



IDC PeerScape: Practices for Supporting Community Open Source Software

Al Gillen

IDC PEERSCAPE FIGURE

FIGURE 1

IDC PeerScape: Open Source Software – Practices to Safely Embrace Open Source Software

 Your Challenges	 Peer Insights
<p>How to ensure long-term success Many organizations are attracted to OSS, but nearly all IT decisions have long-term ramifications.</p>	<p>Practice 1 Build a plan to ensure long-term success with your OSS investments.</p>
<p>Determining acceptable and unacceptable risk Risk levels vary considerably on a specific OSS technology being considered.</p>	<p>Practice 2 Align risk tolerance with the public exposure or exposed surface area of a given OSS technology.</p>
<p>Creating a process to maintain open source Establish repeatable processes driven by an OSPO; use tooling to enforce best practices.</p>	<p>Practice 3 Establish clear guidelines and repeatable processes along with tooling to enforce best practices.</p>
<p>Supporting critical solutions Organizations need to align internal competencies and external services to cover your full portfolio.</p>	<p>Practice 4 Use commercial support for OSS solutions where the lack of internal skills might lead to a compromise.</p>
<p>Acknowledging/highlighting OSS benefits Organizations need to find ways to recognize the efforts and successes of leveraging OSS.</p>	<p>Practice 5 Celebrate the successes of employees' use of best practices for contributing to and leveraging OSS.</p>

Source: IDC, 2022

EXECUTIVE SUMMARY

Open source software (OSS) has penetrated virtually every layer of software and, in some layers, has become the dominant technology – and in an increasing number of cases the only solution – used across the industry. Given the tens or hundreds of thousands of OSS projects in use today, there is likely an OSS option for nearly any need an organization might have. Deciding if, when, and how to use OSS solutions can be a complicated question that has a multitude of nuanced answers.

Every organization has varying levels of competencies with different types of software and different layers of the overall software stack, and different goals when it comes to managing that software stack. For some technically competent organizations whose business is closely related to IT products and services, a stack of software that is dominated by community-sourced open source components, and supported by the organization itself, might make good sense. For other organizations, using OSS technologies that are supported by commercial providers for critical solutions may make better sense, with the organization's efforts concentrated on delivering a user experience that differentiates the company's products and services.

Realistically, the vast majority of organizations live between those two extremes, with those organizations focused on using the optimal mix of commercially and community-supported OSS. Done correctly, this approach can deliver maximum benefit while, in parallel, mitigating potential risk associated with community-supported open source software.

This IDC PeerScape presents five practices for organizations determining when, where, and how to use community-supported open source software alongside commercially supported open source software.

"The attraction of increasingly reliable and secure community-supported open source software, with its zero cost of acquisition, continues to grow in the industry. Few organizations that use open source software today can claim to use no community-supported technology," said Al Gillen, group vice president, Software Development and Open Source, IDC. "However, to fully leverage the opportunity presented by community-supported open source software requires organizations to also know when the right move is to contract with a commercial support provider to support key components of their stack."

PEER INSIGHTS

Practice 1: Build a Plan to Ensure Long-Term Success with Your OSS Investments

Challenge

Although most organizations are attracted to open source software, they need to keep in mind that nearly all IT decisions have long-term ramifications. IDC routinely speaks to clients with legacy environments and applications that are still in use, which are not just old – but oftentimes better described as ancient. What is exciting and new today will be tomorrow's legacy still under maintenance support.

With open source software, the added complexity is that there may not be a commercial vendor that builds a business around supporting a given OSS technology for the long term, leaving an organization to rely on itself or on the community to ensure long-term viability.

Example

Not every organization engages deeply with open source software communities that are developing the technologies those organizations might be using. That said, some mature organizations are proactively engaging with OSS communities. For example, New York-based global finance, media, and tech company Bloomberg is particularly supportive of open source software communities. Andrey Rybka, head of Compute Architecture in the CTO Office at Bloomberg, is a big advocate for engaging early with open source technologies. Rybka says Bloomberg's design philosophy is to use open source first. "That means that, as we start new projects, we start with an idea that we shouldn't just reinvent the wheel. If the wheel was well invented and it already is in some good mature open source community that we can participate in, that is a sustainable way to build and design software going forward. That's the belief that we started with about a decade ago."

But sustainability is front of mind starting on day one and continues throughout the usage life cycle of a given technology. Almost a decade ago, the company established its Open Source Program Office (OSPO) in the Office of the CTO, which is staffed by a team that provides guidance to the company's engineers – but importantly, the OSPO also engages with the community directly. "The philosophy is to start with open source but also to make sure we contribute back to and participate in those communities. And that means providing actual funding, that means making meaningful contributions. The way we typically operate is that we have a strategic list of projects that we proactively maintain, fund, and participate in. If a new project comes along, then we look at the sort of various [support] options, including commercial ones," says Rybka. He says that Bloomberg does not automatically exclude commercial support options, but typically the open source software approach is more aligned with his organization's long-term approach. "Vendors get acquired, vendors might go IPO, and then their priorities change."

Alyssa Wright, who leads Bloomberg's Open Source Program Office, notes, "We work closely with the fiscal hosts of many of these projects. These foundations support these open source projects and are often the shepherds and bridges to the community. In part that's why we support foundations and want there to be a rich space for the sustainability of open source projects."

Bloomberg went a step further, creating a public website (www.TechAtBloomberg.com/opensource) to share information documenting its use of open source software and encouraging engagement across its 6,500 engineers and the larger OSS community outside Bloomberg. This site details the company's journey and cultural shift over the past two decades to become an "open source first" company.

Guidance

Open source software works when there is a vibrant, healthy community that works to enhance the project and continues to develop and support that project after the initial excitement wanes. In many situations, commercial vendors that step in to offer commercially supported versions of open source projects will play a key role in long-term support and maintenance of the community technology. However, not every project has a direct commercial benefactor.

There are other viable options to stimulate a healthy community behind an open source software project that should be considered. For some projects, there is a so-called "tip jar" associated with some projects, intended to route funding back to open source software maintainers who otherwise might be working entirely uncompensated. A more formalized approach to compensating maintainers is made possible by innovative start-ups such as Boston-based Tidelift. The business model Tidelift uses is to engage directly with maintainers and pay them to ensure the projects they are involved with

meet enterprise expectations. Another approach, as Bloomberg illustrates, is to work directly with foundations offering both technical engagement and funding to support the efforts of the foundations to deliver quality software.

The bottom line is that it is important for end-user organizations to take a long-term view when it comes to investing in the use of open source software. An ongoing commitment to the community, to the projects and, directly or indirectly, to the maintainers helps increase the likelihood of long-term success.

Practice 2: Align Risk Tolerance with the Public Exposure or Exposed Surface Area of a Given OSS Technology

Challenge

Risk levels vary considerably with the use of a given open source project, and the internal versus external exposure of that technology factors in heavily into the relative risks incurred. For example, developer technologies that are used for prototyping and proof of concepts may have little or no external exposure, making that experimental use of open source software potentially much less risky than a production system that is hosted on a cloud platform with surface area exposed to parties with malicious intent. For technologies that must withstand public traffic that may at times be malicious, the bar quickly becomes much higher, and frequent patching, use of the most current versions, and having the DevOps tooling and practices to support this rapid updating are all mandatory approaches and solutions.

Example

Jeff Burga is manager of Linux and Cloud engineering at Credit Acceptance Corp., a \$2 billion financial services company based in Southfield, Michigan, which specializes in automotive financing. Burga says his IT colleagues will aggressively immerse themselves in an OSS technology the company decides to use, so they can support internal operations efficiently and promptly, as the need might arise.

"When it comes to, for example, containers, we use open source container technology versus going with traditional Docker [technology] just because we're comfortable in supporting it. We train ourselves to support that technology versus using a community. Community is nice, but sometimes you need an answer faster – that is, faster than a few days. It's worked better for us just to get smarter."

Burga estimates the use of open source software at Credit Acceptance to be substantial – but under 50% of total software in use.

Guidance

Developing deep expertise in the OSS technologies your organization chooses to embrace becomes a required action once you have made a decision to embrace this technology and support it through your existing staff.

Practice 3: Establish Clear Guidelines and Repeatable Processes Along with Tooling to Enforce Best Practices

Challenge

Organizations need to create an actionable plan to maintain open source software, including the establishment of repeatable processes, ideally driven by an OSS program office, along with the use of automation tooling to both enable and enforce best practices.

This challenge becomes complicated by a matrix of open source software technologies in use, each of which is likely to pull in additional OSS dependences that also must be managed.

Examples

Credit Acceptance's Burga notes, "We rely on our security team to help us out with our vulnerabilities. They do quality scanning and other scanning on our systems. They give us a monthly report. They will identify things that we have – call it a zero day – that we have to fix right away." Burga notes other lower-level vulnerabilities may receive a longer time frame for remediation from the security team.

Credit Acceptance uses KernelCare from TuxCare. "Thanks to KernelCare and the patching solution that we developed, we have a very consistent and quarterly patching cycle. We're never far out of spec on a piece of software." He says when the patching takes place, it's surgically focused on security issues but proactively avoids adding new risks. "When we patch, we're not introducing brand-new packages. We're always in pretty good shape."

Burga says community software technologies, even when they don't show up on the security scan, get regular maintenance. "My background is in engineering and architecture, and I've seen old software cause big problems. So I make it a point to make sure we are no more than two quarters out from the latest release of a piece of software that's under my control."

An engineer at a government contractor was interviewed for this IDC PeerScape and made the observation that the security and safety of the OSS that the organization uses is particularly important. That directly influences decisions about externally facing software that needs to be maintained. As with Credit Acceptance, this organization relies on frequent scanning and for employees to respond immediately to scanning results that need remediation of any sort.

"Often one thing we do is use Nessus to do security scanning of all our systems. And it's done on an ongoing basis – the scans are run pretty constantly," notes the engineer. "We are alerted when systems go out of compliance. If there's a critical issue, we're expected to remediate it immediately. That is one of the means by which we make sure that [we] know our programs are within scope."

Bloomberg, which created its OSPO about 10 years ago, uses it as a vehicle to develop policies and give developers guidance. Bloomberg's Wright explains, "We had an opportunity to articulate some of the cornerstone guardrails of our OSPO. One of the things we do is to help find fair policies for engaging with open source communities across the industry, and make that as easy and authentic as possible. We support open source ecosystems. It is important to us to make sure they are sustainable – whether that is with code or financial backing. It is critical for us that these projects are resilient and collaborative – and multi-stakeholder – and are successful in their work."

"It's important for our success and it defines our approach and reasons for our engagement," says Wright. "We also help facilitate collaboration across internal and external stakeholders. I see a lot of

my own work as bridging teams and bridging out to project ecosystems – just trying to be a place where we not only make it easy for people to participate in open source but also bring some of the learnings and open source collaborations into how we operate as a larger company."

Guidance

Establish practices that can be consistently applied to your organization so that responses in urgent situations are done in a thoughtful, intentional, and productive manner.

Practice 4: Use Commercial Support for OSS Solutions Where the Lack of Internal Skills Might Lead to a Compromise

Challenge

Supporting critical solutions is a challenge for every organization, and organizations typically need to align internal competencies and external services to cover their full portfolio. The organization's philosophy and the depth of its technical competency typically will help determine how much of its OSS portfolio is supported internally and how much of it relies on external support providers. It remains rare to find an organization that supports 100% of its OSS deployments internally.

With open source software, there are three basic approaches to commercial support. First, there are cloud platform vendors including all the major players and many second- and third-tier providers, which stand up open source software and deliver it as a managed service. The cloud platform vendors take responsibility to ensure the currency of the software, that vulnerabilities are resolved, and that the software is secure.

Second, there are vendors that offer a commercialized implementation of either a community technology or a fork of that technology, which the vendors support directly. This is the model used by companies such as Red Hat, SUSE, HashiCorp, and GitLab.

The third option for commercial support is provided by vendors that may not be driving a project directly and also might not play a role in the governance of a given project. However, these companies would typically have some level of ongoing engagement (oftentimes, significant engagement) with the community maintaining the underlying project. Examples of companies that play this role include IBM, Tidelif, TuxCare, and Quansight.

Examples

The government contractor subscribes to Red Hat for the enterprise support of Red Hat Enterprise Linux, and it also uses KernelCare from TuxCare to provide live patching on its Linux operating systems. However, the other technologies being tested such as Prometheus and Grafana – which are not external facing in their current use – are community supported. Longer term, as the company continues its evaluation of Prometheus and Grafana, there may be justification to seek external support. But some projects remain off the table for the government contractor if the technology is in a use case where there would be a corporate mandate for commercial support.

While Bloomberg may be highly focused on self-supporting a wide swath of OSS technologies, Rybka recognizes that there are still certain situations where the company needs to look outside. He says, "This is typically where something like [a vendor] comes into play, because they can fill the gap of some project that might be small enough. We definitely want to have a support story with every component we use. So, if there is a vulnerability, if I have a relationship with the vendor that's backing

the open source product, then I can open an IT support ticket with them to say, 'you know what's the story here, right?'"

Guidance

Open source software is best used when it's part of a large buffet of choices, allowing the specific implementation, the support model, and the exact level of support to be chosen by each organization using the technology for business purposes in its daily operations.

Practice 5: Celebrate the Successes of Employees' Use of Best Practices for Contributing to and Leveraging OSS

Challenge

Acknowledging and highlighting OSS benefits need to happen. Accordingly, organizations need to find ways to recognize the efforts and successes of employees to effectively leverage OSS. This is becoming not only a best practice for the company itself but also a way of developing talent on staff, leading to better retention and better outcomes for the company itself.

Examples

Credit Acceptance has a policy to encourage the exposure to and use of open source software as a job benefit. Burga explains, "I support the career development of my team. Everybody on my team. We have a healthy training budget, [and] I talk to my guys every week about, 'Hey, what do you want to learn?' It doesn't have to be what you're working on right now. It could be something interesting down the road." Burga adds, "I try to keep up with things, too." He attends conferences regularly and brings home ideas for his team to consider. "The team is really good about taking that stuff and learning it – even if it's just at a high level, so that later on down the road, if it looks like something that can fit into our portfolio, they're ready."

Bloomberg takes that focus on employee engagement with OSS a step further. Wright says, "We incentivize engagement and recognize the breadth of contribution to open source. A lot of our work is about supporting and celebrating the people within Bloomberg who are contributing to open source communities, whether that's code or governance or documentation or community support. Another area of our focus is raising the level of awareness about the scope of open source that we use across all departments. There are hundreds of thousands of IT projects and libraries that we are building with, and this is something important for us to understand completely."

Guidance

Using open source software is a two-way street. Organizations get value from the code itself, but the employees also gain new skills, may make important community connections, and can be intellectually challenged and stimulated through the engagement that open source software offers. Smart organizations will position this as a job perk, which IT professionals will see as being a positive addition to their skill sets, their marketability, and their overall participation within the larger development community.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and PeerScape are trademarks of International Data Group, Inc. IDC PeerScape is a registered trademark of International Data Corporation, Ltd. in Japan.

Copyright 2022 IDC. Reproduction is forbidden unless authorized. All rights reserved.

