Google Cloud

Advancing Cybersecurity at Scale in the Cloud

The number of cyber attacks reported by federal agencies **increased by over 300%** between 2006 and 2015.

Cyber Attacks in the Public Sector Are on the Rise

According to a July 2019 report by a Senate homeland security subcommittee, the number of cyberattacks reported by federal agencies increased by over 1,300% between 2006 and 2015. Moreover, security threats to the public sector encompassed 75% of the approximately 41,000 total security incidents analyzed last year. Out of these, 330 attacks were confirmed breaches of government data, often caused by hacking, malware and cyber-espionage.

Even though federal agencies are gatekeepers to some of the nation's most valuable and sensitive data, much of the core infrastructure tasked with securing these assets has not evolved — significantly complicating government efforts to battle the most malicious threats. Likewise, a recent surge in IoT technologies and endpoints has injected greater levels of fluidity into the mission landscape, underscoring the need for solutions that can safeguard data from device to data center.

What agencies need now is a comprehensive platform to help them modernize and holistically manage their digital environments, with key capabilities to maximize insights from their data while demonstrating the utmost commitment to user and citizen privacy. More and more, agencies are turning to cloud environments that can scale to address these requirements head on — not just as a resource, but as a critical foundation for becoming the data-driven digital government of the future.

Major Challenges Undermine Government's Ability to Address the Growing Threat Landscape

Today's threat landscape is growing at an alarming rate, with attackers infiltrating not just infrastructure but government's full range of applications and devices. Failing to safeguard the digital environment carries enormous repercussions, which are further complicated by perennial challenges unique to government agencies. These include continuing shortages in cybersecurity talent, significant costs to infrastructure and budget, and fragmented security architectures that hinder effective response and mitigation. Most of all, agencies stand to lose the public's confidence when cyber attacks result in stolen or exposed citizen data. Not surprisingly, public sector agencies are struggling to advance faster than the threat.

Siloed Security Environment
Given the evolving threat landscape, security professionals are buying a myriad of point-solutions to address challenges at different layers (e.g. infrastructure, application, endpoint, network). In many cases, these solutions become too much to manage and lack the proper integration capabilities across systems prevent professionals from maintaining a clear view of their security posture across their environment.

Talent Gap
A glaring shortage of security and IT professionals has further exacerbated these troubles, pitting public sector agencies against unseen foes who have considerable talent and expertise.

Steep Costs
Attacks prove expensive to remedy: recent cyberattacks on Baltimore, Atlanta and other cities have been costly. The recent ransomware attack in Baltimore, for instance, cost the city over $18 million, as security consultants and city employees worked around the clock to rehabilitate disrupted systems and critical infrastructure.

Trust & Reputation
Attacks also have a substantial impact on the public's trust in government institutions, forcing citizens to question their government's ability to effectively protect data. Reputation is key to ensuring citizens view government organizations as trusted partners, which isn't possible when attacks consistently compromise citizen data.

"If we take things individually as a single project, as a single thing, we don't move the entire infrastructure, **we don't build our workforce capabilities in the right way, and in some cases, we make short-term decisions."**

— Suzette Kent, CIO, Office of Management and Budget

The consequences of cybersecurity inaction have already taken their toll. Incidents at the Office of Personnel Management, the U.S. Postal Service, and the Internal Revenue Service have reaped untold damage on IT systems, government operations and citizen data in recent years. Major attacks like these highlight the need for urgency across the public sector for more preemptive measures incorporated within government IT systems — and for changes in federal policy and legislation.

The good news: there's a resilient path forward. The right cloud provider can offer government agencies a cost-effective cybersecurity solution at global scale. Moreover, by embracing Cloud Smart's policy priorities, organizations can use the cloud to alleviate security issues, not create more. "When we said value, we didn't [originally] look at value in a full comprehensive manner," says U.S. Office of Managment and Budget CIO Suzette Kent. "That is what the new policy actually does. Modern technology requires modern policy. If you haven't looked at your whole landscape and know where you are going, then you aren't going to be making the best long-term strategic decisions."

New IT Policy Points Agencies to the Cloud

Policymakers see cloud migration and adoption as a way to improve citizen services, reduce complexity and rising costs of IT, and perhaps most critically, ensure the security of citizen data and critical infrastructure in perpetuity. When the Cloud First policy was first launched back in 2011, it marked the first government-wide effort to frame cloud as a fundamental priority for all agencies, informing the acquisition journey and encouraging 'lift-and-shift' of applications into cloud environments. While cloud adoption increased in the interim, the White House finally recognized in 2019 that a policy update was needed to help agencies achieve full cloud maturity.

The administration's Cloud Smart policy, unveiled in June 2019, centralizes focus around three pillars — security, workforce and procurement — and aims to realize the full potential of cloud-based technologies with security as a front-and-center concern.

Specifically, the policy directs agencies to take a risk-based approach to cloud security, emphasizing data-level protections through use of modern virtualized technologies.

Meeting the mandates of the federal policies such as Cloud Smart can be tricky for agency IT leaders so they're looking for help — and they're willing to spend to get it. With policy and security improvements encouraging adoption, government cloud spending is expected to grow through 2021. A 2018 Bloomberg Government analysis shows federal IT spending grew by 10% last year, with investments in cybersecurity and cloud computing rising to $6.4 billion and $4.1 billion, respectively. Among civilian agencies, cloud spending jumped 9%. Defense agencies more than doubled this jump, upping their cloud spending by almost 30%.

As agencies obtain more funding to spend on cloud advancements, there's a number of considerations they should keep in mind when exploring solutions that provide security-at-scale.

Cloud Provides Visibility and Comprehensive Security

A healthy cybersecurity posture demands a level of visibility, transparency and access that only cloud environments can provide. Agencies know that communication and collaboration are key to informing their full range of stakeholders, which includes not just legal, IT, risk, and security professionals, but also citizens in need of solutions.

This plan entails a **defense-in-depth approach,** where protection is needed not only at the data level, but at the vast network of endpoints and applications as well.

"By enacting a zero trust model, security **administrators can dictate who gets access to specific data based on each user's role,** determining whether or not the person is coming from a device with appropriate security controls and granting access appropriately."

- Scott Fleming, Head of Professional Services for the Public Sector and Security, Google Cloud

In order to deliver these capabilities, any implementation must respect that privacy is personal; it's up to organizations to monitor and decide how accessible information should be to providers and third parties. However, the unfortunate reality is that agencies often possess more data than they can monitor, which make routine "privacy checkups" both time-consuming and expensive.

New management and transparency tools can alleviate these strains. For example, transparency access tools can enable agencies to catch irregular behavior before sensitive data is compromised and damage is done. Cloud solutions with a central management console can also help give CIOs, CISOs and IT teams critical oversight into the flow of data — providing them authority to set privacy and permissions controls, as well as identify and flag suspicious user behavior.

"With the ability to control, manage and monitor your entire cloud infrastructure from a single place, CIOs and CISOs can glean critical insights, which can then be applied to optimize the infrastructure," Google Cloud's Head of Professional Services for the Public Sector and Security Scott Fleming says. "With the cloud offering consistent management and visibility, IT teams no longer need to log in to each virtual machine and firewall, which means federal customers can have central visibility into cyberthreats. This more holistic approach to threat management offers government customers the ability to leverage database insights readily across their cloud environment without the internal manpower traditionally needed to do so. Ultimately, this holistic view of security operations can accelerate decision making and ensure IT teams enact process consistency when approaching possible threats."

Establishing visibility is a major step toward reducing operational redundancies and granting critical stakeholders the knowledge they need to make impactful, organization-wide decisions in service to security.

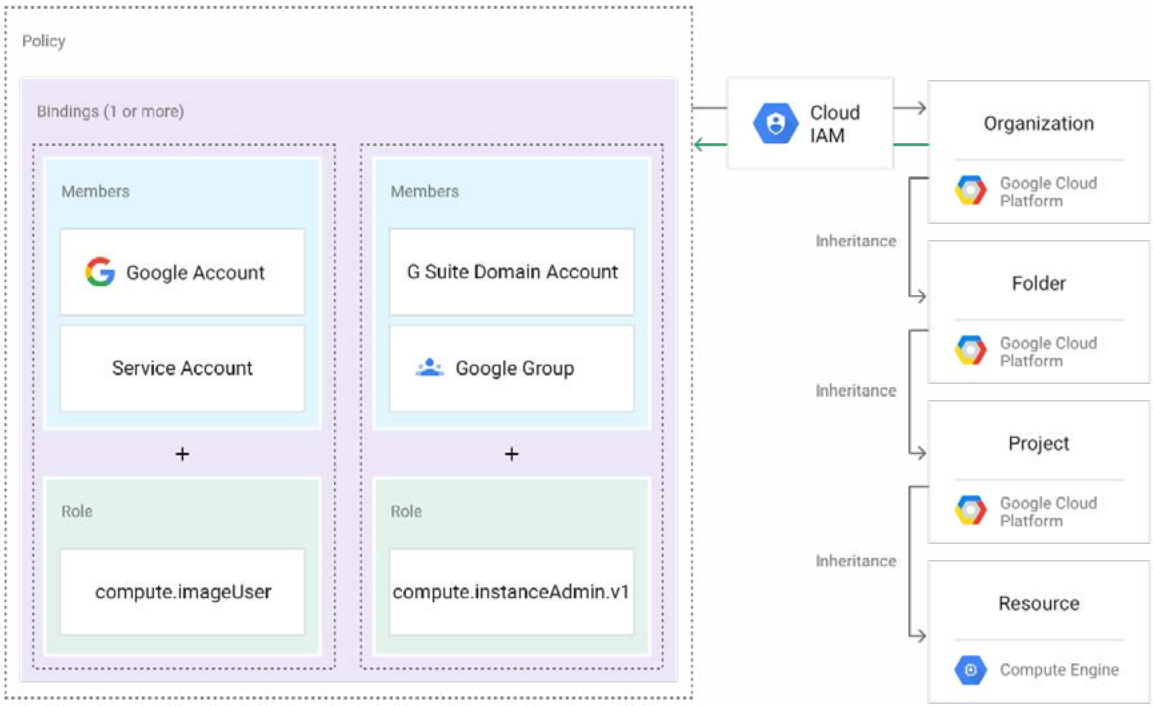


Diagram 1.1 Example of a Google Cloud IAM policy, a collection of statements that define who has what type of access.

Embracing 'Zero Trust' Mentality

By empowering security decision-makers with permissions and privacy controls, the cloud enables agencies to finally realize a 'zero trust' security posture that supports Cloud Smart's initiative of a 'multi-layer defense strategy' where assets are shielded at the data level, in addition to network and infrastructure.

What this means is that the system will assume every user or digital identity accessing the network is a potential threat until it meets appropriate authentication and authorization criteria to access sensitive data. The standard network model employs perimeter security, but this model suffers when attackers are able to successfully breach an organization's network as they are granted unlimited access after that point. In a zero trust approach, access controls and verification shift from the network perimeter to individual devices and users wherever they are, on whatever device.

Moreover, when it comes to protecting data, identity and permissions management is critical. By managing permissions appropriately through the cloud, IT teams can help to prevent breaches while ensuring information reaches the correct people, ultimately helping to safely break down government communication silos.

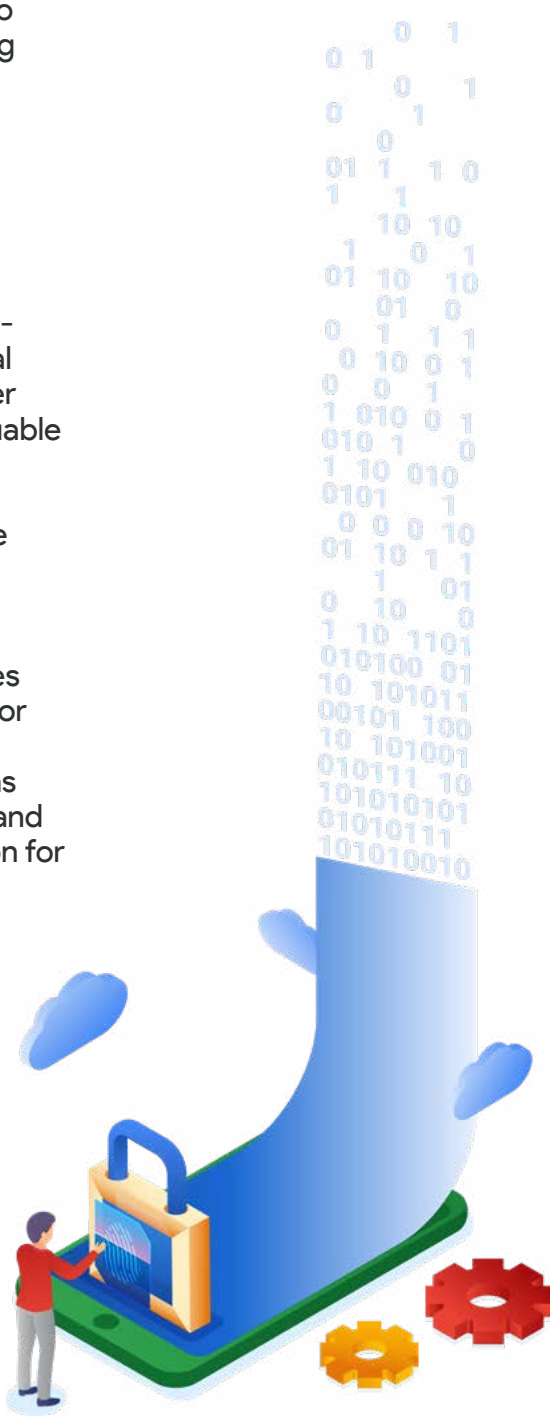
Tools, such as Cloud Identity & Access Management, allow authorized administrators to be more proactive when it comes to data governance and control, helping IT leaders to better manage access to information based on identity.

Moreover, Cloud Audit Logs, a detailed trail audit tool, can help to increase visibility for agencies and cloud users by recording every administrative activity within an organization's cloud platform. That means agencies have the same level of transparency in the cloud as in on-premise environments. A solid comprehensive security strategy also helps outline the clear approach to encryption so agencies understand the handling and protection of their data in an open and communicative relationship with their provider.

Harnessing AI and Machine Learning for Greater Security

More recently, agencies have leveraged cutting-edge technologies in the cloud, such as artificial intelligence (AI) and machine learning, to bolster their cybersecurity capabilities and extract valuable insights from mountains of data.

By embedding AI tools into their operations, the Intelligence Community (IC) and Department of Defense (DoD) are improving their ability to identify worldwide threats before they become demonstrable risks. Back home, civilian agencies are using machine learning algorithms to monitor network traffic patterns and warn or block anomalous behavior indicating that a breach has taken place. This technology is essential today and will only continue to become a critical innovation for security practices in the near future.



Look for Providers on the Forefront of Security

By engaging with the right cloud provider, agencies can fortify their cybersecurity and maintain lock-step compliance. This is particularly beneficial for talent-strapped agencies, where a cloud provider can make necessary adjustments to meet shifting security and compliance expectations around data. This kind of partnership can be instrumental to helping agencies withstand 60% fewer security incidents through 2020, by opting for public cloud infrastructure-as-a-service over protection via traditional data centers.

Agencies should be on the lookout for cloud providers that encrypt data by default at every layer: from data center to device. For example, end-to-end encryption should be an essential feature to any cloud offering under consideration. It's not just the new standard for what it takes to keep data safe today; it's also an integral addition to the policy requirements codified in Cloud Smart. It means that data encryption and automatic updates are by default 'always on', whether at rest or in motion, thus relinquishing government organizations of the responsibility to identify and encrypt data on a case-by-case basis.

By partnering with the right cloud provider, agencies won't just have best-in-class technology at their disposal; they'll also benefit from a dedicated and experienced team of security professionals that are fluent in cloud requirements and system integration. This support will free government IT teams to devote their attention to truly pressing matters — such as long-term strategic transformation and delivering long-awaited improvements to citizen services.

Google Cloud Helps Agencies Stay Focused On the Mission

Cloud security is of the utmost importance to government agencies seeking to keep data in the right hands. Without a trusted cloud partner at the helm, however, data can remain vulnerable. In fact, by 2022, Gartner predicts that at least 95 percent of cloud security failures will be due to client error.

To avoid possible configuration errors and realize true cyber readiness, agencies need to embrace comprehensive security capabilities that can anticipate attacks before they take place, grant authorized users appropriate visibility over data, and scale as needed to foil the most sophisticated threats. With the Google Cloud Security Command Center, agencies receive a flexible platform that integrates with partner security solutions and Google security tools. This makes threat information from Google security tools and partner tools visible from one location to enable rapid response when detecting security anomalies.

Moreover, Google Cloud adds transparency into network health and cloud data operations, ensuring greater commitment to privacy and user transparency. The additional benefit is that government organizations are provided a full stack of tools to enforce encryption, manage cloud workloads, and meet compliance requirements as needed.

The layers of the Google Cloud infrastructure and its devotion to trust through transparency make it a critical partner in the cybersecurity arena. It's a major reason why Google can help agencies succeed in securing, managing and understanding its data, no matter the size of its workforce or its mission.

Security at scale
starts in the cloud.

Check out cloud.google.com/security/ to learn more about Google Cloud's comprehensive security model.

Google Cloud