FEDERAL TECH PODCAST

Ep. 52 Cloud security for large federal organizations “If it’s reachable, it’s breachable”

00:04
Welcome to the federal tech podcast where industry leaders share insights on innovation for the focus on reducing cost and improving security for federal technology. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcast.

00:28
Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Our guest today is Steve Kovac, Chief Compliance Officer and Head of Global Affairs for a company called Z scalar. That's zsC a l e r.com. Very easy to find. And today, we're going to talk about the really quick success here of Z scalar. And, and what impact it has in the federal government, how Z scalar can help my listeners achieve their goals here in 2023 and beyond. But before we begin, Steve, you're calling in from California, maybe you can give us a quick little summary of what Zscaler is, especially from the perspective of our federal listeners.

01:02
Well, thanks, John. And great to be here and great to talk to your listeners. So I'll tell you a fun fact you said these guys, you spelled it out, it made me think of an old fun fact that a lot of people don't know what CCR stands for. So it's the zenith of scalability. And the whole concept around the dhisco, when it first came out was the ability to get security delivered in in the cloud. And I call it native cloud. So born and bred in the cloud security, delivered out to our customer base and get rid of what you might call the legacy castle and moat perimeter based security. And by doing so, if you get rid of the appliances, and you get rid of all these backhauling all the users back to your perimeter or back to your corporate or agency and then going back out, which creates this big hairpin by going to the cloud and making the cloud the first hop, and providing security services in the cloud. By doing that to the cloud, you can provide faster service. And we can provide faster updates, patches, all those things that the cloud brings into what we call it the cloud effect, being able to service our customers, and be able to respond quickly to security threats anywhere at the globe, anytime within seconds. And giving that same experience to every user, something you could never do in this perimeter base Kassala moat environment of the past. So but if you do that, you have to be able to scale. And so that's where concept D scalar came from was for us to be able to scale that service on a moment's notice. And you'd be brought up our growth and I'm gonna quiet periods, I can't speak about our earnings or things like that. So please forgive me. But that's what's had what's given the scale or the ability to grow at the pace we have, because you can roll Z scalar out anywhere in the world in a matter of hours, days, depending on your own capabilities. It's because we're cloud based, because it's a software based system. You're not shipping boxes, you don't need Patch Tuesday, right? You're just Z scalar just becomes the first hop within in the cloud anywhere you are on the planet.

03:01
Well, I'm kind of competitive here. And you start off with a fun fact that I didn't know. So I'm have a fun fact myself. I'll tell you a fun fact here about Zscaler. Let's see if you know this one steep 275 issued and pending patents. Really, I mean, it's hard to get this one patent. But 275. When you get some brainiacs out there headquarters, that's really an accomplishment.

03:21
Yeah, I think that's the key of Z scalar. First of all, we'll talk, I'll go back to that a second. Our culture, you know, is, you know, we really try to focus on, you know, bringing in the elite people to run a culture of delivering elite sort of products and services. And matter of fact, just yesterday, I was at our corporate office at Wired swam out in California, and one of our customers, one of our federal customers was here for an EVC. And they walked out the hall of the EDC room Executive Briefing Center, and on the wall is all the patents, and I was just watching this this customer, and he was from, you know, what are the x labs, I'll just leave it at that. And the, on his face, and he looked at all his patents. So it is a tremendous accomplishment, you know, I take my hat off to, to my brother and at the company that do that for us. You know, it's not none of them have my name on them. But that's okay. They made them happen, make it work. And that's key, right. Making sure our technology is is always becoming, you know, best of breed.

04:19
You know, I've done a lot of interviews, I've interviewed the people at the Air Force Research Labs, I think that is brainiacs and the government, they're really smart, beating people up at NIST, but everyone, especially the physics majors, they respect patents because that means something innovative that no one else has. I think that may be a key to some of the secret sauce that Zscaler can provide to the federal government. And I don't I'm not let you off the hook. I got a number three fun fact another free font pack, here comes a ready Point of Presence. Zscaler has something like 150 points of presence all over the globe. I mean, that must be in a neighbor if you to provide zero trust to the federal government. Is that right?

04:53
It is in some sense. It's more of you know, to bring this into perspective, the 150 data center is to provide service to our global customer base, I'd like to keep it at that. And I will get the second part of that in a second. So the idea around having this 150 days as our own is that no matter where you are in the world, whatever country you're in, we want that first hop to be quick. So we wanted to get you on the network and be able to get get get you on the network, get to the cloud, and get to us first hop to as quick as possible to obviously reduce latency and make the user experience better. That's wonderful. But in the federal world, we have requirements around us boundaries, US citizens, you know, so the data has to be on sovereign US soil in many cases. So we do the same for you for the federal government. But it's all based on US soil, whether it be in the US, or on a military base, or in anything that we would call sovereign US soil, we can put our cloud access point there and do today, all over the globe.

05:56
You know, I think there's a lot of impostor syndrome out there where companies would you know, they're a consulting company, and they redesigned the web Life website they put in Yeah, we do zero trust here. Oh,

okay. Sure. And we've been doing zero trust for 20 years. Okay. Sure. But, but I think the skill and the reach that your company has actually allows you to, to talk to talk and actually say, Look, this is how we're doing it. So this is this is really kind of a unique feature here in Washington DC, isn't it actually showing people how to do it?

06:25

Yeah, that mean, that's true. I mean, I frequently say in presentations that you can drive your car down to the corner market and pick up a bat box is zero trust. If you listen to the environment. RSA last year, I think every single booth at RSA said zero trust. The truth of the matter is zero trust is defined by in our world, the federal space, your trust is defined by the system. It's just the guidelines, the DoD guidelines. And I would also put in there the NIST center of center of excellence, because all three of those have really the leading say what zero trust is. And if you look out there, there's only about I think there's really one of us that does that in the cloud, and does it end to end in the cloud? And I guess you could figure out what to say that is, but yeah, at the end of the day, zero trust means a lot of different things to a lot of different people. So I don't want to, you know, disparage the thought that other companies do provide zero trust. I think the key to our success in this space is we're able to provide zero trust, and, and on every one of our products at the FedRAMP High Aisle Five levels. And that's I think that's really key. But again, I also will hinge that and say, zero trust is a team sport. I mean, you say that all the time, because not every body, including us, because the end is gonna be able to say, Oh, I just go by Zscaler box, and I had zero trust. There's still other components of zero trust yet that you have to do. You've got your, your sample connectivity, which you know, your single sign on stuff. So again, zero trust is, is a is a team sport. As I said earlier, we just were just a very big component of that sport. But you said that very

08:04

tripling of tongues like, yes, my tulips came up in the backyard, and I'm going to vacation this weekend. And oh, yeah. FedRAMP High. Now. Wait a minute. I mean, you know, we cope, Ron Burgundy, it's kind of a big deal. I mean, you know, it's hard to get FedRAMP and then FedRAMP. High, you're dealing with serious stuff here. This isn't, you know, like a walk in the park. And so I think just the fact that, you know, in the last seven years you've made to rise to that level of trust in the DOD. That's, I think that's bragging rights. Let's do that. Let's do that question. Again. You put that the front of the answer maybe.

08:37

Yeah, I, I kind of snuck that in there. So I was interesting. I was at his FedRAMP event yesterday, and over here at Google headquarters that Adi the Alliance digital government had put on. And when I was at a panel, and I was sitting next to my, one of my, my dear partners, and Troy Bertram, and Google, and we were talking about FedRAMP. And he said, Well, Steve, why don't you talk about your FedRAMP story. And you say that a company that besides the Zscaler has for FedRAMP certifications to at the moderate impact level to at the high impact level includes every part of our product set and and for zero trust, it is a huge accomplishment that our company has pulled off and I look back to the people that worked hard to get that done. I just have to take my hat off and almost you know, take a minute to just breathe in because it's it's take my hat off to read it because it is really something and you sit in a room with you know, some of the hyperscalers that don't even have high or are still struggling to get high. And the fact that you have to use high jab high products to get high. And to get the FedRAMP High certification. You realize that there aren't a lot of there aren't a lot to choose from. I was

kind of saying that to the crowd is it was like what's your biggest what was the biggest hurdle and getting to FedRAMP High and the biggest hurdle was there aren't very many people at FedRAMP High and if I want to use a third party cert It's actually FedRAMP High. So it limits to about about 10 of us that have gotten to that level. And, and that's what my buddy Google and I were saying it's because we use, obviously, we use a big chunk of Google in our solution. And we were laughing back and forth that how interesting we are to each other. Because you know, even though we're considered partners, we obviously still compete at times. And yet, we still use each other's solutions. So it creates a fun family FedRAMP world at this level, but it is a tremendous feat that I'm very proud of our company for achieving.

10:30
See if you're in California, and I'm in Washington, DC. And usually around March 8, maybe maybe this year with a warm winter, maybe I'll have the cherry blossoms pop, who knows, never know. But something else is going on here in March 8 is the public sector summit for Zscaler. And you'll be speaking down there. So if someone's listening to this and go, I want to go down and talk to Steve, you'll be down there a lot of smartphones leave down there think it's really good. So it's going to be at the Ron Reagan Building Center, march 8, near metro stop. So well, why put this together?

10:59
Key thing? It's our inaugural Summit. Wow, kickoff. It's good. Yes, absolutely. And I'm speaking but the most important is Jay Chaudry, our founder and CEO will be speaking. And if you haven't had the opportunity to hear Jay to hear his passion and his knowledge for this business, it is a absolute opportunity to get hands on experience with Jay and to get to speak with him and come down and, and learn how and why he put this whole story together. And I'm sure that the listeners, if you get an opportunity, please come see Jay, then sure I will be there, a lot of our great people at Zscaler will be there. From the engineering side to the certification side of that I'm doing, we're going to just really tell our whole zero trust story from the beginning of Zscaler, all the way through where we are in the government space today.

11:52
We got some yin and yang going on there, too. I see that at 915. Jay is going to be there. He's going to be paired with Melinda Rogers from the DOJ. So this is this is like, you know, proof of the pudding, isn't it? Yeah, we use it works.

12:05
Yeah, I think that was really important. I mean, one of the things that we focus on is getting our customers to join us. We've had a lot of great success with with DOJ, as long as many, many other cabinet level agencies, so And there'll be many of them there, you'll see many of our customers will be there. Because we do a lot of working sessions, it's really key because easier, it's not just selling something, but it's really important to educate our customers on using Z scalar. to its fullest potential, right, they've spent their whole lives working in the appliance world and they have the book, put this code in put that code in these killer has so many features in the zero trust space, that these working sessions can really open up the opportunity for people to learn so much more on how to get the most out of their Zscaler incidents.

12:49
Well, I have to admit, I am a fan of words, I study foreign languages and English language as much as I can. And one of the speakers from Zscaler is guy named Han Sang bae, and I've been reading up on him and this guy's got some great lines, you know. And one of the lines from an article that he wrote was, we talked about a cloud managed solutions versus zero trust. He said, If it's reachable, it's reachable. That's a t shirt, isn't it? Just make some T shirts and hand those out to show

13:15
we actually have features. So you do

13:18
get one man I'm walking, I got another one.

13:21
Make sure you get well make sure one thing brings you on Yonsei is a tremendous asset to our company. You know, it's great to have people that are great technologists and you know customer facing but at the same time, can do it in a way that makes our job a little fun every once in a while. And he's he's great with his one line zingers but he's in front of the customer. And explaining the car and explaining how to use your trust in rolling out zero trusted that through the agency. It's one of the best, so he's gonna be down there, I know he's speaking and gonna get a chance to hear him as well.

13:53
zscaler.com To register, I think it's free. It's easy, Metro accessible, everyone's been the Ron Reagan Building, it's it's a pretty nice place. I would be remiss if I didn't talk about our friends in the Pentagon, the DOD, you seem to have a lot of experience with helping people down there. And I'm just going to read a recent press release and let you reflect on it and tell me what you think. There's a gentleman down there, the army CIO, I think his name is Raj Iiar. And he is going to be leaving. And in his exit interview he is and this is the quote, and this is really fits into discussion. So Well, talking about moving to the cloud. He said, you know, talk about the army, and made a lot of changes in the last two years. He talks about the cloud is a perfect example. And here's his quote said, the rate at which we've implemented cloud across the army has now led us to really rethink some of the existing programs for which we had requirements five years ago. So different requirements and duplicate systems. So it's a brave new world there, isn't it?

14:51
Why do you remember what you and I almost five, five years ago when you and I last spoke on cloud first came in cloud smart and I think it We've learned a lot in those five years. And I think it's a, it's a really great point he's making. I think five years ago, DOD, and I think all federal, looked at cloud a little bit different, it was a lot of a lot of lift and shift going on. There wasn't they were using it in very limited areas, and really not expanding the idea of what's what SAS and paths could do for that further for them. We're really looking at the big hyperscalers infrastructure services cloud. I think what you're hearing him say is, there's so much more we can do when you think just past infrastructure, and really start reaching out using services like z scaler, to provide us global security to our to our soldiers. If you go back to what unsynced said. That was that was was

actually in reply to a DOD opportunity we were working on and in our in our what we call it Z scalar private access service, which is one of the key components of our zero trusted and what Z scalar private access does is because it masks the IP address when you when you hit the first hop for Zscaler, say of warfighters in a in a let's say a warfighter is in a country that doesn't want to be we don't want to know where what a warfighter is that a country. And he doesn't want to be identified that we're proud or can log on to his Zscaler 00 Trust, private access. And the minute he hits the Zscaler cloud, his ip ip address vanishes, because it's all done in in virtual IP addresses that are not that are not reachable. His then his connection then becomes completely unreachable. And that was where he came up with it. And if you can imagine how important that is for a warfighter to go into country, log into his network and log into his device, whatever that device is, and immediately vanish, that people don't know he's there. Or she's there. That's, you know, one of the key component of zero trust, if you look at that, right is through micro tunneling and being able to use any network to create micro tunnels and things you can read the guidelines that address this. And I think that's been a big, big advantage for DOD to be able to do that through the Z scalar, or zero trust platform. And I think that really sums up why we always say it's not reachable, it's not reachable. And the last thing we want is warfighter networks or, you know, large CAD, anybody's federal network to get breached.

17:27

Steve, we did a quick interview about five years ago, and I've been doing interviews for many years. And back in the day, people try to dazzle you with the knowledge of coding and very sophisticated interfaces and, and fancy terms and acronyms. And I think maybe, since I just mean five, six years I see this. They're talking more about business objectives and business goals. And in his exit interview, Raj Iyer uses a phrase that this is a new transition. He says, We are economists in terms of decision making. In other words, they want the bang for the buck. They want the security but they want the bang for the buck tune, what's the most effective way we can produce the security for this large organization? And he says it right there we economist so they try to get a perspective that is part and parcel of his job.

18:12

I think it's right in line. I mean, if you look at where DoD is going, and I think last NDA bill passed, there's more and more focused on commercial commercial software, commercial cloud commercial offerings, right? I think the DOD has realized they've got to get away from building their own, and really leverage the knowledge of the security marketplace. If you see how many times DOD has stood out to San Jose, in the last five years, you probably fall off your chair. I mean, they're always out here. They're always talking to the up and the young, upcoming companies that you know, five years ago that they cave is awesome, you know, and several times since that's the kind of thinking that I think is going to make the DOD and I think all a safer, because not everything can be built by the military. Sometimes you got to reach out and look to who's able to build the commercial stuff that the big organizations are using, and then see you can certify it to be able to be used by DOD. So if I can come and have an enterprise grade zero trust exchange, as we call our solution, that is being used by global companies all over the world, at the highest levels, and yet, can be certified at Aisle Five and be used behind the walls of the Pentagon. That's a win win for them. They don't have to spend all their time developing, they should spend all their time protecting the nation.

19:40

Steve, I have two podcasts, one about technology, one about satellites and space and so I listen to all kinds of podcasts to keep up. I listen to cybersecurity podcasts, very well known people and I did a lot of deep dives. And so I'm listen this one guy, he's got a PhD. He's got this, you know, podcast. And and he's referring and he goes, Well, what as far as Guys, businesses Sean Connery and Bubba are going away with it so uncommonly. Right? I mean, he's being respected outside of, you know, outside of even I think in the federal government's gonna be very strong reputation. And I noticed he's going to be one of the people participating on your panel security SmartCloud government so, so maybe you can learn something from Sean Hmm. But if you can't learn from Shawn, you can't learn from the cybersecurity people say, and they have no dog in the fight. They don't care Sean Connery could work for you know, Exxon, or I don't know, who knows tire store somewhere, but he's got a pretty strong reputation. And, you know, when when someone else says, you know, hey, I'm John Gilroy. I'm real smart. Yeah, forget you. But if someone else says, Hey, that, Steve, he knows a lot about transmissions? Well, yeah, he must or that Sean Conley, he has a very deep understanding of how this can be implemented in the federal government. So I think that's, that's the that's the one to circle on your agenda for that day. So it's really I think it's an interesting group you have there to state governments get more involved here, too. That's it's really interesting, isn't it?

20:57

Hey, it is, you know, Leah McGrath has done an amazing job with state ramp. State ramp has been a is a nonprofit, let's call it FedRAMP for state for states. And it's been since Zscaler was the first to get state ramp authorized, we've been heavily involved with state rep, we really believe in the program. Again, I was here yesterday at the Google event we were we were just walking through their growth. And she said to me, they have 3000 companies interested in getting state Brown in just one year of being it's mind boggling the success that I think they're going to have, I think it allows the smaller cloud players that are focusing on the state level business in a state to really get in this fight without having to go through some of the rigor that FedRAMP puts us through. And if they just want to be you know, I'm just gonna have a small cloud provider of a state, you know, something, the state uses it, I need to get a certification, I can go to the state ramp process, which is, you know, easier for them to get through, but still has a lot of the rigor of federal, there's still continuous monitoring. There's still the NIST 853 requirements I heard yesterday, she's gonna go to read five, which really is great. I mean, so yeah, I mean, they're, they don't have to have a job and Leah's gonna be there. On March 8, another person heard her she really has a great message to tell. So I'm excited to have her and her and Brian Conrad for FedRAMP. Together with Sean, it should really be an interesting and interesting session. And I want to just comment one more thing I was we, these processes, we just we have an IBM certification, and we're working in APAC, I reps in Australia and working over in Japan and Singapore, and I was in Australia and Singapore, and the leader of their cybersecurity programs, both said to me, you ever heard of the Sean Connery guy? And you hear his name? It's really exciting. So yeah, it's not just not just outside of security. It's outside of the US even federal policy guy who's tremendous at what he does, who's being recognized, you know, by his compadres, that, you know, in, APAC, in in in Australia, which is pretty packed. But Australia, it's really set something for Shawn. So again, you know, I really love people to listen to the panel and be grateful.

23:12

This evening, I'm going to take the train go downtown, I teach a little course, downtown there. And a couple years back, I had one of my students, one of the managers at Deloitte, he handed me his business card, and

his business card had UI UX on it. I said, wow, it's coming standard now. And I'm thinking about user experience. And of course, if I'm selling shoes, I want to have a good user experience. You know, if I'm selling who knows what chairs or couches, I want a good user experience. But the federal government, that's not a phrase that comes up all the time, until I scroll through your years, march 8 event. And it says, ensuring great user experience and zero trust environments. So there's something new with UI UX and zero trust. No one brings that

23:50

up. Like it's, you know, the problem got with, you know, when we went to this, to adding so much security and so many controls that we do through not only just our products that are in our product experience, but also through certification, sometimes it makes the product, lose that user experience. I mean, look what happened with tick. I mean, when we launched the trusted enters our trusted Internet connection, we brought brought that out, what is it now 15 years ago, I've can't even remember why get started to get older and older. My brain is not working. But so that was 2009. When we launched, we launched tick. That was a great user experience. But also this thing called cloud came around. And you know, which people tried to upgrade tick to that too. But it really became a hairpin it became a it became a reason to gate the technology growth of cloud within the federal government. And then your sister rights to take three Dotto guidelines. Of course, Sean Conley writes it, and you open cloud up for trusted Internet, and then provide zero trust on top of that, to be partially regulated to be able to sell these three data eligible solutions. It's all about user experience. So you Making sure that I can use my o 365. Client without delay. I've heard stories, you know, from, you know, people within the government says, used to take me a minute to open my email Outlook to open, you know, now they now pop right up, you know, through a Tip three Dotto solution to these your solution. So, you know, it's all about user experience. And that's why you talk about my 150 data centers. That's why we add more and more data centers and federal all the time, it's all about making sure that user has that same experience that anywhere they are, on any device anywhere in the planet, it should just feel the same. You should, you should feel, though, you when you use your device, it just works. And just secure it government, you should know it's just certified at the level we need.

25:43

Steve, two hours ago, I was speaking to a gentleman in Ohio who's about to launch a company and a podcast and I said, Well, you got to you got to boil it down, you got to have like a 10 word description of your company. It can't be, you know, 15 minutes of Scripture, it's got to be boiled down to 10 words. And so I try to apply that in my world. And when I have studied this whole, trusted interconnect 3.0 The Tip three point I'm trying to come up with a I'm sitting in the metro later on today, how could I describe it to someone sitting next to me? And so So I the way I guess I look at is that takes me no longer requires to move traffic through the data center. So then it can go through the first half is going to be not, you know, to the data center, we can get that speed. So that's really what happens and is is that a good maybe a distillation of what takes reopened do

26:25

what I like I like to use my J Jr. Founder always uses the term castle and moat right is getting it is literally getting away from castling mom just basically saying your crown jewels, your data, it no longer needs to be in the castle surrounded by a moat, right. It's much easier to get to there's no perimeter. So really tip through that

oh is saying take the castle moat out, you don't need the perimeter first hop to eight security as a service provider that can provide the services of that and straight pure off to the to the SAS provider or to the internet. It's a straight line. But no, no hairpin. It's really I would say fastest isn't two points is a straight line, I want to go I want to go user cloud SAS. I don't want to go user Tick, tick data center data center. Cloud doesn't work. Yeah. So it's more than 10 words. Sorry, but you know, I'd say any, I'd say we're moving the perimeter.

27:15
Well, we're gonna have to end this interview, but you can continue on March 8, and you can meet Steve and meet his colleagues and ask more detailed questions there. But unfortunately, here we're running out of a little bit of time. So it's called the public sector Summit. You can go to Zscaler. And register is gonna be a lot of fun, a lot of network opportunities. A lot of smart folks down there, I'm going to officially tell Han Sang and I'm stealing his phrase from him and in trouble. You've been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Steve COVID, Chief Compliance Officer and Head of Global Affairs at Zscaler.

27:46
Thanks, John. Have a great day.

27:50
Thanks for listening to the federal tech podcast. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcasts.