

Federal access to open source: How GitHub's platform opens wider universe of software development

By achieving FedRAMP operating authority, GitHub's Enterprise Cloud allows federal users to collaborate with millions of open source software developers.

BY FEDSCOOP STAFF

Just as Microsoft Corp.'s acquisition of GitHub solidified the code-hosting service's place in the software development world, GitHub's recent announcement that its Enterprise Cloud has achieved FedRAMP authorization delivers, for the first time, a way for government agencies to securely participate in the entire open source development universe.

Traditionally, federal users have leveraged GitHub's team plan or GitHub Enterprise Server platform by hosting it on-premises or in their own private cloud. GitHub Enterprise Cloud, which resides entirely in the cloud, has been available for the past year. It offers the ability to use single sign-on and a secondary identity provider (including government PIV and CAC cards) and includes expanded support and service level agreements.

"We have historically had [government] customers on GitHub.com, but they were either doing it as shadow IT under a team plan or non-mission critical systems. Because GitHub.com did not have an ATO [authority to operate] it was never deemed appropriate for most organizations' day-to-day mission-critical applications," said Jamie Jones, GitHub principal architect.

That changed in October, with GitHub achieving FedRAMP operating authority under a relatively new process called FedRAMP Tailored, which provides a more streamlined security approval process that is better suited for software-as-a-service providers such as GitHub.

"We're now giving them a place where they can do this in the cloud on GitHub managed and hosted hardware," said Jones.

The features on GitHub Enterprise Cloud are quickly gaining parity with, and in some cases exceeding, the features of GitHub's Enterprise Server, its on-premises offering.

But the big advantage of switching to GitHub Enterprise Cloud is it will give agencies of all sizes access to the entire GitHub universe of open source development and collaboration resources — and the vast community of developers contributing to those resources.

"In the average software product developed today, more than 57 percent of the code within it is actually open source or code that comes from other projects," said Jones. "It's become critical for modern software to be able to collaborate with the open source marketplace."

And the size of that marketplace is mind-boggling. At its most recent annual user and developer conference, GitHub announced it has more than 31 million users currently on GitHub.com. Now, agencies that were once confined to operating within an enterprise GitHub community (anywhere from a handful to a few thousand developers) have access to a much larger code base and talent pool.

"We're now giving them a place where they can do this in the cloud on GitHub managed and hosted hardware

- Jamie Jones

Governments all over the world are using GitHub. At last count, 143 U.S. federal civilian agencies, 14 Department of Defense agencies and 48 state agencies were leveraging GitHub to collaborate on code, data, policy and procurement, according to GitHub figures. In addition to the platform's 31 million users, the number of organizations on it has jumped 40 percent to 2.1 million, as has the number of code repositories, which now stands at more than 100 million.

“*At last count, 143 U.S. federal civilian agencies, 14 Department of Defense agencies and 48 state agencies were leveraging GitHub to collaborate on code, data, policy and procurement*

- Jamie Jones

FedRAMP Tailored

GitHub is among the first cloud service providers to take advantage of FedRAMP Tailored. FedRAMP was originally aimed at helping agencies certify that a cloud computing service met a long list of federally mandated security controls. The idea was that other agencies, once certified, could adopt that same service without repeating the same certification process. But the process was time-consuming, expensive and targeted initially toward infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) providers — in other words, the traditional large cloud providers like AWS, Google, IBM, Microsoft and others.

The FedRAMP Program Office within the General Service Administration, however, recognized an opportunity to fine-tune FedRAMP specifically for software-as-a-service (SaaS) providers that handle low-risk, low-impact data and aren't responsible for a host of network security controls.

According to Ashley Mahan, acting director of the FedRAMP Program Office, the FedRAMP Tailored assessment process focuses only on a subset of the NIST 800-53 technical controls and places a greater focus on policies, procedures and training surrounding the management and use of public or non-sensitive data.

“What that does is it affords for a fast and efficient authorization process that lessens a vendor's time to market and really speeds up the timelines on when an agency can make use of these innovative cloud technologies,” Mahan said.

That put the economics of FedRAMP operating authority within reach for GitHub for the first time, according to Jones. But it also opens the door for agencies to work with a wider range of software-as-a-service providers.

“FedRAMP Tailored was really developed as a way for SaaS solutions, such as GitHub, to get a FedRAMP authorization so that they could be easily consumed by the federal government while taking into account the appropriate security these systems require, as opposed to the traditional cloud providers,” said Jones.

Agencies can now simply go to the FedRAMP marketplace and pull down the authorization to begin using the platform with confidence that it meets the baseline security



requirements established by the government for SaaS. “For some agencies it can reduce the time it takes to receive an ATO to mere minutes,” said Jones.

“*One key benefit of using the FedRAMP-authorized Enterprise Cloud is we can now support your agency's identification and authorization tools*

- Jamie Jones

The Business Case

According to Jones, there is no reason for an agency that is currently using GitHub under a team or enterprise license not to move up to the FedRAMP-authorized Enterprise Cloud version — and in most circumstances, there are a number of advantages.

“One key benefit of using the FedRAMP-authorized Enterprise Cloud is we can now support your agency's identification and authorization tools,” he said. “For the extra capabilities we are providing, including faster support requests or the ability to use SAML and your external identity providers, it's far less of an administrative burden,” said Jones.



The FedRAMP-authorized GitHub Enterprise Cloud also offers enhanced security services and features that are not yet available for Enterprise customers.

For example, GitHub recently rolled out a vulnerability alert service. It began last year through a collaboration with the National Vulnerability Database to provide alerts directly through the FedRAMP-authorized GitHub Enterprise Cloud for vulnerabilities in Ruby, JavaScript, Python, Java and .Net. GitHub has identified more than 4 million vulnerable dependencies and has resolved more than 1 million of those during the past year.

If GitHub finds that you are using a library with a known vulnerability, the alert service will flag it for you and alert the repository administrators. GitHub will even alert the developers to potential upgrades that are known to fix the vulnerability, said Jones.

Offering increased security and vulnerability protections will translate into enhanced business speed for government agencies, according to Jones.

“We’ve all heard stories about how when government staff or contractors get hired and it’s days or weeks before they have access to the proper hardware and systems to even start working on their jobs. But by being able to access GitHub from the Internet, rather than behind an agency firewall, and still be able to use it in a secure and compliant way, this should allow agency users to get up to speed and working faster,” he said.

“Traditionally, we’ve seen great uptake in use of GitHub Enterprise Server, which is the on-premises version of GitHub,” Jones said. “But we’re hoping that the FedRAMP authorization for Enterprise Cloud will really allow our federal customers to take advantage of SaaS and GitHub running on the internet and in the cloud.”

“*Making the move from GitHub Enterprise Server to the GitHub Enterprise Cloud happens seamlessly behind the scenes*

- **Jamie Jones**

Making the move from GitHub Enterprise Server to the GitHub Enterprise Cloud “happens seamlessly behind the scenes,” said Jones. “As you move over to Enterprise Cloud, the key advantage is you’re able to move a lot of the infrastructure and workload into the cloud, which helps you meet the cloud-first mandate,” he said.

Find out more on how FedRAMP-approved GitHub Enterprise Cloud can expand your agency’s software development capabilities.

This article was produced by FedScoop for, and sponsored by, GitHub.

fedscoop

GitHub