Strengthening the security of complex cloud ecosystems

Cross-cloud visibility, automation and robust industry partnerships can counter the unpredictable nature of current cyberthreats

Dre' Abadie
VMware

THE CYBERSECURITY landscape has been changing in two significant ways. One development that has been happening for a long time is the commoditizing of cyberattack tools and automating their deployment. This often allowed threat actors to be more opportunistic and "cast a wide net." However, recent integration of Artficial Intelligence (AI) has made these automated efforts appear exquisite and targeted, as well as more difficult to defend. This new reality will drive a pursuit of AI in cybersecurity solutions.

In addition, although cloud technology and as-a-service offerings are driving outcomes we could not have achieved in the past, they have also created dependencies in terms of who is responsible for managing those services. IT leaders must take the time to truly understand what has been agreed on in terms of the service being provided, and that may mean doing a little extra due diligence, especially if they are used to running everything in-house with their own people. That effort is absolutely critical for agencies to have a clear understanding of their dependencies with cloud service providers.

A MORE COMPREHENSIVE APPROACH TO CYBERSECURITY

Most agencies use more than one cloud provider, which means different agreements in terms of the service being provided across multiple clouds. In addition, government agencies often have to maintain some level of private cloud and on-premises systems. Hybrid cloud — and often multi-cloud — environments are the norm.

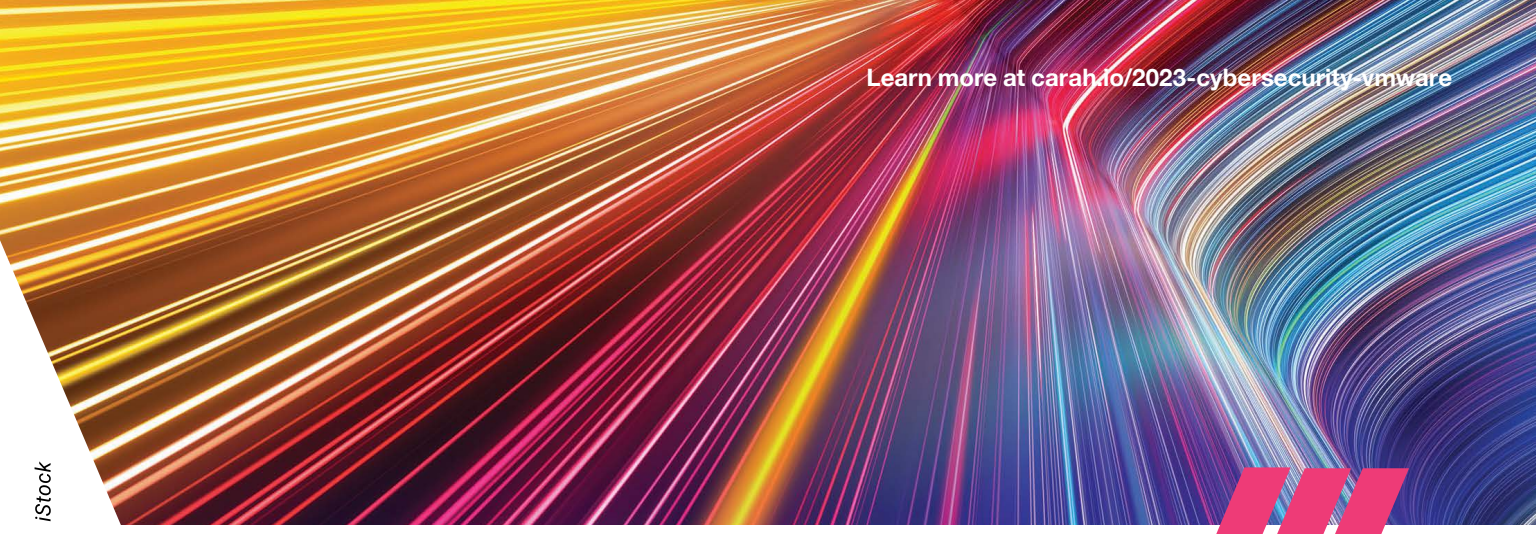
> "**Security is a team sport**, and when industry and government join forces, we can ensure that agencies have the best protection possible."

Agencies can strengthen the security of these complex environments by looking for tools or providers that offer some level of cross-cloud visibility and analytical insights. Also, because responding to cyberthreats in a timely manner is beyond what individuals can do, it's important to automate the majority of security tasks and then orchestrate how attacks are recognized, isolated and contained, and how systems are reconfigured to avoid such vulnerabilities in the future.

The federal government recognizes the need for a more comprehensive approach to cybersecurity, which is why agencies are moving to zero trust. However, no single product can address all the controls necessary to create a zero trust environment, so agencies should be skeptical of any provider that claims to have a one-size-fits-all solution. Instead, they should seek out companies that are clear and transparent in terms of what they can offer. They should also choose companies that have robust ecosystems of partners so that together they can provide the comprehensive security coverage agencies need.

ENABLING EMPLOYEES TO FOCUS ON THE MISSION

Many people focus on specific tools or applications because they make it easy to envision the achievement of an outcome in a tangible and measurable way. Infrastructure and platforms are discussed less often, or at least with less enthusiasm, and therefore, the government is falling behind in those areas. Agencies' technical debt is typically associated with infrastructure and platforms that aren't as up-to-date as they could be.



iStock

However, as agencies prioritize resources to modernize the IT infrastructure and provide stable platforms for their developers, they give those employees the opportunity to focus on providing applications that generate mission outcomes. Employees understand the agency's vision and purpose better than anyone. Let them concentrate on achieving the mission, and let industry partners run the infrastructure and platforms.

Security is a team sport, and when industry and government join forces, we can ensure that agencies have the best protection possible and the ability to respond to situations we can't even predict today. ■

Dre' Abadie is public-sector senior solutions architect at VMware and previously served 25-plus years at the Defense Department tackling the cybersecurity and interoperability challenges of warfighting.