Quick Answer: Is Open Source Software More or Less Secure Than Proprietary Software?

Mark Driver, VP Analyst

23 March 2021

Gartner®

Quick Answer: Is Open Source Software More or Less Secure Than Proprietary Software?

Published 23 March 2021 - ID G00744611 - 4 min read

By Analysts Mark Driver

Initiatives: Emerging Technologies and Trends Impact on Products and Services

Open source software can be the foundation of innovation across the industry. The debate over the security of OSS continues with significant confusion on both sides. Product leaders need to understand the real-world realities of OSS security to succeed.

Quick Answer

Is Open Source Software More or Less Secure Than Proprietary Software?

- The open-source (OSS) software model does not result in inherently higher or lower quality, nor is it more or less secure than closed-source alternatives.
- The transparent and collaborative nature of the OSS model affords several theoretical advantages (e.g., a larger and more diverse developer base).
- Real-world governance and engineering disciplines embraced by individual projects ultimately determine the quality of the final product rather than any inherent advantage (or disadvantages) in the model itself.

More Detail

Quality and security have long been topics of serious debate between open- and closed-source software developers. On one hand, many argue that the transparent nature of the OSS model inherently results in higher quality (and, subsequently, security) than closed-source solutions. Others argue that the traditional “hobbyist” nature of many OSS projects underplays the necessary diligence and engineering best practices when trying to match closed-source efforts. Our research shows the answer depends on a number of critical factors rather than any single rule of thumb.

As the use of OSS assets grows in mainstream IT portfolios, product and IT leaders must set aside out-of-date assumptions and generalities related to OSS security and quality factors (both pro and con) in favor of detailed project-by-project measurements and assessments. Specifically, they must assess the quality and security of every open-source solution on its individual merits, paying close attention to such factors as:

- Community effectiveness
- Project maturity
- Defect tracking and resolution discipline
- Planned product roadmaps versus ad hoc coding
- Robust IP governance
- Security audits and vulnerability management

Because of its transparent nature — and unlike closed-source efforts — it is more difficult to maintain a state of mediocrity through obscurity in well-run and highly collaborative open-source projects. Consequently, many adopters assume that OSS has inherently higher quality than closed-source efforts. Contributing to this assumption is the fact that, among mature open-source projects with effective and resilient communities, overall quality is often high.

Many OSS proponents vehemently maintain that typical OSS solutions have fewer overall defects than closed-source alternatives. This assumption was captured in Eric Raymond's seminal discussion of the OSS model, "The Cathedral and the Bazaar"; there, he proposed that, "Given a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix obvious to someone." In reality, we find that the quality of open source is driven more by individual project governance and best practices than any factor inherent in the model itself; moreover, open-source quality is driven by virtually the same factors that are present in a closed-sourced project.

The key differentiated benefit in the OSS model is its potential to draw a far greater "number of eyes" on the code than a closed effort with a small team. This creates the potential for wider and more-in-depth peer review and investigation before the code is released; however, these advantages are entirely theoretical, unless the project actually executes these practices. In other words, there is a big difference between the dynamics of an open-source project with four developers versus one with 40 or 400. Moreover, there is a massive difference between projects in which only some have the governance and discipline to continuously monitor and manage quality through coding standards, expert committer stewardship, code reviews and security audits.

Don't Assume OSS Is Automatically More Secure (or Less Secure) Than Closed Alternatives

In today's threat and vulnerability landscape, designing secure IT solutions and discovering security vulnerabilities in source code is a specialized and complex skill set. You can't assume that any arbitrary OSS community has these skills in every scenario. Moreover, one could argue with good cause that the open nature of OSS projects may even create lower barriers to entry for security vulnerabilities when their "guard dog" security best practices are insufficient. The monetization, radically advanced market for and technology of vulnerability research now results in closed-source products being subjected to extensive examination. Fuzzing, zero-day intrusion protection system signatures and the regularization of

vulnerability management have brought increased visibility and pressure for closing vulnerabilities in closed-source products and projects.

Much like the issue of general code quality, effective security results from specific project governance and development best practices. A robust and effective developer community that includes specialized resources paying close attention to security-related issues can have a marked impact on security that goes beyond the efforts of any single vendor team.

Evaluate the Quality and Security of OSS Technologies on a Case-by-Case Basis

Don't assume that OSS enjoys automatic advantages related to security concerns over closed-source alternatives. Rather, view source code security as a complex topic that must be assessed on a case-by-case basis in specific projects. For example, any reputable open-source project will have transparent and automated issue (i.e., bug) tracking (e.g., Bugzilla, Jira) accessible to the public (see Gartner's IT Score for Applications). Hold circumspect any project that does not. Use these issue-tracking systems to track the number of outstanding issues and their status and criticality.

Recommended by the Authors

A CTO's Guide to Top Practices for Open-Source Software

Hype Cycle for Open-Source Software, 2020

Ensure Safe and Successful Usage of Open-Source Software With a Comprehensive Governance Policy

How to Manage Open-Source Software Risks Using Software Composition Analysis

Evidence

- WhiteHat Security - The DevSecOps Approach - Using AppSec Statistics to Drive Better Outcomes
- Synopsis - 2020 Open Source Security and Risk Analysis (OSSRA) Report
- WhiteSource - The State of Open Source Security VULNERABILITIES
- Snyk - The State of Open Source Security 2020
- Sonatype - 2020 State of the Software Supply Chain Report

OSS Project Best Practices

- Microsoft - Open Source Software
- The LINUX Foundation - Best Practices for Using Open Source Code
- Eclipse Foundation Project Handbook

- The APACHE Foundation - How It Works

Become a Client

Get access to this level of insight all year long — plus contextualized support for your strategic priorities — by becoming a client.

gartner.com/en/become-a-client

U.S.: 1 800 213 4848

International: +44 (0) 3331 306 809

About Gartner

Gartner is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 14,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

To learn more about how we help decision makers fuel the future of business, visit **gartner.com.**

Gartner®