Trust Reimagined: How Agencies Are Securing Their Cloud Architecture in 2022

iStock / gorodenkoff

In Collaboration with

twosix TECHNOLOGIES

By now, there is no doubt that cloud is a major asset to government agencies. It is proven to increase workflow flexibility, reduce strain on IT departments and is more cost-effective for agencies than many legacy operations. However, as agencies shift sensitive data to the cloud amid an ever-evolving threat landscape, many are weighing how security needs to evolve as well.

"Right now is the hardest, most dangerous time to be on the web for a government agency," said Chris Greenlee, Vice President for Intel Operations at Two Six Technologies, a company that works with agencies across the government landscape to implement cybersecurity. "The threat landscape has never been more fraught. Today, Russian and other state-sponsored actors are coming after both private sector and government entities in the United States on a near constant basis."

These risks were addressed in the Biden administration's Executive Order on Improving the Nation's Cybersecurity, which instructs government agencies to move to the cloud and offered guidance on improving security posture. Among the EO's key recommendations is a call to "develop a plan to implement zero trust architecture (ZTA)," an approach that requires verification for anyone or any device trying to access the network.

"The threat landscape has never been more fraught. Today, Russian and other state-sponsored actors are coming after both private sector and government entities in the United States on a near constant basis."

Chris Greenlee
Vice President for Intel Operations,
Two Six Technologies

iStock / Morsa Images

Now more than ever, agencies must deploy tools and technologies built to enable zero trust architecture and protect mission-critical assets. Here, Greenlee offers insight into obstacles agencies face with cloud, how they can stand up the architecture needed to inject the ZTA model into operations, and how security partners like Two Six provide support and solutions needed to make it happen.

Creating a Consistent Cyber Landscape

Although most agencies have already begun cloud journeys, not all of them chose the same providers — some have government cloud, others use commercial cloud and, depending on the agency, some have access to private regions. According to Greenlee, this disparity is causing a lot of security headaches, especially when it comes to data security. With so many cloud providers in the mix, monitoring access becomes increasingly difficult.

“One obvious challenge when you’re moving data into the cloud is that it becomes more difficult to control who has access to your data and your infrastructure,” he said. “Cloud vendors have very thorough security measures in place, but adding a second set of administrators to the mix will always add risk.”

Transfer to the cloud also means data is operating on the open internet, rather than just within the agencies’ individual networks.

“Prior to moving to the cloud, most government agencies were focused on hardening the perimeter of access so that outside actors couldn’t get into the networks,” said Greenlee. “But now their network is extended out into the internet at large, they have a much greater attack surface and hardening that perimeter becomes a much harder job.”

When data moves to the internet it is increasingly vulnerable to cyber attackers, Greenlee explained. If a hacker gains access into a data center, they can then move horizontally through networks into the cloud infrastructure, or vice versa. “Ensuring everyone has the proper level of access just becomes harder once you move into the cloud,” he said. “The challenge that government agencies are going to hit will be enforcing consistent access, especially when data is in transit.”

aws PARTNER

iStock / gorodenkoff

"With zero trust, agencies can enforce consistent policies to ensure data is protected at all times whether in transit, in use or at rest."

Chris Greenlee
Vice President for Intel Operations, Two Six Technologies

Implementing Zero Trust to Secure the Cloud from Anywhere

In convoluted systems, where some portion of an agencies' infrastructure lives on premises in a data center, and some lives in different locations in the cloud, Greenlee stated that it is critical for agencies to know exactly who has access to data, and from what location they are supposed to be accessing that data. That's where zero trust architecture comes into play.

"With zero trust, agencies can enforce consistent policies to ensure data is protected at all times whether in transit, in use or at rest," he said. "It encompasses identity management, allows users to ensure strong access control, segment networks to prevent horizontal traversal and protect data in individual systems or databases."

When implementing zero trust, Greenlee suggests agencies first work with their cloud provider to understand security best practices.

"From there, according to the individual needs of that agency, they can ensure a strong identity management program is in place to identify who is on their networks and ensure all actions are authorized," he said.

Zero trust applications that control the network connections between systems should also be implemented, Greenlee explained, so if one system is compromised, threat actors can't use it to move into more sensitive systems and exfiltrate data.

iStock / gilaxia

“The more we utilize the cloud, the more we need to ensure that we’re building in security from the ground up.”

Chris Greenlee
Vice President for Intel Operations, Two Six Technologies

Protecting Data at Scale with TrustedKeep

Greenlee and his team at Two Six enable agencies’ secure shift to the cloud with their TrustedKeep platform. TrustedKeep allows users to encrypt data at scale using zero trust architecture, while simultaneously controlling who has access to encryption keys that are stored separate from where the data lives, protecting it from any inadvertent access.

“One of the challenges in protecting data is to provide a consistent answer across both the data center and the cloud,” said Greenlee. “We designed TrustedKeep to handle consistent policy enforcement combined with scalable object level encryption using FIPS 140-2 validated encryption algorithms.”

The tool is also designed to present a policy enforcement point in front of resources both on premise or in the cloud so agencies can protect the data constantly and control who has access to different networks.

Especially in today’s political climate, sophisticated threat actors are only advancing their efforts. Greenlee believes that agencies have no time to waste in deploying solutions like TrustedKeep to ensure their cloud environments have zero trust security built in to meet the requirements of the EO, safeguard critical data and achieve mission success.

“Agencies are required to make plans to move more systems to the cloud, but also to move toward zero trust so that they can protect data in transit,” he said. “The more we utilize the cloud, the more we need to ensure that we’re building in security from the ground up.”

Learn more about how TrustedKeep can help secure your cloud architecture with zero trust.