Limiting Attacks with Cloud Visibility and Security

Highlights from a Government Roundtable hosted by ATARC, in partnership with Wiz, June 2023

As the government rapidly adopts cloud technologies, the number of potential attack targets across various cloud environments and architectural frameworks are increasing. Traditional cloud security approaches have consisted of using disparate tools to mitigate vulnerabilities, but the lack of visibility has left government agencies vulnerable to cyber threats.

Increasing visibility into the entire cloud ecosystem is revolutionizing cloud security by offering government agencies a unified, context-aware view of threats. At a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Wiz, topic experts delve deeper into the significance of cloud visibility and security in the government.

Key Challenges with Securing Cloud Environments

Roundtable participants started the conversation by discussing the challenges involved with securing cloud environments, which are complex and ever evolving. With each new update or innovation, software enters and leaves environments quickly. And with the inclusion of 5G networks, cloud security is becoming increasingly more complex to manage.

With so many components involved with securing cloud environments, panelists contend that agencies must have visibility in order to protect data and monitor assets. Continuous monitoring of assets ensures that multiple user accounts and deployable assets connected to the cloud are accurate and updated.

Roundtable participants shared a key challenge to cloud security is the difficulty of implementing change in a rapidly evolving landscape. Not only does a lack of funding impair an agency's ability to move programs forward, but so does an agency's culture if its people are resistant to change.

Participants also shared a need to balance the novelty and appeal of new technology with the agency's mission. There are many unknown risks associated with new technology, especially AI powered software, which raises concern among security professionals as usage of unverified technology increases among unwitting end users.

Some agencies represented on the panel continue to face challenges operating in a hybrid environment, which pose difficulties securing cloud environments properly. Their priority is to ensure all stakeholders are involved and communicating well to prevent security gaps as agencies continue cloud migration efforts.

Finally, panelists discussed the various challenges with optimizing cloud consolidation in order to achieve parity across large portfolios. As a panelist pointed out, not all cloud service providers are built equally. Some meet the bare minimum compliance standards, whereas others go beyond and become strong partners for agencies. Partners who take steps beyond compliance will become increasingly more valuable as technology advances.

Improving cloud security with real-time visibility

Panelists shifted conversation to the importance of a unified, context-aware view of the cloud, which can be achieved through the implementation of a Cloud Native Access Point (CNAP), to improve cloud security. Continuous Authorization to Operate (ATO) and monitoring are also important for real-time visibility and speeding up cloud adoption. Modernizing the old risk model is necessary to introduce new technology while improving cloud security.

Keeping up with the pace of change

"Security has a play in everything this organization does, because IT has a play in everything this organization does."

In regards to the roving technology landscape, participants expressed difficulty striking a balance between finding solutions to on-demand technology with understanding the risks of new technology, such as ChatGPT. To ensure deliberate adoption of emerging tech, panelists stress the importance of educating people on processes, security, technology, and new ways of thinking to facilitate change.

However, as one panelist pointed out, speed is often hampered by the ability to fund change. Agencies, especially small ones, face difficulties scaling to newer technologies due to limited budgets and resources. Agencies must find a way to keep pace with new technology and while ensuring the technology brings value to the mission.

Roundtable participants emphasize that aligning business objectives with security is critically important to avoiding redundancies and ensuring new technology can be adopted quickly. Panelists highlight the need to shift conversation from technology to outcomes in order to deliver secure and optimized environments.

"The more we can shift the conversation from technology to workloads and outcomes, then IT can actually deliver those secure, optimized environments to execute those workloads. That's how we really start winning."

Prevention strategies to mitigate risks in the cloud

Workforce training

Roundtable participants discussed the importance of finding skilled talent amidst a tough labor market. As one panelist pointed out, adversaries who are successful attack human beings who are the weak links. It's imperative for agencies to offer proper training to develop resilience among the workforce to effectively detect and stop malicious actors.

Agencies must also identify the right skill sets for different cloud environments, and to reinforce these skills by providing employees with technology capable of monitoring environments and mitigating weaknesses.

“We have to be right every time. The adversary has to be right one time.”

Democratizing Security

By democratizing security, agencies make security easy and accessible. Using platforms like WIZ, agencies can begin to break down silos between security and development teams that create unnecessary complexity. Shifting security to development teams not only makes cloud security less complex, but also less expensive to manage.

Zero Trust

Panelists highlight the need for forward-thinking approaches that integrate zero trust models into cloud security. While transitioning from legacy VPNs, agencies should understand the broader context of cloud security and network management while implementing the Zero Trust model.

Automate compliance

Some panelists are mitigating risks in the cloud by focusing efforts on automating compliance in order to avoid time-consuming manual processes that do not add value to their overall security program. They discussed moving towards a security lake approach while balancing compliance requirements..

Panelists also emphasize the importance of getting everyone involved in the threat hunt model, rather than relying solely on the threat team. Some agencies are beginning to realize their security teams are limited with their existing technology stacks, and are unable to get ahead of the next technology wave. They see data lakes as the way to move forward and keep pace with frantic change.

Align business and IT requirements

Panelists wrapped up the roundtable discussion by emphasizing the importance of aligning business and IT requirements to avoid creating solutions that don't align with the mission. Involving business owners in processes, such as in contingency testing, can ensure they also understand potential threats and learn how to respond in case of an attack. This is particularly important in cases of ransomware attacks, where end users play a critical role in prevention.