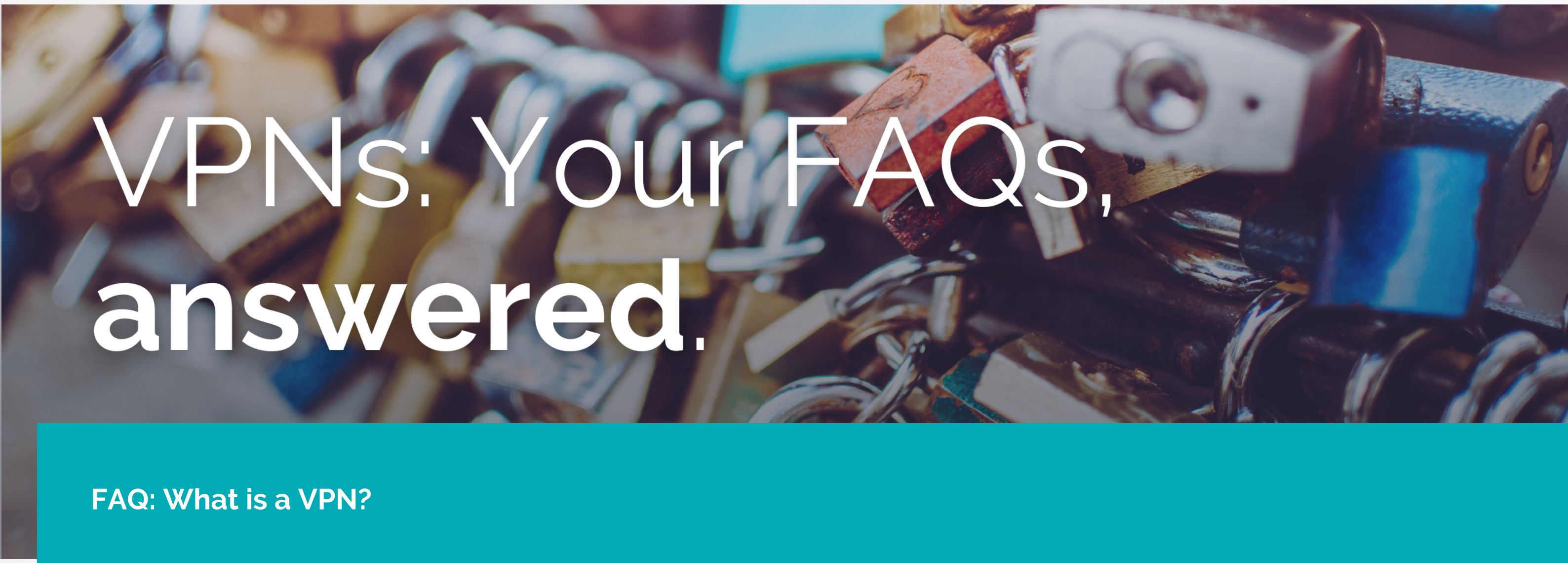

VPNs: Your FAQs, answered.

FAQ: What is a VPN?

A Virtual Private Network (VPN) ensures that your internet connection is secure and anonymous by creating a 'private tunnel' on a public network connection.

Can I access the internet using a VPN?

A VPN cannot provide you with internet access. For that, you need to install a network infrastructure, such as a GSM SIM linked to an APN.

For more on GSM connectivity, read this article about why Cellular is a fantastic option for businesses that require reliable coverage for a large number of distributed assets.

What can VPNs be used for?

VPNs are commonly used for data protection purposes, such as:

- circumventing geo-blocking and censorship on the internet,
- protecting a user's identity with an anonymous IP address.

When layered over an APN, VPNs can also provide advanced remote access to field devices and assets from a configured PC. This is a unique service provided by Trinity IoT if required.

Schedule a call with your sales rep to discuss our VPN/APN layering options.

FAQ: Do I need an APN if I have a VPN?

As we've mentioned above, VPNs do not provide network access to your assets. For that, we recommend using an APN.

APNs are advantageous if you own a large number of SIMs that you would like to manage remotely via an online platform like Trinity Connect. You can think of APNs as a "data pool" that aggregates data usage across all of your SIMs, making it possible for you to manage data expenditure from a single account. The result is better spend management and control of SIMs on a per SIM or estate level.

If you're new to APNs, read about it the basics here.

FAQ: Are my devices/SIMs safer when using an Open VPN?

Although VPNs are commonly associated with private data transmission, the privacy of your SIMs/data/devices and assets is not solely dependent on whether you have a VPN or not.

Firewalling, configuring a RADIUS, and setting up geo-redundant data storage servers are measures put in place by the Trinity team, specifically to ensure the privacy (and security) of information collected - whether you have a VPN or not.

Do I need a VPN if I use the Trinity Connect platform?

VPNs aren't essential when it comes to setting up a secure data transmission framework - and we don't recommend using one unless there is a clear business need that outweighs the risks and costs involved with setting one up.

An open VPN network layer is only needed in conjunction with Trinity Connect if you require advanced remote access to field devices and assets:
VPNs enable a third-party to reach far back through a private network to access asset data and perform specific configurations. For that reason, while you will be able to manage your SIMs and devices from the Trinity platform, you will not be able to do so for field devices or assets.

Example
A business requires remote control of their company laptops to update the operating software. Instead of asking each employee to update their own laptop software, they wish to do a bulk update from an individual remote PC. Since the PC is beyond the SIM or device management layer, we would recommend using a VPN to directly manage the assets.

Can Trinity provide me with a VPN?

Yes, Trinity can provide you with a private access point into the network. The VPN will provide a secure and private doorway for third-party PCs which will enable you to access the network via public network infrastructure.

Service Includes

- **Unique login credentials & VPN certificate.**
- **Private, gated access to the Trinity network environment.**
- **API infrastructure that will allow you to build an integrated platform.**

Service Excludes

- **Design, development or deployment of a VPN-based asset management platform.**

Visit our website:

www.trinity.co.za