The Deloitte On Cloud Podcast

Emily Mossburg, Global Cyber Leader and US Cyber Strategic Growth Offering Leader, Deloitte Consulting LLP

Title: **Emily Mossburg, Deloitte's global cyber leader, talks trends and growth in cybersecurity**

Description: In this episode, Emily Mossburg, leader of Deloitte's Global Cyber practice, discusses growth areas, trends, and key priorities in cloud cyber security. Emily sees zero trust is the most explosive growth area in cyber, while the biggest trend is the need for organizations to adapt to Generative AI, remote work, and hybrid cloud environments. Finally, Emily argues that integration of data sources and components is a key priority to boost security and maximize value to the organization.

Duration: **00:11:19**

Emily Mossburg
Welcome to this On Cloud podcast knowledge short exploring a specific topic related to cloud computing. This is a short tutorial talking about real-world concepts in the emerging world of cloud computing. I'm Emily Mossburg, leader of Deloitte's Global Cyber practice and also serving as the leader for our cyber strategic growth offering. I'm your host today for today's knowledge short on cloud cyber security.

I want to start today by talking a little bit about the cyber security market, and that quickly starts to delve into the growth that we're seeing in cloud. Today if we look at the cyber security market broadly in the services space, we'll see that globally the CAGR for this market is growing 10 percent year over year and is expected to be over $120 billion by 2027. And a lot of the growth, a core component of that growth, is led by cyber cloud services. And it's hard to in today's world break out a metric specific to cyber cloud security because of the fact that just security itself is becoming so synonymous with cyber cloud security.

Let's talk a little bit about the areas within cyber cloud security that are growing the fastest. Those include the cloud access security broker space, or the CASB space, the workload protection platforms that are out there, and anything related to zero trust, whether that be zero trust network computing, zero trust identity services. Anything that you can bundle into the zero-trust space is one that's rapidly growing. And we think about what's driving that, what's happening in the market that's truly driving that, and there's a couple of key things that we're seeing driving that growth.

First is the fact that organizations are increasingly and continuously dealing with remote, as well as more complex hybrid working models. This is leading to the redesign of networks overall. There's also a drive toward SaaS applications as this occurs, and all of that cloud migration, all of those changes to the infrastructure are happening at the same time, or near the same time. That's driving increased exposure.

There's also this concept of the fact that as we have all of these components coming together, the complexity of the security landscape is increasing. We've got so many different disparate vendors, we've got multiple cloud environments, and all of this needs to be managed and dealt with at the same time. There's also just the reality of what's happening in the cyber space. There continues to be an increase in the number of targeted attacks, and the threats continue to evolve. And the more technology that we integrate into our businesses and becomes core to the way in which we're delivering our businesses, the more threat that we see.

Now let's talk a little bit about the trends. What are the trends that are shaping broadly the security landscape but specifically the landscape as it relates to cloud security? Again, the concept of hybrid environment. Very few organizations are really focused on a single cloud provider. They have applications, data, processing happening across multiple cloud environments, and this drives a complexity in getting the level of visibility across the organization's network.

With that lack of visibility comes confusion. On top of that, we've get, as I mentioned a little bit before, a very, very diverse vendor situation across security and specifically in cloud security.

Many organizations are grappling with the number of different vendors and solutions in their environment, and they're focused on how can they drive to a more simplified approach to their security program and managing their security operations on an ongoing basis. And as organizations continue with cloud migration and the transformation of their network, the interest and demand for things like security edge, SSE, continues to grow. And you see that supported by its convergence with specific network services like SC LAN. There's a lot evolving at the same time driving a broad shift in architectures within organizations.

The last concept that I'll mention in all of this is the complexity associated with the talent. When you're out there with so many different initiatives that are being driven at the same time and you're looking at broad cloud migration where you're trying to integrate cyber security into those architectures, this leads to another level of complexity in the market.

So let's talk about what it is that's happening as it relates to embedding cyber into cloud architectures and cloud migrations. First we're seeing that many organizations are coming to the realization that integrating security up front and using it as a business enabler is key. By understanding, at the onset, a cloud migration or a business transformation and technology transformation project, the requirements from a cyber perspective, and building those in up front is really allowing organizations to move faster. I often call it going slow to go fast.

And they're focusing not just on understanding the risks but on building security controls and ultimately resiliency of their technology into their architecture and into their processes by design. And this is really helping in making sure that organizations are prepared for the future, that they have an approach that thinks through and processes what the risks might be, where they may have future vulnerabilities, how threats could actually make those vulnerabilities real and is then ready to action and respond to those threats when they occur.

Another element in all of this that is driving really the growth of cloud and the growth of the need for cyber security in the cloud is the increasing demand for things like artificial intelligence and machine learning. As organizations are trying to move quickly in getting more value out of the data that they have, they're looking to move to the cloud quickly with specific and customized ways in order to take full advantage of new and evolving AI models. This is again causing a rapid shift of certain types of data and certain processing into the cloud, and that is also then causing organizations to think about how they do that in a secure way. and as they look to move that data or make that data accessible to those models, how are they sure that they're building resiliency into their organizations.

At the end of the day, what organizations are really trying to drive toward is greater visibility and a greater ability to observe their environments. You've got to be able to see the traffic that you have, the processing that's happening, have to have an understanding of your data and where that data resides and how that data is being processed and what models from an AI perspective have access to that data in order for you to be able to protect it and to understand when it may be at risk.

It's also paramount, and a key priority today is integration of all these disparate data sources around security, bringing those pieces of data and those data components together, and being able to apply analytical models against this data in order to drive more valuable information, more valuable security insights that you can use. Getting to these insights, getting to this visibility will allow organizations to have greater execution of their cyber security program. This is going to lead to reduced risk from a technology standpoint and from a business standpoint, and ultimately what that's going to allow is for organizations to drive greater business value through their cyber security programs.

Thanks for listening to this week's knowledge short on cloud cyber security. I'm Emily Mossburg. If you enjoyed this podcast, make sure to like us, rate us, and subscribe. Until next time, best of luck with your cloud journey, and stay safe.

About Deloitte

As used in this podcast, “Deloitte” means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.