New cloud security considerations for government

Agencies need to move toward a more robust framework for securing users and data in the cloud

Mike Rosa
Vice President of Public Sector Security, Salesforce

Alicia Rosenbaum
Vice President and Associate General Counsel, Salesforce

AT ALL LEVELS of government, agencies are trusted to hold and protect some of the most sensitive data in the world, including financial, health and national security data. Protecting that information is critical to maintaining the public's trust, delivering services and protecting citizens.

Before the COVID-19 pandemic closed government offices, many agencies required employees to "badge-in" in order to verify their identity and ensure they have authorization to access specific workplace locations. But with a distributed workforce, cloud has enabled employees to have faster and more reliable remote access to critical information and systems. Lack of user authentication and validation for data access in this new environment can expose government information and resources to the potential risk of misappropriation.

Initially, FedRAMP gave the government's early cloud adopters the ability to "trust but verify" based on a set of standards and practices, and officials wisely added third-party assessment organizations as part of the verification process. But this is no longer enough, as recent data breaches have demonstrated.

A zero trust standard protects all parties

The vast majority of attacks on government systems can be prevented by following common-sense principles, principles known to prevent breaches. A zero trust architecture helps agencies implement those protections. It is a shift from "trust but verify" to "trust but verify and validate."

Zero trust is not a single product or service. Previously, organizations deployed a perimeter-based approach to security, treating the organization's network as a trusted zone and placing security defenses at the edges. A zero trust approach never assumes that an organization is safe and sound within its own "secure" corporate network; rather, it places control around the data assets themselves. The purpose is to create a framework in which a person seeking information is authenticated every step of the way, data is isolated and protected, and administrators have the ability to audit who's been where and done what.

The principles are similar to the process you would go through to board a plane. Someone validates your identity when you get your ticket, check your bags, pass through the security checkpoint and right before you are allowed to walk onto the plane.

In a technology stack, tools that create these "checkpoints" are known to prevent breaches and should be common on any secure platform. They include multi-factor authentication, which is one of the core

Shutterstock/FCW Staff

> With the zero trust model, the purpose is to create a framework in which **a person seeking information is authenticated every step of the way.**

tenets of zero trust, and encryption of sensitive data while it's in transit or at rest.

The right partnerships ensure success

Achieving a zero trust framework requires agencies to pick the policies and security practices that work best for them based on the types of data they handle and the users who need access. But it doesn't stop there. Agencies must continuously monitor, iterate, remediate and improve to ensure an appropriate level of cybersecurity. Implementing this framework will require the right partnerships and government and industry collaboration.

Salesforce supports our customers in the journey toward zero trust by building security capabilities into our platform, including multi-factor authentication and multiple ways to encrypt data at rest.

A zero trust approach to security is necessary so that agencies can confidently use cloud technology and so that they can provide assurance and data security for constituents sharing sensitive information with the government. For this to happen, agencies and their industry partners must move from "trust but verify" to "trust but verify and validate." ■

Mike Rosa is Vice President of Public Sector Security and **Alicia Rosenbaum** is Vice President and Associate General Counsel at Salesforce.