Halo Secure SD-WAN. Security, performance and value.

Macquarie Telecom Halo Secure SD-WAN

macquarie TELECOM

Security. Isn't. Optional.

In 2024, the way we think about networks and security looks nothing like it did even just a few years ago.

Applications live in data centres, the cloud, SaaS and the edge. Our apps and devices no longer sit inside the safe walls of an office. Traditional network and security architectures are no longer enough. Cloud consumption has increased, hybrid working setups are changing, and this means a wider attack surface for hackers. Your business needs to be ready.

We've built our Halo Secure SD-WAN Solution to do three things, simply and well. One: protect your network, users, and sensitive data. Two: help you control cost today, and in the long term. And three: deliver onshore customer service expertise that's not available anywhere else.

Most of all, we've used our experience with cybersecurity and networks to build secure packages that make it easy for you to choose and roll out a network that fits your business perfectly.

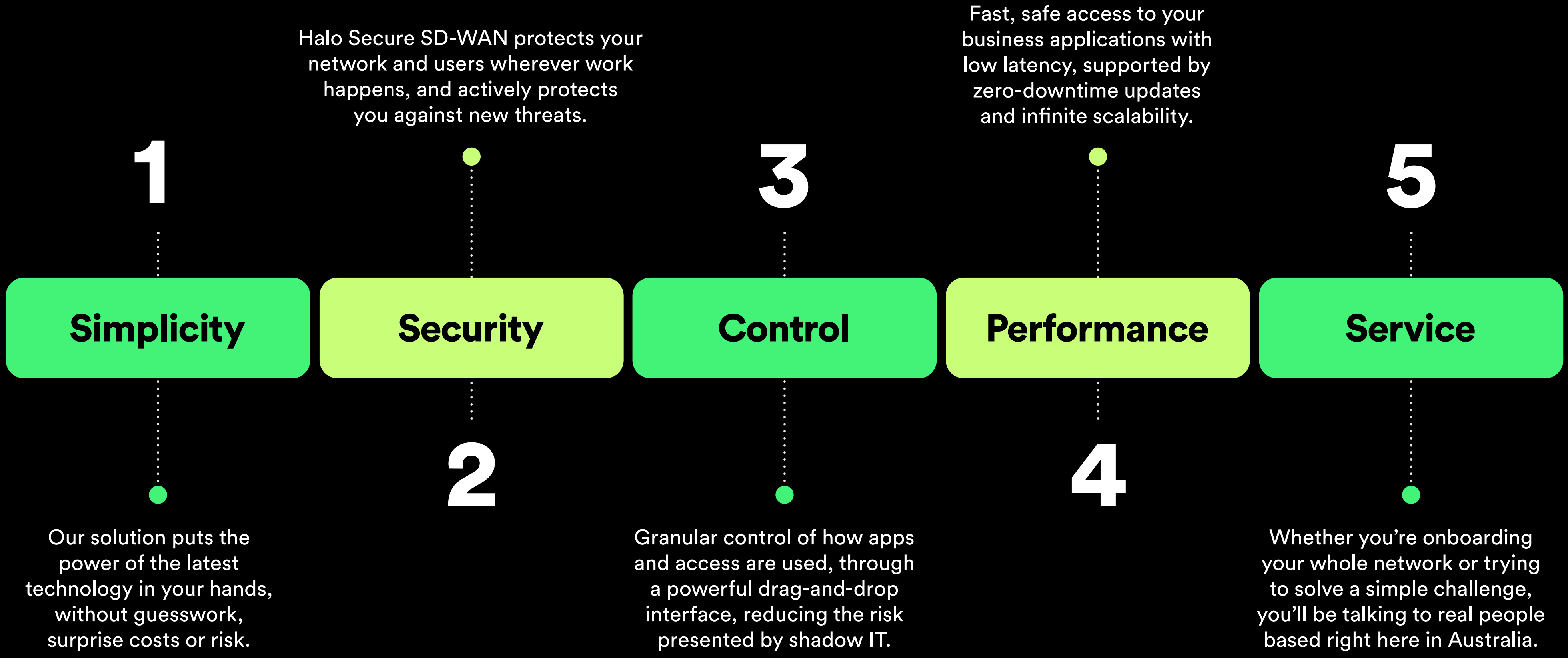
Introducing Halo Secure SD-WAN.

A fully managed network with cloud-powered security built-in.

24/7 access to an onshore team of network security experts.

Simple pricing that will save your business money.

Halo Secure SD-WAN is ready to change your business.



1

Simplicity

Our solution puts the power of the latest technology in your hands, without guesswork, surprise costs or risk.

2

Security

Halo Secure SD-WAN protects your network and users wherever work happens, and actively protects you against new threats.

3

Control

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

4

Performance

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

5

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.

Simplicity

The right features, put together by experts in networks and cybersecurity.

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 way of doing things, all mashed together to fulfil different functions of your security strategy.

That's made it a complex environment to deploy, manage and fund.

Halo Secure SD-WAN brings everything together, to give you a network that's easy to deploy and manage, always up to date, and supported by experts 24/7.

Future-proof technologies working together.

Halo Secure SD-WAN is built on the Secure Access Service Edge framework (known as SASE). It brings together our industry-leading secure SD-WAN and powerful site-based Cloud Web Security (or CWS) included as standard.

This suite delivers application performance that doesn't hold you back, and cloud-based security that will keep your data safe from cyber attacks.

And importantly, we've made everything simple. Our cybersecurity and network experts have built solution packs which match the right connectivity, SD-WAN and security features for your business.

Solution design from the experts.

Choosing the components of your network solution shouldn't be complex.

With Halo Secure SD-WAN, we've taken this unmatched experience and our engineers have created packages that are ready to deploy to make your network fast and safe. No compromises.

As you decide how to build your network, we'll work alongside you to help you make the right choices and design a Halo Secure SD-WAN that's the perfect fit for your business.

An intuitive interface makes everything faster.

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

Exceptional value, now and in the future.

Unmatched value: we've made pricing simple, too.

Halo Secure SD-WAN packages come with a single monthly price for your fully secured, protected network.

Instead of having to choose and pay individual vendors for connectivity, SD-WAN and network security, we include everything for a fixed price.

By choosing an expert you can trust, you won't spend time and resources choosing the right features and specifications for the specific demands of your business. We've worked with companies in a huge array of industries, so we understand what you need.

And we've made sure that features that should be standard are in fact standard, so you won't be caught out by sneaky options that push up your costs.

A hardware and software lifecycle that's all taken care of.

When your network is managed by us, you can say goodbye to the cost and administrative commitment of keeping hardware spares on-site. We'll do all that for you, and deliver them on demand according to your agreed SLA or SLG.

We'll take care of your firmware lifecycle too. Whenever there's an update, bug patch or vulnerability, we'll inform you and manage the appropriate rollout.

Scalability without the CAPEX investment.

Traditional networks are limited by a fixed number of tunnels, and determined by the type of hardware devices running at each site. When a business grows, it has to invest in new 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.

Halo Secure SD-WAN, underpinned by 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.

High availability and fast resolutions mean productivity for your business.

The Macquarie Telecom Halo Secure SD-WAN is designed around cloud-based security to deliver high availability, backed up by 4G failover. Of course, we can't claim zero downtime, but in practice our multi-path technology combined with jitter buffering and forward error correction deliver incredibly low downtime for your critical sites.

In fact, many of our customers have never had a site outage.

Because SD-WAN is fully managed, we'll be in touch as soon as there's a problem on your network. And we'll keep providing updates as we work through the problem, until it's resolved.

Security

It's 2024. 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.

Everything you need to stay secure… everywhere.

Halo Secure SD-WAN comes with all the tools you need to keep every site safe. Cloud firewall, intrusion detection and protection, anti-malware and content filtering all come standard. And we've built tools to make it easy to manage them, giving you simple and powerful visiblity of your network and your users.

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 user across your network.

It also draws on the power of the Global Intelligence Network, correlating data from 175 million endpoints, 80 million web proxies, 126 million attack sensors, 25,000 vulnerabilities and the expertise of over 500 in-house security experts, making your cyber defence fortress even stronger.

Policy control from a simple interface.

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.

Security that doesn't stretch your resources.

By integrating easily but comprehensively with a wide array of managed security offerings, we'll ensure that your network and users are protected from security threats – cutting down costly downtime, data loss and cyber attacks.

And network segmentation is built in, helping you contain the fallout in the event of a hacking incident. By limiting the attacker's movement and then containing the threat to a single segment, the impact of an attack is reduced and the recovery simplified.

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.

An extensive inventory of sanctioned and unsanctioned applications gives you 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 using this optional feature, 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. Using our 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.

Based on ZTNA principles, you'll also have secure access to Web, SaaS, data centres and the cloud.

If you have control over your network, everything just works better.

Halo Secure SD-WAN is built around making it easy to see what's going on in a way that makes immediate sense, so you can troubleshoot quickly and make data-driven decisions about the future.

Operational efficiency plus quick incident resolution.

We've built online tools to make it easy to see how your network's performing using clear dashboard graphics.

Green means good performance, amber is fair, and red means poor. Whether you're looking at the performance of a specific site, application, or aggregated data pipe, you can choose high-level or in-depth data to inform your operational decisions and reduce the time it takes to resolve incidents.

It's simple to run one-off or recurring reports to see the top applications and top talkers across your entire network, helping you make informed decisions or detect anomalies.

App-level prioritisation: the fastest bandwidth for your critical apps.

Now cloud consumption and SaaS have become the norm, traditional quality of service is no longer adequate.

Some applications on your network are going to be business-critical: think real time voice calls, video conferencing and realtime data. Others are much less important: general network updates, personal streaming, and periodic backups.

We've built our SD-WAN network to recognise over 3,500 applications automatically, making it easy to choose which applications get priority so the important ones aren't slowed down by anything that's non-critical. This means less headaches for your IT team, and a better experience for everyone using your network.

Fast, foolproof site rollouts and updates.

Our templates and one-touch deployment make it easy to roll out new SD-WAN sites or push updates out to existing ones. It's all completed with a few clicks, with no need for on-site technicians.

Future-ready: insights and scalability that set you up for tomorrow.

Halo Secure SD-WAN's detailed reporting at an app level doesn't just happen in real time. An array of reports across various time periods can provide you with granular data to help you make longer-term decisions about your network.

We've built our SD-WAN network with scalable architecture, so you can modernise and transform your application stack through secure internet access for SaaS applications.

Performance

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.

It's not only 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 points of presence (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 designs, a planned outage is required every time an update patch is rolled out. This means 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.

High on performance. Low on downtime.

An incredibly resilient network that takes care of itself.

When a traditional network slows down or has an outage, productivity can take a big hit. SD-WAN's multi-path technology doesn't leave all your data eggs in one basket.

Macquarie Telecom SD-WAN networks are built around more than one link .The system intelligently chooses which link to send every packet of data across by measuring the real time performance of each link hundreds of times per second. It then assembles the packets seamlessly at the other end.

What does this mean in practice? At any given second, your data is always travelling along the fastest path, delivering superior data speed and stability.

Clever tech that boosts performance.

SD-WAN provides maximum resilience when you use multiple links, but for sites with a single link, there's still plenty of technology at work to give you powerful performance.

Jitter buffering, negative acknowledgement and forward error correction all work together to mitigate problems at single-link sites. It happens automatically on-demand, for any application that can benefit from it.

The result? A seamless user experience, even if there's a temporary network issue.

Uptime, all the time. (Well, 99.99%).

SD-WAN uses its multi-path design to virtually eliminate network downtime.

By choosing two different network types and amalgamating them, there's always an instantaneous alternative route for your data to take if one network has an outage.

And the failover happens automatically, so the instant one network falls over, the other one picks up the whole load.

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.

From onboarding to management, our service is unmatched.

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 8,000 new sites across Australia. In the process, we've migrated over 600 legacy networks over to SD-WAN. When you choose Macqauarie Telecom Halo Secure SD-WAN, you can expect seamless integration between the SASE and SD-WAN technologies behdind it.

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 network and security experts 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.

Building your Halo Secure SD-WAN.

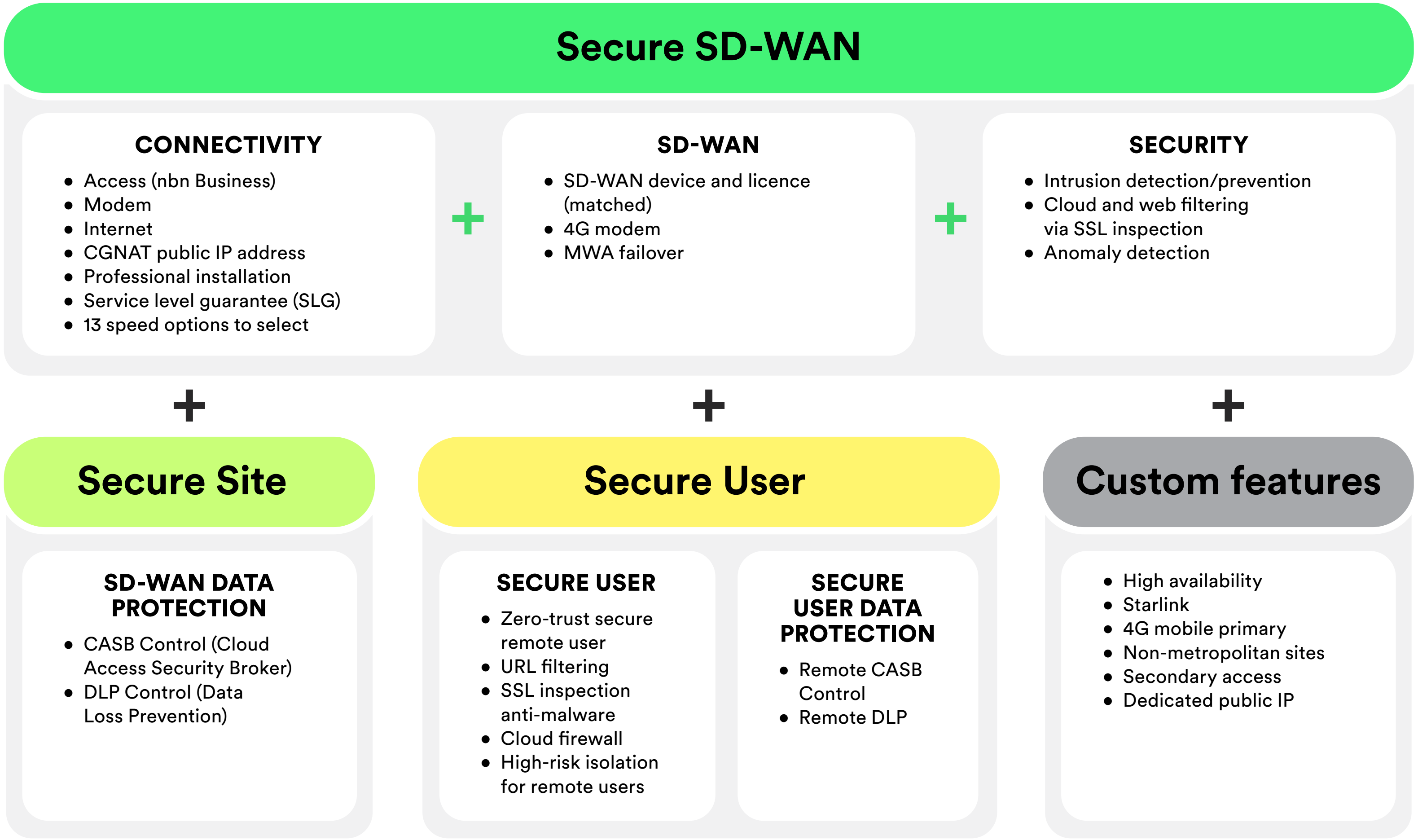
We've made it easy to build your Halo Secure SD-WAN. Choose Connectivity only, or add our Secure Site and Secure User packages for protection wherever your people do business.

1 Select a suitable access speed for each site

2 Choose a level of data protection for your network

3 Choose your level of protection for remote users

4 Add the custom features you need



Secure SD-WAN

CONNECTIVITY

- Access (nbn Business)
- Modem
- Internet
- CGNAT public IP address
- Professional installation
- Service level guarantee (SLG)
- 13 speed options to select

+

SD-WAN

- SD-WAN device and licence (matched)
- 4G modem
- MWA failover

+

SECURITY

- Intrusion detection/prevention
- Cloud and web filtering via SSL inspection
- Anomaly detection

+

Secure Site

SD-WAN DATA PROTECTION

- CASB Control (Cloud Access Security Broker)
- DLP Control (Data Loss Prevention)

+

Secure User

SECURE USER

- Zero-trust secure remote user
- URL filtering
- SSL inspection anti-malware
- Cloud firewall
- High-risk isolation for remote users

SECURE USER DATA PROTECTION

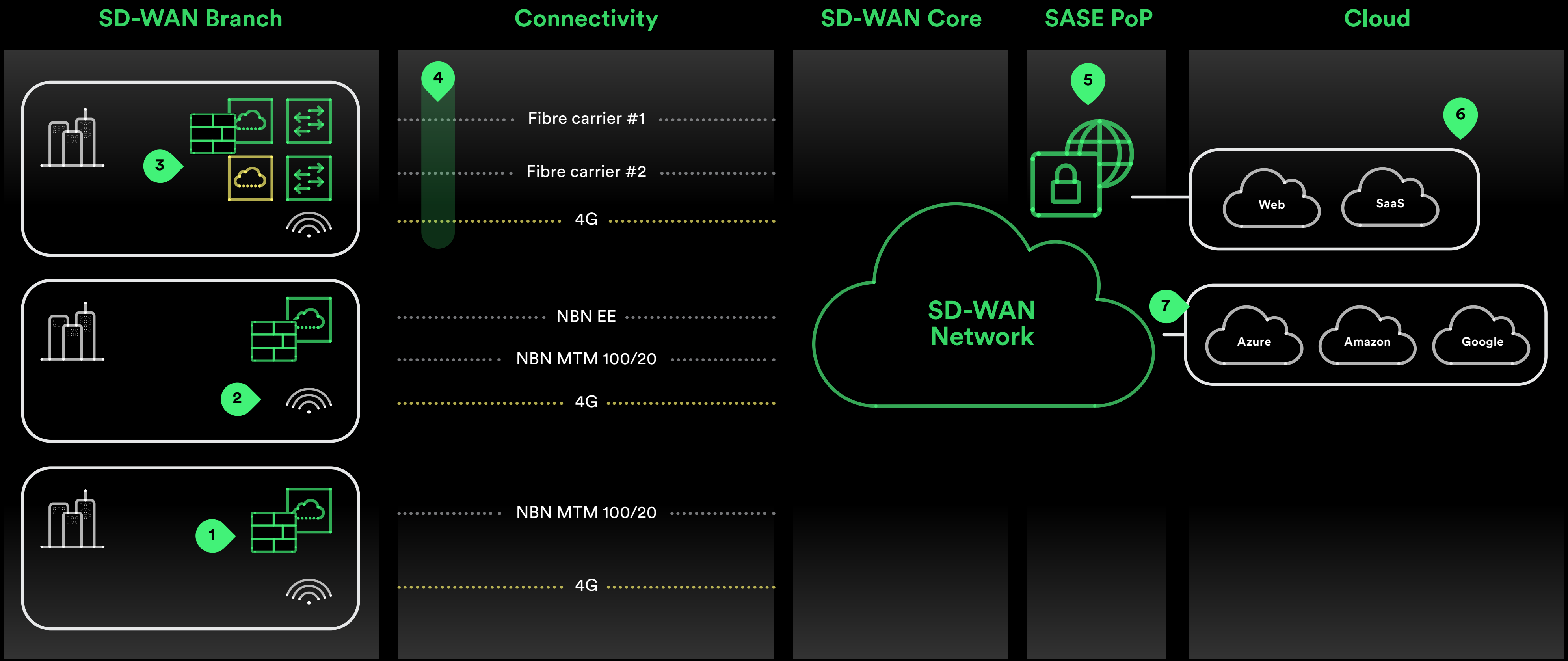
- Remote CASB Control
- Remote DLP

+

Custom features

- High availability
- Starlink
- 4G mobile primary
- Non-metropolitan sites
- Secondary access
- Dedicated public IP

Secure SD-WAN + Secure Site + Secure User



1 Managed SD-WAN appliance with IDS/IPS capability

2 4G Ethernet Modem and data pool for backup

3 High Availability topology with 2x switches and 2x SD-WAN appliances

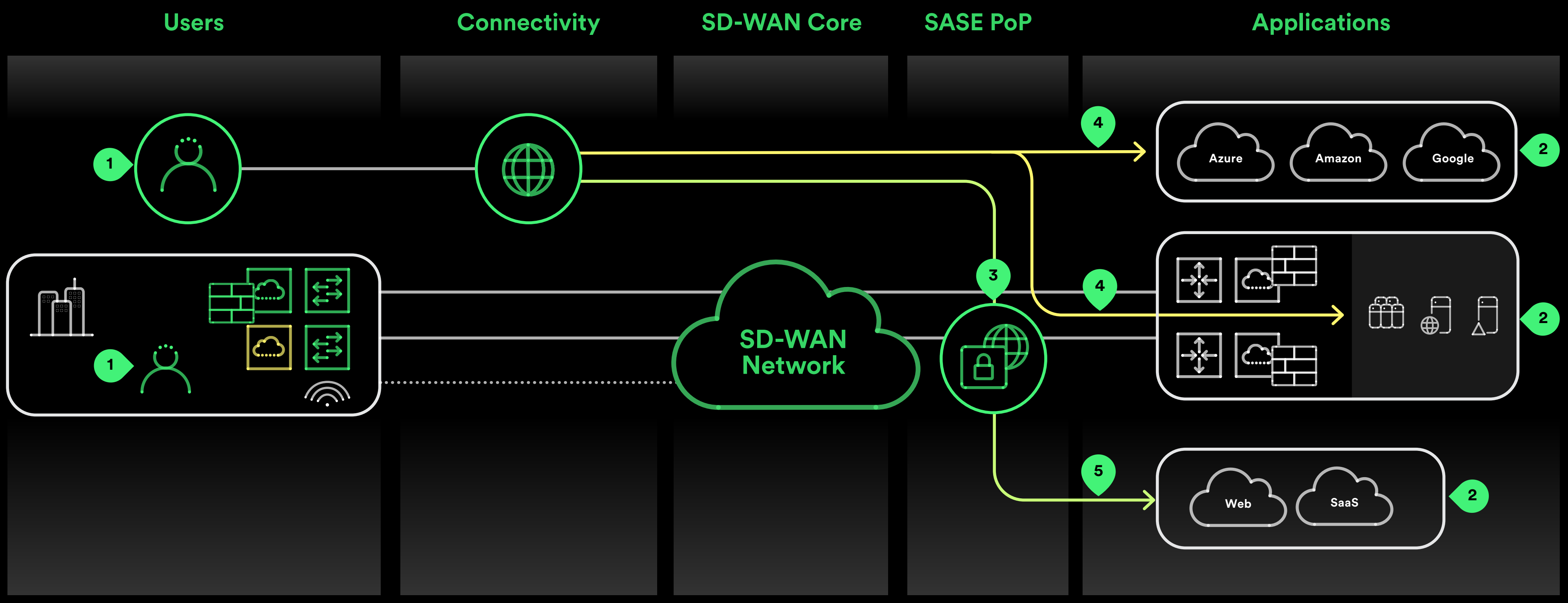
4 SD-WAN Edge bonds multiple access links to form a single logical pipe

5 Internet traffic traverses SASE PoP for security policy enforcement

6 Secure access to Web and SaaS applications

7 Private or public connectivity options into public cloud environments

Secure SD-WAN + Secure Site + Secure User



1 Users working from anywhere – SD-WAN branch, home, coffee shop or the airport

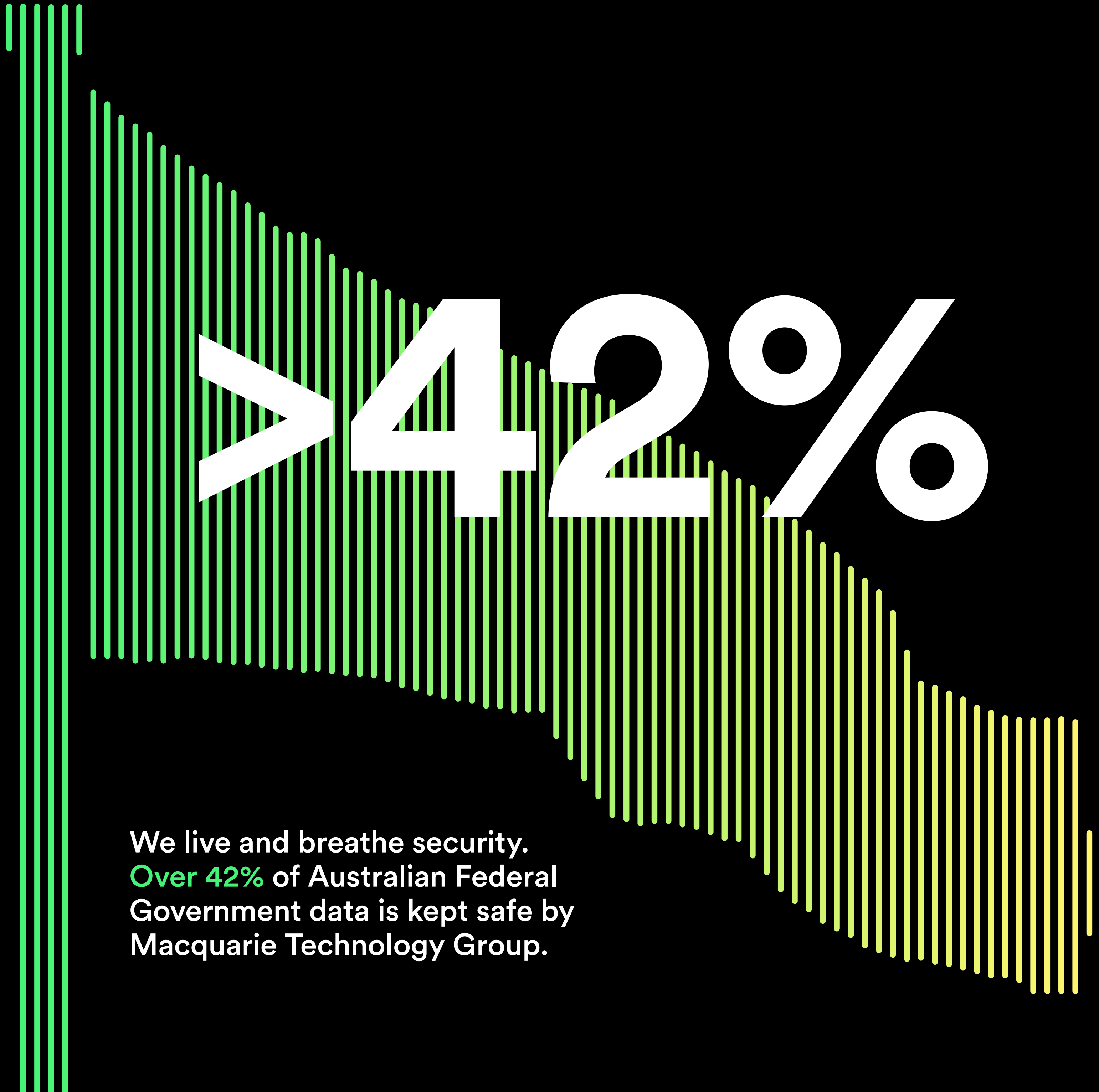
2 Applications hosted everywhere – public cloud, on-prem, IaaS or SaaS

3 Internet traffic traverses the closest SASE PoP for security policy enforcement. PoP locations are available globally

4 Secure access, using ZTNA principles, to internal resources while working from anywhere

4 Secure access to the Web and SaaS applications. Same security policies apply regardless of the users' location – whether they are in the office or working from anywhere

Halo Secure SD-WAN in numbers.



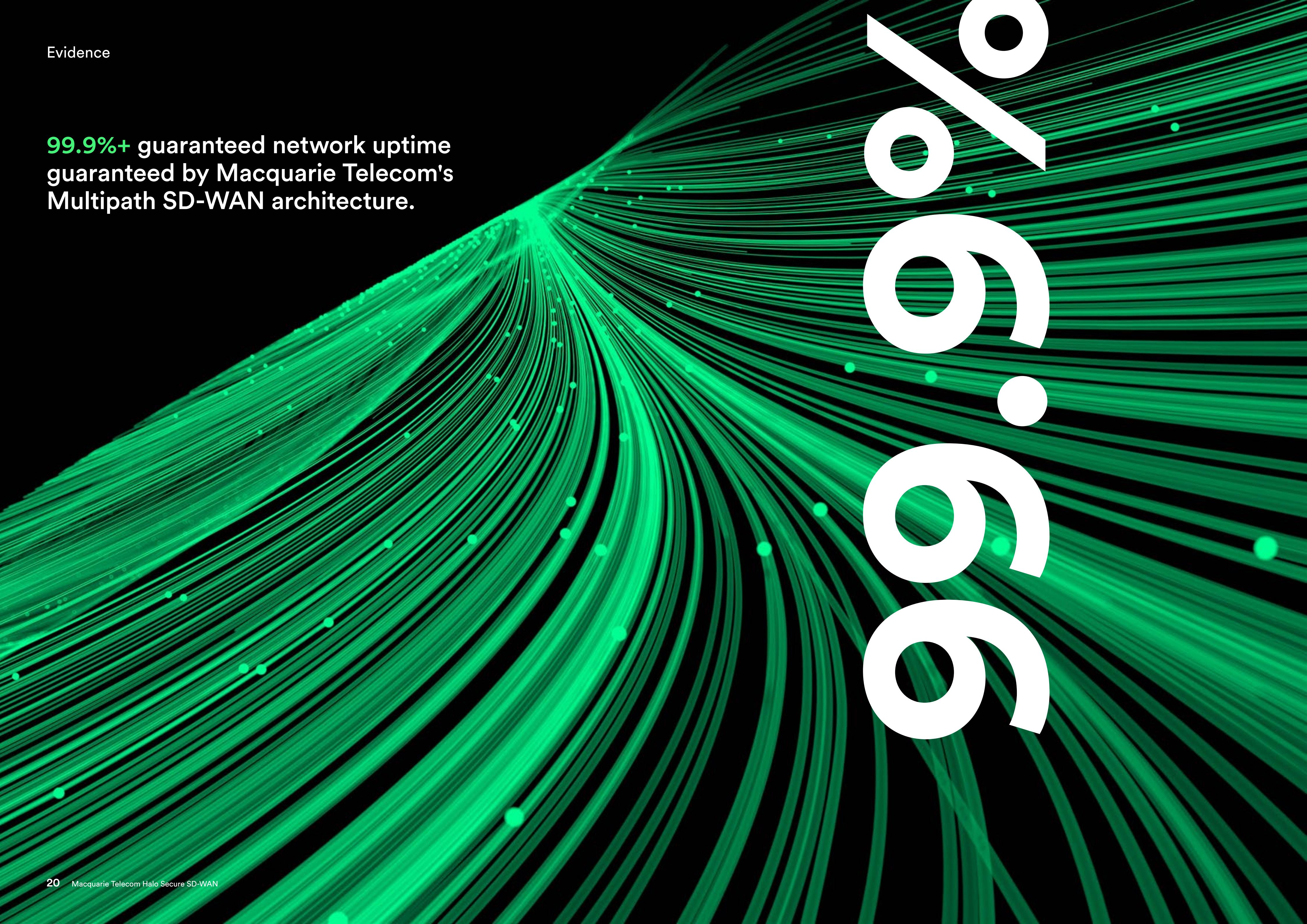
>42%

We live and breathe security. Over 42% of Australian Federal Government data is kept safe by Macquarie Technology Group.

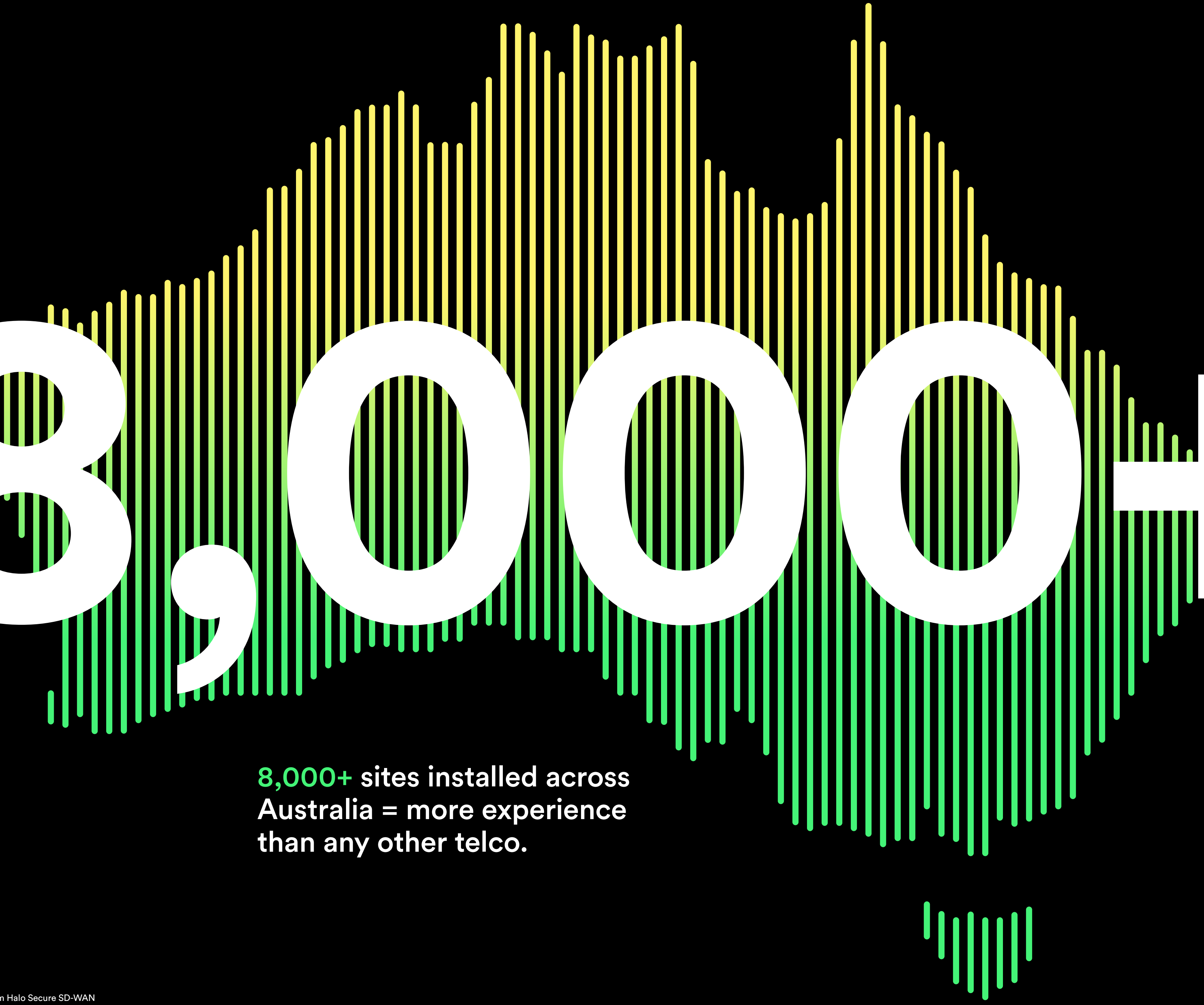
95% of calls are answered in less than one minute, by our call centre right here in Australia.

<1min

99.9%+ guaranteed network uptime guaranteed by Macquarie Telecom's Multipath SD-WAN architecture.



99.9%



8,000+

8,000+ sites installed across Australia = more experience than any other telco.

Connectivity.

NBN tailored for the demands of business.

Our mission is to provide our customers with a robust, low-touch network that's flexible and future proof.

Business nbn helps us deliver. Unlike consumer nbn, it's built from the ground up with bandwidth and technologies that provide a higher level of speed and stability. And it's backed by a dedicated business operations centre and business-specific SLAs.

Our network backbone puts you on the front foot.

We provide access to our fully-owned national network backbone, with points of presence (or POPs) across Australia.

Our access technology connects to our core using redundant fibre backbone with diverse inter-capital links and redundancy across every POP.

What does this mean for your business? In a nutshell, the speed and reliability of a network that's built purely for demanding businesses.

Serious guarantees for a serious network.

The experience we've been providing our customers for years means we're confident in our service level guarantees. The all-core backbone provide low latency and 99.9995% core P2P availability.

Every site comes with our High Availability Service Level Guarantee of 99.95%, and we may even offer rebates for non-performance.

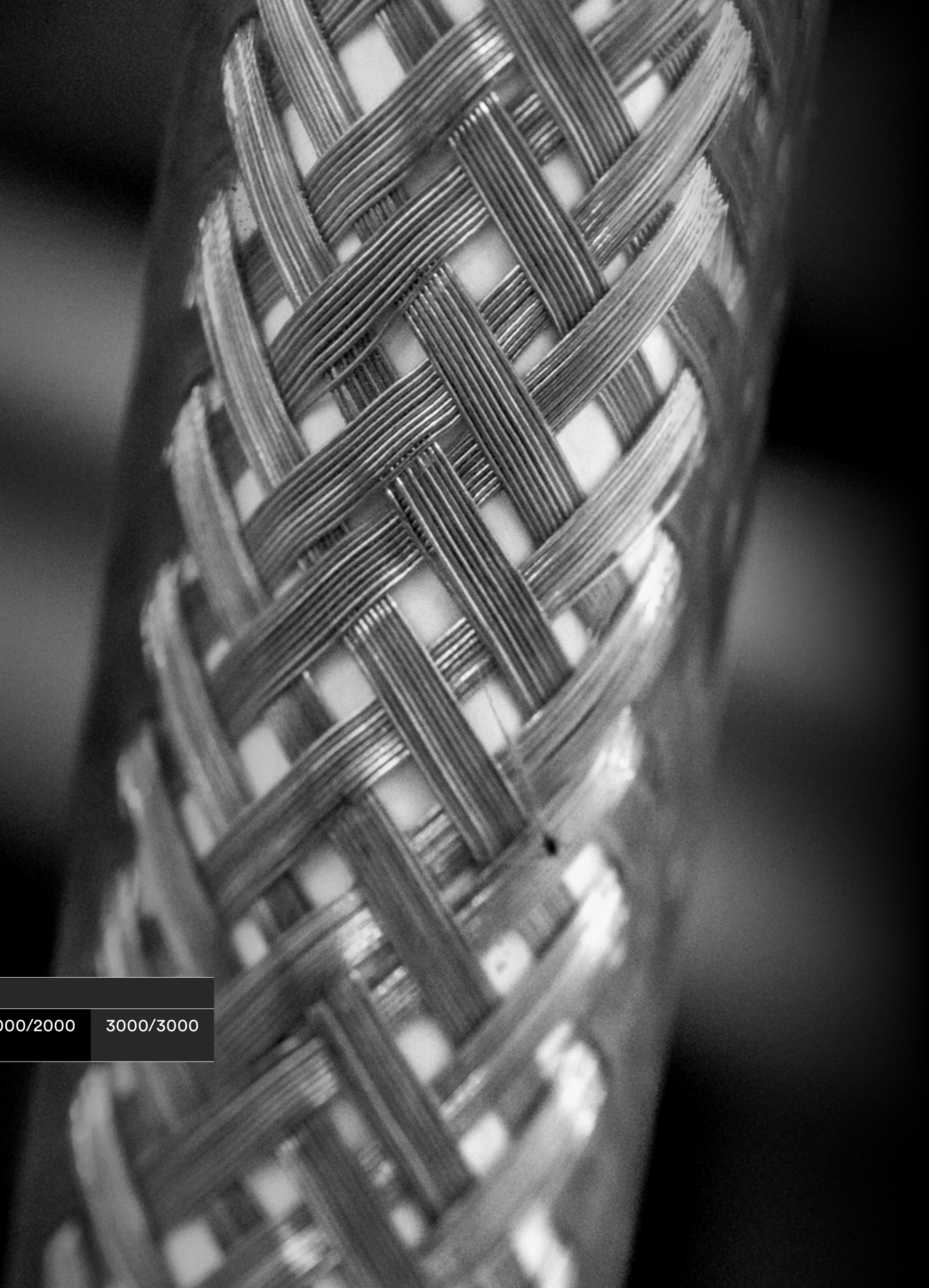
And for specific resiliency and high availability requirements, we have multi-carrier choices available, too.

Asymmetric

	Business				
DL/UL	100/20	100/40	250/100	500/200	1000/400

Symmetric

	Corporate			Enterprise				
DL/UL	50/50 (250/100)	100/100 (500/200)	200/200 (1000/400)	250/250	500/500	1000/1000	2000/2000	3000/3000



The SD-WAN platform.

Edge.

The SD-WAN Edge is a physical or virtual appliance we deploy on site or within a private or public cloud (like Azure, AWS or GCP).

Edges can serve small site or retail environments, large offices or multi-gigabit data centres. Whatever your use case, the technology and functionality are the same across any type of Edge.

Whether the Edge is virtual or physical, it provides optimised connectivity to private, public and hybrid applications. And most importantly, it performs the features that make Halo Secure SD-WAN different to traditional networks: deep packet inspection, application and packet steering, end-to-end quality of service and performance metrics.

Gateways.

Owned and managed by Macquarie Telecom.

Macquarie Telecom gateways are deployed within our Point of Presence locations, right across Australia. We choose locations strategically, making sure they're close to our customer sites and upstream peering locations.

Our gateways provide quick, secure and seamless access to our private backbone network, SIP infrastructure, or your legacy enterprise sites. This means you'll be assured of stable routing between capital cities, and SIP infrastructure which provides access to the PSTN network or any legacy sites you're running that are yet to migrate to SD-WAN. They also offer access to our own data centres for private and public cloud connectivity.

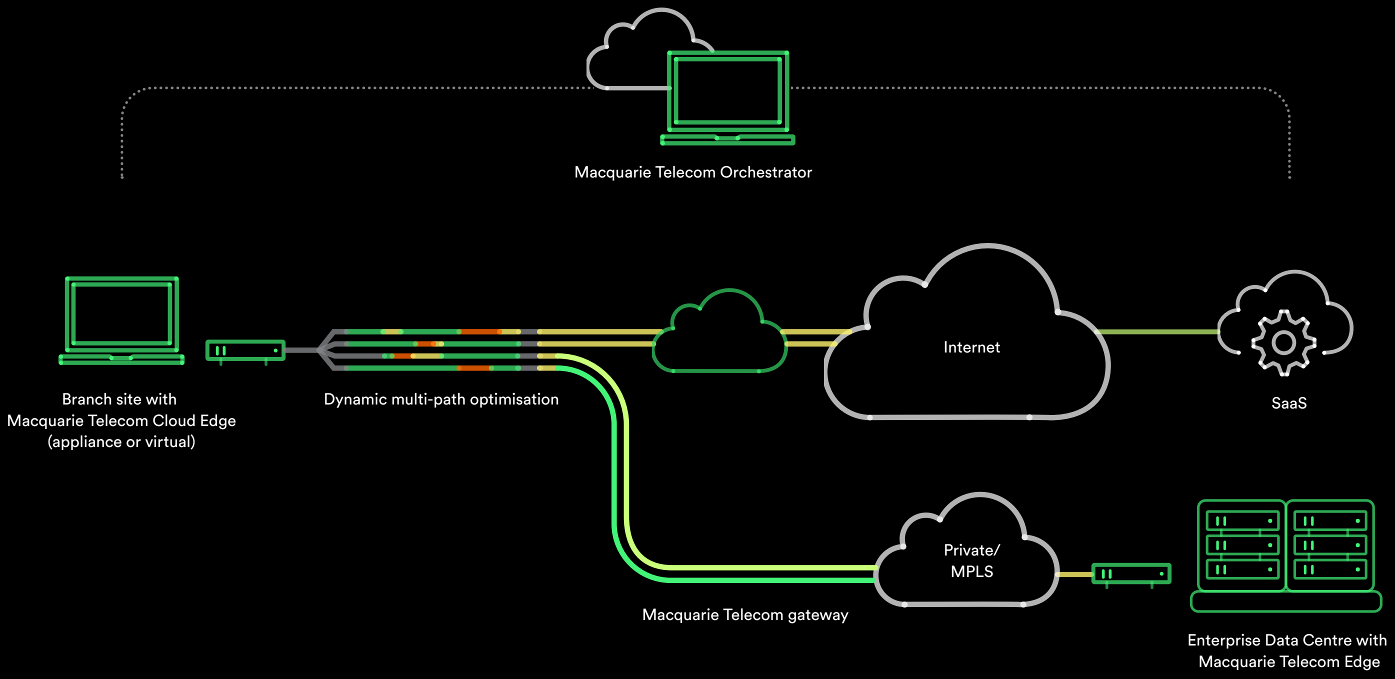
And last but not least, you'll always have the assurance that security is managed rigorously and patches are deployed as soon as a threat is identified.

Built to perform, ready to grow.

Hosting our own gateways allows us to use Layer 2 carrier access links on site. This enhances security, keeps latency as low as possible and ensures traffic traverses the optimal path to its destination.

We'll pick the carrier and bandwidth to meet your requirements. This is particularly useful where critical sites require access from alternate carriers for high availability.

Critical SD-WAN features like bi-directional quality of service, link bonding and remediation also sit within our gateway network. Because we host and manage our own gateways, we can easily scale your network up on demand – whether you're running ten sites or thousands. And just as importantly, support is all managed within our walls, so there's never any need to escalate gateway issues and wait for external technicians to help.


Macquarie Telecom Orchestrator
Branch site with Macquarie Telecom Cloud Edge (appliance or virtual)
Dynamic multi-path optimisation
Internet
SaaS
Private/ MPLS
Macquarie Telecom gateway
Enterprise Data Centre with Macquarie Telecom Edge

The Orchestrator.
Micro control. Macro simplicity.

Everything in its right place.

The Orchestrator is a single pane of glass that offers visibility, control and management of your entire network. Through it, you can see the performance of any site in real time, or hone in on individual links to monitor or troubleshoot them. And role-based access control makes it easy to set policies limiting most end users to read-only access, reserving more comprehensive change access for advanced users.

The Orchestrator is also home to SD-WAN's app prioritisation controls. On a single screen, you can track which apps are using the most bandwidth at any site, and decide how to prioritise them. That means casual users streaming YouTube will no longer bring important video conferences, voice calls or realtime applications to a standstill.

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

Network performance analysis made easy.

Knowing how your network is performing shouldn't be complicated, and it shouldn't demand excessive expertise.

We've built a Quality of Experience panel into the SD-WAN Orchestrator, so you can see how your network's performing in real time.

Application performance is presented as good (green), fair (yellow) or bad (red). You'll see this for every individual link to a site, as well as a combined score for the site's aggregated data pipe. By clicking on a link, it's easy to drill down into individual app performance, so you can quickly understand network performance variations as soon as they occur.

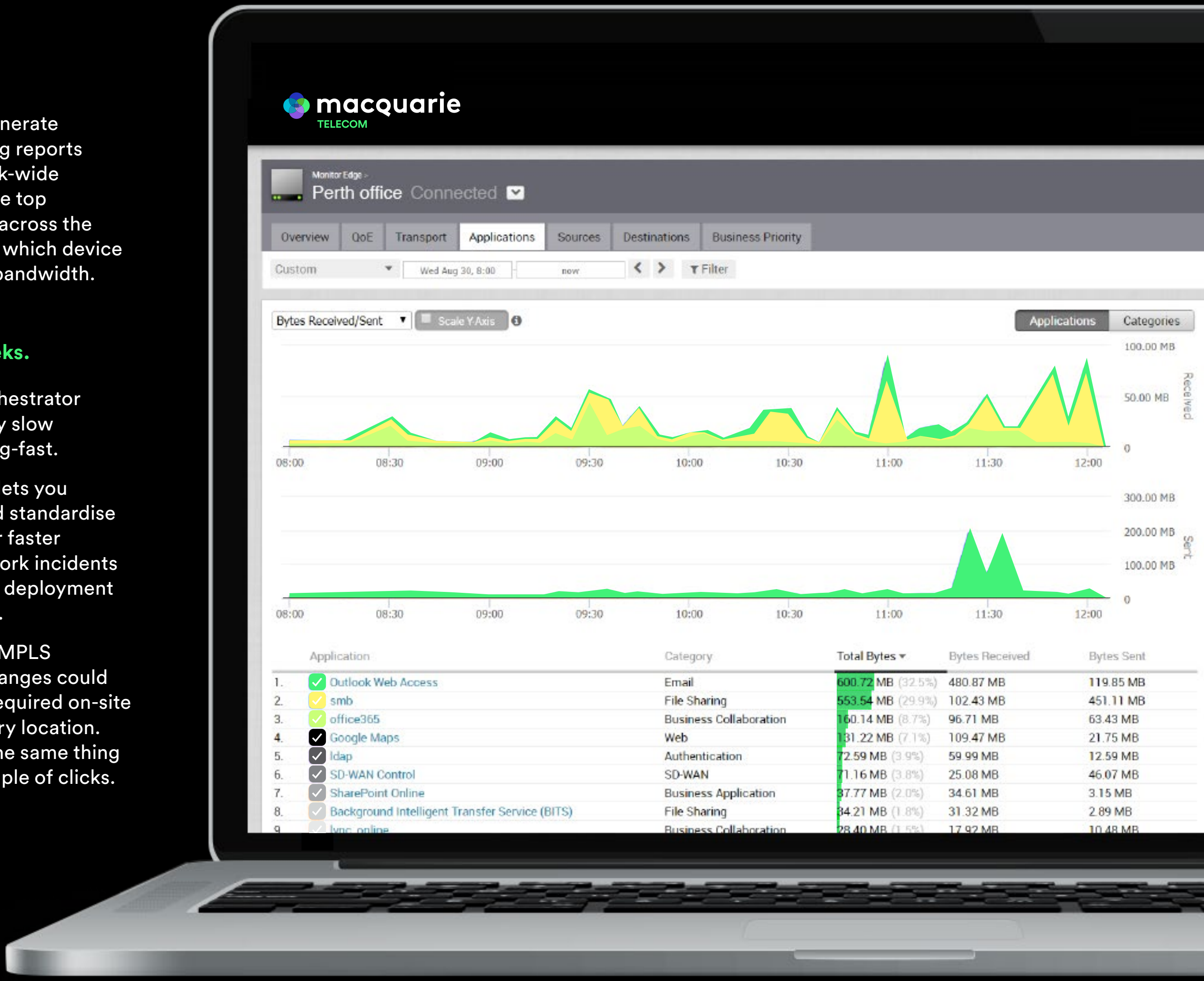
It's also easy to generate ad-hoc or recurring reports giving you network-wide insights such as the top application in use across the entire network, or which device is using the most bandwidth.

Make changes in minutes, not weeks.

Our SD-WAN Orchestrator makes traditionally slow processes lightning-fast.

The Orchestrator lets you create profiles and standardise configurations, for faster resolution of network incidents and network-wide deployment of critical updates.

With a traditional MPLS network, these changes could take weeks, and required on-site technicians at every location. SD-WAN makes the same thing happen with a couple of clicks.



	Application	Category	Total Bytes ▾	Bytes Received	Bytes Sent
1.	☑ Outlook Web Access	Email	600.72 MB (32.5%)	480.87 MB	119.85 MB
2.	☑ smb	File Sharing	553.54 MB (29.9%)	102.43 MB	451.11 MB
3.	☑ office365	Business Collaboration	160.14 MB (8.7%)	96.71 MB	63.43 MB
4.	☑ Google Maps	Web	131.22 MB (7.1%)	109.47 MB	21.75 MB
5.	☑ ldap	Authentication	72.59 MB (3.9%)	59.99 MB	12.59 MB
6.	☑ SD-WAN Control	SD-WAN	71.16 MB (3.8%)	25.08 MB	46.07 MB
7.	☑ SharePoint Online	Business Application	37.77 MB (2.0%)	34.61 MB	3.15 MB
8.	☑ Background Intelligent Transfer Service (BITS)	File Sharing	34.21 MB (1.8%)	31.32 MB	2.89 MB
9.	☑ lync_online	Business Collaboration	28.40 MB (1.5%)	17.92 MB	10.48 MB

High-uptime, high speed. All thanks to multi-path.

Eliminate network downtime.

Halo Secure SD-WAN uses multi-path technology to bind two or more data services together, treating them as a single data pipe to maximise speed and stability.

It chooses which link to send each packet of data across by measuring the real time performance of each link hundreds of times each second (and automatically compensating for packet loss, latency, jitter and capacity). Then it simply assembles the packet at the other end.

Critical real time packets are sent over both links simultaneously, to ensure they have a high probability of getting to their destination fast.

The Edge is smart enough to prioritise data packets according to their application: so a voice call or video conference, which demands very low latency, will take priority over emails or an OS update.

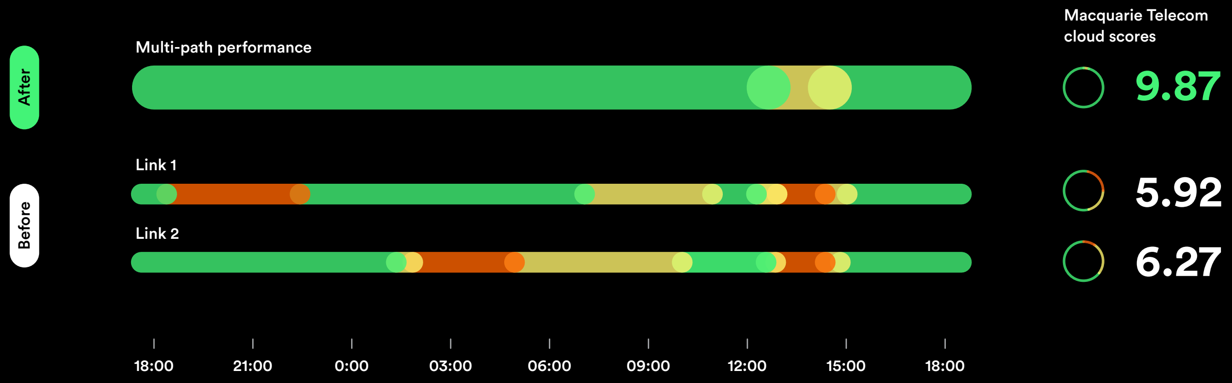
By using more than one link across different technologies, SD-WAN virtually eliminates network downtime. And if you only have access to one land-based network, we can use 5G links to provide the additional bandwidth and resilience you need.

Multi-path offers the ultimate failover, too: if one of your links does fall down, the Edge instantly routes traffic over the alternate link, so you can keep doing business.

AI-powered deep application recognition.

Macquarie Telecom's deep application recognition identifies over 3,500 applications and sub applications using a combination of AI and SaaS application database referencing.

The Orchestrator lets you track trends in application use over time, so it's easy to understand usage patterns today — and make sound network plans for the future.



Device rollout? You're looking at it.

Deployment, without the delay.

One of the challenges of traditional networks is the time they take to roll out. Sometimes they can take months, leaving you to work around technicians and downtime schedules.

SD-WAN can be installed in days. We use a template approach that captures all the important configuration items for various types of sites. Beyond the scope of these templates, custom device configurations or policy changes can all be performed remotely within the Orchestrator.

Plug in and go.

Deploying a new site installation simply requires someone to plug in the Edge. Once it automatically authenticates, it pulls down its configuration from the Orchestrator and it's ready to go.

If you need to set up a site at short notice when there's no land network available. SD-WAN can be deployed over 5G, so your pop-up store or temporary construction site can have fast, secure access to your business network.

Policy distribution made painless.

Halo Secure SD-WAN makes it easy to distribute business polices remotely to every Edge across your organisation, taking away the need for box-by-box configuration.

Transport group abstraction means configurations can be agnostic of hardware or physical interfaces, and you can assign specific policies to custom-defined groups, too.

This creates standardisation across your network, making it easy to troubleshoot faults and isolate the root cause quickly.

We're Australia's leader in SD-WAN. It's not a claim we make lightly.

Becoming SD-WAN experts didn't happen overnight.

Macquarie Telecom introduced SD-WAN to Australia at a time when traditional telcos wanted to keep businesses locked into legacy on-premise networks. With hindsight, it was a genuine turning point for the industry.

Since then, we've deployed more than 550 SD-WAN networks right across Australia. And with well over 8,000 sites, we're not only the national leader, but we've rolled out more networks than any other SD-WAN provider in the Asia Pacific region.

Our industry leaders are still learning.

Our certified engineers are already industry leaders in SD-WAN, but they view every network they deploy as an opportunity to build on their experience.

That means that when you choose Macquarie, you're choosing a level of SD-WAN expertise that can't be matched anywhere in Australia.

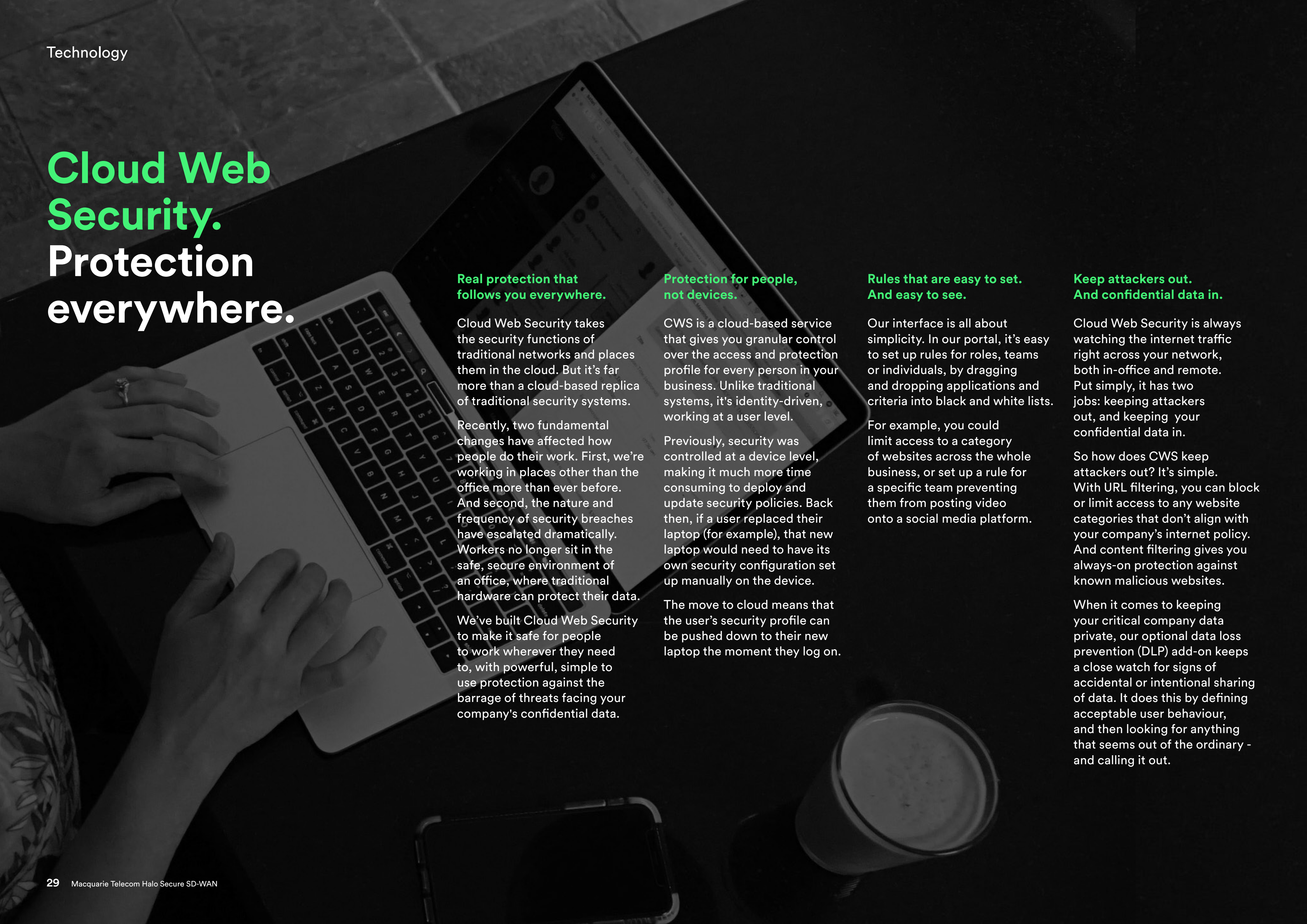
Cheekily leaving out features isn't our style.

Since we introduced the technology to Australia, SD-WAN has become the de facto standard for new networks. But that doesn't mean it's now a level playing field. Our evolving partnership with VeloCloud means we can provide features that other networks silently omit.

8,000+ sites rolled out across Australia.

550+ network deployments completed nationally.

#1 for SD-WAN in the APAC region.



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.

CWS 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's identity-driven, working at a user level.

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.

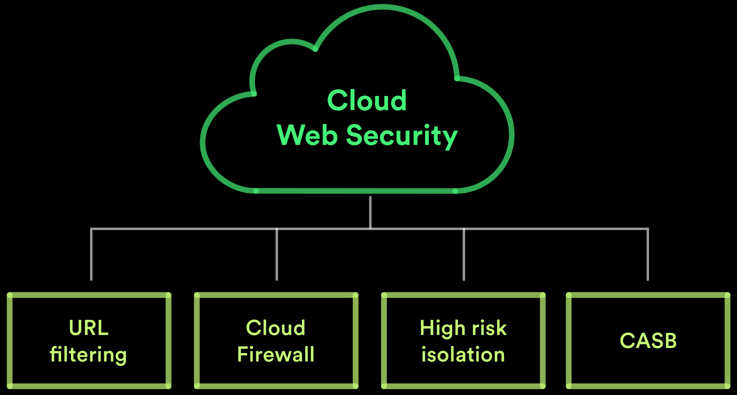
Keep attackers out. And confidential data in.

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, our optional data loss prevention (DLP) add-on 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 - and calling it out.

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



Ready for business as usual. And business as unusual.

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 – either by blocking the action immediately or raising a data exposure alarm.

High risk isolation: built in.

CWS automatically executes risky browsing activity in the cloud to protect you from web-based attacks.

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. 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 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.

Cloud Web Security: features

● Included
○ Optional

SSL decryption

Decrypting traffic and routing to other inspection tools.

●

Identity Provider Services

Supports SAML 2.0, SCIM and security policies per user or user group

●

SIEM integration

REST API that can be used to integrate your SIEM with Cloud SWG

●

Threat intelligence

Global intelligence Network that correlates information from 175M endpoints, 80M Web Proxies, 126M attack sensors, 25K vulnerabilities and 500+ security experts in house.

●

Logging and reporting

Comprehensive report centre with customisable dashboard. ** Logs stored for 100 or 365 days.*

●

URL filtering

Limits a user's interaction to specific categories of web sites based on a website's category, URL filtering based on risk scope, geo-based restrictions and dynamic URL categorisation.

●

Content filtering

Reduce attack surface by allowing only required types of content. For example – blocking the download of .exe files.

●

Anti-malware

Protects users from malware content in websites and documents by checking hash, signatures and performing static analysis and emulation sandbox

●

Cloud firewall

Configure policy to block traffic based on any TCP/UDP Port

●

High risk isolation

Uses Remote Browser Isolation to remotely execute risky browsing activity in the cloud to prevent web based attacks. It is explicitly for traffic that is either uncategorised or risk level 5+

●

CASB visibility

Visibility of SaaS and Web applications in use across the network. Create an inventory list of sanctioned and unsanctioned applications.

●

5 customised rules

5 overrides configured in addition to the implementation of a default template.

●

50 customised rules

50 overrides configured in addition to the implementation of a default template.

●

Full sandbox analysis

Utilises a dual-detection approach that combines virtualisation and emulation to capture more malicious behaviour across a wider range of environments. Create custom analysis profile to replicate Windows production environments, down to the version and applications in use.

○

CASB Control

Granular control of SaaS applications (30000+). There are generic controls available for all applications while offering flexibility to specify controls for specific applications.

○

Data Loss Prevention

Secure sensitive corporate content against accidental exposure, data loss and malicious breach

○

Secure User solution

Secure internet access for the hybrid workforce.

○

Secure User.
Cloud or local, your data’s safe.

Non-cloud files shouldn’t be compromised.

When you choose Halo Secure SD-WAN, 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 SD 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 SD Access is all done through the cloud. And as your organisation grows, you won't have to continually scale remote access 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 imagine 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.

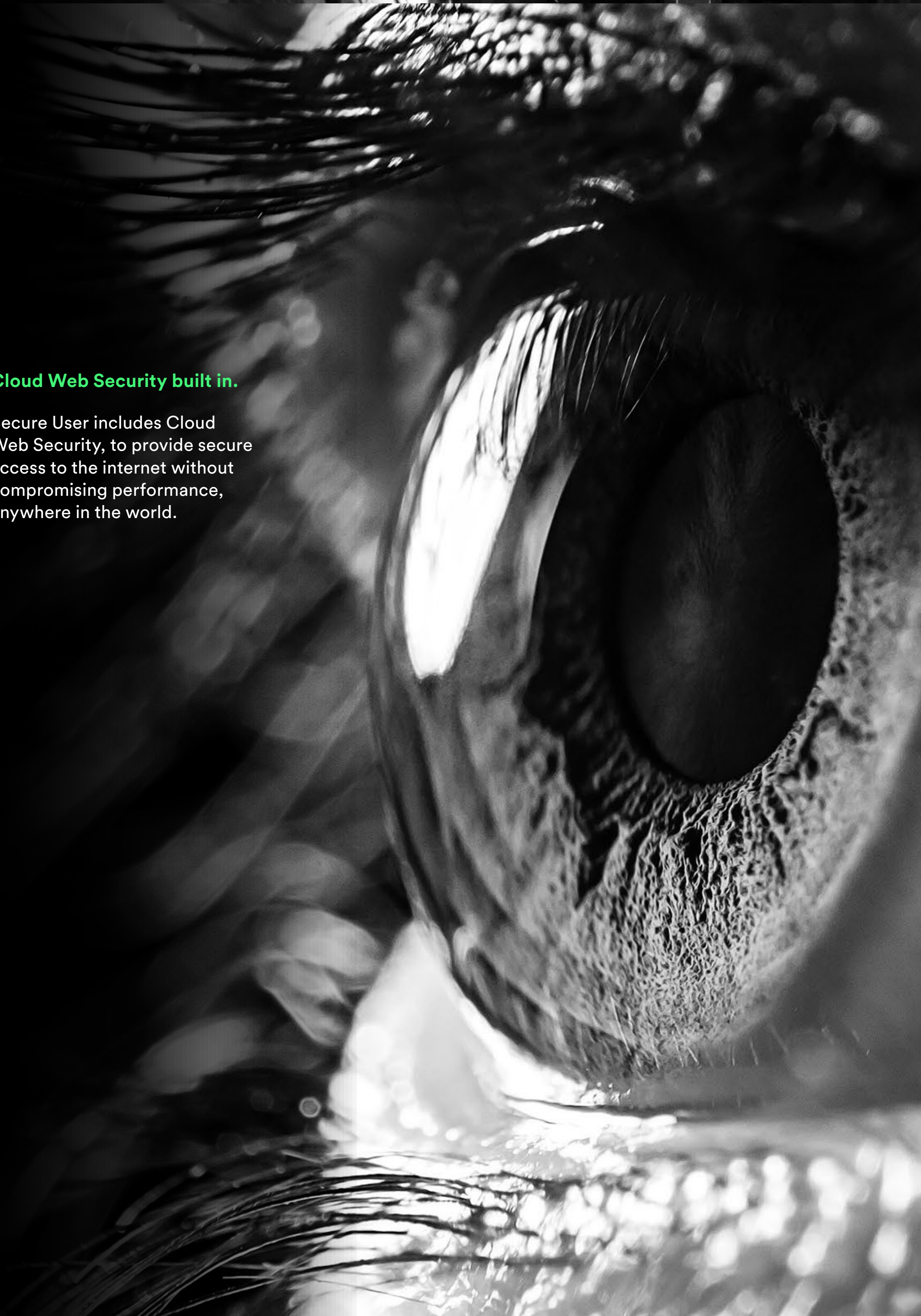
SASE takes the same approach to network access.

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 Access 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.

Cloud Web Security built in.

Secure User includes Cloud Web Security, to provide secure access to the internet without compromising performance, anywhere in the world.



Data protection. Powerful tools to secure your data.

The great CASB. Insanely granular SaaS 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.

Individual app landscapes that are always up to date.

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 at an organisation level – whether they're business-supported or private. From there, it has a comprehesive picture of each person's app landscape.

Control down to the last action.

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.

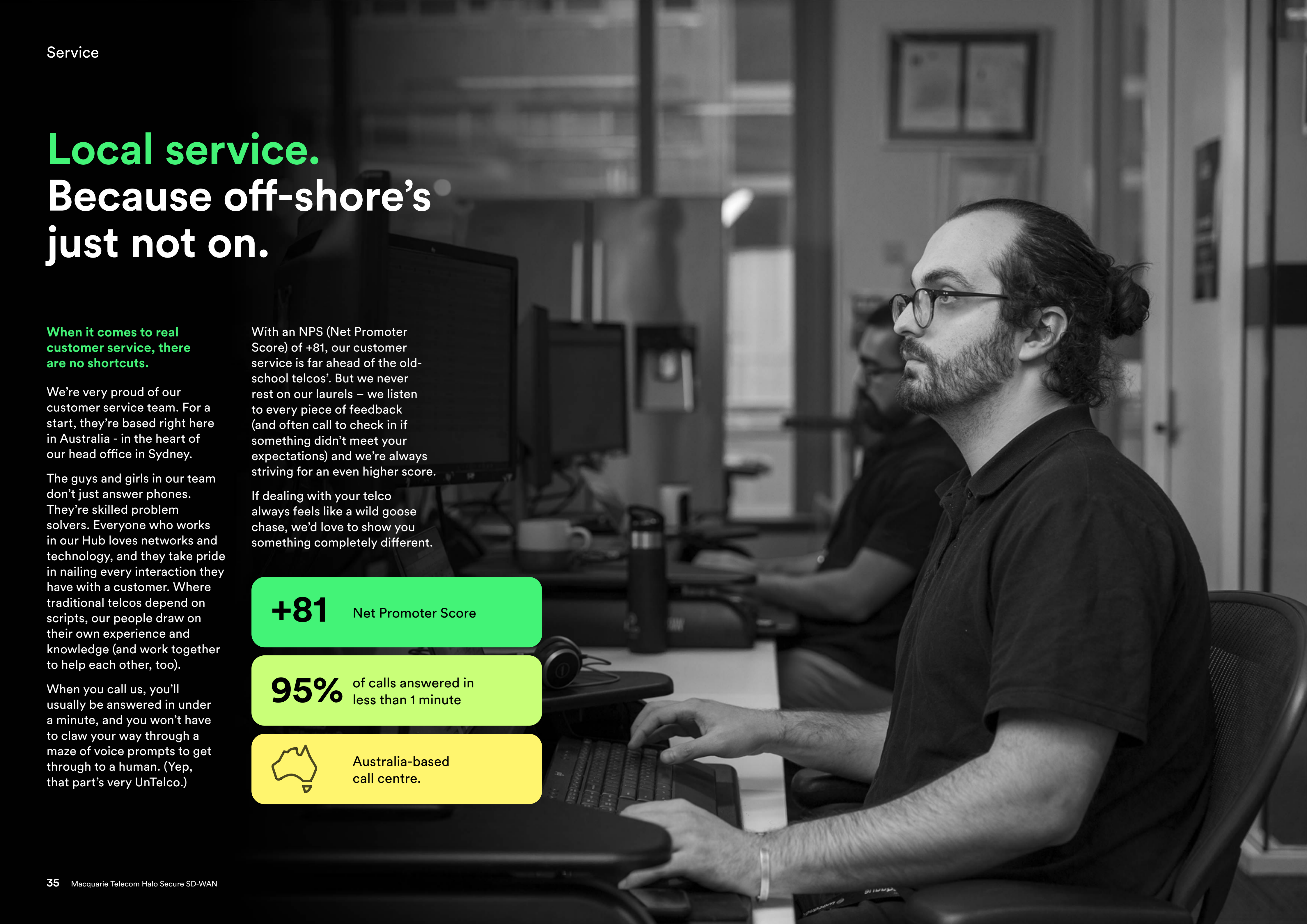
Data Loss Protection

Data Loss Prevention, or DLP, keeps your sensitive data safe by preventing it from leaving the boundaries of your enterprise.

It monitors, detects, blocks and reports data exposure, and makes it easy to comply with data privacy laws.

DLP uses a single pane of glass for simple management, giving you an interface that can be accessed by multiple teams across networking, security and compliance.

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 +81, 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.

+81 Net Promoter Score

95% of calls answered in less than 1 minute

Australia-based call centre.

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 network and security platforms depend on it, that’s a big deal for your business.

Other telcos have guesswork. We have Kate.

People learn best from people.

We believe that providing incredible online tools to manage your network and security 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 Halo Secure SD-WAN, we'll run training sessions to make sure you're ready to fly solo with our network management tools.

And if you've chosen additional custom features, we'll provide even more specialised training on monitoring, problem diagnosis and trend reporting, along with guidance on using your 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.

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 Technology Group'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 experience will help you protect your 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 VeloCloud. An innovative, recognised partnership.

Changing the rules for business networks.

Macquarie Telecom's partnership with VeloCloud 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, VeloCloud is recognised as an innovative leader in cloud-based networks. In just over half a decade they've rolled out over 400,000 SD-WAN sites globally, and were behind the world's largest deployment incorporating 18,000 sites collectively.

VeloCloud's SD-WAN expertise means your secure network is in good hands.

Recognised as a leading Velocloud partner.

A year after we joined forces with VeloCloud 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 VeloCloud sees Macquarie as a critical partner in best-practice network rollouts.

It’s time to talk to the UnTelco.

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

macquarie
TELECOM

1800 004 943
macquarietelecom.com

Sydney
Level 15,
2 Market Street
Sydney NSW 2000

Melbourne
Level 1,
441 St Kilda Road
Melbourne VIC 3004

Canberra
Level 12,
221 London Circuit
Canberra ACT 2600

Brisbane
Level 12,
100 Creek Street
Brisbane QLD 4000

Perth
Level 10,
251 Adelaide Terrace
Perth WA 6000