GOOGLE CLOUD

How multi-cloud amplifies security considerations

With automation and a comprehensive strategy, agencies can put security at the forefront of multi-cloud adoption

Jon Tidwell
Google Cloud

Government agencies are leaning in on the benefits of operating workloads with multiple cloud vendors. The current wave of infrastructure modernization is quickly moving beyond the model of a single cloud provider's capability to meet all the needs of an agency.

However, this "new normal" of distributing operations across multiple vendors presents new challenges that require consideration to ensure security is at the forefront of these emerging architectures. A combination of basic cybersecurity hygiene and emerging technology, such as artificial intelligence, is crucial to securing data in a cloud infrastructure.

Although there is sometimes a sense of urgency to move to the cloud quickly, an agency must first ensure platform features align with its organizational goals. These considerations are amplified when taking into account the nature of multi-cloud operations.

> "A combination of basic cybersecurity hygiene and emerging technology, such as artificial intelligence, is crucial to securing data in a cloud infrastructure."

Compared to a single cloud and/or an on-premises computing environment, a multi-cloud approach ushers in new categories of security threats, specifically:

- **People —** Individuals should be fully trained on the security best practices of every cloud service provider (CSP) with which they work.
- **Processes —** Organizations must analyze how vulnerabilities within one CSP could propagate to others.
- **Technology —** Organizations need to leverage cloud-specific security tools within each CSP to maximize security within each cloud.

Identity is the new perimeter

Identity is the common denominator across any cloud model and any vendor platform. It is therefore imperative that agencies understand the various on-ramps for which identity can be leveraged to access cloud-based resources and services.

In the third quarter of 2023, 75% of incidents reviewed by Mandiant leveraged compromised credentials for initial access. Of those, 75% leveraged some form of social engineering as a means to gain access to credentials, such as spear-phishing email messages, smishing or vishing. Cloud can mitigate those risks by employing phishing-resistant technology, such as token-based logins or anomaly detection using AI, without complex integrations of third-party software.

Agencies can also design controls that harden the virtual security perimeter based on how users traverse these environments.

iStock

Centralization is the key

The wide array of services and resources available from CSPs presents an almost infinite combination of technical configuration possibilities. Designing universal guardrails will ease operational management while also informing what is important from a logging, detection and response perspective.

Consolidating security logs and cyberthreat information in one place and leveraging multiple tools such as Google's Chronicle, Duet AI and BigQuery to increase the effectiveness of an organization's security operations center are extremely important as well. By bringing together all security operations, threats from multiple actors can be addressed aggressively and in parallel. Additionally, consolidated logs can be reviewed with AI tooling to reduce repetitive tasks, allowing more users to implement robust security measures.

The Google Cloud Security AI Workbench is making strides in empowering security operations teams in their detection and response work. This new functionality is breaking down the time barrier to write advanced detection rules for teams not completely familiar with security toolsets. The introduction of natural language queries is changing the game for how responders interact with security event data while elevating the handoff to threat-hunting functions.

The cloud landscape is evolving at a challenging pace for IT and cybersecurity professionals to maintain. Although most cloud providers furnish similar core capabilities and services, each platform possesses unique offerings that should be leveraged to best suit agency missions and goals. Adopting a multi-cloud strategy while consolidating data and insights across the enterprise is paramount for government agencies to securely and efficiently fulfill their missions to the public. ■

John Tidwell is government strategic services lead at Mandiant, now part of Google Cloud.