FEDERAL TECH PODCAST

More Devices than People: Managing the Madness

SUMMARY KEYWORDS
trust, device, people, bill, endpoint, part, attacks, federal government, endpoint management, john, ransomware attack, ransomware, avanti, vulnerabilities, automation, organization, technology, risk, manage, micro segmentation

Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Today, we're going to talk about everything everywhere. We're gonna talk about remote communications. We're gonna talk about working remotely and accessing the Pentagon and security and endpoints. And I thought we'd bring in Bill Herod, he's the CTO public sector vivante. Now if you look this guy up on LinkedIn, you better bring a notebook because I think he's been everywhere and done everything. He's kind like the Forrest Gump of technology. So really a strong background. And I thought if there's someone could address issues involving endpoint security of all people, it's got to be bill I mean, I'm just gonna give you a hint of his background, but he's done a whole lot of things that it would it would take his advice. You know, it's like the running of Ben Franklin, you might hear about, you know, running a business or being creative. That's the guy listen to, but Bill is probably the one you want to listen to when it comes to endpoint security. So Bill, how are you?

05:16
I'm great, John, thanks for having me on.

05:19
Well, there's your moniker, the Ben Franklin endpoint security. Well, maybe you started to give the audience the hint of what you've done, and how you want to move on to I know you have a strong background with the FBI and many large organizations, you present to high level people at the Pentagon. Just give me maybe a nutshell of your background. Sure. Thanks,

05:39
John. So I've been advising on cybersecurity best practices and designing and delivering security solutions to government agencies and fortune 500 companies for close to 25 years. And as you said, I began my career in federal law enforcement.

05:57
I have a daughter who finished a master's degree in finance, and she's looking for a job. And she has to be able to work remote. That's one of the conditions. She says I'm not going to take it I say work remote. And I would take any job I could get and different standard now with the millennial generation. And so the focus

today is working everywhere, and having access, especially for the federal government. And so when it comes to federal government, accessing documents, and accessing it is one nice thing to say to set up a VPN and call in. But I think if we learned anything at COVID, is that it's, it's, it's a circuitous route to have endpoint security, isn't it?

06:36

Well, it really is John. And you know, one of the things that we have seen is that ivanti has a a tagline, a moniker, that is that we help secure and manage the everywhere workplace. You know, in in COVID, we really did see that almost overnight, in February and March of 2020, federal agencies and commercial organizations went almost 100%, remote telework. And what we have found since then, is even though many agencies and corporations are bringing people back into the office, that many people either don't want to be in the office at all, or they want to have the flexibility of being able to work remotely. You know, John, the federal government has suffered a significant loss of personnel a loss of a lot of institutional knowledge, and a loss of a lot of people who have retired out of the top levels. And they're not refilling that nearly as quickly. Avanti did a digital user experience study where they conducted a survey of 10,000 users, including IT decision makers worldwide. And now did the decision out of the digital experience study. One of the things that was interesting was that 34% of the respondents said they've considered quitting their job, in part due to the applications and the technology that's available to them. And 64% said, they claim that the way they interact with technology directly impacts from around the people that are coming to work now for the federal government really have grown up as as what we refer to as digital natives, but they are so used to a an inherent and an easy to use interface. That without that, and the sorts of tools that they rely on the mobile phone, or the laptop or the iPad, that that they really feel like it's it's a burden, not to have those kinds of tools and capabilities. And that's going to be a big piece of what the federal government needs to do, to be able to attempt to attract and retain talent.

09:05

You know, Bill, you manage people I've met as people, and difficult times and all kinds of challenges here. And I think today's managers have to make an environment where they can retain talent and be as flexible as possible. And when he talked about this, people think about quitting. I just think of you know, today I heard about this Gartner study. That's called the 2320 2123 study. And it talks about emerging technologies. He said, Well, there's, you know, proliferation of endpoint devices, there's ransomware. There's all kinds of threats. And we have this whole line list of threats that are out there. But But what they're saying is that the talent shortage is the biggest barrier. And so if I'm managing a group of people, and I want to retain Bill Herod, I'm gonna get to know Bill say what's important for you, Bill, and how can I help you do your job better and, and this is going to be a key aspect of it, but in the federal government, you have to comply with me Any more regulations than in a typical other, I think with a bank has probably as many regulations. And so I think just from from a technology management perspective, Bill, it's important to let people have that flexible just to keep the talent that you do have.

10:13

Well, that's right. And in, in some recent discussions that I've had with some of our federal clients, they've said that the Reliance particularly on mobile devices, has increased even more now that people are beginning to go back to work and beginning to do face to face meetings and conferences again. So things like checking their

email, responding to a service ticket request, any of the things that being able to check on a report, all of that is now going over a mobile device. And and we have to be able to, to make sure that that mobile device is, is being used by the person that we think it's being used by that they're on a protected network, whether it be a per app VPN, or or a VPN back into the enterprise. And that there's not malware on that device. And that the device is in compliance with with whatever the policy and regulatory requirements are. So all of those are things that that are part of the Unified endpoint management. And previously, it's what we call Mobile Device Management, which is really where Mobile Iron excelled where Gartner has recognized us among the leaders. And Mobile Iron is one of the pieces that Avanti brought together. So Avanti started out as a as a service desk company, with LANDesk and heat many years ago. And then in in 2020. They brought together Mobile Iron as as a mobile device management and security piece. They brought in Pulse Secure for VPN, and network access control. And then they also brought in a company called Share well, which is another service desk solution. And most recently, they brought in a company called Risk cents for being able to do vulnerability priority, and really help with risk based prioritization for vulnerability management. So not only knowing what the devices are, but knowing what's being exploited in the wild. So what vulnerabilities are, are being weaponized or being attacked. And then how do we prioritize that? That sort of a requirement to get those patched in and remediated and it really fits with the DHS directive, what was called shields up, but it's really around making sure that that things are patched in a timely manner. DHS is mandate is is somewhat aggressive, maybe in the timelines that they give, but certainly being able to patch legacy pieces and, and vulnerabilities that are out there. That's one of the things that ransomware has taken great advantage of, is attacking things that we've known to be vulnerability for a long time. And they're exploiting that now.

13:31

I'm going to talk about ransomware in a few minutes. But first, I want to talk about Ed Sullivan. Okay. So as somebody said, on the show, you remember, there was one guy who was a plate guy, he had these six and hazy bounced plates, and have one value run over here and get that one about to fall on. Yeah, I don't know if the young people can Google out on YouTube or finding some but but the plate. And so that's what the federal government's doing, you know, if I come up to you and say built zero trust next week, or you're fired, and everyone's in the same building, and everyone's on a desktop computer, a build job, not all that hard. I mean, he probably knows which desktops are in the building. And so that's what happens if I come to you, okay, Bill, it zero trust, we not only have the desktops in the building, we have desktops outside the building and these floating devices, we don't know where they're at, we don't pry a pretty good idea who they are. And so in order to implement zero trust, you have to have identity management, right? You have to know who it is, and who do you trust. And so all of a sudden, this comes, this gets me instead of changing the oil in your garage, you're changing the oil as you're driving to Ohio. And so, I mean, the mobility factor makes zero trust, so much harder to deploy, doesn't it?

14:43

It absolutely does. And part of Avantis mission is to be a global technology leader, enabling organizations to thrive in the zero trust workplace. And part of that is, as you said, is knowing who is involved right who is on the network. And part of it is knowing what's on the network, what's happening on the network? And how do we protect the data and applications that agencies rely on. In many ways, it goes back to the to the CDM. model from from years ago, with zero trust really is looking at how do we eliminate inherited trust for a long time, we

had a concept of once you're on the network, then you're trusted. And I often use an analogy, right? If you go into the Smithsonian, There are guards at the front desk and, and there are guards around generally. But, but they're not guards in every room. But if you go to something like the Museum of Modern Art in New York, there is a guard maybe between each room and in each sets of room. They're looking at both sets of rooms. And in any male behavior, any misbehavior, you're escorted out. And that's really kind of what zero trust is. Zero trust removes the assumption of inherited trust for people for devices, for applications and for sub networks, and really focuses on securing and continuously enforcing risk based access controls and authorization decisions.

16:28

Yeah, I remember years ago, when I was studying from my tests, risk based access control the code our back and our back this and, and it was known. I mean, this isn't breaking news. You know, there's three outs and in any in baseball, oh, breaking news. Phil, did you know that? No, I mean, this has been known for a while, it's kind of I think it's been sitting the back. And we've never had to take that off the shelf and deploy it. But now it's coming back with a vengeance, especially because of these new attacks, like ransomware attacks. And doing the research for this interview. I didn't even know this. But apparently, your company Avanti has a ransomware index, where they, they said, Hey, this is a big deal, we'd have to study ransomware and find if it's going up or down, and maybe we can provide information to people that will know how they're getting attacked. And according to slice lettuce index, there's been a rise in vulnerabilities every year with ransomware. And so it's just it's, it seems to be a threat. That's everywhere, doesn't it?

17:25

It absolutely is. And the the ransomware index is really part of the the ability for risk to be assessed across an organization. So how do we evaluate the likelihood of a ransomware attack really comes down to looking at those devices, what the vulnerabilities are, and then looking at what is being attacked, what ransomware attacks are there in, in the wild, and what other attacks and one of the things that we've seen is that particularly in in the recent past, there are there are sort of the big four. So nation state attacks have have escalated, particularly since the beginning of Russia's invasion into Ukraine. So Russia and North Korea are two and then China and Iran are two more that are really using known vulnerabilities to attack organizations. And a lot of the way they're doing that is through through an initial ransomware attack, either through through phishing, through email, or through through websites, and getting people to click on links. But then part of that is that once an a device and endpoint is infected, that they're actually using remote code, they're using shell scripts and and command lines to to do the attack and move laterally within an organization. And the shell scripts and the command lines make it harder to detect and remediate those attacks. So part of what we want to do and when loop this back into the zero trust, is we want to make that those those controls as as granular as possible, it's what I call minimizing the blast radius. So we want to create the micro segmentation and software defined perimeter to contain whatever risks we cannot prevent to as granular a trust zone as we possibly can. And then focus on those those risk based controls at that level, and prevent that lateral movement within the organization.

20:00

And the numbers are just amazing. If you do the study I, I went to Google this morning and typed in how many people in the world 7.7 billion. And then I put together how many endpoints are there 12 billion now. So there's

more endpoints to worry about in the world than humans. And it's going up every year. And so, because a federal agency may get up on January 1 2022, and have a pretty good, you know, pretty good approach to managing endpoint access and mobile devices, three or four months later, the volume has gone up where your solution then may not be appropriate, it may have eclipsed the capability of the system that was three months ago was perfect. So this moving target gets so difficult, and that's why have to incorporate endpoint. And it's got to be wasted cheese, maybe machine intelligence or machine learning or artificial intelligence, to handle that stress to catch pieces. And

20:55
so that's absolutely right. And a lot of times when I'm doing a speaking engagement all ask people, you know, to raise their hands if they have, you know, have one device with them, or two devices or three devices. And having spent a fair amount of time in federal government, I used to carry two devices. One was a federal phone, and one was my personal phone. So there's two, and then you've got an iPad and a laptop, and suddenly, there are four endpoint devices for an individual and and so how do we control the risk from that, and part of it is that we don't have enough staff and personnel to be able to manage all of this. And so we have to look to, as you said, some some artificial intelligence, some machine learning, and it really is about how do we provide the automation, what Avanti calls hyper automation, to be able to provide for, for self service, for self securing and for self healing. And that's part of what we do with the Avanti neurons cloud solutions, to be able to, to detect a problem, initiate a service ticket, in some cases, be able to, to remediate the problem, whether it be apply a patch, or or sandbox off a device, close to the ticket, log the ticket, and then and then provide the the after action. And we can automate all of that. So that it can be done in a fraction of the time that it would take if we had to wait for a personnel to detect it and, and begin the process. And it allows us to be able to make much better use of technology, and maintain our staff to do things that the technology can't do. Either things that are emerging trends or risks, or things where the artificial intelligence hasn't yet learned the pattern.

23:09
I'm not a big reader of science fiction. I'm a nonfiction guy,

23:14
happen on a plane gonna read a couple of books.

23:17
But there's a phrase that comes up I think in in fiction, as well as science fiction, as well as the federal government. And the phrase is non person entities. And so if you design a system for everyone's got a smartphone, and there's an engine, I mean, there are entities and systems now that are non personal entities that are automatically given permission and have to be identified, this rises level of complexity that really gets it's really going to be difficult, doesn't it?

23:47

Well, it's interesting, John. So prior to joining avanti, I was with Mobile Iron as as public sector CTO, but before that I was with Deloitte as part of the cyber risk practice. And one of the things that I was doing is I managed a team at the IRS looking at identity and how we deal with identity, particularly for for citizen focused or citizen facing identities. And a lot of what we worked on was not only person identities, but as you say, this non person entity, the NP II, and how does it have an identity? And it's not again, it's not really news. It's not new servers and devices for a long time have had some sort of an identity attached to him, whether it was a MAC address or an IP address. The IP address now changes all the time. But what we want to do is we want to know what that device is. What's on that device, what applications are running part of the executor have order 14 Oh 28 was to focus on things like software supply chain, and solar winds and log for J pointed out why that was really important. So we have to know what's on that device, what's running on that device, what's supposed to be running on that device. And then we have to make sure that that device is authorized, just like a request that comes from a person that if a web service call, or a transaction originates from that NP e, that non person entity, that that device is identified, and has the authorization to make that call, and being able to control that does allow us to help us maintain that control that blast radius. And with the world of IoT, those non person entities are escalating in numbers dramatically.

26:00

We talked about automation earlier and the ivanti platform when I think of automation, this little fictional non personality pops up. The other thing that pops up in my mind is I'm a human being. And I can have conflicting responsibilities around the house or on my office, when I write, and I can kind of resolve them. But there must be systems that have conflicting standards or conflicting priorities when it comes to zero trust automation. And I don't know how that gets resolved, there's got to be where here's a set of rules. This is X, Y, and Z. And then you have to comply with these other set of rules that says X, Y, and Z, X, Y and BD. And there's got to be some kind of a concern there. So is that the magic sauce that ivanti brings, it makes it all hears the word orchestrated.

26:50

So it's absolutely part of what we do. So for a long time, we've talked about service orchestration, automation and and response, what they call soar. But what we're really looking at now is in addition to that is what we're going to call war. And it's the vulnerability orchestration, automation and response or remediation. And that's part of that is being able to, to detect when somebody is operating outside of what we would normally consider to be normal behavior. So part of it is behavioral biometrics. Part of it is that artificial learning and machine intelligence to say, Wait, this is outside of a pattern that's normal. And part of it is simply logic, right? If Bill logs in from DC, at at 10 o'clock on a Tuesday morning, he can't also then log on from Taiwan or North Korea at 1015 there becomes a time continuum problem. So all of those things make up this, this orchestration automation and response controls. And part of that is is what Avanti brings as part of not only neurons, but overall the solutions to be able to, to discover, manage, secure and service, IT assets across the enterprise.

28:31

But Bill, unfortunately, here we're running out of time, I'd like to thank you on behalf the audience for giving me a better definition of this whole idea of endpoint management. What it means this confusing world of zero trust architecture, and exploding number of devices are out there.

28:45
You are listening to my pleasure.

28:48
You're listening to the federal tech podcast. My name is John Gilroy, like thank our guests, Bill Herod, the CTO public sector and Avante.

28:56
Thank you, John.

29:00