Episode 47: "Never trust, always verify"

Fri, 10/2 8:37AM 40:31

SUMMARY KEYWORDS

trust, cloud, identity, security, ashwin, requirements, talk, vendor, chris, concept, technology, access, customers, prem, user, control, call, application, microsoft, important

SPEAKERS

Warren du Toit, Chris Goosen, Ashwin Pal, Nicolas Blank

C Chris Goosen 00:19
Welcome to the cloud architects podcast, a podcast about cloud technology and the people using it.

N Nicolas Blank 00:26
The cloud architects podcast is sponsored by Kemp Technologies. Choose Kemp to optimize your multi cloud application deployments and simplify multi cloud application management. A single pane of glass for application delivery, Kemp provides a 360 degree view of your entire application environment, and even third party ADCs. Download Kemp360 for free today at Kemptechnologies.com Hello and welcome to another episode of the cloud architects podcast. I'm here today with my co host Chris Goosen. Hello. And we have a very special guest today is going to talk about something that's wonderfully contentious. And I'm going to ask Chris to introduce our guest twice today.

C Chris Goosen 01:14
Yeah, absolutely. I'm excited about this topic actually. And I'm super excited about the person we speaking to. So we are joined by Ashwin pal, who is the director of cyber security for the APAC region at unisys. And Ashwin, I actually go back really long time he was the really the the reason I got interested in cyber security in the first place. And so super excited to have you actually welcome.

A Ashwin Pal 01:36

Thank you, Chris. Great to be on this and great to reconnect man. It's it's been it's been too long.

C Chris Goosen 01:42

It has it's been, it's been a really long time. I think we could probably trace back the last time we saw each other at some pub somewhere in the rocks. But we won't go into that on this episode. So as a means of introduction, do you want to tell the folks listening a little bit about yourself and what it is you do?

A Ashwin Pal 01:57

Yeah, definitely. So obviously, actually, Paul, and I run the cybersecurity business for unisys across Asia back. Been in Australia now for 13 years. But I'm a kiwi and been doing this for 20 years now. So, you know. Yeah, there isn't much that I haven't touched around the Sophos cybersecurity space.

C Chris Goosen 02:19

Right. And, and the the contentious subject that I think Nick was referring to is a zero trust. Right. I think we hear that. We hear the phrase, I'm soaking in zero trust a lot, lately. Yeah. Right. And I think maybe, probably the best place to start is to probably unpack exactly what that means. Because I think what I've found is in talking to folks in talking to customers is there's a real misconception around zero trust, you know, some folks think it's a product. Okay, can I get me some of that zero trust? You know, I think there's a real misunderstanding in the sort of in the industry as to what it means and what it is who many people have takes on it? So can you help us kind of unpack a little bit about you know, at its core, what it is?

A Ashwin Pal 03:03

Yeah, totally man. And, you know, you are pressing my buttons again, as as you used to when you were a cleaner Australia. So, unfortunately, you talk to anyone, right now, any other vendors, they've got their own definition, right. And zero trust came out of Forrester. So I get along really well with the APAC head of security at Forrester. And, you know, she, she's running a server right now. And one of the key points that if let's actually come out from the survey with silos, it's just a frustration around the multiple definitions of zero trust. So zero trust, it's a philosophy, it is not a tool, okay? It's it's not a particular

technology, it's really a way of actually implementing cybersecurity in an organization. It was actually founded by john can divide. It's for us to go in 2010. And, really, the principle effectively states never trust, always verify. That's the key thing thing. Now, what that effectively means is that any user or application, any device that is actually coming into your organization, any one of those needs to be authenticated properly, needs to be authorized, you need to implement very, very limited role based access controls on a need to know basis only. And you're consistently authenticating, authorizing them. And at the same time, you're using a myriad of other technologies to make sure that you are watching the behavior. You're watching their security posture, you're looking at other contexts and other data sets, things like threat intelligence information, you know, through things like security, log monitoring, etc. To make sure if anything actually goes bump, you actually kick them off in order grammatically that should actually happen by itself. Now, interestingly enough, about two weeks ago now, this has actually released its paper on zero trust architecture. And they have discussed a lot of these concepts. Now one of the concepts that actually they have talked about in there is one of control plane and data plane. Right. So data plane is basically so you segregate both areas. data plane is actually where the data travels control planes effectively, we actually implement access controls or authorization controls. And that's how you actually control access to the underlying data. And you're basically segregating both of those. So when you talk about zero trust, there are multiple ways of implementing it. The segregation that is that I'm talking about, micro segmentation is one of those that I'm most familiar with, to be honest. But at the end of the day, so long as there is a separation between the control plane and the data plane, and you are consistently authorizing authenticating your users, your applications, your devices, establishing the trust, maintaining that trust, through constant posture, checking, behavior, monitoring, and encrypting the data on the wire, that's quite important as well. That's what zero trust will give you. And as I say, you can hear it in what I'm saying. It is not a tool of technology, it is a philosophy. And it really depends on how you implement that in your implement that in your own environment.

N Nicolas Blank 06:31

As well, Ashlyn, I have to ask, I think it's really easy for us who have been around for a long time to hear authentication and assume identity, right? So you approach my application or my service, and we're going to constantly ask you to verify who you are through whatever methodology that we have. However, what is zero trust mean, when we get to the the actual wire of data on the wire? And how do we do zero trust in a physical environment like a layer two, layer three, all the way up to layer seven, where I'm talking zero trust across clouds, zero trust towards my data center? How do I do that in a practical manner? Without vendor locking? Impossible?

A **Ashwin Pal** 07:17

No, no, no, no, no, no, no, no, it is absolutely possible. In fact, you should abstract yourself from the vendors. So what you should actually be doing is coming up with a strategy, which is, you know, not technology focus. So the key components that actually just spoke about, you know, you start off by thinking about what those key components are, and how you would actually address those key components, the core aspect here, and I like the fact that you actually talked about the OSI model, because I would actually walk away from that and actually talk about identity itself. Identity is the new permanent, okay, because what is a network? Where is your? Any answer? You can't, it doesn't exist, you know, even with Cloud is anybody using one cloud, no people multi cloud. So if you abstract yourself from the network layer, or any technology for that matter, and focus on the core principles of zero trust, which actually just mentioned, at a strategic level, and then drill down, try and achieve those outcomes, that's how you would actually achieve zero trust. So if you took that identity piece, right, and anti role based access control, just to those identities at an abstract layer, it doesn't matter where the identity goes, whether it's in your network, whether it's in your home, and that's very, very relevant now. Particularly with respect to working from home remote access, and all that stuff, or whether it's actually in the cloud. And again, that is very important now, as well, because a big part of this COVID working from home shift, his people are working from home now. And a lot of the data is actually now in the cloud, so you can access them easily. Now, if you take the concept of their identity, which stays the same, doesn't matter if it's on prem, whether it's in the cloud, whether it's in your home, you tie your access to that identity, and then enforce quite strict role based vennela access controls. That's how you establish that based on the identity, and that's how you restrict the access.

N **Nicolas Blank** 09:25

Okay, so what I'm hearing you say, is, forget about the new trick. Just don't trust it, and put something else on top, which is completely not network related in any semblance. And what we're going to pivot off on everything is identity.

A **Ashwin Pal** 09:43

Hundred percent, because at the end of the day, how far does your network extend? Can you extend it into Azure Cloud getting extended into Google's cloud? Can you extend it into AWS? You can't Can you extend it into people's homes? Not really, right? I mean, we've got a situation now where there are multiple users coming in from their home using the BYOD machines because not everybody had a laptop. So when they actually went home, that could not procure laptops. I know for a fact Dell, Lenovo, all of these guys literally ran out of laptops, you couldn't buy one. Okay? The option was, okay, cool. We'll

set your home laptop up to actually come in. So now all of a sudden, you're using BYOD machines coming in over an insecure wireless connection straight into your network. Yeah, you trust that connection? Are you going to trust that endpoint? You see what you see where I'm going with this

N Nicolas Blank 10:35
is a

A Ashwin Pal 10:36
challenge that you are trying to address. And frankly, zero trust is the answer. I love, you know, making predictions and just being controversial with neuro cruces Easter, which is always loving. One of the things that I've actually been saying is, you know, zero trust, frankly, last year was a pie in the sky concept. With the whole COVID thing, it's basically giving it a shot in the arm. I can't I guarantee you, within three years, a lot of organizations would either be working towards zero trust, or would seriously have it on the roadmap, zero trusted if you're not easy to put into place. Because there are a number of challenges with regards to compatibility with legacy environments, change resistance, except, you know, time and cost all of that stuff. So you'll need to eat the elephant. Hopefully, there aren't any alpha blockers on this call. In bite sized chunks, right. And that's, that's what you've got to do. But at the end of the day, people simply have no choice now with the work from home stuff with the move to cloud. And trust me, not everybody's honey, anyone's going to come back into the office full time anymore. The whole working from home stuff is here to stay. So you've got to have, you've got to have a response to that business challenge. And zero trust gives you a pretty solid answer.

C Chris Goosen 12:02
So so. So what I what I like about what you've said is because for the longest time, I've been preaching that the identity is the foundational component of any move to the cloud, right? Whenever we talk to customers, I spoke to add a late customer call yesterday, where they tend to get so fixated on the fact that they need to move data from on prem to, you know, on premises servers into a cloud environment, or they need to enable this feature in in teams. And then you take the wind out of the sails when you say, well, hang on, have you thought about your identity? Oh, well, what do you mean? Well, people need to be able to log into stuff. And that really is like, if it's like building the house, right? You can't do it. Without doing that foundational step. I kind of experienced the same thing, because during COVID, I was trying to get a new laptop myself. And I ended up having to use a use a Windows machine for a little while because my Mac was an order, and it just

took forever for me to get it. Right. And it's the same situation like vendors everywhere we're having having issues with this. And unfortunately, you know, I was able to continue working with without problem but you know, you're right. I think this this new norm, this new shift, this is interesting. So I what I wanted to pick on, or at least what I wanted to ask, I had a couple of questions. Now the first one's gonna be a little bit more controversial, right? You're up for? I've heard a lot of talk about something that Google calls beyond cope. Yeah. And and and it comes up a lot in these kind of zero trust type conversations is just is this just Google's branding on some of the same concept, though, is this something that they're trying to turn into? Okay,

A **Ashwin Pal** 13:44

so that's in TNA. Here we go. Now I'm going to start throwing four three letter acronyms at you. That's zero trust, zero trust network access, it is a it's a piece of the puzzle. It is absolutely not completely zero trust on its own. Right. So effectively, what beyond Corp does, and you've got z scalar, that have got a similar technology as well. And, you know, effectively allow secure remote access to certain applications. And the access is tightly controlled, and the applications are not exposed until such time that you actually need access to it. That's effectively it in summary, right. So that's what beyond Corp is, as I said earlier, if you go back to my initial definition, zero trust needs to be holistic, it needs to cover any device anywhere, any access methodology anytime, right? So zip DNA is a piece of the pie. It is not the entire pie. Okay. Very interesting. And the other, obviously, just add to that, Chris. The other thing you've got to be very careful about is vendor locking. Alright, so we spoke about that earlier. And there was actually one of the questions, what you've got to think about is that if you go with a particular vendor, in this case, Google, you know, what are your limitations? What can you do with them what you cannot do without them? And is it going to lock you in and actually prevent you from, you know, implementing the access from, you know, a place where there might not actually exist or something like that. So, again, you've got to be very careful about vendor lock in. And as I say, don't start with a technology. Start with what you want to achieve your and then go from there. That's key.

C **Chris Goosen** 15:36

Yeah, definitely. Sounds like it's so the second sort of, I guess, tack on question to that. We're talking about the identity. It's the key part of that. And you're you're essentially wanting to authenticate based on all of the data points that you have, right. And so when we, when we look at something like conditional access, I mean, is it okay, just, you know, a common a common situation, when you when you use conditional access is to say, Well, if we can identify that we have a known device, and we know the user user credentials, we

trust the user credentials, that we can be a little bit more relaxed around how we, you know, sort of know two factor, for example, right? And maybe we allow that person because it's a trusted identity, it's a trusted device, we can allow them access to some really sensitive data. Whereas that same user identity coming from grandma's device, or, you know, a McDonald's network that we've never seen, maybe we want to do a few more things, right. So would you say that something like conditional access kind of plays into this? Or is a key kind of building block for it?

A Ashwin Pal 16:38

Now, you've absolutely hit the nail on the head there, right? So one of the key issues around implementing zero trust is change resistance. Because, you know, let me take it a step back as humans, as organizations, we've always worked on the principle of trust, right? For example, I'm sure you guys have all heard, why would you hire someone if you don't actually trust them? Right, their trust is effectively going completely against that. Now, just to be clear, we're not saying that we don't trust our employees, what we're actually saying is that depending on their risk profile, and it is related to everything you just said, you know, we want to be able to make sure that we can verify before we can actually trust, it actually makes sense. It's a bit like, you know, someone's actually knocking on your front door. They've got a helmet on. Yeah. What do you mean, do open the front door? Because at the moment, the way network access actually works is that you know, you come in and Chris, you know, this, you know, you either get a wired or wireless connection onto your network. By the time the login prompt comes up, you're already on the network, correct? Yeah. What you've just done is you've actually let this person with a helmet on into the house, you've opened the front door, they walked into the house, and then you go, Oh, are you? Okay? Right, what we're saying is basically keep the door shot, make sure this person pulls the helmet off. And if you know him, let him in it, don't keep them out there goes back to what you just said, right? It's all risk based. So if the person has an issue wearing a helmet, you can see their face happy days, the risk is lower, you will actually have lower controls in place. And you'll let them in because you've got to be very, very careful and Cognizant, off, balancing user experience with enhanced security. And that's always the friction when it comes to cyber security. And that's where risk based decision is very, very important. And then if the IRS, you put further controls in place, and then once they're actually in a key aspect of this is user and entity behavior analysis. So you know, constantly monitoring, you know, what this user is doing, what this device is doing, and whether it actually matches what you would actually expect. And if it doesn't, then hopefully you've got an automatic control to either kill their access or limit their access, because that could potentially mean that something's changed. You know, we've got a man in the middle attack or something like that, that has actually happened, obviously, with men in the middle is, you know, it's a case of a valid user session has just

been hijacked by somebody who is nefarious. So you know, it is risk based. But having said that, you still need to make sure you actually have controls in place that you can constantly monitor and control that very session until the end.

N Nicolas Blank 19:35

I want to just ask them continuous question asked another contentious question. And we spoke about identity, which is wonderful, and I'm completely on that bandwagon. But then, both of you very quickly, Chris, you started off talking about Microsoft Azure Active Directory, conditional access and Ashwin, you didn't bat an eyelid we just go with the flow. There is only one identity provider and for four years for decades, in fact, on premises, it made sense that we would use Microsoft Active Directory. And our users are spoiled because we obfuscate authorization and authentication, one package and particularly with Kerberos. Life has just, you know, it's great and it works. And but then we go to cloud, right? When whose identity model are we talking about? We're still talking about Microsoft identity. And so, let me ask you, Ashwin, I want to ask you a question that a customer of mine asked me, he said, I am concerned about vendor locking. Okay. But what have you literally for 20 years been running in your data centers as well, Microsoft Active Directory, but now, now that I'm going to cloud, I'm concerned, because people have told me about this thing called vendor locking. Yeah. And how do I not get locked into Microsoft Azure Active Directory. However, the other side of the coin is, I don't see anyone else doing conditional access, and doing what Microsoft is doing, that can at least from the outside, in, do that thing of Who are you and where you from? At the same time before I'm going to let you access my service? Right? So

A Ashwin Pal 21:27

how do we answer that question to the market? Absolutely. And and so color responses to that one? Obviously, you recall, I talked about control plane and data plane, right, which is why we started off and discussed the concept of the control plane, the control plane effectively abstracts all the technologies, right. So I have a control plane, which actually enforces authentication authorization, I don't really care where the identity store is where it's coming from. And that's literally, you know, what, what we've actually what we've actually done. So, you know, on prem use ad, as an example, I don't care in the cloud, where you've got workloads, which actually running and don't have connection to your ad, internally, stand up a simple PKR infrastructure, basically use certificate based authentication and that privacy identities for those workloads. So as I said, you know, you've got to be, whenever you start with this, you've got to start with the concepts, the building blocks, and make sure you're actually addressing the building blocks, as opposed to coming in from a technology angle. And it's a very valid point, because yes, you're right,

Chris actually did go down the technology path. But you would have noticed I keep pulling you guys back away from technology. This is not a technology conversation. This is a concept of philosophy called conversation, whereby you'll actually have building blocks from multiple providers that you would then pull together based on the various components of zero trust into a into a cohesive architecture that is then void. So makes sense. And the example I've just given to you mixes up your own Pico infrastructure, which you would have set up in the cloud as an example. And on prem, I don't care.

N Nicolas Blank 23:20

I'm sure you guys would have had the same discussions with customers when we asked them. So let's have the security discussion. They say, oh, mate, I'm secure because I have been to whoever that is, right? And you think But hang on, that's a vendor, that's not a framework. That's not a strategy. A. And when I used to work for a migration vendor, it was also management vendor, I used to talk to my customers and say that software is not a process. software enables a process. And if you were talking to a customer who's in cloud, wants to go to cloud, because to be fair, we still have customers who are in cloud and immature, right. And that's not from a security posture that's not from a mental point of view, or customers who are still evaluating about going to cloud for the very first time. What would you say to those folks?

A Ashwin Pal 24:16

So I mean, in terms of migrating to the cloud, you've got to you've got to get the basics, right first, right, like and again, what is your security posture? What is your risk posture? You know, do you have policies around your minimum cybersecurity standards? It's those things that come into play. I mean, if you look at any one of the cloud providers, they provide security in the cloud, some of it is pretty good. So often, it's pretty average. But at the end of the day, it's a bit like going to a restaurant and somebody gives you a menu, right? You've got all these things that you actually can put in place or eat in this case, it's up to you. It's like, what do you want to eat and how hungry you are? It's exactly the same concept. It's actually not about you can't and you shouldn't start with With a technology conversation, it's going to be about your requirements, etc, etc. And then if you are specifically looking at zero trust, zero trust is one of those beautiful things, which allows you to push your security, you know, based on what you've talked about, into the cloud, that you can control and is actually equivalent to on prem security. It abstracts you from the security that is provided by the cloud provider. I'm not saying you don't use it. In fact, you should. But you know, the concept of security about multiple layers, right? So if there is an issue with the cloud provider, there was an issue with Amazon's cloud director, not long ago, right? There was a vulnerability found now if you actually have the top issue. But if

you actually have a zero trust philosophy in place, whereby you are controlling some of the security yourself, and you have allowed minimum security based on strict authentication, then you have a degree of protection. So those are the things you actually have to think about. But it does come down to, you know, what are your minimum standards around security? what is acceptable from a risk perspective?

C Chris Goosen 26:11

I think, I think it's a very important point, because I always pick on Nick, because he has this phrase that he uses a lot called requirements. elicitation, right, because you don't just gather requirements up like they're, you know, puppies. And, and so I think that's important, because I've had a lot of conversations with customers, specifically security conversations, where they go, Well, we need to secure this thing. And you're like, Okay, well, what is your risk profile? What what are the what's important to you, from a security perspective? What are your requirements? And they go, Well, I don't know the product. So I don't know what it can do. I was like, Yeah, but that's, that's not the question I asked. Right. The question is, what are your requirements? Because we will tailor the product to do you know, the platform to do what? What? meet those requirements. And so you get into this sort of chicken and egg situation where someone standing there with their arms crossed, going, Well, I need to understand what the what features it has and what it can do. Well, that's not really the discussion we're having. Yeah, you need. Yeah, you know, we need to talk about what and I think the other part of this is the concept of, you know, folks tend to sometimes overthink this as well, right? They go into this sort of analysis paralysis, where they want to end up spending significantly more to protect something than it's worth, right. And that in itself is a good idea, either. So it's very important to understand, like, if you if you have things that are not that critical, or our budget public, you know, publicly categorize documents, for example, right? Does it make sense for you to go down this like, super deep path of putting all of these crazy security controls in place? When if that thing isn't all that important to begin with? So understanding that risk profile and understanding your requirements very, very important to this whole discussion? That was my long, roundabout way of getting to that point.

A Ashwin Pal 27:56

I completely agree. Because that's really where the conversation actually needs to start. If you're starting a security conversation with technology, straightaway, the red flag goes up for me, because yeah, you're gonna end up in a very wrong place.

C Chris Goosen 28:12

Yeah, you're almost ticking feature boxes at that point, right, trying to make Features Fit and go, Oh, well, we bought this license. Let's make sure we're using every single one of those checkboxes on the feature list. Yeah,

N Nicolas Blank 28:23

yeah. Yeah. And I use the word elicitation. Because, well, for one thing was taught to me by a business analyst who was fantastically mature in this whole discussion. And how he illustrated it to me was just like Chris says, this requirements online in the ground, fast to pick up because, you know, otherwise, it would be easy. And I roll when we engage with customers. And to me, our customers is anyone who has this kind of conversation and could be an internal or an external role. And for us as an external role, we would go and wrestle with our customers. And it's kind of like standing with our feet on the shoulders with a pair of pliers trying to pull these requirements out of their mouth, because it's not an easy discussion. It's a case of, let's stop talking about this feature. Let's go back to what is our need, what is what are we trying to defend? And very often, when we talk to senior folks in the business, especially the C suite folks who've been marketed to by vendors, they will say, and I'll take the conversation back 20 years, I want a Blackberry. Well, why do you want a blackberry? Well, it's cuz I went down to the pub was living in London at the stage. So I went down to the pub, and Mata, my friend who's a director works for this other company showed me his Blackberry, it's cool. Now whatever is at the back end, can you make that work? But that's not a requirement. So if if we didn't walk them forward to do you need mobile collaboration? Oh, yeah. Well, do you need secure mobile collaboration, and then we take them down that path of let's articulate what it is that we need that in your head is aligned to a feature. But you saw that feature, and you thought, I need that. Because that makes sense. But let's turn it back into something that we can then defend, from a requirements point of view. Yeah,

A Ashwin Pal 30:23

yeah, absolutely. And, and that's the critical part, like every conversation needs to start around, you know, what is your risk appetite? Where are you in relation to your risk appetite? So what is the current risk posture? And, you know, how, if there's a gap, then how do we actually get there, and you know, you look at the building blocks. Now, obviously, a key part of that is you need to understand where your information assets are, and how critical there because that's what's going to drive the security controls. But you've also got to throw into the mix, how the threat landscape is actually changing. So for instance, if you look at what I just said, the massive the move with working from home, effectively changed the threat landscape, you know, for the worse, the whole environment became a lot less controllable, because people were in their homes, BYOD machines,

insecure wireless, what I spoke about earlier, then you've got to take a step back and think about Alright, so how do I actually secure this? Like, what? What access is required? What's the criticality of the data being accessed? Where is this data? And you know, is zero trust a good way to go? Those are the questions you would actually ask before even going down the zero trust path. Going back to what Chris actually said, and I know this is an absurd example. But just go with it. You know, if you've actually got users that are constantly coming in, looking at publicly available information and doing stuff with it, they're who, you know, the controls that you need to put in place is going to be much less However, if they're coming in. And if they're actually playing around with the formula for Coca Cola. Yeah, you might want to think about zero trust in that case.

C Chris Goosen 32:12

Yeah. That makes sense. So, um, last question, I guess, for me that I have is resources, right? Let's say someone's listening to this, they're going, Okay, I understand that zero trust is a methodology or a, you know, a mindset as opposed to a product that I can go buy off the shelf, right, no matter what vendors are telling you, it is not a product. But I want to learn more, I want to I want to understand how I can implement this in my environment or for my organization, or there's some, like other good resources available for folks to go and skill up, or at least, you know, get better acquainted with this. And something that isn't completely kind of marketing skewed.

A Ashwin Pal 32:53

I was gonna say, I could give up my email address, but I won't

33:00

expect Dilbert.

A Ashwin Pal 33:04

Jokes aside, two things come to mind one. And thank God, NIST actually has written the zero trust architecture paper, I would, I'm in this to convert. And I go go to NIST for all of my references. First off, that's probably the one that actually referenced most, because it's obviously vendor agnostic, right. And, frankly, I've written a white paper on this, and you won't believe it. I literally wrote it over Christmas, because I was getting so frustrated with seeing all the different zero trust definitions coming up, I will start I'm going to write my own paper and define this once and for all

C Chris Goosen 33:44

the different time to rule definitions. How am I going? How can I do know about this? In all of my research for this episode, I didn't even know about this. So is that something we can share in the shownotes? It's publicly available paper?

A Ashwin Pal 33:57

Yeah, hundred percent. Man, I'll, I'll flick it to you. After this and feel free, feel free to distribute it with this, go for your life. So it'll cover a lot of the concepts that I've actually spoken about. And, you know, these days, like I've discussed, not just your trust, but what are some of the challenges, organizational challenges as well as the suggested approach. So, you know, zero trust is it's hard to shoehorn or fit into a legacy environment, but a lot of people are going through digital transformation. A lot of people are actually going through cloud migrations, as we discussed earlier. Those are great places to start, because they're Greenfield opportunities and projects. The thing is, you've got to make sure that you're building security and zero trust is part of the entire process as opposed to towards the end and somebody goes, Oh, what about security? Okay. Yeah, yeah, that one before Henry

C Chris Goosen 35:00

I use that example on a daily basis pretty much because I've just discovered so often

A Ashwin Pal 35:06

start, and then it's a nightmare in a disaster, right? So you've got to make sure you're actually putting security in from the start. I mean, this is applicable to security as far as zero trust as much as it is to broader security. When you're actually thinking off a project, oh, my God, I don't understand why you actually wouldn't have security as a key requirement. So when you're doing that requirement, initial phase right up front, before you're even going to like project funding business guessing stage, it should be in there, you should be putting up security against your requirements. And then going ahead with the project, yeah. Mine to stick to your I trusted, and effectively, it's almost a case of land and expand, okay, you land here a trust into your your plan, migrations, your digital transformation projects. And then as your legacy environments are getting refreshed, you expand, you expand, you expand, right, it's a multi year, multi phase journey. But you've got to start somewhere. And as I said, a lot of this discussed in my short, sharp paper, which which I'll share after the call, and feel free to share that with the audience.

N Nicolas Blank 36:17

Yeah, absolutely. I just Chris, before we end this, this, just something I want to draw an analogy to and Ashwin, I'd like for you to, to agree or to correct. So if I'm putting my my Microsoft hat back on, one of the things that I gain from docs.microsoft.com is the cloud adoption framework for Azure. And one of the things I enjoy about that is that it actually is vendor agnostic. So for all of those Microsoft bashes out there, there's this free framework called the cloud adoption framework for Azure. And it addresses multi cloud. And one of the things that you get from that is the concept of building a minimally viable product from day one. And after we finish the envisioning phase of we go to the business and say, What are you willing to spend money on? Right? So what is this thing that cloud is going to do for us in a measurable way, we actually start with a governance framework. And governance starts on day one with an MVP. Now I've taken that methodology, and I've applied it to our productivity customers. So those folks going to Office 365. And after we do this envisioning thing of the cloud, we get the folks in the room. And then I look the governance person, the eye and say, you've just become the most important person in the room. Because without you, we can't move a single bite to the cloud without being compliant to whatever is important in your life. And this concept of going to cloud in a secure manner, including zero trust doesn't have to be the thing that says, Oh, it's going to take me 10 years to become secure, it means I'm going to start somewhere. And then I'm going to be iteratively more mature, as I take my minimally viable product, and iterate through that as I become more mature in my security posture, and become more mature in zero trust, so that I build something that I as an organization can sustain.

A Ashwin Pal 38:20

Yep. Well said, and I'm sure you guys know, Microsoft's my Microsoft is an absolute zero trust convert. Yeah, they taught So actually, they're on a multi year, zero trust, migration journey. Period, right? And then betting in the cloud environment, just just talking about Microsoft itself. So yeah, they're absolutely sold on the concept. 100%

C Chris Goosen 38:46

and if you're listening to this, and you want to know, one thing you can do to start today, turn on multi factor auth. Yes, that's right. That's where you start.

38:56

Yeah, so I'll get off

C Chris Goosen 38:59

my soapbox now. ashran it's been it's been an absolute pleasure catching up again and having you having you talk to us about this. If folks on the call want to reach out to you and and sort of get in touch and talk about zero trust or anything else security related, how can they How can they find you?

A Ashwin Pal 39:15

easiest thing to do is just drop me drop me a line. And my email address is ashwin.pal@unisys.com.

C Chris Goosen 39:26

Okay. And on the socials, you're on LinkedIn. Right I'll while on LinkedIn, so you can feel free to message me on LinkedIn as well. Okay, excellent. I'll put we don't typically publish email addresses but I'll publish a link to your LinkedIn profile. Just keep the spam out of your inbox. You know, do Mike do yeah. Yeah. Well, look, thank you very much. And yeah, we'll look forward to possibly having you back again sometime in future.

A Ashwin Pal 39:51

Yeah, man. No worries. Any any any topic I'll give an opinion is you know.

N Nicolas Blank 39:56

Awesome. Thank you Ashwin. Thanks. Eyes.

W Warren du Toit 40:02

Everyone. Before you go, we just wanted to say thank you for listening. We really enjoyed putting this podcast together for you every two weeks, please visit us at the architects cloud. Alternatively, drop us a tweet. We'd love to hear what you have to say at the cloud Ark.