NOVEMBER 26, 2021

# Does Open-Source Software Hold The Key To Data Security?

BY JAMES CROWLEY

## Open-Source Software Data Security

Whether you realize it or not, open-source software is everywhere in our everyday tech, from mobile phones to air travel, from streaming Netflix to space exploration. Open-source software has played a pivotal role in the digital transformation revolution, and due to its popularity, availability, and rapid uptake, the market is growing exponentially. Research and Markets forecast global open-source services to reach $66.8 billion by 2026, at a CAGR growth of approximately 21.6%.

Due to heavy investment in cloud-based solutions and early adoption of advanced technologies, North America has been the largest contributor to this growth. Open-source initiatives have realized benefits that include reducing cost of ownership, improving security, and a rapid turnaround of higher quality enterprise solutions. First, let's take a closer look at understanding open-source software.

### Open-Source Software: The Basics

Put simply, open-source is software for which the source code is freely available for anyone to inspect, modify, enhance, and redistribute. The source code is fundamental in controlling digital programs and application software, and typically only seen by programmers or DevOps teams who are building software. By making source code public, an entire community of developers are able to share insights and knowledge, and benefit from everyone's experiences, collaborating to quickly find and fix bugs, enhance security, and bring novel tech to market.

With open-source software, 'freely available' doesn't necessarily mean 'free of charge'. Depending on the license type, however, the original author waives any exclusivity rights to profits from use by others of a modified version. The alternative is closed-source software, where the source code of proprietary software remains under exclusive control of the original author, and might lead to vendor lock-ins. Examples of closed-source software include Adobe Acrobat Reader, Google earth, and Microsoft Windows, whereas Mozilla Firefox, Linux, JavaScript, Angular and SourceLoop are examples of open-source software.

The impact of open-source software on websites has been phenomenal, with open-source web servers Apache and nginx having more than 60% of the market share between them (nginx – 35.3%, Apache – 25.9%, as of March 2021). In addition, Linux software powers around 70% of the top 10 million Alexa domains. Such is the success of open-source software, that since the early 1990s, around 200 companies have been created using an open-source foundation and between them generating over $10 billion in capital.

### How Open-Source Software Enhances Security

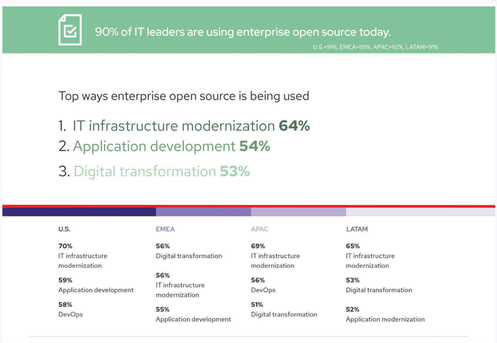
Increasing security by making software more freely available may sound like a complete contradiction. Just as more and more source code is made visible, so too are any weaknesses or security gaps, which means the transparent nature of open-source software actually works in its favor.

The sheer scale in the number of developers around the world, collaborating and contributing to open-source projects, means 'many eyes' are inspecting source code for security vulnerabilities or flaws.

Leveraging this community of pooled resources and expertise from developers, security is heightened as potential bugs are quickly detected and fixed. With closed-source software, broken code can only be repaired by the vendor, which may take longer. With closed-source software, you have to place your trust in the vendor that its software is secure, but with open-source, DevOps teams are able to verify the security of source codes for themselves.

In addition to the 'many eyes' effect, open source software projects often have access to tools that enable a DevSecOps approach to managing vulnerabilities in a code base. GitHub provides supply chain security tools as part of its native dependencies. These tools are often open source themselves, utilize open vulnerability databases, and provide automation to patch vulnerabilities.

When it comes to security, rather than saying open-source software is 'more secure' than closed-source, it is the speed at which security gaps are identified and resolved that makes it a more trustworthy and powerful option. With a literal small army of developers constantly testing and re-testing code, the more bugs that are resolved, the more secure open-source software becomes.




To emphasize the adoption of open-source software, in a recent RedHat survey, 84% organizations said that enterprise open source was a key part of their security strategy, with some solutions providers opting to only use open-source software, like we do here at SourceFuse Technologies. It means we are not having to reinvent the wheel each time, when building new applications, plus the ability to swiftly release new releases or patches mitigates any security risks for our customers.

### Summary

The advancement of the open-source collaboration and transparency culture has brought advantages to many. From young developers learning coding best practices, to large enterprises with limited in-house proficiencies. The speed and agility at which state-of-the-art tech is brought to market is a direct result of the pooling of knowledge and experiences.

DevOps teams have the opportunity to bring about impactful change and improvements to the security of open-source software, to source codes that would have been previously inaccessible. And in the spirit of openness and sharing, each enhancement and improvement is then shared back to the community, so that source codes continually evolve for the future.

By James Crowley

## JAMES CROWLEY

James Crowley, **Senior Enterprise Architect, leads SourceFuse's enterprise architecture development**. He specializes in Rapid Application Development (RAD) for the Enterprise, with a focus on product delivery within compressed time-lines. As a polyglot engineer and architect, he crafts solutions in multiple technology stacks and has architected, built, and deployed enterprise solutions to AWS, Azure, and Google Cloud. One of his areas of expertise is identity and access management, and he has created custom SSO solutions using Okta, AWS Cognito, Azure AD, and IdentityServer. James has 10 years of experience in IT and has worked in the agro-tech, health care, e-commerce, and finance industries.

Outside of SoureFuse, James continuously hones his engineering skills by learning new programming languages, tech stacks, and architectural patterns. James lives in Dallas, TX with his wife and dogs.

WEBSITE


SPONSOR PARTNER
getsmarter® with edX®
Explore top-tier education with exclusive savings on online courses from MIT, Oxford, and Harvard through our e-learning sponsor. Elevate your career with world-class knowledge. Start now!