How Harnessing Google Cloud Helps Agencies Achieve Greater Security

Tapping real-time analytics tools at scale and adopting cloud-based security tools can actually deliver greater security and ROI on cybersecurity investments.

FedScoop Report

THOUGH FEDERAL AGENCIES have come a long way in modernizing their IT infrastructure, the recent COVID-19 response has tested the limits of agencies' cybersecurity architecture to keep pace with threats to their hybrid- and multicloud networks.

"The reality is that agencies have a lot to deal with in their IT environment: too much policy, too much network data, too many tools and a skills deficit", says Dan Prieto, Strategic Executive for Public Sector at Google Cloud.

"An average large enterprise can have upwards of 150 cyber tools installed. That level of complexity and fragmentation hinders the ability of cyberdefenders to operate with agility, scale and timeliness in the face of evolving cyberthreats. To turn the corner on security, organizations need to find the right partners to either take things off their plate or to help transform their productivity," Prieto says.

Agencies need automated solutions, capable of providing a global view of their operating environment, and they also need the ability to store, analyze and respond to security data at scale, he says.

A case for modern cybersecurity

Gaining buy-in for an agencywide approach to cybersecurity is not easy, but today there is too much at risk not to try. And public agencies are discovering, when they try, the benefits can be transformational. That was the case following the decision by New York City Mayor Bill de Blasio to establish New York City Cyber Command in 2017—a specialized unit designed to ensure the security of city government systems and provide incident response.

> New York City faced many of the same challenges federal agencies confront: hundreds of thousands of endpoints; a fragmentation of tools and identity solutions; lots of legacy applications; and limited analytics capabilities.

Dan Prieto
Strategic Executive, Public Sector, Google Cloud

New York City faced many of the same challenges federal agencies confront, recalls Prieto in a recent podcast: hundreds of thousands of endpoints; a fragmentation of tools and identity solutions; lots of legacy applications; and limited analytics capabilities.

"To the extent that historic data was used, it was primarily used retroactively," he says. There was "very little proactive looking for threats, no unified collection and analysis point. Storage of long-term cybersecurity log data was cost prohibitive and analysis was not agile."

What was needed was a greater level of coordination and visibility and that requires a resilient, highly secure and highly scalable data pipeline to help cybersecurity experts detect and respond to threats faster.

"We went with a cloud-first, zero-trust environment because it met our security and reliability needs," said Colin Ahern, Deputy Chief Information Security Officer for NYC Cyber Command, in a recent blog post that discussed how the command structured its capabilities.

In selecting the Google Cloud Platform, NYC Cyber Command gave city cybersecurity experts the ability detect and respond to threats faster by giving them access to:

- A fast, reliable data analysis engine for over 300,000 users.
- A scalable, secure data pipeline to ingest data from city agencies' cloud and on-premise sources, including 400,000 endpoints.
- A simplified identity management and collaboration solution with zero-trust security access controls, totaling about one million systems.
- A collaboration environment for security teams at over 100 state agencies and departments.

The platform also ensures that NYC Cyber Command can support any and all technologies across city government. And by adopting a zero-trust approach to security—based on lessons and best practices from Google's BeyondCorp security model—NYC Cyber Command strengthened and streamlined authorization and access decisions based on the identity of users, their machines and the context of their use of applications and data.

A shift in the security approach

Prieto believes the federal agencies that are still struggling with siloed and legacy systems and security tools spread across both cloud and on-premise environments would quickly benefit from shifting to Google's FedRAMP-approved cloud. It would cost less in the long run than investing to sustain legacy tools. And it would also help agencies to scale up their focus on three key

areas: vulnerabilities, threats and greater ability to measure the consequences from cyberattacks.

Historically, federal agencies have been owners of IT, and their focus was on the vulnerabilities to their network. They built a cyber strategy to respond to questions around equipment, systems configurations or patching priorities. However, today's hybrid- and multicloud environments have made that strategy obsolete; agencies now need to invest in modern and scalable security solutions.

"Security continues to be the biggest perceptual impediment to moving to the cloud. But it isn't because the cloud is less secure," Prieto says. Rather the challenge lies in the massive cultural changes that come with moving toward the cloud.

The need for more modern strategies was made clear in the early COVID-19 pandemic relief effort, which left several key agencies exposed to added risks as they rushed to meet citizen needs. The stimulus program, unemployment insurance and small business loans, for instance, have all been exploited by cyberattacks.

Longer term, CIOs and CISOs also need practical approaches to zero-trust security, available at scale, that address projected budget deficits, finite workforce resources and growing threat vectors.

"That means figuring how to understand risk, how to make resource trade-offs and how to make resources go as far as possible," says Jeanette Manfra, Global Director, Security and Compliance at Google.

A cyber risk framework is critical to help executives identify those areas most vulnerable to the organization and prioritize resources with the largest return on investment. And in fact, after working through this exercise, a growing number of public sector agencies discover that they are able to achieve more effective security controls with greater economies.

Working with a cloud provider like Google makes sense because of their level of understanding of security at a global scale, she says.

Solutions that won't break the bank

That scale — and the ability to harness Google's expertise in artificial intelligence and machine learning can play a game-changing role in identifying and remediating security risks in real time, according to Manfra.

"Google's cloud-based analytic platform, BigQuery, can allow organizations to consolidate and integrate cybersecurity telemetry and essential IT operations data from across all parts of the enterprise; legacy and cloud alike," Prieto says.

Beyond the ability to transform organizations' cybersecurity analytic capabilities, Google provides strong native security capabilities within the Google Cloud infrastructure.

"A good example of this is Google's response to the Spectre and Meltdown vulnerabilities in 2017 and 2018," says Prieto. "Our infrastructure enables automated OS image and patch updates and live migration. So, after the discovery of the Spectre and Meltdown, Google was able to patch and secure its global infrastructure quickly without disruption to customers. It's a serverless approach to security that can make Google an essential security partner to any organization that wants to strengthen its cybersecurity posture."

> **The ability to harness Google's expertise in artificial intelligence and machine learning can play a game-changing role in identifying and remediating security risks in real time."**

Jeanette Manfra
Global Director, Security and Compliance, Google

When New York City moved to a cloud-first, zero-trust environment it strengthened its ability to gather data, monitor networks out to the endpoint and respond to security threats faster.

"One of the differentiators for Google Cloud is our consistent approach to security at scale," adds Chris Johnson, Global Compliance Product Lead at Google Cloud. "We provide customers with the latest revisions of hardware, software and security without requiring them to pay extra, opt in to new environments or require different talent."

Delivering consistency across the enterprise

When organizations move to a hybrid- or multicloud environment, a common misconception is that they can take their existing infrastructure and replicate it. The problem with that practice is that if you have inconsistent application of your security and compliance controls, you're at risk.

That's where the Anthos platform comes in. It gives agencies a single pane of glass deployed across the hybrid-cloud infrastructure to help solve visibility problems around policy and focus security towards outcomes, rather than piling on more tools, according to Johnson.

"Because we have been implementing zero-trust at scale across our global infrastructure for years, there's no reason that any one region will be more or less secure than another," says Johnson. "And zero-trust implementation means that trust doesn't need to be defined at different levels for workloads either."

Johnson adds that Google Cloud has audited and documented its infrastructure to the highest possible baseline, with FedRAMP controls throughout the entire commercial cloud offering.

"That means consistent security controls applied to everything a customer is doing across the globe and consistent security at scale without a specialized workforce and with no specialized purchasing agreements," he explains.

Google Cloud's ability to offer a single pane of glass across the infrastructure, with a number of FedRAMP-approved cloud services, makes it that much more affordable for agencies to take on cybersecurity in a holistic manner.

Learn how Google Cloud helps government agencies improve citizen services, increase their operational effectiveness and deliver proven innovation.

This report was produced by FedScoop and underwritten by Google Cloud.

FEDSCOOP Google Cloud