FEDERAL TECH PODCAST

Protecting Apps across the Software-as-a-Service Platforms

SUMMARY KEYWORDS
sas, app, salesforce, security, application, cloud, brandon, secure, people, configuration, users, data, endpoints, posture, problem, test, customers, omni, scanning, saas applications

Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator today. Our guest today is Brandon Conley, Chief Revenue Officer at a company called App Omni. If you are Federalist or you may not have heard of him before I'm gonna spell it out for you a ppomni.com And, and that's retirement shot apps and App Security specifically for the federal government. So Brandon, maybe give us a thumbnail sketch of your company and how you wound up working for them, please,

05:12
I'd be happy to join the company about two and a half years ago, we're a four year old startup based in Silicon Valley in San Francisco. The company was founded by the former chief information security officer@salesforce.com, Brendan O'Connor and his co founder Brian Sobey, who was the second person on the product security team at Salesforce. After Salesforce, Brendan went on to ServiceNow and lead to security for the SEC ops Line of Business at ServiceNow. So there's a wealth of SAS vendor product security knowledge within the company, including many of the engineers. And the goal of the product is to solve a large and growing problem, both in the commercial space and in the federal space. That is securing the SAS applications that almost every line of business now, whether in public sector or commercial are leveraging for HR products, like Workday for email, in collaboration, G Suite, or in 365, for managing customer relationships, which also applies in the federal government products like Salesforce and other CRMs. And these operating systems, as we like to call them have evolved into far more than simple web apps, right? They are complex amalgamations of different capabilities and functionality that have grown in complexity over time. And there are in some cases, hundreds or 1000s of configuration options in each of these applications. The challenge is that most customers don't realize there's a shared responsibility model, when it comes to securing these apps. The SAS vendors themselves do a very good job, scanning their code, fixing vulnerabilities, hardening their infrastructure, in their data centers. But once the application is on boarded by the customer, and configured by them specific to their environment, that's where the responsibility of the SAS vendor ends. And over many years of using these products, many misconfigurations have been introduced that have resulted in many data breaches. You know,

07:13
Brandon, back when you were in high school, 15 years ago, I was I was interviewing people in the federal government, they talked about the cloud first. And that was a pretty easy cut. You're the in the cloud or not in

the cloud. That was awful, easy, 1518 years ago, and then I had someone on from Salesforce. And it was Oh, it wasn't that popular in the federal government. Now, it's very how it wasn't popular that it would like to I could like go to a whiteboard and say, Well, here's the circle of the cloud. And here's this. And so what's happened is, has been like 40,000 people come in to the whiteboard and drawn their circle on it. And so the simple circles from 15 years ago, all of a sudden, very, that you were amalgamated. I think that's an amalgamation of everything is just so difficult to understand what's going on there. And, and some people pull out the obvious, like, I was listening to a podcast with a guy from Colorado. And he said, You know, sometimes the system goes down, but we have Office 365. And that's always available. And so you get the Lord into this, you know, so it's a, it's a complex environment to understand, isn't it?

08:09
It is, and I think most organizations, again, commercial or public sector don't have the SAS expertise in each of these platforms to fully understand whether they're configured correctly or not. And so we've taken it upon ourselves to amortize the work of understanding all the security implications of the settings across these major SaaS applications, every time that the vendor updates their product, and adds new knobs, dials, switches and levers. And we do the work of understanding the security implications of those features, and helping our customers automate the process of ensuring secure configuration. It's a big challenge.

08:44
And that's why I say about this guy in Colorado. Yeah, they're using Microsoft, that's fine. They have certain proprietary ways to control the cloud. Well, so as Google, well, so as Amazon, I mean, it's, it's like, well, you, what are you going to do? You're going to be in a federal agency and hire, oh, here's the Google guy, Brandon. And here's a Microsoft guy, John. And here's Mary, it gets to the point where you can't have them in its expertise with each cloud, because they're all different.

09:09
They are. And I think we've done a pretty good job over the last decade understanding and securing IaaS Infrastructure as a Service and platform as a service from AWS from Azure, from Google Cloud. But those three clouds are very similar. So once you build tooling to monitor and manage one, it's not that difficult to translate that capability to the other two major clouds. And the concepts in AI as and pas are much more analogous to traditional legacy on prem networking servers, host databases, then SAS so unlike I as in past, where you only have three primary clouds, and the security issues with them are fairly consistent from one to the next. Each SAS application is a snowflake. They are completely different in the way that they're architected. How authentications controlled or managed How authorization to data occurs inside the application. They all have different capabilities and building a tool to secure one does not solve the problem for the next and there are 1000s 10s of 1000s of SAS business applications that organizations are using.

10:15
Speaking of 10s of 1000s, I live in the Washington DC area, we have 10s of 1000s of acronyms, CIA, DOD, all kinds of acronyms. And I think the focus of this discussion today is s s p m. And this involves a technique to manage these applications that maybe can tell us about Asus pm and how it fits in the discussion, please.

10:35
So SSP M stands for SAS security, posture management. It is a somewhat unfortunate acronym or name given to the category because it focuses on only one aspect of SAS security. And that is the posture, which refers to the global system settings that apply across the entire environment when you configure something like Salesforce or ServiceNow. That is indeed important. And it's one of the things that SS pm vendors do out of the box, they will scan your instances of these apps, compare them to best practices, sort of out of the box policies for security, and then show you what your posture is relative to those best practices. And that's ever changing as the vendors add new features and security functionality. However, that's just the tip of the iceberg. So beyond the global system settings and posture for each of these, which need to be monitored for drift continuously, there is who has access to what within each system. And again, that's that's handled completely differently from Salesforce ServiceNow to Mt six, five. So analyzing what roles and users can get to what data within that application is an incredibly important aspect of SPM. It helps you to identify when PII pH i or intellectual capital may be exposed to users roles or even the the public internet without authentication, which is very difficult to determine without a tool to automate that process. So there's posture, there's data access, then there's monitoring the user activity, all the logs coming from these systems are in different formats, and most organizations aren't ingesting them and analyzing them today. And then there's compliance as a outcome of all of this scanning and telemetry.

12:13
I was just going to use a nasty word that's used inside the beltway here, and it's word compliance. And if there's current, you have to be continuous maintenance. And there's new standards and regulations all the time. It's just I don't see a one human being can even monitor logs, I talked about 15 years ago, maybe you could monitor the logs back then, however, it was tedious and boring or unwanted. But today, with the incredible number of devices out there the kind of normal apps, I mean, I've heard numbers like hundreds and hundreds of apps for a typical federal agency. And so if you're focused on your data center, if you're focused on your identity management, if you're focused on zero trust, very focused on you kind of put the apps down the checklist, but they should be up on the checklist, couldn't they?

12:56
They absolutely should. And the way that the process works today, and onboarding a new SAS app into an environment, it's usually introduced by a line of business user, right? It's not it who's selecting the SAS application and bringing it into the environment, it's the users trying to get their jobs done. And so all that happens today is a one time vendor security assessment of ESA, of the SAS platform itself, which happens at the time that it's on boarded, if they're lucky. In some cases, these apps get in the environment without any vetting by security. But if there's a contract process involved, they'll typically do a VSA. They'll establish that the SAS vendor is following all the correct protocols, and then it's quote unquote, secure out of the box, but they never look at it again. And that's where things go wrong. Because every day they're making changes to these applications, data is getting added users are getting added new functionality is being turned on. Administrators are making changes to maintain the application. And if you're not continuously monitoring, you can find yourself in a state where data is exposed and subject to a potential breach.

13:55
When we look at the big picture, like 1015 years ago, I I can see that, you know, started being used more and more 1015 years ago, now now we have a situation where Oh, yeah, maybe one branding out of college, we had one app, and then it becomes a few of them a few more. And I have 1000s of a sudden this is an accumulation of pride in some worlds is called technical debt, I guess. I guess this is a tactical obligation, you have to manage these apps. And I think people are putting the port in the back put in the trunk, we'll get to that when we get to the vacation house.

14:28
I think they've they've sort of had to because up to this point, there hasn't been tooling to automate this. And if they don't know about it, they don't feel like they have to secure it, but everybody should be aware of it. Now there's been multiple high profile breaches as a direct result of misconfigured, SAS places like Marriott and racket 10. State of Colorado State of Washington. The list goes on and on. I think it gets even deeper. So you can think about it in terms of the number of sass apps that users are accessing. But then when you go into a single platform like Salesforce, there could be as many as 50 or 100/3 party applications plugged in to that organization's product production data. And many of those third party apps that are plugged in or done so by users granting OAuth token access to this application, and they're persistent, they don't go away. And so most most organizations have no idea of the ecosystem apps that are plugged into their primary app of Salesforce or in 365, or others, and so inventorying, all those third party apps showing what their scopes and permissions are within your environment, what data they can get access to how many users are using it, the last time it was used, so forth and so on, is another important aspect to SPM. So it's a multi layer problem

15:43
from SS pm to SI systems integrator. And that's what a lot of big companies is Tomic called SI systems integrators. And when I think of systems, I think just I guess, I think the more the is more than the larger systems coming together, but what do you want to focus in on? What about the apps within the system, all of a sudden, the apps are becoming a subset of the system and integrating all on their own nothing to do with the largest systems themselves? I think there are organizations like the Cloud Security Alliance that give suggestions or guidance for some of these gaps aren't there?

16:11
There are, but I think it's still an evolving space. It takes companies like app Omni to do the work of mapping the individual, you know, configuration options and secure security settings in each of these apps to things like compliance frameworks, and best practices for security. And no one has done that up to this point. Right. So it is an app by app by app process. It's really an application security issue, as opposed to an infrastructure security issue, which we've done a fairly good job of covering with cspm tools, or cloud security posture management tools.

16:42

I was once speaking to a leader at the department education years ago who ruined nameless, and they had a lot of legacy systems there. They had a legacy system that wasn't written in C, it was written in B. Class, write this one down and figure what the heck it is. This is just like a case in point of the legacy systems that are out there. I am sure Progressive Insurance has got legacy systems, I am sure that MariaDB got legacy systems. And I'm sure that the DOE and depart of education as well have legacy systems. And so all of a sudden, you got to throw this monkey wrench into the whole works. It's like, well, what are what am I what, how even deal with legacy systems?

17:20
Well, we do have an answer for that, right. So there are applications that we support out of the box where we've done the work to understand them. And we have a, you know, large number of customers that can leverage that functionality. So it makes sense for us to develop it for things that are custom. And that we will never get to from an in house out of the box perspective, we have something called the developer platform, where customers can support any application, SAS or otherwise ingested into the app on the platform, and do the continuous monitoring and drift detection that we do out of the box for the apps we support today. So we can theoretically support any application, pull it into the same environment for continuous monitoring, reporting, alerting, so forth and so on.

18:02
To the skies in Utah at a satellite show, small set show and jammed just couldn't even walk around so many people 1000s of satellites going up in the sky, all kinds of endpoints, and the endpoints and not going to the moon. And the endpoints are, you know, circling around the moon and maybe going to Mars. And so when you think of a start of a race, you know, like the Boston Marathon or swimming, it's all these hundreds of people lined up and and I think of all these hundreds and hundreds of endpoints coming in. And and just managing those, it seems like that has to be a consideration when you have all these different apps, it's almost like the problem is multiplying almost beyond control.

18:43
It is and we'd like to sort of flip the script on how people think about endpoints, right? In the past endpoints have been laptops, servers, mobile devices, right, the actual user endpoint. And that's obviously important to secure. You know, Microsoft's been around for decades, but they haven't fully secured their operating system, right? We'd like to have people think about SaaS applications themselves as the endpoint. Because it doesn't matter where the user is coming from, or what device they're connecting from, they're getting to these applications through a browser. And 100% of that app lives somewhere else in Salesforce has data centers or service. Now as the configuration is abstracted away, or much of it is the the network is abstracted away from the end user. So the only way to protect access to SAS is to secure the SAS app itself, as opposed to the device. So really, you can think of SaaS apps as being endpoints that need to be protected. And the only way to do that is to analyze their configuration and monitor them for drift.

19:43
Where does this fit in with managing the data?

19:47
So configuration impacts data, right? If you look at like Salesforce, there are multiple layers of access control. It starts with profiles of which there can be many. Then you add permission sets to those profiles and there can be n num Over permission sets. And then finally you have something called record level sharing rules, right? So in that one system, you have at least three levels of access control to data. And that, as I mentioned before, one of the things that an SPM, like app Omni can do is calculate definitively, exactly who has access to what data all the way down to the field level inside an object. And then you can set policy that says nobody external to my agency should have access to any of this data classified as PII or Ph I, or whatever it is, that needs to be protected. And you can monitor for that over time. So as as your teams are making changes to the environment, you can ensure that that data doesn't become exposed by mistake, because in most cases, breaches are caused not by malicious actors, but by well intentioned business people and it people that are simply trying to do their jobs and run the business

20:49
on unintended consequences. Indeed, I have driven to Oklahoma from Virginia many times, and we always go through Missouri. I love the license, but to show me state, you know, and so I gotta turn the show me on to us. Oh, focus on old Brandon here. So I guess you've worked with the CMS. And so let's talk about some bragging time here talking about how maybe you helped them with this whole idea that management?

21:12
Well, I give CMS a lot of credit and their seaso for having foresight in this area, and understanding that securing their SaaS applications, their SAS estate is a critical aspect of their risk management, I think we play a role in helping them to establish an authority to operate with these SaaS applications on a continuous basis. And so we started with one or two platforms, we've now expanded to other SaaS applications, they've done a really good job of bringing multiple teams together, because for each of these things, there are different owners. And today, most security organizations and CISOs have no visibility into the configuration of the SAS apps. They're owned by the BU's the HR department, the customer relationship management team, whoever it is. So they don't even have accounts to see what their posture is, from a security perspective. And CMS has done an incredible job bringing those teams together helping them understand the importance of monitoring and analyzing these applications and improving their their posture and NA to

22:12
use the word ATO. And it seems like, let's go back in history. It used to be that the Pope would put an imprimatur on a book and kneel opposite and say, yep, it's good. And then the book could sit there it is okay to read. And, and so when I think of it, it's almost like an imprimatur saying, Okay, you're good. Now, wait a minute, that book can change. I sit on the shelf, there's not not like a book. And maybe that's, that's the whole idea behind he goes, Well, yeah, it's fine. Fine. Now, what about a week from now? What about when new configuration rules come in? And so I'd say to things, maybe have to understand a little bit better in order manager apps, don't you?

22:50

Yes. And we will take the concept a little bit further. And it's very analogous to what dev SEC Ops is in the cspm world, right in the eyes and pas world, our more mature customers have baked app Omni into a software development lifecycle, and SDLC for these major platforms. Some of our customers have multiple instances of a single app like Salesforce, and they have teams of people that do nothing, but code on these platforms and build new custom functionality every day. And the key to SAS security is not catching things in production. That's your last line of defense. The key is to be continuously scanning, all tests, Dev, staging builds, that are being developed before they are pushed into production. And so you can automate the process of scanning, configuration changes as part of a CI CD pipeline, right? software development lifecycle, specifically for SAS. And this type of security scanning can automate that process and speed it up for customers

23:50

in defense of some of the systems administrators, I mean, tell the truth. I'm pretty comfortable with security with Salesforce. Sure, I mean, I'm pretty comfortable. I mean, I've talked to people at Google for years and years and years. And so, but I think it's a mindset here where, you know, they may make a Toyota Land Cruiser and the last 400,000 miles, but I could drive it into a tree. It's still safe. It's still reliable, but I could drive it off a cliff. But wait a minute, that can hold five people and the motors great. And so I think it's a mindset here where you really, you really lulled into thinking well, yeah, I mean, what, what harm could possibly go wrong? Because we're just, we hired a private contractor to connect to our Salesforce data. Whoa, whoa. And it's done in the commercial world, too. And son all the time in the commercial world with all kinds of problems.

24:39

I think people will be shocked at how often when we do a risk assessment or scanning environment, we find internal data exposed to the public Internet. It's very similar to the open s3 bucket problem that we've had for many years in the public cloud computing space where customers simply aren't aware that their data is sitting out there waiting for somebody to come Find it. And the minute that they do, it's gone. There is no attack Kill Chain and SAS if you've misconfigured the application to allow access to data, it's gone the minute someone finds it.

25:09

And what if Brandon opens up something so then Brandon quits, goes to another agency, John Gilroy gets his job handled Brandon did. I mean, he's a great guy, but maybe he left something. And I've left the lights on in the bathroom and in the family room and, and going out to the store or something. So humans, I think this is a level where maybe humans need some don't want human supervision by me assistants in automating some of their responsibilities. How's that for gentle phrase?

25:42

You know, sometimes we do get pushback from the application owners who assure security Oh, nothing to see here, right? It's all perfectly fine. But I can tell you that in the hundreds of risk assessments we've done that is almost never the case. And you can't start to secure an environment unless you have visibility into it. So everything starts with visibility. And the beautiful thing about SSP M and CSDM, is that it's out of band, right?

It's all API, there's no hardware to deploy, there's nothing in line, you can literally be up and running and gaining visibility in your environment in 1530 minutes.

26:15
Okay, I got a survey question for you here. And you got to put your, your sword in the sand here and make a decision. So we're gonna call it multi cloud public cloud, super cloud distributed cloud, cloud native, meta cloud, abstract cloud, Brandon's cloud, the great cloud, but I guess I'm voting for meta cloud. It kind of seems funny like science fictiony. The meta cloud, you know, what term are you voting on here?

26:41
Geez, I guess the metaverse is is ascendant. So I suppose versus ascendant,

26:46
you lower voice from that. ascendant and

26:50
Resistance is futile.

26:52
Yeah. Yeah. Maybe that's what will be who knows? Your company a PP O. M, and I go there.com. I went to your website couple days ago. Are you going to be speaking at any events coming up? Are you participate in any, you know, lectures in the Washington DC area in the future?

27:09
We are going to be attending the Forrester cybersecurity conference in DC. I believe it's November 8, or ninth? Well, that's good. Yep. We just did Blackhat will be at Dreamforce, which is Salesforce is big conference. We always do RSA every year. And we always do the Gartner conferences. And I do want to get one stat in here. And that is Gartner estimates that 95% of all cloud breaches is past SAS are caused by mis configuration.

27:36
Human beings, we talked to these Meski human beings they really no way. Yeah. Yeah. And and if you have a misconfigured system, Salesforce is gonna say, hey, not my job, not my job. It's not It's point, go look in the mirror and find where the problem is. Yeah, misconfiguration, the basic things that that's really hurt, believe a lot of percent. And so you know, a lot of my listeners may not email you. But what they like to do is maybe see you at an event, and then kind of saunter over and have a conversation, a friend of mine has this problem. And that's, that's usually the step by step relationships, how they're built in this time, maybe they get some credibility from podcasts, they watch a video, and they kind of like these, like these guys kind of weaseled their way into the ocean kind of slowly working your way. And so, so maybe someone can meet you at an event and ask them questions that are more pertinent to their specific problem and their agency here.

28:28

Well, I am based in the DC area, so I'd love to meet.

28:31

Great, great, great. Well, we are running out of time here unfortunately. You've been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest Brandon Conley, Chief Revenue Officer at app Omni. Thank you, John.