uberknowledge

Rahul Kashyap, President and CEO, and Rudolph Araujo, VP of Marketing, of Awake Security

Protecting the New Network

Rahul and Rudolph describe Awake's approach to network security and explain the only way to earn credibility in the market is to be honest with your customers. They admit CISOs would love to see one vendor provide that single pane of glass but the fragmented nature of the industry prevents it. In an effort to balance the lack of diversity in cybersecurity, Rahul encourages every executive to mentor.

01:52 Network security has not really evolved.
03:57 The new network: cloud, data center, IoT.
05:33 Have to build a partnership with your customer. It's not just about a product sale anymore.
07:16 As we learn about it, we automate it.
10:03 We have to make security more and more mainstream. Security cannot be something that only the elite can do.
10:43 Attackers are equal opportunity offenders.
11:39 There are so many good problems out there, but execution is key.
12:48 The reality is cybersecurity is a very fragmented industry.
15:12 Distinguishing yourself as a vendor is not about marketing or your AI, it's about solving operational challenges and showing value.
17:59 If you want to earn credibility in the market, be honest with your customers because that's what they really care about.
19:56 Education should be for everybody.
20:48 We are not educating children about cybersecurity early enough.

22:10 Give back and mentor. Change the landscape of cybersecurity one young person at a time.

Ashwin Krishnan: [00:00:53] Welcome to another episode of the UberKnowledge podcast. Today, I'm actually in the offices of a really interesting company called Awake Security. And with me, I have Rahul and Rudolph. I'll let them introduce themselves and explain what they do for Awake.

Rahul Kashyap: [00:01:11] Hi. I'm Rahul Kashyap. I'm the President and CEO of Awake. I've been in cybersecurity for nearly two decades, and I'm super excited to be part of this amazing team.

Rudolph Araujo: [00:01:24] I'm Rudolph Araujo. Kind of similar story to Rahul, I've been in security for a couple of decades now. I'm the VP of Marketing here but focused on a bunch of things. Typical startup life.

Ashwin Krishnan: [00:01:38] So Rudolph, you've been here longer than Rahul, right. Can you talk about, from your perspective, what was Awake's call to action. Why did you even join Awake and what are you guys about?

[00:01:52] Sure. You know, one of the things that we've seen over the years is network security has not really evolved. I mean, we think about the way IDS engines were from pretty much the late 90s, Rahul, in fact, founded one of the companies that was an early IDS vendor. And that's still very prevalent in many, many organizations today, and they're hard to maintain, they're noisy, there have been a lot of challenges. So one of the big inspirations was the network has a lot of good data but it hasn't been tapped. If tapped well, especially now with some of the advances with data science and machine learning and things like that, there is a lot of opportunity to both provide a detection solution that detects the latest and greatest of threats but also the support of the investigative and threat-hunting work flows that more and more security teams are looking for today.

Ashwin Krishnan: [00:02:46] Got it. So, Rahul, from your perspective, you've been in this company for seven months?

Rahul Kashyap: [00:02:51] Yes.

Ashwin Krishnan: [00:02:52] And based on what Rudolph is saying, you've obviously been in the valley many, many times. So, why Awake?

Rahul Kashyap: [00:02:58] Yeah, good question. I started my career doing IDS and I built two IDS products early on. Then I got to McAfee, and it was a very successful IPS product. And then I got into endpoint security and did a bunch of products and technologies there as well.

[00:03:19] And I'm now back to the network. It was almost like a homecoming for me. But besides all that, the reason why I think Awake is very uniquely positioned in the industry is because the threat landscape has changed dramatically. And as Rudy just mentioned, most of the technologies which are there in the market are just not catered to tackle that, right. You could produce too many false positives, almost becoming irrelevant or not very useful for a SOC analyst, or you just don't have the capacity to process that amount of data. So now, in this world, what I call the new network, you're talking about cloud, data center, IoT. There are several aspects of the new network which you have to think about when you build or architect a solution, and you just can't have all of these isolated. All of these combine and create a new threat for your organization. So we're looking at that in a very broad spectrum, and we believe that what we are building is not just catering to the needs of the current threat landscape but also is expandable as it evolves. We are building a flexible architecture to tackle that problem.

Ashwin Krishnan: [00:04:37] I know last time when I was here Rudolph, you mentioned, which stuck in my head, typical buying behavior, expected buying behavior from a vendor standpoint. You go all in with your sales force, you get this big deal, and then you rest easy until the renewal time, then it’s all hands on deck saying, are we going to get the renewal or not. You do something very different in terms of how to go beyond that very myopic, not very customer-centric thinking, and be there throughout the journey, through the entire year, and not have these peaks and ebbs of when you really want to extract dollars. Talk a little bit about that.

Rudolph Araujo: [00:05:18] Yeah. You know, one of the advantages we have at Awake is we brought together a bunch of people that have been security practitioners, so fortunately or unfortunately, we've lived on the other side of it and seen the impact of it.

[00:05:33] To get to your question specifically, I think this notion that you can deploy a product and it's going to magically solve everything, is just not valid anymore. I don't know, maybe it was never valid, but the reality of it is we believe in this product as a service; a kind of experience that customers deserve. And we view it as a partnership with the customer because we can't proclaim to have all of the answers. So, for instance, we've got customers that have very, very unique requirements. They'll say, this particular part of our network we really care about more because this is where our executive sits or this is where our PCI card data sits. And we won't know that ahead of time, but by partnering with them, we can then tailor our detections, tailor our technology to focus on that. So, that's an example of where we can partner with customers and really help them achieve their security goals and achieve their business goals, which in a way is more important. So that's a little bit of how we view the model. And I think the security industry in general is coming to this realization. I think more and more, especially with the newer companies but even some of the older companies, now you're starting to see this trend that it's not just a product sale anymore.

Ashwin Krishnan: [00:06:44] OK. So that begs the question of investment. So that's a big cultural shift all the way down. Obviously, you guys are leaders, and if you talk the language of the security practitioners, it obviously helps, but to get to that level of truly walking in your customers' shoes it means you have to understand each of your customers intimately. How do you solve the scale challenge of being able to both run a business effectively yet at the same time, like you're saying, understand the customer's point?

Rahul Kashyap: [00:07:16] I think the way I can describe it is that it's not actually very complicated. We have built a playbook wherein most customers have similar challenges; they just have different networks and different configurations and so on. So, we have a playbook that we use for that. And the idea is that as we learn about it we automate it, so the next time we go in that vertical, we do not have to start from scratch. In some sense the experience from a customer's point of view is that they're getting value, and it's almost like an autonomous network traffic analysis solution. That's kind of the ultimate goal: How can you build out a solution which delivers value with minimal training required on the customer side.

[00:08:03] As we just mentioned, we are in 2019 now. We have to think differently about, as you mentioned earlier, the very classic way of you sell now and then go back after one year and take your next check. We have to build a solution which delivers value and customers appreciate that continuously. And how you do that in a manner which is scalable, as you mentioned, and at the same time customers appreciate it, that's kind of what we are focused on. And our focus on the back-end piece is how do we automate this. We have some exciting announcements coming up at RSA in just a few weeks which will talk about how we are going to achieve that.

Ashwin Krishnan: [00:08:52] You mentioned earlier, Rahul, about the IoT devices, the explosion, and just the level of noise that's in the network. Were there some assumptions when the company started that have been validated? What are some of the newer things that you didn't anticipate that you now are having to deal with and be able to address? So, just give an idea of how things have changed and not changed.

Rudolph Araujo: [00:09:23] I think the fundamental thing that hasn't changed is we went in with the assumption that there was a lot of value in the network, and I think that is still true. People these days have become skeptical sometimes saying, a lot of things in the network are encrypted. But what we found is if you can invest in interesting R&D around things like encrypted traffic analysis, you can still draw a lot of information from the network. And the network is really the ground troops because you may not have an agent on every single device. If you have a thermostat, you don't have an agent on it. You may not have logs for every device ...

Ashwin Krishnan: [00:09:59] But I do have a microphone on Nest.

Rahul Kashyap: [00:10:03] [Laughing] But that microphone is communicating with an app, so it has a presence. That assumption has stayed true for us. We've had to adapt to the evolving network and think about how we get that same level of visibility in the cloud, etc. From a perspective of what has evolved, I think we've come to realize, and I think as an industry we've come to realize, that we have to make security more and more mainstream. Security cannot be something that only the elite can do. It used to be that if you were JP Morgan, if you were the biggest bank in the world, you needed to worry about security. But if you were the local regional credit union you didn't need to worry. The reality of it is the attackers are equal opportunity offenders. So, we've spent a lot of time over the last couple of years really focusing on usability, user experience, and made some big investments there. It's not just about the core fundamental underlying technology, it's how do you manifest it, if you will.

Ashwin Krishnan: [00:11:06] Anything to add, Rahul?

Rahul Kashyap: [00:11:08] I think Rudolph covered most of the important aspects. I think the important part for us, what we really recognize here, is that there is enough juice in the network — the way I call it — there are enough good quality problems for us to solve just looking at the network. So, we are hyper-focused to be the best in that category. There are a lot of things you can add in the solution, different feeds, etc. But we are convinced that there are so many good problems out there, as we dig in and we talk to more and more customers, I think focus on execution is key. We are hyper focused on just being the best traffic analysis vendor out in the market.

Ashwin Krishnan: [00:11:51] So we talked about device explosion and proliferation of workloads, and everybody wants to be or every self-righteous vendor wants to be the single pane of glass. But every time I hear single pane of glass, it's like how many single panes of glass can you have in a SOC? So is there also an evolution that you're trying to see, where finally a McAfee and a Symantec and a Cisco and a Palo Alto really start to work together to solve the problem? Or is each one saying, I have feeds going out and feeds are coming back to me and let me be the "single pane of glass" because clearly certain things have changed and certain things have not. What's your sense of the big guys and the small guys coming up with something that actually truly solves a problem versus each one trying to be this single source of truth.

Rahul Kashyap: [00:12:48] I think that's been a problem in cybersecurity for a while. And I would say most large vendors are attempting to be the single pane of glass. In some sense they have succeeded, but the reality is this: cybersecurity is a very fragmented industry. There are very unique quality problems across every fragment. So being a single pane of glass is going to be very hard for a customer. To be honest, there is a good reason why you want to be single pane of glass, from a customer point of view that's what they want. But the reality is given the nature and diversification of attacks and the problem scope, it's going to be really hard for just having one big large vendor.

[00:13:35] I remember McAfee and Symantec were the only two who covered everything, that is not so today. Attempting to be that is going to be incredibly hard to accomplish. With that in mind, I think customers should start understanding how they can derive value autonomously from each product as opposed to trying to integrate everything together because that itself is a very complex problem. So I think it's a good part to solve, but we are not there yet. Saying, single pane of glass, everything solved, I think we are far away from that.

Ashwin Krishnan: [00:13:25] It's interesting you talk about security practitioners because there's a really interesting article that I read about three days ago that talked about the 30 things that CISOs absolutely dread hearing. Everything from we clean out the competition to we can get you 100 percent secure; things that are not believable. You mentioned this whole ecosystem of security vendors that are obviously solving a problem. How does a vendor rise above the noise when the customer is jaded? They obviously have fewer hours of the work week, every week. So how do we even go through anything? POCs used to be three months long, now it may be down to three days. So, how does somebody distinguish themselves, like you were saying, to truly understand what the customer needs and be able to solve that and thereby do well?

Rudolph Araujo: [00:15:12] Yeah, I mean, ultimately, it's not about your marketing message, it's not about your AI.

Ashwin Krishnan: [00:15:19] Hey, you're the VP of Marketing saying that.

Rudolph Araujo: [00:15:20] [Laughs] Unfortunately, that's the reality, right? It's about what value you can deliver. And one of the ways we've tried to really stay on top of that is as we were building this company out and building the product, we spent a lot of time with development partners, where we would just observe them. For instance, how are they operating with their workflows with and without Awake. Right, now we throw Awake into the mix. What difference does it make? Where are they getting stuck, where are they not getting stuck? And I think what that has helped us to do is really build a product that solves some of what my team call very simple, trivial, mundane problems but are so repeated and so often come up that they become points of frustration. So ultimately, I think it's about how you can solve these operational challenges for customers. Don't just make these bold claims that we catch everything, we are 100 percent secure, you're never going to need another security product because, you're actually right, I don't think any security team, any CISO believes those claims anymore. And so, we're really focused in showing value. When we go to market, we've got a base structured program where we say, here's what we're going to show you each week.

Rahul Kashyap: [00:16:36] I think Cybersecurity is a very fascinating industry. I remember when I did my first startup, most of the time I was trying to convince the customer that there's something called an attack and you're vulnerable to an attack. This is early 2000s, late 1990s. But now the awareness is not really a problem. People know that they have a problem. Now their challenge is who is the best person to solve it for me. As Rudy mentioned, it's about everybody trying to outmarket the next person, making bold claims. I think in some settings, we have gone through that phase, those silver bullet claims, I think people now see through that. The market is fairly educated, thankfully, and they understand what is compete noise, versus something that provides value, I think.

[00:17:37] The way I look at it is just honestly saying things that you do and you don't do is more powerful than claiming to have everything. You know, I've actually been in customer meetings and I tell them that we just don't do this, maybe we could do this, but that is something which we just cannot do. And they are fully surprised, they're like, you're the first vendor who's telling us what you cannot do. If you want to earn credibility in the market, be honest with your customers because that's what they really care about. That's the only way to go through the hype cycle, provide value and have some amount of integrity in what you deliver and stand up for it.

Rudolph Araujo: [00:18:18] Rahul was telling me about a conversation he had when he was on the road, where the customer heard our pitch and said, "I've got to give you credit because you didn't say the words AI, but I can clearly see you guys have AI behind the scenes." And he appreciated the fact that we weren't just, you know, AI, AI, AI, but at the same time we were using very powerful technology behind the scenes. So, I think we should respect the customers more. They're much more educated, they can cut through the BS, if you will. And you know, if you don't respect that, I don't think the customer, the prospect is going to respect the vendor.

Ashwin Krishnan: [00:18:53] So I can tell you this you are one of the few vendors who are talking about integrity and saying what we don't do. And like you said, walking in the customers' shoes but with an agenda to learn, not an agenda of what can I sell. It's like playing the long game, which is very unusual.

Rahul Kashyap: [00:19:10] It's a harder way. That's the hard path, but you know, that's how you earn credibility in the market. Once you get a few customers behind you, they will be advocates and we believe in that.

Ashwin Krishnan: [00:19:22] So switching gears a little bit, Rahul, I know this is a passion of yours. There is a lack of diversity in cybersecurity, whether it's male / female, whether it's underrepresented demographics, whether it's even the next generation of people who are looking at this and wondering, should I even make a career out of this. I know you're invested personally. What are you doing personally about it, and what do you think has to happen to be able to get the next generation of leaders to be interested in this?

Rahul Kashyap: [00:19:56] This is one of my personal passions I've been pursuing for many years now. The first thing is I believe that education should be for everyone. I believe that; I sponsor children and so on, in some countries, because I believe that education should be for everyone. Second thing, I realized cybersecurity is my passion. I'm here simply because I love this field. I'm very passionate about this industry and the challenges it brings forth. We keep on talking about the skills gap and the fact that we don't have enough people — I'll cover diversity in a bit. We just don't have enough people, so how do we tackle that? What I found was we are not educating children about cybersecurity early enough. Typically what happens is by the time you're in grad school, you have kind of made your decision on what you want to do or where you want to go. So, what I have done over the last few years, I have teamed up with a group of people, an open source kind of a group, where I mentor high-school kids, the entire LA school district is actually covered by that. On weekends I talk with kids and mentor and inspire them to get into cybersecurity. I kind of have a small kick startup program on how to get from zero to where you want to be. I talk with several kids and it's fascinating. For most kids, cybersecurity is what they see in Hollywood, you know.

Ashwin Krishnan: [00:21:36] [Laughs]

Rahul Kashyap: [00:21:36] So they come up with a completely different set of expectations. I have to level set that and strike a balance where they don't feel that this is boring because cybersecurity is a lot of work also, not just the cool stuff you get to do in Hollywood, right? I bring them to that point, and then I start coaching them on what you really need to do to be successful. And then I use my examples, what has worked for me, what has not worked for me, and so on. So, this is what I've been doing offline on weekends for the last couple of years now.

[00:22:10] Besides that, the other big problem, which is not just in cybersecurity, it's an IT industry problem, is the lack of diversity. I'm engaged with a bunch of nonprofits to enable and empower the girl child to make sure that at the high-school level they get the right mentorship. And I'm up for more opportunities there as well, if it's required, if I can help in any way, because I really believe that the way that our industry is skewed, it should not be this way. This is not a healthy sign, and it is on us. If every executive just takes on mentoring and inspiring one person, one girl child; that's all it takes. It's not very complex. We have to take that on as leaders. If each of us did that it would make a huge impact in society and in the industry at large.

Ashwin Krishnan: [00:23:09] Now that's very inspiring to hear because you're absolutely right. I think that by the time they get to, these days, 15 or 16 they've pretty much set a course, so the earlier you can influence them, the better.

[00:23:19] So one last question for you. What are some of the questions? I know with some of these engagements, high schoolers are already — you never know what kind of question you're going to be asked. What are some of the surprising questions that you've been asked?

Rahul Kashyap: [00:23:31] Oh boy, I had this kid once who was really, I mean I'm not sure if she was really interested in cybersecurity, but she really wanted to talk to me about cybersecurity. We had this long conversation and towards the end I ask, "What do you really want to do?" We talked about a lot of stories, but then it got to a point where she said, "You know what, I want to drop out of college." And I'm like wow, this is going in a totally different direction! So starting from talking about cybersecurity and higher education, I had to sit down and really hear her out in terms of why she wanted to drop out of college and what challenges she was facing. And, you know, she started opening up and we had a three-hour conversation out of that. I was totally unprepared for that, to be honest, but it gave me a lot of new perspective on some of the challenges that kids are facing. When they start to trust you, they start to open up. So, it's a big responsibility from my side as well to make sure that I'm giving them the right advice. I'm going to follow up with her, but I think the call went fairly well. And I think she's back in school.

Ashwin Krishnan: [00:24:51] Wow!

Rahul Kashyap: [00:24:51] But that was something which I was totally unprepared for and hopefully I made a difference there.

Ashwin Krishnan: [00:24:56] Wow. We can't top that. Thank you for your time. It has been a really interesting conversation. Hopefully we see you guys at RSA above the noise!

Rudolph Araujo: [00:25:08] Sounds good! Thank you.

Rahul Kashyap: [00: 25:08] Thank you.