

State and Local Agencies Privately Become Cloud Providers

Gartner projects that governments will adopt private cloud at twice the rate of public cloud.

[Kevin McCaney](#)

Fri, 09/21/2018 - 17:30



Photo Credit: Rick_Jo/iStock

Any organization planning to move to a cloud computing model soon comes to a major fork in the road: whether to choose a public, private or hybrid cloud. Government organizations are taking all three paths to various degrees, but of late, are showing a preference for private clouds, which appeases some of their concerns over security and privacy while giving them the opportunity to share resources with other agencies that have the same concerns.

A recent [report from Gartner](#) shows that governments, as expected, are avidly moving to the cloud. And although growth in public cloud — the most popular model across all sectors — is going strong, with public cloud use expected to grow at a 17.1 percent rate through 2021, Gartner projects that governments will adopt private clouds at twice the rate.

Private clouds don't have all the scalability, functionality and price advantages that public clouds have, but they hold a couple trump cards in the view of government IT officials: they can better protect security and privacy, and keep organizations from getting locked into one vendor for years, according to the report. Private clouds allow agencies to combine and share resources while staying behind their own firewalls, keeping defenses up while reducing costs and making the transition viable. In some cases, state and local agencies are able to become cloud users by becoming cloud providers.

“Government private cloud is the new legacy,” Neville Cannon, research director at Gartner, said in a blog post accompanying the report's release.

Keeping the Public Private

The government's push towards cloud computing has been gathering momentum for years. The federal government established a cloud-first policy in 2011 and this year revised it into a [Cloud Smart](#) strategy. The National Association of State Chief Information Officers' list of the [Top 10 Policy and Technology Policies for 2018](#) puts cloud services at No. 2, behind only security and risk management. And the roughly 86,000 local government agencies in the U.S. are spending, on average, 20.6 percent of their IT budgets on cloud services, according to Gartner.

In the process of adopting cloud infrastructures, they face the choice of a public, private or hybrid cloud. Public clouds, which offer the lowest prices and least amount of effort on the part of a purchasing organization, are the most common, whether in the public or private sector. Typically offered on an on-demand, pay-as-you-go basis, public clouds save organizations the expense of operating and maintaining their own hardware, and performing their own upgrades. And because they tend to be provided by large companies (Amazon Elastic Compute Cloud, Windows Azure Services Platform, IBM's Blue Cloud, and Google AppEngine), they offer nearly unlimited scalability and a high degree of availability.

A MeriTalk survey cited in [StateTech](#) found that that 54 percent of state and local governments use private clouds, compared with 33 percent using public clouds and 13 percent using both types. Private clouds [host applications](#) such as email and those dealing with public information, but also handle sensitive information limited to specific groups, such as those granting police access to crime reports.

Nevertheless, government agencies still like to keep much of their data close to the vest, a factor that is a big part of the appeal of private clouds. Fifty-four percent of state and local organizations, as well as 64 percent of federal agencies, keep the [majority of their applications](#) in private clouds.

A private cloud is a on-premises data center run by the organization that makes use of virtualization, automation and other technologies, to act as a cloud provider to users within an organization as well as other agencies. A long-running example of a private cloud is the Interior Department's [Interior Business Center](#), which offers financial, acquisition and human resources services to other federal agencies.

But a number of cloud providers establish private clouds specifically dedicated to agency customers. While not as flexible as public clouds, it offers advantages in security, data privacy and compliance with federal or state mandates.

Perhaps the best-known example in recent years is Amazon Web Service's [Commercial Cloud Services](#) contract with the Intelligence Community and its 17 agencies. AWS late last year added a [Secret Region](#) for handling data classified all the way to "top secret," and made it available to the IC and other government customers, as long as they have secret-level network access and their own contracts with AWS.

The Defense Information Systems Agency's [milCloud 2.0](#) is another private cloud with a third-party provider, offering infrastructure-as-a-service services to customers throughout the federal government. MilCloud was originally run in-house, but DISA this year launched 2.0, which is operated by CSRA while being located on DISA's premises, within the security of the network's perimeter, with DISA retaining ownership and control of the data.

Private clouds also come into play in hybrid approaches, which combine public and private clouds in various ways, allowing an agency to, for instance, keep its data private while running applications on a public platform.

The California Department of Technology uses a Microsoft Azure hybrid cloud for its [CalCloud program](#), offering IaaS, email and vendor-hosted subscription services to 17 agencies around the state, including the departments of Motor Vehicles and Child Support Services. Oakland County, Mich., a suburb of Detroit with more than a million people, provides software-as-a-service to more than 100 smaller agencies, [StateTech](#) reported. (It also takes a different kind of hybrid approach, calling its services G2G Cloud Solutions on the idea that a commercial-sounding brand would have more appeal to those agencies than accepting services from another government agency.)

Clouds Forming, But Yet to Take Shape

The pursuit of private clouds from state and local governments still has a long way to go, however. Gartner points out that a lot of what those organizations call private clouds are only partial implementations, making use of advanced virtualization or outsourced IT infrastructure. But less than 5 percent of them have the full characteristics of cloud computing, the report says.

This could partly be a sign that the cloud transition is still in its early stages, but there are risks for agencies that don't follow through. "What this highlights is that there are political benefits to talking about moving to cloud, even where that transition is not taking place in a meaningful way," Cannon said. "Poor or incomplete cloud implementations have the potential to produce the worst of both worlds, leaving government employees and citizens poorly served in the end."

[View PDF](#)
[cloud](#)

report

Gartner

intelligence community

Amazon

DISA

cloud computing