EP31 Improving Secure Access to Federal Systems

SUMMARY KEYWORDS
people, access, mfa, trust, permissions, privileged access management, conversations, sudden, security, solution, federal, forefront, patents, user experience, listening, business processes, thought, podcast, remote access, years

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

00:02
and I'm Josh Broadbent with beyondtrust Software.

00:04
Today we're gonna talk about Privileged Access Management hit the music cloud.

00:13
Welcome to the federal tech podcast where industry leaders share insights on innovation with a 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.

00:36
Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Our guest today is Josh Broadbent, regional vice president solution engineering for a company called Beyond trust. And we're gonna delve into something called privileged access management. And it's a topic that needs to be brought up because we're in the world of the hybrid cloud, the multiple cloud, public cloud, private cloud, and everyone's concerned about identity here, especially with these initiatives that involve zero trust architecture. So I'm gonna jump right in here. Josh, I heard about your company from a previous guest. And I thought to bring in because I've never heard of you. Maybe you can give us a nutshell, a bit 32nd description of what beyond trust is all about?

01:19
Yeah, sure. So beyond trust is about intelligently protect protecting identity access, especially specifically around privileged access accounts. So what we want to make sure of is that those accounts that are privileged, such as admin accounts or network accounts, those types of accounts are secure both inside and outside, we want to make sure that those particular accounts have the ability to be used by the administrators that are there, while at the same time their password and credentials are secure.

So we want to make sure that there is as little threat vector as possible across all of those privileged accounts that may be inside a network to manage that particular network.

02:08
My wife went to Oklahoma, and she follows the team year in year out. And whenever they have a winning season, everybody's an Oklahoma fan, yay. But with have a tough year, you know, no one's a fan. And I see this thing happening with privilege access management. I've been doing interviews about federal technology since 2006. And you know, I know companies who've been around since then all of a sudden, you're their website, and they say, privileged access management. It's like, when I went to your website, it wasn't a bolt on, it's like, no, we've been doing this since the beginning. Is that right?

02:41
That is right. So we actually have over 70 different patents. And in this particular space, we actually have patents going all the way back to the 90s. And I know some of the listeners will go, Hey, look, this wasn't a thing in the 90s. Well, you know, early 90s, we had the the advent of Linux systems, Linux servers, and we basically had the progression of sudo and sudo type elevation commands. And we needed a better way to manage that. So we actually have some patents around that, moving all the way up into into current. So this is something that we've been doing for a very long time. This is not a side thought. For us. This is not something that we've we've thought about as an afterthought, but it has definitely been a core focus of who we are for, for the length of our business.

03:36
So if you don't get the link to your business, you've been out there screaming in the wilderness. And all of a sudden, we have COVID hit, we have the federal federal governor with a move towards remote access, different type of cloud, and all of a sudden, the on trust is in the headlines here, because all of a sudden, you have a lot of deep experience with this. And they can rely on you and providing information about access management, from soup to nuts. So it's really positioned yourself really well now, doesn't it?

04:00
Yeah, it's it's definitely been a change the last few years, we have found ourselves at kind of the forefront of this conversation, both from a privileged access management perspective and a remote access perspective. When COVID hid, have in March of 2020. It didn't seem like the work was going to stop from a remote access perspective for a while, and it didn't. And we've definitely been having these conversations about how to secure remote access. People didn't know what to do. It was amazing how little preparation had gone into our thought had gone into, you know, work from home. We had state governments calling us going we're not prepared for this. We need a solution, you know, by this weekend to be able to have all of our workforce work from home. So it definitely put us in the forefront of that conversation. And now as we are on the you know the backside of that, not only the work from home conversation, the remote access conversation, but but also that privilege access and zero trust conversation around how do we handle this from an MFA perspective? How do we handle this from a perspective of of zero trust and a password list movements? Right? That's that's kind of happening. Aaron, who is our federal marketing director, she and I have have been putting in a lot of hours supporting conversations all across the country in in this particular topic. And we regularly see rooms at

conferences that that are standing remotely as we have these conversations, and we're constantly invited back. And that is, I think that's a, a definitely a pointed moment towards the topic and the timeliness of the topic. They're certainly not coming to hear me speak. But you know, they're, they're coming because this is important right now. And we find ourselves kind of at the at the forefront of it. So

05:58
well, someone's coming to hear you speak ATAR has got a whole working group on zero trust. And I think you run it, don't you?

06:06
Yeah, so I am the industry chair for the a torque Working Group on zero.

06:10
Come on. Now. Let's you know, let's just talk about truthfulness here. And I think I think the I went there this morning, and I saw the members of the group, this wasn't some old boys club out of Silicon Valley. Now, this is people from the federal government. This is people from the industry. This is someone like you who's trying to herd the cats, and everyone's get a chance to talk about what they need. And when he's talking about listening, I think that's listening in a small group like that six, eight people in a room zoom call. Boy, you can learn so much more than a big conference, it's 100 people in the room, isn't it?

06:39
Oh, I mean, absolutely. And, you know, I, I'm going to absolutely give credit where it's due, as the industry chair there, it has been an eye opening experience to listen to the government chairs talk in that group, they they do a ton of work there, they do a ton of that research and organization themselves. It's It's honestly, they, they kind of make that show what it is. So I don't I don't want to take anything away from from the government chairs that help with that group. But yeah, you know, as we have conversations around zero trust, as we have conversations around the things that they do, they definitely, you know, it's it's definitely something that we have had to that we've had to have conversations around and work through. From Biden's Executive Order, all the way through, you know, guidance that Cisco has put out just a month ago, it's something that constantly has been at the forefront of government. And as one of my co workers said not too long ago, it's a place where we, the government is almost leading the public sector in this particular space here recently, rather than the reverse, right, so with the way that they're handling zero trust architecture, with with NIST, with Sissa, putting out maturity models around it. And, you know, having the conversation about privilege access management, and how important that is to it. It's 100%, you know, a spot where the government is actually kind of putting together a plan for this, which is exciting.

08:14
I went to your website beyond trust.com. And then it dawned on me zero trust, while he went beyond just before zero trust was even topical here. Anyway, beyond trust.com. And what it says is you protect identities, you stop threats, and you deliver dynamic access. Now, I know a little bit about role based access, live about attribute based access, but dynamic access, I haven't even been caught up to even catch what that means.

08:40
Right? So the concept around dynamic access is the thought that it's not just about your role or an attribute, but it's also about understanding what you're doing with your access, where you are location, time of day. So we want to respond dynamically to when you're making that request. For instances, this is a normal request for access that you make, during the course of your work during the day nine to five, you're sitting at your desk, you know, we're going to probably have a lower level of workflow for you to step through to be able to authenticate for that. If all of a sudden it's two in the morning and you're accessing via VPN from China. You know, all of a sudden, this might throw off some red flags. And we're gonna require some manual approvals before you get access to the things that you need access to. So we're going to dynamically adjust the the appropriate level of permissions, the appropriate level of, of workflows that you have to do to authenticate based on where you are and what we would perceive or the you know, the software would perceive to be the threat level that you represent at that moment. which the same person can represent a significantly different threat level, regardless of of where you are. So

10:08
I guess everyone has studied a little bit about Japan and maybe learned about their manufacturing process. And, and one of the big innovations and the 70s and 80s was just in time delivery. And so they could manufacture things efficiently because it was just in time. And I think people today are appropriating that term from, you know, the type of manufacturing system in Japan, they talk about just in time access. And so platform or a system that is designed to allow access quickly, it would fit in time with it, I think they have an acronym now, JT, so Justin time is, is talked about a lot in federal government, isn't

10:43
it? Yeah, absolutely. So the idea here is, is pretty simple, and honestly straightforward. What we want is for people to be able to do their jobs. But if they require an elevated set of permissions to do their jobs, we want to deliver those set of permissions, while not allowing those permissions to sit vacant. And what what I mean by that is, if they need those permissions for 20 minutes of the day, we don't want to sit for seven hours and 40 minutes where that accounts not being used, that permissions not being used, where essentially it becomes or represents a potential threat, or something that a threat actor can use, to, you know, to have a breach or to have lateral movement around. So what we want is a situation where they have access for exactly how long they need it. And however long that may be, we don't want to impede the mission work that they're doing, we don't want to impede the job function that they're doing. But then when they're done with that, we want to make sure that that access is appropriately removed, so that we just don't have those extra credentials or those extra, those extra things floating around out there. So that's that's kind of the concept there. Same with, you know, the it's the manufacturing concept, right? It's about making sure that you have inventory hitting the floor just in time to assemble the component. And you're not sitting on a bunch of extra inventory. Right? Well, this is that but but from a security concept.

12:09

So Josh, you obviously listened to garvies at a talk and throughout your career, you've listened a lot of guys, I'm sure. And so I do want to bring up this topic, but well, how do people fail at Access Control? What's the biggest failure point here,

12:23
there's a lot of ways that people fail. And really, I think, when we talk about access control, a few of the biggest things that happen is number one, a lack of understanding or planning. You know, understanding what we're trying to achieve how we're trying to achieve it, and then planning for what that's going to look like in a future state. So that as I said a few minutes ago, so that your your mission is still achievable. When you begin to plan for access control, you can make the mistake of putting security so much at the forefront of it that you are not allowing your admins to do their job. And before this, I ran a an MSP. So I sat in the seat of doing the daily admin chores. And as an admin, I can tell you, if something gets in my way of doing my job, I will find a way around it. So when you're looking at access control, if you're not focused on the user experience of the tool, you will absolutely fail at delivering access control. That's, that's, you know, number one. Number two, is something that is as old as as admin permissions themselves. And that is that that idea of, of permission creep, right? As you get friends inside your IT department, you know, it's really easy to say, hey, look, I need permissions for this one thing. And so a buddy who is an admin of that, all of a sudden adds your permissions to this next thing. And the next thing you know, you have 20 people who are domain admins, and none of them are actually active directory admins, just because they needed permission to one particular attribute. So as they handle access control, you know, we see a lot of we see a lot of that we see a lot of pushback around. Well, anything else, we see a lot of pushback around change, right? So people have been doing access control similar or the same way for 15 years, and they don't want to see it doing anything different. And they see a tool that's designed to go in the middle of something that's designed to impede their work, and it's not. So a lot of times we will we'll see a lot of, of resistance in deployment, as they're attempting to work through a certain thing to work through it. Just because they're afraid of that change. They're afraid of those business processes. And I mean, I guess that's that's another thing that that really impedes tend to the entire access control conversation is we've put in workflows and business processes to handle how we did things 20 years ago. And as we're implementing new tools, we don't want to have conversations about those business processes, you know, to match the tools that we have. And so sometimes those are required. And as you well know, people, people in government are they're really easy to change things. And I'm saying that sarcastically, you know, we still use manuals in in the army from 50 years ago for procurement. So, you know, getting people to change business processes and workflows. To match what it's going to look like in a in a zero trust environment is is a challenge sometimes,

15:33
if you're listening to this podcast and want to hear more about maybe a solvation variation on this, you may want to listen to episode 25, controlling the hybrid cloud with Rob Kerry from Cloudera. This morning, I went to a Federal News Network. And lo and behold, you wrote an article for them a couple months back, and in the article, you talked about multifactor, access MFA. And shocking news. I think you said that MFA may not be enough for some access control. What's your take on that?

16:03

Well, in probably my biggest bit of of prophecy yet, claiming you better claim it, buddy. Yeah, I wrote that article. And in the last month and a half, we've seen two different major breaches where people have leveraged a form of social engineering that I like to call MFA fatigue. To successfully breach they've been so far they've been corporate customers. What happened at Cisco in August? What happened last month at Uber? You know, those wonderful little, I'm going to spam your MFA thing until you think that it's you and you're going to accept it. And actually talked a little bit about this on a systems integrator roundtable, about a month ago, what I'm most worried about around MFA and the reliance on MFA as this kind of this faux passwordless solution, hey, look, we're going to rely on that second factor of something you have, rather than the things that, you know, you know, that's the idea, we're gonna skip the thing, you know, we're gonna go straight to the thing that you have, right. And I hesitate to say this sometimes, but I'm gonna say it, we're assuming that our user base is smart enough and steady enough to handle the power that comes with that. It was, it's been attributed to many different people, the way that I heard it attributed was to a park ranger at Yellowstone that said, the challenge with making bear proof trash cans is that there's significant overlap between the smartest bear and the dumbest tourists. That is, it's the park

17:43
and say, probably graph that out.

17:46
So, you know, it's the challenge we have in IT security comes to that when we when we go back to MFA for security, as much as it is something that I firmly believe in. In fact, I probably have too much done because I have even the two FA app on my phone is YubiKey secured. So I have to plug the YubiKey into my phone before the little OTP app will appear on my phones, you are assuming that at some point, people are going to not be overwhelmed with this MFE fatigue, they're in the middle of doing their work. They're getting 1500 pushes from 1500 different apps. And we're assuming that that that's that they're going to just know that they have to click no every time, right and that they need to report that instead of just thinking oh, well, I'm doing my work. So it must be re authenticating in the background, or whatever it is. People who do tech understand that people who do finance and not tech may not understand exactly how that works and relying on that is going to be a challenge in the future. You know, and the truth is that we're all susceptible to these weird things in weird ways. This is an anecdote that happened last night. There's a table in my living room that we set up to play board games sometimes. And my son was studying with his mom doing some flashcard review. And so I had taken my laptop into the kitchen and I had left my wireless mouse on the table. And my son fidgets a lot he takes after his dad. So I'm working on my laptop and all of a sudden my mouse starts moving. And you know, I'm kind of looking around for a second I'm like, did I touch my touchpad what you know what's going on? Well happens three or four more times and I just turn off my computer. I'm like, somebody has no idea what's going on. I just straight turn off my computer.

19:39
That's an insider threat but

19:42

but but that's the way you know, that's the way security guys are trained, right? Like, I don't know what this is until I figured out what is my computer's turning off? Yeah. So I walked in the living room and I looked at my wife and I was like, I have a problem on my laptop. Like I don't know what it is. And my son who's in eighth grade looks at me and he has Hold up the mouse and he's like, is this still connected to your computer? Ah, you little brat. But, you know, it's an anecdote of, you know, I'm, I'm an IT professional of 25 years, right? And in that moment, it's my son that's unknowingly playing a prank on me. But I have no idea what's going on. So the first thing I'm going to do is is panic, right? Well, luckily, my instincts are to panic in one particular direction. I'm not sure our end users are trained to do the same thing.

20:34
And so what you're suggesting is maybe a safety net would be there, where it prevents some of these things from happening. And so one way to manage privileged access controls was some kind of a platform of foundation.

20:46
Right? Exactly. So I mean, the concept that, hey, look, you know, this isn't just about let's install some MFA, but it's actually about let's have some dynamic access control and understand that we're not going to push MFA every time if you're sitting at your desk. That way, if you're sitting at your desk, and you get an MFA prompt, you can look at it and go, Hey, that's not supposed to happen. So we have a problem. You know, those kinds of

21:10
things. If you've listened this far, in the podcasts, you've maybe piqued your interest. So so how do you compare? I mean, why are you folks different? Why folks different? Well, there's

21:19
a few ways that we're different. And I alluded to it earlier in the podcast, the first thing is, we put the user experience of privilege access. Absolutely. First, a month ago, I spent a week with our UX team. So we have an entire team of developers and researchers and analysts, dedicated entirely to the user experience doing research, doing a B testing, all of those things, and I spent a week with them, I having conversations with them about, you know, ways that that we could support them ways that that we could improve. Because as a company, we believe that having a user experience that almost doesn't exist, that that doesn't interfere with the mission that allows people to do their jobs, is the best way to handle privileged access. And similar to that, we want to make sure that if someone does invest in a privileged access solution, that they're able to get up and running as fast as possible. So you know, we want to make sure that as we deliver these solutions, they get the fastest time to value on the market. And those are all things that we invest heavily in that we support in every aspect of our business. So when people ask us, How are how we're different, the first thing that I always go to is, you know, our focus on the user experience. And that stems from us as a company and our culture as a people of wanting our users. And believing in the concept of what we do and our users to be secure and still able to do their work in a way that is a pleasant experience, or at least not a painful one.

23:05

Well, 25 years managed services, a lot of experience in cybersecurity, where's all headed in five years? What do you think is if people are going to accept this or something bad's gonna happen before they make a transition to zero trust architecture and managing your access?

23:20
I think people I'm at least seeing motor come of support for this, I think people are are hitting that moment of, they understand it has to be done. They understand they have to plan for it. They understand that they have to get it implemented. So I think we're gonna see a lot more of it over the next five years, I think we're going to see a lot of these solutions, kind of drawing together to present a cohesive kind of zero trust solution that that fits together. I say it a lot in the talks that I give that, you know, zero trust is an architecture, NIST released 800 207. It's it's a concept, it is absolutely not just like one silver bullet product. So the thing that I think we'll see out of it over the next five years is more industry collaboration. Because we understand that as a set of products, we have to work together or the customers don't achieve zero trust because it has to be unified. It has to work together and has to present data together. But yeah, I think I think we're gonna see a decent amount of adaption over the next five years for zero trust architecture and privileged access management. And then again, I think we're gonna end up having more and more conversations about MFA and it as a solution and whether or not as we add that as a as a permanent fixture to every type of security that we do, whether or not that is a solution that there is human tolerance for and whether or not we need to To adjust that in a different way,

25:01
while I'm taking notes, I wrote down MFA fatigue. And I'm going to contact the people at the Library of Congress and see if you get a patent on that. And some apps give you a nickel every time they say it, but it fits appropriately because I never thought of that perspective. I thought the attack vector was using the public phone network. I never thought of in fact, it was just the task itself. Multifactor authentication. Well, if you enjoyed this interview, please like it and share it with friends. You've been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Josh Broadbent, regional vice president solution engineering at beyond trust.

25:38
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.