Why multi-cloud and zero trust are **now essential**

Open-source technology and partnerships with industry are the keys to flexible, secure cloud systems

Shannon Sullivan
Director of Federal, Google Cloud

THE CORONAVIRUS PANDEMIC has underscored the government's need to offer a secure cloud environment that allows employees to access their data and applications anywhere, anytime and at virtually infinite scale.

Many agencies found themselves unprepared to support the sudden move to telework in response to the pandemic. Some didn't have enough VPNs or smart-card readers for their employees' remote devices, for example. Google Cloud customers that were already using G Suite or Cloud Identity were able to make the transition to telework smoothly without the need for VPNs or other special technology. That was due in part to G Suite's reliance on a zero trust architecture, which shifts access control from the network's perimeter to individual users and devices.

Google implemented BeyondCorp, our zero trust model, for our global infrastructure nine years ago — long before the pandemic demonstrated that this approach could be a foundation for continuity of operations.

Keeping up with the state of the art

To achieve true, ongoing cloud security, agencies must move beyond compliance-based checklists and build strong partnerships with commercial cloud providers that have taken the time to understand the government's security and mission objectives.

Over the decades, the government has repeatedly committed to custom single-vendor solutions, which have locked agencies into long-term commitments with proprietary systems. When that happens, agencies fall behind the state of the art, they don't get security updates at the speed of the industry, and their costs increase dramatically.

Instead, agencies should be moving to open standards, open-source tools and commercial best practices with the goal of creating secure hybrid, multi-cloud environments. That's how agencies can get the most out of the cloud, keep costs low and incorporate best-in-breed technologies. Tools like Kubernetes offer agencies the ability to operate across multiple cloud vendors, and a zero trust architecture can help create a security regime that operates across cloud environments.

A safer internet for everyone

Security is a top priority at Google. It shapes the way we design our data centers, our applications and even our hardware. The infrastructure that Google runs on is the same infrastructure that runs our customer data and applications.

Our security engineers and researchers have led industry coalitions to identify and fix vulnerabilities exploited by the likes of Heartbleed, Spectre and Meltdown. Google's goal is much broader than just securing our own cloud. We're out to make the internet a safer place for everyone. ■

Shannon Sullivan is director of federal at Google Cloud.