DRAFT

Conference Debate Session I:

The Future of secure cloud connectivity

Introduced and chaired by Jason Bloomberg, President & Principal Analyst, Intellyx

Featured Speakers:

Analyst chair: Jason Bloomberg, President & Principal Analyst, Intellyx
Renuka Nadkarni, Chief Product Officer, Aryaka Networks
Prakash Mana, Chief Executive Officer, Cloudbrink
MK Palmore, Director - Office of the CISO, Google Cloud
Srinivas Rao, AVP& Solution Specialist, Tata Communications

Jason Bloomberg, President & Principal Analyst, Intellyx
Good morning, everybody. It's a pleasure to be here. This is my third NetEvents. So it's good to be back. Our session this morning is on the future of secure cloud connectivity and I have a few slides and then we'll get right into our panel. I'm founder of a boutique industry analyst firm called Intellyx. We cover a diverse range of different enterprise IoT topics, including cybersecurity, Cloud Native Computing, but also big data, AI, low code tools, mainframe modernization and variety of other topics. I've also written or Co-written several books, those are my last two books, Low-code for dummies and the agile architecture revolution from 2013. So in terms of our topics, just sort of frame the discussion of secure cloud connectivity. The first topic is, is how the attack surface for the enterprise really any organization is exploding. So all the different points of vulnerability where attackers may be able to break into an organization or achieve their nefarious ends. There are many more of these points of vulnerability as we move to the cloud, as we move to the edge, as the modern technology world expands. So this frames the discussion of secure cloud connectivity, because the cloud represents a vastly expanded attack surface, compared to enterprises, before the cloud where they had their close walls with firewalls. Well, now that that perimeter based mentality is, is no longer sufficient, we have to deal with security in this broader context of cloud, cloud computing and cloud connectivity. So when we talk about secure cloud connectivity, we talk about what does security mean in the cloud? One of the first challenges that enterprises run into is the shared

responsibility model. This basically means that cybersecurity is not entirely the responsibility of the enterprise, but not entirely the responsibility of the cloud provider either. Organizations often make the mistake of assuming the cloud provider, they say they're secure. So that means they provide all of the cybersecurity and organization needs when they move into the cloud. But that's not the way it is right? What the cloud providers do is provide a way for organizations for their customers to configure their security, how they want it to be configured. But it's up to the organization, the cloud customer to do that configuration properly. So on the one hand, there's a certain responsibility that the cloud providers have to provide an environment that is internally secure and configurable. But it's up to the organizations who leverage the cloud to configure that security properly. So that implies to the connectivity part of the story as well, that it has, it's not up to the cloud providers to do everything the customer, the enterprise has to configure that properly as well. Okay, so another part of the cloud story is zero trust story and as your trust story is continuing to evolve. So this is a Forrester term from 2009, it's been around for a while, basically saying that we can't rely upon our perimeter to provide security. We have to treat every endpoint, every individual, every individual laptop or device, server, as untrusted until we can confirm that is appropriately trusted. We understand who is behind those using that technology and what their privileges, what they're entitled to do, we have to understand that every single time they interact. So this is a whole new way of thinking about how to secure any environment where it's not about the perimeter, it's about securing each individual endpoint. Well, this is the story of zero trust evolving as we move to Cloud Native Computing because with Cloud Native Computing we not only think about the identity of human beings interacting with devices, we have to think about every endpoint, including those that aren't necessarily associated with human beings. So they could be endpoints internal to the organization, internal to the cloud native infrastructure that raises the bar on what it means to have zero trust computing. Finally, there's an old saying that if you want to secure a house, you can't just lock the doors, right? You have to lock the windows as well, because the bad guys are smart enough, if the door is locked, they'll try the windows, right? This is the way you need to think about cybersecurity as we advance in a more modern environment. You can't just secure the cloud connectivity, that's not going to be the whole story, you have to secure every layer of what you're doing. You have to secure the network, that's obviously a core part of the cloud connectivity story. You have to secure your infrastructure, you have to secure your data, you have to secure the middleware, that's often the middleware that software that connects things to other things. That's often overlooked when you think about cybersecurity, and then the applications as well. And securing applications is really a question of building secure software in the first place. If you don't do that, it's hard to get security anywhere else. Okay, so let's go ahead and introduce the panel. We start with Renuka, why don't you just briefly introduce yourself and your organization, and we'll get into the questions.

Renuka Nadkarni, Chief Product Officer, Aryaka Networks
Yeah, so I'm Renuka Nadkarni, the Chief Product Officer at Aryaka. I've spent 22 years in security building pretty much every kind of security enforcement product that's out there. Jason, to your point, where we are today is essentially users or anywhere on applications or anywhere. It's not that we don't know what security needs to be enforced. I think the problem we are dealing with is really is how do you make it make security enforceable. I'm very excited to join this panel to talk about where we see the future evolve.

Prakash Mana, Chief Executive Officer, Cloudbrink
Hey, everyone, thank you so much for joining this morning. Prakash Mana, I am co-founder and CEO of Cloudbrink. Cloudbrink is in the business of delivering secure in office experience to modern hybrid

workforce anywhere, everywhere. Been in the security infrastructure networking industry for last two decades and look forward to the panel.

MK Palmore, Director - Office of the CISO, Google Cloud
Good morning, everyone. MK Palmore. I'm a senior leader in the office of the CISO for Google Cloud, longtime security practitioner, also former longtime government practitioner, I'm a retired FBI executive and looking forward to the discussion around the impact on cloud and also tying back into the opening keynote from this morning, so should be a good discussion.

Srinivas Rao, AVP& Solution Specialist, Tata Communications
Hi, this is Srini from Tata Communications. We are a global company carrying about 30% of all internet routes all across the globe being the in the top five all the five continents. Where a digital ecosystem enabler will eraser capabilities for Unified Communications is divan, security, and cloud. So looking forward to the discussion today

Jason Bloomberg, President & Principal Analyst, Intellyx
Very good. So we have quite a high powered panel here. So what are the most pressing issues for our connectivity today? What are the most pressing issues? So who'd like to jump in?

Renuka Nadkarni, Chief Product Officer, Aryaka Networks
Yeah, as I was mentioning, the most pressing issue is really enforcing security. Because users are now not just in the office, they are working from home, they are actually working from airports, coffee shops, and they are going to the applications which could be in the data center that could be hosted in the public cloud, it could be a SaaS application. And as we all know, security is wherever the weakest link is, so how do you secure the connectivity all the way from this user to the applicant, machines which are anywhere? It's not that we don't know that we need access control, we need threat protection there is no dearth of security technologies. How do you make it operationally simple? How do you enforce it, and which is where what area cause vision is to have this connectivity between a user and application no matter where they are, and no matter where they are going by building it into the network fabric. So as we see the future of security, number one is operational simplicity. Number two is integrating networking and security when needed in a hybrid model, where you can enforce all the security policies uniformly, wherever it's required.

MK Palmore, Director - Office of the CISO, Google Cloud
I'll jump in here. So to go back to your original question, I think part of the pressing issue is around organizations understanding that they really need to be thinking differently about how they approach the subject of security, especially and then since the wide scale adoption of cloud now changes the parameters of how organizations need to protect their data and where their data resides. And of course, the issue of connectivity to data depending on where your users or stakeholders are operating them becomes a paramount issue. So organizations I think, need to take a moment and strategically address their cybersecurity needs and in doing so make sure that they understand the impact of their environment through by cloud adoption and the other technologies that they're looking at, and ensuring that they're really taking a look at how these the old school frameworks for cybersecurity still applicable. But there needs to be some adjustment changes to those frameworks as organizations look at how to protect the information where it resides.

Prakash Mana, Chief Executive Officer, Cloudbrink
To add on to what MK and Renuka said, when we look at cloud transformation, we've been on this journey for last 10, 12, 14ish years, right? What has changed significantly in the last couple of years are two things. First one is, Cloud is no longer this one entity where everybody moves, your applications have moved from this data center to somebody else's data center, aka cloud, it has now become such a distributed computing architecture that your application itself is spread across 2000 different edge nodes, locations and stuff like that. So you've got that level of distribution going on. Then second aspect is people previously would go to business facilities to access those applications. Today, people are working in hybrid fashion, as Renuka mentioned, and hybrid fashion itself has changed significantly. You see previously, it was oh, somebody is working at let's say Google Cloud. And when they go home after 5pm, they will go to Sunnyvale, they will go to Santa Clara, one of the local communities here today, hybrid means that a person over the winter is going to be in Switzerland skiing on the hills. During summers, they will be in Utah, doing mountain biking and mountain climbing and stuff like that. So you've got applications moving significantly, you've got users moving significantly. So this mash of connecting all these dots, creates a massive challenge for enterprises when we talk to them.

Jason Bloomberg, President & Principal Analyst, Intellyx
Srini, do you wanna jump in?

Srinivas Rao, AVP& Solution Specialist, Tata Communications
Yeah, I think absolutely. So one is, as you move, I think one thing we need to remember, we all know that network is as strong as the weakest link, we all read that and we all kind of imbibe that into our built up of networks. But today, security, when we say significant networks, network security is as strong as its weakest link today. Therefore, you have to ensure that you're covering the network with associated security at all sorts of endpoints. It could be even the personnel level changes that's happening in the organization, for example, it's not just about our laptops, machines, servers, endpoints and all that, right, it could be 5G device, or it could be an IoT device that is talking directly to the cloud. So you have to then magnify and amplify your security posture to this evolving persona changes. And more importantly, a couple of things is required in this paradigm shift, right? Number one, is your internet fit for business? Like Prakash said, you may have internet from different places, but then you want to have that team's call going, right? You want to have that file data transfer happening, right? So therefore, have your internet fit for business. Second, and most important you go into a single cloud, no offence to my friend in Google. But yeah, it's a multi cloud right because you desire it, you need it, by design of your organization. So therefore, how do you look at that multi cloud visibility and then stability or SLS across multiple (inaudible).

Jason Bloomberg, President & Principal Analyst, Intellyx
So common theme here? For us that we're not just talking about enterprises in the cloud, but we're talking about this much broader landscape that includes edge computing includes remote workers, hybrid work models. So there's a whole lot going on here. So next question would be, how do we actually extend secure cloud networking to end users, especially in these hybrid work scenarios where they're moving around? I don't know if I'm going to be working while I'm on mountain biking. But you get the idea. So how do we actually accomplish that in a secure cloud environment?

Prakash Mana, Chief Executive Officer, Cloudbrink
That's a great question. Srini, and partners talked about, you have cloud first, but you also have internet first, right? So we have to take that into consideration in the modern enterprise world whether we like it or

not, Internet has become the enterprise land network for us. So once we start building certain definitions, once we start thinking that even when people are coming into an enterprise, an enterprise is no different than a giant Starbucks coffee network. So you start building these common security definitions that Renuka you were talking about, around who your users are, what kind of device they are coming from, the network they are coming from, is it a trusted untrusted network, all of that, and the application that they are connected to, once we start tying our security across those four pillars, then all of a sudden, it doesn't make any difference whether a person is coming over a 5G network or the coming over the enterprise LAN, when network and stuff like that. So you make this network so unanimous that any end user can consume the network or consume the application in whichever fashion they want to consume. And they continue to add with an excellent experience to the mic, the team's call and file transfer all of that, and in the best secure fashion possible.

Renuka Nadkarni, Chief Product Officer, Aryaka Networks
Yeah, and I think just to add on to that, I think the expectations of employees are also changing. People, when they had remote access earlier, it typically was if you're sick at home, or you know if you just needed it occasionally. But what COVID did was remote access actually became a de facto. And we heard from a lot of our customers where they had people from call centers or they had people you know, who needed like, we're working on business critical applications. And while they had the connectivity, which was secured with a very nice IPsec client, or SSL VPN, whatever it might be, it was very secure, but it wasn't actually performant. And one of the things that we saw, especially in our business is the rise of these kinds of demands, where people wanted a LAN like experience on LAN. So they said, I want to be at home, and I'm gonna use my IPsec VPN client, but I want the same performance that I would have had if I was online. So Aryaka did this accelerated secure remote access, wherein the remote access user terminates at our local edge, edge, Bob, and from that point onwards, they get almost like LAN like experience, because they use our very high performance network apart there. So very interesting convergence of not just security, but I want security with performance, I want this customer experience to be so easy, that I can actually do my job and I can actually run it just like I was sitting in an office.

MK Palmore, Director - Office of the CISO, Google Cloud
So part of what we understand is we knew when we were discussing this topic is that it would tend to go off in lots of different directions. And so I want to go back to the concept of as we look and think about how we're going to operate in this new world. One of the things that we can be doing as enterprise is making the user experience a lot easier on folks, obviously, the idea of remote work, the hybrid nature of work has really become preeminent in terms of discussing how businesses will allow their stakeholders to operate. So what we need to be concentrating on is the ability to deliver security at the point of entry, right? What you know, looking at the security stack everywhere from where the user engages their hardware and device and then writing that all the way to wherever the business related information resides. And if you think about it in those terms, and we're not we're not saying the word but zero trust, right, we're talking about coupling identity with device information and then having a decision point as to whether or not those two concepts in the telemetry match what they need to match in order to gain access, you begin to get the idea of how it is that you will allow users to get a seamless experience and at the same time maintain business operability so pushing that, you know that that stack down to the device and then thinking about things like you know, what, what browser are you using to operate or gain access to the information? What information or telemetry Can you glean from the device to ensure that it's a device and the user are both coupled and things that you've seen before in action and that particular IP or that particular region. And then there's a of course a time factor to it as well. When you begin to couple

all those things together and make decisions about access to information, you get a much more secure capability. But you also get a user experience that replicates anything that they've seen in a desktop.

Srinivas Rao, AVP& Solution Specialist, Tata Communications
Yeah, absolutely. I think, security, we all know for a reason that security has to be built in, not bolted on, because as much as you try to bolt in security for multiple facets of your journeys that you're taking in network in terms of, let's say SDWAN, and you want everything to go in terms of managed from something like network and security as a SASE option again, right? So yes, you're trying to get into multiple facets of these technology journeys. But then we shouldn't let loose of the fact that see, normally, when you're trying to pivot a new technology, what you like to do, you want to really test it before you trust it, right. So therefore, you have to have that shift left kind of thing happening, not just in DevOps for developing an application, you should also embed that into your, what is known as to my mind, I call it as net sec, DevOps might be a little complicated, but then water soluble, you should write in DevOps, you actually got into sec DevOps, wanting to do net SEC DevOps. So when you put an SDWAN, for example, are you trying to enforce your security at the edge of security on the SDWAN box, or you want to really take it on to SSE and then make it as SASE, which is really network compatible. So therefore, these options is something that (inaudible) and then test it, and then deploy it, and then look at the maturity point of it. So therefore, there is nothing like, you know, one size fits all, for every router, enterprise and organization, for small organizations may be SASE might be quite right fit. But for larger organizations, because it's all hybrid, as we talked about, and it's all multi cloud, so therefore, you have to choose your options very wisely.

Jason Bloomberg, President & Principal Analyst, Intellyx
So you've mentioned a few different things. I know Renuka, you mentioned WANs, Wide Area Networks. Srini, you mentioned SDWAN. So the next question is really getting a bit into the technology, we don't want to get too far in the weeds. But how has cloud connectivity changed? Since the pandemic right before the pandemic we relied upon MPLS? That's essentially a legacy wide area network technology relied upon VPN, virtual private networks, to connect from home, but then all of a sudden, everybody went home. So what sort of what is the next generation of technology? What are organizations implementing to solve all of these problems that we've been discussing?

Renuka Nadkarni, Chief Product Officer, Aryaka Networks
Yeah, so I think that's where I'll go back to my first premise, which is operational simplicity with security enforcement is actually like, really, you know, difficult practical problem to solve. And the way we solve that problem is we essentially have multiple security enforcement point, points actually to MK is comment earlier, security has to be enforced closest to the source. And what that means is you need to have consistent security policies for access control, for data protection for data, like data leakage, prevention, acceleration, even have application security, all kinds of DDoS mitigation, because when you have a presence, you can actually be compromised at many points. And Jason, that was your one of your slides. So now, the problem statement is how do you enforce these different kinds of technologies consistently, and in a hybrid fashion? And it's not an easy problem to solve, but it's not something that is actually very difficult. I would disagree with one of Srini's comments that it's applicable only to small enterprises, it's actually a bigger problem for large enterprises, for precisely the reason that they have a broader footprint, and they are going to multiple different places. And I'll just go down the technical path for a second, right? When you say I want to enforce security, what does it mean. it means that you have to do SSL certificate distribution, because you're probably gonna have to open up the stuff and really look at the packets and look at the traffic for attacks. That's a non-trivial challenge. The way we solved it at Aryaka is

we have a distributed data plane which is could be on the customer drivers could be to your point at a client at a user. And it is all managed by the centralized control plane. So all the consistent security policies are actually created in one place. And then we actually make the determination of where are you doing the decryption? Is it going to happen in the cloud? Is it going to happen locally is the user or is at a device. So I feel like we need to evolve it further. And like I said, making it work in a practical way with you know operations. on simplicity is what makes or breaks the security posture in my opinion.

Prakash Mana, Chief Executive Officer, Cloudbrink
Building on to your point that I couldn't agree more around operational simplicity, security enforcement, what we see when we talk to global CIOs goes back to the original point of distributed applications across multiple cloud distributed users as well. When we look at the post COVID world, going back to your question, think this level of distributed nature of enterprise that we are facing, it's quite challenging, if not humanly impossible to solve. What we are seeing is IT budgets are not growing it we all understand the current economic conditions and stuff like that. So the future in terms of the enterprise consumption around security infrastructure is all moving towards SAS, what I meant is that we can no longer rely on an enterprise IT admin to be managing gateways here gateways, the future is that you consume the entire network, all security, all applications, just as if you consume any application, nobody is deploying Microsoft SMTP servers and all of those things, we just consume office through an Outlook email through Office 365, for G Suite and stuff like that. So in future, infrastructure and security will be consumed in the same way that gateways, all of that management, all of that will disappear, you just simply connect, a AI driven platform should be able to identify which network you should be part of and stuff like that. So that's number one. Number two, is when we talk about security everybody loves the term perimeter less, when you start digging deep into perimeter. Last, what it means is that, oh, my perimeter has moved from data center into the cloud, that's not perimeter, less, you are just extended the perimeter of your security from data center into the cloud. I don't think there is a way to get around perimeter less. But there is one thing that Renuka touched on that I want to connect back is that when you go all the way to end user, this is where data is being curated and consumed. So if there is a way for us to bring security knowledge from data center to the cloud, but bring all the way down to the end user, that's when we can say we have gotten as close to Perimeter last as possible. Then the last point I want to make is around the whole SSL security, all of that, I think we continue to work really hard around this term, zero trust. And obviously, we are all supportive of the zero trust arm. But we should also learn something from dark network. The beauty of dark network is the reason we don't hear dark network getting hacked. And all of that is the dark network is not even visible. So you don't even know what you should be hacking. So there is a way for us to bring dark network into enterprises, so that moving forward enterprises, when they publish their applications, the (inaudible) publishing applications to public Internet, their public, they're creating their own dark networks through which only their constituents can get access to those services. So tying all of these things together, that's what we're doing here at Cloudbrink, little plug in here is with Cloudbrink, you just download our app, the moment you download that app, your device becomes intelligent, call it personalized SD, when it becomes a deny all firewall, and everything that you do from there on is dark networks principles, zero trust levels of security.

Srinivas Rao, AVP& Solution Specialist, Tata Communications
So I think particularly since you said Jason, so what happens now from hybrid state back to maybe two offices that we are working or something like that. So I mean, this paradigm shift, how many times we can really handle is there a fix once for all kinds of stuff, right? We need to understand one thing, most of the enterprises during the COVID time or otherwise suffer from one thing, which is lack of IT skills or

understanding of the cloud, for example, you mentioned, something like whose job it is of the cloud is, you know, the service providers and in the cloud is customers. But then the interpretation becomes so difficult when you are deploying an application where it has got some critical data, for example. So therefore, you really look up to someone who is a real good advisory for you to circumvent that sort of a grey issue, so to speak, right from that emanate from the cloud journey. Second, and most important thing is governance of data. Did all the people adopted, you know, cloud during the COVID time? The answer is Not because, you know, look at banks, for example, did they go on to the cloud? No, they couldn't. Because there are a lot of customers and a lot of banking customers when I was talking to them. They said, Okay, tell me what other banks are doing. So that means what you're not able to take a call based on your security posture on your, you know, governance limitations, right. So that is when a lot of cloud solutions have come in, as a, you know, like a break, fix kind of a solution for them. That's where they adopted something like, what's your desktops and, you know, Thin Client kind of applications and all that. Now, we are back into the Geni. So whichever way you adopt whether you go for full cloud, or you continue to remain hybrid, or whatever most important thing is data in all its facets, whether it is addressed in motion, or it is in use, let us try to have a conscious call of protecting the data that is very important.

MK Palmore, Director - Office of the CISO, Google Cloud
Yeah, I just want to tie it off on a comment around the shared responsibility model, which has been mentioned a couple of times here, we've taken a bit of a different approach at Google Cloud, we believe that the shared responsibility model has actually evolved into something we're calling shared fate. And it's this idea that cloud service provider actually needs to make a significant investment in security on behalf of itself and the customer. In such a way that it's a partnership in terms of how it is that you then ultimately present yourself to the world. And because the cloud service provider, we can no longer just simply rely on these bifurcated understanding where your responsibility ends. And where the responsibility of the cloud service provider picks up at the end of the day, breach in any particular environment is a negative for any entity that has data that resides in that environment. And so we just believe that there's more of a significant skin in the game, if you will, the cloud service providers need to recognize and then subsequently invest in and it's the really the differentiator of security in the approach to security. I think that that will enable organizations to make decisions about where they want to put their workloads and that assumes we all understand that cloud adoption. You know we saw through the pandemic the rates of cloud adoption increased exponentially over time and I think we're we will continue to see more of that, as organizations understand more robustly how it is that they maintain the sense of resiliency that we need today in business operations, that really you can only get through a combination of cloud adoption and of course, understanding what security parameters need to be instituted after the fact.

Jason Bloomberg, President & Principal Analyst, Intellyx
Okay, let's go right to the Q&A.

Antony Savvas, IT Europa , IoT Now & Vanilla Plus
Anthony Savas from the UK, IT Europa, IoT Now & Vanilla Plus. I was quite interested about this concept was mentioned by Prakash I think about looking at network connectivity is like as a software as a service. I'm quite concerned by that because I've seen research saying there's 17,000 vendors of SASE in North America alone, and only a handful actually secure the data for their customers. So if people are consuming this as a software as a service, where's the security going to be? Because people automatically assume that if they use Microsoft 365, for example, their data is secured, but it isn't. It's up to them to secure it as a Software as a Service. So what does the panel have to say about that?

Prakash Mana, Chief Executive Officer, Cloudbrink
That's a great question, and that's where we go back to the principles of zero trust and that dark network that I talked about. As MK mentioned it's in the best interest of a cloud provider, whether it's office 365, or (inaudible), however, to secure your data. But I think you're right, in that enterprises cannot rely on just that level of security. Right? And that's where we need to find ways to make sure that when I have my office 365 Run, what benefit are we getting by publishing your office 365 to public Internet, where all your end users can get to it but then a bad actor or a malicious user can also get to your office 365? Do you really need to publish those applications to internet and that's where tying zero trust with the dark network principles those level of securities plays a critical role, which is I'm only going to publish These enterprise services within my user base, I'm not going to publish those services outside my enterprise boundaries, does that answer the question?

Antony Savvas, IT Europa
Not entirely, no, because the whole idea of the cloud is that it's supposed to be easy to use, and everyone can actually share data and use and benefit from it. If you start restricting the availability of it, it just stops the functionality.

Prakash Mana, Chief Executive Officer, Cloudbrink
I don't know if I agree with that. 100%. The reason is when we at least when we talk to enterprises, today, enterprises have gone in a mode where any end user is subsequently accessing multiple applications. Yes, of course, Microsoft claims that, hey, you only reside all that your applications reside in Microsoft, not true people have Ai workloads that they may be running in Google Cloud, at any given time, I may be consuming application that is a data center centric application and my data centers may be sitting in Equinix. So I feel like I have gone on a quote unquote, private cloud journey with Equinix as well. So while I agree with your point that, hey, a cloud should be easy. All of that, when you go down this path of multi cloud, all of a sudden, your complexity increases exponentially. And at that point in time, you do need an infrastructure SAS provider, where as an end user, you know, you don't have to worry about oh, I have to log into this gateway to access this application, or oh, I need to go there to access that application. Now, you should be able to, you should know that, hey, once I'm in a particular infrastructure, then all of these applications are accessible to me.

Jason Bloomberg, President & Principal Analyst, Intellyx
So final, final question.

Unknown speaker
Yeah. So I have a question about security. So in the private network context, the concept that is very popular, and I haven't heard any complaints about it, that once you have identified a user with SIM card identification and authentication, which happens automatically, you're secure inside the network. I'm kind of puzzled why that hasn't been even mentioned. And why wouldn't it work more widely, because once you have the identification, it should work with the public cloud as well. So operation simplicity, and effectiveness boat.

Renuka Nadkarni, Chief Product Officer, Aryaka Networks
Yeah, that's actually a great point. In fact, we use the term zero trust one. And what we mean by zero trust one is exactly the principles that you applied in your land for zero trust, which is identify the users and

based on that do access control and you know, all the things that apply to the user, we actually have build, same exact philosophy, where we call it zero trust one, we identify the user. And because we own the network fabric, which also answers the previous question that the other gentleman asked, the most important piece is having control of the pockets and owning the network fabric. Once you own the network fabric, you can apply all these other conditions on top of it. So yes, I didn't mention it explicitly. But that's really where we see the future going. That's where we see. I think Prakash mentioned it as well, which is it's most important to bring the user to the network first. If you own the network fabric, then you can apply zero trust principles, and making sure that you are able to take that traffic or have that network fabric connectivity is actually very important. So was he what he was explaining was when we bring the client side enforcement and connecting that to the network fabric, the combination of two is what gives us a very viable zero trust one or zero trust anywhere, I would say.

Angus Robertson, MC
Thank you Jason and panel - a critical topic.