Protecting Your Remote Workforce with SD-WAN & SASE

Keeping your company's information secure has always been a challenge, even for companies as large as **Medibank** and **Uber**. But in the era of remote work, where **more than 35% of job holders can work from home full-time** and 23 percent can do so part-time, managing corporate data security has become far more complicated.

This is largely due to the **COVID-19 pandemic,** which forced millions of businesses to transition quickly to a remote work model. So quickly, in fact, many companies didn't have the time to properly update their data security, let alone monitor how their employees accessed that data. If we're honest, most of us assumed everything would be back to normal within a few months.

medibank PRIVATE

Medibank, an Australian health insurance company, confirms all 39 million customers had their data exposed to, and accessed by, a hacker.

Uber

Uber discovers that a hacker has "full access" to their internal systems, and maybe even the data of their **118 million customers,** thanks to a social engineering scheme.

However, hundreds of thousands of employees are still working from home. And companies are still operating on less-than-ideal security practices or none at all. This leaves their employees vulnerable to all kinds of cybersecurity risks, including ransomware, malware, and phishing schemes.

Even businesses that have taken the necessary precautions are struggling; not with a lack of security, but with how to effectively manage it. In fact, **almost 50% of all businesses** say they're using four or more vendors to make sure their remote teams are secure. That's four bills, four tech support lines, four platforms to know, and a whole lot of complications.

Thankfully, there's a way you can simplify (and strengthen) security for your remote teams – without compromising on quality or breaking your budget: leveraging **SD-WAN**.

Over

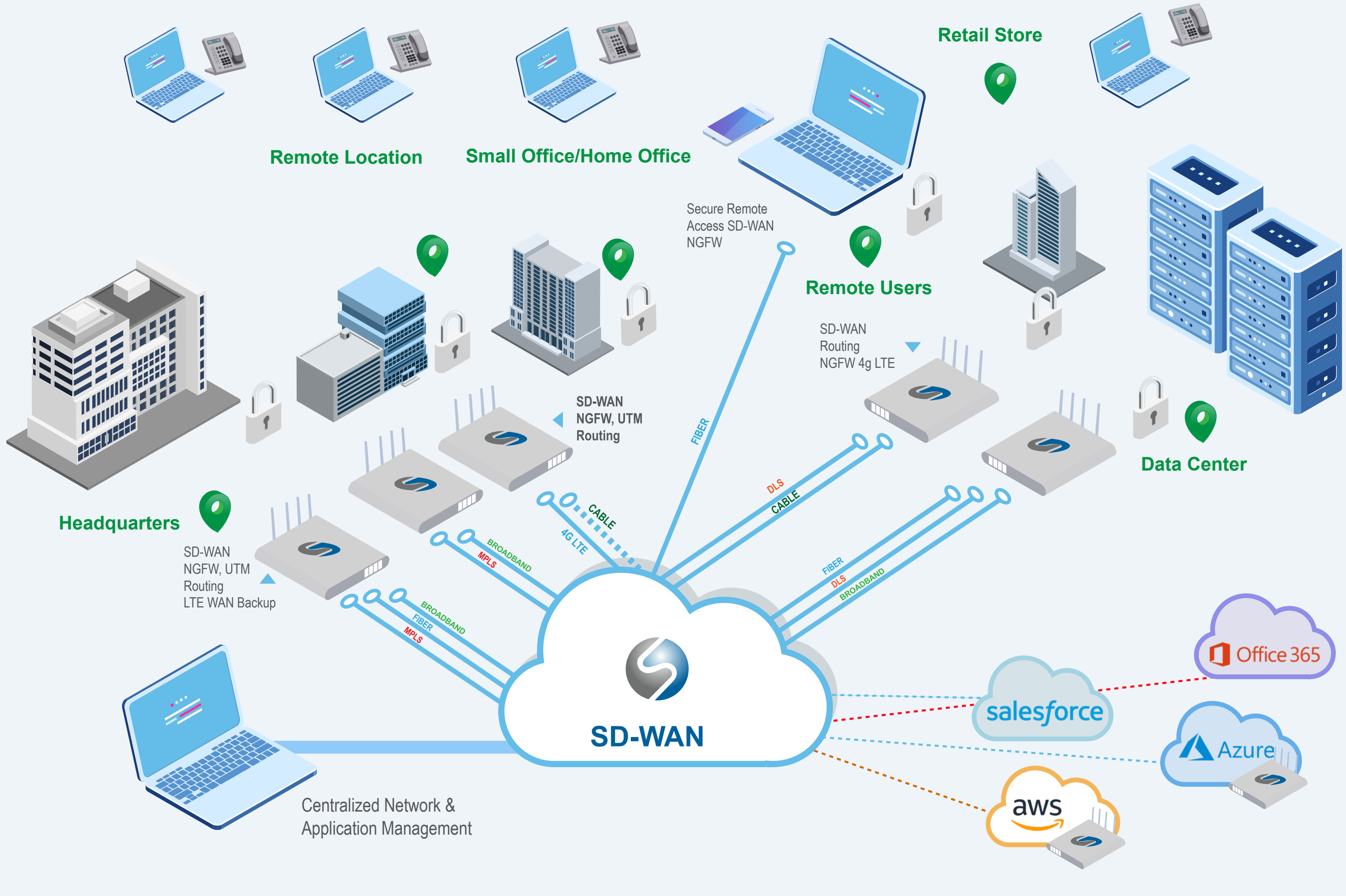
70%

of companies allow their employees to access corporate assets from their personal devices, **yet only 9% of them are equipped with all the "must-have"** protections their remote teams need to stay secure, such as SD-WAN.

What is **SD-WAN?**

SD-WAN stands for Software-defined Wide Area Network. Essentially, it is a virtual network with a software overlay that allows companies to use any kind of connection (DSL, Fiber, Multiprotocol Label Switching (MPLS), Broadband, etc.) to securely connect users to proprietary data and applications.

SD-WAN is, in essence, a powerful router that analyzes your traffic, tells it where to go, keeps it secure, and ensures that managing it is as simple as possible – all while improving your connection speeds.



866-404-7638 sales@snetconnect.com snetconnect.com

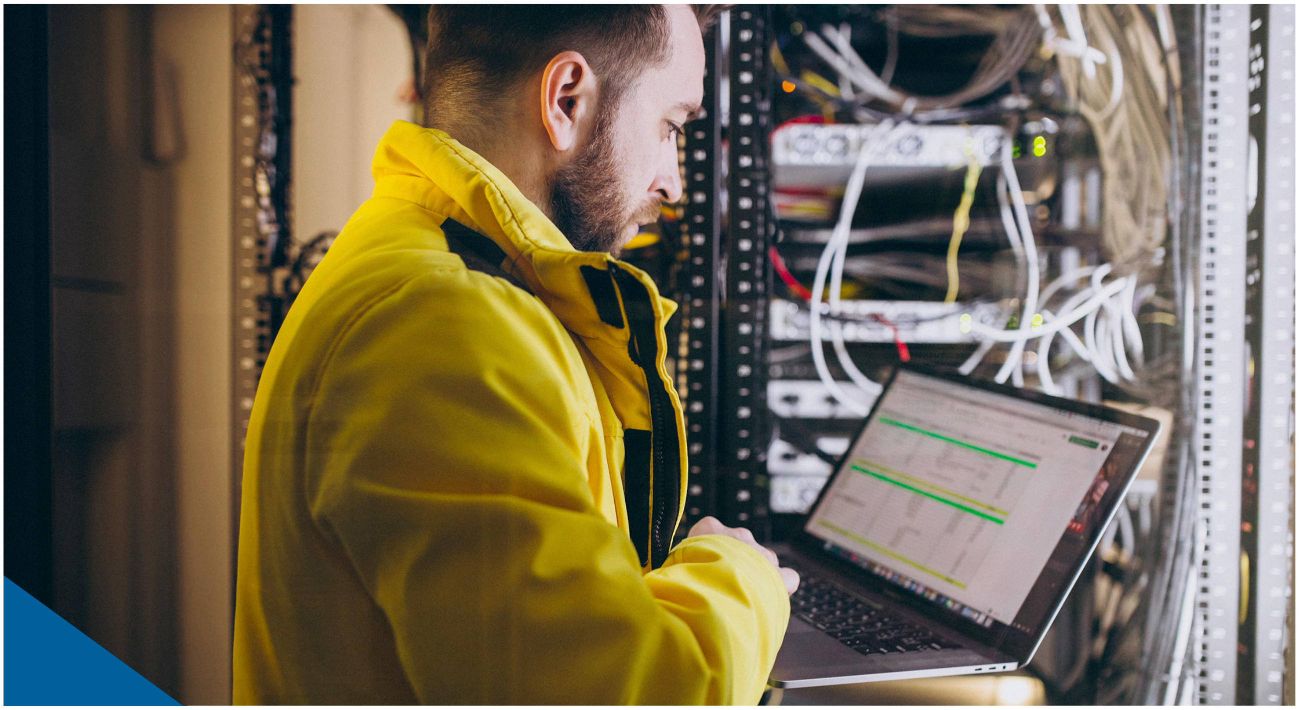
How is **SD-WAN** Set Up?

Typically, installing an **SD-WAN** begins when your provider installs an **SD-WAN** box, usually in your corporate headquarters. Once that's been set up, the **SD-WAN** will connect to local networks and establish encrypted links (or "tunnels") between all pre-determined devices within the office. Once these tunnels are established, you and your company can enjoy:

- Full visibility into how your network functions
- Insight into which devices are connected to your network and when
- Complete control over how all traffic is treated coming in and out of your network, and
- Heightened security for said traffic thanks to **SASE** functionality

What is SASE? A Brief Definition

Gartner coined the term "secure access service edge" (SASE) in August 2019 when it published **The Future of Network Security Is in the Cloud**. **SASE** is an approach to network architecture that combines wide-area network (WAN) capabilities with security functions delivered from the cloud through a secure access service edge device like an **SD-WAN** box.



SD-WAN for Remote Workers

Now, that's great for in-office teams, but how can remote workers benefit from all this additional functionality and security? The answer is simple: by establishing an encrypted link between their devices and your **SD-WAN** solution. Once this link is up and running, all traffic from these devices will be sent through your office's **SD-WAN** device and thoroughly vetted. It's like giving your remote team members their own individual VPNs – without the additional costs!

SASE SD-WAN: Security Benefits for All – Especially Remote Workers

And not a moment too soon. For far too long, remote workers have been operating outside typical security parameters, with devastating results. Now, with a **SASE SD-WAN** solution, you can monitor your remote workers better and provide them with the same level of security as your in-office employees.

Actively Monitor Remote Workers Utilizing:

Application Visibility & Control. As more and more remote teams use cloud-based applications to do their jobs, making sure those applications haven't been compromised is a must. **SASE SD-WAN** solutions like ours constantly scan applications accessed by remote teams to ensure they're properly vetted, sorted, and supported. Your IT team can sort these applications by risk factor, overall productivity, or a custom tag unique to you!

Active Directory Integration & User Control. Managing who connects to your network is key when you're dealing with remote teams. After all, you don't want just any device accessing proprietary information. **SASE SD-WAN** solutions like ours easily integrate with Active Directory (Microsoft's proprietary service) or other database services, allowing you to associate IP addresses with specific users in your organization and give them access to the appropriate data. Once a team member is identified within the system, you'll be able to:

- Authenticate them. Make sure the person accessing your network and database is who they say they are by asking them to enter their user ID and password.
- Manage them. You'll be able to quickly and easily program what kind of permissions each user has from the SD-WAN's online platform.
- Protect them. Once users are logged within the system, any threat originating from them – or targeting them – can be identified, targeted, and stopped either at the packet level by a next-generation firewall or at the application level by a secure web gateway.

Automatically Protect Your Remote Workers With:

URL Filtering. Remote employees with unfettered access to the web pose significant risks to your business, especially with how many malicious phishing sites and email links are targeting them. With **SASE SD-WAN**, your administrative team can set up URL filtering parameters on all connected devices, blocking or allowing URLs based on predefined categories. Now remote workers won't be able to access suspicious – or known – spam sites.

IP Filtering. In a similar vein, a **SASE SD-WAN** solution also filters IP addresses your remote workers access, identifying ones that have a bad reputation or could initiate DoS or malware attacks. Your IT team can automatically block traffic to these addresses, preventing any security breaches for both in-office and remote work teams. For instance, **S-NET's** solution provides protection from over 12 million malicious IP addresses and allows users to create their own blacklists and whitelists based on any new information they find.

SSL Inspection & Decryption. It used to be that only trustworthy websites could gain an SSL certification. Unfortunately, many spoofers and hackers have become more advanced, using SSL certificates to cover traffic that contains trojan horses and other network threats. Thankfully, a SASE SD-WAN solution – like ours – is constantly decrypting and inspecting all SSL-certified traffic on the network. Once the traffic is approved, it's re-encrypted and sent to the proper destination.

In short, a SASE SD-WAN solution gives you the opportunity – AND CAPABILITY – to protect your remote employees at every level, from the data packets they're sending on your network to the cloud applications they're accessing.

Looking To **Increase Security for Your Remote** & Hybrid Teams?

Look no further than **S-NET's SD-WAN** solution. From advanced content filtering to next-generation firewalls, our offering has everything your business needs to keep your remote employees' traffic and data secure, no matter how it's accessed.

Unsure where to start with **SD-WAN**? Don't worry! Our team of experts will listen to your needs and goals and set everything up for you accordingly. Also, you'll be assigned a personal technology advisor who will be there with you every step of the way.

Reach out to us today to start securing your network one connection at a time!