"The Covid-19 Pivot to the Cloud: Securing it at Scale and at Speed"

The Accenture APAC Cybersecurity Forum (ACF) convened a virtual roundtable titled, "The Covid-19 Pivot to the Cloud: Securing it at Scale and at Speed," on December 15, 2020.

Enterprises across the APAC region are pivoting to cloud computing. What are the security impacts of that migration? What are CISOs' top security concerns—talent, automation governance? What are the best practices for maintaining a strong security posture in a cloud-enabled environment?

APAC Forum members examined how the rapid shift to the cloud is impacting enterprise security. Our speakers included Accenture Security subject-matter experts and peer CISOs. The session was hosted by Kris Burkhardt, Accenture CISO and ACF chair, and Andrew McLauchlan, APAC Lead, Accenture Security.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

Close the Talent Gap

APAC CISOs find a deficit in cloud cybersecurity talent a major challenge. It is difficult to find people with the right blend of security, cloud and industry skills. In addition, CISOs are finding that employees with traditional cybersecurity skill sets sometimes struggle to adapt to a cloud environment.

Fortunately, the developer community is emerging as a promising pool of security talent. CISOs report that developers are starting to recognize that security skills are a valuable addition to their own skill sets. In addition, as the distribution of security controls reach developers who are working with automated infrastructure and data pipelines, there is an extension of security capabilities into other areas of the business. As one security expert said, "In the cloud, security is code."

Automate, Automate, Automate

Leadership at some enterprises are still struggling with the implications of migrating to the cloud. It can be challenging to achieve cloud cybersecurity that is analogous with on-premise

architecture. CISOs are finding it difficult to keep up with the pace of cloud innovation, particularly in the category of platform as a service (PaaS).

Automation and controls can help CISOs overcome the talent deficit and keep cybersecurity on pace with digital transformation. Tools can be applied across the cloud environment: securing infrastructure, digital identities and data while also promoting efficiency, compliance and security of core business services. CISOs highlighted the value of analytical tools that help the security team detect and remediate or block misconfigurations before they create a crisis and automated remediation tools that can minimize the escalation of threats. A security expert added that it is worthwhile to automate security at the edge and in the cloud computing environment.

However, other CISOs have said that cloud service provider (CSP) native accelerators and default settings aren't always adequate and developers have to accept constraints on the security they can provide. "Cloud computing isn't inherently insecure or inherently more secure. It's all about how you manage through the process," said a security expert

Governance

Governing during a pivot to the cloud is a strategic issue, particularly when teams outside the IT department set up cloud services without appropriate security measures. Without proper security governance, these rogue initiatives can put the enterprise at significant risk.

CISOs are trying to be nimble in establishing the policies and processes of good cloud cybersecurity governance. Making the organizational and operating model changes for a successful cloud migration requires creativity, training and monitoring. For example, one enterprise has rolled application development under application security so that security is built into apps from the start. Another enterprise physically moved the cloud team to another building.

Don't be overwhelmed by innovation

Innovation is both a blessing and a curse, CISOs and experts said. For example, Alibaba Cloud offers more than 100 services. AWS comprises more than 175 products and services. And Azure claims to offer more than 600 services. CISOs should be prepared to regulate the pace of new technology adoption in the face of an increasingly dynamic cloud industry and enterprise demands for strategy execution in weeks or months, not years.

"CSPs are introducing new capabilities that, frankly, are outstripping the pace of change most enterprises can maintain," said one expert. "What I would advise someone today is far different than what I would have recommended a year ago."

CISOs acknowledged that security in the cloud requires different approaches than traditional on-premise security. "The 'what' is the same, but the 'how' changes significantly," said a cybersecurity expert.

For example, cloud migration strategies are evolving and becoming more complex. An original focus on Software as a Service (SaaS) and point-in-time computing has given way to multi-cloud service provider computing environments and platform-as-a-service models. Getting transparency into this complex environment is not straightforward. In particular, hybrid and multi-cloud computing environments make establishing a single approach to cybersecurity

difficult. “Having a single pane of glass (for managing cybersecurity) is the holy grail, but we’re a ways off,” said a cybersecurity expert.

Suggested Leading Practices:

- **Security by design**—Focus on breach prevention from the start. Make it easier for business units to take initiative using the right tools and platforms. “Give them the right sharp tools and prevent them from playing multiple choice,” said an expert. “The last thing a CISO wants to do is play catch up with shadow IT.”
- **Talent—**Tap the pool of developers for cloud cybersecurity talent—“Having people with a development mindset is a real plus,” said one expert. Provide opportunities for SecOps professionals and developers to rotate into cloud security teams.
- **Automate**—Using tools effectively can hold down the costs of compliance and security. For example, systems configuration automation can accelerate speed-to-market and reliability of new apps. Be aware, however that the half-life effectiveness of many tools is getting much shorter as the pace of innovation accelerates.
- **Alignment**—CISOs confirmed the value of looking at cloud migration through a strategic lens. It takes clear strategic intent, a nimble governance model, alignment—across the IT organization and the rest of the business—and implementation in line with acceptable enterprise risk tolerance. Teach the Board of Directors and business unit leaders to ask the right questions about cloud security. Help auditors climb the cloud’s steep learning curve.
- **Transparency**—CISOs have encountered friction in moving some enterprises to the cloud. The recommended approach is to deliver clear, consistent and regular communications about migration strategy and its implications. “Pivoting to the cloud isn’t just about technology; it’s about managing change within people and processes,” said an expert.
- **Boundaries**—“Start with multi-factor authentication for everything,” said an expert. “And focus particularly on securing high value credentials.” Consistent, firm compliance requirements are essential. “The risk is that anyone with a corporate credit card can stand up a new cloud service,” said a CISO. “We monitor that very carefully and have people answer for exceeding their boundaries.” An expert added, “Run discovery every day, and give people no choice but to comply.” Implement processes and tools that centralize and streamline access to cloud and enterprise services and applications. Consider zero-trust provisioning and establishing a security access administrator. Shut down credit-card provisioning to halt shadow cloud projects.

Conclusion

APAC CISOs are learning that people, processes and technology are all key elements of successful, secure pivots to the cloud. A multi-disciplinary approach is required for several reasons. The cloud attack surface has the potential to be more porous than on-premise environments. Threat actors are becoming increasingly sophisticated. And there’s increasing pressure to help the rest of the business quickly adapt to market demands. To be successful, CISOs will need the authority, support and budget to maintain security controls across the enterprise. It is a major challenge,

but cloud migration is also an opportunity to reframe the relationship between security operations and the rest of the organization by establishing the CISO not as the person who often has to say 'no' but rather as an innovation accelerator.

CONTACT

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 514,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.