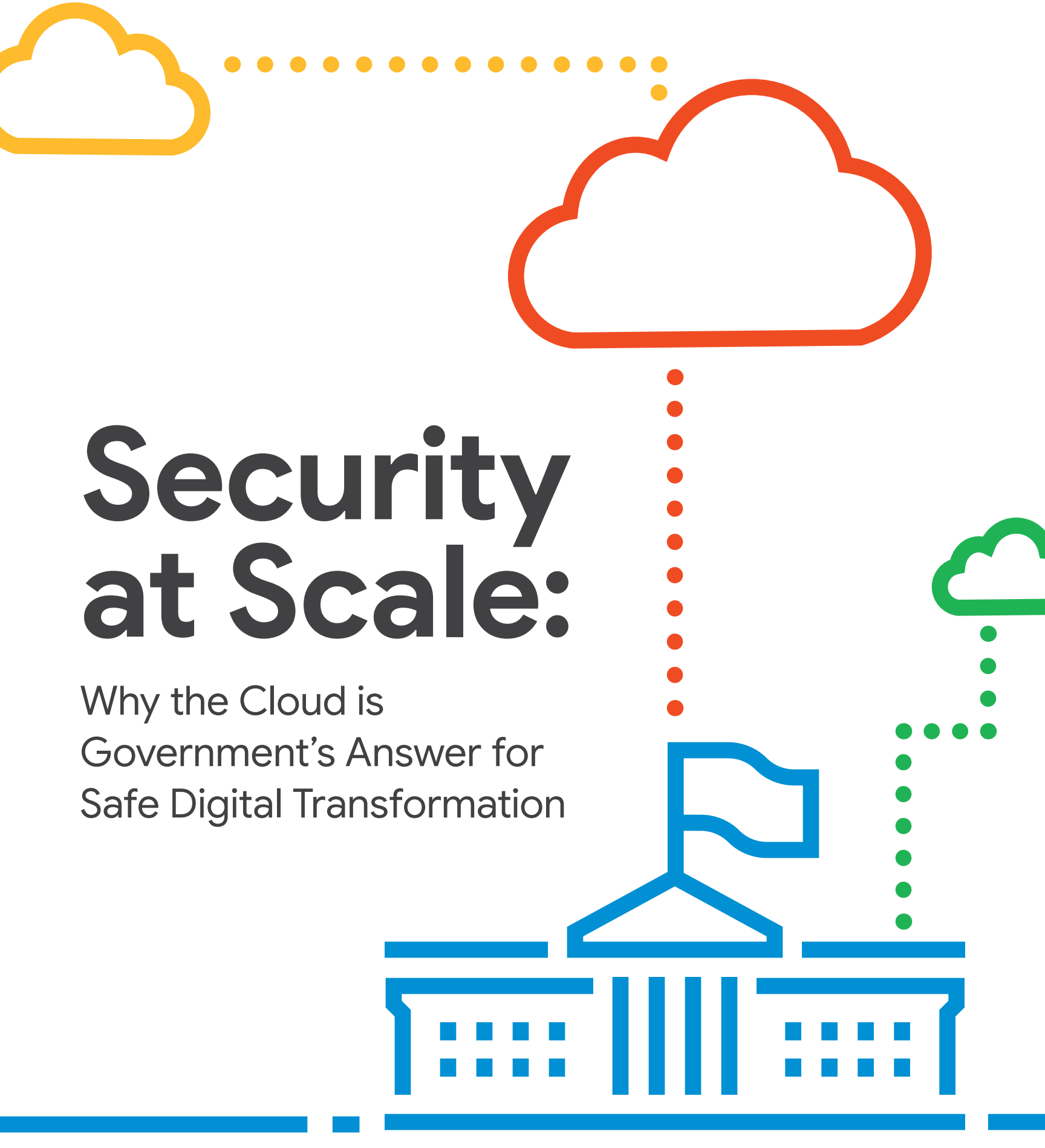
Security at Scale:

Why the Cloud is Government's Answer for Safe Digital Transformation



CIOs and CISOs continue to raise concerns about cloud security. But with a comprehensive framework for evaluating service providers, officials can safely accelerate their move to the cloud.

Government IT leaders are continuing their careful journey to the cloud. A national survey by the Center for Digital Government found only 29 percent of state and local government workloads are running in the cloud.[1] On average, the 110 state and local government IT executives responding to the survey said they could run 57 percent of their networks, systems and applications in the cloud, showing a gap between current and potential cloud usage of 28 percent.

This modest acceptance of the cloud model is well behind commercial industry. The technology research firm Forrester reported in late 2018 that 60 percent of enterprises in North America were relying on public cloud services.[2] Multiple factors explain government's slower pace, but one long-standing roadblock looms above all others: CIOs and CISOs remain concerned about cybersecurity, including how to tightly control access to information from external and internal parties.

Security and risk management, followed by cloud services, were the top two priorities in NASCIO's annual CIO ranking.[3] Even as IT leaders feel pressure to modernize their technology environments and support digital transformation with cloud services, they're opting for cautious approaches that reduce the risk to sensitive data. But some of these executives are learning an important lesson: The right cloud options can deliver enhanced and comprehensive security — not only for IT resources running in the cloud but also for on-premises data and applications.

29% of state and local government workloads are currently running in the cloud.

57% could be in the cloud.

This equates to a gap between current and potential cloud usage of **28%.**

Unfortunately, with so many cloud providers to choose from — and so many claims and counter claims about their security capabilities — it can be difficult to find the best solution. This issue brief lays out a framework for understanding the latest trends in cloud security and what government CIOs and CISOs should consider to deliver modern services to constituents in the most secure way possible.

Overcoming Cloud Myths

As governments become more comfortable moving workloads to the cloud, they will likely maintain a hybrid cloud environment in the foreseeable future. And while hybrid cloud can potentially make IT environments more secure, a host of lingering fears — and myths — continue to make government CIOs and CISOs move cautiously with deployments.

Myth #1: Confusion over the security responsibilities of clients and providers will create gaps in protection. The hybrid cloud model can quickly blur the lines delineating who is responsible for setting security policies and maintaining compliance standards. The notion of shared responsibility can be a problem with all types of clouds, but it is exacerbated in hybrid models. In these environments, governments may incorrectly assume cloud providers will apply and maintain security policies under the terms of their service contracts. Uncertainty around these responsibilities can cause serious vulnerabilities if, for example, they result in sensitive data being left unencrypted.

Myth busted: Leading vendors clearly define responsibilities. The most security-conscious providers offer a matrix that clearly shows where customer and provider duties intersect and where they diverge. A matrix not only provides important details about security duties, it will help government IT managers show auditors which organization is responsible for specific regulatory requirements, as well as reporting and auditing functions.

Myth #2: Hybrid clouds mean more work for security staffs. This pragmatic concern stems from the fear that management workloads for IT organizations will essentially double if technicians continue to perform their current administrative duties for on-premises resources while adding new security responsibilities for cloud services. But the concern is valid only if

CIOs don't partner with the right service providers. Many vendors continue to make clients responsible for properly setting security configurations for cloud IaaS and PaaS resources. If a government organization contracts with multiple cloud vendors like these, security professionals can quickly become overburdened when trying to set and maintain a range of complicated security policies throughout the hybrid environment.

This does more than just add administrative hours to lean IT staffs. It requires government agencies to cultivate the technical skills needed to support different service platforms with slightly different security tools and default settings. That may mean hiring new people or increased investments in training.

> "By enabling the holistic application of security controls, the cloud helps security staffs ensure all new projects adhere to enterprise standards, and that security policies remain in place as the IT environment evolves."
>
> — Dan Prieto, Strategic Executive, Public Sector, Google Cloud

Myth busted: The right clouds reduce administrative tasks.

Fortunately, not all cloud providers burden IT departments with these extra duties. The best providers offer policies and tools to centralize security administration for on-premises and cloud resources. Holistic configuration management available in the Google Cloud Platform is one example of how cloud services can bolster security in hybrid clouds. Strong security requires the comprehensive application of policies and standards throughout data centers, departmental offices and cloud resources. Leading cloud providers offer tools that IT staffs can use to deploy standard security controls across the digital environment. This reduces the management burden of traditional, on-premises data centers where administrators must manually configure security settings for each server.

"By enabling the holistic application of security controls, the cloud helps security staffs ensure all new projects adhere to enterprise standards, and that security policies remain in place as the IT environment evolves," explains Dan Prieto, strategic executive, public sector, Google Cloud. "Similarly, security updates — such as patches for operating systems or defenses against a new malware outbreak — occur automatically in the background, so IT staffs aren't pulled from strategic projects and end users don't experience system maintenance downtime."

Myth #3: IT leaders can't easily see or control access to their information in the cloud.

IT managers take comfort in the security logs generated in on-premises data centers that show who's accessing sensitive data stored on-site. They fear that by moving to the cloud they'll lose this monitoring ability, creating a risk that service provider employees could access protected information without being detected. What's needed are logs that track who's accessing data so managers can see if unauthorized users are viewing protected information, as well as data loss prevention tools to reduce risk.

Myth busted: The best cloud services provide full visibility.

Certain cloud services provide a central management console to view activity throughout the hybrid cloud environment — in cloud services as well as in traditional data centers. In addition to visibility, aggregating all this information allows the security staff to centrally manage the environment and quickly apply new policies as they're needed. The alternative is forcing security professionals to check a different dashboard from each vendor and potentially missing signs of an emerging threat. Cloud-based data loss prevention tools provide an extra layer of protection for sensitive information, allowing IT managers to redact certain data and implement the right set of access controls.

4 Questions to Ask When Evaluating Cloud Providers

It's clear hybrid cloud can provide the foundation for digital transformation, but the key to secure transformation is choosing the right cloud provider for your agency. What should CIOs and CISOs look for when evaluating cloud services? Getting answers to the following questions can help government agencies overcome their cloud security concerns.

1. **How turnkey are your security settings?** A broad and deep range of default security settings will help IT departments avoid increased administrative responsibilities in hybrid clouds. In fact, the best cloud options may reduce workloads for security staffs. For example, the Google Cloud Platform enables critical security controls such as data encryption, multifactor authentication and automatic patching by default.

   "Rather than turning on these safeguards, clients must actively disable them if for some reason they become unnecessary," says Prieto.

2. **Do your published performance ratings account for any overhead from security settings?** This is an important follow up to the first question. A service provider's performance specifications may reflect the raw speed potential of its services instead of showing what's possible when encryption and other capabilities are in place. The best service providers post

> "These types of tools let administrators search for correlations in large volumes of structured and unstructured data, which provides better visibility and a security health check for the entire environment."
>
> — Arthur Deane, Strategic Executive, Security and Compliance, Public Sector, Google Cloud

performance numbers when standard security settings are applied; if a potential provider doesn't typically do that, ask for updated specs to make accurate comparisons.

3. **How do we know your management console will give us the full visibility and control we need?** The resource should display traffic flowing into and out of the enterprise network, including any cloud services. Just as importantly, the tool should tell administrators which people or digital entities are trying to access data and applications, as well as who are the internal and external recipients of protected government information.

   Follow-up this question by requesting a list of all integrations a cloud provider offers to connect with products from other cybersecurity vendors. Integrations ensure the central management console incorporates log information from on-premises systems, third-party security applications and other cloud providers for a complete view of the organization.

4. **What analytic tools come standard to assess the security status of our hybrid cloud?** Sophisticated applications for slicing and dicing log information and other data related to security will help organizations uncover anomalous network activity that may indicate heightened risks.

   "These types of tools let administrators search for correlations in large volumes of structured and unstructured data, which provides better visibility and a security health check for the entire environment," says Arthur Deane, strategic executive, security and compliance, public sector, Google Cloud.

A Secure Path to Enhanced Citizen Services

Research by the Center for Digital Government and others show that cloud adoption will continue to grow in the public sector. As IT managers move to the cloud, they'll capitalize on hybrid cloud models that let organizations incorporate modern services while continuing to take advantage of existing data center investments. Hybrid clouds have the potential to introduce new challenges, including onerous administrative burdens and a lack of visibility into the security status of the entire environment. Fortunately, leading cloud service providers understand these risks and offer comprehensive solutions to address them. By asking the right questions, IT managers can identify the best cloud options and launch hybrid clouds that deliver higher levels of service to constituents.

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Google.

ENDNOTES

1. http://www.govtech.com/library/papers/How-State-Local-Governments-Are-Embracing-The-Hybrid-Cloud-110374.html
2. https://go.forrester.com/blogs/predictions-2019-cloud-computing/
3. https://www.nascio.org/Portals/0/Publications/Documents/2019/NASCIO_Top10_lettersize.pdf

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com**

For: Google Cloud

Google Cloud is widely recognized as a global leader in delivering a secure, open, intelligent and transformative enterprise cloud platform. Our technology is built on Google's private network and is the product of nearly 20 years of innovation in security, network architecture, collaboration, artificial intelligence and open source software. We offer a simply engineered set of tools and unparalleled technology across Google Cloud Platform and G Suite that help bring people, insights and ideas together. Customers across more than 150 countries trust Google Cloud to modernize their computing environment for today's digital world.