Sprint Networks
Creating Networks With More Possibilities

Sprint Networks

The Most Wanted Cyber Security Tools for Your Medical Practice

Keep Your Practice Always Online and Protected

Sprint Networks
Creating Networks With More Possibilities

TABLE OF CONTENTS

Sprint Network

Creating Networks With More Possibilities

About Us

We are the leading provider of affordable and powerful Cyber Security and Internet solutions to medical centres in Australia. Our vision is to be the trusted partner of choice for medical centres nationwide, providing them with the peace of mind that their data is safe and secure. We understand that your patients' data is your number one priority, and our solutions will help you keep it safe. Our solutions are tailored to meet the specific needs of medical centres, and help protect them from Cybercrime, Data loss, and downtime.

Primary Drivers for Healthcare Cybersecurity Investment

Medical practices in Australia are increasingly reliant on technology to store and share patient information. This reliance has made them a target for cybercriminals, who have attempted to access patient data through malware and ransomware attacks. Cyber security is therefore an important consideration for any medical practice, in order to protect the confidentiality of patient information.

Malware downloaded from malicious emails or websites is the most common type of security incident that medical practices are experiencing. Many medical practices are seeing a wide variety of other attacks, as well, including:

- Unauthorized access and hacking incidents.
- Theft of customer data, including credit card information.
- Ransomware attacks.
- Theft of critical business data and electronic files by external parties and insiders.
- Attacks against industrial controls and equipment, including (IoT) devices
- Security events typically result in system downtime for SMBs.
- Damage to PCs, servers, and other hardware, which can be costly to repair, is another top impact. However, other fallouts from a security incident can be much more costly and even cripple a business, such as the loss of customer trust.

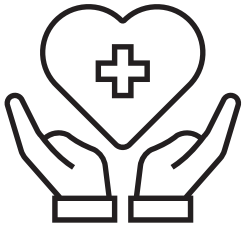
The criticality of services delivered by the health sector is of high importance and any disruption of service could be catastrophic. Therefore, more the reason for medical practices to adopt sound security solutions to keep themselves always online and protected.

Covid-19 has further changed the landscape of the medical industry. Patients have increased the use of telehealth facilities, which require a stable and secure connection. Any vulnerabilities, in the network, could be utilized by a potential attacker. Changes to social and working environments, such as working from home, have made the public vulnerable to cyber attacks.

The Current State Of Cybersecurity In Australian Healthcare

Australia's healthcare system is under threat from a growing number of cyberattacks. In the last year alone, there have been a number of major incidents, including the 'WannaCry' ransomware attack that crippled the UK's National Health Service. Australia is not immune to these threats and, in fact, is increasingly being targeted by cybercriminals. This is due to a number of factors, including the country's strong reputation in the medical field and the large amount of personal data held by medical practices.

The current state of cybersecurity in Australia is therefore a cause for concern. However, there are steps that can be taken to improve the situation.



For instance, medical practices can invest in better cybersecurity measures, such as firewalls and intrusion detection systems. Additionally, the Australian government can provide more funding for cybersecurity research and development. By taking these steps, Australia can help to protect its healthcare system from the growing threat of cybercrime.

What is a Ransomware Attack

In a ransomware attack, a hacker uploads a form of malware that encrypts the victim's files. The attacker then demands a ransom to restore system access

> *"Among the hacks reported last financial year was a ransomware attack on one of Melbourne's larger metropolitan public health services"*
>
> The Sydney Morning Herald

A Modern Way to Tackle Cyber Threats for Medical Practices

By adopting the proper technology; resource-constrained healthcare providers can navigate the challenges brought on by an *expanding attack surface*, *necessary compliance adherence*, and *obscured network visibility*, all the while dealing with the new trends that drive patients and employees toward cloud services.

We recommend Six (6) security capabilities for Healthcare and medical practices to deal with the ever expanding threat landscape;

1. Zero-Trust Network Access (ZTNA)
2. Secure Web Gateway (SWG)
3. Remote Browser Isolation (RBI)
4. Cloud Access Security Broker (CASB)
5. Data Loss Prevention (DLP)
6. Next-Generation Firewall (NGFW)

Zero-Trust Network Access (ZTNA)

Trust No One

In Australia, medical practices should be looking at having Zero Trust Network Access (ZTNA) in place to ensure the security of patient data. ZTNA is a security strategy that uses a combination of technologies to verify the identity of users and devices before allowing them access to internal resources.
This ensures that only authorized users can access sensitive data, and that all traffic is encrypted, preventing eavesdropping or tampering.
By implementing ZTNA, medical practices can help to protect patient privacy and safeguard sensitive information. As such, ZTNA is an essential part of any medical practice's security strategy.

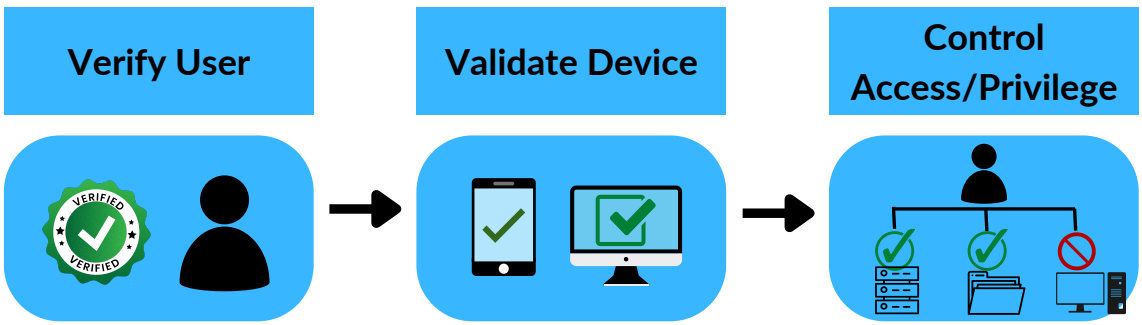


Fig 1-Shows how ZTNA works

Secure Web Gateway (SWG)

Best Defense to stop Internet Threats

In Australia, medical practices are bound by strict privacy laws. As a result, it's essential for doctors and other medical professionals to use a secure web gateway when accessing confidential patient information. By using a secure web gateway, medical practices can ensure that patient data is protected from unauthorized access.

In addition, a secure web gateway can help to prevent malware and other threats from infecting computers and devices used by medical staff. As the use of electronic health records becomes more widespread, it's becoming increasingly important for medical practices to implement a secure web gateway. By doing so, they can safeguard patient information and help to ensure compliance with privacy laws.

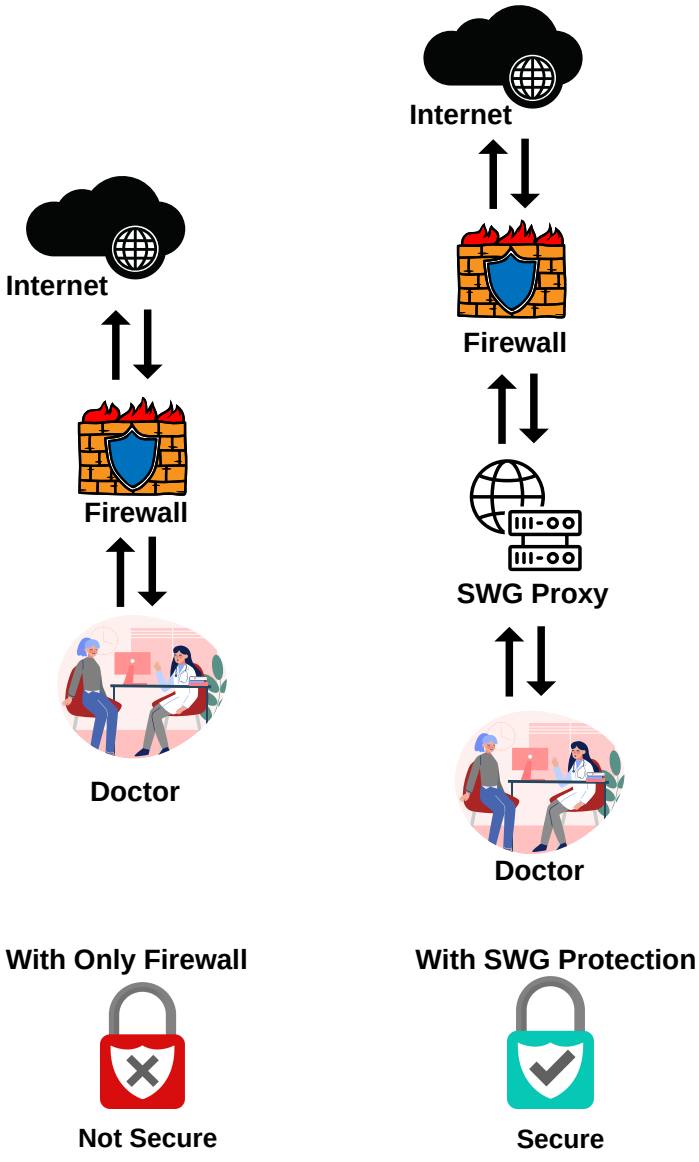


Fig 2-Shows how SWG protects the end user

Remote Browser Isolation

Safeguard Your Browsing Activity

Remote Browser Isolation (RBI) moves the execution of a user's browser activity from the client device to a remote server — hosted on-premises or in the cloud. This protects against browser-based security exploits and provides a means of anonymous browsing and risk-free open Internet access. In other words, RBI creates a virtual isolated container for users to browse the internet. It creates a secure connection between a user's (e.g: Doctor) device and the isolated browser. The attack is limited to that isolated container and no breach at the Doctor's device.

As the user browses the public Internet, the remote browser is isolated from the user's physical endpoint (Laptop or PC) and the Medical Practice data network. Therefore, any attacks on the remote browser session are constrained to the virtual environment.

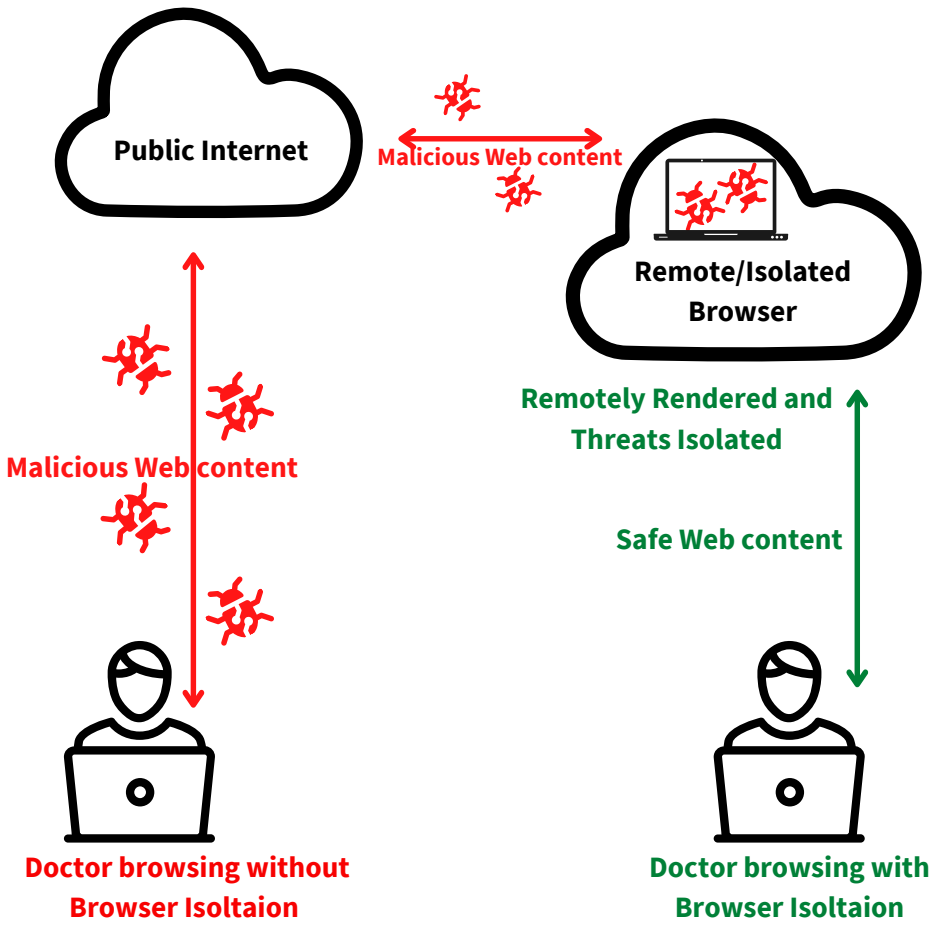


Fig 3-Shows how how RBI ssafeguards your browsing activity

Cloud Access Security Broker (CASB)

Securing your Medical Application Data

Cloud Access Security Broker (CASB) products and services deployed on-premises or in the cloud address security gaps in the Medical Practice's use of cloud services. This technology is the result of the need to secure cloud services, and enable secure access to them from users both within and outside the Practice's perimeter, and support secure cloud-to-cloud access.

For CASB products and cloud services, the protection target is different from that of an on-premises security system. It's still Medical data, but the data is processed and stored in systems that belong to someone else. CASB provides a central location for policy and governance concurrently across multiple cloud services for both users and devices along with granular visibility into and control over user activities and sensitive data.

Data Loss Prevention (DLP)

Prevent Loss of Your Critical Patient Data

Data loss prevention (DLP) is a technology protecting a Medical Practice's data against loss, theft or misuse, regardless of where it is located.

DLP solutions can be used to classify and prioritize data security. You can also use these solutions to ensure access policies meet regulatory compliance, including HIPAA (The Privacy Act 1988), GDPR, and PCI-DSS. DLP solutions can also go beyond simple detection, providing alerts, enforcing encryption, and isolating data.

DLP, also ensures that unauthorised employees do not send sensitive or critical information outside the corporate network.

Next-generation Firewalls (NGFW)

Protecting Against External Threats 24/7

In Australia, medical practices are under increasing pressure to protect patient information from cyberattacks. To meet this challenge, many practices are turning to next-generation firewall (NGFW) solutions. NGFW is a type of firewall that uses deep packet inspection to examine traffic at the application level, rather than just inspecting IP addresses and port numbers. This allows NGFW to identify and block malicious traffic, even when it is encrypted.

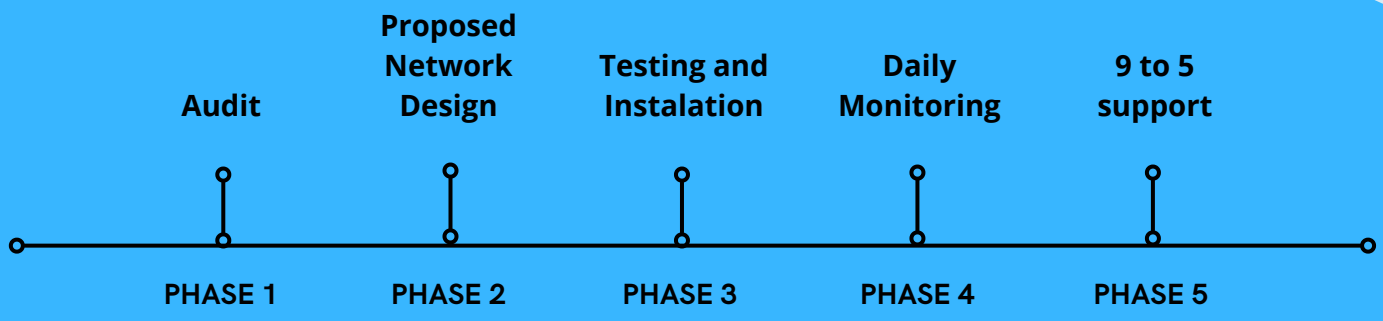
In addition, NGFW can provide comprehensive visibility into network activity, making it an ideal solution for medical practices that need to comply with data privacy regulations. As the threat landscape continues to evolve, NGFW is an essential tool for protecting patient data in Australia.

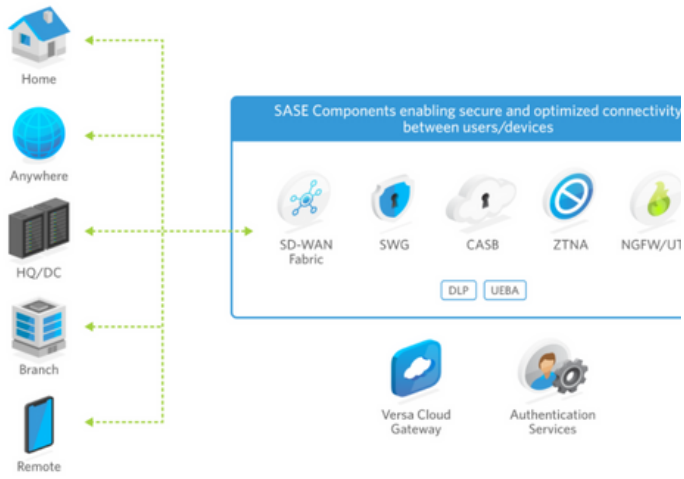
How we can help your Medical Practice?

- **Reduce practice downtime**
- **Secure and uninterrupted Internet connectivity**
- **Protection from cyber threats, malware and viruses so that your patient data is always safe and secure**
- **Better application performance for your critical medical applications**
- **Secure access to your important medical data from anywhere**
- **Periodic backup of patient data and records to a secure service**
- **Secure and reliable connectivity between multiple medical branches if you own more than one**

KEEP YOUR PRACTICE ALWAYS ONLINE AND PROTECTED

Proposed Timeline from Start to Finish





Phase 1- We will audit and assess your existing Network infrastructure. Understand your major pain-points.

Phase 2- Our team of Network Engineers, would analyse and recommend changes and lay down the plan to implement the new network.

Phase 3- After implementing the design, we would run tests and ensure every device runs effectively and is completely secure.

Phase 4- We also would be providing regular maintenance of the network and support in case anything goes wrong. Sprint networks would be your one-stop fix to any of your network troubles.

Phase 5- Add-on services like ZTNA, RBI, SWG and CASB would help enhance your network. These tools would help increase network security by using the cloud to securely store your information.

TALK TO US

Tel: 02 7252 3885

info@sprintnetworks.com

Contact us for further information

Sprint Networks

www.sprintnetworks.com.au

Info@sprintnetworks.com

+61 2 7252 3885

Sprint Networks

Creating Networks With More Possibilities