Daniel Newman: Samantha Madrid. Welcome to The Six Five Summit, 2022. I am super excited to have you here.

Samantha Madrid: Thank you, Daniel. Really excited to be here. Thanks for including me.

Daniel Newman: Yeah, it's really great this year that we were able to put extra emphasis on security. If nothing else over the past two years, the world has become acutely aware of a few big technology topics, supply chain and the impact on semiconductors, just how important the PC is to keeping our businesses running. And if by now they've not seen the light on security and then hardening our enterprises and making sure our data is safe, I don't know that there will ever be a time that they will. What do you think about that?

Samantha Madrid: I think you're 100% right. It's a topic that I have daily with CISOs and CIOs about new architectures, the geopolitical dynamics that are happening, what does this mean? How do I evolve? What do I do? Absolutely spot on.

Daniel Newman: Thank you. I was looking for that validation. That's exactly why I asked you that question. But it is super interesting because this has always been one of those topics, and you and I have talked before, you've come on some of my podcasts in the past and we've had briefings and conversations and we've always kind of talked about, what is it going to take for companies to fully get it? And by the way, it's not always the people you're talking to. I think the technologists do tend to understand it, but it's the budget approvers. It's the board and the governance of when, how bad does it have to get? Because it is that when, if statement. It's not when you're going to get hacked or breached or something's going to go wrong. It's not if, it's when, right?

It's not if, it is when. Sorry, I'm correcting myself in real time. So, you know what I'd love to talk about starting off a little bit, is the cloud. And you talk about all the conversations that you were having, Samantha with the CISOs, with the CIOs, we're seeing this huge migration. Again, cloud is still pretty early days. We're really only at about a third of workloads, not even quite, from the most recent research I've looked at. But we're seeing that migration happen. When you're having these conversations, how are you sort of enabling them to envision security evolving along with the architectures?

Samantha Madrid: Well, I think the operative word that you just said is evolve. And to me evolve an evolution of any architecture of any technology has to start with experience, right? I think where things fall down is we lose sight of the experience that we want our users to have. And so as a CIO, as a CISO, I need to be able to envision, how do I want my business to operate? And from there, what and how do I want my users to be a part of that? And so everything starts with the evolution. And for me, I think where we've fallen down in the past as a technology, as an industry security specifically, is that we lose sight of that. And one of the things that we have at Juniper have been very laser focused on is that of the experience and being experienced first.

And so what that means for security in particular, it means not abandoning where you are today. And I think a lot of times for a lot of customers, the concept of newer architectures, right? Whether it's Zero Trust or SASE means starting from scratch. And I think that is the wrong way to look at it. And back to what you just said, it's the evolution of it. And so for me, I always start with customers, where and how do you want your users to access your data? And I mentioned that we've fallen down here in years past in the security industry.

And you probably recognize the term shadow IT. Shadow IT came to pass because we lost sight of experience. Users in an organization decide they're going to take it upon themselves and they're going to build out the tools that they need. That left tons of holes and discrepancy in policy. And so for me, I always tell and advise customers, what is the experience you want? Step one. Two, don't abandon where you are today to evolve to that utopia. And in wherever you're envisioning your organization to go. And then three, don't assume because a vendor has packaged something nicely and puts a lot of marketing budget behind it, that it's going to meet where you need to go. So I think for me, it's just all about evolution and experience of evolution.

Daniel Newman: Yeah. I like that you mentioned that. And by the way, just thinking back to that shadow IT narrative. It's so true. I mean, my gosh, how did the iPhone become one of the predominant devices in the enterprise and it sort of ended up displacing BlackBerry. The BlackBerry from an enterprise standpoint, met a lot more of what the CIOs and the IT leaders at the time wanted from both the security and the technology standpoint. But the users, we always used to sort of joke. Started off with the CEO coming in like, "Hey, I got this new thing." Slapping it down on the IT person's desk and saying, "Figure out how to make this work with the business," right?

And that was kind of a great example of how new designs and architectures were finding their way into the company, because it was what execs and what people were using, because they enjoyed it more. The experience probably felt more productive. But then again, there were people out there saying, "No one's ever going to type on a touch screen." Oh my gosh, I still remember that. I think there was a CEO that said that at one point, I won't say any names. But let's just say sometimes we pretend to be futurist, but we get it all wrong. So shadow IT has definitely been a great example. By the way it's also had a massive number of security implications Samantha, right?

Samantha Madrid: Yeah, hundreds.

Daniel Newman: We opened so many doors and risks. Because it's not just phones, it's PCs, laptops, people's home computers, all kinds of different devices that get introduced to networks that never were designed to meet policy within an organization's security strategy. So, I think you started kind of alluding to this a little bit, but talk through, you talked a little bit about, at a high level don't kind of throw out the baby with the bath water, right? Don't just blow up what you're doing and say, "Okay, we're going to cloud and we're just..." But kind of, as you go through this, you mentioned that there's three considerations to move to the cloud securely. Kind of, what's that process look like? How do you walk them through to make sure that they balance on-prem cloud and that they make sure that they're able to keep security in place as they do evolve to meet what's going to be expected in the future?

Samantha Madrid: Yeah. So great question. I will encourage everybody to take a step back and realize what are you trying to do? You're trying to identify and secure the data. It all starts with data and it start the second it's accessed. It doesn't matter the architecture that you are evolving to, if you lose sight of those two points. And so from a data standpoint, the cloud just means better access. To put it simply. The reason everybody is leaning into cloud is because it brings the data to your users in the best possible experience. At least that's the goal. And so, access wise, you can't lose sight of all the micro perimeters that you've established in a Zero Trust data center architecture. Which we've spoken about for years as an industry. And so when you kind of evolve to a cloud based architecture, whether it's multi-cloud, it's specific to mobility around SASE, you want to make sure that the data is intact. The integrity of the data remains intact and the access to that data doesn't get compromised.

And I don't mean compromised from an outside entity, I just mean that you are suddenly opening the door to that data that you otherwise had securely had in place. So for me, it's about building the bridge to what you have today in the data center to where you want to go for your mobile users. And that's really what we've been doing at Juniper. We launched last summer Security Director Cloud. And it's been really effective for a lot of our customers and gain a lot of interest from our CISOs and CIOs that I personally have been talking to. In that, it allows for you to manage your Zero Trust architectures and create those micro perimeters around the data and really these centers of data that you have scattered perhaps all over the world.

But then it also evolves it to a mobility based architecture that SASE has the goals of fulfilling, right? So when you have a mobile workforce, you have branch offices, you have locations of your users also globally dispersed, that you are able to bridge those two. The problem that organizations run into is that they bifurcate policy. They eliminate and obstruct their visibility. And the way you eliminate that, the way you maintain complete 360 of your organization, the way you maintain the build and evolve the policies you've already established, is by leveraging the capabilities and all the work that the teams have put into place. And so Security Director Cloud for us has really been that anchor point for customers. So, they've had the Zero Trust architectures, the micro-segmentation based kind of projects in place and then they've been able to extend that to all their mobility users. They're not having to create two separate sets of policies. They're not having to create two separate systems.

Daniel Newman: Yeah. Then that's a pretty sizable challenge. And also, like you said, with so many concurrent migrations taking place, because security is almost like a layer that has to move precisely along the line of all the other architectural changes that go on within an organization. And companies right now are implementing, they're changing network fabrics, they're building EDGE architectures, they're bringing in a massive data. What did I read? Something like the EDGE is a hundred times or some exponential number larger than data center. And so, you said we're going to talk about SASE in a minute, but that's a whole nother area that has to be secured. You've got the migration to next generation networks. You guys do a ton with Telco and that's a big part of the service providers.

They've got upgrades going out consistently and their material, these are large up upgrades with very structural differences from say 4G to 5G. The structure's going to be significantly different. We kind of talk about cloud, but now it's not even just cloud it's multi-clouds. It's multiple clouds that tend to have different requirements, architectures. You've got whether it's a container strategy or you've got certain applications running cloud-native, some running on container, some running on-premises. So all these things add a ton of complexity and security has to able to build policies to manage all these different accesses to the data, which by the way, it can be stored in all these places. Depending on how close the data needs to be to the application, the data can be replicated and duplicated and stored to make sure the applications are working efficiently.

So it creates a ton of complexity. But I want to talk a little bit here, I want to sort of wrap up talking about SASE. Because that's been a big topic. You and I have talked about this in the past. It's still early innings though. It's gaining momentum, it's growing. You're probably having a lot of conversations like, "What do we need to think about when we start going at a SASE architecture?" So answer me that, Samantha. What are the questions that CISOs and CIOs that are getting it right and from what you're seeing, what are the questions they're asking to make sure they're able to take advantage of the power of SASE architecture?

Samantha Madrid: Well, I think the what is, the biggest conversation I'm having is to try and eliminate confusion. Because I think a lot of CISOs are seeing a referenced architecture that they think, "Am I having to start from scratch?" And the short answer is no, you shouldn't. And if that is the recommendation, then I would re-evaluate. Because what it really, is an extension and it should be an extension of what you already have in place. And that's what we have been really guiding our customers. So all of our customers that have SRX firewall, as an example, whether it's containerized, virtual, physical, or now are SASE delivered firewall as a service, all should be able to be managed in the same way. And the only difference between what we're seeing in the kind of early innings of SASE to what is being proposed architecturally, is a delivery change.

Instead of delivering the service on premise or virtual, you're delivering it as a service. So I always ask the question, why does your management have to change? Why does your policy structure have to change? If it's being proposed to you that in order to implement SASE, that you need to have a completely different set of policies, a completely different vendor and a completely different way of architecting, then I question that that is actually going to serve you long term. Because to what we were just talking about with shadow IT at the start, that's just going to open up holes within your network. So we've really been working with our customers on leveraging their existing policies, having a single software stack that can evolve with wherever the data resides and wherever the access may be. If it's from your mobile phone, if it's sitting from a branch office, if it's sitting at the corporate HQ, it's the same. But the thing that's most important in addition to the manageability piece, the second most important thing is efficacy.

I think a lot of times we lose sight as an industry that a compromise is a compromise, right? And it doesn't matter where you're accessing from, if you're not putting in a solution that has the best efficacy in the market for you to protect you, then it's really not going to be very helpful. So most people don't realize that Juniper has been number one in security effectiveness amongst every single firewall and network security vendor in the market for the past three years. And so we couple that with our Security Director cloud, to be able to bridge that transition to SASE and connecting all their investments in Zero Trust data center architectures with their mobility goals has really just been really exciting and really been generating a lot of interest.

Daniel Newman: I'm catching a little bit of a theme here by the way of don't basically re-invent what can be innovated upon, right? You've kind of said that in the beginning when we started. Don't blow up everything you've done and let's talk about how to evolve. And it sounds like with SASE, it's very much the same as that some of the customers that you're dealing with may be being kind of told that, "Hey, in order to make this work, you're going to have to kind of rewrite history," proverbially speaking. And you're basically saying, that's not how it has to be. This can be done in an evolutionary format that can take advantage of what's been done well. And in many cases, organizations have put a lot of time, effort and energy into protecting their current estate and doing so could be gradually implemented, iterated upon and innovated upon in a way that could be less painful as well, right? Less costly, less painful, shorter time horizon. So there could be a lot of benefits.

Samantha Madrid: Absolutely well said. And I would say, one of the things in this approach that we're taking, is we're reducing operational overhead and cost for our customers. Because if you are having to stand up a completely different architecture with a completely different set of technologies, you're having to invest in individuals within your organization that have to learn it. And there's a learning curve associated, there's a cost associated when learning new technology. And so we're eliminating that cost. It's an evolution as we said at the beginning, it's not a start from scratch or an added investment on top of everything else. The other thing I will say is, you have to factor in to the fact that there is going to be mistakes made. And so taking this step wise approach is giving people the chance to evolve at their pace that aligns to their goals. I mean, I say this a lot to my teams and in meetings, we have erasers and pencils. We're going to make some errors. So the way to minimize that error is to start with what you have, evolve it and then build from there.

Daniel Newman: I think that's a great way to end it here, Samantha. I want to say thank you so much for spending some time. I think this migration is going to be challenging. It's going to be also a great opportunity for companies to start to get ahead.

Samantha Madrid: One hundred percent.

Daniel Newman: And again, this is always a race. It's always a race between getting ahead and staying ahead, because those that are trying to get at your data are increasingly sophisticated. And as CIOs, CISOs and leaders, it's going to be more important than ever that you're building an estate of data that can be trusted and protected, because it's not just about the security, it's about the reputation that it can cause for your business. So great conversation, I don't think we can talk about security enough ever. I look forward to having these conversations again with you in the future. We got to say goodbye for now. So thanks for joining me at this year's summit though. We'll see you again soon.

Samantha Madrid: Thank you so much.