Ep. 118 An Update on Zero Trust for the Federal Government

00:03
This is John Gilroy here today, a progress report on zero trust for the federal government hit the music Manny. Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator in the virtual studio today we have Jonathan troll, Chief Information Security Officer at a company called Wallace qu, a Lys. Jonathan, you're like the report card for the federal government today. So we're gonna ask you to give you a perspective on kind of progress is made with the challenges they have and, and what kind of timelines they have. And, and all kinds of topics here include zero trust and compliance and, and Internet of Things, all kinds of things. So Jonathan, maybe you can give our audience a 32nd overview of your company, and then we'll dive in.

00:49
Yeah, sounds great. Yeah, so Qualis is a cloud based security and compliance platform, we've been around for over 20 years now. So actually, our claim to fame is we were really the first cloud born. security vulnerability management, continuous monitoring solution on the market. So our company works with all of the Fortune 50 large financial institutions, federal agencies, and government agencies across the world, delivering a platform that helps them measure, communicate and de risk their environments.

01:30
Well heard is late December, early January. And I think everyone looks at what happened last year, what's gonna go on next year, whether it's in your house, we have all kinds of house projects for next year, we're looking at maybe some travel next year. And I'm sure the federal government is looking back on some of the projects, they've started as well, a little bit bigger projects in my house projects here. And so if you look at next year, 2024, it looks like the zero trust is going to come. I think it's in September, is that when the compliance can start for that?

02:00
Yeah, that's right. Yeah, September timeframe, really, when the, the deadline is to get the initial implementations, you know, get the architecture signed off and have that working, you know, at a certain maturity level for federal agencies.

02:17
My wife is a principal in high school. So I know all about report cards. We talk about valuations all the time. And so from your perspective, I mean, you have a strong background in this. So So where are the opportunities for improvements? I guess, 135 agencies, 135 different situation reports, what, where can you see some of the opportunities that are for some of these agencies? We're talking about?

02:36

Yeah, I think, you know, definitely, you know, it goes back to the basics, right. And, and probably the largest area for improvement that I see in working with, especially the larger federal agencies, is continuous asset visibility. Right. And without that, you know, it's very hard to have a complete zero trust architecture implementation, you know, you really don't know where your assets are, they're their value to the business. And, of course, the challenges have gotten even more difficult, you know, now you have cloud assets, you know, assets in your own data center. You know, you've got IoT devices and other smart devices. So it's no easy task. But but, you know, honestly, I think you got to start there, right? You have to start with just consistent real time, visibility of all of your digital assets to really do zero trust, right.

03:28
And it's just we can sit and have a chat about, just look at your digital assets. But what about Slack discussions? What about maybe code that is, is in a system you don't even know? And what about people doing shadow IT? And what about people doing, you know, all kinds of shadow activities? I mean, it sounds like you and I in a room and whiteboard, we can, okay. observability will not have this, this in and of itself can present all kinds of problems, you know, in the federal government. I'm not going to name names, but it's obvious. Sometimes compliance maybe ties people's hands they go, No, I'm just gonna use a Jonathan troll software. And no one needs to know anything about this happens in the commercial world happens in the government, doesn't it? Oh,

04:09
yeah, absolutely. I mean, you're, I think shadow, it continues to be one of the hardest things for security teams, right, one of the biggest risk items. And when you think about doing comprehensive inventory, and, you know, I think what we can say is failed is like their traditional, like, you know, it view, right, like, you know, you have your ServiceNow implementation, or you have, you know, whatever software where you're, you know, inventorying you have an asset tag and, you know, it's too slow, right, you know, you know, that is, you know, too prone to human error.

Again, you have a lot of other shadow IT that's probably on your network that you need ways to discover, right? That that's unknown to it. So it's not going to be in any, you know, asset inventory that they're tracking manually, you know, so you have to be pretty creative, right about how you're going out and finding these assets and whether they're Yeah, I think we categorize them in two ways. It's either manage, you know about it, you know, and it was deployed and it has the software on it, and then it's unmanaged. And this listen, you know, for some, the, the percentage of managed versus unmanaged could be really high, right, you could have a whole lot of unmanaged assets running on your network. And I think the idea is over time, right, you bring those under control, but But you're absolutely right. Like, I mean, you're gonna discover, you know, personal devices, you know, people's personal digital watches, software that was bought without, you know, the right procurement vehicles. And, and, and again, it doesn't matter, right, like, I mean, to the security team, you know, it's handling federal data. It's a problem, right, it's something you have to manage the risk around. So you're absolutely right, like there is a lot of unmanaged, you know, devices and assets that are out there handling federal data right now. Jonathan,

05:54

I went to your company website this morning, que ualys.com. And I read a couple of blogs, and, and the words that popped up into whoever wrote this. Pretty brilliant, I think you could have managed and unmanaged, we know that we could have undiscovered and then well, what about poorly managed? Well, there? Is that system manage? Oh, yeah. John Gilroy did it? Well, let's take another look at that. So so just because it's identify as a managed system? Well, guess what it may not, you know, may not be well managed, or maybe infrequently managed?

06:24
Yeah, no, that's exactly right. You know, so once you once you have the visibility of your assets, it's then about bringing down the risk of those assets. And again, the way that we think about risk and hopefully others do is, you know, it's about the configuration of that asset. It's about whether it's currently infected or not, in fact, it was some type of malware or, you know, there's some type of advanced persistent threat actor on that, on that assets. Does it meet compliance requirements, you know, whether it's DISA sticks, or some prefer net security benchmarks, you know, it should be properly configured to reduce the risk of some type of exploitation? So that's absolutely you know, the way we think about it, that's your next step, right? Is what what how well, is that device manage? How well is it configured? how resilient is it to cyber attacks, that is absolutely the next step that you have to focus on.

07:20
I've been doing this a while. And I tend to make black and white decisions and put this in a box and that in a box. And, and we all man, were either not working, we put all five computers and room with network cards, and we learned how to use routers and all that kind of traditional stuff. Now things are changing. You know, when I interview people from Akamai, like Patrick Sullivan, he says, We know, John, really, the network is the API. I mean, that's really what's going on here today. And you can talk about your MAC addresses and everything else. But it's dynamic and changing and fluid. And it's just, it's so we have considered a lot about API's. That's part of the network, too, don't you? Oh,

07:54
yeah, absolutely. And I mean, I mean, thus, you know, the emphasis on zero trust, right, that the federal agencies have put in place, right, because if you think about zero trust, you know, the idea used to be in the day, I will listen, if it's on my protected network, then I can trust it, you know, trust it fully, you know, it has access to everything, do whatever it wants. And, I mean, listen, there are a lot of flaws with that approach. I mean, maybe it worked 20 years ago, but you know, nowadays, I mean, I'm working out, I'm in a hotel room, and then you know, I'm going to be in a corporate office, and then I'm going to be on a plane overseas and losing my assets going all over the world, right, you know, and again, the idea that it's just connected to a network, and now it's trust, it really doesn't make any sense any longer, just with mobility of, you know, our employees COVID Definitely accelerated this right and work from home, and how do we get work done? You know, and where are these assets now? And so, you know, the whole idea about zero trust is, is, you know, really kind of breaking down that paradigm of, you know, your network is your only security layer, right? And now it's pivoting, or listen, it's not about the network, and that's one component, but now it's about your identity, like, Who is this person on this device? And can we trust that person and the health of that asset? And and and then again, network is

just one component, right? It's one data point that should feed into these these authentication decisions that are being made, you know, all the time, right? And milliseconds.

09:24
Well, if you do research on Jonathan's company, what you can usually go to Google and type in QALY, S and come up with some Gartner reports, and they've got you classified as working with vulnerability assessments. So that's a pretty good, I think you're known for that for 20 years, possibly. So the question to ask is, what, at what point did what do you draw the line of vulnerability assessment? I mean, I'm talking about you know, a software bill of materials and and what happens with code that is written and ostensibly approved, then it's injected into a system so so what happens with something that's third party Jen? Writing code. You know, if you look at the numbers, something like 80 90% of systems generally today have third party apps in there written by who knows who. And so, here it is Wednesday morning at 9am. Hey, we're good. And all of a sudden, John Gilroy, download something, and hey, we're bad. So it's like this, the dynamic nature of this and the code that's entering can present problems that are hard to detect. Yeah,

10:25
no, absolutely. And honestly, I think, although vulnerability management and detection has been around for a long time, you know, I think we really want to change the way people think about it and approach it. And and listen, we've developed software to help do this, you know, I think one, like you said, is scale. Right?

Like, like, you have to be able to detect, you know, code vulnerabilities, third party library vulnerabilities, first party, you know, operating system level vulnerabilities, you have to be able to do that at scale, you know, again, across all your assets, whether your Department of Defense, and you have, you know, millions and 10s of millions of assets, whether the assets in the cloud or not. And it's got to be near real time, right, you know, so for us, and the way we've designed our platform, you can get up to date information, you know, roughly every four hours, you'll have the most recent snapshot of what vulnerabilities are associated with that asset and those those digital systems. And now, the second part is how do you think about remediating those? And again, we're trying to change the industry? And, and I know, listen, I talked a lot of federal partners, and, you know, the struggle they have as you can't treat all vulnerabilities the same, right? I mean, you run into hundreds of millions of vulnerabilities. And, you know, the worst thing that happens if you have your security teams that dump a spreadsheet, you know, it's not prioritized over to your IT team who's already overwhelmed, and you say, hey, fix all of this stuff, you know, and they're like, yeah, thanks a lot, guys. Right, like, you know, not that I had, you know, a busy day. Now, I got to deal with this. And the idea is, you really got to prioritize, right, there's only a very small fraction of vulnerabilities that are out there today that actually create the majority of the risk, and I'm talking like less than 1% of the vulnerabilities that are out there are really the ones that are targeted by AP T groups, threat actors, you know, really expose you to some organizational risk. And again, those are the ones you got to prioritize. And, you know, unfortunately, I think oftentimes a lot of, you know, federal compliance, and you know, even things like FedRAMP, get in the way of some of this stuff, to be honest with you. Because it's like, if I'm going to follow the letter of the law, I'm going to do all of them. But listen, no one can do all of them. You know, we know that doesn't work.

12:34
Jonathan, before the interview began, we mentioned, one of my buddies is David Linthicum writes about the cloud, writes about vulnerabilities just has a recent book that was released. And oh, by the way, if you want to listen to his interview, go to federal tech podcast.com. And type in David, and you'll find it there easily. And he, in his book, he talks about repatriation. And so, okay, you start with the cloud a and then you're gonna move it back in maybe back in house or move it to cloud beat, which seems like you know, I don't know, taking your couch and taking a pillow from a couch and moving to another couch. Oh, easy. Well, in terms of asset management, what kind of assets are left over at in cloud? I mean, and are you responsible for that? And how can you, that's just another checkbox to add, okay, what's going on the agency this year? Well, we're migrating from this to there. Well, what about the old data on Cloud? A? I mean, you've never thought about that. 20 years ago, did you? I mean, the complexity is immense. Yeah,

13:31
yeah. No, it is enormous. And, and, and that, that complexity even grows, right, because, you know, you've got different cloud regions, right. And you some people running workloads, and obviously, kind of the GOV cloud for federal agencies.

But listen, you may have reasons where you need to run in Europe, right, because the majority of the people consuming that, you know, that service are located in that country, so they get better availability to that data center, you know, so now, you know, you've got data in a, you know, European data center, and you got one in the United States. And, and you're absolutely right, I think, you know, one of the key components is, is obviously ensuring that you destroy data that's no longer needed. Right. And, and even with clouds, you know, it's more difficult, right, you're reliant on, oftentimes, they're controlled, depending on how you've implemented the services, right, you know, so now, now you're trying to verify through a third party, you know, that this was done on there. And and so that complexity just gets higher and higher and higher. And it does make for a very difficult job to make sure you're destroying all of your sensitive assets and data.

14:37
You know, when we did some research on your company, I found out that you have a FedRAMP, high certified gov cloud, and I've done enough interviews to know that FedRAMP is a pain and everyone hates doing it, and they curse the day they started it, but FedRAMP High, I think people run out of not a clear room in downtown DC cram it. And so so you guys managed to do that you can answer some of these questions with the system you provide. Yeah,

15:06
yeah, absolutely. We, you know, we know, as a cloud provider, it's important for us to, you know, meet these major, you know, accreditation and authorization. Programs, right. So our federal partners can use our solution. And listen, FedRAMP is tough. I mean, you know, I think we completed FedRAMP, moderate in 2016, decided to go with the high route. And again, even more controls, you know, even harder scrutiny. And listen, I appreciate where it's coming from. I think I'm also excited with the recent OMB announcement about looking to modernize the FedRAMP program, I do think the FedRAMP program is a little out of date doesn't quite keep up with kind of the pace at which, you know,

commercial software is built how cloud providers work today. So those I am excited to see that, that the program will hopefully undergo some changes as well.

16:03
You know, I've been an observer here, and I've seen it for over a long period of time. And so on the DoD side of the house, they had this thing cmmc And everyone was talking about earlier, their airplanes flying by with cmmc and marching bands was cmmc than nothing. Yeah. And was FedRAMP because the same thing, you know, it must have been 10 years ago, you know, the marching band is skywriting, and then nothing. All of a sudden, it's, Hey, we got to catch up to SAS. So, so the changes there, and I think it's good. And I just want to know, what's the timing, what precipitated this? I did COVID precipitate this change in fed wrapper. So what do you think nudged him on?

16:45
You know, I think it was probably just, you know, continuous feedback from the industry and federal partners, at least, I'm hoping, you know, I think, you know, the problem is just kind of the pace at which things move, you know, you know, it's a long arduous process. And listen, there's there's never enough, you know, I think resources to do the assessments, right.

So there's always a long waiting line. And, you know, at the end of the day, what that means is, you know, listen, the federal government may not necessarily get the best in the greatest software. Right, you know, and unfortunately, there's what that means, right, you know, the longer it takes. And then I think, you know, the other challenge is, you know, it's, it's, you know, again, why are we downloading stuff and spreadsheets? Right? Why are we writing 600? page documents, you know, that aren't machine readable? Right? I mean, you know, I think part of is like, hey, we just have to, you know, modernize this, right?

You know, we we can create machine readable documents, you know, those, you know, a lot of that, that review and attestation can then then be done by by computers, right? And they can do that assessment, and there's always a human element. But, you know, I think it's just reducing that kind of human manual workload into keep pace, right. Like, I mean, commercial software, if you think about it, you know, continuous deployment, like, that's a very real thing for all of the major commercial software developers, Right you are, you are writing code every day, you are pushing code every day.

And you're creating and testing new products every day, right. And so, you know, the beauty of the cloud as you can do that extremely fast, you know, and you can bring really great new innovation to market. And so, you know, when I was even talking about our product, you know, the idea of being able to continuously assess and have real time visibility, well, there's a reason for that, right? It's because that's the pace at which, you know, most of the cloud providers and commercial software providers are moving, you know, every day, they are, they are pushing code, and every day that needs to be assessed. And so I think the longer that takes, and the more manual that process, you know, unfortunately, you just, I mean, you get stuck, you know, you're buried, you're never able to dig yourself out to keep up.

18:54

I talked about a marching band, and I'm gonna beat the drum again and beat the drum about your FedRAMP High. But I mean, you know, you might as well, this is not bragging if it's true. I mean, you've done this for 20 years, I mean, your company has been there, and, and you do have a certain reputation. In fact, you are working with the HS and the continuous CDM area, aren't you?

19:11
Oh, yeah. I mean, listen, we, we've been long partners and doing, you know, continuous assessments and diagnostics, you know, back when that that program kicked off. You know, we have a lot of federal partners that use us, again, to get the asset inventory then to obviously do the vulnerability assessments and remediation components, getting the configuration of all of those devices, and then and then obviously, all of that data is, you know, feeding up into DHS and, and again, everyone gets a scorecard and a check and, and, and, you know, we think we do it really well, right? We think our software is obviously you know, the best in its class at it meeting the scale and the complexity of what federal agencies are facing these days.

19:58
Well, I don't think DHS is gonna I look around the corner for you know, a startup in Alexandria with couple of college kids and, and now they could have some ideas. But you know, you really, this is a situation where you've been in the boxing ring two decades you've been beat up, you've seen this, you've seen that there's not gonna be a whole lot of surprises. Now, what surprises me is your ability to do dynamic application security testing. i That's like, Wow, man. I mean, the difficulty that must be really, I mean, so how do you even accomplish that? I mean, new revisions in software, hybrid cloud disconnects, connects IoT data coming in. I mean, so how does one even start to do any application dynamically? Application Testing? I mean, I don't know. Well,

20:42
I'll tell you, it starts with a really, you know, and again, like you said, and this is 20 years of building up the this experiencing capability is just a tremendous research team, right? You know, again, you have to, you know, have, you know, tremendous insight into these applications, you have to have signatures that detect, you know, the common vulnerabilities, right. And, again, some of these are, are static, that are very easy. And then some, our research team has worked very hard, you know, with this proprietary detections to, you know, keep up to date with with these evolving, you know, web apps, right. And it's, it's, you got to give them the credit, you know, again, the technology is there, but you know, having these hundreds of researchers that this is what they do every day. And then obviously, you like, listen, we've been doing this for 20 years. So this, you know, huge corpus of data, you know, of research and signatures that really go into doing the work. And it lives. And we saw some of it. I mean, I think, where it really came into play a log for j, if you remember, log for j, right? Like, oh, my gosh, it was everywhere, you know, there was a lot of like, Hey, can we detected? Is it vulnerable? Is it not? You know, we think we've mitigate it. But I'll tell you through the dynamic testing, like it's a very, like, solid detection, right, you know, in the way that we we did that is listen, if we send a payload, and we get a response back, there is no saying like, listen, we mitigated or whatever we know, that's a true positive.

Right, you know, and so, you know, with a lot of our federal partners were I think they were getting, you know, trying to get kind of steamrolled by the administrators. Oh, we fixed it, don't worry about it, you

know, it's like, no, no, you know, we're still getting a bounce back. We know, that's a vulnerable web app.

Right, like, and you're gonna get exploited if you don't fix it. But yeah, I would say, you know, it's the technology is obviously really good. Being web enabled, cloud enabled. But at the same time, it's really these researchers, right, these hundreds of folks that this is what they do every day.

22:41
Well, Jonathan, thanks for years zero trust update. And we're gonna have to this dynamically as well, only my Do you have dynamic because every six months, I can work in your world of ideas. Okay, mid 2024. Okay, Jonathan, new set of questions and see what happened. And that's what's going to be I mean, Jonathan, six months from now, we could not even maybe not even mentioned zero trust because of another incident that causes all kinds of problems. So, so we'll dynamically update in six months. Sounds good. I love it. You have been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Jonathan troll, Chief Security Officer at Qualis.

23:19
Yeah, thanks, again, really appreciate having it. And I'd really just ask everyone to visit our website, especially blogs.qualis.com, crud, a lot of great content, a lot of articles that I've personally written and others on these topics that I think will be enlightening for this discussion as well. Thanks.