



Modernizing FedRAMP is Essential to Enhanced Cloud Security

By [Tom Gann](#) on Sep 10, 2019

According to an analysis by McAfee's cloud division, log data tracking the activities of some 200,000 government workers in the United States and Canada, show that the average agency uses 742 cloud services, on the order of 10 to 20 times more than the IT department manages. The use of unauthorized applications creates severe security risks, often resulting simply from employees trying to do their work more efficiently.

By category, collaboration tools like Office 365 or Gmail are the most commonly used cloud applications, according to McAfee's analysis, with the average organization running 120 such services. Cloud-based software development services such as GitHub and Source Forge are a distant second, followed by content-sharing services. The [average government employee runs 16.8 cloud services](#), according to the [2019 Cloud Adoption and Risk Report](#). Lack of awareness creates a Shadow IT problem that needs to be addressed. One of the challenges is that not all storage or collaboration services are created equally, and users, without guidance from the CIO, might opt for an application that has comparatively lax security controls, claims ownership of users' data, or one that might be hosted in a country that the government has placed trade sanctions on.

To help address the growing challenge of security gaps in IT cloud environments, Congressmen Gerry Connolly (D-VA), Chairman of the House Oversight and Reform Committee's Government Operations Subcommittee, and Mark Meadows (R-NC), Ranking Member of the Government Operations Subcommittee, recently introduced the [Federal Risk and Authorization Management Program \(FedRAMP\) Authorization Act \(H.R. 3941\)](#). The legislation would codify FedRAMP – the program that governs how cloud security solutions are deployed within the federal government, address agency compliance issues, provide funding for the FedRAMP Project Management Office (PMO) and more. The FedRAMP Authorization Act would help protect single clouds as well as the spaces between and among clouds. Since cloud services are becoming easier targets for hackers, McAfee commends these legislators for taking this important step to modernize the FedRAMP program.

FedRAMP provides a standardized approach to security assessment and monitoring for cloud products and services that agency officials use to make critical risk-based decisions. Cloud solutions act as gatekeepers, allowing agencies to extend the reach of their cloud policies beyond their current network infrastructure. To monitor data authentication and protection within the cloud, cloud access security brokers, or CASBs, allow organizations deeper visibility into their cloud security solutions. In today's cybersecurity market, there are many cloud security vendors, and organizations therefore have many solutions from which to choose to enable them to secure their cloud environments. [McAfee's CASB, MVISION Cloud](#), helps ensure that broad technology acquisitions maintain or exceed the levels of security outlined in the FedRAMP baselines.

McAfee supports the FedRAMP Authorization Act, which would bring FedRAMP back to its original purpose by providing funding for federal migration and mandating the reuse of authorizations. FedRAMP must be modernized to best serve government agencies and IT companies. We look forward to working

with our partners in Congress to move this legislation forward. Additionally, we have seen that agencies overuse waivers to green light technology that sacrifices security for expediency. We must find a better way to thread this needle and ensure that broad technology acquisitions maintain or exceed the levels of security outlined in the FedRAMP baselines as this bill works its way through the legislative process and finds its way to the President's desk for signature into law.

[About the Author](#)

[Tom Gann](#)

Tom Gann is the Chief Public Policy Officer at McAfee. In this capacity, he manages the U.S. and international advocacy activities and partners with the public relations team to help position McAfee as an industry leader in capitals around the world. Prior to joining McAfee, Gann managed cyber security policy, government relations, alliances, product marketing, ...

[Read more posts from Tom Gann](#)

