AGENCY SPOTLIGHT: NAVY

Michael Afonso / Unsplash

Automation Offers Efficient Path to ATO

In the 21st century, the Department of Defense, intelligence agencies, and government agencies large and small have come to rely on increasingly advanced and complex software applications, but getting them secured and in place is not easy when they're using 20th century processes, like manually gathering security data to do it.

Even though it's meant to ensure software and IT systems inside agencies' enterprise operations are documented as secure, getting an official Authority to Operate (ATO) from an authorizing agent, including the General Services Administration's secure cloud adoption service FedRAMP, can become a labor-intensive, time-consuming ordeal. The process can rely only on a handful of risk and security managers tracking down security data manually.

A signed ATO ensures software and systems securely meet Federal Information Security Modernization Act (FISMA) standards as well as National Institute for Standards and Technology Risk Management Framework (NIST RMF) specifications. The process is a detailed review and analysis of potential IT systems and the risk they might present. Although the ATO process and NIST framework were meant to be roadmaps agencies could follow to ensure security, they are often reduced to labor-intensive exercises that can slow technology adoption and efficient operations, and blunt agency missions.

"Properly used, the ATO process was supposed to equal security," said Dale Hoak, technical delivery manager at RegScale, the world's first real-time Government Risk and Compliance (GRC) platform. "The ATO process has become so labor-driven and time-intensive that the roadmap has become a requirements checklist. When you're just checking a box and not validating security, that's a problem."

The slow journey to gathering pertinent security data can have lasting impact down the road as well, as agencies discover two or three years after the system has been implemented that significant gaps have developed, said Tyler Sweatt, chief revenue officer at Second Front Systems, a provider of a continuously certified PaaS platform.

There are many ways to navigate the ATO process, but automating the verification processes that inform the ATO can be a valuable key to getting the authority quickly and efficiently. Platforms like Second Front's continuous authorization to operate (cATO) PaaS platform and RegScale's real-time GRC platform solutions can automate gathering backing details inside an organization and effectively packaging that data for submission to ATO certification agents such as FedRAMP, according to Sweatt and Hoak.

Second Front's Game Warden platform-as-a-service (PaaS) platform, said Sweatt, can accelerate adoption of advanced modern commercial software applications for the DoD and national security organizations. Apps hosted on Game Warden run through an automated continuous integration/continuous deployment (CI/CD) pipeline and then inherit the platform's authorities to operate on government networks. The PaaS decreases time to market significantly and cuts time, labor, and associated costs of legacy ATO timelines.

piranka / iStock

RegScale's real-time GRC platform, said Hoak, allows agencies to take any cybersecurity framework, digitize it, automate it, analyze it, and report on it. The platform allows agencies to automate the NIST RMF, generating audit ready documentation on demand for FedRAMP ATO approval in human-readable Word and Excel as well as machine-readable NIST OSCAL XML or JSON This shortens that tedious process from six months to six weeks, he said.

The two solutions offer two paths for quicker, more efficient ATOs, at a time when defense agencies need to get cutting-edge apps in place as quickly as possible.

"Our adversaries aren't taking 18 months to deploy their software," said Sweatt.

Learn more at regscale.com and secondfront.com.

PRODUCED BY FCW

SPONSORED BY carahsoft. RegScale SECOND FRONT SYSTEMS