Building A Resilient Cloud Ecosystem: What Are the Issues? Where Do We Stand?

The Accenture Cybersecurity Forum (ACF) Threat and Operations Community convened a virtual roundtable, “Building A Resilient Cloud Ecosystem: What Are the Issues? Where Do We Stand?” on May 12, 2022.

During this roundtable, Accenture subject-matter experts joined Community members to share best practices in security operations, threat intelligence and the capabilities needed to assure a resilient cloud ecosystem.

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

Below is a brief summary:

Proactively protecting the digital enterprise

Cybersecurity experts know all too well that they cannot rely solely on cloud service providers to protect their enterprise. While some in the group acknowledged that the rest of the business and the board may still believe in that myth, security experts agree that securing a large digital footprint—often comprised of on-premises, multi-cloud and third-party environments—requires a holistic, proactive cybersecurity strategy.

Key elements of that strategy include:

- Visibility across all computing environments. “You can’t treat the cloud as a silo,” said a subject matter expert. Another added, "Overall, I think we should acknowledge that a multi-cloud environment requires exponential increases in resources rather than a single cloud platform.”
- Robust governance and policies, including security guardrails for developing business apps, app ownership documentation, zero-trust, regulatory reporting compliance, redundancy

requirements, network security practices and guidance on protecting against host-level threat vulnerabilities.

- Rigorous threat intelligence. Nation-state and criminal threat actors are constantly coming up with new ways of exploiting vulnerabilities. "Don't expect to rest on your laurels," said a subject-matter expert.
- Automation wherever possible, including the use of multi-cloud and third-party tools such as Kubernetes for software deployment, scaling and management.
- Network segmentation. For example, private clusters where nodes are isolated from the internet by default, ingress controllers and web-based application firewalls.

Making the business case for building a resilient cloud ecosystem

There is no one-size-fits all model for estimating cybersecurity investment requirements, subject-matter experts said. For example, data retention can be costly, and the requirements are typically unique to each enterprise. However, in a world where "the internet is the corporate network," making the business case for zero-trust policies or Secure Access Service Edge (SASE) to enable secure and fast cloud transformation typically requires demonstrating how investments will increase visibility into risks, reduce administrative costs and empower the enterprise with new capabilities more quickly and securely.

Polling Question:

When asked about the most significant challenges in cloud security, compliance was most commonly cited. The response reflects the importance of governance and maintaining alignment with the rest of the enterprise and third parties regarding sound security practices.

Polling Question:

When asked about creating a safer, more resilient cloud security environment, responses reflected the complexity of the challenge. Improving asset management processes was cited as a high priority, particularly given multi-cloud and on-premise computing footprints. Establishing zero-trust policies is also important but can be difficult given that the term means different things to different stakeholders.

Leading practices

The following insights and recommendations were shared during the roundtable discussion:

- **"Consistent compliance"**—Work with the DevOps team to create a culture of shared ownership so that application security is a high priority up front. Document app ownership so the response team knows where to turn when an incident occurs.
- **Conduct readiness and resiliency testing**—One Community member, stressing that cybersecurity is a constant journey, has been conducting focused red team testing with key customers and third-party partners. Another cautioned that "cloud providers have significant limitations on client red team testing," but a subject-matter expert also said, "I think our red team has been largely navigating the various cloud environments without too many restrictions."

  Another community member said that purple team engagements before environments go live as defenses are being architected (or as continuous improvement), can be "a great tool to validate defective controls."
- **Analyze relevant threat intelligence**—Threat intelligence specific to the enterprise should inform where to prioritize effort and investment. Analyze and anticipate why nation-state threat actors would want to attack your enterprise. Monitor the dark web to uncover where credentials might be at risk. A subject-matter expert recommended "an adversarial mindset."
- **Uncover dependencies**—Threat actors often target on-premise legacy systems for access to critical cloud infrastructure. Manage asset inventory and permissions across the larger computing landscape because, as one subject-matter expert said, "Even small changes in on-premises access can have a huge impact on cloud security."

- **Add business capabilities while reducing the attack surface**—The CEO and board of directors might be anxious to embrace cloud strategy without first thinking through risk. Thus, security executives may have to tell a coherent, impactful story that debunks the myth of intrinsically secure cloud environments. "Anticipate that reluctance about investment, a lack of resources or resistance within the business may all present challenges when trying to keep the enterprise secure," explained a subject-matter expert. Another Community member advised: "Take the time to plan your cloud journey."

On behalf of the Accenture Cybersecurity Forum Threat and Operations Community, we thank our subject matter experts and those of you who were able to join the roundtable for your valuable contributions.

Josh Ray
Accenture Managing Director — Global Cyber Defense Lead
Accenture Cybersecurity Forum Threat and Operations Community 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 699,000 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 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.