FEDERAL TECH PODCAST

Ep. 47 Understanding FedRAMP High and Platform Technology

Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. In the studio today. We have Rob San Martin. He's the EVP public sector and Patrick Sullivan CTO security strategy at a company called Akamai Technologies. Today we're gonna talk about securing the federal government and a little topic called FedRAMP High. But first before we begin, we are recording this from monk's barbecue in lovely downtown Purcellville. So the real important question is for Rob first, what are you enjoying for lunch this afternoon,

01:09
John, I'm a pulled pork guy all the way. Sample pulled pork up and down the East Coast. If I can,

01:15
right, Drake and Patrick can walk here from his house. He lives so close. What are you enjoying for lunch?

01:19
Yeah, I got to do with Rob the pulled pork is the way to go. Also the Gouda mac and cheese. This is fantastic.

01:25
Wow, Gouda, mac and cheese. It's almost addictive. I think it's really, really good. Now we gotta get serious. The federal government's gone through a lot of changes. Since COVID. Everyone knows about remote, people will look at different systems. And I've done over 1000 podcast interviews with every technology available. Everyone claims to have a product now Everyone claims to be a platform. It's almost like zero trust. You know, it's like, Hey, my name is Randy, from Randy software. We've been doing zero trust for 10 years. Really have you? Oh, yeah. And so what you have to do is put things in perspective. And I thought we'd put things in perspective today with Akamai Technologies 20 years ago, and I was writing for The Washington Post 911 happened. And I remember what Washington Post said, they fell back and asked me to help them cover the load that they had that David's surgeon there. And so that's what I learned about Acme, but it's changed over the years. So I'm gonna let Patrick start, oh, maybe paint the picture of what Acme is all about? And then we'll dive into the FedRAMP. High, please.

02:19
Yeah, absolutely. So So aka my, as you said, has been around for a couple of decades, you know, we're in the business of making sure that the internet is fast, reliable and secure. And as part of that, you know, we

continue to expand what we do into zero trust and segmentation, to really continue to meet the requirements of customers as you embrace cloud and other modern technologies.

02:42
You know, Rob, when I read about different platforms that are out there, I always think it's kind of stretching, you know, it's like, some people maybe can ride 50 or 60 miles, and they stretch to 100 mile ride, you know, and maybe they can't make it or they stop, they quit. And when I think people claim to be a platform, it, it may be a stretch. And so the word that's normally associated with your company is ubiquitous platform. So why did why can you claim that

03:04
you're John, that ubiquity that aka my brings to the table because of our presence around the world and the delivery platform that we can provide to customers. It's just something that we believe is unparalleled in the industry. And the service that we provide that they take benefit from, and that we learn from that, again, with some intelligence just continues to modify our behavior on the system, and enhance the performance we can bring to customers.

03:30
Patrick, I spent a lot of years arguing with software developers and always with the whiteboard, you always draw boxes and long things that whiteboard and then we talked about hot sauce and go back to the whiteboard. And so if you drew a line of what occupy technologies really started, as it was a content delivery network, right, it would be all over the world. And it positioned optimized to be able to understand what that traffic was doing, where it's coming from. And over the years, they've transitioned, they've leveraged that ability in to be more of a cybersecurity folks.

03:58
Yeah, I mean, we we certainly missed a whiteboard, you know, as we've been, you know, stuck at home with with COVID. But But you're right, we started sort of as a CDN. And if you think about that, we ended up building sort of, inadvertently, at first, the ideal architecture upon which to build a security platform, right. So if you think about what we did is, as Rob mentioned, we have a pervasive set of servers very close to end users, or compute wherever that is. And then what we're doing is we're terminating SSL or TLS. These days, to look in clear text at each request all the way up to layer seven as you have to do these days. And in the process, we're, we're gaining intelligence around threats, treating our ability to be in the middle of all that traffic as a giant sensor network. So we understand if there are clients or networks that are more likely to be committing fraud or introducing attack, we can leverage that insight to make a better security decision.

04:56
So Rob, there is a technology out there called Open Web Application Firewall. And a lot of people associate that with Acme is that one of your offerings or how does that fit in the picture here,

05:06

it's a component of the offering. So certainly the web application firewall is key in today's quest for zero trust and the security component that's out there. But it's just one of the pieces as Patrick was talking in our in our zero trust offering, right, there's several pieces that we provide, in coordination with pieces of the customer and other companies provide for a complete solution that helps to solve that problem.

05:29
So So is this a distributed cloud platform is that we're talking about here,

05:33
it's a distributed cloud platform, we think kind of when you reach the level of distribution that we have that you move into a different category, which we will call edge, meaning that we have a point of presence very close to your compute, or your end user, regardless of the network, that they they come in, whether it's wireless or wireline, where they are around the world, doesn't matter, you don't need to think about that, there's always going to be a point of presence very close to that end user, anywhere they are around the world.

06:00
So Rob, yesterday, I had a woman from a company call me and want to come on the podcast, and she could strong background in software development and security. And she was very proud of herself, spent the last three years trying to get a company on FedRAMP. And she was like, at the end of the race, you know, it was in the Boston Marathon, she finished it because it was really, really a big major accomplishment. And, and I think a company getting FedRAMP is a major accomplish, and just tell us what would basically that entails, then we'll take it and move it up to FedRAMP. High,

06:26
okay, it is an accomplishment, the process has improved over the years, we went through it initially, probably five or six years ago, aka my has a FedRAMP Moderate platform. And we're in the business right now of working to submit for a FedRAMP High. The things that have made it more interesting is that I think with the recent budget that just passed FedRAMP became law where before it was just a mandate. Now it's a law. And I personally believe that within the next couple of years FedRAMP High is going to become the minimal standard is acceptable out there. And you know, the tangential component that businesses that work with the federal government are gonna be able to take advantage of their state and local businesses, the state ramps that are coming out seems to be that there's going to be some acceptance that if you are FedRAMP accredited already, you're not going to have to go through those state. But that's my impression of what's going on.

07:20
You know, Patrick, people asked me who listens podcast, and generally speaking about 60% of the audience are federal, and 40% is probably other companies. And they say, Well, why would own companies listen to this, because they're constantly looking for people to partner with, or maybe this company is, has got this one advantage, maybe a service veteran disabled or a certain technology. And it would think that the affiliates in the Washington DC area here might be very interested in alchemize ability to move up from FedRAMP to FedRAMP. High?

07:46
Yeah, I think that is very relevant. And as you said, I mean, that's, you know, part of a ecosystem that that we participate in, we're obviously looking at strategic partnerships where we can find those. So that makes a lot of sense.

07:57
So what's the nitty gritty here? Where's the differentiator? And how is high differentiated from the Federal Real Food ramp? Yeah, there's

08:04
a there's an extra set of controls that get put on from FedRAMP, moderate to FedRAMP. High, I think it's about 150 155 controls. And then dealing with the military, the DOD, you know, they're looking for impact level five, potentially impact level six, which are accreditations that they hand out uniquely, that's not, that's not on the on the civilian side of the world. The biggest, the biggest situations you have to deal with or, you know, the data has to be air gapped. It can't be commingled with somebody else's data. And then there's a requirement for US citizens support for some of that information. It's a lot of information out there.

08:41
So I'm trying to draw an analogy here. So if FedRAMP is a marathon, then FedRAMP High is a 240 mile run through the desert. Is that the difference? Or is it a lot harder than that?

08:53
Yeah, no, if you're starting from zero, going straight to FedRAMP High. There's there's a big community out there. This developed between the the assessors and the advisors, that are become very efficient in helping companies steer their way through these things that weren't, weren't as prolific when we started this the first time. Now make a big difference in steering you what you need, and can you assist you in putting your package together, get it done.

09:15
The next interview we're doing from MGS BBQ is going to be talking about cmmc. And then inevitably, we talk about CMC, you're inundated with controls and this and everything else says NIS play a role with FedRAMP higher where they all fit that's separate completely,

09:29
it's commingled together. And then when you get to the C MMC, right, people have been required to do some assessments already and audit yourself to see where you fall and then are you going to have be able to fit into the moderate or what level of cmmc Are you going to have to abide by there's going to be some challenges there for some companies, especially like ours, that are not exclusively federal, because the commercial side of the business which is the prominent business, you know, doesn't necessarily meet all of the credentialing that's going to be required. So that's going to be we'll see how we handle that as it goes forward.

10:02
When I first heard aka Mike, I kept thinking about like a big unified package you bought, you bought it or you didn't buy it kind of like that. But phone I've been reading, it seems that there's different separate offerings that are available to other companies may will take advantage of kind of like amongst barbecue, instead of having a whole dinner, might want to just have the mac and cheese or something like that. Yeah. And so is this important for people who listen to this knowing that you can work with acumen a different way than maybe they traditionally think?

10:27
I think it is. And we've been pivoting over the last couple of years. As you said, John, before, when you bought aka my you had to have optimized to deploy it to change it to fix it into everything else. Now we have products that are deployable by integrators and by customers. So the ability for us to be combined and to work with influencers to be part of their go to market solution and strategy where they can perform the work and we don't have to perform all of it has increased significantly. And that is absolutely the direction that we're moving with the zero trust solution and providing those components, I have

11:02
to remember my radio days every now and then, and I have to spell out the name of the company. So it's a que a mai.com. And I'm sure they have a blog there. I don't know if they have a podcast or not, but a lot of information@akmai.com. So Patrick, you have done a lot of traveling and seen a lot of different things. And so what can my God, he's learned from all the time you sat in these stupid planes play on it knows that. Yeah, another, you know, 50,000 miles this week. Patrick's so what's in it for me? So what lessons can people from Singapore from India from Africa, learn the federal government, especially with that,

11:36
let's say the first thing for the US federal government is, you know, that it's really perceived as a model around the world. You know, I was recently in Singapore, and I think they're they're seeing the the great work that that the US has done with Sissa, as an agency being proactive sharing, and other governments around the world are trying to pick up on that, you know, can we do something similar in our geography? So I think that's an area where the US government is to be commended. You know, I think there are other areas where we see maybe working with technology companies that will move down a path maybe a little bit as an earlier adopter, that, you know, relative to the government, for example. So I think they're we're seeing a lot of focus on securing API's. As you know, the whole world is kind of, you know, shifting to an API first world. And then I think we, you know, more focus on software, replacing hardware based appliance based solutions, that shift continues to take place. And maybe that's an area where, you know, some of those early adopter companies in the technology space, maybe have a little bit of a head star relative to the to the federal government.

12:37
So Rob, I don't know if you read the executive order that Biden signed this morning. But it's now a mandate. Every time you do a podcast, I have to say zero trust. Oh, that's fantastic. Do a 170 dash 123. And the OMB is going to be auditing me. So make sure you haven't seen zero trust?

12:55
You sure didn't say aka my zero trust, right.

12:58
So where does this fit in discussion? Can you help federal agencies achieve that nebulous goal of zero trust? Or where do you fit this whole discussion?

13:05
We can, we can. And we have several pieces of the solution that we believe are very credible, worst, whether it is credentialing, or whether it's identity, segmentation. We talked about some firewall technology. And in the FedRAMP package that we're putting together, there's, you know, there's platform there that is the underpinning of the offering of zero trust that can be very valuable within the within the federal system of integrators and solutions.

13:35
Patrick, to do my research for this interview, I watched several Jason Bourne movies and some Bond movies, and I learned about what people steal, and they steal the data, okay, they steal the data, okay, that's all it was focused on the day, it's got to be encrypted, this encrypted data, and it's in thumb drives and people die over it in its day to day data. And you're telling me no, John, man, may we look at the API's here, maybe that is the key to getting to the data. And so when I read about API's and data, you know, the next topic is going to be quantum well, quantum is going to decrypt everything. So if you're sitting in a plane to Singapore again, and someone says, Well, so what's the priority here? Is the quantum is data or is it API? Or how does this all work? Yeah, what's the priorities?

14:13
Yeah, I mean, I guess depending on who you are, you know, that kind of shapes which threats you need, if you're Jason. Yeah. But But I think, you know, statistically, if you look at sort of the corpus of research on breaches, how do people get get breached? It tends to be the more mundane things it's less James Bond are Mission Impossible hanging from the ceiling. It's, you know, an exposed API, or it's, you know, somebody has an initial access via phishing or some other technique, and then they're able to leverage kind of the the trust that's extended across the enterprise network, to move to crown jewels. It tends to be the more mundane things that that break down in the vast majority of cases. So Rob,

14:53
when you look at the federal government today, and all the transitions taking place, the cmmc and moving to the cloud and hybrid cloud All kinds of challenges. What advice would you give a group of federal CIOs if you had them at a barbecue place like this? And they said, well give us two or three things we can do that's low lying fruit, that we can actually reduce our risk.

15:12

You know, I think one of the leading pieces out there, it's it's not real attractive to talk about, but it's creating an amazing amount of noise and traffic that's not useful is bot mitigation. There is, you know, we saw we all saw the Taylor Swift tickets that went on there that we assumed bots, were out there that were buying tickets, and then building up the networks for everybody. But it's, it's there, you can create a bot every day, there's a bazillion of them, and it's nonstop. So you're chasing forever. So we would like to offer help there, right? We actually are searching for humans in our bot mitigation. So so we think we have a little bit of an advantage here, because those are finite to some degree. And then zero trust, it is a journey, people have been talking about it, there is no one product, we do not have the only product and we do not have the entire solution. It is a partner. It is an elastic partnership between the government and industry to be able to bring all the parts together along with internal procedures, so that it can be a useful and successful deployment.

16:09
Well, I talked about the executive order that was released today. Well, tomorrow, my good friend of the White House, tell me there's another one going to be released. A new mandate is going to be every time I talk to Patrick Sullivan, I have to use the word artificial intelligence. Ai Oh, well, how do you wash your car? I use artificial intelligence to wash my car. Oh, really? How do you get to Pittsburgh? Well use artificial intelligence to the Pittsburgh. And so I guess we have to ask, does artificial intelligence play a role in how I can help my federal audience increase security.

16:36
So I love the fact that we're being compliant with

16:41
it right piece of paper, he's got a piece of paper and a pen. So you got to comply with that,

16:46
without a doubt. So I think we, in the security industry of seeing the opportunity to leverage machine learning, you know, to keep up with the reality is you cannot hire enough analysts to continue to look at a screen all day 24 by seven, so where you can you want to leverage machine learning. I think Rob leveraged or mentioned a good area where we had early introduction to machine learning technology, a lot of sort of how we disambiguate a human from a bot, is based on machine learning, if we see the mouse movement and key press, how much does that resemble human interaction versus a bot? Similarly, we sort of have threat hunting capabilities, you know, based on segmentation, where the first pass is machine learning to look for anomalous behavior, and then you have a human, kind of refine that and filter that and add their expertise. So it's, it's an ever growing part of our lives and with with chat, GPT it's, I guess, you know, doing the homework for for our children and passing the medical exam, I guess, recently, to be a certified doctor. So it's, it will be a ever growing part of both our opportunities as defenders, but unfortunately, also the the available tools that attackers will leverage to write better malware more compelling fishing bait that they create. So I think both sides of the equation will leverage that technology.

18:07

So Rob, I was reading this morning about Chet GPT. And apparently it costs them $10 million a day to keep the servers running to go through some experiments or playing around. Wow, there's a whole lot and thinking amount of traffic that's going through there something traffic, kind of called Rob St. Martin, for this traffic guy. Yeah, we would love to serve that traffic traffic up and personnel but on the real traffic. So that's where you'd fit in this discussion.

18:30

Yeah, we would be more on the we'd be moving the data back and forth between between the application and or the consumers that were looking for it. So we would fit in that kind of FedEx model in the middle where we take the package and deliver it efficiently to where it needs to go. With the appropriate Yeah, with the appropriate security that the customer wants to wants to have on it.

18:50

Before this interview, we talked about mongst Barbecue, we talked about a lot of different things. And I referenced a guy named Niels Bohr. And I have to quote him because you know, I want to impress him with my intelligence, you know, and he said something very, very important. He said, prediction is difficult, especially about the future. And it's too much for me, but I'm gonna have two smart guys in front and someone asked them so I will start with a Patrick here. So give me a five year plan here. What do you think's gonna happen? You think there's gonna be an incident people gonna get serious about this? Or is cmmc gonna solve problems or give me a prediction here?

19:22

So I think the right incentives have been set up, you know, if you look at the federal government, all kidding aside, you really have no alternative other than to kind of pursue a zero trust architecture. And most of what zero trust when you strip away the the buzzwords, it's common sense, you know, good first principles. So I think we will continue to see, you know, more progress in that direction. I think, you know, cloud and API's we touched on, there doesn't seem to be anything that would suggest that those trends are going to slow down in the future. So I think it's a pretty safe bet, that we'll see more of each of those. And that's going to shift the way that that attackers try to come at you. So a zero trust. You know, hopefully the goal there is that five years from now, when you read a breach report, it's radically different when somebody you know, was successfully breached, then really kind of the Groundhog Day of the last 10 years where you could kind of change the year on the breach report. And nobody would notice, because you're basically saying the same thing year after year after year.

20:20

Yeah, I interviewed the people from Verizon about their breach report, and most same interviews year before almost, there's nothing new there, you know, but it's good company, everyone has a lot of trust in that. Rob San Martin, I do see this trend towards looking at API instead of the data. I lived in talking about web hosting for a while and examining traffic and everything else. So where do you see this as the next four to five years? You think it's going to be more and more focused on that? Or is there going to be some some unknown chat GPI artificial intelligence? It's, it's the Patrick Sullivan bot that is attacking? What do you think's gonna happen? Yeah,

20:50
I don't know. I, I look at it and talk with friends and family all the time, from the perspective of how is it going to affect us, and our credentialing or how we get access, and what we get access to, I think is going to be noticeable to us. You know, MFA is, you know, the most recent one that we do a little bit. We do a little bit of authorization on but I think that's going to really amp up because the opportunity for attacks, and as quick as they can change and the bread trails that they're not leaving any more to what they're doing is only going to intensify, in my opinion. So the lot of the onerous I think is going to shift to the end user to are you really who you say you are, and are we going to let you in? And what are those controls is going to be? I have no idea. No idea.

21:40
What do you said edge user Arrowtown. edge edge computing is a podcast in town called pheasant the edge. And so when I think of this idea, in other words, if someone is that is in Utah, and they have some data, their choices, do they take and relay that data to Patrick's house and Washington DC? And were there or do they process it there? And I'm thinking, Well, if this is the case is going on, they're talking about this, by the way, in satellites as well. And so edge computing is not just down the street edge computing now isn't here. It's it's in Singapore, it's up in the sky, it's an outer space. And so it seems like to some companies that are placed very carefully, they're ubiquitous. And they can understand exactly where all this new traffic is coming from. So Patrick Sullivan, edge computing should be your sweet spot.

22:28
Without a doubt. Yes. So I think the way that we want to approach this is to give developers options, right? There are to your point, there is some compute process that should exist very close to the end user, that's optimal. There are other forms of compute that are very, very heavily tied to a centralized database. And it probably makes more sense to run those in a less distributed capacity. But I think if you look at modern development practices, where you've got microservices, and you're decomposing those applications, I think, where we want to end up as developers as part of their planning process, figuring out where each microservice should run, some are gonna run at the edge, some are gonna run centralized. And they'll optimize based on that, given the choices that are available to them.

23:13
Micro segmentation data centers, now we're talking about micro grids, and it's really becoming very edgy. But that's really what's going on. It's a lot of things about the edge, just because the data center doesn't mean it can virtually connect to another data center where the traffic is going to have to be inspected and care for it's got to be secure. That's right. This has been a very interesting conversation. You've been listening to the federal tech podcast with John Gilroy, like to thank my guest, Rob San Martin EVP public sector and Patrick Sullivan, CTO security strategy at Akamai Technologies.

23:46
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 podcast.