
# Architecting the Cloud, part of the On Cloud Podcast

Mike Kavis, Managing Director, Deloitte Consulting LLP

**Episode Title:** **Debunking cloud security myths: truth vs. fiction**
**Description:** As companies—especially those in highly-regulated industries such as financial services and healthcare—contemplate migrating their data and applications to the cloud, they are often apprehensive about security. Worries about unauthorized access to data, compliance risk, and network and security monitoring often top the list of security concerns. The good news is that, in many cases, cloud security fears are based more in myth than fact. In this episode, Mike Kavis and guests Deloitte's Arun Perinkolam and Kieran Norton and Google's Hauke Vagts, debunk some of the most common cloud security myths and set the record straight on how security is often actually better, and less costly to implement, in a cloud environment, and on how companies are overcoming their security fears by taking a risk-based approach to migration.
**Duration:** **0:24:07**

**Operator:**
The views, thoughts, and opinions expressed by speakers or guests on this podcast belong solely to them and do not necessarily reflect those of the hosts, the moderators, or Deloitte.

Welcome to Architecting the Cloud, part of the On Cloud Podcast, where we get real about Cloud Technology what works, what doesn't and why. Now here

is your host Mike Kavis.

**Mike Kavis:**
Welcome to Architecting the Cloud podcast. We're here with a bunch of security experts, and we're going to talk a little bit about security myths, a topic that we always seem to have to talk about, right. So, with us today, first is Kieran Norton from Deloitte. Tell us a little bit about yourself.

**Kieran Norton:**
I've been with the firm for about 15 or 16 years. Been in the security game for about 20 to 25, to date myself. And currently I lead the infrastructure security and cloud security practice for Deloitte.

**Mike Kavis:**
Next from Google - tell us a little bit about yourself.

**Hauke Vagts:**
Sure, yeah, hey, I'm Hauke. I'm a security specialist for the Google Cloud Platform. I'm based in New York, and due to that, I think I mainly work with our financial service customers. It's helping them being successful in the cloud and secure.

**Mike Kavis:**
Good stuff. And last but not least, Arun Perinkolam who also works at Deloitte.

**Arun Perinkolam:**
Yeah, hello, everyone. Arun Perinkolam, I'm a partner at Deloitte, lead the Deloitte relationship back to Google from a security perspective. Also work pretty closely Kieran on our (Inaudible) Infrastructure practice.

**Mike Kavis:**
Great. So, first topic, security myths. What – you may all have your own top three, so we might wind up with a bunch, but what are your top three cloud security myths?

**Arun Perinkolam:**
Yeah, so I'll probably start off. I mean, I think the biggest myth that a lot of our customers have right is moving to the cloud inherently less secure than on-prem, and they have – a lot of the customers also have concerns around do I have control over the data that I put onto the cloud, will the CSPs actually have access to a lot of the data, et cetera. So, I'm sure my fellow panelists have others that they can share.

**Kieran Norton:**
Yeah, well, I mean, I think there's a lot of – initially, and I think it's less so now, but there used to be a lot of fear about moving to the cloud. There was a lot of concern about it and people like, oh, the risk, the risk, the risk. But when you look at actually how companies manage their on-premise environment versus what's possible in the cloud, you can probably do better in the cloud in many cases. Yes, there's risks you have to address, there's things you have to think about that might be new and you might have to translate some things you've done previously in different technologies and processes to work differently in the cloud, but all the tools are there for you to actually operate in a more secure fashion in many cases. And, so, I do think a lot of it has just been uncertainty, causing fear as opposed to a real comprehensive understanding of the actual risks, and then the capabilities and what you can do with those capabilities in the cloud.

**Hauke Vagts:**
Yeah, so I totally agree with that. So, I think a very interesting point is I think it's mainly the fear because you haven't done that before. The tools are all there. And then what you used to do in the past for like 20 years, you know how to do network security monitoring network on-prem. You can still do similar things in the cloud, or even better things, but starting to make the change and be trustful in the new tools, I think that's a challenge area.

**Kieran Norton:**
I mean, when it really hit for me was a number of years ago when I started thinking and looking at how you manage patches and VMs in the cloud. And the massive challenge and effort that most of our large enterprise clients have with patching and configuration management and asset management, and the fact that you design it from the beginning and you build it the right way in the cloud, you can achieve such a more mature and automated and efficient operation and capability. That's really when, for me, it kind of really hit home, just on the basics of infrastructure alone, let alone getting to paths and all these other kinds of things. That alone is a huge game-changer that if our clients could realize, and can realize, it'll make a huge difference.

**Mike Kavis:**
Yeah, I think that fear is a good thing because it made security a first-class citizen, right. It's number one in design now, so many years ago I was doing a startup and we were selling into the government. It was like a digital couponing thing, so you're doing digital money to the point of sale, right. And we got this big thing to fill out, a million security questions, and we go in and we're getting drilled, and halfway through it they go, "Oh, you're on the cloud?" We go yeah. "Oh, we've got this other set of questions here." And I'm like, so if I wasn't on the cloud, I wouldn't have to adhere to those, but that's kind of a common theme is the fear, and I get like, as you said, there's less than there was, has made it a first-class citizen and now application development used to not really care about that stuff in general that much, and now it's like it's an early requirement, which I think is a good thing.

**Kieran Norton:**
Yeah, for sure. I mean, DevSecOps, right. I mean, that's just – you think about the way it used to work with checklists well after the application had gone all the way into production, and people just basically going down and saying did you do this, did you do this, did you do this? The effectiveness of that as a security mitigation or a risk mitigation to the point of actually embedding security into the entire design, development and testing process in an automated way, I mean, that's a massive gain.

**Hauke Vagts:**
So, I think originally the vulnerability management, I think that's the best example, right. Our customers I work with – you have probably the same experience working with your customers doing patch management in like an environment that's grown over like 20 years, acquisitions, totally different hardware stacks, it is painful. We always (Inaudible). I think it happens in one place where it's done great because you can. It's too many resources, not effective, and you're not moving to an automated way, like more containerized way. I think it is way easier to do that, and you don't need to care about that at all.

**Arun Perinkolam:**
And in all those aspects, I actually feel moving to the cloud has more advantages, right, because at the base network and infrastructure level, a lot of the security features you cannot get for free almost, right. Like if you look at GCP, for so many security capabilities, right off the bat when you think of logging and monitoring and encryption and so on and so forth, and really the customer needs to focus only on the application side of the house, right, and they're responsible.

**Kieran Norton:**
Yeah, I mean, if you're a Fortune 50 and you've invested $1 billion in your cybersecurity program, you probably have a pretty secure network. You probably do it pretty well. But if you're not, and you don't have that kind of money, you're talking about cloud providers who can dump way more resources, and technology, and R&D and everything else into building that base infrastructure and securing it in a way that you can leverage it that you will never match.

**Mike Kavis:**
Well, and the other thing is what's your core competency? Is your core competency building security or is it banking or is it healthcare? And you look at the CSPs like Google, that is a core competency. I mean, security's a big piece of your platform. So, there's also GCP-specific myths. So, being the one that gets nailed with the questions from the customer, what are some of the myths that you have to fight specifically about Google?

**Hauke Vagts:**
So, I think a question that I always get, and you touched on it I think already earlier, but briefly is like you're Google, you're looking into my data, right. So, – which is obviously totally not true. So, I mean, first of all, like where we have contracts in place that already prevent us from doing the things, we have technical control someplace, and what's really nice, is we have different products and we try to be fully transparent. It's called X-Transparency where we provide our own log files to our customers to see where Google has accessed data, and we're going to go even a step further and like allow you to authorize access or prevent access if you don't want to have that. And I think this transparency's very helpful to build the trust relationship, but I think it is an uncertainty because you're not knowing where you're moving and you're giving, of course, up some of the control and (Inaudible) up a shared responsibility where it's not really clear that you're on the journey like what you own, like what does the provider own where, yeah, you are just expecting bad things are happening. It is totally natural, nobody looks into your data, and there are very strict controls in place for that.

**Kieran Norton:**
And again, I think there are real world examples of where people have been living with those risks for a long time. So, if you've outsourced a lot of your technology infrastructure to a third party, even if it's on-prem, you have, in theory, the same shared risk of they're going to use that access to access something of mine that I don't want them to otherwise see. If you're using an outsourced application provider, if you're doing anything like that, if you're using a large telco, I mean, the same theory is that. If you're using the post office, well, in theory, someone in the post office could be reading your mail. I mean, that's a risk we've lived with or a long time. And again, because it's in the cloud, it seems a little bit scary, and maybe there's more automation, more scale. I'll definitely grant that, but the risks, I think, are things you've been looking at for a long time.

**Mike Kavis:**
So, let's talk about containers because there's a lot of myths about containers, and I think container's a little bit behind cloud, but follow the same path where the myth was containers are insecure, and now we start looking at smaller surface space and stuff. So, let's talk about some myths about container security.

**Hauke Vagts:**
Yeah, so I think the first one, because I think it's the most important one to start it off, many people now think containers are new. So, because they're getting all this media attention, now people finally start using them, they get a lot broader attention, but containers are actually existing since quite a few years. And speaking about that security in containers, I think the (Inaudible) extensions existing since 2004, if I'm not mistaken, so it's quite a while since that has been around. That has been, of course, a maturity growth there since that time, but now I think people understand what needs to be done in container security. And, of course, you can still do it the wrong way. But how we try it on our platform is we try to give it a standing point and start with a good basic level of security with having up-to-date systems, which already mitigates a lot of risk. And then overall, I think containers might be even a secure way of doing things. We spoke about the vulnerability management, right, and you don't need to do that anymore when you're adding containers.

**Kieran Norton:**

Yeah, you're greatly reducing your attack surface, you're shrinking the exposure you might have from a technology perspective, and I mean, vulnerabilities may pop up in containers as time goes on, and certainly Struts was around for, what, 22 years, 20 years by the time the big Struts (Inaudible) popped up. So, I mean, it can certainly happen in technology. That's a fact of technology, but again, you're actually reducing your risk by using a simplified, tightly controlled, smaller risk, smaller attack surface solution. So, there's a lot to be gained.

**Hauke Vagts:**
Yeah, and I think as simple as you don't need to SSH into container, right, to do changes. It's just like – so just like removing all this risk, and if – I mean, that's what I tell my customers. If you use SSH in your production environment, you're not doing things right. You need to question like what are you doing, why is that even necessary. So, that's all, to your point, highly reducing the attack surface and way easier to patch all of your containers, and you don't patch on the machine; you patch the container and deploy it. I think that's just a way better approach, cleaner and more scalable.

**Arun Perinkolam:**
Yeah, and when you see some of the new announcements that Google has made, like Anthos, right, which is all based on Kubernetes and containers, it has several neat features, at least from the announcement, where you can automate a lot of the security policy and enforcement and scale that across your kind of hybrid multi-cloud environment. So, I think they're tying a lot of the new innovations to the existing container security features and in terms of automation and scaling as well.

**Mike Kavis:**
Yeah, so – let's talk about managed services, right, managed services as an API service, not as a company managing your data center, but all that patching, all that stuff just (Inaudible), right. Where you look at – I wrote my own Kubernetes cluster and all that stuff, and I have all these open source projects I'm constantly patching, all those create risk. Whereas, if I leverage something like Anthos and it's managed and it's patched for me, I'm just writing code on top. So, how does using these higher level distractions, I'll say, help mitigate risk as well?

**Kieran Norton:**
Well, I'll jump in and start with it because I think this is important, so I'm going to step back a second and I'm going to come back to that. So, number one is you need to commit to actually doing things in the cloud the way cloud's designed. So, if you're not doing cloud native in the cloud, you're hampering ultimately the value of what you're doing, and from a security standpoint, you're going to hit some roadblocks as to how much you can automate and how fast you can respond and do some other things. So, setting that aside, let's say someone's fully leveraging the cloud and its capabilities. Speed is a great mitigant when it comes to risk. If it takes you nine months to find and fix something, versus something you can find and fix and react to in a day, that's a huge difference. And, so, using these higher level tools gives you that kind of automation and capability to be able to identify, react, respond and basically fix or recover in a much shorter timeframe, that exposure window matters. Matters very significantly, so from my perspective, there's – maybe there's a little bit of a tradeoff there, but you're trading speed and agility for what used to be a very thorough checklist-based process that took a very long time. You know, the business wants to go move to the cloud, I mean, business drivers move to the cloud, they adopt new technologies, they're really driving to take advantage of a lot of these capabilities, and so security's got to go along for the ride.

**Arun Perinkolam:**
Yeah, the one thing I would add to what Kieran mentioned is customers are also concerned, and rightly so, in terms of how do they integrate a lot of the capabilities that they are now putting into the cloud with their on-prem kind of secure investments. And major CSPs like Google do offer a lot of those features where you can integrate, for instance, logs from your GCP environment to an in-house security monitoring system, right. So, those are some aspects that customers maybe think are harder problems to solve when they probably are not. And there is that integration feature that they should kind of exploit and leverage as opposed to thinking, oh, if I move to the cloud, it's going to be net new capabilities that they need to stand up.

**Kieran Norton:**
Yeah, I mean, you need to speak Stackdriver as a language, so there is some work to be done from that perspective, but once you do, then a lot of the same kind of capabilities and the way you've handled it before, apply.

**Hauke Vagts:**
And I think the nice about it too, I mean, it comes on the platform for free, right. I don't even know like our competitors are doing it, probably the same way but on our GCP you can use all those because we want our clients to be secure, and especially, like you said, we don't have like a $1 billion program. I think it's great. You just use what's there and we be cloud native with those tools.

**Mike Kavis:**
And I think another myth specific to GCP is that it's an analytics platform but there's no enterprise workloads there. And we just saw, I don't know how many enterprise clients get up there and talk, so how do you deal with some of those perceptions that this is just a sandbox for analytics, machine learning when there's real enterprise workloads going into the cloud?

**Hauke Vagts:**
Yeah, I think time will tell actually. So, I think now that we're – we have more customers that are open here and to speak, and we have the internal view, right. We had a lot of those customers already here in the past working with us, but I think people were a bit too scared to go too public with it, and they're considering the financial space and working with quite a few customers in that space, but we just had JPMorgan Chase on the stage, but they're – others are taking similar steps, right. So, I think it is just because you're not seeing it doesn't mean that it's not happening. I think – how it feels to me right now across the board is that there has been now like a change here of how cloud has been seen. I think everybody now really understands this is the future and this is what we want to do and seeing all the benefits and letting a bit go of really, okay, like we want to fully control it and stay in our on-prem environment then

want to make the move. I mean here with connected that all to the other announcements here. Nothing is going to happen overnight. Nobody – if you're heavily invested in your on-prem data center and you have your skill people but you're – there's no reason to give that up overnight and, like, leave your processes running there in a very risky state by not really knowing how to make the right move. But I think being in a hybrid model and slowly move, especially as a big enterprise where you don't have the need to spin up quickly and get your application to market because you're not liquid anymore, it's possible, right, and you can take your time and that's – I see that happening right now across the board, and I feel people recognize it, that this change is happening and see their peers moving. Our customers talk to each other, so I think that's all building trust and building that ecosystem.

**Kieran Norton:**
Yeah, and earlier I was talking about cloud native being important in order to gain the value, and I still think that's the case, but we do see from a client perspective, I would say, a lot more interest and focus in hybrid and multi-cloud as kind of where they're thinking about going in the future. And, so, while we might see something like GCP come in initially because of analytics, then with familiarity of the tool set, the toolbox, comes maybe a change of view of like what else can you do with the toolbox. So, I think we see some of that as being kind of the sharp end of the stick, but then leading to other uses of the platform.

**Arun Perinkolam:**
And we are seeing, you know, in a phased manner, big enterprise applications also moving. Like SAP is the classic example where a lot of the customers are seriously contemplating moving S/4HANA moving SAP into the cloud, so that is – it's definitely coming, even though today the focus may be more use case driven, more compute (Inaudible) driven, but the move to – and up on stage, I mean, Thomas had so many customers on G-Suite as an example. And big customers that have then consciously made that move.

**Mike Kavis:**
Yeah, so let's talk about data a little bit because that's usually the thing most people are scared of moving to the cloud. And I work more on the greenfield apps, and these are all data – you know, IoT streaming in petabytes of stuff. What's going on is like disruptive technologies are coming, and it's almost not even feasible to store that data on-prem. So, the hand's kind of being force that, hey, if we want to do these disruptive things, the only place it's feasible to do some of these when we're talking about that scale is on the cloud, so they're being forced to go to the cloud. So, let's talk about how companies are starting to be a little more reluctant to let sensitive data live in the cloud. There's a lot of use cases where it's out there. There's health companies that have tons of PHI stuff out there and it's certified and all that.

**Arun Perinkolam:**
So, I guess I'll apply the lens of the industry sector here, right. When you look at certain industry sectors, like financial services as an example, when it comes to data, given that they're so highly regulated, I think there's an increased focus at their end from a data security standpoint and making sure from a regulatory perspective they're able to kind of meet some of those regulations. We will probably see a little more time in those industry sectors where there are data-driven kind of use cases or data-focused use cases, a little more time, them kind of migrating to the cloud, but I mean, in sectors that are maybe not as highly regulated, I don't see that as necessarily an impediment in terms of use cases and workloads they want to kind of move in the cloud.

**Mike Kavis:**
But even like a lot of the banks have a huge digital initiative, because the thing that differentiates them is how they talk to the customer, and that's all data mining, data analytics. So, you know, I see a lot of banks, even though they may have their core apps maybe not putting that data into the cloud. Their digital initiatives are being all done in public cloud.

**Kieran Norton:**
That's right. I mean, for the most part, they're taking a sort of risk-based approach. So, they're not putting the most – the highest risk, most sensitive data in the cloud first. They're starting with something else, getting their feet wet in some cases, some of the banks have been doing this for a long time. And then they're maybe going to the next tier of data, so then they're going maybe to medium-risk data and then they're working with that in the cloud and getting comfortable and getting the regulators comfortable with what they're doing. And then they'll approach high-risk data at some point. But to your point, I think it is very industry-specific.

**Hauke Vagts:**
So, that's actually – that's a good point, speaking with regulators, because I'm having a lot of regulator interactions here too, and I feel I see a change there too. So, like how we educate regulators and seeing how they – I don't see any fears from regulators, right. I mean, I – they ask us like, hey, for instance, in financial services space, what should we tell our regulated entities? Like what should they do? Like please tell us, help us finding like the right regulation and the right requirements. I've never heard from one regulator so far, like we don't want the cloud, we don't think it's a good idea. So, I think they're generally very supportive, but they want it to be done in the right way. And apart from that, I told you here was your – I'm seeing the same strategy with our customers, right. You do it in a risk-based approach where you – there's different strategies to do that, but yeah, I think that's the way to go. And then also, speaking about the native controls (Inaudible) as a platform, if you're moving a medium-risk application, you have your encryption by default and (Inaudible) at risk, that all comes out of the box and makes it actually way easier to be cognitive and (Inaudible) things. But yeah, you still need to do your risk assessment, of course, for your big applications and just like moving the big applications, so still a complicated task, right.

**Arun Perinkolam:**
And, Hauke, I think I would actually double-click on the whole education and awareness piece, because that's so important, you know, having the ability to tie back the regulatory requirements that the customers have around data protection to actual feature sets that GCP has. So, be it the way you do encryption, the way you chunk up the data, have unique cryptographic tokens associated with each user account, and kind of encrypt that along with features like BLP API, that offers kind of data loss prevention capabilities to prevent things like data exploitation. I think it's a matter of tying some of the

technical features to the actual requirements that the customers really care about.

**Kieran Norton:**
I would never start that conversation by saying, "Hey, I'm going to move this risky data out to the cloud." Like, that's – I would start it with, you know, we're going to – we're looking at a migration. These are the risks we're facing in our existing environment, these are the requirements. This is how we're addressing all these risks in the move to the cloud, and by the way, here's how we're going to be able to do it better, here's how we're going to be able to do it faster and get people comfortable with the fact that you're actually improving it, because all that capability is there, as opposed to just starting the conversation by saying, hey, we're going to do it and, again, people will have concerns if they don't have knowledge.

**Mike Kavis:**
And a lot of what I've had to do at large enterprises is coaching the compliance and risk teams. Just tell us what the policies are we need to hear. Don't tell us how to implement it, because they're telling us how to implement the way it was implemented in a data center. And they – fellas, we need to go see Google's data center. Well, you can look through a glass and see lights, but you can't go touch a machine, and would you want someone else's regulator to come in and touch our machine? So, there's a lot of coaching to just tell us the policy, and we'll bring you how we implement that policy in the cloud, and that's a big differentiator.

**Kieran Norton:**
Yeah, you can object, right. There's always a dialog like is the implementation sufficient in their mind. That's completely fair, but you're right. I mean, you're not going to go do a walk around at a data center. Unless something's changed, none of them are actually allowing that, so that's just something you – that's a risk you are going to live with and you'll seek assurance around that risk in other ways.

**Mike Kavis:**
All right, gentlemen, great conversation. We have to wrap it up here, but appreciate the talk. Hope you enjoyed the show this week. It's been enlightening. That's it this week for Architecting the Cloud from San Francisco. We'll see you next time. Thank you.

**Operator:**
Thank you for listening to Architecting the Cloud, part of the On Cloud Podcast with Mike Kavis. Connect with Mike on Twitter, LinkedIn and visit the Deloitte On Cloud blog at www.deloitte.com/us/deloitte-on-cloud-blog. Be sure to rate and review the show on your favorite podcast app.

Visit the On Cloud library

www.deloitte.com/us/cloud-podcast