Podcast Transcript

EPISODE #225

The Death of the VPN: Moving Toward a Zero Trust Future

Published January 13, 2026 • Runtime: 24:01

https://myweirdprompts.com/episode/vpn-zero-trust-evolution/

EPISODE SYNOPSIS

In this episode, Herman and Corn dive deep into the rapidly changing landscape of remote connectivity, questioning whether the traditional corporate VPN is finally reaching its expiration date. As businesses move away from the "castle and moat" security model, the duo explores the technical inefficiencies of "tromboning" traffic and the rise of more elegant, high-performance alternatives like WireGuard and Tailscale. From the granular security of Zero Trust Network Access to the invisible "ghost bridges" of software-defined perimeters, this discussion provides a comprehensive look at how modern enterprises are securing their data without sacrificing speed. Whether you are navigating legacy technical debt or implementing a cutting-edge SASE stack, this episode offers essential insights into the future of how we connect to work.

DANIEL'S PROMPT

Daniel

Hi Herman and Corinne, I'd like to discuss the continued use of VPNs for remote connectivity. While newer technologies like Tailscale and Cloudflare are available, traditional VPNs are still common in many industries. There seem to be various levels of security for remote work, ranging from highly restrictive models using company-issued hardware to more flexible access for general tools like CRMs. Are classic hosted VPNs on corporate networks still a prevalent model, or are they being phased out in favor of alternatives like software-defined perimeters and zero-trust networks?

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. We are coming to you from our usual spot here in Jerusalem, and I have to say, the weather has been surprisingly crisp this morning. It is one of those days where you just want to sit with a hot drink and talk about something complex.

Herman

Herman Poppleberry at your service, and I have my tea ready, Corn. I am very excited about today because Daniel, our housemate, sent us a prompt that really hits on something I have been obsessing over lately. He was telling us about his sister, who is a high-level lawyer in London, and how she still has to use these old-school corporate Virtual Private Networks to get anything done.

Corn

Right, and it struck him as a bit of a dinosaur technology. He is seeing all these newer, shinier tools in the tech space like Tailscale and Cloudflare, and he is wondering why the corporate world is still clinging to the old ways. Are we seeing a slow death of the classic hosted Virtual Private Network, or is it just that the alternatives are not as robust as the marketing makes them out to be?

Herman

It is a classic tension between the old guard and the new school. And honestly, it is a perfect follow up to what we discussed back in episode one hundred fifty-one when we were looking at why gigabit internet sometimes feels so slow. A lot of that comes down to how your traffic is being routed, which is exactly what a Virtual Private Network handles.

Corn

Exactly. So today we are going to peel back the layers on remote connectivity. We will talk about the traditional hub and spoke model, why it is still the standard in industries like law and finance, and then we will dive into this newer world of software defined perimeters and zero trust architecture.

Herman

I love this because people often use the term Virtual Private Network to mean two very different things. There is the consumer version where you hide your location to watch a different version of a streaming service, and then there is the corporate version which is about extending the office network to your house. We are focusing on that second one today.

Corn

Right, the corporate tunnel. So Herman, for those who might not be deep in the weeds of network architecture, let us start with the classic model. When Daniel talks about his sister logging into a company hosted Virtual Private Network, what is actually happening on a technical level?

Herman

Think of it like a physical tunnel. In the classic model, the company has a big, expensive piece of hardware sitting in their data center or their main office. This is the gateway. When you are at home, you run a piece of software that creates an encrypted connection directly to that gateway. Once you are in, your computer acts as if it is physically plugged into the wall at the office. You get an internal office IP address, and you can see the printers, the file servers, and all the internal tools.

Corn

It is the castle and moat analogy, right? The office is the castle, and the Virtual Private Network is the drawbridge that lets you over the moat.

Herman

Precisely. But here is the problem with that model in two thousand twenty-six. The castle is empty. Most of the tools we use now, like our Customer Relationship Management software or our email, are not actually in the office. They are in the cloud. So, if you are using a classic Virtual Private Network, your traffic goes from your house, all the way to the office, through their security stack, and then back out to the internet to reach the cloud service.

Corn

That sounds incredibly inefficient. It is like if I wanted to send a letter to my neighbor, but I had to drive it to a central post office in another city first just to have it stamped and then drive it back.

Herman

That is exactly what we call hair pinning or tromboning. It adds a massive amount of latency. If you are in Jerusalem and your office is in London, but you are trying to access a cloud tool hosted in a data center in Germany, your data is doing a massive, unnecessary loop. We are talking about adding maybe eighty to one hundred fifty milliseconds of delay to every single request.

Corn

So if it is that slow and inefficient, why is Daniel's sister still using it? Why are law firms and banks still buying these big hardware boxes?

Herman

Because the castle and moat model is very easy for a compliance officer to understand. If you are a lawyer, you are dealing with incredibly sensitive data. The classic model gives the IT department total control. They can see every single packet that goes through that gateway. They can log it, they can inspect it, and they can shut it down instantly. It is a single point of failure, yes, but it is also a single point of control.

Corn

That makes sense from a legacy perspective. But Daniel mentioned these other levels of security. He talked about level one being total lockdown, no remote access, and then moving down to more flexible models. It seems like the classic Virtual Private Network is trying to bridge that gap, but maybe it is failing the user experience test?

Herman

Oh, it definitely is. And it is failing the security test too. Gartner actually predicted that by twenty twenty-five, seventy percent of new remote access would move away from Virtual Private Networks toward something called Zero Trust Network Access, or Z-T-N-A. This is where tools like Tailscale come in. Tailscale is built on a protocol called WireGuard. And Corn, I know you appreciate elegant code. The traditional Virtual Private Network protocols like Open V-P-N or Internet Protocol Security are massive. They have hundreds of thousands of lines of code. WireGuard is only about four thousand lines.

Corn

Four thousand lines? That is tiny for something that handles encryption and networking. I assume that makes it much easier to audit for security vulnerabilities?

Herman

Exactly. And because it is so lean, it is incredibly fast. But the real magic of something like Tailscale is that it is a mesh network. Instead of everyone connecting to a central gateway in an office, every device connects directly to every other device. If I want to access a file on the office server, my computer talks directly to that server. No tromboning.

Corn

Okay, so if I am an IT manager, why would I not just switch everyone to a mesh network tomorrow? If it is faster and the code is cleaner, what is the catch?

Herman

The catch is the shift in philosophy. This brings us to what Daniel asked about regarding zero trust. In the old model, once you are across the drawbridge, you are trusted. You can often wander around the castle. In a zero trust model, we assume the network is already compromised. Just because you are connected does not mean you get to see everything.

Corn

So it is more like having a key that only opens one specific door, and every time you want to move to another room, someone checks your ID again?

Herman

Spot on. Every single request is authenticated. Your identity, your device health, your location, and the time of day are all checked before you get access to a specific resource. This is what we call a software defined perimeter. The resources are effectively invisible to the public internet until you have been verified. It is the difference between a big front door and a school buzzer system where you are stuck in a glass vestibule until they verify your face and your ID.

Corn

I can see why that is appealing. It moves the security from the network level to the identity level. But let us go back to Daniel's tiers. He mentioned that for things like a Customer Relationship Management tool, people just log in through a web portal. That feels like level four, the most relaxed. Is that actually secure, or are we just sacrificing security for convenience there?

Herman

It can be very secure if you use something like Cloudflare Access or what people call an identity aware proxy. Instead of a Virtual Private Network, you put a gatekeeper in front of the web application. When you go to the Customer Relationship Management website, it redirects you to your company login page. Once you authenticate, the gatekeeper lets you through. The advantage here is that the user does not have to launch any special software. It just feels like using the regular internet.

Corn

So, it sounds like the classic Virtual Private Network is being squeezed from both sides. On the high end, you have zero trust and software defined perimeters for deep system access, and on the low end, you have identity aware proxies for web apps. Is there actually a middle ground where the old school Virtual Private Network still makes sense?

Herman

There is, and it usually comes down to legacy software. Think about an old accounting system from fifteen years ago that was never designed to be on the web. It uses weird ports, it is finicky, and it expects to be on a local network. Moving that to a zero trust model is a nightmare. It is much easier to just put it behind a traditional Virtual Private Network and call it a day.

Corn

So it is technical debt. We are keeping these old tunnels open because we are still running the old engines.

Herman

Precisely. And there is also the factor of specialized hardware. Daniel mentioned company issued hardware in his prompt. In some industries, like defense or certain parts of the medical field, they do not just want a secure connection; they want a secure device. They want to know that the physical laptop has not been tampered with. A lot of traditional Virtual Private Network solutions are bundled with device management tools that give that level of assurance.

Corn

I remember when we did episode two hundred twenty, we talked about private Domain Name Systems and how that adds another layer of security. It seems like the modern approach is more like a stack of different tools rather than one big hammer like the Virtual Private Network used to be.

Herman

That is exactly right. It is defense in depth. You might use a private Domain Name System to prevent your employees from accidentally visiting phishing sites, an identity aware proxy for your web apps, and maybe a mesh network like Tailscale for your developers who need to get into the raw servers. This whole stack is what the industry now calls S-A-S-E, or Secure Access Service Edge.

Corn

But does that not make life much harder for the employees? If I have to remember four different ways to connect to four different things, I am probably going to find a way to bypass it.

Herman

That is the big risk. We call it shadow I-T. If the official security tools are too slow or too annoying, people will just start using their personal Dropbox or messaging sensitive info over unencrypted apps. This is why the shift toward things like Tailscale is so popular in tech companies. It is almost invisible to the user. You just turn it on, and everything works.

Corn

I want to go back to the idea of the software defined perimeter for a second. Most people probably have not heard that term, but it sounds like it is the real successor to the Virtual Private Network. How does it actually work in practice? If I am a user, what do I see?

Herman

From your perspective, you might not see anything. You just open your browser and go to an internal address, like project-alpha dot company dot internal. The software on your computer talks to a controller in the cloud and says, hey, Corn wants to see Project Alpha. The controller checks if you are on a company laptop, if you are in a safe country, and if your password was entered correctly. If all checks out, it creates a temporary, encrypted path just for that one session.

Corn

So the path does not even exist until I ask for it?

Herman

Exactly. It is like a ghost bridge. It appears when you need it and vanishes when you are done. This is much more secure than a classic Virtual Private Network because in the old model, the gateway is always there, sitting on the internet, waiting for connections. And if there is a bug in that gateway's software, hackers can find it. We saw this in twenty twenty-four and twenty twenty-five with some massive zero-day vulnerabilities in Ivanti and Fortinet gateways. Once a hacker gets through that front door, they have the keys to the entire castle.

Corn

That is a powerful shift. It is moving from a static defense to a dynamic one. But I wonder about the cost. For a small business, setting up a zero trust architecture sounds expensive and complicated compared to just buying a router with a Virtual Private Network feature built in.

Herman

It used to be, but the market is changing fast. Companies like Cloudflare offer a free tier for their zero trust services for up to fifty users. For a small business, that is actually cheaper and easier than maintaining a hardware Virtual Private Network. The real barrier now is not cost; it is knowledge. Most IT managers were trained on the old model, and it takes time to unlearn those habits.

Corn

It is that classic thing where nobody ever got fired for buying the industry standard, even if the standard is getting a bit long in the tooth.

Herman

Exactly. But let us look at the performance side again because I think that is what Daniel was really picking up on. When his sister is working from London, the latency is a productivity killer. In a world where we are doing more video calls and working in real time on shared documents, even fifty milliseconds of lag makes a difference.

Corn

It really does. It is the difference between a tool feeling like it is on your computer and feeling like you are reaching across the ocean to touch it.

Herman

And that is where the modern protocols win. Because they are designed for the modern internet, they can handle things like switching from your home Wi-Fi to a cellular connection without dropping the tunnel. If you have ever used an old Virtual Private Network, you know that if your internet blinks for one second, the whole connection crashes and you have to log in all over again.

Corn

That is the worst. Especially when you have two factor authentication and you have to find your phone every time your Wi-Fi hiccups.

Herman

It is maddening! Modern tools like Tailscale or even modern implementations of WireGuard are what we call connectionless. They do not maintain a constant, fragile state. They just send packets when they need to. If your internet goes out for a minute and comes back, the connection just resumes instantly. You do not even notice.

Corn

So, looking at the landscape as it stands in early two thousand twenty-six, if you were advising a company, where would you tell them to put their resources? Is the classic Virtual Private Network ever the right answer for a new setup?

Herman

Honestly, for a new company? Almost never. If you are starting today, you should be building on a zero trust foundation. Use identity aware proxies for your web apps and something like Tailscale or TwinGate for your infrastructure access. The only reason to go with a classic hosted Virtual Private Network is if you are forced into it by a very specific regulatory requirement that hasn't caught up with the times yet.

Corn

What about the security sensitive roles Daniel mentioned? The diplomats, the high level security officials. Surely they are not just using a web proxy?

Herman

Those are the interesting edge cases. In those worlds, they often use something called a double Virtual Private Network or an obfuscated tunnel. They might run a traditional, highly audited government Virtual Private Network inside another encrypted tunnel. They are less worried about latency and more worried about state level actors trying to see where their traffic is going.

Corn

So for them, the inefficiency is actually a feature. It is about creating so many layers of noise that it is impossible to see the signal.

Herman

Exactly. But for ninety-nine percent of us, including lawyers like Daniel's sister, that is overkill. She would be much better served by a modern zero trust setup. It would be more secure because it would limit her access to only what she needs, and it would be much faster because it would avoid that London to data center trombone effect.

Corn

It is funny how often we find that the most secure solution is also the one with the best user experience. Usually, we think of security as a series of hurdles we have to jump over.

Herman

That is the big shift in the industry right now. We are realizing that if you make security easy, people will actually use it. If you make it hard, they will find a workaround. Zero trust is fundamentally about making the right way the easy way.

Corn

I think we should talk about the practical takeaways for our listeners because a lot of people listening might be working for companies that are still using these old systems. What can they do, or what should they be asking their IT departments?

Herman

Well, the first thing is to understand what you are actually using. If you find that your connection is slow, try running a speed test with your Virtual Private Network on and then with it off. If the difference is massive, you are probably experiencing that hair pinning effect. You can ask your IT team if they have considered a split tunnel configuration.

Corn

Split tunneling. We should explain that. That is when only the work traffic goes through the Virtual Private Network, and your regular internet browsing goes out through your home connection, right?

Herman

Exactly. It is a huge performance boost. Some companies disable it because they want to filter all your traffic for security, but many are moving away from that because it is just too much of a burden on their network.

Corn

Another takeaway is for the small business owners or freelancers. You do not need to be a giant corporation to use these tools. You can set up Tailscale on your home computer and your laptop in about five minutes, and suddenly you have your own private, secure network that works anywhere in the world.

Herman

I use it to get to my home server when I am out at a cafe here in Jerusalem. It feels like I am sitting right at my desk. It is a game changer for productivity.

Corn

And what about the privacy aspect? We should probably touch on that because a lot of people use Virtual Private Networks for privacy. Does a corporate Virtual Private Network actually protect your privacy from your employer?

Herman

Oh, absolutely not. That is a huge misconception. In fact, it is the opposite. When you are on a corporate Virtual Private Network, your employer can see everything you are doing on that connection. They are the service provider. If you are browsing the news or checking your personal email while connected to the office tunnel, they can potentially log all of that.

Corn

So the rule of thumb is: work stuff on the work tunnel, personal stuff off it.

Herman

Always. Never assume privacy on a company managed connection.

Corn

This has been a really enlightening deep dive, Herman. I think it is clear that while the classic Virtual Private Network is not going to vanish overnight, its days as the king of remote work are definitely numbered. The move toward identity based security and mesh networking is just too powerful to ignore.

Herman

It is an evolution, not an extinction. We will see these old gateways hanging around in server rooms for another decade, but they will be the exception rather than the rule. The future is invisible, fast, and built on zero trust.

Corn

Well, I hope that gives Daniel some good ammunition for his next conversation with his sister. Maybe he can convince her firm to upgrade to something from this century.

Herman

Or at least get them to stop tromboning her traffic through London when she is trying to work from a beach somewhere!

Corn

Exactly. Well, before we wrap up, I want to say a quick thank you to everyone who has been listening. We have been doing this for two hundred twenty-four episodes now, and the community that has grown around My Weird Prompts is just incredible.

Herman

It really is. We love getting these prompts from Daniel and from all of you. It keeps us curious and, honestly, it gives me an excuse to read way too many technical white papers.

Corn

If you are enjoying the show, we would really appreciate it if you could leave us a review on your podcast app or on Spotify. It is the best way to help other curious people find the show. You can find all our past episodes and a way to get in touch with us at our website, myweirdprompts dot com.

Herman

And remember, we are on Spotify as well, so you can take us with you wherever you go. Just maybe don't listen to us over a slow corporate Virtual Private Network if you can help it!

Corn

Good advice, Herman. Thanks for the deep dive today. This was fascinating.

Herman

Any time, Corn. I am already looking forward to the next one.

Corn

Alright everyone, that is it for this episode. Thanks for listening to My Weird Prompts. We will be back next week with another deep dive into whatever weird question crosses our path.

Herman

Stay curious, everyone!

Corn

Bye for now.