accenture

EPISODE 2: SECURITY

PODCAST TRANSCRIPT

Barbara: Welcome to Episode 2 of Trending Topics in IT: A Deep Dive into Today's Emerging Technologies, a new podcast series on emerging enterprise technologies and sponsored by Accenture and AWS.

I'm Barbara Call, Senior Director of Content Operations and Strategy with IDG. I'm joined today by Hart Rossman, Director of Global Security Practice with AWS Professional Services, and Chris Lachaux, Security Lead for the Accenture AWS Business Group. Welcome, gentlemen.

Chris: Morning. Thank you.

Hart: Morning.

Barbara: 00:00:36 – So today we're talking about how more rigorous data security is a top business driver behind the adoption of pubic cloud. And I'd like to start off our conversation with some research results that I think our listeners will find interesting. So even as recently as two years ago, most of our IDG research studies showed that cost savings was the main driver for moving to the cloud. But in our exclusive survey of 600 global companies for Accenture and AWS, we actually found 38% of respondents cite security as a top driver for cloud adoption. So I'm wondering what's driving this shift, and Hart, let's start with you.

Hart: 00:01:15 – Thanks, Barbara. I think there are a few things that are driving this shift, one of which is the ferocious pace of innovation that you see with cloud providers. For example, with AWS a little over 30% of all capability we launch year-over-year provides net-new security capability to customers and so they're always getting the best we have to offer in terms of security capability. And when you couple that with sensible defaults and familiar control patterns, it's often easier to achieve the security outcome they're looking for at scale when working with a cloud provider as a partner.

Barbara: 00:01:54 – Great. And Chris, what are your thoughts?

Chris: 00:01:56 – Yeah, so I would agree. What we see is the default security posture that cloud providers offer is often much more secure than what they have on-premise. And the inclusion and the breadth of security services that are provided, typically at much lower cost than if you had to integrate all of those capabilities yourselves, plus the operating expense of managing all of that. So it really lowers the bar for enterprises to move into cloud.

Barbara: 00:02:26 – Okay, great. So it's clear IT leaders are starting to see the benefits or already seeing the benefits; but we also know it's a complex landscape and there are challenges, such as integrating the security of multiple cloud options. So Hart, again, what are your thoughts here?

Hart: 00:02:45 – I think it's a tremendous opportunity and really good time to be in the security space. When you've got infrastructure as code and you're exposing all of that capability via API, on the one hand you've got a lot of options on how you do things. On the other hand you have this really interesting opportunity to take the best security capabilities from a variety of different partners and solutions

and integrate them into a planetary-scale security solution that meets your needs in a way that you just couldn't do on-premises when the primary goal was to configure independent security products. And so from that standpoint, I think it's less about the complexity of the landscape and more about having the choice to take the best of what's available and in an API-driven approach, integrate it into a solution set that best meets your needs.

Barbara: 00:03:39 – Right, okay. Chris, what are you thinking?

Chris: 00:03:42 – Yeah, I think what we see in hybrid deployments and multi-cloud deployments is a focus on consistent security model across the spectrum, trying to have equal security capabilities across all platforms and equal level of visibility across each is critical.

Barbara: 00:04:02 – Okay. Thank you. So I'd like to share some other stats from our survey results and get both of your reaction. So integrating data security was the most challenging aspect of deploying applications in a public cloud. That was cited by 45% of our respondents. And this is well ahead of some of the other challenges, including managing variable cloud cost, which was 36% of respondents, and compliance and legal risk management, which was 34%. So let's start with Chris. What's your reaction to these stats?

Chris: 00:04:38 – So yeah, I think we've seen attacks moving from infrastructure traditionally to operating system to applications over time, and applications have become kind of the weak link that they're choosing to attack. So I think there's generally less consistency in the security model within applications and it requires developers to have added security knowledge in their development cycle. So there's a need to shift left on security and incorporate application security from the get-go.

Barbara: 00:05:11 – That's great. Thank you. Hart, what are your thoughts here?

Hart: 00:05:14 – I think there's a combination of things going on. One is, as Chris mentioned, there's increasing complexity and sophistication in the applications that are being built and deployed in the public cloud; and with that comes the necessity of having more sophisticated security solutions that at the same time are easy for developers to integrate in. And so I think what you'll see is, is certainly with AWS, that over the last couple of years we've begun to make available more sophisticated planetary-scale data security solutions that are easier to integrate in via API.

00:05:55 – And so we've got solutions like Macie, which helps you from a data analytics and data protection standpoint; KMS; and even most recently our AWS Secrets Manager that helps you manage the credentials that you use to integrate in with your application. So it's an area that's being recognized where we can all do better, and we've begun to, over the last couple of years, really make really sophisticated capability available that is easier to integrate via API for our developer community.

Barbara: 00:06:28 – Okay, great. Those sound like integration options. I hear a lot about the terms gaps and visibility, especially when we're talking about securing data among multiple cloud options. So what's the answer to filling those gaps and ensuring visibility? Chris, let's start with you.

Chris: 00:06:47 – Yeah, I think there's different approaches based on whether you're deploying to a single cloud provider such as AWS versus looking at hybrid or multi-cloud scenarios. I think whereas our approach would be to leverage cloud native capabilities, so some of the services that Hart was just talking about on KMS and Macie and GuardDuty, if it was a pure native play. For multi-cloud you would start to look at capabilities that bridge all of the cloud providers and provide a single pane of glass and lower kind of the operating expenses of managing security in that case.

Barbara: 00:07:24 – Okay, great. Thank you. Hart, what are you thinking?

Hart: 00:07:27 – Just about all of what Chris was saying. I think another really important aspect of this is having a shift in your mental model where you're focusing on using the cloud to secure the cloud. An observation I have is that when customers are in a multi-cloud scenario or in a hybrid scenario they often want to protect those assets from their existing on-premise environment and that can sometimes challenge them and that may expose some of these gaps or visibility issues that you refer to. When we see customers use the cloud to protect the cloud in a multi-cloud environment, we get much, much less of that kind of feedback in terms of their inability to see or scale the security solution. So having that focus on using the cloud to protect the cloud, I think goes a long way towards achieving that goal.

Barbara: 00:08:19 – Excellent. Thank you. So before we continue our conversation with Chris and Hart, I want to say a few words about our sponsors. Trending Topics in IT: A Deep Dive into Today's Emerging Technologies reports on emerging enterprise technologies and is presented by cio.com in partnership with Accenture and AWS. Now back to the show.

00:08:43 – Welcome back. I have another set of stats I'd like to share; 44% of respondents to our survey flagged security integration as the most sought-after skillset and 40% identified risk management capabilities. So I'd like to ask both of you, why do these skillset gaps exist? Hart, let's start with you.

Hart: 00:09:07 – Sure thing, Barbara. I think there are two fundamental drivers here. The first is that there's a shift in the overall IT space towards DevOps and agile and this concept that we need to be able to insert security into that program. And then some folks talk about it as DevSecOps and building that rich set of skills around building and deploying in operating systems in this new software development lifecycle is a big part of it. And I think the second part is that today many on-premise security solutions are console-driven and it's all oriented around being collocated at a physical space to collaborate.

00:09:49 – And what we see in the cloud is that when you have infrastructure as code and everything is exposed to you via API, your security has to be embodied in code and all of the solutions you're going to build, in order for them to scale and have some agility, have to be API-oriented themselves. And so what we're seeing is a need for the security community to shift from configuring static solutions and then working together in a physically collocated environment to do analytics and make changes slowly over time to their security posture to be able to do it in a very DevOps, agile, near real-time environment where the way you make a change is by pushing code through an API. And that's just a difference in the way we've done business than we have over the last couple of decades.

Barbara: 00:10:40 – Okay, great. Chris, what are you thinking here?

Chris: 00:10:44 – Yeah, so I would agree with Hart. DevSecOps is an important shift in security. Incorporating security earlier in the stack into the application development process and pushing that throughout the CI/CD pipeline into production, I think that's a different skillset than most traditional security people have faced; and they're having to adopt and adapt to kind of the shift in the cloud paradigm.

Barbara: 00:11:14 – Okay, excellent. Thank you both. So why should CIOs consider partnering here? Hart, let's start with you again.

Hart: 00:11:23 – I think whenever you take on something new where there's a lot of potential or there's a lot of opportunity, you want to build an ecosystem around you that positions you and your partners for success. And so I think CIOs really want to consider partnering here so that they can create, for lack of a better term, positive feedback loops where as they learn something their network of partners learns as well and that the ecosystem that they're building around their organization develops this capability together. And so they get better outcomes faster with shorter learning cycles, so that the more they learn the better they get and

the better they get the more they learn. It's really a win-win scenario for their business to bring in partners.

Barbara: 00:12:11 – Chris, what are you thinking here?

Chris: 00:12:13 – So I would agree with Hart. A few other points to keep in mind is, as you engage in this journey, that you need to partner with other organizations that can help accelerate the path to cloud; you have the experience in all facets of a migration to cloud; and bring security competency to the effort.

Barbara: 00:12:37 – Okay, excellent. So we have time for one last question here, gentlemen. I'd like both of you to offer maybe one or two key takeaways that CIOs or IT leaders need to keep in mind regarding security and cloud. And this time, Chris let's start with you.

Chris: 00:12:54 – Thanks, Barbara. I think that one of the biggest points is the DevSecOps and the shift left of security. That's a critical way of approaching security in the cloud. Avoid bringing bad legacy security practices from existing environments. Use this as an inflection point to really revisit how you're approaching security and look at kind of the use cases and the requirements to drive a better security model.

00:13:25 – One of the things that we're really looking at going forward is kind of security automation and remediation. So not only incorporating automation to lower the operating cost and improve the reaction times to security events; but also the ability to implement remediation capabilities, for instance, which is something new, a newer capability that's coming to bear with things like Lambda.

Barbara: 00:13:52 – Excellent, okay. Hart, a few last thoughts for you.

Hart: 00:13:56 – Our CTO Werner is often fond of saying that there's no compression algorithm for experience, and I think that's particularly true in this space. As customers make the journey to the cloud and are leveraging that rich ecosystem of partners, they have a lot of opportunity to build new skillsets and significantly raise the bar for security and it's an iterative process. And so the advice I give to all of our customers is that you can put a lot of good effort into planning an architecture and assessment and that's important; but you're going to get the most learning by building, deploying, and operating security solutions in the environment you intend to run your production applications. And so the sooner they can get to that point where they're working with the code in the environment, the better off they'll be. And so really to focus on building, deploying, and operating.

Barbara: 00:14:52 – Excellent. Thank you, gentlemen. This is a really great discussion. And thanks for listening to today's podcast. Trending Topics in IT: A Deep Dive into Today's Emerging Technology reports on emerging enterprise technologies and is presented by cio.com in partnership with Accenture and AWS. Don't miss future episodes by subscribing to the IDG Tech Talk channel on SoundCloud and on iTunes. For Accenture, AWS, and IDG, I'm Barbara Call.

END