Aspire Technology Partners - The Digital Aspirations Business Podcast – Series 1, Episode 3

The Power of Software-Defined Wide Area Network (SD-WAN) for Your Organization
Doug Stevens, Vice President for Managed Services, Aspire Technology Partners
Cody Harris, Director of Digital Architectures, Aspire Technology Partners

Doug Stevens (DS): Hello and welcome to Episode 3 of the Digital Aspirations Podcast Series. My name is Doug Stevens, and I'll be your host. This edition of Digital Aspirations comes to you from my home office. Aspire is following the work-from-home directive. Honestly, I would say, almost 70% to 75% of our workforce works remotely on a regular basis anyway. So, frankly, it's been an easy transition for us. We're very much in a business-as-usual mode, if you could call it that, but we're certainly operating at full capacity while, most importantly, practicing social distancing.

So, I hope all our listeners are safe and well and doing the same. In the meantime, business must continue. We're going to get through this together, I'm sure. Aspire is here to help in any way, but, in the meantime, we're going to keep innovating. And we're sure that we're going to be stronger when everything returns to normal here in, hopefully, just a few weeks.

With that said, our topic today is software-defined WAN or SD-WAN. Joining me is Cody Harris. Cody is the Director of Digital Architectures for Aspire. Welcome, Cody.

Cody Harris (CH): Thank you, Doug.

DS: How are you getting along with the work-from-home mode that we're all finding ourselves in?

CH: Struggling, I would say. In general, to your point, we can certainly get our work done, and we can continue to be effective and provide services and support for our customers, but after taking this role on, I've spent a lot of time doing the opposite of social distancing, by which I mean spending a lot of time with my team, as well as leaders from other teams within Aspire. This change has been difficult for me because now we're apart and we've been social distancing. That having been said, I think the use of

video technologies has, at least, given the appearance that we're interacting with each other in the traditional fashion. So, that has certainly helped.

DS: Yeah. No question. For our listeners, Cody leads our pre-sales engineering and our service delivery teams, specifically around enterprise networking, wireless, and our information security practice areas. To his credit and the credit of his team, despite some of the recent challenges around work from home, he and his team were successfully able to pass the Cisco Masters Enterprise Networking Certification here within the last week or so. Congratulations, Cody, on a job very well done.

CH: Thank you very much. Yeah, we got the official word last night from Cisco at about 11 p.m. So, that was not a surprise to us because our auditor had kind of given us the green light, but it's not official until Cisco lets you know. It was a huge endeavor with a lot of team members involved, including members of my team, and many members from other Aspire teams as well. The process involved four or five months of really dedicated work in order to complete it. Now that it's all done and behind us, it was 100% worth it.

DS: Goodness gracious. Yeah. A huge lift. By the way, that is our fourth Masters. We now have Cisco Masters in Security, Collaboration, Cloud Managed Services, and Enterprise Networking. So, big feather in your cap.

CH: Absolutely.

DS: All right, let's put you on the spot here a little bit. What other interesting tidbits should our listeners know about Cody Harris?

CH: So, I've been with Aspire almost 13 years now. I started off as a delivery engineer focusing primarily on the wireless world and collaboration world, although I certainly dabbled in many other products within the Enterprise Networking portfolio. I moved over to a pre-sales role about five years ago, focusing initially on wireless technologies and enterprise networking technologies; then, in 2018, I moved over to provide free cell support for our account managers selling our managed services offerings. So, that was really awesome for me. A lot of fun. I got to learn a lot of really good things, and work with a lot of really good people. And what I've liked the most about that was my job was to promote Aspire and our capabilities, which is very easy to do when you believe so wholeheartedly in our capabilities, as I do.

In 2019, I moved over and took more of a leadership role and a leadership direction with Aspire. To your point earlier, that role is called Director of Digital Architectures. So, it certainly keeps me busy. I have my fingers and toes in a lot of different things, for sure, but busy is what I like to be. So, outside of that, I live right here in Fair Haven, New Jersey, right here in Central New Jersey, about three miles from the beach. I moved down here in August. I have two young sons - five and eight years old. And that's pretty much my life.

DS: Yeah. That's awesome. Well, we're happy to have you. And I can't think of anybody more suitable to share their experience and perspective, especially around the market and what we're seeing from an SD-WAN perspective. So, thank you for being with us today, and let's jump in. What do you say?

CH: That sounds good.

BUSINESS ADOPTION STRATEGIES AROUND SD-WAN

DS: All right. Last fall I read the latest research from Gartner around SD-WAN. Gartner predicted that by 2024, 60% of enterprises will have implemented SD-WAN, which is up from about 20% in 2019. So, it's real. There's a ton of momentum around SD-WAN. And my question to you is, what are the business strategies that are driving this adoption around SD-WAN?

CH: Yeah, good question. It's no surprise to me that we're seeing this kind of proliferation of SD-WAN and this market movement towards that technology. Some of the business strategies that are driving SD-WAN adoption are application performance. So, no longer are all our applications living on-prem, in some data center somewhere. More and more of our applications are now living in the cloud, let's say, or off-prem. And so, dedicated access to these resources is becoming more and more critical to businesses.

Branch resiliency is another thing we see. We have a lot of customers and a lot of different verticals that have a distributed branch set up. So, maybe they have a headquarters site. Maybe they have some data centers. But in addition to that, they have many small typically similar branch offices. So, the resiliency of those branches, the ability to provide ubiquitous access to these applications and to the critical data for these branch offices is another main driver for some of our customers.

When you think about SD-WAN, another main driver, and this is also one of the standard components or critical components of SD-WAN, is carrier independence and internet circuit flexibility. And what this provides to our customers is the ability to break free of the ball and chain of ISPs. I mean, for years, we

would work with our customers, and we would say, 'Okay. So, you're bringing up a site in Quincy, Illinois. What kind of circuits are we going to be able to get there?" And the typical response would be, "Well, I can only go through Comcast," or "Well, I can only go through Verizon, and they're only offering me this type of circuit." So, the ability to break free from the providers to be able to leverage more commodity broadband internet connections, 5G connections, and more standard connections, rather than dedicated MPLS connections, which can be expensive as well, are also a main driver.

Also, direct internet access at these local sites. In many traditional WAN infrastructures, you would tunnel internet traffic through to your headquarters' environment where you would then have your egress point for your internet. Obviously, leveraging this type of technology eats up critical bandwidth on the WAN. Maybe a few years ago that wasn't such a big deal because all your applications were typically internal and stored or handled internally. Now, though, as we are increasing that load on the WAN with accessing applications and data, we are seeing the need to free that bandwidth up as much as possible for those specific use cases.

Lastly, I would say that traditional WAN infrastructure is difficult to manage. You're very often accessing these devices one-on-one. There is no overlay architecture, or what I call an overarching intelligence, that is able to have visibility into the health and viability of all the links within your WAN and to be able to make intelligent decisions on how that traffic should be routed based on the health of those links. So, I would say those are some of the main drivers that we are seeing, and some of the main reasons our customers are coming to us about the SD-WAN technologies.

DS: Yeah, for sure. I mean, from what I'm hearing, it's all about the applications. We're seeing a migration, or expansion, to the cloud where some apps are in the cloud from the SaaS provider, some are at the head end, and you need to provide that no-touch quality of service and redundant paths at the branch level to be able to provide that quality of service to your users at the remote site. So, definitely business aligned from an SD-WAN perspective.

CH: Absolutely.

THE BUSINESS CHALLENGES SD-WAN TECHNOLOGY SOLVES

DS: Speaking of business, what are some of the business challenges that SD-WAN technology is solving, from your perspective?

CH: Yeah, sure. I mean, you talked to it a second ago. Every customer is going to tell you they have different digital initiatives. We hear this term "digital transformation" a lot. Digital transformation is a drive to leverage these cloud-based applications and machine learning automation. SD-WAN fits perfectly into that bucket. Customers are requiring additional bandwidth or multiple paths to their cloud, or SaaS space applications, or infrastructure-as-a-service applications as well. Customers need agility. Customers want the ability to turn these sites up quickly, to turn these sites up with less management or administrative overhead, and to turn these remote sites up in a similar fashion to other sites. I mean, you want to make sure when you're bringing these sites up that there's going to be some components that are going to be a little bit different, like your IP addresses scheme and hostnames, but you want the look and feel of every one of these branches to be exactly the same. And that's one of the things that SD-WAN can provide.

We talked about local direct internet access. This is another thing that customers are coming to us and requesting that, whatever WAN topology that we are suggesting, and by and large, now, that topology is SD-WAN at this point, it has the ability to prioritize traffic based on policy. So, it's going to be policy driven. And that internet traffic is no longer traversing the WAN.

They want to leverage cheaper links. MPLS links can be expensive, and there's no business out there that isn't looking to reduce costs where it makes sense, and internet links or WAN links are a big piece of where you can see cost savings. So, to leverage commodity broadband internet and/or if you're not looking for savings, maybe you're looking to spend the exact same amount, but you are now increasing overall bandwidth.

Finally, they need to ensure that any user who needs access to data and applications can access it At that time, we're talking about equality of service setup or a policy-based quality of service set up where we have certain applications that are critical to the business and ensuring, through the SD-WAN configuration, that those applications are always available and that we have the bandwidth and data we need in order to leverage them properly.

DS: Yeah, for sure. Going back to the topic of cost reduction, I think, in the early adoption of SD-WAN, there was this notion of, "Hey, if we can reduce the number of MPLS links we have in our network and utilize a cheaper form of transport, we can create a positive ROI". I think what we've learned is that cost is less of a driver around SD-WAN, because it's more business focused, and it's about providing quality of service and ensuring that the users have secure access to those applications, and, from a business continuity perspective, providing the necessary bandwidth and redundant paths to make that resilient. Do you agree with that in what you've seen and the conversations that you've had with clients?

CH: A hundred percent. I mean, I would say that cost savings are always going to be a good selling point, no question, always. That having been said, let's consider the situation, and we have customers that are leveraging MPLS circuits as a primary SD-WAN connection. SD-WAN doesn't necessarily preclude you from using MPLS circuits. In certain situations, that certainly does make sense. So, yeah, I agree. I mean, while I would say a customer could realize cost savings, it's not one of the main benefits that we necessarily discuss with the customer ahead of time. It's more the type of thing that, hopefully, when we go through our ROI calculations or TCO calculations, it does end up with some sort of overall decrease in costs. But if it doesn't, that's okay because cost savings wasn't among the main benefits we were touting when we were pitching the solution to the customer.

CONSIDERATIONS FOR REFRESHING THE WAN EDGE ENVIRONMENT

DS: Right. Yeah, for sure. Okay.

So, the customer's environment. The WAN edge environment is older. They're up for a refresh. They heard a ton about SD-WAN. They know that's the direction to go. What's the right solution? And what are some of the important considerations that our listeners should be looking at when they're thinking about refreshing the WAN Edge?

CH: Any time we talk to a customer about any technology, whether that'd be SD-WAN, or wireless, or collaboration, or WebEx, or security, understanding their business requirements, and initiatives, and the drivers behind the adoption of that technology, is critical. Here at Aspire, we really believe in a solution-based or an outcome-based selling strategy where our intention is not necessarily to push six boxes into the customer environment. That doesn't behoove us. It doesn't behoove the customer. Instead, what we're really looking to do is to turn that IT team from a call center to a profit center; and very often we're doing that through aligning the technology with the overall business initiative.

The first thing I would ask the customer is, 'what are the business drivers behind this? Why are you looking to do this?'

The next consideration I would have would be, 'where are you in your journey to cloud adoption? Do we have a customer that has a couple of applications in the cloud?' Maybe they're leveraging 0365, and salesforce.com, or something like that. We also may have customers that have no cloud presence at all. That's not very common anymore. We do not see that very often. Most customers have some level of cloud presence. But there are some out there that have no level of cloud presence.

And then, finally, some are full-blown all-in on the cloud. The cloud is nothing new. It's been around for quite a few years. So, we do have some customers that have, like I said, gone all-in on cloud adoption. Where those resources reside is very critical to how we're going to design their WAN infrastructure.

Along with that is knowing where the critical apps and workloads reside. Do these critical apps and workloads reside in the cloud? Do they reside in a data center somewhere? Do they reside in a large NDF environment? In a customer's headquarters? That's a critical piece of this. What's the makeup of your IT staff? It's critical that we align the complexity of the solution that we are providing with the capabilities of the IT staff. So, obviously, if the IT staff of our customer is lean and mean, then, we're going to look to an SD-WAN solution that's a little bit easier to administer. Maybe it doesn't have all the bells and whistles and nerd knobs that some of the others do. If they have a sophisticated staff, then that opens up additional offerings that we could provide to the customer.

Branch requirements are going to be critical. How many branch offices do you have? What do those branch environments look like? Are they branches that have a couple of users at each site? Are they branches that have ten, dozens, or hundreds of users? These branch offices are leveraging very bandwidth-intensive applications

And finally, I would say, what does your existing WAN infrastructure comprise of? And we want to know that because it's not necessarily our intention to rip and replace every piece of your infrastructure in order to get you enabled on SD-WAN. It's easier for the customer to reuse some of the devices that they have within the environment if possible. Many of the solutions that we provide to our customers do have the ability to upgrade the software on a hardware platform, so that they can leverage SD-WAN in the future.

So, I would say those are some of the main points, and business initiatives being the most critical. Obviously, the current infrastructure is critical because, look, we want to save costs where possible. So, if we're able to re-leverage hardware, that's really, really good.

I would say there are different customer verticals, and those customer verticals could determine what solution makes the most sense. So, let's say retail, for example, and we could talk about that a little bit, but in retail you're going to have a main headquarters site very likely depending on what type of retail level you are. Maybe you have a very nice headquarters environment in Midtown Manhattan with a lot of slick bells and whistles there, but then your remote sites, 500-600 remote sites across the US, may be kind of stamped-out. So, understanding the vertical, and how that particular vertical leverages

technology and the applications that are critical to that business, are also very important things to consider.

DS: Yeah, for sure. That conversation upfront is tremendously helpful to understand what their initiatives are, what some of the routing capabilities are that they're looking at, and whether all the sites the same, are they cookie cutter, or do they have a voice in the environment, and what are some of the applications that need to be prioritized? All of those help your team identify the appropriate solution. And then, also, understanding from a maturity level where the IT staff is, and are they capable of managing it themselves, and those types of considerations.

CH: Yeah, yeah. I mean, just to expand on that a little bit: we often provide options to the customer. We take all this information. We hash it out internally. We develop solutions for the customer that may include multiple options. For our customers that may have a more lean and mean IT staff, there are management offerings out there that we could include in these options. So, we work with our customers. We really do a good job of understanding their requirements. We really listen. I mean, I know that sounds very simplified, but that's ultimately what it comes down to. We listen to the customer, we understand their needs, and we provide a solution that best fits those needs.

DS: Yeah, for sure. And that's what we've been built on.

SECURING SD-WAN AT REMOTE SITES

DS: All right. One thing we haven't talked about here, and it's one of the most important aspects of any SD-WAN deployment from my perspective, and that is security, right?

CH: Sure.

DS: What are your recommendations around addressing security at the remote sites?

CH: Security is a very interesting component of this. Everybody agrees that security is probably the most critical component of determining the best fit for an SD-WAN solution. There are a few things you really must look at.

I would say number one is you're going to look for an SD-WAN solution that has embedded firewalls. The reason being is because, obviously, you want to reduce latency. The whole purpose of this is quick access to resources. You want to reduce latency as much as possible; therefore, leveraging an SD-WAN

solution that is baked into a firewalling solution, a next-gen firewall solution, is important. I wouldn't say it's critical, but I would say it's very, very important. You're going to want to lean towards that way.

Another reason is you're going to reduce the device footprint that you have. So, obviously, the fewer devices that you have within the environment, as long as they provide the same functionality, less devices means less footprint, less overall cost, less power consumption, so on and so forth.

Lastly, there would be providing a single pane of glass for visibility or security within the environment. Cisco has this saying that the internet is now the WAN. And that's why this is so critical because the first thing you think of when you think of internet is the Wild West, the absolute Wild West. And we said before that there are customers out there that are leveraging MPLS circuits to affect SD-WAN. But, by and large, the customers are going to want to leverage standard internet circuits to do so. So, it's important that you have a single pane of glass for visibility and troubleshooting to understand the health of the environment, to understand any sort of security issues that could potentially be popping up.

Along with that, we would also consider, or I should say, tell our customers to consider that you need a comprehensive suite of security tools to secure these technologies. Traditionally, you would just have a firewall at your edge that would protect you and prevent those unauthorized users from getting in, and attacking the environment, and getting access to resources you're not supposed to be getting access to. That's the way we used to do it.

Now, we have a way more comprehensive security strategy, and that security strategy must include next-gen firewalling. So, not just leveraging the old-school firewalls, but leveraging next-gen firewalls in order to better — how should I put this--to better firewall that traffic. Leveraging technology such as IDs and IPS in order to be alerted when there is an anomaly that happens, so that you can act quickly and resolve it if necessary.

Endpoint security. Make sure that all your endpoints are properly secured will be critical to this.

Web security. Make sure that you're providing security both on your cloud access, the access to your cloud resources, as well as URL filtering. Ensure that users can't access websites that are known bad websites. And if they do, and let's be honest, a lot of times, a query for a malicious website isn't necessarily going to be known by the user. A piece of malware will sit on the device, and it'll look like it's a web query, but it's actually some sort of nefarious attempt to access resources. So, that's going to be critical as well.

Encryption. One of the beauties of SD-WAN is that all this traffic is being encrypted over the internet, and that's not necessarily the case in MPLS. So, that's a main differentiator here. We are encrypting all that traffic and decrypting it on the other end. So, if it is intercepted, it cannot be decrypted and viewed.

Finally, leveraging segmentation: ensuring that you have the proper segmentation, that resources are locked down and only able to be accessed by particular users, and that users within different groups that don't need access to each other are also locked down.

So, those are some of the things that I would consider from a security perspective. The last thing I would say is that you should consider leveraging some sort of SIM tool to provide contextualization and correlation of these security events because, let's be honest, none of us are up 24x7 staring at our IPS sensor. It's not going to happen. You may have customers that have dedicated resources, and they're looking at those things on a 9:00 to 5:00 basis or something like that. Typically, they're going to be splitting their time between that and other endeavors, but leveraging that SIM tool right to ingest those security feeds to understand what's going on comprehensively in the environment and to contextualize and correlate the different events, and to understand what's a true positive and what's a false positive, will certainly go a long way in better securing your SD-WAN.

DS: Now, you're talking about what's near and dear to my heart. So, thank you for bringing that up.

CH: You know, I'm there for you, Doug.

DS: Yeah, shameless plug, as I say. But there's a lot to chew on there. And I think the good news out of all of this is that a lot of the controls that you talked about there, more and more of them are being integrated directly into the SD-WAN appliances and the hardware solutions that are being deployed today. So, from a complexity and a footprint perspective, I mean, that's a huge advantage. And the other thing that I would say is a lot of this can be achieved with cloud-based security solutions as well wherever possible. And again, just thinking about it from the clients' perspective, not everybody's got an army of people to be able to deploy all these security controls and to be able to manage it all.

So, leveraging cloud where possible and providing integrated solutions that are easier to manage is important for us. And again, a shameless plug, Aspire has very robust managed services that can offer this solution as an SD-WAN-as-a-service. So, being able to combine the hardware implementation and the SD-WAN deployment itself, bring in the circuits to the local remote offices, and provide that redundancy, and then, the third piece, being able to manage it on a 24/7 basis, so that it takes all of that

operational aspect off the plate for customers if they don't have the resources to do it. We can help fill those gaps. And that's part of what we do on a daily basis as well.

CH: Absolutely, yeah. So, you touched on cloud apps. So, you're absolutely right, and I would say that, at Aspire, we are chomping at the bit to get more and more access to cloud-based security products. They're a no-brainer. As long as they work then the beauty of it is that we are not necessarily having a device. Let's take some examples. Maybe identity management. Identity management on-prem is affected by having some sort of an appliance that you are configuring, staging, adding to the customer environment, testing, and making sure it works. Going forward, the customer may or may not be upgrading it. I mean, we all know how that is. If it's working, then a lot of customers don't necessarily touch it, but there's obviously security risk there. There are a lot of patches, and security patches, and vulnerabilities that are fixed on a regular basis.

So, the beauty of cloud is (A), that the resources are already there on the internet, in the cloud. You're just setting it up and doing the configuration component. The management of that is being completed by the vendor that is providing it. No longer are we performing updates. The updates are being performed automatically. And then, also, access of that piece. So, the beauty, one of the really nice points of the cloud, is it doesn't make a difference if we're here in our home office in Fair Haven, as we are, or if we are invited to go on a trip to the Bahamas. No matter where we are, we can get access to those cloud resources without leveraging VPN and other technologies that we used to need. So, yeah, I agree with you wholeheartedly. I think, at Aspire, and my team, we want more cloud security offerings. We think they make a lot of sense for our customers.

DS: No question. Honestly, we could talk about security and cloud security specifically for a whole podcast. But, unfortunately, that's all the time that we have today. So, Cody, I want to thank you for being with us and sharing your perspective. I really appreciate the experience and the know-how that you, not only help our teams with, but also help our customers with all the perspective that you provide.

I'll say to the listeners, if you like the discussion that you heard today and you want to hear more, by all means please go to our website, aspiretransforms.com, and listen to some of the other podcasts. Thank you for listening. We'll see you next time on Digital Aspirations. I'm your host, Doug Stevens. Bye for now.

Outro: Digital Aspirations is brought to you by Aspire Technology Partners, a premier technology solutions and services provider designing, implementing, delivering, and managing digital infrastructure and IoT solutions to enable transformational business outcomes, creating more agile and efficient IT

environments that deliver differentiated customer experiences for your organization. To learn more about Aspire Technology Partners, visit aspiretransforms.com or email us at podcast@aspiretransforms.com

Aspire Technology Partners is a Cisco Gold Certified Partner engrained in solution pillars that set us apart as a true Cisco solutions provider. We are committed to the continuous improvement of expertise and skillsets around Cisco initiatives that enable us to help and guide customers in the adoption and management of technology architectures designed to transform their organization. We hold Cisco Master Specializations in Collaboration, Security, Cloud & Managed Services, and Networking and is one of only 25 partners in the US to receive the Cisco Advanced Customer Experience Specialization.