ceocfointerviews.com

Issue: November 4, 2019

Managed Security Service Provider, Trusted Internet using VPNs is protecting Home and Business Computers from Cyber Attacks

Jeffery Stutzman
Founder

Trusted Internet
www.trustedinternet.io

Contact:
Jeff Stutzman
800-853-6431

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Stutzman, according to the Trusted Internet website, when you are connected, you are protected. What is your approach to making that happen?***
Mr. Stutzman: One of the things that we do is with every customer we go in with something that we call a reference framework. If you need architecture as a standard framework that we built up and use, it automatically will connect you to our ability to monitor and protect and do all the things that you probably would never even think about doing. One of the things that I tell people is this reference framework is exactly the same way that I protect my own family.

My wife received an extortion email the other day where someone wanted $900 from bitcoin from her. She called me frantic, it was 8:30 am and I was on the road. Because of the way that we've got this thing set up, we were able to log in and find out that there really was no malware on her computer as the extortionist had suggested. Even though she does not always listen to what I have to say, in this case she was very happy. There are two ways this can happen, if you are a company we can come in and put our architecture in your company, it snaps into place or snaps out, whichever way you prefer. Typically they do not like to snap it out.

The old AOL model was one that I had fashioned this company on when we first started, where you would get a CD in the mail and you would plug that CD in, and AOL would log you into its own back end, and on the back end there was a lot of security people that were watching what you did. With us, if we do not put in our architecture, we can set you up with a VPN that automatically brings you into our environment so no matter where you are as long as you are operating in the VPN, we are monitoring and protecting you. We can do that for a small office, for an individual, we can build you burner telephones so if you travel overseas you can throw the phone away on the way home. There are a lot of different ways but the idea is that once you are connected to us, you do not have to think about it; we got this.

CEOCFO: ***Are people understanding what you do when common thought is a cloud solution is good? Do people care how you do it as long as they are protected?***
Mr. Stutzman: We get it both ways. We get people that do not have any idea what security means but they are hearing the story about ransomware on the news and they will call us. In fact, that was a proposal, I just got a call from an entrepreneur that has a couple of locations but he said he did not want to take a chance, that he could not afford to take a chance, so those are things that we just jump into and we do it. Now the other ones are folks like defense contractors, healthcare providers, where there is maybe a compliance fee.

If you are a doctor you do not want to think about security, you just want to be a doctor. We will get the calls, in fact, we have a couple of dentists also, but we will get those calls where they will say that they want us to do it and they do not want to think about it. We like those calls. Sometimes we get the third one where they have actually had a real problem. Last year we paid out an enormous ransom for a company that was losing tens of millions of dollars a day and that is the third scenario, they call us when it is too late.

CEOCFO: ***We have interviewed many security companies and rarely does someone offer an external device. Why is it important to provide that option?***
Mr. Stutzman: There are two ways that you can do it now. An external device is nice because it gives us local access and speed. I will tell people that I am like the guy that is going to stand between them and the UPS guy, so the UPS guy is going to show up my house and hand me a package and I am going to look at it and check the addresses and make sure that they are valid, I can shake it and smell it and make sure it is not a bomb, and if I think it is bad I can get rid of it before you even know. When you talk about the local devices, it is always a privacy discussion, so you have to come back to the idea that we are not there to violate you privacy, we are there to make sure you do what you do safely. I do not care what you do, I just want to make sure you do it safely.

The other flavor, are the folks that just want to be able to plug into something in the cloud and go. For example, I love the idea that Comcast and AT&T are going very large, so if you login into AT&T you are going to have a VPN. You are one of millions of customers, you are not necessarily going to get what you need but you are going to get something that is good. That is one of the big differences about the way we think about security. You can login to the cloud, you can get it that way, you can get a box that is on-premise, or you can VPN to us just knowing you are going to get the box.

The value proposition that we bring to the table is we are going to bring a high level of skill, a high level of knowledge all with experts and all certified. We can give you the standard fare MSSP or we can give you the high-end managed detection and response with that level of knowledge at a price that most small companies can afford. My service starts at $549 a month."- Jeffery Stutzman

CEOCFO: ***Why is a VPN not just another layer that can be penetrated?***
Mr. Stutzman: I want you to think about culvert pipe under the road, so a culvert pipe is typically steel or concrete shaped like a pipe and it is designed to move water under the road to wherever you want to move it and keep it safe. The challenge is that you can go out and buy a VPN for $10 a month today. However, when you think about that culvert pipe and you thought about whether or not it would be safe to crawl through that culvert pipe, would you actually get on your hands and knees and crawl through a culvert pipe not knowing if there was an alligator or snake coming in from the other side? The way that I talk about VPNs is they are a great layer of security but VPN has to be terminated at a place that is monitoring it to make sure that no alligators or snakes get in. That is one of the big services that we provide, so we do not put people on some of the big VPN providers that you can buy for $10 a month that puts you on where you are going to be safe.

The other way to explain it is, if I set up an architecture for you to be safe, I have a proposal here for six homes and in one case I am putting a big firewall in one of the homes and I am going to have the owner on a VPN, and no matter where he goes he is going to come back to that same firewall. From the way I think about it, a VPN is another layer of security that you have to have to make communications as tamper proof as possible. You have an antivirus, a managed input solution, and something that is an anti-evasion on every computer, as well as a VPN client. You have a firewall that gives me the ability to terminate a VPN client, do malware analysis, do antivirus, and then you have a VPN, so why do you want to use a VPN if you are inside of the house? When you are traveling or sitting in Starbuck's or a hotel, there is not a hotel in the world that is not compromised. I tell people that I am going to set them up with a VPN that is going to bring them back to our environment and give them the same level of security that no matter where they are, as it would be in their home or office. For me it is a required additional layer of protection but not the only layer of protection.

CEOCFO: ***What is your geographic range today?***
Mr. Stutzman: I have clients in London, I have one going in Mexico as we speak, but are primarily in the US. We have two installs that are going in Switzerland; we have one that is scheduled for Monaco and another for Milan. We have partnered with a couple of really good security companies so if they are out in the field and they find out that there is a geopolitical risk that is going to create some kind of a cyber problem or someone has had a problem, almost no matter

where they are we can deliver a box within a couple of days and have it installed, and then everything else is done remotely. Predominantly right now we are US, but we are expanding globally very quickly.

CEOCFO: ***How are you reaching out and how would people find Trusted Internet if they are looking for something better. How would they you can provide safety?***
Mr. Stutzman: It is funny because we have not really done a lot of marketing and almost everything we have done is by word-of-mouth and we get referred in by attorneys and we get referred in by security companies. We have great partners in the D.C. area that tell everybody about us, so that channel strategy has been paying off. It was good because I was a bootstrap company, we started in a basement, so that gave us the ability to crawl, walk, run. We are ready to scale now so we are going to start a marketing campaign probably in conjunction with one of these physical security companies. It has been through channels.

CEOCFO: ***Why is now the time?***
Mr. Stutzman: For a startup, we have had two years of building and the first year was building and proving it. The second year is stabilization and as you head into the third year, it is all about ok we are stable, we have been in the black since day-one and it is time to be able to scale out. This is kind of the normal way you go through as a bootstrap startup. One of the challenges as a bootstrap is you never want to stop selling but you cannot stop delivering. Why now? It is because we are stable and I have made an enormous amount of investments in the infrastructure this year, we have really smart people. I have literally almost kept no money for myself, and I have reinvested almost everything this year, and still profitable. It is the right time in our maturity.

CEOCFO: ***What do you look at when you are assessing what a specific potential customer might need, that a less experienced people would not think is important?***
Mr. Stutzman: One of the things that we do a lot of is try-before-you-buy program. We put up a next-generation firewall on your network behind your current defenses and in every single case we were able to show that because that other firewall might have even been a really good one, but if they are not managed then they miss a lot. One of the ways that we get most of our customers is we go in and say look why don't we just test and see what we got. We do that in a couple different areas.

We have also hired some former intelligence officers, one is a former CIA case officer and these guys have really good skills in being able to go out and identify risk to people, so we will look at the person and look at the computers. Typically I do not do pen tests because you almost see them as a waste of time because they are a snapshot in time, but that is generally the way it works, we have a good conversation and if it sounds like they have a need, then we will just say try it and if you like it, I will send you an invoice. I can count on one hand how many deals we have had where they just did not want to do that.

CEOCFO: ***What has changed in your approach over the last two years and what have you learned as the business has grown and evolved?***
Mr. Stutzman: We are a small company but we have been hypersensitive to our customers' needs since day-one. When I say hypersensitive, I mean we put them up on a private Slack channel and have clear communications with them. One of the biggest things we did was give them direct access to the analysts without making them wait for a report or a situation report. It is so much better when you can have direct one-on-one communications. The other thing, and this is a realization for me more than anybody else was that the typical small business has an internet connection and a wireless connection and that is it. It might be a variation and if it is a little bit bigger, they may have some switches in there but they typically do not have firewalls. Maybe they will have an antivirus and typically they have not chief information security officer.

Because I had come out of the government, I thought everybody had that stuff and it is really not true, they do not. The biggest thing that I have learned is to go a little lightly, I can be an intense guy and some like that and some do not. The real lesson that I have learned is that the people skills are more important than the technical skills. If I go in and make somebody feel like an idiot because they got an internet connection and a wireless device, then they are probably going to not like me very much. It is how you deal with the people, the tech is easy.

CEOCFO: ***What about delegating? As businesses grow it is hard for the founder to trust or give up some control.***
Mr. Stutzman: That has been difficult but it is a lesson that I learned a long time ago. I had fifty-six employees and until I became an entrepreneur I had never worked in an environment with less than 100 thousand computers. I came out of the navy and in 2001 I went to work for Cisco, and was an information security guy there. I then went to Northrop Grumman Corporation and worked for Carnegie Mellon twice, so in that situation, it was a one-man-show. You learn that lesson in the military, as you promote you have to learn how to delegate. That has not been difficult, what has been difficult is finding people that look at things the same way I do and knowing that I can trust them.

Secondly, I am a former navy intelligence officer and I was an enlisted guy ten years before that. My number-two is a former navy pilot and flew H60 helicopters. I have a director of security operations who is a retired air force colonel, who ran the security operations center for the air force. I just hired a guy who is a retired navy surface warfare officer, but also retired from the CIA so at least at those levels I have stacked the deck with people that I believe I can trust and know I can communicate. Because we are all former military guys, we know. The air force guys have a certain way of working and that is good, that is the place I need them to be. If I went out and took $25 million, I would 2004 with people just to fill those holes but one of the reasons I am self-funded is I can select the people that I want and I do not have to be in a rush. So that is how we do it.

CEOCFO: ***Why choose Trusted Internet?***
Mr. Stutzman: We have worked in cyber intelligence, we have worked in information work fair, we have strong organization skills and all that does not really matter but what does matter is I think that the value proposition that we bring to the table is that we have all worked in large companies, we have seen the high-end tricks, we know what the espionage threats look like, we are one of the small MSSPs that can walk in the door and treat you like a small company but have a lesson to learn from those big companies. For example, I did an incident response on a four person company in Indiana, and they make technologies for NASA, they had no idea what they were looking at but I have seen that because I worked on it when I was at Northrop Grumman. The value proposition that we bring to the table is we are going to bring a high level of skill, a high level of knowledge all with experts and all certified. We can give you the standard fare MSSP or we can give you the high-end managed detection and response with that level of knowledge at a price that most small companies can afford. My service starts at $549 a month. That is really the trick here. They need it, they can find experts and look us up online and find out who we are and we can give it to them at a price that no company can say no to.