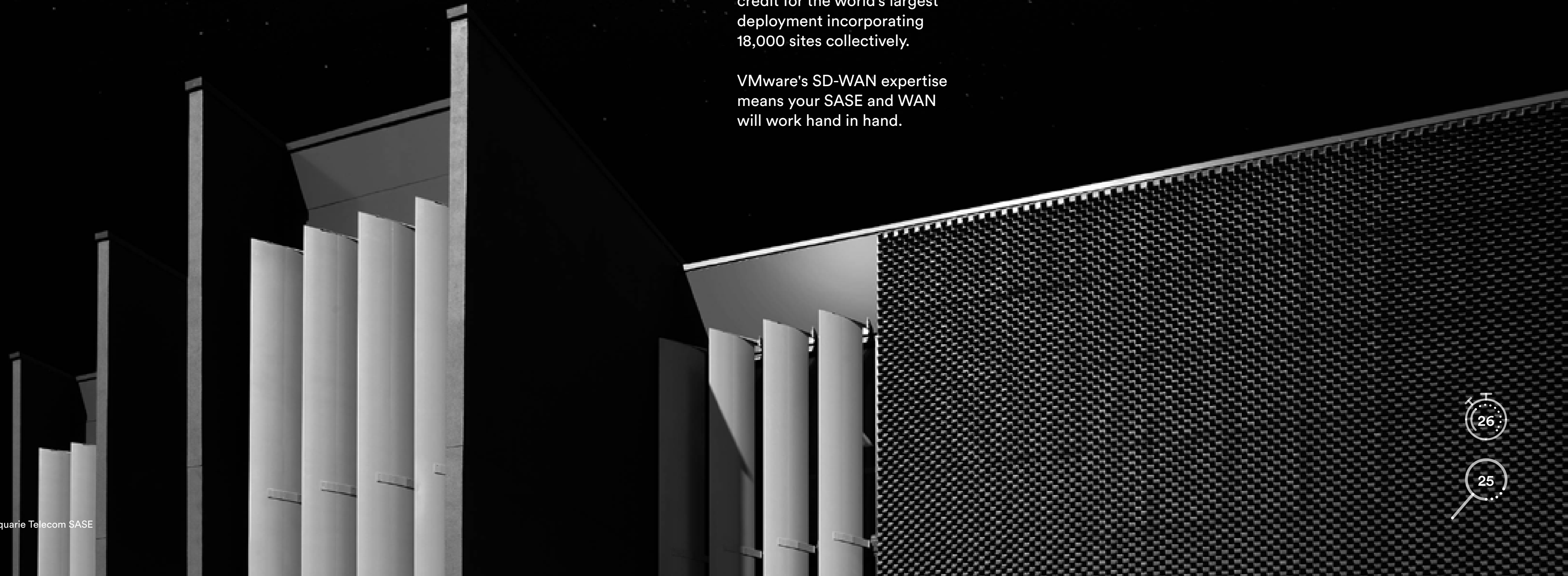
VMware's SD-WAN expertise means your SASE and WAN will work hand in hand.

Recognised as a leading VMware partner.

A year after we joined forces with VMware to launch SD-WAN in Australia, they awarded us their Partner Innovation Award for the Asia-Pacific region.

Winning this award not only acknowledged the leadership we showed in pioneering SD-WAN in the Australian market, but also the industry-leading customer experience we delivered to every business which chose to adopt this new technology.

Recognising not only our site rollout track record but also the proven performance and peerless customer experience delivered to every one of our SD-WAN customers, the award confirmed that VMware sees Macquarie as a critical partner in best-practice network rollouts.



With Macquarie Telecom, you'll always be ready for what's next.

From data centres to mobiles, Macquarie is always looking ahead.

When you join us, you can be confident that we're always innovating. We're not tied down to the traditional technologies that old-school providers continue to sell. And we're small enough to be ready to embrace new technologies early and provide them to you with exceptional execution.

Our services range from business networks through to office telephony, data centres and cloud. We bring all of these together, and provide #SoUnTelco service that's human, local, and always has your interests at heart.

macquarie
TELECOM

It’s time to talk to the UnTelco.

Give us a buzz on 1800 004 943.
Or learn more at macquarietelecom.com/SASE.

SASE v1.0.3