DEFENSE in DEPTH

HOSTS

DAVID SPARK
Producer
CISO Series

ALLAN ALFORD
Co-Host
Defense In Depth

GUEST

ROHINI KASTURI
Chief Product Officer
Pulse Secure

SEGMENT SPONSORED BY

Pulse Secure

DAVID SPARK
What is the Holy Grail of secure access? There are many options, all of which are being strained by our new work from home model. Are we currently at the max?

ANNOUNCER
You're listening to Defense in Depth.

DAVID
Welcome to Defense in Depth. My name is David Spark. I am the producer of the CISO Series. We're available at cisoseries.com. We're on the subreddit CISO series. You should join us every Friday, if you're not currently doing this, for our weekly CISO Series Video Chats, which happen at 10:00 AM Pacific every Friday. Just go to cisoseries.com. There's a button to join, register for the one that's the upcoming Friday you're listening to this.

Our sponsor for today's episode is Pulse Secure, and I am joined by the way, I was remiss, not mentioning this earlier. I'm joined by my co-host Alan Alford, who is here all the time. I want to talk about our topic today, which is secure access. Why are we waiting this long to talk about this? You, Allan had a post where you mentioned quite an extensive list of deployed technologies that we have used, some historical, some very new. Walk us through the secure access challenge, and how it's so drastically changed.

ALLAN ALFORD
I talked about VPN. I talked about split tunnel VPN. I talked about VDI, and SASE. I talked about EDR, secure management. What I utterly failed to talk about in this post was identity, and access management. Believe me, I paid the price for that in the comments. We'll have a fun bit about that down the road here, as we progress through the show. But at the end of the day, we talk about secure access being not just about end points, but about users as well. We talked about the fact that the modern tech stack you've got to really truly make it as dynamic an experience as you can.

DAVID
To help us get through all of that is our sponsored guest for today. He is the chief products officer at Pulse Secure. It is Rohini Kasturi. Thank you so much for joining us today.

ROHINI KASTURI
Nice to be here, David, and Allan.

ANNOUNCER
What's the issue here?

DAVID
Eli Migdal of Boardish said quote, "When companies don't use a VPN, they will focus their security efforts on the identity, MFA for VDI, and conditional access." You referenced this earlier, Allan. And Petr Spirik of PWC said, "I would not say that VPN is the solution to protect the endpoint. You need to focus your effort to protect at the end point, and the identity of the user". And Harold Walker of Terra Nova Security said quote "Conditional access can be more secure than full VPN access." So I would say in general, there's not a

HOSTS

DAVID SPARK
Producer
CISO Series

ALLAN ALFORD
Co-Host
Defense In Depth

GUEST

ROHINI KASTURI
Chief Product Officer
Pulse Secure

DAVID (CONTINUED)
huge amount of love for VPN, although so many people rely on it, Allan, don't they?

ALLAN
I think so. I think Harold's right, that conditional access can be more secure than full VPN access. I think conditional access has to be based on, once again, identity. I think this is a factor that's come in to play. I'd like Andrew, if you would please to cues from patriotic music, now. I'm going to read my statement to the crowd.

I, Allan Alford being of sound mind and body, do hereby solemnly declare that identity, and access management is crucial to modern security. And is so vital to the security cause in fact that it should be owned by InfoSec, and not by IT. It is the linchpin, and the glue that holds everything together. And is so vital, and so integral that I often forget to mention it because I think of it as breathing.

DAVID
All right. Well, Rohini, Allan really kind of set the stage for the patrioticness of the importance of identity, and access management. Is that a story we need to be telling about secure access, or is it the historical case of put the walls up like we've done in the past?

ROHINI
David, I would say great question, and Allan you're spot on. When it comes to identity and context, they're becoming central to secure access. I think the most important thing here is identity access management, and conditional access is about control plane security. Whereas zero trust is all about data plane security, or session security. So, what I mean by that is, let's say you're accessing applications on the cloud. Let's say you're accessing SaaS applications.

Then what would happen is you are checked, you'll check various items to be processed, like your username, login. You will check the location through multifactor authentication. You'll also check various conditions like what device the user is using, et cetera, to actually grant access to the user. But the end of the day, once that is all done, the data is going over the internet, and that's where the session security becomes important.

This is where the zero trust comes into picture. So zero trust is about session security, because the data is all going encrypted through MTLS. The reason this is important is you have generally three types of applications sitting on the cloud. One is SaaS applications, which already have strong security posture, and they can also enforce a lot of security on the end points, or the browsers, to make sure the session is secured.

These are going to be constituting only 10 to 20 percent of the applications. But there are a lot of other applications enterprises have, which are generally called as private applications, which are applications that are put by the enterprises on the cloud. The other is on premise applications, which are sitting in data centers. In these cases, what happens is the session security becomes super important in addition to identity, and access. Identity, zero class, and VPN are all complimentary to have a relative security posture.

DEFENSE in DEPTH

HOSTS

DAVID SPARK
Producer
CISO Series

ALLAN ALFORD
Co-Host
Defense In Depth

GUEST

ROHINI KASTURI
Chief Product Officer
Pulse Secure

SEGMENT SPONSORED BY

Pulse Secure

ANNOUNCER
Who has a solution?

DAVID
David Lagacé of Lowe's Canada said SASE, by the way, the acronym is S A S E and Allan, what does it stand for?

ALLAN
Oh, I knew you were going to ask me it's secure...

DAVID
Hold it, wait. Rohini, you must know, what does it stand for?

ROHINI
It's secure access service edge.

DAVID
Secure access service edge. Okay, thank you. Hold on. Let me go back to David's quote. Quote, "SASE," that's how it's pronounced, but S A S E, "is a convergence of all of the above." Sort of all these things we've been talking about, "some would say identity is the new perimeter, and screw what hardware you're on. As long as you pass the different gates." And Philip Beyer of Global Payments said, quote, "The most powerful aspect of most SASE solutions is how they shift the mentality from the allow by default, that's block via exclusion lists, to deny by default, which is permit via allow list." So I'm going to go with you Rohini first on this. This seems kind of like your charge here, yes?

ROHINI
Absolutely. Pulse is launching the zero trust offering here, and that is do the direction of SASE. If you look at SASE, SASE talks about the super convergence of secure access, security, and SD-WAN. What Pulse is doing is the hyperconvergence of secure access. Where identity, and context becomes central to managing users, devices, applications, and gateways. That becomes the foundation of SASE.

I also like the fact that in the new world of zero trust, and SASE, what happens is you are always making sure, or verifying various stress, like users, user trust, device trust, application trust, data trust, and infrastructure trust, and last but not the least the session trust. You verify multiple trust postures before you provide every access. That is very important in the new world, because the world is hybrid and multi-cloud. Verifying all the trust brings a lot of security posture, or direction of security posture. This is where the hyperconvergence zero trust strategy that Pulse is embarking on, becomes the foundation for the SASE.

DAVID
All right, I'm jumping over to you, Allan. Allan, this SASE play, what part of it sounds potentially too good to be true, and I'm not specifically talking about Pulse Secure for the matter, but just in terms of, is any of it sort of putting fear in you that its too good to be true, or is it a convergence that you're very excited about?

DEFENSE in DEPTH

HOSTS

DAVID SPARK
Producer
CISO Series

ALLAN ALFORD
Co-Host
Defense In Depth

GUEST

ROHINI KASTURI
Chief Product Officer
Pulse Secure

SEGMENT SPONSORED BY

Pulse Secure®

ALLAN
I think it's a convergence I'm excited about. Honestly, this is one of the more exciting changes to come along in the last several years. If you go back just five years ago when everybody thought NAC/NAP was the way to lobby systems, right? In other words, you want to bring a computer on the network. You run it through NAC/NAP. You make it wait in the lobby, verify it's passed a health check, has the things you want on it, certificates, et cetera. Then you let it on the network for real.

NAC/NAP was a great vision. That's a great thing to want to do, but it was so finicky, and so costly, and so painful to deploy and set up. With SASE you're not only saying, "Hey, I've replaced a lot of basic connectivity type technologies here, but you've even done this whole lobby paradigm." To Rohini's point you're looking at a stack of trusts, right? I'm a huge fan of SASE. I think it's a really good play. I think it ties nicely into EDR, and of course as Philip points out, identity, identity, identity is so key as well.

ANNOUNCER
Can this problem get even more complicated?

DAVID
Tony Chryseliou mentioned that all the techniques you mentioned Allan were necessary, but they vary from country to country based on cost and regulation and quote, he said "The network, and security architects have to be creative to come up with secure solutions that are cost effective for the business units, no matter where they are located. Flexibility is key."

Then Reginald Parris of TWOSENSE.AI said, "As long as security professionals have to deal with the risk of human error, and user experience, these models will be difficult for organizations to adopt, although they should be the future." So Allan, Tony, and Reginald, just talk about like, "Hey, this is all exciting, but the reality of the world makes this difficult to deploy." Yes?

ALLAN
So Tony's right. I worked for a company a while back, I'm not going to name names here, but we made products that happen to do a lot of end user logging, logging of end user activity. We very quickly got into Germany, and Finland, and all of these countries. There was a stack, Japan, like we actually had it stack ranked at that company, what the privacy laws were in terms of like easiest to hardest to deploy and what all hoops you had to jump through, and how difficult it could get.

We had a full awareness of this global impact, right? Anything that touches, and manipulates, and manages user data, endpoint data that much you're going to run into regulatory stuff, you are. That's a totally fair point on Tony's part, but I think it can be overcome. Even at that company, again, we stack ranked it, but it was all attainable. It was all feasible.

As to Reginald's point. I'm not sure which models he was talking about, because we kind of went back, and forth in the thread, and there were quite a few things discussed. I would argue that the newer model proposed, the identity, and access management, plus SASE,

DEFENSE in DEPTH

HOSTS

DAVID SPARK
Producer
CISO Series

ALLAN ALFORD
Co-Host
Defense In Depth

GUEST

ROHINI KASTURI
Chief Product Officer
Pulse Secure

SEGMENT SPONSORED BY

Pulse Secure

ALLAN (CONTINUED)
plus EDR, plus secure management is not only the best modern security, but I think it's also the most user friendly, as well.

It's so important that we as security practitioners always keep the user experience in mind, right? This is something that historically we suck at. Part of what's beautiful about zero trust, and SASE is there's a dynamic underpinning that just says, "Hey, we're doing the work behind the scenes. We'll let you get to what you need to get to or, or not. If you're not supposed to, and it'll all be this nice seamless UI kind of experience" That's what you're looking for. So, I think the modern stack really is more user friendly than the legacy stuff. Again, back to NAC/NAP what a nightmare that was.

DAVID
I'm going to throw the same to you, Rohini, in that what Tony and Reginald talk about is that they're excited about this, and it should be the future as Reginald said, but there are other limitations that aren't allowing this future to happen. What do you think about that?

ROHINI
Allan was spot on and so is Tony here. Allan made an important point, which is that user experience, and time to market, which is addressed through zero trust, and SASE solutions. If you look at the new world of this hybrid digital era, which we are in and right now in which we plan to be in for the next several years to come. There are four important elements, David. One is speed, speed and agility, time to market. How fast can you onboard your customers, your end users, and your partners if you have to provide them access that's one.

The second one is scale. How quickly can you scale if your organization is scaling, how can you meet the demands of scale as an IT infrastructure security organization? The third one is economics. How do you keep the business model simple so that you only pay as you go, and keep the economics very easy to understand from an end customer perspective, and last but not the least security. Because your apps and this data are distributed across clouds. Now you have multiple perimeters to deal with, right?

So how do you reduce your attack surface, while dealing with speed, scale, economics is super critical. Again, this is where zero trust and SASE concepts are right spot on. If you look at Pulse zero trust solution that we're announcing, is just doing like that, which is addressing security on one side, speed scale economics on the other side, to really bring the best to the market.

ANNOUNCER:
How would you handle this situation?

DAVID
Klint Price, CISO at Inland Real Estate said, quote, "For us, it depends on the application stack, and the end point." He went on to describe different scenarios based on personal laptop, versus company laptop, and the sensitivity of the data. Then he says, quote, "I really don't think there is a one size fits all solution unless you have a simple application stack."

DEFENSE in DEPTH

HOSTS

DAVID SPARK
Producer
CISO Series

ALLAN ALFORD
Co-Host
Defense In Depth

GUEST

ROHINI KASTURI
Chief Product Officer
Pulse Secure

SEGMENT SPONSORED BY

Pulse Secure

DAVID (CONTINUED)
Let me just start with you again, Allan, on this is that, does the complication of the application stack throw this whole model into a tizzy.

ALLAN
It can, and I think that his comment about one size fits all, and personal versus company laptop. I think there's factors there as well, that again can influence. I think, and I don't know why we're talking about secure access, and I keep talking about NAC/NAP, which is really sort of a squirrely thing to bring up, but ditch that paradigm go with the modern stack, go with identity, and access management, go with SASE. Look at more the MDM and the MAM model.

If you want to look at how we're supposed to be doing it, going forward, look at mobile device management, mobile application management. Couple that philosophy and that paradigm, mixed that with your SASE and your ADR, and your secure management. You've now got dynamic connectivity. You've now got application, and identity aware trusts in place and established. You've got a dynamicism that allows you to, if you choose go full on BYOD. I think it's viable. I think it's there. I think it's completely doable.

DAVID
What do you think, Rohini, in that maybe with what you've done with Pulse Secure, have you seen more complicated stacks, and also different scenarios like the personal versus company laptop, essentially complicate this matter to make deployments more difficult?

ROHINI
There are three different use cases, David. One is you have users, like end users like us, who are using devices. They could be personal devices, or office devices to access applications. Those applications are data spread across clouds. That is the first use case, which is around end user device access, and user application access. That's one.

The second one is about network devices. Like if you have printers in your office or various network devices. Even they are trying to access applications to send emails, or send notifications, or alerts. That's another type of access. The third type of use cases, really IoT device access. Where IoT devices now want to push data to the cloud, or push data to the cloud applications. That is IoT device access.

If you look at these three challenges from a CIO/CISO perspective, you have users, devices, applications, data, and clouds, okay. Then you have network devices and IoT devices also wanting to access. There are today, there are so many multiple siloed solutions out in the market. That makes it very cumbersome for a CISO to understand the security posture. Makes it impossible to have a holistic view of what is going on in the enterprise.

So, this is where Pulse secures hyperconvergence strategy really comes into picture. They give a single pane of glass to the customers, at the same time have a single dashboard to manage users, devices, applications, networks, and you can manage guest users. You can manage IT administrators, you can manage partners, different types of users.

DEFENSE in DEPTH

HOSTS

DAVID SPARK
Producer
CISO Series

ALLAN ALFORD
Co-Host
Defense In Depth

GUEST

ROHINI KASTURI
Chief Product Officer
Pulse Secure

SEGMENT SPONSORED BY

Pulse Secure

DAVID
I get that. Let me ask, that when you were developing this, you foresaw this very problem that we were just talking about, yes? This is why you tried to develop, they're saying, "Hey, people are going to have this issue. They're going to run into this very problem of having multiple scenarios, complicated stacks. We better try to make this easy for them, yes?"

ROHINI
Absolutely. Absolutely. This is what is resulting in a lot of breaches, David, because you don't have a centralized security posture to manage. It's resulting in breaches.

DAVID
I'm just going to throw in what, and I don't know how you feel Allan, but my other co-host, he has an issue with the single pane of glass thing that everybody is marketing. The problem is if everyone's got a single pane of glass, what you got is a hundred single panes of glass. Which is kind of the issue that you guys are running into. Which by the way, I'm sure the model you have is good. But the core principle is, I think what's important here is, you're trying to get ahead of this problem that everyone knows they're going to run into, yes, Rohini?

ROHINI
Absolutely. David. Absolutely.

DAVID
All right. So Allan, do you necessarily need a single pane of glass in this situation, or you just need to know that, "Hey, I'm addressing all these issues."

ALLAN
I like it, that I can address the IoT, the network devices, the networks, the users, the identities, the end points. I like that I can address all of that in one way. That's a huge win for me. Back to a single pane of glass. That phrase always sticks in my craw as well, but I love the idea that you can manage, and manipulate these things in the same way, right? That ultimately what's being said here, is I can treat a device the same way I treat a user, and have that same level of access control, and trusts, and established, et cetera. That's elegant. That needs to be happening.

DAVID
Excellent point. Well, that's a good place for us to stop this conversation, and review our favorite quotes from the episode. I'm going to start with you, Allan, what was your favorite quote that I read out here, and why?

ALLAN
I'm going with Petr Spirik over at PWC who said, "I could not say the VPN is the solution to protect the endpoint. You need to focus your effort to protect at the end point, and the identity of the user." He was the one who best called out like, "Hey, what are you doing? You can't do this without identity. I think he was spot on.

DEFENSE in DEPTH

HOSTS

DAVID SPARK
Producer
CISO Series

ALLAN ALFORD
Co-Host
Defense In Depth

GUEST

ROHINI KASTURI
Chief Product Officer
Pulse Secure

SEGMENT SPONSORED BY

Pulse Secure®

DAVID
Rohini, your favorite quote and why?

ROHINI
My favorite quote, David, is a Philip from Global Payments. The reason is I think the most important thing in this world of hybrid digital data is reducing your attack surface. The reducing attack surface starts with zero trust, and SASE, which means that you reduce the access policy to such an area you have any granular access policy, or a secure access policy to say, which user through what device has access to what application.

For example, you might want to say David, if he comes through his personal device is only allowed access to two applications or Allan, he is coming through a corporate device is allowed to access these five applications. That granular policy, and application access policy makes the attack surface very low, and it can prevent any breaches, et cetera. So, that's why I love his quote.

DAVID
Well, that brings us to the conclusion of today's episode. I want to thank you Rohini. By the way, I let you have the last word. So hold tight for just a moment. Obviously thank Pulse Secure for sponsoring this very episode and some of our past episodes as well. By the way, just in general, Rohini your wisdom on this topic is very clear. So, we greatly appreciate you bringing it in. Also bringing in sort of a sensibility, and basic understanding to really what is this new way of dealing with secure access with SASE. So thank you very much. Allan, your last comments.

ALLAN
This was fun. This one was a good one. I'm a big fan of SASE. I'm a big fan of zero trust. I'm a big fan of identity, and access management being integral to the stack. I think this is a lovely play you guys have come up with. I'm glad to see what you guys are doing. I'm going to poke around a little, and see if I can arrange a demo or something, but it sounds fun. What you guys have come up with sounds fun.

DAVID
Okay, Rohini. I let you have the last word.

ROHINI
First of all. Thanks David, and Allan for having me. I think Pulse is having the right vision, which is around hyperconvergence of secure access to really solve all the challenges that we talked about. Users, devices, applications, infrastructure, gateways, et cetera. You solved all those three use cases that we talked about, and our strategies send us through an as a service platform. At the same time, have customers only one client to access various types of use cases.

Pulse has a very powerful vision, and a strategy, and we're super excited to be announcing our Pulse zero trust offering today.

DEFENSE in DEPTH

HOSTS

DAVID SPARK
Producer
CISO Series

ALLAN ALFORD
Co-Host
Defense In Depth

GUEST

ROHINI KASTURI
Chief Product Officer
Pulse Secure

SEGMENT SPONSORED BY

Pulse Secure®

DAVID
I believe you announced it two days ago. It's two days old as of the drop of this very podcast episode. I'm assuming if they want to know more go to pulsesecure.com, yes?

ROHINI
Absolutely. David.

DAVID
All right.

ROHINI
Puslesecure.net.

DAVID
Pulsesecure.net. I'm sorry. pulsesecure.net. Don't go to pulsesecure.com. Nobody wants to go there. Thank you very much. Rohini. Thank you very much, Allan. Thank you our audience, as I always say, as you can see our contributions that we get from you are critical for this show even existing. Thank you as always for participating and listening to Defense in Depth.

ANNOUNCER
We've reached the end of Defense in Depth. Make sure to subscribe so you don't miss yet another hot topic in cyber security. This show thrives on your contributions. Please write a review, leave a comment on LinkedIn, or on our site, cisoseries.com where you'll also see plenty of ways to participate, including recording a question, or a comment for the show. If you're interested in sponsoring the podcast, contact David Spark directly at david@cisoseries.com. Thank you for listening to Defense in Depth.