The COVID-19 pivot to the cloud: Securing it at scale and at speed

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, "**The COVID-19 pivot to the cloud: Securing it at scale and at speed,**" on September 22, 2020. CISOs examined the security impacts of the quick pivot, and best practices for maintaining a strong security posture in a cloud-enabled environment.

The journey to the cloud raises important questions for cybersecurity leaders. How has the rapid shift impacted enterprise security? What are CISOs' top security concerns in pivoting to the cloud? What steps should security teams take to strengthen security?

Our subject-matter expert was Dan Mellen, Accenture Security managing director and global cloud security lead. The session was hosted by Andy Vautier, Accenture CISO and ACF chair.

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.

Impacts of accelerated cloud migration

The COVID-19 disruption is increasing the speed of cloud migration in many enterprises. The primary business drivers include speed to market, enhanced customer experiences, and imperatives of working-from-home policies.

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. Achieving transparency in this complex, rapidly evolving computing environment is essential but difficult.

There is a shortage of security and cloud talent, particularly professionals with cloud-specific security capabilities. The high demand forces CISOs to be creative in attracting and retaining talent. One possible source is the pool of traditional security professionals: infrastructure SecOps professionals with native premise security skills and a desire to make a change and succeed in a new specialty. The developer community is another promising source of security talent. Developers are starting to recognize that security skills are a valuable addition to their skill sets.

Security threats in the cloud

Cloud migration can pose a "clear and present danger." It can be easier to make fatal flaws in the cloud than in other environments. Attack vectors include connections to the on-premise environment, cloud-to-cloud interaction and APIs. Traditional data protections may be inadequate in the face of increasingly sophisticated threat actors.

From a security standpoint, the same characteristics that make cloud computing attractive, particularly flexibility and scalability, also present risks. For example, some CISOs have seen functional teams spin off new instances in the cloud without the proper attention to detail. Cloud service provider (CSP) default settings are not adequate, and developers must accept constraints on what they can do. Continuous monitoring and alerting are essential. Cloud computing isn't inherently insecure; it's all about how CISOs manage through the process. Extending a security mindset across the entire enterprise is a major CISO challenge.

Correcting misconceptions

CISOs discussed the challenge of explaining to the rest of the business that moving to the cloud is not a panacea for security; additional enterprise security investments are essential.

CISOs may have to overcome a perception that CSPs provide all the security for the enterprise. CSPs such as Amazon, Google and Microsoft have been upgrading their native security services faster than the third-party market and offering feature set improvements and capabilities. However, it is critical to define security authority and accountability between the enterprise and its CSPs. It is ultimately the CISO's responsibility to configure CSP security features since they are not always enabled at the onset of service.

It is much more efficient to build secure-from-the-start cloud instances than to add security retrospectively. Establish standards, practices and processes that work across functions and platforms. Make the case for security investments in business terms.

Best practices

Misconfiguration, misunderstanding and misuse are top contributors to lapses in security in the cloud. Subject-matter experts and CISOs offered a variety of best practices for pivoting quickly and securely to the cloud:

1. Education and transparency—Provide opportunities for SecOps professionals and developers to rotate into cloud security teams. 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. Ask and expect functional IT leadership to keep the CISO up to speed on their cloud migration plans; avoid having entrepreneurial leaders build their own environments. Consider becoming an expert in Certified Safety Professional® provisions via coursework and certifications.

2. Operational and organizational change—In leading enterprises, the security governance process and implementation of security controls is being distributed to groups such as developers running automated infrastructure pipelines or automated data pipelines. Security capabilities are being extended into other areas of the business.

3. Security from the start—Build security controls into migration practices from the beginning. Establish common principles, guardrails and nomenclature that can be applied with developers and CSPs and across the enterprise. Apply a tiered approach to security, starting at contracting and licensing and building in operational and IT controls. Set up a foundational infrastructure so that when cloud instances are turned on, they fit within predefined security parameters. Empower the SecOps team with tools such as privileged access controls and encryption keys.

4. Vulnerability management—Provision a secure cloud foundation with each instance rolled out, regardless of where in the enterprise it originates. Maintain continuous compliance and validation controls to spot deviations from acceptable risk tolerances. Experts reported CSPs are now providing features that aim to support multi-cloud security and sound configuration management. What is still unclear is whether enterprises can build vulnerability management tools and practices that span multiple instances and CSPs.

5. Access control—Implement processes and tools that centralize and streamline access to cloud and enterprise services and applications. Consider implementing zero-trust provisioning and establishing a security access administrator. Shut down credit-card provisioning to halt shadow cloud projects.
6. Security control testing—Explore the value of chaos engineering security practices and “bug bounties” to identify weaknesses in the digital architecture. Use automated breach and attack simulations. A dashboard that provides visibility into security control effectiveness can be invaluable.
7. Interface protection—The perimeter is a diminishing concept; in its place, interfaces are key. Security organizations are paying increasing attention to how they are dealing with APIs and connectivity back to the on-premise environment. Points of connectivity within a distributed environment are attractive attack vectors for bad actors and a major potential blind spot for many enterprises; provide extra protection. CISOs are considering zero-trust authentication policies whereby the user’s identity is the new perimeter.
8. Attack-surface reduction—Moving to the cloud presents opportunities to rationalize legacy IT portfolios. CISOs can get greater security by having less to actually secure. Adopt a structured approach to the difficult task of getting legacy cloud subscriptions under control.
9. Adoption of new technologies—Some capabilities enabled by the cloud require advanced thinking around data and analytics security. Traditional data protection methods such as encryption may not be adequate for applications of AI, machine learning and other newer technologies. Advanced capabilities will likely be needed to enable the new applications and services.

Conclusion

Pivoting to the cloud securely requires discipline across the dimensions of people, process and technology. CISOs must address misconceptions within the enterprise about cloud security, and adopt security standards that emphasize building in security from the start. Establish processes to automate the resiliency that cloud computing offers, while carefully monitoring for vulnerabilities. Keep pace with advances in AI, machine learning, graphics processing and other technologies enabled by cloud computing to help the enterprise compete and succeed.

Effective governance means that CISOs have the authority (and budget) to enable secure cloud computing, and the transparency required to monitor and maintain security controls across the enterprise. The risk of misconfigurations is high; threat actors are highly sophisticated; and the potential attack surface is expanding. As the COVID-19 disruption continues to impact many enterprises, CISOs need to help their enterprises balance security and business needs while moving rapidly to the cloud and realizing cloud computing’s potential.

CONTACT

Andy Vautier

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 509,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. 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.