Google Cloud Press Corner

Google Cloud Announces Zero Trust Offerings for Government

New services will help U.S. government organizations guard against increasing number of cyberthreats and comply with the White House's Executive Order

Washington, D.C., July 20, 2021 -- Google Cloud today announced new Zero Trust offerings for government, a set of services to help U.S. federal, state, and local government organizations implement Zero Trust architecture in accordance with the Biden Administration's Executive Order on Improving the Nation's Cybersecurity and in alignment with National Institute of Standards and Technology (NIST) standards.

"COVID-19 disruption has exposed, accelerated, and introduced new threats to agencies and their digital assets," said Adelaide O'Brien, research director, IDC Government Insights. "Enhanced reliance on virtual work and interactions created new threat surfaces and new vulnerabilities exploited by organized actors. Ransomware, cybercrime, and nation-state attacks have caused significant disruptions and high costs. To mitigate this crisis, it is critical that federal agencies take a sweeping approach to protect the security and privacy of digital assets and cultivate the ability to anticipate, identify, contain, measure, and address cyber-risks."

Google Cloud is launching three new service offerings to help departments and agencies meet Zero Trust requirements:

- Zero Trust Assessment and Planning offering: Delivered through Google Cloud's professional services organization (PSO), the Zero Trust Assessment and Planning offering is designed to help the government reach security goals through Zero Trust architecture planning for core applications and data. Google Cloud's PSO team will advise government organizations on the culture change, policies, and technology needed to achieve a Zero Trust framework—delivered in phases to ensure success within the customer's infrastructure. This new offering will help government agencies leverage Google Cloud tools to support existing assets and infrastructure in cloud-based, on-premises, or hybrid environments.
- Secure Application Access Anywhere offering: Google Cloud is also launching Secure Application Access Anywhere, a new, container-based offering for secure application access and monitoring. Secure Application Access Anywhere can serve as a scalable, highly responsive alternative to government network boundary systems. Delivered in partnership with Palo Alto Networks and Google Cloud's PSO team, this offering leverages Google Cloud's Anthos to deploy and manage containers that provide secure access and monitoring for applications in cloud or on-premises environments. A recent successful prototype of this solution with the Defense Innovation Unit (DIU)—an organization within the Department of Defense—helped accelerate DIU's zero trust journey by providing fast, secure, and controlled access by users to software-as-a-service (SaaS) apps directly over the internet.
- Active Cyber Threat Detection offering: Google Cloud's new Active Cyber Threat Detection services offering can help government organizations quickly determine if they may have been compromised by cyberattacks that they have not yet detected. Delivered through Google Cloud alliance partners Deloitte and Fishtech CYDERES, Active Cyber Threat Detection leverages the proven capabilities of Google Cloud's Chronicle threat hunting, detection, and investigation platform. This offering will allow government organizations of all sizes to readily analyze their historic and current log data to detect threats confidently and quickly.

In addition to these new offerings, Google Cloud also offers several existing solutions that help government agencies accelerate their journey to Zero Trust and to protect against and recover from cyberattacks:

- BeyondCorp Enterprise: Google's Zero Trust access solution provides secure access to internal web applications, SaaS applications, and cloud resources by leveraging access policies based on identity and device contextual information. It also offers users integrated threat and data protection, such as malware protection, data leakage protection, and credential protection.
- Google Workspace also leverages Google's Zero Trust technologies to provide a secure email, communication, and collaboration solution.
- Actifio GO can help organizations to better address ransomware attacks by providing scalable and efficient incremental data protection and a unique near-instant data recovery capability.

Together, these Google Cloud offerings can accelerate the U.S. government's Zero Trust efforts to protect against cyber attacks, and to also better detect, respond to, and recover from cyber attacks when they do occur.

"From COVID-19 to recent ransomware attacks, the events of the past year have demonstrated that government agencies need to rethink security frameworks of the past," said Mike Daniels, vice president, Global Public Sector, Google Cloud. "Google Cloud has the deepest expertise in implementing Zero Trust. We've seen many of these threats on our network and implemented Zero Trust architecture to defend against them more than a decade ago. We are prepared to share our experience operating in a Zero Trust model, along with Google's technologies that are secure by design, to help the U.S. government prevent, detect, assess, and remediate cyber incidents."

About Google Cloud

Google Cloud accelerates organizations' ability to digitally transform their business with the best infrastructure, platform, industry solutions and expertise. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology – all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems.

---

https://www.googlecloudpresscorner.com/2021-07-20-Google-Cloud-Announces-Zero-Trust-Offerings-for-Government