Enterprise open source: The best of both worlds

The combined power of community-driven innovation and industry-leading technical support is expanding the government's capacity for innovation

Open source technology accounts for a significant portion of most modern applications, with some estimates going as high as 90%, and it is the foundation of many mainstream technologies.

"Phones, cars, planes, and even many cutting-edge artificial intelligence programs use open-source software such as the Linux kernel operating system, the Apache and Nginx web servers, which run over 60% of the world's websites, and Kubernetes, which powers cloud computing," wrote Hila Lifshitz-Assaf and Frank Nagle in a Harvard Business Review article.

Open source's strength lies in the fact that a broad spectrum of developers contributes to and continually improves the underlying code, which keeps the software dynamic and responsive to changing needs. In addition, enterprise open source solutions have sprung up to augment the technology's flexibility and innovation with the ongoing support of industry experts. By providing the best of both worlds, such solutions represent a powerful arsenal of tools for addressing the government's most pressing challenges.

Tackling the top priorities of government CIOs

In a recent pulse survey of FCW readers, 93% of respondents said they were using open source technology to some degree, with 18% of those respondents saying it's a key component of their agencies' IT systems.

In a research study of federal technology leaders conducted by GBC on behalf of Carahsoft, participants were asked what they see as the biggest benefits of using open source solutions. Cost-effectiveness was the clear winner at 58%, followed by flexibility and agility (33%). Participants also cited the fact that such solutions are designed to work in the cloud (26%), offer full visibility into the codebase (25%) and help agencies avoid vendor lock-in (23%).

The government is using open source technology to tackle some of the biggest challenges that agency CIOs face. Sixty-four percent of Carahsoft study participants said they use enterprise open source solutions for application

Open source by the numbers

Sources: Carahsoft, FCW, Gartner

45%

Organizations worldwide that will have experienced software supply chain attacks by 2025

69%

FCW survey respondents who said open source has a role to play in facilitating IT modernization

58%

Federal IT leaders who cited cost-effectiveness as one of the biggest benefits of open source

53%

Federal IT leaders who said they were somewhat or much more likely to choose a software vendor that contributes to the open source community

development, while 49% use them for infrastructure modernization, 44% for application modernization and 40% for digital transformation.

Experts point out that using open source technologies can also help the government from a workforce perspective. Large communities of developers and users are well-versed in the technologies; by contrast, training in proprietary software is typically only available from the company that created it. As a result, there's a much lower barrier to learn open source software, and agencies will have an easier time finding job candidates who have those skills.

Protecting the digital supply chain

Interestingly, 55% of respondents to FCW's survey said open source can be an integral solution for strengthening cybersecurity. That number reflects a positive trend toward a better understanding of open source's inherent security. In Carahsoft's survey, 43% of respondents said open source and proprietary software are equally secure, but only 11% said open source is more secure than proprietary software. The study dug deeper to ask about the ways in which security is a benefit of using enterprise open source. Participants cited the fast availability of vulnerability patches, the ability to use well-tested open source code for in-house applications and the fact that security patches are well-documented.

Earlier this year, White House officials convened a group of government and private-sector experts to discuss ways to prevent defects and vulnerabilities in open source software and improve the processes for identifying problems, fixing them and then distributing those fixes. Among other things, "participants discussed ideas to make it easier for developers to write secure code by integrating security features into development tools and securing the infrastructure used to build, warehouse and distribute code," according to a White House statement released after the meeting.

In addition, participants discussed ways to accelerate the use of software bills of material (SBOMs), as required in President Joe Biden's Executive Order on Improving the Nation's Cybersecurity. According to the National Telecommunications and Information Administration: "An SBOM is a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships."

The focus on visibility into software and all its components has increased in response to the growing number of attacks on the digital supply chain, which Gartner lists as a top security and risk management trend in 2022. "As vulnerabilities such as Log4j spread through the supply chain, more threats are expected to emerge," a Gartner press release states. "In fact, Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."

Cross-pollination between government and industry

Given the concerns about the digital supply chain, it may come as a surprise that the Defense Department has championed the use of open source technology. In an online document that addresses frequently asked questions about open source software (OSS), DOD's CIO office states that "continuous and broad peer review, enabled by publicly available source code, improves software reliability and security through the identification and elimination of defects that might otherwise go unrecognized by the core development team."

The document addresses concerns and misconceptions head-on. "OSS (as well as proprietary software) may indeed have malicious code embedded in it. However, such malicious code cannot be directly inserted by 'just anyone' into a well-established OSS project....OSS projects have a 'trusted repository' that only certain developers (the 'trusted developers') can directly modify. In addition, since the source code is publicly released, anyone can review it, including for the possibility of malicious code."

Choosing enterprise open source solutions can further ease security concerns because those technologies and services come with the support of industry experts who keep the software up-to-date and secure without compromising any of its flexibility and innovation.

Within DOD, the Air Force has been a pioneer in using cutting-edge approaches for software development. Its Platform One merges the top talent from across the Air Force's software factories and serves as an official DevSecOps enterprise services team for all of DOD. Air Force CIO Lauren Knausenberger told FCW that community-based and enterprise open source components feature prominently in the technology offered through Platform One because of their cost-effectiveness, security and flexibility.

She added that technology companies play a key role in helping the Air Force meet its mission goals. "Because we don't have thousands of software developers, we have vendor partners help us deploy our platforms to get the most out of our open-source software, coding side by side with us," Knausenberger said. "That's part of how we continue to cross-pollinate and make sure that we can bring commercial best practices into government."

The power of enterprise open source technologies lies in a combination of crowdsourced talent and industry expertise. As agencies expand their use of such technologies, they maximize their ability to achieve mission success in the most secure, agile and innovative way possible. ■