Speaker 1 (00:00):

Podcast confirmed. Welcome to the Official AWS Podcast.

Hawn Nguyen-Loughren (00:08):

Hello, everyone. And welcome back to the Official AWS Podcast. We got some game-changing updates with AWS Verified Access. I'm Hawn Nguyen-Loughren, also known as Han Solo, your friendly neighborhood co-host of the Official AWS Podcast. And I'm joined by Chauvon Doss. Thanks for joining us.

Chauvon Doss (00:25):

Yeah. Thanks, Han Solo. Thanks for having me. Happy to be here and talk more about AVA.

Hawn Nguyen-Loughren (00:30):

Awesome. So, tell us a little bit about yourself and what do you do for Amazon Web Services?

Chauvon Doss (00:36):

Yeah. I'm Chauvon and I'm a product manager in Amazon EC2 AWS Networking Team. I've been here for last four years. I have worked on all the networking products here, such as AWS, IPAM then bring on IP. And for the last two years I've been working on this cool thing, which is now called AVA. It is a security and connectivity product and I'm happy to talk more about it.

Hawn Nguyen-Loughren (01:02):

Super cool. So, again, we're here to discuss AWS verified Access, also known as AVA. It's built on AWS Zero Trust guiding principles. And AWS Verified Access validates each and every application requests before granting access. Verified access removes the need for a VPN, which simplifies the remote connectivity experience for end users, and reduce the management of complexity for IT administrator. So going back to basic, what is AWS Verified Access or AVA?

Chauvon Doss (01:33):

Yeah. Thanks, Han. I think you gave a good introduction on AWS Verified Access. As you said, it allows our customers to give secure access to their corporate applications on AWS, to their end users, right? So, let me say, what is a corporate application? Corporate application is a application that is developed by customers engineering team using AWS resources and hosted on AWS. For example, it can be your corporate directory, where you go and look for your employees or your colleagues' email address, phone numbers and other things. Or it can be an internal hiring tool or a billing tool.

(02:09):

So, these are corporate applications and they're used by employees and staffs and contractors. And, this product gives secure access without using a VPN. And the IT administrator can set up policies. They can say that, "Hey, Bob can have access to this financial application, whenever Bob is using a compliant device." Or, "All my employees can have access to this IT help desk application. And what Verified Access does is that it evaluates whenever Bob or your employees tries to log into those application. It evaluates the policies and, if allowed, they go into the application. The cool thing about this one is that it doesn't use a VPN. So mostly you need to go into a VPN and then access your application. It doesn't need a VPN, and that means that you can work from anywhere. You just need your internet connectivity and a laptop. That's all.

Hawn Nguyen-Loughren (03:00):

Wow, that's really interesting because I used to work for a financial institution and we definitely always had two VPN in and having to have that connectivity. So, that's very interesting that we have this product. So what is exactly the purpose of this product?

Chauvon Doss (03:16):

Yeah. Our purpose here in AWS is to help customers to connect to their application in whichever way they prefer. So, this is actually the third generation of our connectivity product. In the first generation, what happens is that either the employee or staff has to be in the corporate network. So, you are sitting inside the office building. Or you VPN into your corporate network. And then we have these products like side-to-side VPNs DX, which connects your corporate network to AWS. So these are our first generation of product.

(03:48):

Then some customers said that, "Hey, can I just directly VPN into my AWS network without going into my corporate network?" So then we came up with a second generation, which is client VPN, which is quite popular these days. It is one of the largest VPNs in the market. But then some customers said that, "Hey, why do I even need to do VPN? Can I just log into my applications and I can set per application granular policies, where I can say that, 'Hey, this employee can access this application and that employee can access the other application,'?" So, essentially, these set of customers were looking for something what we now call a Zero Trust, which is something simpler for the users but has more security controls for the IT administrator. And that's when we start developing AWS Verified Access. So, it gives you that Zero Trust access without VPNs into your corporate application.

Hawn Nguyen-Loughren (04:36):

Cool. And Zero Trust environment is what I've seen more and more popular. And, security is the highest priority and it is the forefront of all that we do. So, in terms of network access, all right, what is Zero Trust Network access?

Chauvon Doss (04:52):

Yeah. That's a great question, because Zero Trust can carry a lot of meaning for a lot of different folks. And, at AWS what Zero Trust means is that you shouldn't just decide access based on network location. You should use non-networking signals to decide access. So, if you use multiple signals for example, you use network-based controls, you also use non-networking based controls. So, that's how you'll get a better security posture. So let me give you some simple examples, right? In a traditional network, what happens is, whenever you log into the network, so you have broad access to all your applications or all your resources. But, Zero Trust says that combined non-networking signals. So what happens is when you try to log in, Zero Trust will use your corporate identity, like a "Chauvon is Chauvon. He works for EC2 team for AWS, for Amazon, and his role is product manager. So that's why he should have access to this application."

(05:52):

It'll also use my device post chip. So, for example, Chauvon is using a good device, compliant device, with malware, XON antivirus on, those kind of things. And you can even further use more and more signals, like geolocation and whatnot. But the idea is to combine more and more signals, and that's how you'll get a better security posture. Let's say somebody has access to one of the servers, and just

because they have access, they can't go to your sensitive corporate application, because either device check will fail or your identity won't match. So, that's how it gives you a better protection.

(06:26):

The other thing is that Zero Trust emphasizes on continuous verification. So let's say I go into an application and moments later I log out. I want to go again to the same application. Zero Trust will reverify your device, your credentials, and if anything has changed in between, it will deny access to the application. So, essentially, Zero Trust gives you, because of continuous verification and because of non-networking signals, it helps you to reach a higher security posture. But, at the same time, it doesn't use any VPNs. So, for the end user, it's actually much more simpler. So, it's a win-win situation. End users don't need to use VPN, and security administrators, they get more security controls.

Hawn Nguyen-Loughren (07:07):

Yeah. I really appreciate the enhanced and evolving stronger security posture that this is providing. So, how has Zero Trust been implemented until now?

Chauvon Doss (07:18):

Yeah. Zero Trust is not a new concept and it has been there. You can say that even 10 years back when I was working for different employer. So I used to log into my applications and I couldn't belong to some applications. So, essentially they were implementing the Zero Trust, but in a different way. And how it is implemented today without AVA is slightly complex. So, let me give you some examples. Now, you will have a set of VPN and networking policies, which is operated by the networking team. So, they will decide who can have access to the network. But then, the security administrator will work with the application developers, so your application developers will integrate your applications with your corporate identity provider. That's where the corporate identity is a place where you'll keep records, like who is shown? What is his role? And all those things. So, application is integrated with that.

(08:08):

And then you implement controls that, "This set of employees can use this application," but these are all done by your application developers whose core job is to write applications. And they're working with your IT administrator or security administrator to do these things, which are not part of the core job. Then there comes a third set of policies, which is, which device is actually healthy? And IT team will write policies that, "Hey, this device is healthy. So then only allow this device to log into your corporate network or VPN," Right? Three set of policies at three different places, and if you need to add one new application or if you want to make a policy change, so it can take days or it can take even weeks because you have to coordinate with different teams. That's where AVA comes in and it simplifies this process.

Hawn Nguyen-Loughren (08:53):

Gotcha. And once upon a time when I was a developer, I had to put all of these controls in, and you just don't know if you did it. So, it really great that we're enabling the developers and making it more secure. So, now how does the verified access simplify all of this?

Chauvon Doss (09:10):

Yeah. So, what Verified Access does is that it integrates with your corporate identity provider. It also integrates with your device management provider, and then brings those signals at one single place. And you can use it as a front door for all your applications. So let's say you have hundreds of applications. So your front door for hundreds of application. And you don't have to write point policies for each

application. Now, add AVA, you can write a single set of policies for all your applications. And, as a IT administrator you don't have to go and coordinate efforts with developers or device management team. So, at one single place you write all your policies related to network access, related to corporate identity and device posture. And that's how it simplifies. We have some customers who have told us that, "Hey, they can onboard applications and enable access within five minutes." So, you shrink the process down from weeks to just five minutes.

Hawn Nguyen-Loughren (10:04):

That is awesome. Definitely with that onboarding and making sure the application secured is a win-win for sure. So, how does Verified Access get identity and device data?

Chauvon Doss (10:16):

Yeah. What we have done with AVA is that we have built an open ecosystem. So, we rely on standard-based methods. And we integrate with actually third-party providers or who are our partners to get this identity and device postures. For example, customers can still continue to use their existing corporate identity provider or device management provider. We will integrate with them and we will bring those signals for the customers to write policy. The advantage is that you don't have to migrate to a different provider. You can continue to use an existing provider and still onboard with Zero Trust architecture.

Hawn Nguyen-Loughren (10:56):

Gotcha. And I just want to double-click a little bit more on some of the features of Verified Access. So, what are some of those enhanced capabilities that we're providing?

Chauvon Doss (11:05):

Yeah. Sure. So, we already talked about fine-grain policies for Zero Trust. So, you can write a single policy for a single application, and each policy can be different for each application. So, essentially, you are trying to build a micro perimeter, what we call as micro perimeter for each application. Each application will have its own set of policies and who can access and under what conditions. That's the number one feature. The other feature is that actually we have integrated with VAF, or web application firewall. So Zero Trust gives you that micro control.

(11:43):

But, you still want to have traditional perimeter-based control. You want to have L7 inspection for cross-size scripting or bots and other things. So, that's where VAF integration comes in. And you can combine traditional network perimeter controls with Zero Trust controls and get a better security posture. Then, the other thing we do is that we log each and every access attempt. Whether success or denied, we log it, and this itself is quite valuable for our customers, because now they get complete visibility. Who is accessing their application? When they're accessing, whether they were allowed or denied. And we put all this log information in a standard schema. And using this schema, actually our partners can consume the logs and give richer security insights for our customers. For example, they can triangulate all this information and they can say that, "Hey, this particular user is trying to access the application from two separate location at the same time." So it might be a signal and they can do the further investigation.

Hawn Nguyen-Loughren (12:43):

Gotcha. And, yeah. Really important that we enable some of those SQL injection cross-site scripting and et cetera to make sure that we do protect the application. So, awesome that we have that ingrained [inaudible 00:12:55] integrated with it. So, a last question I have for you are, what are the next steps?

Chauvon Doss (13:00):

Yeah. So it's already live. We are already GA, and you can go to our AWS management consoles, search for "Verified Access," and it gives you easy steps to start using it. And also, we came up with the workshop, so you can go to your favorite search engine. Just type "AWS Verified Access workshop," and it'll take you to the link where we have certain steps on how to get started. and it gives you more insights how to use the product.

Hawn Nguyen-Loughren (13:27):

Awesome. I'm definitely going to check this out. So, Chauvon, thank you so much for joining us on the podcast today.

Chauvon Doss (13:33):

Yeah. Thanks for having me.

Hawn Nguyen-Loughren (13:34):

Awesome. And as always, we love to get your feedback. There's a link in the show notes to "Submit feedback." And until next time, keep on building.