Intel

SD-WAN Security and SASE

CORPORATE PARTICIPANTS

Lilian Veras
Moderator

Charuhas Ghatge
Nuage Networks – Product Marketing

PRESENTATION

Lilian Veras

Welcome, everyone, to the Intel Network Builders webinar program. Thank you for taking the time to join us today for our presentation titled SD-WAN Security and SASE.

Before we get started, I want to point out some of the features of the BrightTALK tool that may improve your experience. There's a Questions tab below your viewer. I encourage our live audience to please ask questions at any time. Our presenters will hold answering them until the end of the presentation. Intel Network Builders Webinar Series takes place live twice a month, so check the channel to see what's upcoming and access our growing library of recorded content. In addition to the resources you see here from our partners, we also offer a comprehensive NFV and SDN training program through Intel Network Builders University. You can find the link to this program in the Attachments tab, as well as a link to the Intel Network Builders Newsletter.

Finally, at the end of the presentation, please take the time to provide feedback using the Rating tab. We value your thoughts and we'll use the information to improve our future webinars.

Today, we're pleased to welcome Charuhas Ghatge from Nuage Networks. Charuhas Ghatge is a Senior Product and Solutions Marketing Manager at Nuage Networks and is responsible for promoting SD-WAN, SDN, and security products and solutions for service providers and enterprises. Charuhas has held a number of engineering, product management, and marketing roles during his 30 years in the networking industry, primarily at Cisco, and then at Dell and Juniper Networks prior to Nuage Networks. He was educated at the University of Oklahoma with a master's degree in computer science.

Welcome, Charuhas, and thank you for taking the time to join us today. Over to you.

Charuhas Ghatge

Thank you so much. I appreciate Lilian for the kind introduction. Hello everybody, my name is, again, Charuhas Ghatge and welcome to you all. Good morning, good afternoon, good evening, wherever you are, and thank you for allowing me to give you one hour of your time.

Today we are going to be talking about SD-WAN Security and SASE, S-A-S-E, and we will be discussing, the agenda is as follows. We will be primarily dividing our presentation in two sections. One is talking about security for SD-WAN, the basics of what security for SD-WAN consists of. And the second one is the more important topic of secured access service edge. This is what we call SASE, which is the current most important consideration for SD-WAN security and the networking convergence thereof. Things like we will be talking about what is SASE, or why is it needed, and what are the components of SASE, or what are the functionalities that consist of SASE or construct a SASE solution. We'll also discuss deployment considerations and a SASE implementation as done by Nuage Networks.

In terms of the security for SD-WAN, of course we will be talking about the basic branch security requirements, what's the security paradigm, the way Nuage Networks is implementing the prevent, detection, and response paradigm, and what are the basic security functions like IDS, IPS, web filtering, monitoring, etc. And then we will also talk about the customer verticals and its use cases.

So, let's begin with what is the need for SD-WAN, and also how's SD-WAN security different? What are the driving factors for SD-WAN and SD-WAN security?

If you look on the left-hand side, this is what the network's consisted of prior to SD-WAN. You have a hub-and-spoke architecture, branch-DC primary connectivity, and hence, and since every packet used to go through the centralized DC location, you had the centralized security. Enter SD-WAN on the right-hand side and you have all, from the mobile, to So-Ho, to Office, to factories, all the branch networks connecting to the public cloud internet, private cloud, and even service provider hosted services connections going through to the SD-WAN network. In other words, basically, a transformation has occurred, as all of us know, from the centralized DC model to a decentralized cloud model, and this is the primary driving factor for the SD-WAN, and SD-WAN security because by doing this cloud access, using internet as one of your primary transports, we are actually exposing a lot of security vulnerabilities and we need to protect the traffic. In one word, basically, the security parameter has vastly extended, been extended all the way from your branches to the public cloud. And this has a lot of ramifications that we will be discussing.

So, let’s look at branch security first. As I mentioned in my earlier agenda, that we will be talking about SD-WAN security in detail before moving onto SASE. The approach that Nuage has taken for branch security is these three paradigms. One is prevention, detection, and response. First, you need to secure the local internet breakout access. One thing that SD-WAN has allowed is the internet breakout. In other words, you can directly go to the internet from the branch without backhauling your traffic into the data center. That is one of the primary driving factors or architectural considerations of SD-WAN.

Now, why did we do that? The reason being very simple. For the access to the cloud from the branch, you don't want your traffic to be backhauling to the data center. That introduces delay, as well as jitter, and that's not ideal for the time-sensitive traffic, like video. So, we need to make sure that we are allowing the time-sensitive traffic to go over the internet, which is largely unprotected. We want to--SD-WAN security must secure the traffic and that is exactly what we are doing in terms of prevention, and it is done via, typically, firewall, URL filtering, and IDS/IPS, the intrusion detection system, as well as the intrusion prevention system. What does that do, is prevents lateral malware spread from the branch to the DC. As I mentioned, because of the SD-WAN, we are allowing the traffic to go from your branches all the way to the cloud, and of course, to the DC as well. The security perimeter has largely been extended, so you want to make sure that if the malware enters your network from the cloud, or anywhere else, you don't want to have that spreading into your enterprise network.

Detection. The detection is, basically, you can't manage anything which you can't see, so you need to have real-time visibility and monitoring for all the traffic entering and leaving the branch and emerging threats. And response, what good is it that you have detected some vulnerability and you're not able to respond in real-time? So, one of the paradigms is to respond, or try to respond, in near real-time to the threat. You see the threat, you insert some functionality or redirect that particular packet, or the traffic flow to a functionality that can take care of that vulnerability. That is what the response functionality is all about. So, these are the three important paradigms on which the SD-WAN security for Nuage Networks is based on.

Further details about the functional blocks that comprises of this branch edge security is the usual suspects. You need a stateful firewall to protect your branch from outside, restrict your branch user access to corporate network and etc. And second is the application control. You need to do the security per your application base as you need to be able to configure security policies based on your applications. So, the policies are based on business policies, such as I need to allow the video traffic from the data center to the branches, but I need to block the users sitting at the branch from using Facebook for example. So, you need to have an application level control and application level security control.

Next is the URL/web filtering. Basically, you need to block the malware, you need to be blocking some illegal content access, etc, and also this is needed for regulatory compliances. A lot of the web/cloud customers require the enterprises to have this compliance so they know that their traffic, their data, is safe. And of course, the URL/web filtering also consists of the whitelist and blacklist. Blacklisting meaning you block certain websites. Whitelisting, obviously, you want to allow the access to and from those things.

Threat prevention, IDP, antivirus, and of course, the real-time security analytics and monitoring. As I mentioned, this is a very critical portion, the monitoring, of any security product or solution, because you cannot control what you cannot see.

Again, the same, the prevent, detect, as well as the response functionalities, explained in a little more detail, and divided by the functionalities we already talked about. Again, in prevention, you have the IDS, web/URL filtering, and also application control. In terms of detect, you have the policies based on the network security analytics. In other words, you can set policies based on applications. You can set based on users to/from the user, and also IP addresses, etc. In response, you first look at the real-time analysis and based on that, you can do some dynamic service insertion for doing threat mitigation.

Going in a little bit detail on each of those functionalities, such as the L3, L3-L4, and also the lower L7 application control and SaaS application controls. So, how do we do this? So, L7, L4, stateful distributed firewall is, basically, limit your branch access to and from internet using stateful L3-L4, level three-level four, security, packet level security, and our implementation is validated by third-party PCI-DSS requirements, and we do log all of the ACL actions for compliance and auditing.

L7 Application Control restricts branch users, as I mentioned before, user access to specific applications using the L7 DPI. The DPI meaning deep packet inspection. We currently-- the slide is slightly dated in terms-- We currently support more than 24 application signatures, so any applications out there, we recognize them, and you can set filters based on them. You can view or monitor which applications are trying to access-- the users are trying to access. And we also do logging of this information, of course, so that you can monitor, as well as analyze, at a later stage.

We have a very nice feature where all the supported SaaS services have been templatized, and you can actually look at the-- you don't have to configure these applications manually yourself, such as Office 365, WebEx, Salesforce, the most common SaaS applications.

The next feature is the web/URL filtering, and in terms of the use cases, as I mentioned before, it is used to restrict your access to some branches to the cloud services to only the whitelisted websites. There are blacklisted websites which have been blocked, and the key features of these URL/web filtering functionalities are these. They are DNS-based, meaning we are monitoring each DNS query to the websites. The content category is based on filtering, block malware, adult content, and certain streaming media. And we support more than 180 website categories. Mind you, these are not 180 websites. These are websites categories, and the categories are thousands. I mean, the websites are thousands. We also subscribe to the predefined website categories, and that list is daily updated, so we don't hard code those. It's a dynamic list that we subscribe to, and the government agencies and security specialists, whoever, add to these categories. We are real-time with that and we are subscribed to that already.

As I mentioned before, filtering is based on the custom website list as well, and we do logging of the blocks, websites categories, so you know which websites have been used, or which websites have been using to hack your branches.

Threat prevention, IDP, basically, IDS/IPS, the classic security functions, which is detection and block of known threats from outside of the branch, as well as from the inside. On one of the servers that we have seen a few years ago, there are as many threats from inside as well as from the outside. This is typically for-- in our function, it’s typically targeted for medium-to-small sites with about 100-meg connectivity. The key features of this functionality are embedded security in this. This is important to note. Our NSG, which is the CPE device in our SD-WAN implementation, which is the CPE device that resides in your branches, is the one which is capable of providing all security functionalities. This is the embedded security functionalities. All these functionalities of SD-WAN security that we are discussing in this section of the presentation are implemented in our NSG, basically our CPE. They're embedded, we don't need any external security functions or security gateways, etc. This IPS/IDS uses signatures from known attacks to match the traffic that passes through the NRG in order to prevent attacks. The signatures are divided into different groups containing relevant signatures. And the IPS, obviously, the policies are defined centrally by our SD-WAN GUI, which is the same graphical user interface that defines the policies, not the security policies, the SD-WAN policies, from your console. So, there is only one console that defines SD-WAN policies as well as SD-WAN security policies.

Just to give you a flavor of how the flow visibility looks like, this is one of the captures from our SD-WAN security portal. This is showing a traffic flow to and from, and how much traffic is flowing, what kind of traffic is flowing based on the color. As you can see here, from Branch A to Branch B it's an orange, and then DC to a partner site is in green, etc. So, you can see the heatmap of different traffics going through based on the pair.

And the network security monitoring is for compliance and auditing. Not only it's for management for your day-to-day, but you can use this data, and these reports, for your compliance or audit, for external audit and compliance agencies, if you have them. Basically, it is used for, as I mentioned, network forensics and troubleshooting on your day-to-day basis when you want to look how the traffic is flowing, what are the security threats. You can do the threat hunting, you can filter them, etc, etc.

And this is one of the captures from how you can actually do the security monitoring. You can set thresholds, threshold-based alerts, and also security event reports based on near real-time flows and ACL analytics. You can set the filters based on port scan detection, port sweep detection, ACL denies, TCP, very deep packet level security.

The last important paradigm of-- and probably in my view one of the most important ones is the automated response. What good is it that you are monitoring the security threats and you're not able to respond or mitigate or correct the security risk. Here in the automated response, we can do multiple things. As soon as a threat occurs, and this is predefined in your policies that a particular security threat occurs, then you want a particular action to be taken. The actions can be you want to start a sniffer capture like functionality to deep dive into it. You want to run a specialized security function to take care of that security. In our case, we typically, or our customers typically have a specialized security function from a security vendor and you want to invoke that functionality for this particular threat. So, the packet capture that you did can be redirected, or even the real-time traffic can be redirected to this functionality within our CPE that is running a security VNF, the virtual network function, from a security vendor, our security partner.

So, here is what happens. You define that for this particular advanced threat, I want this traffic flow to be redirected until that is corrected to the VNF of a security vendor, and by the way, that VNF is of course running on your local branch CPE.

So, having looked at all this detailed security functionality, let's look at some of the deployment scenarios of how we can do some of the partner ecosystem that we have in terms of the security functionality. So, Nuage Security, we provide-- First and foremost, we provide the embedded security, which is the basic and most important security functions. For some of the advanced security functions, we partner with our ecosystem of security specialist vendors. On the left-hand side, you can see our SD-WAN architecture, where in the middle of the picture, that's where the WAN transport is. On the left-hand side, you have the data center, the branch, and on the right-hand side, you have the cloud. The cloud is where also we can do cloud security vendor integration, that our virtual NSG or virtual CPE is implemented in the cloud. That acts as a cloud gateway, but also acts as a gateway to the-- for example, one of the partners that we have is Zscaler. So, it acts as a gateway to the Zscaler cloud. So, as I mentioned in the previous slide, the traffic, which is vulnerable, or you defined you need to be looked at in detail, or you need some security functionality implemented, then you can send this to the Zscaler.

So, on the CPE, we have the third-party VNFs, that the NSG is also a host to a bunch of VNFs, and as of today, we host a few of the security vendors such as Zscaler VNFs.

And to wrap this up for our SD-WAN security, just to mention what are the customer use cases, and how are customers using our SD-WAN security and why are they using it?

So, let's look at a healthcare. One of the SD-WAN's many verticals is healthcare, where you have a distributed healthcare system, a large hospital system, which has multiple branches, multiple clinics, and even some of the doctors or technicians can, at their home, have the capability to log into the data. So, in other words, the security perimeters vastly enlarge. In this scenario, you need to identify the malware activity at the branch site. For example, a doctor's site or even a doctor's office, and I mean a doctor's home, and based on our embedded network traffic analytics. Our financial and banking vertical, typically, a user walks in a branch, the agent, he or she, is helping the guest user, the guest user has his or her own iPhone, it's going to use something else, so it needs a guest user Wi-Fi access, as well as the information that he or she wants to access from his or her bank. So, how do you segregate the traffic? How do you do some-- and that's where the URL filtering and the firewall comes in the picture. From the managed service providers, which are our main customers, Nuage Network customers, who are the-- We propagate our SD-WAN solution through managed service providers, so they need to obviously-- they provide security to the end customers, as well as they need to protect their own network from vulnerabilities.

The value-added security services from SD-WAN, our SD-WAN, which is the Nuage embedded security capabilities, allow this service provider to provide security functions as well as to protect their own network.

With that, we have exactly come to the halfway mark of my presentation, and we would be talking now the advanced topic of secured access service edge, the SASE, which is the latest buzzword in the WAN industry, and rightfully so, as you will see in the presentation further down.

So, for those of you who are new to SASE, we will be discussing the need of why is SASE needed. What is the need? What does it do? How is it done, especially how Nuage Networks implements SASE, provides SASE functionality? And if you are an end customer, you obviously want to know the deployment configuration. When should I deploy it? How should I deploy it? And of course, who you want to choose, what are the vendor selection criteria, what are the important things that you need to look at?

So, the need for the new architecture in terms of security. And security, we have seen this in the prior slide, which is on the left-hand side you see the typical hub-and-spoke connectivity, you connect to a data center, and your data center was responsible to go to the cloud. Now, enter SD-WAN, you have turned that model upside down and instead of hub and spoke, you have a mesh functionality where you can access the cloud not only from a data center, but from the branch directly, and why do we do that? The cloud transformation that has occurred, and many enterprises are obviously accessing many of these cloud applications, SaaS applications. Not only that, but in many of our customers, what we observed is the branch, their branches are not just dumb branches. They are smart branches. What I mean by that is they themselves offer cloud functionalities, or they are the cloud providers themselves, cloud application providers, so their end customer can directly go not just to their corporate headquarters but go to a particular branch. So, there is any-to-any traffic. This creates the complexity in terms of managing the networking in the first place and, hence, network security secondarily. As I mentioned, the reason for doing this is the cloudification of the enterprise IT.

So, what is SASE? So, over the last few years, especially the last five years, we have seen the proliferation of SD-WAN. The network has been growing. The branch networks are becoming more important in terms of not just dumb branches, but intelligent branches. So, a big transformation has occurred where all the functionalities that were spread out in different devices like your basic security functionalities, bandwidth aggregators, the WAN optimization, CDN, and now coming to SD-WAN, they were all different devices. SD-WAN essentially consolidated all those functionalities into one device.

At the same time, the security industry was proliferating, was growing, and offering different services. Again, at the branch level of course, security level-- at the DC level was occurring before anyway. But there was this indirect clash happening at the branch, whether it is security, or whether it is networking. But if you really ask the users, they wanted all-in-one, SD-WAN consolidated security and networking console in one, in terms of setting the priorities and your policies, networking policies as well as security policies. So, this was happening indirectly and known to our customers.

Gartner very cleverly observed this trend and they came up with a new term called SASE. And the SASE networking-- sorry, let me go back here, yes. And the SASE functionality, as is described in the left-hand side here, the security functions, for example, the CASB, the cloud SWG, the security gateways, the ZTNA, zero trust network access, the FWaaS, the firewall as a service, etc, were all the advanced functionalities that were offered by the security gateways. Those needed to be consolidated in one architecture, and that's where Gartner came up with the term SASE, secured access service edge.

The networking requirement, let's look at some other networking requirements for SASE. You need comprehensive routing capabilities, that is first and foremost a requirement in my view. Although security is equal importance to SASE, in my view, the SD-WAN is the foundation of SASE. I mean, we are doing all this to help provide access to the end user and, of course, then offering security to make a secured access to your transport. So, the basis is the networking requirement, and we need comprehensive routing capabilities. We need full stack of protocols, and support, as well as access and connectivity from anywhere to anywhere. You need to provide L2-L3 mobile WANs, the LTE, 4G-5G, application-aware routing, and traffic setting. Not only you need to provide the routing capability, which is the packet level, but you need to provide application level routing. At the end of the day, your users want an application level performance improvement, and if you have the application-aware routing, that facilitates that, number one. Number two, business-level policies are also set based on application level and not just the user level anymore. Even having WAN support, of course, even though with the proliferation of SD-WAN, MPLS still plays an important role, will continue to play an important role, for mission-critical applications. So, you need to have coexistence of MPLS and SD-WAN.

The multi-cloud and hybrid cloud connectivity. Multi-cloud connectivity is extremely important. You should be able to go directly from your branch to any SaaS applications. Also, from your data center, which is your private data center, you should be able to use your public cloud, so if you have some AWS instances that you are augmenting your database data center with, you should be transparently able to go. Your workload should be able to migrate transparently from your data center onto AWS for example or Azure, and SD-WAN provides that transparency.

Of course, the SD-WAN Service Portal. Service Portal, ideally, should be all-inclusive of not only the networking configurations, but security configurations as well, and in our case, in Nuage case, it has to be multi-tenant because our primary customers are you, the service providers, who in turn provide the functionalities to enterprise customers like you.

The SASE requirements for security and how the vendor should implement, these are our recommendation, our guidelines. The SASE requirements, IPS, as we have seen, IPS, IDS, firewall, real-time security analytics, these are the functionalities that we saw in my first section of the presentation, and these are implemented natively in our CPE. In other words, they are doing it on-prem, on-premises. Some of the other advanced functionalities, SWG, the software gateway, and DNS filtering. ZTNA, zero trust network access. Let me elaborate a little bit on the next couple of these functionalities. The ZTNA's a set of functions that operates on an adaptive trust model. What does this mean? Meaning a trust is never implicit, nothing is trusted, and access is granted only on a need-to-know basis. Least privileged basis defined by a granular policy, and by the way, these are the policies which are, again, defined on the SD-WAN Portal.

CASB, cloud access security broker. CASB is on-prem or it can be cloud-based security policy enforcement. In our case, since we collaborate with Zscaler, it's a cloud based security enforcement point. That is placed between a security service, like an AWS, and the cloud service customers. As I mentioned, we provide this integration with specialized cloud service vendors like Zscaler. Then there is data loss prevention, and firewall-as-a-service. All these functionalities, advanced functionalities, Nuage Networks, we provide via integration with our cloud security vendor integrations.

Going a little bit into the details of SD-WAN security, as well as SASE. One design tenet that Nuage adopted, and we were not only fortunate, but we were ahead of the time, because we did embedded security ahead of the industry. Given the detailed functionality, or security function, embedded security, we designed our security functionality with the tenet that it should be expandable. The service provider, as well as the enterprise customers, shall have the flexibility to incrementally add security functionality, as they evolve their deployment, their network.

So, if you look at the top left corner, number one here, which is the embedded security, we discuss this in detail, that is what you start with. Secondly, number two, you can augment that embedded security with a third-party firewall VNF, as I mentioned previously. What I mean by this is our CPE, which is going NSG, the network-secure gateway, is also a host of multiple VNFs. It has a large CPU and a large capacity to hold many VNFs. Some of the VNFs in this particular case can be security VNFs. So, combine one with two and you have not only a basic security model, but an expanded security model where you have the advanced security taken care of as well. Number three, our MSPs can also do SASE through service chaining. You have number one and number two, plus-- So, the end service provider can access their preferred vendor, security vendor, to offer the security functionality to their end customers.

And number four, this is our Nuage-specific, Nuage-provided SASE platform, and we'll come to a little more detail on that as well in the next few slides. So, what we have is we have our own Nuage Security SASE PoPs that we have deployed strategically, and an end customer can access those PoPs, whichever is the closest PoP to them, and have SASE functionality implemented. Our service provider customers can also provide-- Nuage helps them in creating their own SASE PoPs so they can offer SASE service to their end customers. So, it's really flexible. To summarize, we have detailed, deep embedded security functionality in number one. Number two, we can augment that with third-party VNFs, any vendor that we have tested. Number three, the MSPs, our primary customers can offer the SASE through the cloud security threat, through doing their own service chaining. And number four, exhaustive SASE platform is offered by Nuage via Nuage PoPs, as well as we enable our service providers to create their own PoPs.

So, let's go into some of the deployment considerations. As we have seen over the period of time, any new technology goes through what we call a Gartner Hype Cycle. Typically, if you look in the graph, there's an innovation trigger, a technology is introduced. Soon enough, there is a peak of really inflated hype, you know, expectation. This is what I call the peak of the hype itself. Customers start deploying. They see a trough. Immediately you see a dip in the expectations and disillusionment sets in. As they go through the cycle of deployment to learn more, the vendors learn more, the customers learn more and there is a deployment reality phase that they go through, and then the actual advantages of a technology are realized slowly, surely, and that's the slope of enlightenment, and then the plateau of productivity where the technology is fully deployed and utilized.

Right now, the SASE is at the peak of inflated expectations. For example, the SD-WAN, in this case, is slope of enlightenment where about 35 to 40% of the enterprises are currently using SD-WAN. SASE is definitely going to reach that state. However, SASE, as Gartner has mentioned in their original white paper, that it is not a-- It is not something that is a hardbound solution. It's an architecture, it’s a recommendation, because the vendors like Nuage, some of the security vendors or SD-WAN vendors, are providing solutions based on their expertise, based on the need as per their end customers, as they interpret it. So, some of the recommendations that we, as Nuage, have, are although SASE is an end goal, because of the things that we looked at, why is it needed, or how it is used, etc, but it is not something that you must do today. It has to be done over a period of time.

So, here are the deployment considerations where SD-WAN and cloud security are widely deployed. You can't do a rip and replace SASE deployment because customers have already some security function, security vendors they're using. A complete SASE will be a greenfield environment. You can do that but then you are doing vendor lock-in. You're compromising completeness, you're tying to an architecture, not flexibility. A good SASE solution, on the other hand, should provide flexibility. A highly scalable and feature-rich SD-WAN, as I mentioned, SD-WAN is the foundation of SASE. You need exhaustive security functions within SD-WAN. You need integration with SASE, with cloud security platforms for advanced functionalities, and then this flexibility enables the MSP to create a best-in-class SASE solution for our enterprises.

So, with that, I would like to take a break at this time, if you have any questions.

Lilian Veras

Hi Charuhas, we do have a question here from the audience, if you want to go ahead and answer this one first.

Charuhas Ghatge

Yes.

Lilian Veras

There's a member from the audience asking, what are the key considerations for a SD-WAN SASE vendor from the service provider perspective?

Charuhas Ghatge

Oh, yes, sure. As I mentioned, the main thing is, the service providers are-- If you look at today's SD-WAN deployment, there are two approaches that we typically took, say, three years ago, four years ago, when SD-WAN was new. There were a couple of approaches with DIY, where, as an enterprise, you can do the SD-WAN implementation yourself, or you can subscribe-- just like today, you're subscribing to MPLS, you can subscribe to an SD-WAN-as-a-service. Today, if you look at the number of deployments, only 11% of the deployments are the DIY. In other words, the largest of the enterprises, the Fortune 50 deployments have occurred as DIY, but more than 80% are through the service providers. And hence, SASE also-- we think, in our opinion, SASE is also going to be important from service provider perspective to be offered so that their end customer SASE requirements are satisfied. The most important criteria for the service providers is flexibility. Your SD-WAN has to be feature rich. Your SD-WAN has to be powerful, scalable, and so that you are offering very high bandwidth application-aware routing, the basic IP routing, that can offer the power and performance. Flexibility in terms of securities, it must have the features embedded. It has to have the flexibility to have the VNFs. It has to have the functionality of the SASE itself. The SASE platform needs to be their own PoPs, the vendor's PoP, and the vendor must allow or facilitate the service provider to create their own PoPs. So, the service providers should be able to design their SASE solution with these two or three different choices. So, flexibility, flexibility, flexibility, this is the mantra for this.

Lilian Veras

Thank you.

Charuhas Ghatge

Any further questions?

Lilian Veras

We do have another question here. How do you see the service provider's role in SASE?

Charuhas Ghatge

Yes. Continuing with the first question and answer, I think this-- Whoever's asking the questions, thank you. Service partners clearly, as I mentioned, are clearly playing the big role in terms of SD-WAN service offering today. That deployment paradigm, and also the business paradigm, is going to be extended to SASE. The end users today, the enterprises who are subscribing to the service provider to provide an SD-WAN service, are going to mandate the same service providers to provide the SASE service. So, SASE implementation is becoming of extreme high priority within the service provider community. Service provider communities are approaching vendors like us and asking for the-- I mean, they're deploying, they're testing the functionalities within their own network, and within their own implementation before offering this service. The key criteria again, as I mentioned, right now are the integration with the cloud security providers, integration with the security functionality that the service provider has in-house or within their service provider network itself. Those are the two important criteria or functionalities that are important for them to test so that they can offer SASE functionality.

Lilian Veras

Great, thank you, Charuhas.

Charuhas Ghatge

OK. Are there any further questions?

Lilian Veras

As for now, we do have one more, and this question is, what should the enterprise customer be looking for in a SASE solution from a SP?

Charuhas Ghatge

Yes, that's a great question. So, we talked about what should service providers be looking from the SD-WAN SASE vendor to have this. The most important thing is what should the enterprise customer look at. Now, the enterprise customers are the ones who are of paramount importance in this whole SASE paradigm, because they are the ones whose network is to be secured. Their access to cloud needs to be secured. Their cloud to their data center needs to be secured, etc. So, the most important functionality that an enterprise customer has to be looking for is two criteria. Number one is the networking, which is SD-WAN, and number two, the SD-WAN security, which is the SASE.

In terms of the security, let me go back to this particular slide, which will elaborate more in detail what I mean by that. So, the networking, you have to make sure the SASE provider has this functionality from the networking requirement, most importantly, the comprehensive routing capability. Is the vendor, what kind of pedigree that vendor has, or is it a vendor that just designed their routing capability just for SD-WAN a few years ago, or their routing functions have been embedded in the service provider network for four decades, right? So, very established vendors, the networking vendors, who have the pedigree of their routing code in there for many years is important. The cloud access, the cloud functionality, cloud connectivity is extremely important, and also whether the MPLS, their own MPLS in most cases, they offer the MPLS service themselves, the vendors, so how's that MPLS service important?

So, these three criteria will be important for networking, and of course, from the security perspective, the advanced security, how is that integrated in the SASE solution, or what kind of flexibility do they have by integrating with the state-of-the-art security vendor, is the most important. So, performance from SD-WAN perspective, and flexibility from the security perspective, are the most important criteria in my view.

Lilian Veras

That's great, thank you.

Charuhas Ghatge

Thank you so much. Thank you for the opportunity.

Lilian Veras

Well, Charuhas, thank you so much for sharing such great information with us.

This will conclude our webcast then and thank you for taking the time to join us today. Those of you who attended live, please do not forget to give our team a rating for the live recording so that we may continuously improve the quality of our webinars. Thank you once again, Charuhas.

Charuhas Ghatge

OK, thank you.