CASE STUDY

Protecting a Nation in the Cloud

Many federal agencies are in the process of shifting sensitive information to public cloud systems. This movement started back in 2011 when the goal of transforming the federal government into a "cloud first" organization was first introduced. The need was great: Nearly 75 percent of the government's $80 billion IT budget[1] had been spent maintaining expensive legacy technologies that lack the speed or scalability offered by the cloud. Efforts continued in 2017 with an executive order[2] to move all federal civilian agencies to a "shared services" IT infrastructure and in 2018 with the Modernizing Government Technology Act[3], which encouraged the move to commercial cloud computing.

Trustwave®

Client Spotlight

This government sub-agency offers web applications that millions of American citizens use every day. In fulfilling its mission, the sub-agency generates and collects massive troves of data that is rapidly outgrowing its physical server network.

The Challenge

A major government sub-agency needed a database security tool that spanned both Amazon Web Services and Microsoft Azure, the two commercial cloud providers it selected. To raise the stakes even higher, the sub-agency handled not just run-of-the-mill data, but the personally identifiable information of American citizens, including social security and driver's license numbers. As such, it required assurance that its cloud operations would meet or exceed the stringent regulatory standards to which its physical servers had previously been held.

> “*DbProtect scans not just for misconfigurations, but also user rights. And we can therefore determine where high levels of privileges on weakly configured databases trigger internal and external threats.*”
>
> – Thomas Patterson, Senior Product Manager, Trustwave

The Solution

The government sub-agency enlisted Trustwave DbProtect, a highly scalable security platform that would allow their organization to secure their databases with distributed architecture and enterprise-level analytics. The platform would enable the agency to uncover configuration errors, while also identifying access control issues and missing patches. Moreover, it offers a unified view of its database and risk levels through a single dashboard that flashes real-time information about vulnerabilities, user privileges, anomalies and incidents. And crucially for the government agency, DbProtect can comply with more than one set of security and regulatory policies and be easily deployed across any cloud computing system. Trustwave was there every step of the way, ensuring that the sub-agency's data was secure and compliant as it shut down its on-premise equipment. Today, the sub-agency enjoys capabilities far beyond what the old government server system allowed—and with significantly less manual work.

Americans don't 't realize they routinely accesses a government database that is being constantly scanned by DbProtect. And because Trustwave's platform is zealously guarding against vulnerabilities before they escalate into breaches that must be disclosed to the public, it's safe to say that, in this case, ignorance is bliss.

Industry Threat

The federal government has long been situated directly in the crosshairs of bad actors who are eager to hack into the United States' vital assets, access top-secret data and cause potentially catastrophic mayhem. Though Congress is put under constant pressure to increase cybersecurity spending[4], those incremental increases may still not be enough. Threat actors are mercilessly targeting devices and networks, and are weaponizing our own technology innovations against us.

> “*The most frequent feedback we receive from Federal customers is that DbProtect helps address their concerns around securing databases across multiple clouds.*”
>
> – Bill Rucker, President Government Solutions, Trustwave

[1] Source: Beckerman, M. "Commercial cloud is the bipartisan solution to modernizing government IT." Federal News Network, 20 April 2018.

[2] Source: "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The White House, 11 May 2017.

[3] Source: Mulvaney, M. "Memorandum for the Heads of Executive Departments and Agencies." Executive Office of the President., 27 Feb. 2018.

[4] Source:"24. Cybersecurity Funding." The White House, Accessed: 22 April 2019.