FEDERAL TECH PODCAST

Ep. 20 A Breakthrough Network for Managing Apps

SUMMARY KEYWORDS

user, scope, controls, people, build, network, platform, cloud, jamie, visionaries, data, protecting, architecture, net, single, access, context, interview, security, agencies

Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Our guest today is Beau Hutto. He's the Vice President federal at a company called net scope. That's n e t s Kope. Yes, I'm compulsive about spelling because people will cutting their grass and listening to podcasts. And I want to get the spelling correct. Because it's a great company and a great website, I went to your YouTube presence, strong YouTube presence, a lot of very high level people recommended net scope. And I thought it'd be worth exposing the concepts of net scope and their way to manage networks to the federal audience. But before we begin, just a quick background on your bow, I look at your LinkedIn profile, a lot of success, wide variety of organizations. Why did you select net scope?

08:18

Now? Hey, John, it's great to be here. And I really appreciate the opportunity for sure. Very nice meeting you. And but why Netskope? Great question. And the answer is that the vision that our founders had, when I first sat down with them in late 2015, this was a couple of years before I actually ended up joining. I had known this crew from my Juniper days, and they were running this entire security product line over at Juniper. And they really and this is something that we've done consistently is they've, they've had an idea of what they wanted to build for this platform as a service in the cloud, and really skating to not where the puck is, but where the puck is going. And they've consistently done this. And so when we sat down in late 15, and I looked at the napkin that they had drawn up just a few years before that, for the vision of what they wanted to build. It was very similar to what I just walked away from, which was building the first iterations of JRSS, Joint Regional Security section, the DOD. And we had just one that was the biggest contract in history. Were when I was at Bluecoat. And we, we had our great, great initial success there. And then it was time for me to move on after eight years within that organization, the, the just seeing that vision and, and looking at how they were actually designing it, which was really taking all of the, you know, 2030 plus capabilities that are siloed off in that stack of JRSS Today, and actually pulling all the best in the industry that had built those individual silos out of the valley. And giving them the opportunity to say, all right, 1015 years later, if you were to redo this and build it into a single platform, what would that look like? How would you do that differently than how you what, what you did originally? And how would you make it work more effectively and efficiently. And so they came together, and they put together a single platform. And that's what lets go has built that literally takes in the best of the best out of the valley. And they were able to take their lessons learned from past successes. And then and lots of failures along the way, and then build in what would be the actual next generation of each of those capabilities,

but in a single platform, single security stack, a service in the cloud. And that's really what they were building towards. Gartner has called it many things, and will continue to go by Gartner's guidance, because that's what our customers look for, for, you know, overall guidance to a great extent. But you know, it was never building to a Gartner term per se.

11:12
And so the term we're referring to indirectly here is S A S E, secure access Edge Service. That's correct.

11:18
Yeah, yeah. So sassy, secure access service edge. And then there's SSE, which is secure service edge. And as Gartner defines it, they would suggest that SFC which is where Bullseye in the middle of that upper right hand quadrant of that MQ, is the foundational security layer to a sassy architecture. And so sassy is not necessarily a product, right? It's an architecture in which really gets to the edge of protecting the data protecting.
Because you no longer have this brick and mortar of a network, your everything's hybrid, your data is living on premise, it's living out in the cloud within an, you know, an infrastructure platform or software as a service. It's living right here on our mobile devices, right.

So the multiple mobile device is really the edge now. And so being able to protect that data is critically important. And that's what you know, Sassie, the construct the architecture is really all about,

12:25
well, you've had a lot of successes, I've had a lot of failures, I want to detail, one of my failures. When I was in college, I wrote Thomas Kuhn structure, scientific revolution, I debated a philosophy major about that, I was crushed. And this guy was using phrases like, well, if you take that text out of context, you get pre text on me, but when I think of what SSE it's got something to do with context, because it if I walk up to a baseball stadium and present my ID, they're gonna find out many different things about me. Imagine this is the context is presented. And so is this, the key word to understanding what net scope can do is the whole concept of someone trying to access a system or trying to enter a system, this context where we're worried about here,

13:07
I would say context is a core component of what you need to have in place as part of your security posture, right? Need a control mechanism that puts context around, not only what the user is doing, where the users coming from, where the data lives, and breathes, what the data is, the risk score of that user over time that you've noticed, you know, and historically, and all of that context, then gives you the ability to dynamically authorize their access to certain areas, applications or data within those applications, or gives you the ability to limit that access.

And by limiting it might just be being being able to acknowledge that it's there. And it's been touched, and it's actively being worked, right, it might not be even visibility to it. And other times, you might have visibility, but you may not be able to download it, it really depends on where that user is at. And the context in which being

contextually aware of the surroundings as well from that device, to where they're at what Wi Fi network, they're on, et cetera, et cetera.

And this all really comes back to if we look at the OSI layers, right? Up through seven. And we jokingly say this but at the same time, it's kind of the next evolution of it really the context awareness is layer eight, and that's really where NetScaler place. Got it.

14:50
I did some research on you and I think you have recently written an article and looked at large federal agencies. Now I got the quote here in front of me and you can defend that'll expand on it a little. I think you wrote that. large agencies. i This is really hard to believe. I mean, a typical large agency accesses 20. I mean, 2500 apps and only 3% are managed? Wow, that's a it's a tiny number, isn't it? I mean, once you think more,

15:19
actually, I would think, as far as managed apps, is that what you're asking? today? Yeah. So it's, it's just wild. It really is the Wild West, when you think about shadow it as it's been known, it's really the user led out applications that they bring into the business at times, it's very different depending on you know, whether it's a government organization, a commercial organization, but we're speaking more to the the federal end here.

But then the federal side doesn't go without its flexibility, right, with, with institutions like NASA, with institutions like our national labs, these are areas where you may not want to necessarily limit the creativity of some of those users, and their ability to go out and use different tools to get to the end result that you're looking for you're trying to create. So you're always going to have the mission lead applications, those that are authorized, those that are actually purchased and owned by the business and they're protecting, and that and that's that 3%, out of the 1000s that users are actually utilizing throughout some of these are larger agencies.

And the most important thing is, you know, part of this comes down to who we're hiring. And the the flexibility they'd like to have, at the same time, the most critical point is you want to protect the data, you need to protect the debt. And so if you're going to allow users to use other applications, number one, you need to be aware of what those applications are, you need to be able to then put risk scores, give them a Cloud Confidence Index of how risky those applications are, make them aware that coach them through that. At the same time, you may want to also make sure that a user might have something as simple as their own instantiation of Microsoft 365 versus the business lead version of that.

And you want to make sure that no matter what, by malicious intent, or more likely by mistake, let's give our users the benefit of the doubt. But by mistake, they don't move data from a mission supported instance, to a private instance. Now that that that's a real risk, right, so we put controls around all that. And that's also putting controls around all this shadow IT components that exist out there today. Pardon me, one point is gonna close the store in my office,

17:56

no problem. We're in the middle of interviewing Beau Hutto. And we're talking about an innovative way to manage the network to improve security. Now that we have a little break, in the beginning of this interview, talked about meeting the people that noscope and how they were visionaries. And when I did my research for this interview, I found out that Netskope actually has a group of Netskope network visionaries, I guess these are people get together and and just try to detach themselves and look in their work and try to improve ways to increase security reduce cost is, is this a part of the offering that noscope has?

18:31

Absolutely. And they've really come around on this in a really significant way from our our team of CEO, former CIOs and CISOs. They, they have built a bunch of a huge team of that globally throughout the organization. And part of that is not only the visionaries component where we'll do our podcasts and things of that nature, tied to that. But these folks, these teams have also been intimately involved with really setting the direction of where do we need to focus our priorities, because they're coming from real world experiences, and what it means to then prioritize certain things within our engineering and platform engineering teams to make it most effective for not only our mission critical, you know, government, agencies and customers, but also for those that our commercial our financials are big financials and you know, there's a, there's a number of really large customers that Netskope protects, and so being able to really understand and help educate their leadership on where the rest of industry is really headed. And this is where these teams are just an amazing knowledge point for that and being able to go and share and evangelize and help our leadership in the federal government make better decisions based on what where they want to go based on where everybody else has gone, and had had the setbacks and lessons learned, and hopefully not, you know, and learning from those that came before them. Right. And that's really what this team is all about. And they've been absolutely instrumental to our overall success.

20:27

I want your company Twitter feed. And in the description, they talked about redefining the cloud. And what some people in the business like, yes, it's not a cloud. It's a multi cloud. It's a super cloud. It's a massive cloud. So that's how we're talking about redefining just the terms here, we're talking about an approach. So instead of a firewall with some rules that change every 10 minutes, it's a complete different different approaches, this risk management approach with, I guess this would be a way to actually use zero trust, isn't it?

20:57

Absolutely. And if you think about what we've built as Nesco, the the entire infrastructure, we call it new edge. And what new edge is, is the most performant private global security network in the world, it was built by the team to build AWS Limelight video on demand, Joe DiPaolo. In his his team, they've come in and built our own telco grade network. And that is massively different than what any of our competitors have. Oh, yeah. It's huge. And so we're able to now have full QoS controls, we are we are this second only to thing you know, the, the Facebook's the apples and others that have the peering that we do at these colos. And so we're able to onboard you to your mission critical apps faster than anyone elses. So literally, this is replacing multiple latency components that our users have suffered for decades, and giving the user experience one that is much faster than they would have typically had without net scope. And they're not even realizing all the security controls that are being implemented along the way, which is critical to the mission of protecting the data.

22:23
15 years ago, I intensely studied VoIP. And I learned this from QoS quality of service. But you're you're building, you know, this is the classic Wan, you're reducing latency by having your own stuff. It's like no one's build our own. And I think that really helps selling it as a service is what we kind of talked about here. Back in May of 2020. I interviewed Jamie Holcomb from US Patent trade office, and everyone's flipping out, and it was COVID. And he was very common and relaxed. It was like it's a seventh inning of a baseball game. It's kind of a you know, having some popcorn or something. And, and I saw Jamie, why are you so confident? Well, we've been remote for a long time, we didn't have to change much at all. But he said he's always looking to improve. He said, You know, I may be pretty good for a couple years. But since going to change, this is 20, twice as two years ago, already 2020. He's changing. And he's looking at new ways to increase security of his network, reduce that latency, reduce the friction, and he turned to you guys, which is the big announcement you have I mean, USPTO some of the smartest Jamie's looking at you, you know, he's vetted you. I mean, I know has.

23:30
Absolutely and so and so this whole space has evolved so fast. And I will hand it to Jamie for getting ahead of it when you and there's been other agencies within the federal government that have actually adopted sassy, the architecture, the concept faster than you would have ever imagined the federal government would move and I praise those that are kind of leading that Jamie is certainly one of them. And he's just done an excellent job of realizing that he had some of the pieces that you would bring into that architecture, but he needed something that would bring it all together.

That's really what net scope gives you the ability to do. We're not it's not as if you purchase that scope, and you check the box of sassy, it is you you bring that scope on we partner with you. And we allow you to then take and use the efficiencies of everything else that you've actually invested in. And there's significant investments out there. And we just make them better, right? And so we pull it all together. We give you that cloud security stack so that you can leverage where we make the most sense and where the investments the legacy pieces that you have on prem today make make the most sense, and a lot of that is moving to a single platform instead of a portfolio play. You might call it where a lot of legacy vendors might Be just trying to add in bits and pieces to stay relevant. This is all about being able to provide a single platform that actually is the first time in 25 years, any of our customers have had the opportunity to sit back and and think, okay, if I'm going to do things differently now that I've been moving a significant amount of my data to the cloud, and my users are now remote.

And some of my dad is still does live and breathe back on prem. How do I need to rethink this, and when you have a solution that can actually come in and provide all those services, that's what I would recommend, you know, anybody taking a real serious look at because building silos in the cloud, like we've done for the last three generations on premise, is not the most effective way to do it, you want a single pass architecture that allows you to put implement those zero trust controls the policy in which you've designed, find that architecture, find the platform that makes the most sense to your organization.

26:10

I think that's why federal agencies should look at patent trademark. Because if you take a look at, let's say, you're doing research, you go to NIH, you get some information from them, you maybe get some information from the CDC, Atlanta or something, what you're doing is you're looking at and bringing it down, by by definition, when you apply for a patent, you're providing data, and you're loading that up to the patent trade office. And so, I mean, you're putting stuff on their system, and then I think, by definition has to be so much more risky. And that's maybe why Jamie is, is realizing that, you know, there could be malicious code involved and getting patents and you read on what's going. So it's just the agency is defined differently from so many other agencies that except stuff every single day, and addition to the remote workers. And so I think the unique problems that presents probably forced influx, a solution that would be a platform based and reduced latencies, like your your white air system does,

27:07
absolutely 100%. And you have to also take into consideration the user at the end of the day, right? Because you can build in all the controls in the world. And you still need to be able to protect the user almost from themselves, right? Because you as much as we all go through our training of click through this, don't click that, etc, etc, we need to be able to proactively realize that if a user does click on something, and it's going somewhere, that's nefarious, perhaps or we haven't classified, we actually can put that in a browser isolated browser instance.

So it's not going to go into effect that that user, that system, or the data behind it. And that's really critical. When you think about all that mission critical data within the patent trademark office for sure. You don't want a user clicking on some link that could potentially have disastrous, disastrous effects on the back end of things. So if you can actually put controls around automatically dynamically, putting them into an isolated browser, when you're not sure of where they're reaching out to, that still allows them the flexibility to operate and also be protected. The other side is, as we're talking to earlier, the shadow IT components, and that's probably a little bit more locked down in the patent trademark office. But in general terms, they still exist.

And you want to be able to realize, you know, what those applications are when they're happening being in line, and then being able to then put up coaching pages to the user and suggest, hey, you have you're trying to get to Dropbox here, there is a sanction version of box that we recommend you use, please let us know why you need Dropbox instead. And usually, by doing that, you cut out 90 some odd percent of anybody continuing to click forward because they know they're being watched. And then they've also been giving a given a strong alternative. So that's really helpful for mitigating the user making the mistake. And so I think that's part of the overall solution as well.

29:22
You know, I think to users something in this equation here, if you read the FISMA, from 2020, they talk about well, you know, are people gonna attack with spear phishing and weak passwords. This is all human human. And so if there's a way you can prevent people from doing that, without increasing friction, and this is the whole thing, I'll have to jump to this soup and change my password, just nine digits every 30 days. And I've got to, you know, humans just aren't going to do it. And so if you can have an automated way to prevent them from making those mistakes, and I'm not just focusing on this is the same structure for for banks and Ohio and

manufac Actually in Oklahoma City and, and who knows what restaurants in Seattle, so I think it's just human beings. They don't want to change your password every 90 days to do nine digits, they just don't. And people are gonna get lured into spearfishing. I mean, if you sent me, or someone sent me your email bow, I'd probably click on it because I know Bo, right. And so I think it's a human thing. And so anyway that the system can be prevented. I know a guy who wants a, drove some equipment on a U haul truck out to California. And I said, Well, how many speeding tickets do you get? He said, Well, there's a governor on it, I couldn't go over 55. So that system was preventing him from spending a lot of money on speeding tickets. Ah,

30:37
that's, that's great. And as we all used to get behind, you know, thinking of governors, I remember getting into go karts and reaching back and you know, the governor was on a go kart, but if you could reach back far enough, you might be able to, you know, get in the middle of that one.

30:51
But wait a minute, that's a federal offense here, well, you are going to be in trouble here, we got to change the conversation. I'm gonna erase that part of the podcast, I do a homework and I read an interview with you. And he's a very fancy phrase. And I said, Wow, this Bo's got to be smart using his fancy phrase, and the fancy phrases, machine device control plane, Whoa, let's be an engineer there. So maybe you can take that phrase and just break it down for normal human beings. So what is the, you know, a machine device control plane, and what's this got to this conversation of net scope?

31:22
I think when we start thinking about, you know, end to end, and really putting together from the, the user, the device, all the way to the data, you want to be able to have controls across that entire, you know, effort, right? When you're going from, whether it's your laptop, your mobile device, and you're reaching out to the data, whether it's on premise or out in, you know, an infrastructure software platform as a service out on the web somewhere, you you want to make sure that no matter what, that that single pass architecture is in place, and what I mean by that is that control plane that when you hit the security stack, the platform that you're going to hit on your way to that data, that all those controls that you buy, your policy dictate should be in place, are and you can do that ubiquitously across all of your data, you know, because it's off of a single platform, and you're hitting that along the way, you now have the ability to make sure that every single time consistently, that you're getting access to only the data that you should have access to, and that it's being protected in a way based on the context in which we spoke to earlier, where you're accessing it from and where you're at what you've done recently, and putting all those different components together to make sure that we're protecting where we're implementing the security posture in which that agency has asked us to do.

33:13
You know, I was just thinking, if I drag someone here from France is teaching them English and had them listen to our conversation here. This person might say, well, that sure sounds like zero trust architecture. I mean, the words you were using, it's almost painting a picture that's describing zero trust. I mean, it's, it's not using that terminology. But what you're doing is you're you're limiting a person's access to certain information,

and you're confirming who they are, before they go up the chain. And it it really is, I know, zero trust, is it just a model kind of a concept, and so is a secure access service. But it seems like a practical way for an agency to make a move towards zero trust doesn't it?

33:52

Absolutely does. And when you start thinking about zero trust, I think everybody has raised their hands as soon as Z TNA or ZTA, however you want to abbreviate it acronym of your choosing, right? We're for we're full of them. But the but zero trust architecture is just that and it's also a zero trust policy, right? You need to figure out exactly what it is that is going to be your zero trust policy. What should your architecture look like? What are the tools in which can most easily be implemented, to then apply that policy to your architecture? And so that's what net scope does. Net scope is the platform in which applies the controls that you've deemed appropriate and we help you through that if you'd like us to write through policy and other components and how you have it architected within the net scope confines but it's also where you You're accessing that data and what controls you want to have in place. And once you do it once, once you figure that out, it's a policy that's been applied. And it's ubiquitous across the entire platform. So no matter what one or many users can have that policy attached to them across all the controls, whether it's data threat, basically looking at the Cloud Confidence Index scores, using, you know, user entity behavior, analytics, machine learning, AI algorithms, all that within the construct of a single platform. And so, and again, this is all based on what we were talking about earlier, the new edge architecture, so you're doing it at speed is the most performant cybersecurity network in the world. And what we've done significantly different with our FedRAMP, high instantiation that just passed our three P ao audit last week, which is great, and we're moving. This is all based on new edge. This is a private New Edge network set up cones for our federal customers. So it is a telco grade network that is massively different than how anybody else is doing it.

36:15

It sounds like the old CDN content delivery network. Yeah, we manage it better, and we're faster and better. Sounds good. So what about so on premise part of the conversation, too? I mean, it's not just limited to the cloud, right?

36:27

No, absolutely not. So that the cloud is if you go back to Gartner definitions and how we grew up than the first definition that was attached to NetScaler. But as we were growing up with Caspi, cloud access security broker, and it was really the concept of protecting all of your data that lives and breathes off premise, right? Anything that's in infrastructure, platform and software as a service out on the web, and being able to put those controls around that whatever level of controls that you deem appropriate. And then you then you bring in the concept of private access, so the new modern VPN, right, the next generation, whatever you want to call it, VPN, but it literally is the control mechanism that allows you to access whether that data is on prem or in the cloud. And so if you, you're gonna hit our control plane, first, our service. And then if that data is back on premise, we will give you the access in which you've been allowed to have access to that data back on prem. And then contextually aware, again, of where you're at, you know, what you're on, you know, and, you know, the network in which you're coming from and your recent behavior that is either risky or less, less so so then, then you're granted access.

37:52
Yeah, contextually aware. Well, unfortunately, we're running out of time here. We have to end this interview. You have been listening to the federal tech podcast with John Gilroy. And our guest today was Bo Hutto. He's the Vice President federal at Knightscope et et Skop. Thank you both.

38:11
Enjoy. It's been a pleasure. Hey, thanks so much for the opportunity.