FREEWAVE

Why Choosing Zero Trust Network Access Over Virtual Private Networks is a C-Suite Decision

Richard Reisbick, CTO FreeWave

You're leading the company. Why do you need to care about your business' network security approach?

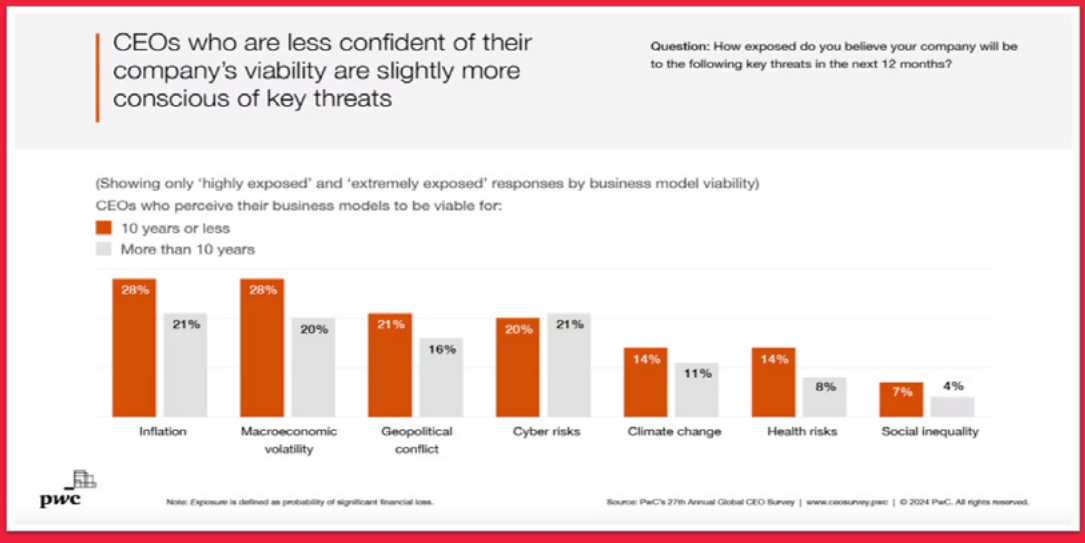
The answer comes from something all too familiar: the accelerated rate of change – and the quest by modern leaders to build a resilient company. PwC describes today as the "age of continuous reinvention" in its 27th Annual Global CEO Survey report. One of the most startling findings is that 45% of CEOs do not believe their company will be viable in 10 years if it stays on the current path.

Part of the challenge is knowing what could take your company down. Cybersecurity vulnerabilities at the network level is on the list.

PwC's report shows that CEOs who believe their organization is viable for more than 10 years perceive inflation (21%) and cyber risks (21%) as top threats with macroeconomic volatility (20%) just a half-step behind.

As chief technology officer for FreeWave, part of my role is to find weak spots in a network connected to the industrial internet of things (IIoT). I talk to many senior leaders from companies in the oil and gas, agriculture, mining, water treatment and other remote industries. What's the number one pushback I run into? They tell me they use virtual private networks (VPNs).

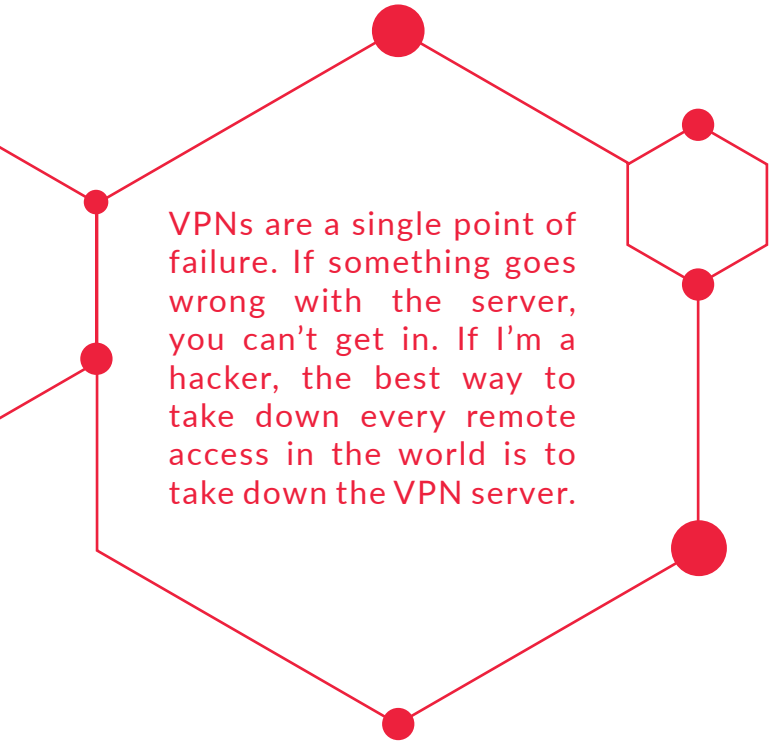
I call this "pushback" because, at FreeWave, we don't let VPNs into our data platform.



At their most basic level, VPNs are used to create a secure connection between a user's device and the VPN server. Through that connection, data is encrypted, and a user's IP address is hidden. As a result, VPNs can allow remote users to securely access internal networks, including machinery, control systems, and databases.

For those who may not be familiar with a VPN (although we've all probably used one at some point), here's a simple analogy. Think of a VPN as a tunnel buried far below intersecting highways. One end of the tunnel is an IIoT device and the other end is the server. Your car (let's make it a Maserati, while we're at it) is a data packet. Instead of traveling across potentially dangerous highways where threats abound (a malicious attempt to steal your Italian beauty and hold it for ransom, as an example), you take the tunnel built just for you and other authorized drivers you trust.
The challenge today is that the tunnel is no longer safe.

Why Are VPNs Insecure?
Technology ages faster than a male tsetse fly. Our tiny-winged friends hit their teenage years by week two or so. In contrast, technology ages by the nanosecond.



I think the reason why many people use VPNs is the same reason hackers infiltrate them so easily. VPNs are old technology. They have long been the go-to solution for providing remote access to industrial control systems (ICS) and other critical infrastructure.

They were born during the rise of the internet late last century. One solution begets other problems. The world wide web went from 3 million to 16 million users between 1990 and 1995 (today, there are 5.45 billion users, around 67% of the population).
As a result, a group led by Microsoft sought a solution to growing security concerns. That's how VPNs were born.

To be fair, there are ways to make VPNs secure, but the enormous expense doesn't make financial sense for most companies.

Here are three reasons why VPNs cause concerns when protecting an IIoT network:

1. **VPNs have outdated authentication models. Username and a password is all you need. I can get into a VPN easily.**

2. **VPNs are a single point of failure. If something goes wrong with the server, you can't get in. If I'm a hacker, the best way to take down every remote access in the world is to take down the VPN server.**

3. **VPNs are hard to monitor. The actual traffic on the network makes it hard to identify nefarious activity flying across it.**

Let's say you have this machine on the edge (edge is simply the source of where your data is – this might be where oil is drilled in upstream oil and gas, for example). The data is being processed on that machine (edge computing) and is connected to the corporate network via a VPN. A disgruntled employee leaving the company can sit in their car and use their username and password to access the device through a cellular system. What is the potential damage?

In 2020, several prominent VPNs experienced critical vulnerabilities that allowed attackers to bypass encryption and access systems. The Colonial Pipeline attack, for example, was traced back to a legacy VPN, according to then CEO Joseph Blount. The East Coast company paid hackers $4.4 million to restore service quickly.

FREEWAVE

VPNs create easy targets. Once you're in, you have free rein to do what you want.

Solving the Challenge to Scale Network Security
A report by McKinsey and Company predicts 50 billion devices will be connected to the IIoT by 2025. The pace of change, according to the report, has increased tenfold. This means the risks and insecurities behind VPNs for organizations, especially remote industrial leaders, are rising.

I talked to a large agricultural company recently that uses a VPN. Here's how the conversation went:

Them: How can we add 20,000 sites to our system?

Me: We'd have to add 20,000 VPNs.

Them: Wait, what?

Me: It's really difficult. VPNs are hard to scale. One VPN is one thing, but many VPNs are a nightmare.

We believe a better way to secure a network is to use Zero Trust Network Access (ZTNA). ZTNA creates a network fabric using the principle of least privilege access (PoLP). The premise: trust no one. Each user accesses only the data they need.

See how the lens flips from inside out to outside in? In a ZTNA, each user has a policy. This means they are authenticated for access to specific areas.

The disgruntled employee mentioned earlier? They cannot go anywhere in the fabric without authorization. Even better, that user's access can be easily removed or revoked. Ever after, they will never be able to access the network.

Compare propagating VPNs to scale a network versus using Zero Trust.

Imagine a house. With a VPN, once you get past the bolts on the front door, you can go to any room in the house. But what if every room has a locked door – on both sides of each door? This goes for machine-to-machine (M2M) communication too. With ZTNA, devices must be authorized (or authenticated according to policy) to "talk" to another device or the server.

The policy set for each user, device, or process dictates entry into each locked door. With a single policy, a user (let's call her Diane) can access 20,000 locations across this network fabric. You can even get more granular. If you only want Diane to enter the living room and use the bookcase, but not sit in the yellow chair, you can create network segmentations that define access to that level of detail.

Modern CEOs, ROI, and Business Resiliency
ZTNA is how the modern company sets the stage for scaling the network, protecting the network, and building an impenetrable fortress rather than an air castle vulnerable to attack. This is why FreeWave will not allow VPNs on our data platform. This outdated technology is not the trusted choice of the network.

There's a financial risk to network vulnerabilities. C-level executives I talk with readily admit that the ROI on Zero Trust is hard to quantify unless something goes wrong. However, it's damn expensive when it does. ZTNA is an insurance policy for business resiliency.

FREEWAVE

You don't want to join the 45% of PwC's CEOs who believe their organization won't be around in 10 years. Also, companies pay a lot of money for cybersecurity insurance. If they can prove, down to the granular edge, that their network is more secure, insurance costs go down.

I hope you've found this article to be helpful. Today's resilient leaders know the risks and resiliency of their businesses, and that includes network security.

To recap, while many businesses have long used VPNs to create a secure connection and gain remote access to industrial control systems and other critical infrastructure, the technology hails from the last century. VPNs use outdated authentication models, provide a single point of failure, and are challenging to monitor. Also, a VPN network is not scalable. In contrast, ZTNA creates a network fabric using the principle of least privilege access: trust no one and protect everyone. ZTNA grants each user access to only the data they need through a predetermined policy. Security with a high level of granularity reduces risk across the entire network, thereby protecting people, sensitive data, and the business.

CONTACT US TODAY →

FREEWAVE

FreeWave Technologies, Inc.
5395 Pearl Parkway, Boulder, CO 80301
866.923.6168 info@freewave.com

Made in the U.S.A. www.freewave.com