uberknowledge

# Krishna Narayanaswamy, Chief Scientist and Co-Founder of Netskope

## Security in the Cloud Is a Shared Responsibility

Krishna discusses the need for swim lanes in the cloud, asks who actually has control of access to services in the cloud and argues for a layered approach to security.

02:58 Security in the cloud is a shared responsibility
03:46 Where does the dividing line on responsibility fall between user and cloud host?
04:37 The security implications of collaboration within the cloud
06:12 From on-prem to in the cloud represents a significant shift in control
08:25 How do you manage versioning within a hybrid on-prem/cloud system?
11:05 Could you accurately estimate your company's cloud footprint?
12:45 Is security now a shared responsibility across the entire ecosystem of an enterprise?
13:44 Swim lanes in the cloud
17:09 Encryption is a sledgehammer
19:30 The blurred lines between personal and business accounts in the cloud. How can they be monitored?

Ashwin Krishnan: [00:00:01] Welcome to another episode of the security podcast with UberKnowledge. Today, actually this is the first one for 2019, with me I have Krishna Narayanaswamy, who is the chief scientist of Netskope. Krishna, would you introduce yourself to the listeners?

Krishna Narayanaswamy: [00:00:18] Thank you, Ashwin. Happy New Year. So, my name is Krishna, and I'm one of the co-founders of and chief scientist at

Netskope. Netskope is a cloud security company; we fall in the area of cloud access security brokers but expanding beyond that into general cloud security. I'm looking forward to having this conversation with you.

Ashwin Krishnan: [00:00:41] Thanks Krishna. So, we're going to be spending a lot of time on the demystification of what cloud security is. And on the topic you were discussing just before the start of the podcast, if I go and ask two people — even within the same company — about the definition of cloud security, I can guarantee I'm going to get two different responses, right? So can you describe, for the purposes of the people out there who may be scratching their heads listening, how two vendors are going to a conference and coming up with different interpretations of what cloud security really is. What in your mind are some of the principles behind cloud security, and then we can talk about the manifestations of what cloud security is?

Krishna Narayanaswamy: [00:01:27] Sure. Yeah, that's an excellent question. So, what we're observing right now is a transition of services, like people having applications. Go back 10 years, private data centers were very prevalent. Most organizations invested in private data centers and applications within private data centers and had security services like remote VPN and DLP and firewalls for those data centers. Over time, I would say over the last 10 years, there's been a move of applications that are hosted on premises moving to the cloud. And this points into two categories. One is if you look at turnkey solutions like Exchange or SAP or things like that, they're moving to the vendor-hosted cloud for example, Microsoft has its own Office 365 cloud. But Azure cloud maybe hosts typical services which used to be hosted on premises for example, SharePoint or Exchange and so on.

[00:02:31] So that's one aspect. And that is what we call SaaS or Software as a Service. And there are many more such vendors that are not on-prem but have mushroomed over the years.

Ashwin Krishnan: [00:02:42] So, let me just ask a question on the security of that. When something like Exchange versus Office 365, when it goes on-prem hosted by the local IT — was that security the onus of the IT, and now is it the onus of Microsoft?

Krishna Narayanaswamy: [00:02:58] That's a great question. Exchange is part of the Office365 suite. So, when Exchange was hosted on-prem, the security was completely owned by the IT of the organization. Now, when it moves to the cloud as part of Office 365, it becomes a shared responsibility. The responsibility does not automatically fall onto Microsoft. To some extent, Microsoft secures the servers from things like making sure it's patched for vulnerabilities and making sure that the data is stored safely and so on. But still, who accesses the exchange online, who has permissions to do various activities, is still the responsibility of the enterprise or the organization's IT.

Ashwin Krishnan: [00:03:46] So, again this gets very fascinating. If you are the IT person, if you are racking and stacking those servers, you are buying those licenses, you are setting it up, there is a natural understanding of you being the owner — you have the keys to the kingdom. You have no idea where it's hosted. With GDPR there are lots of compliance issues that are all being taken over or, in some sense, assumed by Microsoft. Yet, like you are saying — who has access to what, permission control, location, VPN versus non-VPN — how does an IT person come to terms with, yes, it may have physically left the enterprise but the responsibility, like you're saying, is shared, and is where that dividing line is, is that well understood?

Krishna Narayanaswamy: [00:04:37] I believe it is not very well understood, in my experience, because there are a few different things that play into that. There are certain things, in terms of how you configure Exchange or a SharePoint, which are pretty much the same as what they were: you're just taking the application that was running on premises and running it in the cloud.

[00:04:57] So that aspect is there, and people are well versed in that and are being updated based on the newer things that are happening in the cloud. But, I think where it starts to blur is, when you have your data center hosted on-prem, you know who is coming into your data center. Now, these are being hosted elsewhere. These services are publicly available for a reason because people no longer work from just offices; they work from home or from Starbucks or wherever they are. So now, it becomes a responsibility. You want to figure out from the time somebody authenticates and logs in to these systems, what are the various things that they can do? Because one of the other aspects of the cloud is also collaboration. More and more services allow you to share information using a click of a button. Now, when you hosted something on-prem and you're sharing, you're assured that you know who's coming in through the door. Whereas now, you've got to know if someone is inadvertently getting in. Insider threat becomes much more of a big issue when things move to the cloud because people can share things with unintended parties and so on.

Ashwin Krishnan: [00:06:12] And with the click of a button you're able to share. So, let me ask one other thing: versioning. If you're on-prem, you control what software version is running and when patches are applied and so forth, does that all magically happen in the cloud?

Krishna Narayanaswamy: [00:06:28] Yes, it does magically happen. So, you have no control of that. And usually the cloud providers are very careful, especially the Tier 1. They kind of have a beta period, and then they do it region by region. So, to a large extent that is well controlled. I've not heard, at least, of any horror stories there.

Ashwin Krishnan: [00:06:50] Ok, but it is a significant shift in terms of our control. This is interesting. Now, let's get to the manifestation, so these are some of the cloud principles we talked about before. Where is cloud? I mean, in the original days, maybe 10-15 years ago, it was definitely off-prem. You get off your physical data center and you're somewhere in the ether, hosted by your cloud provider. But today, whether it's Amazon on-prem or whether its vendors like

Netskope bringing things on-prem, is the definition of what cloud is or where cloud is also getting blurred?

Krishna Narayanaswamy: [00:07:33] To an extent that is right because even when you look at cloud, cloud means somewhere that is not under your control. That is what it used to mean, right? And this could be a public cloud like an Amazon or an Azure or a GCP. It could even be a private cloud, like data centers where services are hosted, in the way part of Netskope's services are hosted in private data centers. But to the customer it's to the cloud because it's not something under their control.

[00:08:00] But we are also seeing more and more hybrid natures, where you have some services that are hosted on-prem. And if it's a networking service, for some traffic it's handled on-prem, and when a user goes off-prem it gets handled in the cloud. So that kind of hybrid nature of physically where the resources are located, is pretty common.

Ashwin Krishnan: [00:08:25] Given your mention of the shared responsibility, let's put two and two together now. Is there a constantly changing line depending on where the cloud manifestation is happening? Like who is responsible for it? For example, if Amazon brings their cloud to your data center, access to those servers — is that the responsibility of Amazon or is that the responsibility of the on-prem versus that actually being delivered through Amazon's own colo services or Amazon's own data center; is that also changing? I mean, does an IT person have to worry about where the cloud physically is in order to establish what they are actually responsible for?

Krishna Narayanaswamy: [00:09:08] That's also changed – that's a great question because one of the advantages of the cloud goes back to the previous point of versioning. Most of the cloud providers are CI/CD model, they are continuously deploying newer versions, and so they have full control of what runs in the cloud. The moment you start putting some of those aspects on-prem, again it varies from vendor to vendor, some vendors allow the customers to

control what version goes on-prem, but then it becomes a nightmare of compatibility between what runs in the cloud versus what runs on-prem. The preference for vendors is always to control even the on-prem versions with a common version, so that you don't have to worry about compatibility issues.

Ashwin Krishnan: [00:09:54] We've barely scratched the surface, and already you're seeing so many different things. Given your experience, when Krishna goes out there and talks to customers — in terms of what you are hearing and seeing from them — is there a preference? Given just the services that we've touched on and how complex things are, is there a … It's almost like the early adopters of cloud are coming back and saying, "Okay, this is way too complex." And we just talked about SaaS as an example, I mean there's IaaS and PaaS and all the other combinations. Is there a need or is there a sense that we need to go back to a few trusted providers because of this whole best of breed thing? I think the biggest reason for going to cloud is efficiency. And if you're spending more cycles trying to figure out shared responsibility and SaaS on-prem or in the cloud or somewhere in between, would you rather just say, "Let's go back to the heydays of the 90s, where you never got fired for buying IBM, and you never got fired for buying Cisco."? Are those large players at a significant advantage at this point because of what we touched upon?

Krishna Narayanaswamy: [00:11:05] That's a good question because I think the cat's out of the bag. Typically, going back to your first point of when we go and talk to customers, one of the first things that we do is a cloud risk assessment. So, first of all, step zero is most organizations' IT departments have no idea what cloud footprint they have. So, you need to first discover that. And when we go and discover that in an average organization of, let's say, 1,000-2,000 employees, we see over 1,000 cloud services; I'm not kidding you.

Ashwin Krishnan: [00:11:39] This is everything: SaaS, PaaS, IaaS.

Krishna Narayanaswamy: [00:11:42] Normally SaaS, I would say. In fact, we have a running joke here. When we go and talk to our customer's IT department, in

our first engagement, we ask them how many cloud services they have. Usually they come up with a number, and the number we discover is usually 10 times the number they give. The reason being, the number that the IT knows about is what is sanctioned cloud.

Ashwin Krishnan: [00:12:05] OK, and these are the unsanctioned, right?

Krishna Narayanaswamy: [00:12:06] And that's become very important. I don't think it's going to be very difficult because the larger the organizations are and the more decentralized they are in terms of business, they just go off and acquire applications because they can just use a credit card, and it's all right. So that's when I think, from a security point of view, it becomes even more important that you not only control sanctioned cloud applications, but also unsanctioned ones. And that's a big education gap because there are many people out there who are looking to solve the sanctioned apps when the sprawl of the unsanctioned apps is clearly the bigger problem.

Ashwin Krishnan: [00:12:45] So, and this is probably a mind shift, but let's assume that in a 2,000-person organization you've discovered 1,500-2,000 apps. Now, given the small size of the security organization and the responsibility to maintain harmony and some level of hygiene for the sanctioned apps, if all of a sudden you say, "Hey, you're responsible for 2,000 apps," — I mean I haven't used shared responsibility in this sense — but is that a shared responsibility within the organization? Security is not just the onus of the CISO and his or her organization, it is actually the onus of the broader marketing group and the PM group and the engineering group who are out consuming this. Are you seeing a broad-based awareness of security being a shared responsibility across an entire ecosystem of an enterprise, or do you still think it's siloed within the CISO's organization and that has to change or not?

Krishna Narayanaswamy: [00:13:44] I'm starting to see that shift. Going back to the example of over 1,000 apps; clearly, they fall into three buckets. One is the sanctioned. The unsanctioned fall into two buckets. One is you can go — there

are many systems out there — actually I want to call out the Cloud Security Alliance (CSA) or CCM, it's called the Cloud Control Matrix, that defines what are enterprise-ready attributes of a cloud service. So, there are many rating systems out there that tell you these apps have a good rating versus these apps have not a good rating. I will just give you a very simple example, there are many cloud apps where if you upload the data, the ownership of the data goes to the service. Now, imagine if somebody is uploading a product spec and now it becomes an ownership issue. So, the first part in the unsanctioned bucket is to weed out the ones you really want to block because there's no reason for using those apps. Then when you get to the shorter list, which is the apps that have a reason to be there otherwise the business would not proceed. Then it becomes a shared responsibility where certain guardrails are put in. That's where security solutions are available in the market, like cloud access security brokers. For both sanctioned and unsanctioned, you want to provide the guardrails because you don't want to block these apps because business would come to a halt. But you want to provide that swim lane, so to speak, where users can continue to use them, but if they tried to go out of the lane, they are put back.

Ashwin Krishnan: [00:15:22] So, going back to that original piece that you mentioned, from a mindset perspective, you're actually putting the business at risk by putting product specs out or some of your own customer research information that, obviously, you don't want to get in to competitive hands. Where does data privacy and ethics fall into that? Are you seeing, at least from the forward-leaning organizations, them saying, "OK, the next time we acquire a cloud service ..." We used to have these things in the old days where you actually have vendor-rating systems. Obviously, cloud has made things quicker and easier to consume, and you don't even think about uploading anything to Dropbox anymore, versus saying it's OK to upload to Dropbox, as long as things are encrypted and you have the key. So, at least, are you seeing that very basic person, credit card swipe, or PayPal, or some other mechanism of seamless transaction, but also just a basic question of saying, "Hey, is the data encrypted?" before you upload it? Again, is the onus of that on the CISO's organization or do vendors like Netskope also play a part? Where you engage

with customers and actually become an ally of the CISO so that she doesn't wage a lonely battle inside a vendor. You say, "Hey, guess what, this is what we are seeing with other competitors of yours that we also service."

Krishna Narayanaswamy: [00:16:52] Yes. So, it's definitely not just the CISO's battle there, and vendors like Netskope come in and help in that situation. I would take it one step further which is, I think encryption becomes like a hammer.

Ashwin Krishnan: [00:17:07] Solves everything, right?

Krishna Narayanaswamy: [00:17:09] Right. A sledgehammer. So, what we see is most organizations are forward-leaning in the sense that they give — in fact it's kind of expected these days that employees can have an open environment where they can use any of the apps for their personal use and things like that. So, the idea here is, you monitor the data going to these apps. So, the first level even before encrypting is almost all organizations have some idea of what is sensitive for their business. For example, if you're in a consumer-driven industry like retail, PCI compliance is important, that means you need to be careful about PII information, PCI information. If you're in healthcare, it's PHI information, and so on. So, the first level is to apply some level of DLP. That's why DLP has got resurgence with the cloud because it becomes all the more important to be able to classify the data.

Ashwin Krishnan: [00:18:04] So, context aware depending on the industry.

Krishna Narayanaswamy: [00:18:06] You can also have simple policies that say if I find sensitive documents being uploaded to a poorly rated cloud service, I'm just going to block it. So that is something before you go to the encryption. So where does encryption come into play? Let's say there is a legitimate use case for putting sensitive data in the cloud and sharing it maybe with some external partner because one of the advantages of the cloud is you don't need to have an FTP server anymore.

Ashwin Krishnan: [00:18:30] Correct. You just send the link.

Krishna Narayanaswamy: [00:18:33] So, that's where encryption can come, as a layered approach to securing data as opposed to just saying, "I will let anything go the cloud, but I will just encrypt it." It has other implications.

Ashwin Krishnan: [00:18:48] So it's interesting, everything we've talked about has multiple layers. The first piece is, like you said, just go and figure out how many services you're using. Then within that, which are the "rogue ones" which have very poorly defined privacy policies and therefore block those. And the third piece is, in normal day-to-day use there are certain principles that need to be used, but every user doesn't have to be burdened with understanding everything. Instead, using technologies available, you can provide deeper level and DLP. A great example of technology which was probably there in the late 90s, early 2000s and is now suddenly coming up with the usage of cloud.

Krishna Narayanaswamy: [00:19:30] I think one of the things that I'd add to this is the blurring is even worse because many of even the Tier 1 cloud services' PaaS services follow freemium models. The consumer gets a free version and the organization has a paid version. So, for example, let's use Google. I have my Gmail account. So, I go to drive.google.com, but if you look at the URL, it's drive.google.com. So, how do you know, even when you're monitoring, if somebody is going through the corporate instance or the personal instance? And that's where, again, security services like those we provide at Netskope are able to identify the instance and you can set policies. Okay I'm going from a sanctioned device that is given to me by my company, and I'm going to my personal instance — I'm allowed to go to my personal instance because I may want to upload my vacation pictures or whatever — but if I am uploading something sensitive, you want to be able to block that.

Ashwin Krishnan: [00:20:25] Interesting.

Krishna Narayanaswamy: [00:20:25] And it becomes very difficult with legacy security solutions because all of them are operating at a URL level. If you look at a secure gateway it's looking at a URL and saying allow. But then take OneDrive, for example, I can have a live.com account in Microsoft and have my own OneDrive as opposed to the corporate one.

Ashwin Krishnan: [00:20:47] So that's interesting. I think we're probably reaching the end of the podcast, but you bring up a really interesting point, which I want to spend another couple of minutes on. That is the awareness that it's not just a corporation, there are people inside the corporation, there are humans inside the corporation, who have lives, and they are context-switching all day long. Whether you like it or not. People are posting a Facebook update or sending a tweet or something like that. And you have to be aware of that. So whatever technology you use has to be frictionless when it comes to understanding the motivation behind why something is happening. And unless you're able to take that into account, you're actually going to be "pissing off" employees.

Krishna Narayanaswamy: [00:21:27] Exactly. That's exactly what we're seeing, and more and more forward-looking organizations are falling into that band of allowing their users to use freely the applications. They're putting in the guardrails so that they can be assured that their data is protected ...

Ashwin Krishnan: [00:21:49] while allowing their employees to be human beings.

[00:21:52] This has been really, really fascinating. Again, thanks for being a phenomenal guest and the first 2019 podcast for UberKnowledge. Thank you for your time.

Krishna Narayanaswamy: [00:22:02] Thanks very much, Ashwin.