accenture

CIO 24/7: CLOUD SECURITY PODCAST

AUDIO TRANSCRIPT

Don: There's just a level of innovation that's going on in research and development that would be very difficult to keep up with if you were doing it on your own.

Jen: Hello and welcome to our Accenture podcast on cloud security. I'm Jen McHale-Bryar, director of operations excellence within Accenture as Global I.T., and I'm excited to explore our cloud story today. With over ninety five percent of our applications in the cloud and clients across the globe, we know how important it is to ensure that our data is secure at every step along the way. Our story is powerful and we've learned a lot throughout our journey to the cloud. Today, I'm excited to dig into cloud security with two of our own Accenture experts: Don Galzarano and Simon Gooch. Don, will you start?

Don: Yeah, sure. Thanks, Jen. It's good to talk to you and Simon again. My name's Don Galzarano. I lead our intelligent cloud in network practice here at Accenture CIO. I transition in the space recently, after working in infrastructure services for Accenture, where I saw the power of the cloud firsthand, I was responsible for the Microsoft Teams implementation, which really served us well through the pandemic. I've always been excited about the cloud and really happy to be part of this practice and I'm excited to be here today. Simon, you want to introduce yourself?

Simon: Thanks, Don. And hi, Jen. So, Simon Gooch here. And I'm the global identity and access management lead. In this role, I have the responsibility to ensure that all of the CIO services are a minimum meeting the information security, security policy and standards. But I'm also driving the future security strategy for all of the CIO portfolio.

Jen: Great. Thank you both for being here. Let's, let's dig in. I first want to go back in time to about seven years ago when our own cloud journey began. What happened to the concept of security when you migrated applications to the cloud?

Simon: You know when we first started our cloud journey, this was a lift and shift activity. So in that first phase, the only real change was that rather than owning the infrastructure or the environment that all of our technology was housed in, we handed that over to someone else. Everything else remains the same, the kind of technology that we were using, the way we used it, none of that really changed. So the big value in that initial phase of the transition from a security perspective was that actually we were handing over the securing and running of that kind of cool ecosystem, that core environment to some very big organizations who were in the business of doing that and doing it securely for some of the biggest companies in the world. So they were invested in making that as secure as possible. But from a security perspective, actually, we were giving it to experts to manage that. So that was actually a positive shift. And it really did offset any of the perceived risk around handing over control and not necessarily having some of the insight that we might have had previously.

Don: Yeah, that's right, Simon. And I think that the fundamental shift that we had to adjust to was, you know, we really moved to a shared responsibility model and previously running all of our own infrastructure on premise. And we were solely responsible for our security and the mindset that we that we are now going to share that with a third party. I think it's something that

we had to adjust to. But if you think about running in the cloud, it's very akin to, you know, an automaker, for example, right, that relies on OEMs to provide the parts for the car. So, you know, they provide the parts. The parts have to be high quality, but at the end of the day, you're responsible for assembling them and creating a well-functioning automobile. The same sort of exists in the cloud when it comes to using their services and using them securely. Right. So they provide you with a number of different, very powerful services that can be used to achieve business objectives. But it became our responsibility to use them responsibly and to adjust our security model and our security practices in a way that adjusted to that shared responsibility model.

Jen: So it's great. We're actually, it sounds like we're getting more out of our cloud native security services than if we were doing them ourselves. And so, And you mentioned strategy. On that security strategy, how did that change as we began migrating to the cloud?

Simon: It changed because it enabled us to really rethink and evolve our strategy, and that was driven by what is the future of our services. What does it mean in terms of, you know, how are we going to run applications and products in the cloud? And that's that's evolved over the last few years, so we could start to look at what that meant and then we could start to think about, well, how will we need to secure in that different way of running that the cloud is now enabling? So that's that's kind of, you know, that's a fundamental driver for changing our strategy. But on top of just changing our strategy to align to the broader I.T. roadmap, it also enabled us because we're in the cloud with security as well. So we're not only securing the things in the cloud we run, we have an intent to always run our security products and services in exactly the same way. And because of that, we were able to start thinking about, Well, how can we take advantage from a security services perspective, but also being in the cloud? How can we look at the new services that are evolving and consume those to align to the broader technology changes that are coming? So I think, you know, all of those things kind of come together and helped us really accelerate the development of our security strategy.

Jen: Can you maybe, Simon, go back to something you said earlier? Just give us a little more thoughts on how do we know that our cloud providers are actually secure?

Simon: We have to secure this stuff originally. So what we did was we looked at what we required in terms of the security of the environment when we run it and the services, and then we just built those requirements into the way that we define the services with the providers. So we were able to really go back, look at what the requirements were and then build them into the contracts that we signed with these providers and then obviously make sure that we had the appropriate ability to kind of audit and ensure we were getting the security outcomes that we were having them sign up to.

Jen: Great. Now that helps, I guess I'd like to ask each of you your opinion about what's truly different about the cloud. Don, maybe you first.

Don: Well, what's different about the cloud really is the flexibility that it gives a business across the board not only to serve the business faster in a more agile fashion but also in a way that it can drive value that you really couldn't do on premise that allows you a level of control over your consumption that you don't have on premise. It allows you to innovate at a much more rapid pace. And I think most importantly, is if you think about the amount of investment that the major cloud providers are making on an annual basis, there's just a level of innovation that's going on in research and development that would be very difficult to keep up with if you were doing it on your own. So it really does unlock an entirely new world of opportunities for your business to move faster, to be more nimble, to be run more cost effectively and also to be more sustainable.

Simon: Yeah, I'm not. I'm and I agree with Don. I mean, the bit about because the provision of services is that focus in terms of their cloud providers. The investment that they make is really concentrated. So the effectiveness of that is, you know, is really powerful.

Jen: So let's ask both of you, what are your guiding principles for cloud security today? Don, you want to go first?

Don: I think I'd like to start that with a phrase that's being more commonly adopted in the industry, which is identity is the new firewall. You know, over the years, this concept of security and security in the data center was always anchored to, you know, creating, you know, using firewalls, creating a barrier between your data, your applications and the bad actors. And what we know now is that the bad actors are becoming more sophisticated and the cloud is more sophisticated. So what I anchor to is that we are identity centric, meaning that our access is all based on identity and getting on to a network, for example, no longer creates an implied trust, right for an end user or an application, for that matter. So identity is at the core of all cloud security today. From my perspective.

Jen: Simon anything you want to expand on?

Simon: I think that whole kind principle is identity does the control plane is interesting and I talked about trust, and there's this concept of zero trust. Zero trust doesn't mean that we don't trust anything. What it means is that we repeat the cycle of trust or validation. So don't give a great example in terms of just because you're on the network now, that network no longer means that you can do anything you want, right? That's the concept of zero trust so that the point at which we ask you to validate who you are, what your state is, what your intent is. And check that you can perform the actions that you're trying to perform. That's, that's the zero trust concept. That's a thing that's now fundamentally driven by identity and role. That's a core principle and tenant of everything that we're enabling in the cloud is probably worth just describing what we mean by zero trust. And I actually think to some degree, the term zero trust is a bit misleading because it doesn't mean that we don't trust anything. It means that we have this constant process of validating and understanding a state, an activity and making sure that it's appropriate. So that's not no trust. That's constant trust checking. And I think that's that's important to understand because we work in the cloud in this ecosystem where we have enabled, you know, many more channels of access and consumption. And there's a lot of interactivity now behind the scenes so we do need to make sure that we have this concept of zero trust, which is the constant validation between systems of points of access of activity of people and then really kind of layering on top of that zero trust principle, which is that constant validation is the key component of the validation, which is tied to, as Don mentioned, your identity. So who are you? Is a key part of deciding what you should do, what data you should have access to. That's worth just understanding as a principle.

Jen: And with our move to cloud, sounds like being able to have that kind of identity got a lot easier than if we were trying to do it on prem by ourselves.

Simon: Yeah, it got a lot easier there. There are a lot more tools that we can bring to play, but to some degree, I'll move to cloud accelerated the thinking about, well, if you don't own one of those controlled planes, how do you ensure that you understand that there's an appropriateness of activity? So that acceleration of the thinking is a key part of the move to cloud it, I think yeah.

Jen: Excellent. Thank you. Thank you both. Don, anything else you want to add here about the future of cloud security, anything you've seen?

Don: Well, I just wanted to kind of go back to the power of the cloud just very briefly and just sort of give our audience a scale of what that really looks like. And if you think about what you would have done on premise, the major cloud providers are collectively spending in the tens of billions of dollars per year, right, to innovate, right? And to bring new security solutions, as well as new offerings for hosting. So just wanted to kind of touch on that right? The ability to sort of keep up with that on premise would be very, very challenging for any individual organization. So some very exciting things are happening in the background as we speak.

Simon: Yeah, and I think, Jen, I mean, because I've talked a lot about kind of zero trust and identity as the control plane, but there's a new for me, there's a new kind of. Evolving aspect of being in the cloud that's tied to identity because we've got completey new concept of identity and identity, identities and identity attributes in the cloud. And we need to think about how do we tie all those together, how do we

understand, you know, as a, as a developer in the cloud, across multiple, potentially multiple cloud providers, multiple systems, you know, how do we apply? How do we apply some of those zero trust principles and rules? So there's that there's a real evolution coming in terms of the actual identity concept, not, you know, not the use of identity as the control plane, but the the construct of identity. And what are the different aspects of it? You know, how does it become a thing that can live between different services and different cloud providers? Because at the moment, you know, a lot of a lot of these cloud services has been built up based around the kind of. Their own ecosystem, so I think that's one of the big things that's coming is is the transport ability of identity constructs across cloud providers and cloud services. Yeah. And I think we haven't even really touched on this point. But, you know, similar to the investment talk track, right? Artificial intelligence and machine learning are also going to play a big factor in the future of cloud security. Each one of these cloud providers are getting billions of signals every day from around the world, and the AI and machine learning capabilities are becoming more and more advanced as computing power continues to increase. So, you know, the ability to detect anomalies in behavior and make rapid decisions to act on threats in the cloud. Right. We're going to see those capabilities grow, expand and become much more powerful. Responses will become much more highly automated and as well as the fixes to the problems themselves. So I think there's some exciting things on the horizon, Jen.

Jen: That's incredibly exciting to look forward to. I'm really interested in seeing how AI is going to pave the way in the future. So at this point, we've walked through our journey from beginning to now. If we look at it all in retrospect, I'd love to hear some lessons learned or advice you might have for those who are either starting out or currently on their journey to the cloud. Don, you want to take that on?

Don: The number, one thing I would tell the audience is that you can't really copy what you did on premise in the cloud. If you tried to do that, you will really struggle to achieve the full value that you're seeking. I talk to clients every day and I also talk to a lot of my peers who are in different phases of their of their cloud journey, and we often hear the term, for example, lift and shift right from the data center. And I think that's kind of a legacy term, but it's really about lifting, transforming and landing right? Your workloads into the cloud because you're really different, dealing with two very, very different operating models, sets of capabilities and ways of thinking about how you run your business. Really think about when you go in your cloud journey, think about the destination and not trying to recreate what you had internally prior to the start.

Simon: And Don mentioned earlier on again, right to do those things. That's not a technology change. While it is a technology change, but it's not just a technology change. That's a cultural change. That's a potentially skill set and a people change. And you have to factor all of that into your journey and you have to be prepared to transform the way you work, the skills your people have. Otherwise, you won't extract the value that you can extract as you're on that cloud journey.

Jen: So that brings us to a good question, this cultural shift. Can you tell us a little bit about how you did that cultural shift and how that played into your ability to be successful in the journey?

Don: Yeah, I think it's for us. It started again at the beginning, and the first big shift was convincing everyone that the cloud itself can be secure. There, there, there was and can be not across all organizations, but in some. The idea that you're handing over everything, your security, your data to a third party, and there's a lot of fear that can be generated in that process. So the first thing right in terms of changing your culture is changing that mindset that you know you have to have everything under your control in your, in your backyard, I guess for lack of better words. That's the first big thing. And and that comes with education and really understanding the benefits of the cloud and how you can really adventure security posture right by leveraging all of its, all of its different capabilities. And then secondly, just changing your organizational culture around how you operate, how you secure, right? And, and all of the things that you used to do, all you know on

premise, right? You really have to rethink those and start, start from the beginning again, because what's on premise is completely 180 degrees different than what you're going to have in the cloud. And designing with that end in mind is key.

Jen: Simon, anything you want to add maybe specific about our security controls that the vendors provide?

Simon: Yeah, I mean, there's a, I mean that that is definitely part of the culture shift. The culture of partnership and trust it is, is important in that kind of transformational journey. So you know, you're going to be handing over to Don's point, you know, a lot more of the things that you use to control other parties. So, you know, you have to understand, well, how do you define the. The things you want to see from those providers and the kind of controls you want to see that are appropriate to how you then consume the service, so yeah, that's a that's a cultural mind shift change in the way your organization thinks and works.

Jen: OK, well, thank you both. I mean, definitely sounds like a cultural shift that requires real leadership from the top. Don, Simon, I really enjoyed our conversation. Thanks for your time today and talk to you soon.

Don: Thanks, Jen.

Simon: Yeah. Thanks, Don. Thanks, Jen.

Podcast Close: Thank you for joining today's podcast. Be sure to subscribe to the Accenture CIO Podcast Series on Apple Podcasts or Spotify. Find the full CIO 24-7 podcast series and additional ways to subscribe at Accenture.com slash CIO podcast.