FEDERAL TECH PODCAST

Ep. 85 When Cybersecurity is National Security

00:02
This is John Gilroy from the Federal tech podcast.

00:06
And this is Eric Trexler, Senior Vice President of Palo Alto Networks public sector.

00:11
And today we're gonna talk about how Palo Alto Networks can help your agency hit its goals. Hit the music, Manny. Welcome to the federal tech podcast. My name is John Gilroy. And I will be your moderator, I guess is Eric Trexler, Senior Vice President, US public sector, and he's also an award winning podcaster for a company called Palo Alto Networks. Eric, how are you today?

00:32
I'm Well, John, I'm well and you? Good.

00:35
You've been in business a while many of my listeners know all about your background, various things you've done putting your podcast work. What do you want us to do is is bring in today, and many of our listeners are also familiar with Palo Alto Networks, maybe you can focus a little bit more on what Palo Alto is doing today. Try to help all our federal agency people get their systems more secure. So give us maybe a thumbnail sketch of your background. And what's new for Palo Alto today.

00:58
Yeah, early in my career after I graduated from business school, I got into it started building systems and improving processes for customers. The second part of my career, I went into cybersecurity start protecting those same systems and processes. It's been an exciting run.

01:17
Great, you know, I normally have open ended questions about technology. But what I'm going to do is I'm going to use a quote to start off with, and you have to tell me who said this quote, this can be a tough one could be anyone in the whole world. So here's the quote, cybersecurity is national security, no said that.

01:33
There was an occasion roar our CEO at Palo Alto Networks, you've probably also heard me echo it a few times. Yeah, I believe in it.

01:42
So what does that mean? It means that Palo Alto is focusing on security of the whole United States and the federal government, what kind of focus Do you have?

01:50
So national security, protecting our information systems, whether public or private, is critical to our intellectual property that the way of life as Americans that we lead, I mean, this is such a critical industry, as well as rip leaves these borders. It's, you know, it's nothing but a cost to American society. We recently saw this happen with the, with the accreditation issues, on email, with Secretary Blinken going to China and in the month of June, right commerce and State Department had adversarial activity, looking at what's happening, you know, what's happening on the email schedules and things like that it was unclasp. But you know, what people are thinking, you know, where they're going, you know, what their timeframes are?

02:35
Yeah. I went to LinkedIn to prepare for this interview, I saw your background. I mean, it's fantastic background. I mean, start off as a ranger, all kinds of big organizations. And you're at a position in your career, where you're well known will experience and you wound up working for Palo Alto Networks, I'm sure they're listed, especially in the head, no. Now, why that company? I mean, he can work for any McDonald's in town for Palo Alto Networks. So give us the why. Yeah, the

03:02
sad part is I'm in this I'm in the latter stages of my career, right. I'm in the second half of my career, and I want to make a difference. I looked at where would I be able to make a difference in this industry, move the needle, I really deeply believe in America, I believe in the mission were on protecting the public sector, there was the opportunity to learn the state and local business. And and Palo Alto is the number one cybersecurity company in the world. It's got the products, the people and the scale to accomplish the mission and really move the needle when I looked at what are the other options was really hard to come up with who's number 234 and five and cybersecurity. When I talked to my peers when I talked to my friends. You've got companies that dabble in cybersecurity, it's it's a, it's a side business for them. You've got other companies that just don't have the scale and the breadth, John, to really make a dent in this problem.

03:58
I did research this morning, I went to YouTube and I saw some of your YouTube interviews, which are pretty good. And there's one they did RSA 2023. And you're talking about the number of companies at RSA and it was like you've been going to for 10 years and it's just explosive number of companies and maybes have point solutions that may fit a specific problem. But I get the question is how do you get all these birds to fly in formation? I think that's the system integrators challenge, isn't it?

04:27

I think that's the globe's challenge. We've been working on that for almost four decades the entirety of the industry. We have more and more companies with more and more capabilities. The problem is and we studied this with Steve Grossman at McAfee, something on the Grohmann curve right? Over time, efficacy of a product decreases, right desired results, the effectiveness of a product, why the adversary understands what the product is doing. And they develop, they develop workarounds. They develop ways around it. All right. So we keep buying products, we keep implementing products, we do it poorly. We've got to look to consolidation like it. We've we've got to look to platform and cybersecurity, how do we drive integrated protection systems. To do that you need scale, and you need money. And that's something we have in spades at Palo Alto with 90,000 customers and billions in the bank. And we're investing heavily, not just in today's products in problems and capabilities. But in tomorrow's.

05:30

Well, I like to talk about, you know, 3000 vendors and big companies and big problems and solutions. But a lot of times what my listeners want to a real specific is, Oh, give me a, give me a, for instance, give me a specific. And I'll give you a specific, I was listening to a podcast couple weeks back, and they're interviewing a gentleman named Shane Barney from a federal agency. And, and they said, Give me your experience with going to the cloud. And Shane said, Well, you know, before the cloud, we had 200 gigabytes a day in our logs. And we can maybe go through that pretty quickly. Today, they're getting 10 terabytes a day. So this is just one teeny little tiny aspect of the federal government. And you can see the explosion there. So so how can Palo Alto maybe help Shane here in his little dilemma?

06:13

Well, I think Shane is the CIO at Customs and Immigration Services. So they're not super tiny. But the problem is the same across the globe, that data is exploding, right? Something I've talked about for years, more than a decade, probably 15 years at this point is human and machine teaming. You'll, today you'll hear a bit talked about as machine learning, artificial intelligence, automation. In addition to consolidation, we've got to drive automation. It's not going to solve problems, like the talent gap, but it is certainly going to help us we've got to take activities, expanding logs, the Biden administration kicked out an executive order in May of 21. Enhanced logging, that's great, but then you run into Shane's problem. I get 200 gigs a day. I can't get through that. How do I do it? You've got to drive automation. Right it Palo Alto, our sock, we're down to 10 people running our sock globe for our global operation, the largest cybersecurity company in the entire world. The most attacked organization in cybersecurity, we believe 10 people,

07:24

automation. You know, when you say automation, I reflect on my students at Georgetown, and their ability to get jobs, they get scooped up pretty quickly. But but there's all kinds of openings in cybersecurity. I mean, we can talk about hundreds of you pick a number pick a number in the hundreds of 1000s 600,000 400,000 7000. And so it seems to me that maybe automation, maybe be able to address some of this issue.

07:50

It absolutely can and will and we're driving hard on it. I mentioned our SOC, right, we had three times and our projections were significantly greater than that as the company grows, we've acquired 17 companies in the last

four years. That's a lot of process. That's a lot of consolidation. We're doing this internally. We're doing it for our customers, how do you drive automated workloads so that the humans get involved in the hard problems where you need a human to make a decision. But things like logs scanning things, like looking at behaviors and doing correlation between different tool sets that can be done by machines today?

08:28
That's fine. It should be. I have a mandate from the White House. I just got it this morning. I have to say artificial intelligence and every podcaster. So it's mandatory.

08:36
I think my customers have the same mandate. But let's talk right?

08:39
Yeah. But you want some coffee? Is that artificial intelligence? No, I get a tire from my car. Okay, tire. Is that so? So? So where does it fit in with Palo Alto? Where do they view it as applying.

08:50
So we believe that this is going to be key to cybersecurity in the future. We also believe that the most the most capable companies will have an advantage in this space, just due to the cost and the amount of data, you've got to look at the sheer amount of data that you have. Additionally, there's a there's a complexity that I don't think a lot of organizations and companies understand. You can't just throw data into a model easily, and then run AI against it. Right? You've got to understand the data. One of the things we see as an advantage to us from a consolidation perspective is we have, we have endpoint, we have network, we have cloud data, it's all coming in. It's normalized, it's rationalized. We can create a pretty pretty proprietary AI model that we can use against six specific security use cases and tasks. The second you throw a third party into the mix. We don't understand their data. We don't understand their format. We don't understand the frequency of the data. There's a lot you have to learn. You start customizing, and that's where integration becomes really, really complex and expensive. Do it at the factory floor. Not the customer floor is where I keep saying.

10:06
I'm trying to assemble this interview and themes run around the back of my mind. I have a friend named Dr. Chase Cunningham. He's a podcast,

10:13
Doctor zero trust. It's a no Chase Well,

10:17
oh, he's hilarious, I think is one of the funniest guy, he should be a stand up comedian or something. I think he's hilarious. What what's fascinating is that, he talks about zero trust. And I do my research, I listen to different podcasts, and rinses one podcast where this guy in the army had no money to deploy zero trust. So

he took his existing stack and altered it to comply to the point where the red teams didn't have any problem with him anymore. And so So is it a matter of system integration? Or really what's going on here?

10:53
I think a lot of it is rethinking. And I think in a pilot, it's relatively easy to take existing technology, especially in the federal government, where we have we have deep budgets, we have a lot of technologies. And you can prove things out pretty quickly. I think when you start to go to scale, how do you scale something across the Department of Defense? How do you scale something across DHS or a component of the civilian space? Or, you know, let's say a state or an education institution or an r1? Research University? How do you scale that across 10s of 1000s, hundreds of 1000s millions of users. And that's where I think consolidation and standardization comes to play. Things need to be repeatable and predictable. We've got to drive our higher confidence and consistency, and look at reducing risk. But to do that, we've got to have systems that work together.

11:49
And, you know, when you look at look at a company called SmartCare, soft and you work with Parasoft, they do have different vendors. And it seems like you're leading, from my perspective, the whole charge on trying to get these systems to work together. And and you talk about the factory floor in the show floor and maybe the floor of the Pentagon. I mean, this is a this is a tough long term task. This isn't something you do before September 1, isn't?

12:14
It's not and there are a lot of standards out there. And there are a lot of initiatives. And the one thing I ran into John all the time, the people we work with deeply care about what they're trying to do, but they're siloed. Their budgets are siloed. The acquisition process, which we've talked about in the past, highly, highly complex, doesn't allow them to drive, drive drive initiatives that are aligned with long term strategic goals the way they think is shorter term. I think we need programs you can look at the distance Thunderdome program as an example, right? Zero trust network access, does it meet all of the 152 advanced controls? DOD CIOs office put out? No. But it meets a large number of them and protects the users in the cloud, and gives them a user experience and a security experience that's well beyond what they're getting today, through the Joint Regional Security stacks. To me, that's a great example of the government actually putting capability into play, that helps us move the needle forward, even though it doesn't give them all of the zero trust checkboxes they want. It's a great phase one and two,

13:25
and you can build on it. And I keep thinking of the the gentleman we talked about in the US Army who who they they go after Him do pen testing at BT pentesting at BT, and then he just realigned his existing stack and it seemed to have value there. And and I think that's a story that needs to be told because there are a lot of pockets of agencies that are just like that they they may not have as much money as other people or they spent their there a lot of security budget on something and and I don't know, what are the places you can learn this as Palo Alto, maybe head of school or maybe a Test Lab? Or where can people learn how to put these different disparate elements together?

14:03
So the first thing I would say is reach out, ask for help. There's a ton online, but I've got an entire team of almost 500 people focused exclusively on the US public sector that can help educate. Additionally, you mentioned Charisse off, we're about to you're going to get a scoop here. This is an exclusive John. We're about to launch an initiative. We're trying to figure out how to do it well, but we're going to launch an initiative where we're going to provide enablement classes, certification classes, to government and partners in the space to help build their knowledge of the capabilities out there because I believe if they understand their business problems, we understand technology that can solve them. When we merge the two together, we're better together today one of the biggest challenges we have is we'll get an RFP or an RFQ. For something we'll get an initiative from from, you know, from from the government. but it really doesn't talk about the business problem, what problem are they trying to solve? How are they trying to enable or protect mission? To the extent we would like, give us your hard problems is what I would say. And let us come back to you with ideas and how to solve them. Us being industry?

15:18
Yeah, I think what can happen is people can slip into technobabble and go into all kinds of variations. And and I'm sure there are people work for you who can just really go into detail on some things. But, but sometimes they kind of they miss the whole problem, don't they? And it could be something very, very small. But they're they're focused on the focus seems to because there's so many things going on and so many opportunities, what's going on? Here's the recent attack, here's his going, Microsoft has had was that mean? For me, it's just I can see how you can get become a short order cook and just be dazzled by the orders not worried about cooking any food?

15:55
Well, in many times, what we'll get is we'll talk to a to a prospect or a customer. And they were put on a project to deploy, you know, a SD Wan offering. Yeah. Okay. Well, that's great on on site to site communications, but how are you protecting your users today? What are you doing with your existing legacy VPN capability? How are you tying it into the zero trust initiative? And oftentimes, those are questions they can't answer. Right. So how do you tie in this SD Wan project into the greater zero trust initiative? Security, let's call it security initiatives of the agency, or the state or the school system? Those are the conversations I want to have. That's how we move the needle. Yeah,

16:41
that makes sense. Let's look into the future. You say you're at the midpoint, your career, we can pretty easy

16:46
to get beyond the midpoint. But I like the way you're going.

16:49

Yeah, I don't know. You're kind of a young puppy. When I look at you here on Zoom. So give me a five year plan. Eric, tell me what's going to be in five years. What do you see the just transition taking place not to think there's going to be a big incident. What do you think's going to happen next five years?

17:04

Well, we're going to continue to have incidents, we have yet to see the catastrophic incident that changes the industry. And I'm not quite sure that's ever going to come at this point in my career Early on, I think I was naive enough to believe it. But what I'd like to see is as the largest cybersecurity company in the world, I mean, we came out in 2010 ish, with the next gen firewall, and nobody said would work. We basically brought IP URL filtering, excuse me, an intrusion detection to the firewall. Over the next decade, we took out entire industries, if you remember sandboxing, from the 2020 timeframe, DNS security, we have customers with it ot problems. It's a feature in the firewall right now. DLP, Caz B, you know, remote access problems, swigs software, web gateway, remember the Bluecoats of yesterday? Right? SD Wan problems, were just consolidating them as features into the platform, which is cloud, virtual or physical. Wow. Right. And that's the bulk of our business today. What I'd like to see tomorrow to directly answer your question is really automating the SOC. I think that is the next we really believe that soc. Automation is the next big area in cybersecurity. Because, as Shane said, it's CIS. Right? The data is just growing. The executive order mandated they collect more data, how do you automate that? How do you get to security, John, which is what we care about,

18:36

you're backed up against a wall, you can't hire new people, you have goals you have to achieve. And so you know, necessity mother invention, which you have to do is maybe apply something you don't have or automate something. Because there's, I think, with the increase in volume here, there's no choice this has something has to rise to the top here, because if not, you're you get fired. Well, you're not gonna reach any goals and get attacked,

19:01

or your agency or school or state government is at risk or your commercial industry, your commercial business. So we did it with the next gen firewall, we revolutionize the industry along a whole bunch of those. I mean, those were entire companies. If you think about the sandboxing industry, there were half a dozen companies in that industry, with products and keep, it's a capability now you just license it and go. It's on the existing platform. It's not a new contract. Maybe it's an addition to a new contract. It's a little new training, but you're teaching you're working with the same people. Yeah, it's over layering, lead layers of security, which goes back to defense in depth, not vendor in depth. It's integrated on the factory floor. We're going to do it again for security operations. That's our aspiration.

19:48

What we'd like to have you back in six months and maybe switch around the federal tech podcast to look at sled look at state and local and what are they doing? And I used to make the argument that you know, more malicious actors would go after the federal agencies and just go after the state of Ohio. But I think what's happening having a C shift now is taking place. I think there's a lot of innovation taking place and people working in state local governments with the federal government. I think this is a topic that works on both sides.

I think the Fed should know what's going on. And a lot of state and local people are have some great stories to tell about innovation and breakthroughs. And in you know, the same thing. We don't have any people winning money, and all of a sudden we put something here that seems to work. I think it's a great story for six months down the road.

20:29
It's a fascinating topic. I'd love to talk to you about it. It's been eye opening to me in the last year. These are people who are protecting hometown America. Yeah. And they don't have the budgets, they don't have the staff that the feds do. They don't have the protection. Ransomware ransomware actors are coming after them constantly. And they do better security than certain components of the federal government because they have to, they don't have the budgets and the people. So they've got a turn to industry. And I've seen I've seen some amazing organizations at the state, the local, the tribal, the education level, where they're doing amazing things with with few resources. It's a great story and young

21:11
people and the most that's no I was born and raised here. Now I was born raised in Colorado, and no one's coming after me. It's a it's personal with these people and and they get very How can the government help me? Attached? Yeah, it's that's it's that's how I think that's, that's kind of all American is. Yeah. Well, you may attack some guy in the Pentagon, but this is me, you're coming after I'm gonna, I'm gonna use everything I can. And I, the I'll take this paperclip and this duct tape, and we'll figure it out. And they do and I just the stories are coming out of state and local are starting to wait a minute, you know, this is the maybe the big dog can learn from the little talk here.

21:45
I was talking to the CIO of the state of the great State of Alaska. And we were talking about some of his challenges. And he said, Eric, you've got to understand in some places my IT leader runs the snowplow. Most of the time. Yeah, he's got to make it simple. It's got to be effective and simple. Witch my mantra with my people is always streamline and simplify. Like how do we make cybersecurity more simple, small town America state local is a great place. It's a great place to talk about love to talk more.

22:19
Good, good. Complexity is the enemy of success. Some people okay, let's, let's send this up here. You've been listening to fiddle tech podcast with John Gilroy. I'd like to thank my guest, Eric Trexler, Senior Vice President, US public sector and an award winning cyber street podcaster and he's at Palo Alto Networks. Thank you, Eric.

22:37
Thank you, John. It's been great getting back together and chatting with you.