Ep.37 Federal Tech and the Secure Service Access Edge

This is John Gilroy from the Federal tech podcast.

00:05
This is Dr. Tim Robinson from worldwide technology.

00:08
And today we're going to talk about Sassie hit the music cloud. Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Today we have Dr. Tim Robinson, consulting solutions architect at worldwide technology in the studio today. And the reason why he's here is he's going to tell you everything you need to know about sassy s a se and who else would be better than him to describe it. He's like the Forrest Gump of technology. He's been here, he's been there. He's been in the military. He's got all these academic degrees. And he claims to have top notch humor. But Tim, I don't know have to show me the top notch humor for me to believe it. But

00:46
this is far too guy, you know, I'm gonna pay you a little bit more than than what we agreed upon before the

00:51
show, even mode that bribe with that good introduction, huh?

00:55
It was, it was awesome. It was amazing. Thank you so much. I am super excited. Super happy to be here.

01:01
Okay, so hold on to your hats. Ladies and gentlemen, I'm gonna use a four letter word. Are you ready? FCC, come get me it is S A S E, this is a four letter word we're gonna talk about today. And Tim, what in the world does that stand for?

01:14
You know, that's, that's, that's a great question. And I'm going to try not to get myself in trouble. For a lot of words. Vendors are watching. So I need to make sure I say the right thing. So sassy stands for Secure Access Service edge. A lot of people think of it as a framework, I think of it is more of a paradigm shift, and how we leverage security. So so I'm going to take a little time, if you don't mind, John, I'm going to talk a little bit about how Sassie came to be and just sort of develop it. So we can sort of talk about this throughout the rest of this podcast. If you think about it, you know, we work in office offices we typically use Well, I'll say this, we used to

work in offices, and all of our data used to reside in a data center. Nice, nice and neat nestled, you knew where it was, you know what I mean, you didn't have a lot of the problems that you currently have now, and in traffic to that data was kept in the confines of that agency of that building of that organization, you were at now, you know, fast forward, you know, for you know, I'll just talk about the last five to five years or so stuff happens, you know, rent goes up, power, space and cooling, that stuff gets very expensive, your workforce could get larger, and most workforces have gotten larger. So what you tend to do is you spread out geographically. So that has large implications for security. And then other stuff happens that we have no control over, like COVID. So for a number of reasons, we have kind of a much more globally displaced or mobile workforce. And not only that, a lot of our data has moved to this thing that that we talk about all the time, it's called Cloud. And that gives us kind of two decisions. Or you can call them bad if you want to a lot of people, I call these decisions bad, you can do two things. Either, you can send your remote users first to your data center. So I'm at home now, I'm no longer in the building, I'm at home, now I have to go all the way to the data center to get my data. That's one way of doing it. Or you can have mobile users go and access your software as a service applications directly via the Internet. In the cloud, what that does for you is that gives you kind of a faster experience. So no longer am I sitting at sitting in my cubicle at work, I'm at home, I have to get to that data that's at work that can be cumbersome that can induce a boatload of latency and what I'm doing slow down my workday and frowns all around, right? So what organizations typically do, you put data in the cloud, and then I can go and access that data from the cloud a lot easier, a lot easier, a lot quicker. One of the concerns out to I'll tell you, John, and then I'll leave it at that. One of the current concerns that we have is that you're, you're bypassing this nice security stack that I told you remember I said we had a data center, you're no longer inside of a building, you're at home, you still have to get to that data in the data center, where you have to go through a security stack in the data center to get there. When this this paradigm is slightly different, and I'll talk about why in a little bit. So what are my concerns with having a remote workforce that has to has to work from home or work from a different country or a different state to access data, my data center, the volume of traffic increases, remember I said COVID that push a lot of workers outside of the building right, so now everybody has to get back to the bill. So now that you have an increase of track and gets going to your data center, there's all sorts of threats because now you're at home doing all sorts of things on your laptop. Right? So how secure is that laptop? up. Another thing we have to deal with is, is updating, appliance, updating software, a lot of these things can be cumbersome can be complex and time consuming. So let me summarize and then I'll give it back to you, John. You know, I get excited when I talk about IP stuff. So sassy, secure access service edge, it's really, it's an architecture, right? It offers a worldwide fabric of network security capabilities to users to any users connecting to users from anywhere, their devices, their applications and our platforms, anywhere at any given time, with a reduction of impact on the user experience, because data is now traversing a most optimal path to get to your application, you're no longer going from home, going into your data center, traversing that security stack, getting to your data coming back out of that security stack, and coming to your desktop at home, you're going directly to your applications through another security stack, if you set it up right in the cloud to get to your your software applications that reside in cloud. Hope that makes sense.

06:08

Yeah. So S E allows for a couple of things. Number one, allows for scalability, that also allows you to avoid one stack that goes in to your datacenter and also allows for compliance because it's handled from one central location. So those are the three main benefits. I think, for federal people. Now, federal technology, people are listening to this and they're listening to you and go that Tim, Dr. Robinson, he must be some academic guy. So 95 pound weakling reading books all day long. But if you go to his back and finds out that you are in the Marine Corps, and you serve tough places,

06:43
yeah, I like to tell people all the time, I carried a rifle and a router. Oh, I

06:49
know, you steal that. From David bass, like, didn't you?

06:52
Oh, we're not talking about events, if he's old news, these elements. I'm the new guy.

06:57
All right, on a router that says line. I love that line, isn't it?

07:01
Awesome. But it's kind of true. Lots of experience, I would like to tell people is that, you know, when I was in the Marine Corps as a communications Information Systems officer, everything that you have on your desk, from your phone, your computer, we project those services and those devices onto the battlefield so that we can make decisions. And we can become successful in everything that we do. So lots and lots and lots of fun of functioning as an IT guy in the Marines.

07:24
And the reason I brought that up is because Washington DC has a place called Georgetown University's Georgetown Hill. There's Healy hall there, and it's a it's a Classic Ivory Tower. And there's a lot of people pontificate, and they have no idea what's going on in the street. But someone like you know, you started from, you know, the trenches and worked your way up. So I think anything that you say to this audience is going to have a tremendous amount of resonance, it's not going to be Oh, yeah. You know, no, it's going to be effective because you've been in a situation or you had to have secure communication. And we laugh about a rifle router. But today, I think the warfighter is increasingly, depending more and more on digital information from from all kinds of different edge devices, which calms us back to secure service at edge, doesn't it?

08:05
Absolutely. Absolutely. 100% agree with you.

08:08
So the question I have is, I'm a mere mortal, I'm just looking outside. And so how do people fail in trying to implement sa SC sassy? So,

08:20

man, you know what I will say this, and this is more Tim Robinson speaking, right? I think a lot of people fail to understand what the actual problem is. Sassy is not for every organization. Sure, we're moving towards it. Sure, you can see the federal government making a huge push towards the cloud. But and there are other technologies and things that that we're concerned with as well, for example, like zero trust, for example, comply to connect, I think, if you have a security paradigm that has failed, you've, you've bypassed a few steps. One is to write down what your actual requirements are, what I do a lot at worldwide, John is, is I go in and we perform workshops, and these workshops help us meet the customer to where they are, there's a term we use, it's called ideation, we, we get a whiteboard, and this is where I break out the clipboard and you know, my glasses, and I push him up my nose and the pens and the markers. And I start just writing over the whiteboard understanding from a people processes and technology standpoint, what should we be doing? Because a lot of times customers ask for things. But they don't necessarily need those things, or they need a derivation of those things to achieve the common goal. So when I walk in these workshops, the first thing I do is I go to a board and says, Hey, what do we want to get out of this workshop? Is sassy. You want to implement sassy? Is that truly the problem? What are your concerns that you have up front? So to answer your question, John, the first thing you have to understand is what's the problem in the first place and if Sassie is a failure to implant And that's probably because we were working on the wrong

10:02
problem. Start with the end in mind, a famous man said that I know that line, that's what you're doing there. By the way, if you're listening to this, you may want to visit WWE t.com and take a look at his company's website. So I've done about WWE for years, and they have an office in downtown DC with all kinds of demo facilities. But if you're listening to this, and there's snow on the ground, or you're watching the Super Bowl tomorrow or something, and you're listening to silly podcast, you can go to WWE t.com. And then take a very close look, because it's gonna remind you of the YouTube site. It's kind of like, it's kinda like a YouTube for nerds.

10:39
Guys, we're better. We're better than YouTube. But But, but if I could looks great. It's amazing, right? If I could just double click on on the point you just made our Advanced Technology Center. Man, I will tell you when I first came worldwide, it was it was it was it was shocking, that that the capability that this lab provided, I call it a lab, but it's not really that to me, it's a digital playground. It's like Disney World for it, guys. Everything in anything that you could think of is probably in our ATC spans across the campuses. multiple buildings are racks and racks and racks of equipment and what you can do as a user, if you're listening to this, you could go out to wwe.com, making an account. And you could do things like look up sassi. And I can guarantee you there should be a lab there. There's white papers, there's documents, there's other podcasts with me on talking about these types of things. But you can go there and you can navigate through these labs, you can learn what SAS is, what are the top vendors and sassy how you implement it. Was it a Roblox just like John asked earlier? What are Roblox and implementing sassy? Those types of things? So I would I would, I would, I would ask that all of you go off to worldwide technology.com or WWE t.com. Get an account, take a look at our Advanced Technology Center, surf around, get yourself educated.

11:56
Yeah, it's a it's a nice site. It's some it's been a lot of work into it.

12:00
Thank you. Quick all the credit for building that website. I'll take the credit.

12:04
So I am a mere mortal here, and I'm looking at this problem. And I'm trying to get a perspective on it. I try to detach myself and say, okay, so if you look at technology last 15 to 20 years, what you see is you see this wide area network, okay. And then something called a software defined wide area network SD Wan came about and people start using that. And there's certain limitations in that. And it seems to me that the limitations volved in SD Wan, probably have something to do with security. And this is this and enhanced. SD Wan, is that really what it is? It's a software defined wide area network with sacks of security built in.

12:48
So yeah, so let me Oh, I think the easiest way to put this is, is I talked about the data center, and people going into the going into their agency and sitting at their computer logging into their data center. And there's a security stack there. One of the one of the one of the great explanations I'll have for SAS is think about that security stack virtualized in the cloud. So not only do you have access faster access to your applications that are in the cloud, you can put a security stack right there in the cloud. So you can traverse that security stack. Before getting to your applications, making sure you are who you say you are, you're not doing anything malicious, and your data remains safe. So the idea is that same risks that you have on prem, we call it on prem, I keep calling it a data center. But but your risks that are on premises, your security stack there is supporting your risk. Same scenario with Sassie in the cloud. There's a security stack there. Network Access there, that's going to do the same thing for you. With sassy

13:49
Tim, I was just handed a telegram from the White House and I'm not allowed to go 20 minutes without saying zero trust architecture. That's I said it because I have to say it's a man shot. Same thing with you next time you have to seven love and you got to say zero trust architecture. Can you come down to the store and every 20? You have to say it in the sound? Don't you? Mandate?

14:10
I cannot draw. I mean, we were being facetious right now but I tell you I can talk for five minutes without somebody asking me I know. But But the bigger question is I get it's how do we implement zero trust? So I'm not sure what your question is. But let's go give it to me. Let's talk about Yeah,

14:33
no, I guess sassi can help. With the deployment of zero trust architecture. I assume that's part and parcel of one of its strengths.

14:41

Sure. So what I will tell you is as when we open our called sassy a paradigm. I look at zero trust is more of a framework and I'll tell you why. So zero trust is more data focus where I believe sassy is more connection. Focus to keep to keep it simple. Dave and I were talking about this. And we both thought that, you know, when you think of SAS, we think of how traffic is handed out to public destinations. With zero trust, we think of it as a who, what, when how people access my data. So So whereas zero, you know, sassy is more connection, focused, zero trust is more data focus and who has access to the data, who should have access to that data, because we don't trust anybody with a zero trust in a zero trust architecture. So zero trust, and specifically, the network access piece of zero trust is about securely connecting users to their mission application sounds similar, similar, right? But it's, but it's just, it's different. Because we tend to focus on our data, we tend to make sure that data is tagged appropriately. Because when you look at identity of people and their access management, you want to make sure the right people have the right access to that to that data. Now, I'm not saying that some, some SAS vendors don't have some of that built that functionality built in. But when you talk from a historical standpoint, sassy connection to my dad on my app, my applications, zero trust is not trusting anybody not trusting anything, all the way down to the device on the network, wouldn't even trust devices on a network, given that device, that person the appropriate access to the appropriate data, so they can be complimentary in a way.

16:30
You mentioned, your colleague, David Vasek, just a few minutes ago, and I wonder, when it comes to trust, I wonder if he's going to trust you. After he finds out that you sold his line in the Marines. I carried a rifle on a router, because I'm gonna be the first one to tell him that.

16:44
You know, I don't I don't know. But you know, David, David, and I go back. He's a he's a good dude. He's a smart guy. We're both Marine. So so we have that going for us.

16:54
So my question is, this terminology began in 2019. And apparently, it's just blown up, if you go to Google, you get 200 million search results. I mean, so people are blown up and talking about a whole lot. And so I imagine that there are other companies that are trying to deploy this technology. So So where's the fail points? I mean, where's the where's the problem? You know, if you look at a use car, this one is bad brakes. And the other Well, this one is bad transmission. So where the typical fail points when someone tries to deploy a sassy solution, so

17:24
I will tell you this. And again, this is Tim, Rob's we're gonna we're gonna separate worldwide technology and all of my partners from from Tim Robinson, I can do that. Right? I I can Oh, yeah. This 15 seconds. So, so so so it sassy. It's not to me, it wouldn't be suitable for, say, a combat for deployed combat unit. Right? If I was, if I was to advise a combatant commander, if I wasn't by a battlefield commander, on on technologies like this prop probably wouldn't be there. But I will say if I'm, if I'm looking at the Marine Corps, or the Navy, think about recruiting commands, right? You have all these recruiters all over the world, and you know, going grab these guys from high school guys and gals from high school, and bringing them into our services to support our

company, our country. That could be that's an amazing SAS use case, right? No longer are, you know, are you pulling open a laptop getting ready to do a presentation at a at a trade show, or job fair, you know what I mean? And you have to go all the way back home to the data center and pull things back out, sassy would work well for for organizations like that other organizations, we can talk commercial now, I'm putting back on my worldwide head now. So you know, we've talked about organizations that have to deal with BYOD, bring your own device multicloud at you know, applications. And as I said, when we open this is for those, you know, we're we're distributed globally. Now, you got people working in Alaska, Hawaii, Singapore, Brazil, everywhere, and they need access to your company data. So if you're an organization like that, that's dealing with hyper scaling, that that's moving, that's growing faster, and you know, because you know, you gotta go make money. This is a is a is a superior use case. For an organization like that.

19:14
I want to ask a question about bandwidth optimization. But first, if you're listening to this and have more questions, want to learn more, you may want to listen to episode 22 with Tony D'Angelo. He's from lookout, and they talk about endpoint security. So the good kind of handoff after this interview. Okay, the next time we do this, and we're gonna have like a big ol whiteboard, and we're gonna have a battle of the boxes and the whiteboard and go back and forth, and back and forth. And, and you mentioned this earlier about the cloud and then about places like Microsoft and Amazon and different ways to use the cloud. But it seemed to me a benefit of this structure is just optimization of the bandwidth, isn't it? I mean, it makes it cheaper. I mean, that's the bottom line. Guess what? It's cheaper.

19:57
Absolutely. I talked about several things at the beginning. So we've talked about why people are moving away from sort of data center. Now, I will say most organizations won't get rid of their data center, it will probably be some type of derivation. If they're implementing Sase. They're probably keep their data center. But they're also probably have applications in the cloud. So you know, we talked a little bit about multi cloud, whether you have an on prem cloud and the cloud, you know, an Amazon or, or pick your pick your cloud provider, you're probably keep both of those. But when you're talking about optimization, I would love if our user base would go to worldwide, pull up the sassy lab and do it because it shows you it does a better job at navigating you through how, you know your bandwidth is optimized by utilizing Sassie, then I can tell you, it's legitimately shows you how it's done. So I'll try to explain it. And Tim Robinson Sturm, really, I talked earlier about us moving our workforce away from the actual mothership, right, all these folks have to get back into your data center, they have to get to those applications, those applications are in a data center, you force them to go to the to the data center, traversing that security stack, then up to the cloud, where you have the applications, then back to the data center, then back out to the users, man, that is just You're crushing your bandwidth, you don't want to do that if you have applications in the cloud, why not leverage a sassy solution, so you can gain access to that. So you're not putting all of that you're not all of that data is not traversing through your data center. That's really where your optimizations come in. And you will see in this lab, how much faster it is to access your data.

21:36

wwlp.com for that one, that's it. Well, Tim, I don't want to get in trouble with your folks at headquarters there. But I'm going to use another four letter word. Okay, this is gonna be tough. This one is MPLS. This is kind of a traditional way of communications. And many times if you want to enhance your communication, to be flexible or increase it, it may take 10 days or two weeks to get something done. If we change the approach with a sassy approach all of a sudden that that gives you so much more flexibility as far as timeframe goes. doesn't I mean, it's just it's a lot faster as well.

22:11
It totally is. But for those of you that are listening MPLS multiprotocol. Label Switching, it's really a I'll think of it as not think of it it is a networking technology that routes traffic. Shortest Path First. So think of OSPF I'm nerding out Emma, I'm talking about

22:33
it's just it's an old school communication technique. It's a rotary phone, it's a rotary phone. Okay, digital phone. That's it. That's the best explained. I mean, the VoIP guys can talk for 10 hours about this and go on and on and on. And they love them. And the term cloud originated with the telephone, guys. I mean, we know that. And so we're calling this out. But the the older way to do it was inflexible and time consuming. And the runway is extremely flexible. And quick. So another on the checklist. I mean, if you're, if you're a Federal Information Technology Professional, got a little pat out there. You got Tim Robinson, the top you Okay, faster, cheaper, optimizing the bandwidth. Well, so what's left?

23:14
Right, yeah, yeah, you're absolutely right. And I'm not I'm not being mean to the MPLS guy, MPLS gurus. You know, I love those guys as well. But But you're right, I think where we can glean efficiencies in today's workforces. And if technology is involved, we want we want to leverage that. I mean, that's the whole reason why we're here. If there's something that's out there, that's going to help a customer have a better user experience, then we're going to recommend that but I'll always go back to what I said at the beginning of the podcast, when you ask the question, you know, what are issues with with implementing SAS, it's, it's really because a lot of times we'll get these policies and these directives in DOD, and we'll start trying to solve the problem the wrong way. So I'm not you know, I'm not saying one protocol was better. I'm just saying, let's take a step back. Let's talk about us come to the table, let's have a workshop and talk about what the real problems are. So that then it's not such a culture shift, because I will tell you, John, walk into any organization doesn't have to be DOD, and throw out the term zero trust. And you know, they will fight you back out of the door, because it's a cultural shift. It's not just a technology shift. People have to learn new ways of doing things, especially your security guy, if my role in life is to reduce risk for the CIO and the CEO and the CEO. I do things a certain way. I'm not apt to trust this new guy coming in is trying to sell me on this, this framework or this new technology. I want to understand how that works. And again, here's a plug for the Advanced Technology Center. If you want to know how a technology works. We do a great job at worldwide technology of putting together we'll call it we'll call it demonstrable labs. For that, we'll show you how technology works. So again, I know I'm plugging worldwide technology a lot. But it truly is John, a way for organizations to come in, understand how technologies integrate with their current infrastructure to see if it's going to improve, to see how we can improve, to see which way we should go. So then it's we're not getting the cart before the horse,

we're looking at technology, we're seeing how that technology works in real time, before we even push it into our production environment.

25:31
No, in two weeks, I'll be speaking with a doctor, Elsa Schrader, and we're gonna talk about machine learning. And that that's an issue that they have is trust, because they may not trust the data they get. And so I think this is the brave new world here is technology is one thing, but humans understanding and appreciating some of the strengths and weaknesses. And so it's, I think it's more of a human thing than a technical thing. But I think for machine language applies to SAS sassi as well. So it's, I think it's a human thing more than anything else.

26:01
I do if you and here's a plug for me, I did a, my dissertation was on the verification of a cyber attack. I could remember and I will tell you where what organization I was in, you can check my LinkedIn profile, but I was I was in an organization. And there's this person, given the morning brief, you know, you go into these government organization, you give the morning brief, hey, we're susceptible to this specific attack. And she was basically telling, telling leadership, how the attack have propagated, and the peanut gallery, it wasn't me, I will say, John, it was not me if somebody else steals. I don't know, if they're playing stump the chump. They raise their hand and I said, Hey, how do you know that you've been attacked? Well, because because this document that I printed out from my ideas, said so and folk, what happens if your IDs has been compromised? Yeah, I get it. She learning all of that good stuff. Great. But what happens? Yes, your IDs has gone right, then what is, you know, is your report true? Or is it false, because one of the things as as as certified ethical hackers will just use that term. If you go into an organization and you do something, you're gonna do what's called cover your tracks, you're gonna back up on it or so. So I said all that to say that, yes, machine learning is great. I don't think we'll ever get to the place to where we were replaced the human in the loop. And I'm all for machine learning. I talked about this in my dissertation. But there's ways there are ways that we can reduce our risk to get away from this kind of alert fatigue. That I'll tell you, I've been in organizations and interviewing folks in in organizations and on the watch floor, and I'll say, Hey, I'm looking through 500 alerts today. Dr. Robinson, I don't really know which alerts I should spend time on. Well, that's a situation where machine learning can help you. Right? Yeah.

27:50
That's a practical application. Dr. Tim Robinson, you got the last word here. So I've used this as a journey. And your your job here is to tell me it's gonna be a long journey. Is it going to be a short journeys gonna be with bandits on the road journey? So what kind of journey we looking at in the future for Sase?

28:08
I think, I think if you keep an open mind, I will tell you that the US government is pushing towards cloud adoption rapidly. Organizations are already there. So I think the journey is what we make it, right, you if you try to handle this alone, I completely recommend against that. Because again, we as security guys can, can can tend to be stubborn, in the way we're comfortable with what we are comfortable with, when our job is to secure the castle, right? So you start introducing these things, these new paradigms, these new frameworks, that don't necessarily make sense that don't come without their inherent risk as well. I think I think we can we can make

decisions that will ultimately end up hurting the organization in the future. So thank you. So right, you look at it as as a journey. But you also pick up people all along the way in that journey. Think of it as big of worldwide technology as Sherpas. You know, we're helping you go along this journey so that you can make the right informed decisions. The whole way we I like to, I like to, I like to call the people I work with not customers, but partners, I partner with our customers to help them understand where they are currently, where they need to go so that we can hit the appropriate milestones to

29:32

get there. Well, the milestone we're reaching is the end of this podcast. Oh, man, we're having so much fun. Yeah. You've been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Dr. Tim Robinson, consulting Solution Architect at worldwide technology.