FEDERAL TECH PODCAST

Ep. 45 Network Management to Improve Federal Cybersecurity

00:14
Welcome to the federal tech podcast where industry leaders share insights on innovation, for the focus on reducing cost and improving security for federal technology. If you like the federal tech podcast, please support us by giving us a rating and review on Apple podcasts.

00:38
Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Most of the listeners most of my gobies out there know about f5. And they have a pretty good idea what their history is maybe heard of they seem to trade shows, maybe they use a product, what do you want to do is every now and then to bring f5 in the studio, give them kind of an applied update for 2023. And I think I want to do is position themselves as how they can help federal agencies with a lot of the new goals I have. They have a hybrid cloud there for about zero trust, I have to worry about security and and I think f5 has got a strong reputation, the community, but maybe my listeners aren't familiar with what's currently going on with a company. And that's why I brought in Peter, Peter. Kirsten is our guest today. He's the Regional Vice President with that five Peter, how are you? Good, thank you. Okay, so let's say you're sitting in the metro or you're at an event downtown and and someone sees your name badge. They say f5? Well, I know all about f5. You guys do load balancing. Right? And you go now wait. So so how do you how do you disabuse them of that notion of how do you amplify that? So so people got this in their mind? Talk about f5 and load balancing? And really what you can help our agencies do

01:45
so generally, if I'm in a situation like that, I'll let them know that that's absolutely where we got our started. Right. But we've been around for 25 years. And like I say, it's typically all up in a meeting and asked what do you know about us, and they'll say load balancing. But if you think about it, a lot has changed in 25 years, right? So we moved from, you know, initially, it started with load balance, it moved where we created a space called application delivery, which was more than just load balancing, but making sure that the applications were available with the right performance, resiliency, and then we moved into security and making sure that we were protecting them. But in the last five or six years, we moved to embrace the move where the government is moving to containerized applications and cloud deployments, providing services to scale and secure modern applications and API's. So we've been calling this adaptive applications. And we're working to use layer seven telemetry, along with artificial intelligence and machine learning to simplify and enhance application deployments and maintenance. Right. So today, where are we We're preferred partner about 18,000 customers globally. 85% of the Fortune 500. And we power about half of the world's apps. So here's an interesting fact job. And what I share with someone on the metro, right, what you may not know about us is the role we play in cybersecurity, we've established what I think is a leading position in protecting the digital world.

And the US government, because we're one of the few players 100% focused on application security at a time when those threats are growing rapidly, right? We just passed a billion dollars in annual security revenue. Right? So that makes us one of the largest players. And we're the only company that can deliver secure and optimize any app, any API anywhere, right through this diverse portfolio, and distinctive capabilities, from hardware to software to SAS, and managed services. So it's been a long time since we've been just a load balancer, but it's still a core competency.

03:53
So I talk to young people all the time in the classroom and Thursday night downtown. And if I told you about your company, and I use the phrase that you faced application application, they may raise their hand and go, no, wait a minute, I just listen to a podcast about quantum encryption and encrypting the data. And Peter, you don't get it. It's all about the data. It's all about the protected data. Isn't that I mean, isn't isn't that a differentiator is that, you know, some people focus on the data, some people focus on the API's of the app. So So what F five in there 25 years of being beat up in the cybersecurity world and learning lessons, I guess, the the data is the priority for you folks, is the API naps. Is that right?

04:32
That's right. It's all about the apps, right? I often joke that we're like, remember your Dr. Seuss, the Lorax for the app, right? We speak for the app. We make the apps work in any environment. So traditionally, I think that apps have been in a singular enclave and now we're thinking about data and we're thinking about how data gets spread to different data centers into the cloud, etc. You have to protect the data Often the data sitting behind the apps, and the apps need to be protected a little bit differently than the data. And as we move to a more digitized world, where there's more and more dependency on those applications, you've got to make sure that the applications work, or you don't function as an agency or organization. I went to

05:23
your website, F five.com. And I took a bunch of notes this morning pretty early. And load balancing, of course, App Security, API management, and then fraud prevention is right in the list there. It's like, okay, connect the dots here. How does the Lorax connect these dots together with fraud prevention?

05:41
Well, so fraud prevention is absolutely something we focus on more in the commercial market than federal that we do have a couple key customers and what has been happening in the world kind of cyber criminals is they've been focusing on how do they find the money, and they can do that by compromising identity. And often the tool sets that they're using are leveraging bots, and machine learning, and the ability to automate attacks around bots to take maybe compromised credentials that they're finding on the dark web, spraying them out there. So we have an entire solution set that's focused on fraud, but it intersects into what we do with our other security kind of protections. And we leverage kind of the information, the data around how we look at authentication. So that's how I tie the two together. Right? It's,

06:47

it's the choke point, or it's the bottleneck that can examine and see what's going on. So it actually, it's not out of sequence at all load balancing app security, payment fraud, French fits right in there, because that's that's the net result of effectively accomplishing those three tasks, isn't it? It is

07:01

it is, the other way to look at it is like our primary use case for government typically, is authentication. And when you look at fraud prevention, it's about looking at the authentication tool chain, and how do we communicate users that don't have a CAC, or, you know, some type of a higher level of identity and multifactor authentication?

07:21

Right, right. Makes sense. And, and maybe we can talk about this a different, a little bit off topic here. But but the the key pillar to zero trust is identity authentication, and this is the first pillar. And so I think this is f5 is positioning itself. Right. And, and I, I'm thinking of architecture here, and buildings and everything else, and I'm thinking about enterprise architecture. So maybe, maybe the phrase is, is API architecture API design or something. Maybe that's what it's all about, is it?

07:50

Well, if you talk about API's, I think the first thing that I would say is that API security is critical. And it's new. And a lot of people think about it right. And API security gets kind of merged in with other things. We think that it's critical, and that everyone should have API security on all their API's. But if you back up a second, let's say you were talking to the college students maybe start with kind of what an API is, right, because it's an application programming interface that enables applications, or with modern application different parts of a single application to communicate with each other. Right. So it's an intermediate layer, that processes data between end transfers between systems, and allows that application data and the functionality to be available to third parties or other departments within an organization. Right. So most of your new modern web applications rely on API's to function. So they're kit and parcel to the same thing you've asked me about API's. And when you add them, you also introduce risk into the application by allowing outside parties to access it. So even though the backbone of modern apps or API's API's suffer from some of the same exploits as the apps that they service, and those type of exploits are different, right? They're a little bit nuanced, right? Their vulnerability exploits authentication based attacks, unintended access, right? And users getting data, they shouldn't have data exposure, DoS attacks, right. And it's one of the fastest growing attack vectors that we have seen in the last two years, right. So we have a whole suite of solutions that protect API's, right? Big IP does engine X f5, cloud services, they all have API security. And it enables us to kind of apply that because as you look at the API's, and where those API's are operating, you need the right system that was constructed for the environment, right, a modern application that sits inside containers is going to have an entirely different kind of nature based upon how containers work and the size of the software that works in the micro services. It's different if you need a fully managed service, it's going to be different, right? So we kind of pull those all together. And when we talk about API's, particularly also talking about web application firewalls, and we have this concept of one lap, which ties everything together with kind of a common control plane, so that you can deploy a security policy in one area and map it to other areas. And so you have a universal defense that isn't

different, just because you happen to deploy in AWS, or just because you deployed it on pram, versus a SaaS service that you that you purchased. Well,

10:49
Peter, let's take a look at this suite and pull out a couple of topics here. So let's go from the classroom into a conference in downtown DC, sitting around with a bunch of cybersecurity people, I'm sure if you toss out a term like big IP, they would kind of have a fuzzy idea of it. Or maybe what you mentioned earlier is Nginx. So maybe for our audience, maybe you can differentiate those two for the people who who don't really know as much about FYI, as they normally should. Sure.

11:12
So like high level, just answer the question quick, and we get a little bit of nuances. Big IP is typically what we deploy for traditional applications that traditionally sit inside the data center, behind kind of one environment. And nginx is what we deploy for modern applications or micro service environments. So if you think about it, you know, traditional apps, relatively large, tough to deploy and maintain, but but pretty well understood. And big IP offers a lot of flexibility. So that is, as the apps neat, those are really tough to to modify those apps, right, you might get like one time a year. And so big IP is flexible enough that you can adjust around that application for that application. TLS is moving or something else will take care of that for the app for big IP or modern apps, they're built into an entirely different framework, right, where pieces of the application are broken apart based on functionality. And they sit in separate areas of what's called a container. And they communicate with each other via those API's. Right. So they're faster to deploy an update that with the idea that it can be updated as much as several times a day. And so that's where nginx sits. And then big IP also plays a role because it can sit above nginx, and big IP, and directing and securing kind of web traffic to either the modern apps, or to traditional apps. In a hybrid scenario, which is often what we see with the federal government today, we don't see that going away, because people are gonna have their legacy apps, they're gonna have modern apps. And the government's kind of been traditionally struggling to get to full modern application, both because of concerns about security. But also you need the right people on board in the right environment. And you want to make sure that those are really well thought out before you deploy a system that governments can deploy on. They rely on for that. And those generally are there today. But it's not going to be one size fits all, no.

13:22
Well, let's talk about the struggle. And when you get a complex environment, with all these different firewalls and rules and API's and apps, it gets difficult to really understand and, and I think once a year, what your company what f5 does is put together a public sector symposium, and there, you can't go back to the classroom analogy. It's like a classroom, you go there, and you can say, oh, so So where should I use big IP? No, no, well, Peter is gonna give a talk and he's gonna talk about, you know, three places where you can use IP or they work better with engine X. And so tell me more about supposing I think it's coming up in the next couple months, isn't?

14:02
It is it's March 21 to 23. It'll be at the Ritz Carlton in Tyson's Corner. And it starts with some keynotes where we traditionally try and address from an F 5% surtax, excuse me, and a government perspective, some of the key

trends or upcoming kind of challenges for government. And then we have for in depth user focused engineering breakout tracks, where we're really focused either on nginx or big IP, and it might be a 100 to 200 or 300. Those are all designed to lead people to certifications and they're free for government. Good, good. And then it's full day interactive. We got, you know, partners, and we've got other groups within that say you can have face to face interaction with f5 folks or with partners, and they have the opportunity to take a exam on site for free. If you're a government employee, if they just go to f5 dot com. And they search for the 2023 public sector symposium that'll lead them or registration and get registered early. It's pretty big show. It's a great event.

15:09
Tomorrow, I am going to interview a gentleman, we're talking about software development, lifecycle and security, talk about software libraries, and talking about this thing called shift left. When I was doing my research on F five, I saw some articles about, you know, big IP actually helping in that endeavor. And being involved in fixing vulnerabilities. I said, wow, it's got more power than I thought. So I guess that's an area where you also plan is that right?

15:36
That's right. Well, so and typically shift left is a term that is referencing the move to modern application deployments, and being able to deploy applications a lot faster. And so traditionally, when we think shift left, we're thinking, how do we apply the services associated with Nginx? into that environment? Right? And in that environment, right, nginx open source as a, as an application tool set is deployed all over the world all over the government, etc. And this is about how do we apply those services into that area? And specifically, shifting lectures means how do we get things to go faster, right? Well as pushing security earlier, as pushing into a continuous innovation, continuous development type of a pipeline versus a traditional application would be called waterfall environment. So we

16:32
actually fit in with that discussion for tomorrow, doesn't it? 100%. Wow, that's really great. And I'm just trying to put some of these concepts. When I think of zero trust and security, we talked about, you know, authentication, and I'm thinking about firewalls, I mean, just does a firewall fitness discussion, or is a firewall just complete different MIT having different a different firewall than that's normally understood? To be?

16:57
Sure, why do you think that a traditional firewall I live for, right is looking for information from the source and making a decision about whether to allow or not allow something where a web application firewalls a little bit different, and a web application firewall is an absolutely essential and incrementally separate, kind of part of any organization cybersecurity arsenal, right? We have, just like we talked about with API's, every app should be covered by a web application firewall, right? When you think about application layer attacks, for example, if someone is trying to insert code into a form field, or break in through some sort of user authentication in the application, a regular firewall doesn't have the visibility into that layer. And therefore they can't protect against those type of attacks. And that's why there's a need for an additional layer of protection at layer seven, right? So we had, for example, so several large agencies that had already deployed their web application firewall.

And the flexibility that it gives them as an adjunct to a traditional firewall was they were able to block and protect against law enforcement a virus, because of the difference in how those security mechanisms are deployed. Right. And that's just an example of having a tool set that's differentiated and flexible, that enable them to extend their cybersecurity boundary. When you think about you mentioned zero trust networks, and zero trust networks are, are mandated and necessary. And it's a pretty hot topic right now. But what zero trust networks traditionally don't do is they're not focused on the application. And even though they may, you may have it in place, or you may have a plan based on the Presidential Record to put one in place, your application infrastructures still vulnerable, because as eta is going to determine who has access to an application, and usually it's going to be for internal users, but it doesn't know a user's intent. And so in order to kind of have complete security, a web application firewall should be protecting every AP, and really every API from all traffic, both internal and external.

19:21

And so I'm going to talk about remote code execution. And I'm putting it in perspective to my own architecture here. So that's so that's what the adaptive application is all about. Because John, it doesn't you know, punch a clock eight o'clock in the morning, go home at six, it's there 24 hours a day, and it adapts to the threats and the threats have to vary during the day and and I imagine all kinds of different types of threats to so adaptive applications means they can analyze live apps and this remote code execution could be one of them, they get blocked. So it's it's almost protecting the the it's almost like a river going by and protecting everything going back and forth through that firewall and stopping the bet. It's This has got to be difficult.

20:02

Yeah adapted apps is is an f5 coined kind of term of how we look at how we are going to interact with the application. Ah, so applications are getting more and more complex, right? We talked about deployments in the cloud or hybrid models on prem, you know, modern app, legacy apps. And so adapted applications at its core, is the concept that as those become more complex, you're still going to have hybrid environments. And you're going to need to be able to look at the layer seven telemetry that unique inside the application and make decisions based upon some of that information to speed up and simplify how that decision process is being made. And if you can apply artificial intelligence and machine learning to that you are kind of closing a loop on some of those decision trees are making those available to someone much quicker before the problem exists. Or if you've identified a problem, how quickly can you resolve that problem, right from a troubleshooting or a forensic standpoint,

21:08

we're kind of running out of time here. If you're listening to this and want to learn more, do a bit deeper dive into the product offerings at f5 have public sector symposium March 21, down at the Ritz Carlton Tysons Corner, you can go to f5 dot com and and find the registration there. You have been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Peter Kirsten, regional vice president f5

21:29

Thank you very much. I appreciate you bringing us on and hopefully we'll see folks that are symposium.

21:35

Thanks for listening to the federal tech podcast. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcasts.