Defense-in-depth strategies in the cloud age

Constantly evolving tools are helping agencies take a more proactive stance on security

Brent Hansen
Federal CTO and Director of Sales Engineering for Cloud Protection and Licensing Activity, Thales

CYBERSECURITY THREATS TARGET the heart of our country and our government by, for example, potentially compromising our elections, damaging the United States brand or seeking to breach our mission-critical systems. Agencies are under constant threat of their data being manipulated or stolen.

According to Thales's annual Data Threat Report-Federal Edition, at any given time 60 percent of federal agencies' networks have been compromised. In 2018, 35 percent had been breached in the past year, and 14 percent had been breached multiple times.

Whether the adversaries are cyber terrorists, hacktivists or malicious insiders, the goal is gaining access to data to steal, manipulate or hold it for ransom. Even if stolen data is retrieved, it has been compromised forever.

A modern approach to data security

Historically, those resources were housed in agency data centers, but the expansion of the internet of things and the expedited migration to the cloud have created an attack surface that is significantly larger than it used to be. Fortunately, simply migrating infrastructure and software to the cloud improves security because they are now easier to update and manage. The cloud's more agile, sophisticated environment allows agencies to modernize their approach to data security while they're modernizing their applications.

It becomes the cloud provider's responsibility to ensure the availability and performance of those systems, including the ability to handle large workloads and spin up resources as needed. But agencies must not lose sight of the fact that they're ultimately responsible for securing their own data.

Encrypting data when it's created

We're entering a new frontier, and industry and government must work together to evolve existing strategies so that data is protected whether it resides in agency data centers or in the cloud.

In "as-a-service" environments, agencies should run encrypted workloads and keep their encryption keys in an on-premises data center where they can protect those keys using the FIPS 140-2 boundary key appliance. That way, agencies can supply encryption keys to their cloud providers and revoke them if necessary.

Finally, agencies should look for vendors that can weave platform-as-a-service offerings into the fabric of their software so that data is encrypted from the moment of inception. At Thales, we can go out to the boundary of an application, encrypt data when it's created and pass it through the application stack until it ultimately resides in a database, where it is protected in motion and at rest.

Security policies will continue to evolve. At Thales, we're committed to finding innovative ways to adapt and improve the best approaches to securing government data in an ever-changing IT ecosystem.

Brent Hansen is federal CTO and director of sales engineering for cloud protection and licensing activity at Thales.