FEDERAL TECH PODCAST

002 FTP John Pelso AvePoint

SUMMARY KEYWORDS
john, microsoft, talks, cloud, systems, agencies, salesforce, collaboration, technology, organizations, built, kinds, moving, product, rube goldberg, management, ransomware, drive, prem, security

00:03
Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Our guests in the studio today is John Peluso, Chief Product Officer at a point, a point is a well known Microsoft partner. They work with many organizations in the federal government. And I had John in the studio last year, he did a great job. He's one of the top 10 reviews and I want to bring him back in the studio. So John, let's start off and tell him about a point and and some of the work you've done with the federal government, then we'll get into some of the questions.

00:29
Yeah, thanks, John. It's a it's a pleasure to be here. Thanks for having me on, had a great time last time. And so looking forward to the conversation today. For those that are unfamiliar with that point, where we're software companies, the best way to think about us, right, we build compliance management, governance solutions, in many cases, to support collaborative efforts within and across agencies, organizations, etc. The goal here is to increase their ability to collaborate with confidence. And that's a specific phrase that I use, because it implies the two things that are that are really important, collaboration, productivity, easier, faster, more effective, communication, sharing, etc, while at the same time being able to meet my critical security, compliance and regulatory responsibilities. So we work very, very closely with the public sector. It's a very big part of our business, working with agencies like Department of Energy IRS, Department of State across a lot of, you know, specific use case scenarios, coming back to this collaboration with confidence, whether that be regulatory compliance for information management records, whether that be securing the way that they collaborate across external parties and external partners, and external agencies. Right. So really exciting work. And we see that work just getting more and more interesting as the time goes here.

01:59
Last year, we did an interview in the middle COVID, and understood the whole concept of collaborate with confidence and Microsoft Teams. And that that seemed to work very well, for many big organizations. Well, here we are, we're in a different world here. Today, federal agencies have to collaborate with confidence when it comes to cyber attacks. I mean, in the last few months, we've seen drastic, and just commercial organizations ramped up and ransomware. And in federal organizations, there have been a lot of attacks in many different areas, including infrastructure tax, and some we talked about sometimes don't talk about so what does the Microsoft strategy have to do with protecting the federal government from from the new threat and new needs for collaboration with an attacking environment? Yeah,

02:41
no, great point. And I think, you know, certainly, issues like ransomware are all over the news, but I don't think it's fear mongering. Right. I think there's very some very real things going on here. Right. So 37% of global ords, saying this is not just public sector, right. This is global organizations, but 37%, saying they suffered some kind of ransomware attack in 2021. Right, this is not just the biggest, this is not just the craziest, right. This is, you know, everyday organizations, so it's out there, it's a real issue and problem. One of the things that that we've been noticing, especially as we focus help, you know, customers on this journey to the cloud, it's important to realize these ransomware type attacks seem at first to be attacks that target users infect local devices, right endpoints like their laptops, that's how data then gets encrypted, and then spreads to servers and systems. And, you know, it really becomes a quite a headache. We've worked very closely with with some federal agencies and some federal agency service providers who've been, you know, hit with these kinds of things. They're absolutely debilitating, right. So where we've been investing, there are things like tools to help you recognize early signs, early detection is critical. So early signs of ransomware. And we've done things like embed that right into the basic tool sets you used to every day. Like imagine if you're the tool you that you use to keep the plumbing flowing, right, your backup application suddenly can come and tell you Hey, John, you got some real unusual activity going on over here over time we've been tracking seems like something's going on. Oh, by the way, here's a last known good point, I think you might want to think about spinning back to those are some of the end to end scenarios that we've been trying to drive to help out with this with this particular issue.

04:38
I mentioned that I had you on the show a year ago. And we're in the middle of the pandemic and we're kind of getting away from that now. We're in a different environment where there's a war that's threatened like a cyber attacks being out there. And I think the theme in the last three years has been changed. And there's a local author in town kind of well known guy named David Linthicum, and he wrote an article for infill, he talked about mistakes people make in cloud architecture. One of the mistakes he says that many people and I assume federal ties to is that they don't architect their systems to accommodate change. And he said 20 years ago, they didn't thought of it. And but now it's almost it has to be part of any system design doesn't. Absolutely,

05:14
absolutely. There's a stat that I love because it well, I don't love it. I wish it wasn't true. But, but it's it's a great one for illustrating a point. And so the number I saw recently is much higher on the stat than previous but 92% of organizational security. Data security incidents are unintentional. So the headlines are grabbed with, you know, state actors who are, you know, infiltrating systems. And those are absolute realities. And as you say, John in our current world, but let's talk about those 92% of security incidents, which are not based on an external attack, not based on any malicious intent. That's, that is interesting to me, because it's been growing, right? The when I started quoting this stat a few years ago, it was in the high 60s, now we're up to 90%, right? 92%? What's going on here? Right? What's going on here is that more and more, we have our agencies, our users using technologies that were built from the core to be collaborative in nature, to improve the productivity and sharing and access to data. And all of those things are good and noble. But what that means is the burden is on us now to apply appropriate controls and processes. And John, where I think the the gap sometimes is an

agency will take a legacy mindset, at least initially for management and operations in terms of how they're going to secure these cloud collaboration systems. That doesn't account for all of the nuances and changes in an in a modern system. Even if you're moving, let's say from SharePoint on premises to SharePoint Online, your your management strategy has to evolve, it has to change, because the technology has changed drastically. So the theme that we're seeing now, across our government customers, is this idea of moving from digital transformation to digital realization, what does it actually mean to be in this system? Right? It's great if we can can plan for that upfront Measure twice, cut once. But just as important, how do we understand get a sense of the landscape that we have that we've been working in, because let's face it, right, we're still in that world that is never going to go back, you can't put the genie in the bottle, the move to remote work, the move to hybrid work is never going back to what it was. And even if it did, think about all the data that got created over the last two years, right, we have to have a way to rationalize get on top of that draw insights from it. And again, that's an area that we've been investing heavily in, in our in our various tools.

07:48

I'm glad use the word hybrid, because I want to go down that road a little bit, especially when it comes to Azure and Microsoft and federal partners. When I go back to David Lynch comes article about cloud and architecture. He says number this is number one rule of good card architecture is that locate processing and data storage for the same apps as close as possible. And so you can, I've been in rooms with all kinds of, you know, software developers with whiteboards, and they've just decided everything looks like Rube Goldberg kind of here and there and everything. It turns out that that may not be the most efficient way to have an old man be the safest way. And so maybe an umbrella product, like as your might provide some of that local processing? Closer, Dave's talking about

08:36

her? Yeah, no, that's absolutely true. And I think I think, you know, proximity, right is one way to think about the word close. And another way to think about it close is, am I able to associate these things with each other? And I'll give you an example. This was this was a this was an interesting one. I'm not sure if I brought this one up on our last podcast or not. But I think it's indicative of this point. Exactly. So, you know, we have various tools. One of our one of our tools is, is a data protection and resilience product for Salesforce for Microsoft, 365, etc. We got a we started engaging with a state agency out in California. And they came and said, Hey, we have this urgent need for you know, Backup for Salesforce and my, my, you know, my initial response. That's weird, right? Are you What are you selling? Right, that sales force? And they said, no, no, you don't understand. We had to build a rapid COVID tracing application. Right? Salesforce makes a great core for that because of the, you know, relationship management contact management that it's gotten. And so it was really wise. And so here we are. Now we have a situation where I'm building a mission critical application. Part of it has to do with Salesforce. Part of it has to do with some code that maybe I'm going to host in Azure. Part of it has to do with some data that I'm going to put in a database somewhere. Let's just say for the sake Have argument we put that in a in a cosmos DB in in Azure, I put that in SQL Azure. If I'm going to protect and ensure continuity of that application, John, I can't say, hey, who backs up Salesforce, you guys worry about this, who backs up Azure, you guys worry about this. Because if I ever had to put the pieces together, it's going to be impossible. So we've got to take a holistic look. And that's, you know, again, one of the things that we're looking at trying to drive out here in the thinking is, don't think about your infrastructure, especially your cloud

infrastructure in the same way you thought about, who is the team that backs up sequel, let's take a higher level approach. Let's worry about this closeness, not just proximity, again, the association between these things as we expand our application architecture. And I think that's what Microsoft

10:47

supplies and, and I've done this for many, many years, I see Microsoft, I think of, you know, strange looking guys throwing chairs and screaming. And then and then all of a sudden, in doing my research for this, I hear about a study that was released by Microsoft in February, it's called the zero trust Guidance Center. And it wasn't a bunch of guys in suits and ties pounding your chest saying, You're the greatest buy from Microsoft, are you going to fail? No, it was, it sounds like a bunch of software developers that just said, look, here's a six point process for enabling zero trust in large organization 12345. Here's what we found work kind of made mistakes in this kind of works, this doesn't work. And they provide this and you can you can type it in right now. If you're listening to this and, and it was World Series going out or something you can type in zero just guidance, you know, provide that guidance to you, no matter what, maybe your whole Salesforce shop. But that's not important in Salesforce. So Michael, it's from, from the new Microsoft perspective, is that here's the best practices for enabling zero trust, because we're all in this together, and we just have to figure it out. I'm just it's not it's not your father's Microsoft, John.

11:58

Yeah, you know, Hey, listen. On one level, when I have a candy store, right, I'm gonna go out and tell everybody how cool sweets are so so for sure. But no, no, you know, to to be serious here for a minute. You're absolutely right. And this kind of practical guidance is fantastic. I'm really, you know, excited to see Microsoft take a thought leadership role here. It's certainly you know, a topic that's on everybody's lips, Federal CIO mandates, obviously, moving from cloud first to cloud smart. Things like, you know, zero trust being kind of a barometer. How does your product support zero trust is something we get asked quite a bit. Now, when we walk in for those early stage meetings. One of the things I think is cool if you if you if you go to that guidance from Microsoft, not that we want everybody to go there right now, right? We want to stick around this podcast for the moment. But if you go out there, what you're going to see is a you know, sort of six pronged approach, as you say, and this idea of different layers, layered security approaches is not new, right? It's something we've been hearing about for a long time, what I think is cool about zero trust, and the way people are talking about it, is it does a great job of identifying what are those specific layers, and then we can dive in? So as an example, data and apps are two of these layers, right? And how am I protecting data and apps. But again, just like we don't want to think about a perimeter around our entire approach to security, we also can't think about, hey, I built a perimeter around data and a perimeter around an app. And so I I'm, you know, I'm in a good spot. Example. Can this user should this user access be able to access my Microsoft 365 tenant or not? Okay, right. That's an app level thing. But there's so many different things going on day to day within that single office 365 tenant, where AvePoint gets involved is, let me help you understand the nature risk, and other attributes of this collaboration that's happening within that tenant across multiple tenants, right, get a sense of the inventory of that collaboration. And we also are going to highlight out to you areas of higher or lower risk and exposure, because it's not just access to the app. That's important. It's not just protection of the data in general. Right? We've got to think of these things. Back to your point, John, if I get a little metaphor a minute, right? I should be treating a team that team's data, the applications associated with that team and everything that team touches. I

should be treating that like a business application. Right? So I've got to protect that business application. I got to classify that busy business application I get to be able to understand its compliance over time.

14:55

I look at Washington DC I spent our time in LA and began to business out there in Washington DC, of course, big government business and big headline news here, March of 2022, is a lot of budgets have been approved here. And it looks like CES is going to have a lot of money coming in $1.5 trillion in this sub budget coming in. And and, and what they're going to require out of agencies is to, to operate critical infrastructure. And they'll have to notify Sissa of a breach within 72 hours. Yeah, yeah. Now, if if you get together with a bunch of software architects and get that whiteboard that, you know, 30 feet long and have this and the Rube Goldberg here, and then everything. I don't know, if 72 hours you can understand where stuff is. And so there has to be a more systematic approach, if you're going to ally with some of these requirements. Just I love Rube Goldberg. I love arguing with software developers about hot sauce, it's great. But I got 72 hours, I don't have two weeks or two months, do I?

15:53

Absolutely. And again, this is one of those you mentioned change right? Earlier and and being able to sort of take a look at am I thinking about how the cloud by definition is different than what I did on prem? One of the things and AvePoint, you know, one of the businesses that we're in, right, as is consolidation, migration of content. So we're regularly faced with the fact that look, this isn't your architecture, right? When you're our chief, information security and risk officer. She's got great, great little anecdotes. And one of the things she says Remember, the cloud is just someone else's computer, right? And they get to say how many actions I can perform every second. So when time when we're against the clock down in a response and Incident Reporting type of timeframe. I can't start my strategy then. Right? I've got to have my strategy in place that's accounting for the fact that, hey, listen, crawling through all these systems and all of the areas within these systems, that's going to take weeks, I don't have weeks. Right. So again, this is an area that we've looked at in terms of how we know what if I had to in a moment, this is a good challenge. If I asked you that on my desk by tomorrow at 6pm, could you show me everything that John has access to has access to across all of your office 365 tenant? Could you produce that? The answer, in most cases is no. Right? Because you have to be proactively maintaining that information to be able to produce a report like that. And that's another area we've been investing is that kind of thing of like being able to have at the ready information. The cool thing about it about that is if I'm gathering that information, I'm not waiting for someone to go get it, I can use that to also produce some insights and guide you to things that maybe you didn't even know about. And now we're getting into the idea of proactive management, as opposed to reactive management. And that's really where we, we want to aim.

17:59

So John, I want to ask about blind spots and multi cloud environments and how to avoid those. But first, one of the best ways to keep up with the fast changing world of technology is through attending webinars, you learn at your schedule, and you get continuing education credits. I think the best webinars are from Fed insider.com. Just last week, we had Paul Cunningham from the VA talking about zero trust. And so I liked hearing what he's have to say. And and I want to hear what you have to say, John, too. When it comes to systems architecture

and design. It seems like the know talks about some hybrid environments can have blind spots, and multi cloud environments are going to be well, I didn't think that unintended consequences, you know, I didn't know that was gonna happen. And I think this is if the government is getting serious about reporting on breaches, then people got to get serious about their enterprise architecture and their blind spots, because you you don't know where they're at

18:56

or do you? Absolutely. Absolutely. And, and this is where, you know, there's, it's a challenge, right. And on some level, your cloud infrastructure might actually be easier to monitor. Just because it is always accessed outside the perimeter. Many systems are built with a, you know, rich API surface the ability for products obviously, point builds products, other companies build products. So the cloud just by nature of its exposure is sometimes sometimes anecdotally easier to report on. Where I see some challenges in the flux right in the flux where we're in right now and and it's it's not specifically related to security. This one will be related to information compliance, right and governance but we're working with a with a very, very large agency right now. Who is very conscientious about their enterprise records management programs, right in their in the past process of moving very large environment from on premises to the cloud. And they're having these considerations right now. Am I going to be hybrid? Yes, of course, I'm going to be hybrid for how long I have applications that are running on prem. I've got collaboration that's running on prem, I have an operational model about how I'm going to move that stuff. But there has to be a tight coordination between the operational thinking of how can I get this stuff from where it is to the cloud as quickly as possible. So I can realize a return on my investment, reduce my storage burden, my infrastructure burden? What happens to the protection of that data in transit along the way? Do I maintain the systems I had? Do? How do I extend protection from the systems I had to the systems that are going online? And you know, many vendors, ourselves included, have hybrid capabilities that are built into our on premises products that help you extend their capability to the cloud. But I think something that should be asked every step of the way is is that the right approach for me, right is that the right approach, or is a cloud native system that is tuned and built to be able to monitor and react to these cloud systems a way to go and truly live in a hybrid world for a while where I'm managing on prem with my on prem assets, but I'm going out and securing net new approaches, systems products, for my cloud systems, then, of course, you've got to tie them together.

21:30

I teach at Georgetown, and two weeks ago, I entered the classroom face to face and I'm all about communities and discussion and going learning more and more. When I went to your Twitter feed your company Twitter feed, I found out there's something called Microsoft 365 community talks. And so listeners can just taken advantage of the free learning here. So this is seems like a nice little community. I like this exchange of ideas. So tell us about this 365 community talks.

21:56

Yeah. And you know, you, you talk about Microsoft, and their their guidance around zero trust. Look, the way here's how we look at this, right, we look at this many folks who are on this journey, this modernization journey, which is where we started, of course, in the last couple of years, that took a pretty hard right turn to a modern collaboration journey with a lot of these instant hybrid work challenges, right? We here's how we look at it, shall

we go through this, you know, 50 times a month, with different customers, right? I can tell you, I myself have gone through hundreds of conversations with customers who were moving from, you know, where they were to where they're going. The benefit of that is that we get a lot of exposure to different great ideas, thinking what works, what doesn't work. And we're very sensitive to the fact that a lot of the people that we're working with will go through it maybe once or twice in their lifetime. So the whole idea behind these community talks is how do we share that knowledge? Right? Goodwill begets goodwill, right? So as you say, this is not, this is not a set of talks that are just for AvePoint customers, we're happy to spread these thoughts and best practices, because we feel, honestly, that we incorporate some of these best practices into the way that we approach our product set. But by no means are these you know, AvePoint sessions. So you see things like how do I look at Citizen development in in things like power automate? How can I leverage that in a safe way? Looking at changing workspace at workplace patterns? Right, what are we seeing out there? How can we, you know, collaborate and peck, you know, these things are are collaborative as well, because the conversation needs to happen, the more conversation, the better. Because look, this is new to all of us. Right? We may be a little bit further ahead, because we've talked to, you know, so many customers about it, but we're going to solve these problems together.

24:06
Kind of a tougher question for you here. In my world, the OM B's kind of a popular topic, and they come up with a deadline at 2024. For a lot of zero trust initiatives here. They have 19 different requirements. I think that's too aggressive 2024 I think that's reasonable.

24:29
Okay, so here's what we'll say about mandates and timelines. Right.

24:33
I know you're gonna have opinion on this 1/3 Laughing

24:38
things generally don't happen without them. That's the first thing right. And and understandably so again, this is not this is not a Manyana attitude. This is there our priorities there are everyday priorities and in some ways, you know, the past two years have only added to and complicated those priorities. However, it's critical that there's a North Star, right, it's critical that there's a North Star to work towards. If we go back and we look at some of the the timing and mandates that narrow put in place, back for 2019, evolving now to 20, you know, 21 and 2022. We saw real and true action that was taken based on not only the guidance and the importance of it, but also the timelines. So again, everything will always be a combination of priority and budget and things like this, some agencies will be able to move faster than others, depending upon things like how much sponsorship there is within the organization. I think the heat that zero trust has the criticality there, you know, probably not fair to say, but you know, security, cybersecurity gets a heck of a lot more airtime than Information Management and records. Let's be honest, right. So I saw a good traction with the narrow mandates. I only expect the same here with some of these OMB mandates.

26:06

I talked about David Linthicum earlier on, he has some profound things to say. And, and because let's face it, John, you have pre lot of environments, commercial environments, and federal environments and seen their ability, got the T shirts in all kinds of different things and a lot different organizations. And so as Dave, and here's the observation that he makes, and I'll see if you agree or disagree with him, he says that failed cloud projects rarely trace back to technology issues. So we got these pesky humans here. Hi. I mean, I mean, you know, you and I are human, and we got all kinds of flaws. And we click on bad links, and we do wrong things. And what's your 92% of thing? unintentional consequences. I left the back door open. I'm no,

26:52

I not only do I agree with David there, I think even where it does map back to a technology problem, it's probably because somebody made a dumb decision about how to use the technology, right, like, so. So no, I totally agree with that. And I think that, you know, I always my, my, my shoulders always perk up a little bit when someone says, we have a product, we're covered. I don't know, write a product. You know, products are like tools, right? They do what you tell them to do smarter products, maybe even suggest to you how you should use them. But this needs to be a conversation, what we find is, and it's okay, right, it is okay. And it's something that you should expect. If you've had one or two discussions, and you feel like you've got your strategy mapped out, that's an almost certain clue that you're missing stuff. Right? These are conversations that need to evolve. They're very nuanced. We had, you know, I can I can recall conversations with a large agency, again, another one that we're pursuing some information management solutions for. I can, you know, I remember sitting in office saying, Oh, we're covered, you know, I think there's a there's an out of box solution for that we're going to be covered, right? And don't you know, what, a year later, the conversation is deepened, it's more nuanced. And now all of a sudden, it's like, okay, for it to really have a comprehensive strategy, there are things I'm going to have to think about that I didn't think about initially, it's okay. Right, that is the world that we're living in. So proactive, active engagement, these community talks, go seek out those Georgetown Technical meetings, right? Because the more you can educate on this stuff, the better it's going to be. But you'll never be able to educate fully one of the things that we see, and I see this across both commercial and public sector, build that digital workplace engineering muscle within New York. It's not a single muscle, it's not a single team. Right. In fact, having differing opinions, differing priorities in there, folks that are focused on operations, folks that are focused on engineering folks that are focused on productivity, bring the compliance folks to the team, right? All of these are really important perspectives, if we're going to be able to solve this.

29:08

I keep thinking of Microsoft platform and, and, and how a lot of human weaknesses can be prevented. And a lot of they'll prevent you from making these basic, you know, rarely trace back to technology issues, I think about my driveway. So I've got a 2005 s 2000 manual transmission sports car in my driveway. I can drive down that street a million times. No store is still gonna be unlocked. It's everything manuals, everything's manual. Now I have a Honda Pilot, newish one in the garage, I drive two feet down the road ever all the locks lock up. And so it it prevents me from being human doesn't have a whole lot safer in that big old pilot. I know that too. It's not as fun and maybe it's nice to design something that's a male transmission sporty and take the turns fast. But, you know, when my wife gets that I'm very calm. Through driving through the drive because I know it's going to be blocked. And so I think there's a lot of platforms that can can look at unexpected situations and

human weaknesses and unintended consequences like that 92% keeps coming back to me. And so maybe there's ways to automate things to prevent people from dragging you out of your cars, cars.

30:22

Oh, man, I love that. I love that story. So let me tag on to it here. Right. Think about what was the precursor to that? You know, the the way the the doors lock in the Honda Pilot? They're the child locks, right? Yeah. And we've all been in that situations, usually embarrassing, usually or out with coworkers, right? Who's going to drive to the dinner, and I'm sitting in the back. And you know, they moved the child seat into the, into the bag into the trunk. So I could sit there very nice. And then we get to the restaurant. And here's John trying to open his door. And of course, he can't write because the child lock is on and he can't unlock the door. And that's the old world of control, right? The old world of control as I put it in place, it's there all the time. What does it keep me from doing keeps me from being able to do what I need to do, John, I can't get out of the car. We have a new way of looking at automated controls, right? Those automated controls need to be risk based. There's no risk to me, John, when the car's not moving, but there is when it's moving. And so those locks on that Honda Pilot, how do we make those kinds of things available in our everyday patterns of collaboration, the way we talked about it, and my I'm directly involved with our the team that builds our governance solutions, and they're probably sick of me talking about the bowling alley analogy, I say it all the time. It's the guy is, we need bumpers, right? We need bumpers that I can put up when I need to, but then come down when they're not needed. Because I want people to play the game. I just don't want them to hurt themselves.

31:53

And you know, a year ago, I bought this on the pilot. And when I went to the dealership, I didn't have my little checklist and say, Okay, now the doors gonna lock at five miles an hour? And no, no, it's not. I looked at something completely different. I compared it with the Highlander. And I was worrying about that. I didn't even think of that. But now whenever my wife dies, that's what I think about is a dog going to be locked when she drives down the street. So I think a lot of people can can you're in a competitive environment, and you're comparing product A and product B and platform and Platform B and and sometimes you're Hocus Pocus, who's got the focus, you're not focused, and that magician saying Hey, where's the pee? Hey, look at that the cards over behind your ear. And I think that's why sometimes a proven platform can do the stuff that's not on your checklist. Yeah,

32:41

and you know what, there's, let's be honest, as I'm a technologist, I work for a technology company, I will tell you technology has its limits, right? We've, most folks have a long way to go before they get to those limits. But there are limits. And so you're absolutely right. The technologies should suggest itself, right? We should suggest, Hey, John, there might be a problem over here. I know, John, that you don't understand the highly complex nature of how someone gets access to a document, right? I wish it wasn't so complex. But guess what it is? I'm going to suggest to you something though, because I think you have responsibility for a document that is, seems to be sensitive and seems to be pretty broadly exposed. And so let me give you an easy way to review that right? Boom, the lock goes up at five miles an hour. Here's where I think sometimes organizations over estimate the capability of technology. I have been hearing for probably three or four years. Oh, I have a technology that can tell me exactly what's happening in every document across my entire

enterprise. And that's my strategy. Guess what? That's not a strategy. There's no silver bullet that's going to be able to do that. Right. technology gets better the technology helps suggest, but there we're not off the hook. Right? Tesla Autopilot doesn't exist for collaboration, security today. Assisted driving, that's the way we should be thinking about it.

34:08
Well, unfortunately, we're running out of time here. I think the takeaway from this interview is Av e, poi and t.com. And look at this Microsoft 365 community talks. Because I think it's a it's a wide range I found on twitter, all kinds of topics that come up how to use this, what about Kubernetes? What about that, and and you may have three topics have nothing to do with you. And then that's exact topics that you want to know more and you do a deeper dive into that so I think that's really good to take away from this one. Well, good.
You have been listening to the federal tech podcast with John Gilroy. Blank thank my guest John Peluso Chief Product Officer at avepoint.

34:46
Thanks, John. It's always a pleasure.

34:49