FEDERAL TECH PODCAST

How to optimize federal identity management

Thu, 6/2 11:54AM • 26:58

SUMMARY KEYWORDS
trust, people, password, technology, important, security, attackers, folks, cybersecurity, credential, kinds, unfunded mandates, talk, identity, management, chase, podcast, access, aws summit, mfa

00:00
Hey John Gilroy here recording this from the AWS Summit in Washington DC Sean Fraser from Okta make sense of all the acronym soup involved with zero trust architecture or ZTA.

00:16
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 like the federal tech podcast, please support us by giving us a rating and review on Apple podcast.

00:39
Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Well, here we are at the AWS Summit in Washington DC at the Washington Convention Center. Last night, I was in the local Whiskey Bar. And the guy next to me starts throwing down shots and I said, Hey, you want to be my podcast? Aren't we said certainly. To be dragged in Sean Fraser here, the CSO at octus. Sean, how are you?

01:02
I'm great, John, it's always good to see you. And yeah, whiskey bars. That's my that's my thing.

01:07
That's your jam. Well, anyway, just grab people in coffee line waiting in line drag him in here. Yeah, actually, Shawn is very well known in the federal community. And today we're gonna talk about identity management and zero trust and access management and digital transformation and all kinds of different topics. But before I ramble on endlessly, it gives maybe a thumbnail sketch of your background, Shawn and a little bit about Okta. Most people know a little bit about Okta.

01:32
Sure, yeah, John, I've been around the cybersecurity realm for longer than I care to admit. So probably about 2025 years, not all of it in public sector. I live in California. So I spent a fair amount of time working with innovative startup companies as well, but my passion is is protection and in cybersecurity. One of the reasons why I find myself at octet because I think Okta being the premier cloud based identity and access management

solution has a very important role to play in cybersecurity, and specifically around zero trust. And this this world, we find ourselves in with least privilege being the important rule of the day.

02:05
Yes, yes, yes, yes. Go to Google Trends. You type in zero trust. It's up into the right. It's a hot topic. It's a hot topic. And banks in Chicago. It's a hot topic and tire stores in Boston and in federal agencies, and we're certainly surrounded by federal agencies here. Well, I listened to a lot of podcasts. And we're on a podcast and I was listening to this podcast, and this guy from Australia was being interviewed, and these guys from Australia, and they're really rough. And and he said, the interviewer said, are the tools that we use for zero trust? He said, Well, tools are fine. They can't use a hammer to make a cake.

02:39
That's probably true. For the job.

02:42
So is Okta tool. Is it a platform? Is it a methodology? So it's active for our listeners?

02:48
Yeah. So I think it definitely is a platform. So when you think about kind of modernizing your identity stack. And we've been doing identity for a long time, right? We've always had to log into things as long as computers have been around for the most part. But modernizing that and making that kind of work at scale. You need a platform approach. And that's really where Okta kind of comes in being the platform. I think that there's still a lot of philosophy involved in what Okta does, for example, I always tell people that zero trust is not a product at all, you can't buy a zero trust at the grocery store. This is something that you kind of have to bring in it's kind of muscle memory. It's a skill set. It's a it's a lifestyle change in your cybersecurity realm and Octa, we have an important role to play to help people do that. But we can't make up zero trust.

03:29
It's right. There is a bromide how's that for fancy word, that kind of an observation that people make about technology in general, and let's say, maybe an axiom, by the way, let's see if it applies here. Some people say that the people who understand zero trust can't afford it. And the people who can afford it don't understand it. Says that situation with the federal government.

03:53
You know, I think the neat thing for me about zero trust is it actually if you look at it really for what it delivers. And again, if you think about it as as kind of changing your thought process, changing your model and around how you deal with security, you actually can take this opportunity to simplify. I think it's one of the things where it's one of the few things I think in cyber where we haven't just layered on over time, right? If you think about the kind of the layers of land, right? If you've ever been to Rome, and you see how they dug down through the layers, right, and then ever layers like 100 years and next thing you know, they call it, they call Rome, like the lasagna of of architecture, right? Because they have all these layers of time. Well, we've been living in that in

cybersecurity where we've been just layering things on top of another thing and next thing, you know, you're like 10, layers deep, and all this technology and all this new cruft. And you create a complexity and the only beneficiary of complexity is the attackers. You know, the users don't benefit from complexity the attackers do. So zero trust has a chance to kind of flip that script a little bit. And think about it in more simplistic terms of just worrying about the data, worrying about the access and making sure it's easy for the users and make sure it's hard for attacker so yeah, folks saying they can't afford it. Yeah, I get that you spent And on these 10 new things, and this is what you think is this is the 11th thing. But if you could remove eight of those 10 things, then you're actually ahead of the game, I've

05:07

got a big sister logo in front of me, it's pretty impressive got an eagle in there, it's kind of kind of like Tronic things and, and every time, I imagine if I went to a local McDonald's, I see a sister logo, I see him everywhere, it seems to be very, very popular. They're getting some funding and being made more demonstrative in the area here. And they come up with all kinds of recommendations. And there's companies pillars and everything and say, one of the pillars of, you know, zero trust. The first pillar is identity. And so I imagine that's why some people should start talking about identity and access management factor, because it seems to be the starting point for zero trust. Is that right?

05:40

Yeah, it's exactly and I think that I love the fact that they even kind of joke themselves that security so important, they put it in their name twice. So I agree with them, it is pretty important. What I really love about CES is it really brings a sense of community to cybersecurity in the public sector that we haven't had before used to be kind of silos, all the different agencies kind of did their thing. And there were certainly communities mean, you know, CISOs, from one agency would talk to CISOs, another agency, but I think Sissa kind of codifies that by creating this community approach. And since it didn't invent those pillars, those pillars came from work that was done for a while over the last handful of years. So there was the Fed CIO Council put together this research about five years ago that me and other folks were a part of around zero trust, which culminated in 800 207, which is the NIST documentation on zero trust. And that's where the pillars started to really be talking about. And what Cisco did was just kind of put a fine point on it, and really kind of codified the pillars into something that were discrete and people can understand. And there's no accident, that identity is the first pillar because nothing really happens to someone or someone accesses something. So having, you know, having strong identity and access management, whether it be secure single sign on, or multi factor authentication is usually where you got to start in this journey.

06:52

I'm looking at this logo, and it does kind of repeat itself and ever notice that, you know, two weeks ago, I interviewed a guy named Jason gets. And we talked about dev ops and Dev SEC ops, and he said, My company puts the second dev SEC ops. And I said, No, no, I put the fun in fundamentals. But maybe ces puts the cybersecurity and cyber security into Cyber Security does wrap it all in and say enough times and it'll raise important maybe they should have twice more. We know Sean, I've done many interviews with you and all kinds of different people. And, you know, one character kind of stretch. It's a stands out, his name is Brigadier General Greg touhill. He's just a fantastic guy. He's just an every category is great. I mean, family, man is smart. And the military is got all can check, pass check match up. He is. I think he's teaching school in Pittsburgh now and running around with search. So what role does public private organizations have in this whole transition to zero trust for a federal government?

07:47
So first of all, I'm a huge great to Hill fan. So Greg's an awesome guy, he, he's one of those, I would say, early believers in zero trust architecture, there was a time where there was a kind of handful of us floating around the beltway, and we would meet down at NIST and eat stale doughnuts and drink bad cold coffee. Be like 10 people in a room talking about zero trust and lamenting it. And I think, you know, obviously, John Kinder bag is kind of the father of zero trust. And he's done an amazing job kind of bringing it to the forefront. The folks like Greg and chase and others have really kind of brought that into public sector. And they were kind of true believers from the beginning saying that this is the path, right, this is where we got to go. So I think that that's important, because, you know, again, folks who have been kind of steeped in cyber for years and have looked at kind of the things that we've done over the years, and some things we've done right, and some things we've done wrong, have seen a better way. And this better way really kind of culminated when we went through with the pandemic, where everyone was kind of forced to kind of work from home or, you know, not go in the office, and we still needed to be able to solve the problems and do our jobs. And we needed to do it from a technology perspective. But we also needed to do it securely and zero trust was really made for that moment.

08:55
There's an episode of Seinfeld, we talked about naming names. Remember that so I'm gonna name names. And what you did is you named names. You named Chase, Cunningham.

09:03
Yes, I did. I dropped the chase name.

09:06
He is a well known scoundrel in this town. Let me tell you about Chase. He's got five patents, five books and a PhD. I don't think he's that smart. Hey, not that smart guy and I need to get to work on springs.

09:17
Oh, man, I love Chase. I'm a big fan of him, too. I love him because he's, he's, he's a pragmatist, right? When you talk to him, it's like, it's right there. What do you think? And he's telling you, and I love that about him. And he's also one other one who has really kind of, you know, kind of move the needle on, you know, different thinking around cyber and you know, and obviously, he's got his podcast and a bunch of other things that he does and, and he's very passionate about it. So very, very passionate about getting it out there.

09:43
Are you referring to the doctor zero trust podcast?

09:46

I am. Yeah, I have not been on that podcast. So I'm not sure what's wrong with that or what's going on with that but

09:52

well, let's go to his house tonight in the shot around he's kind of a weakling isn't it? Well, Chase is working on this project. He's got this type of wall in his house. Also, he's putting all these companies together that are part of different parts of Xero. Have you seen his chart? I have this magic chart. And it's like, how do you magnifying glass? Or has he put us all together? It's several graphic artists, but he's trying to sum up the world of ZTA, zero trust architecture. So it's graphically understandable. It's it's a noble, but futile, cause I think,

10:22

like so futile, I think it's important to be able to tie it together. Because I think one of the common places that people get stuck is how do I do it? Right? We've been talking about for years what zero trust is, and most people, most people understand it now. But then the next step is, well, how do I do it? How do I implement zero trust? I think, you know, it's definitely a noble effort of chase to try to put bring all the players together talk about who does what, in the zoo, right, who's who in the zoo for zero trust? And what what role do they have to play? You know, I think at some point, you know, commit to this on this podcast, Octave will be part of that, I know that he's reached out to me, and I've been remiss in getting back to him, but I will, I promise. So recorded, it is being recorded now. So I'm committed now I'm committed, so it's there. Um, so I think it's important, it's also and it's very analogous to the work that's being done at NCC OE. So the cybersec, at the National Cybersecurity Center of Excellence at NIST, has put together the zero trust building blocks. So a lot of the same people who are kind of doing demonstrations and putting together the information for Chase are also the same people who are coming to NCC OE and doing the reference architecture, because again, what we're trying to show folks is, you know, what does this look like in practice? If I if I have a network, and I've got access to applications and have users coming in? How do I wire all this stuff together? So it's important to have those reference architectures and those visualizations, because as we all are visual learners anyway, rather than reading the book, you could actually go see the movie, and you can actually kind of see the, you know, the reference architecture in action.

11:47

Well, here we are at AWS Summit in Washington DC, we can probably take a little stroll and visit 20 different federal agencies within walking distance here. And I'm certain that if you walked into the coffee room there and talk to one of the technical folks there, there'd be a Fraser popped up and the phrase is going to be unfunded mandate. It's my wife says, Well, we're gonna have to take and redo the kitchen. Where's that money gonna come from? And well, we still need to redo the kitchen honey. unfunded mandates. Now, in universities, they have unfunded mandates. This was some ROI on this. What about isn't? So how do you justify ROI for making a transition to zero? Trust me? Is it that obvious? It's just implied or? Or how does the government agency justify the expense?

12:29

So I think it's important to think about really what it is and and again, back to my kind of layered lasagna analogy. If you think about it as another layer on top of the stuff you're already doing, then yet, it's unfunded mandate, I got no money for this, I'm already paying for these 10 things. If you think about those 10 things you're paying maintenance on already, right, your your eye cam solution, you're paying maintenance on, you know, your your, your your endpoint, posture, assessment, solution, all these different things, they all play a role in zero trust. So you can leverage those things, you can either kind of use that money for different technologies in those spaces, or you can say, I already got these pieces, I just need to figure out how to put all these things together. So you what you end up doing is you end up again, building that muscle memory around security. It's not really a technology problem. And if you look at zero trust as a technology problem, you're not looking at it the right way.

13:16
Okay, we have a American culture question. This is a category movies 1951 Are

13:22
you ready? 51,

13:24
you got to come, we got to get to 1819. There's a movie called The Earth Stood Still. And there's a robot in the movie and $400 Shawn, what's the name of the robot?

13:36
Gore, Oh, I lost the $100. You pick the one movie that I always get to know something

13:45
about robots, increasingly in federal systems. And there's this thing called robotic process automation. And it dawned on me what they need to do need to, don't they? I mean, they have to have credentials. And so how does this automation? And does this throw a monkey wrench in the whole works of zero trust?

14:03
So you definitely have to think about automation in a couple different dimensions. So the first dimension is, there's just too much for people to do, right. So you need to be able to do analytics have to be automated, you need to be able to do kind of assessment, for example, when someone logs into something and you do continuous authentication, you need to be able to do that automated in an automated fashion. And you're right, there's the IoT, right? There are things that there are devices that log into networks that request access to data, so they all have to be part of your model and your thought process around zero trust. It doesn't throw a wrench into it as much as it you got to figure out where it makes sense to automate and where you can't automate things. So again, making assessments doing determinations on large datasets. That's right for automation, because humans can't read data that quickly. So automation is going to play major roles there. Specifically around cybersecurity and don't think for a second that attackers aren't using automation to attack you. So you know, at least in our world, you got to use it for defense as well.

14:57
Okay, television shows the 1960s All right, we're narrowing. Isn't there a TV show that survey says to attribute some shooters anyway, here was Family Feud. Survey says, Okay, here we go. I was reading results of a survey this morning survey says that only 35% of people said they're very familiar with zero trust concepts is that high or low for you?

15:22
It seems a little low. And I think mostly again, because we're thinking of this as an other thing. The zero trust concepts are really steeped in things we've been talking about for 20 years. And I always kind of point back to the least privilege, right? When you start out access to something, you start out with no access, you get access only the access you need. Whereas Conversely, in the world, we've largely said, If you log into something, you got access to everything. And that's where you got prompts a lateral movement, once again, you get credential compromised, someone gets your credential and logs in as you they can do anything. So at least privilege has been around for a long time. So I think a lot of the concepts of zero trust people already know if they dig down a layer deeper, and you talk about things like lease privilege, and you talk about things like multi factor authentication that are things people have been working on for a while. A lot of the constructs people know, it's just the new name and people like oh, yeah, I don't know what this zero trust thing is. Well, that's all it is. It's just kind of a rebranding of philosophies we've had for the last 20 years.

16:13
I don't know if you know, Matt Alderman or not. I think he works for the cyber risk Alliance. And he wrote an article I was taking some notes on last night. And he said, the biggest obstacles to identity management, zero trust are management support and budgets.

16:27
I think that's the biggest obstacle for almost any program or project within an agency is management support and budgets. I think there's a culture thing that we it's kind of the elephant the room we don't always talk about, there's two dimensions of culture that I always think about. One is the user culture, which is always changing, right? So we have this expectation of user experience, it's much higher than it's ever been before. And we have to kind of recognize that in the workforce, we got to bring in technologies that I call them, the kids because I'm an old guy that the kids are used to using like touch ID face ID, their iPhones are used to, you know, kind of paying for their Starbucks and paying for their things with, with Venmo, and all these different technologies. And we got to kind of replicate that and bring that culture into the enterprise. But the other culture thing which you touch on is, it's the management culture, right? It's the management culture of bringing security in culturally into an organization and having management buy into that. And it's not just the security people, right? It's not your just your Cisco, and the folks doing security, they're already steeped in the security world, it's your business line owners, you know, it's your business, folks in your management have business of kind of convincing them or talking to them about why security is important to build in to their applications from the beginning. And the pushback commonly is always well, it makes things harder, it makes things harder for the users, it's harder for me, it's more money. But again, at the end of the day, if you think about the constructs

that you can leverage some zero trust, you actually can reduce your security footprint, from a technology perspective, save yourself some money, and you get better user experiences in the bargain, because we talk about things like webauthn, right? That's an enterprise technology that's tied into to biometric like touch ID and face ID. So you kind of get the benefit of that, that user experience high bar with the benefit, benefit of security, and you just have to be able to have that conversation with the business owners to be able to get them on board.

18:06

There's a guy in town here has a website called Dotson bridges. He tries to connect dots and build bridges. And think that's a fun thing. And I'm trying to build bridges right here. On my left, I have a statistic here from SC magazine. They say that 73% of top attack techniques involve mismanaged or stolen credentials. On my right, I have the three sis a bad practices. And number two is poor password management. It says it fits in perfectly with this discussion does it's almost like they coordinated that. Yeah, what's going on here? I mean, what is commercial organization? Of course, and this is this is ces a bad practice. Number two is poor password management. It seems to be prevalent.

18:45

Yeah, I think. So the the Verizon data breach report for 2022 just came out yesterday or the day before this week. And it talked about that it's still the number one hit right. You know, I was I talked about my my talk this morning about Casey case, I'm back in the 70s. Again, to date myself right to the top 40 hit. It's like the top five you know, hits of cybersecurity. There's the keep on comment or steal, credential breach phishing, it's still you know, getting access to credentials, because that's the easiest low hanging fruit for attackers. And we're still not making it hard enough for them. You know, people talk a lot about patching your software and vulnerabilities in software. And that's important, right? I, you know, I think about, you know, kind of basic hygiene for security as a couple of things. One is patch your things others MFA for identity, and the other is encrypt all the things. But by and large, you know, you're not going to get bit by someone who's going to take advantage of a vulnerability in the piece of software as often as you will about a credential breach, because it's just so darn easy for attackers to get there. And one of the reasons is in the bad practice that Sissa points out is that passwords suck, and users hate them. And they're not really good for security. So we can talk about bad password practices. The worst practice of passwords is actually using them. Because what we end up doing is we end up putting all the onus on the end user for security, we say look, you got to have a long password, you got to change that. seven days, you can't repeat your password, you can't use the same password for your bank as you do for your enterprise. I mean, users are fatigued around cybersecurity to begin with. And what you do by creating these complex password requirements is you just make it worse because you've made it long. And they got to change it all the time, they're going to write it down. They're going to reuse it over where, and we can tell them to use password managers. And I always encourage people to use password managers. But the fact of the matter is, it's hard for my mom to use a password manager. It's hard for you know, most people use password managers, IT passwords themselves are just too difficult. So what we have to do is we have to find a way to get rid of passwords. And that's what a lot of us like Octan folks are working on which is how do we leverage you know, open standards like webauthn to kill the password Finally, after all this time, we referenced

20:44
Dr. Chase Cunningham earlier and in his LinkedIn fess up this morning, it was hashtag kill the password.

20:51
Seven hashtags are appropriate. Here we're simpatico man, we're thinking the same thing.

20:55
I was taking notes during your last few words and used MFA. For the first time I heard that, because I'm involved in academia as Oh Masters in Fine Arts. No, you idiot. No, John, that's not an AMA Yeah, it's a Master's in Fine Arts, you go to Boston, that's all kinds of you can write is no no multi factor authentication and comes right back down to the bad practices. So number three, on the CIS a bad practice list is guess what? Use of single factor authentication does.

21:27
Yeah. And again, if you're single factor is that password, which by the way, is so terrible. And so easy for an attacker to get you need to have something else if you if you must use a password, you have to use MFA. And and the thing with MFA is, again, it's a little bit of a necessary evil because we use the passwords. And I'm hopeful that in the not too distant future, we have kind of strong single factor thing like webauthn, which has all the strength of MFA, but until we do, we have to use multi factor authentication because the password on its own isn't helping us. And it's one of the reasons why the hits that keep on common are credential breaches, and phishing and all these different things. Because if the password is the only thing that the attacker needs to get access to something, it's a pretty easy thing to get.

22:05
I'm a big fan of, uh, tools on the interwebs. I use tools all the time, I use tools that measure speed websites, I use tools to discover keywords, I use tools to evaluate HTML code, all kinds, I'm a big fan of using tools. And I was at your website, and there's a zero trust assessment tool that you have there. Is that practical for GIS?

22:24
It is, because it's all the same concepts. I mean, all the things that that that private sector organizations are trying to do are the same things that public sector agencies are going to do so guppies are looking at all the same thing, there is no different technology, there's no special technology that a government agency will go by, that a commercial entity can buy a commercial enterprise can't buy. So it's all applicable all the things that you need to do your, your your journey, what you're really doing is you're tracking your journey, it's almost kind of like a weight loss goal or an exercise regimen where you got to track your journey on zero trust. And oh, by the way, just like a weight loss goal or an exercise regimen, it never ends. You never have an end point where you say, Well, I'm done. I'm zero trust, I'm good, right? Security is the gift that keeps on giving, you have to keep doing it. Let's

23:05

track back to unfunded mandates. And I tossed that kind of facetiously and light hardly talked about it. But there's a way out and the way out maybe with the technology management fund the TMF. And what I noticed on your website, was that and I wrote this down, and I just got to make sure that believe this. So what Octa can do is that can help agencies writing zero trust project proposal to the TMF. Really, that's fantastic.

23:32
Well, we want to try to make it easy, because again, as you point out, you know, and I kind of mentioned the fact that you can find other buckets of money to make it you know, so you're you're not thinking of this as another mandate that you've got to do on top of all the other things you have to do. But one of the things that it's important to do around zero trust is you gotta have to take kind of a center of excellence approach to this. So it's got to be it's got to be pervasive in your organization. I talked about business owners being bought in security teams need to get bought in your tech ops, and your operational folks need to get bought in what this this can kind of help you do. What the TMF funds can help you do is build that muscle memory inside your organization that doesn't exist yet. So rather than just going and buying technology, you got to build a plan. So building the plan is where you can spend the money.

24:11
I have a neighbor named Alec, and he is a high level Microsoft Enterprise Architect, really smart guy, and he works out of his house. And he works with several sensitive agencies in that regard. And if I say the ad to him, I'll Active Directory. Sure. Anyone knows that. However you can folks have something called universal directory, what's the difference?

24:30
So it's a similar concept. The difference is that octave is kind of born on the cloud. We are a cloud only cloud first technology company we were founded based upon the fact that we knew the cloud was going to be important for all aspects of technology, including identity and access management. So universal directory is that cloud based Uber directory, you know, think of as a meta directory for all the entities that you may want to track authentication and authorization access into application. So I would say it's a it's a updated, more cloud focused version of

24:59
that. Oh, Here we are in May, June here in 2022, and all kinds of events going on AWS Summit, all kinds of summits and all kinds of conferences and everything else, I think in a few weeks is going to be the GOV identity Summit. And so coming to town here, what should listeners know about this?

25:15
Yeah, so this is our kind of flagship event that we we've done in the last couple of years, obviously, last year was a little different because of just the world being different. But this is an important opportunity for government folks and for industry to get together and talk about identity as being that first pillar of zero trust and how folks can embark on that journey. We'll be talking about some of the work we're doing with NIST and with NCC OE, we'll have some customer testimonials, customers, we talked about exactly how they're

leveraging Okta to kind of solve these problems in their organization. And it's a good opportunity to just kind of meet and mingle and talk to your peers and figure out how, how far down the rabbit hole of zero trust some of your friends are. And maybe you can get some help.

25:53
It's like, it's like listening to a Mustang mechanic from Cleveland, Mustang mechanic, and oh, from Alabama, and then, and you find all the mistakes they make. No, I'm not gonna make that mistake. Oh, he did. Oh, well, that's where you get your carburetor from in the 1960s. You know,

26:05
we're not Sissa but we're gonna try to create a community right? So we're this is our community of helping agencies help each other, you know, on this journey.

26:14
Or earlier in the interview here, I referenced the movie. And now I'm going to conclude referencing another movie, and the movie is Back to the Future. There's a car and back to the future, the license plate and the license plate says out of time, because we're out of time here, Shawn, I'd like to thank my guests Sean Fraser, federal CSO at auction corporate. Thanks, John.

26:33
Thanks, John. Always good to see you.

26:35
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.