VMware Tanzu

The State of the Software Supply Chain: Open Source Edition 2021

Presented by: VMware

vmware

Introduction

As companies accelerate their digital efforts, the software supply chain becomes critically important. Because open source software (OSS) is taking on an expanded role in the enterprise software ecosystem, the goal of our inaugural survey was to examine issues surrounding OSS.

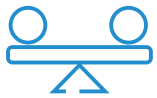
It's a safe assumption that almost all large organizations worldwide are running at least some OSS. From operating systems to web servers to databases to programming languages to Kubernetes—there's an open source project for almost everything. In some areas, OSS has become the de facto standard if not the only option. The benefits are well worth clearing the hurdles. Even the secondary benefits can be significant. For example, there's the issue of attracting and keeping talent. Companies that use OSS and contribute to open source projects have an easier time finding, hiring and retaining qualified engineers.

With the popularity of OSS comes a significant set of concerns for enterprise IT executives, decision-makers *and* developers. Given the pace of OSS adoption, we wanted to investigate its use in the enterprise further. This survey was designed to dig deeper on OSS usage, including what types of OSS companies choose and why, what they like, and what the challenges are. In particular, our goal was to understand challenges and opportunities in two critical areas: **OSS packaging** and **security**. Enterprises haven't settled on the tools and processes necessary to package and secure OSS in production, and the OSS supply chain remains a critical security risk that must be taken seriously.

This report is divided into four sections:

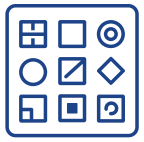
Open Source Momentum

Enterprises are deploying all types of OSS in production



Benefits Outweigh Challenges

Reduced costs and greater flexibility counterbalance perceived challenges and risks



Packaging Remains Challenging and Complex

While Kubernetes is getting easier to use, teams still face challenges

Software Supply Chain Risks

Security is the single biggest concern keeping companies from using OSS

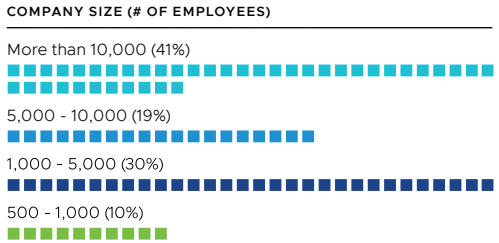
Demographics

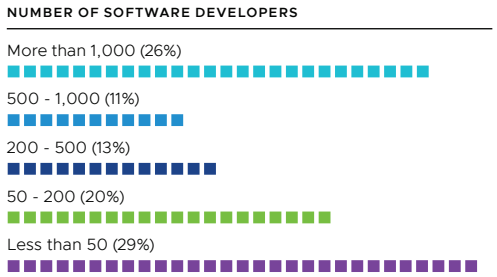
VMware commissioned Dimensional Research to conduct this study in order to understand the experiences and attitudes of technology professionals responsible for open source software. Our study surveyed a mix of professionals in IT development and operations roles, including technology executives, team managers, and individual contributors at companies with more than 500 employees. A wide range of industries and job levels are represented by the 518 respondents.

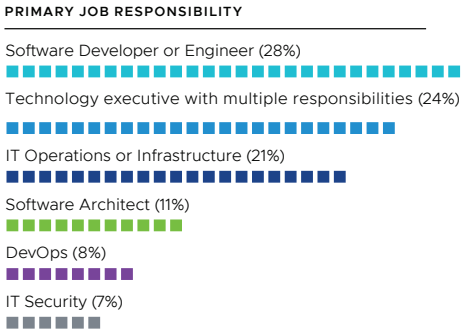
Our sample skews toward the software technology industry (20%), but—given its importance—this is not an over-representation. Other major sectors represented include financial services (16%), healthcare (8%), government (8%), and manufacturing (7%). All the organizations surveyed have a significant software development footprint: 29% have less than 50 developers, 20% have 50-200, 13% have 200-500, 11% have 500 to 1,000 and 26% have more than 1,000 developers.

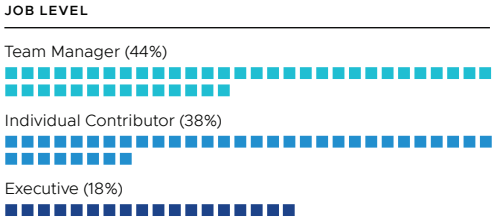
When asked about infrastructure, 39% said they operated mostly on-prem. Another 39% were evenly split between on-prem and cloud, suggesting hybrid cloud operations are the norm for a large slice of organizations. The final 22% were mostly or entirely in the cloud.

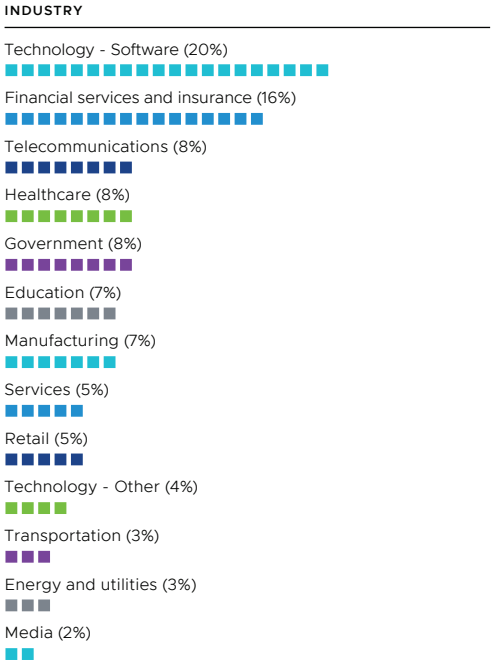
DevOps has been adopted by 84% of companies surveyed, with 41% having a "mature" DevOps organization. DevSecOps has been adopted by 66% of companies with 27% saying they have a mature DevSecOps program. This suggests that fewer organizations are focused on the security of their DevOps efforts or they have yet to consider security a part of DevOps.











Open Source Momentum

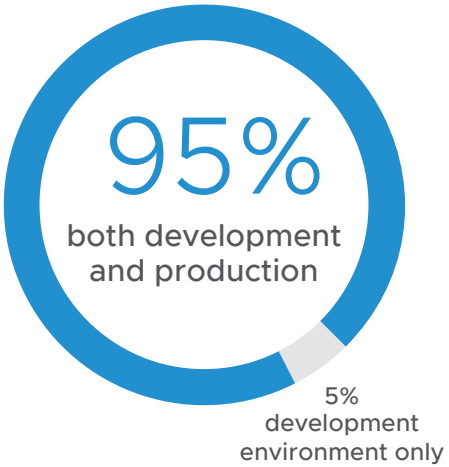
Almost all of the enterprises we surveyed deploy OSS in production—including *commercially supported OSS*, *commercial software that includes OSS*, or *community OSS*. Much of this software is infrastructure- or development-related, but many companies use OSS line of business software as well. Despite widespread use, most companies still manage OSS software differently than other software in their portfolios.

Almost everyone uses OSS in production

OSS is used in production in 95% of the companies covered in this survey. As companies get larger they are slightly less likely to have production OSS deployments, possibly because of more rigid policies in companies of greater size. For the small number of companies that don't use OSS in production, reasons include: *we're still figuring out how to manage OSS in production* (46%) and *we have a policy against OSS in production* (46%). Another quarter said: *we haven't released the product yet*.

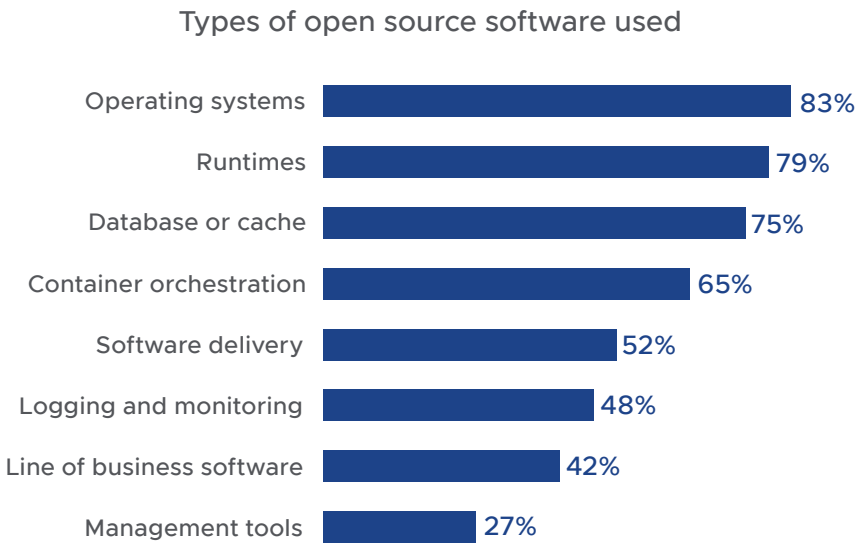
When we asked where organizations get their open source software, we saw an almost even split. About 79% use *commercially supported open source* (commercial Linux distributions such as Red Hat for example), 75% use *commercial software that includes open source* (as an example commercial software products often use an open source database as a backend), and 70% use *community open source*, meaning they compile and package the software from public source code and support it themselves. Companies with more than 1,000 developers are more likely to use *community open source* (83%), possibly because they have the most resources to self-support.

Use of OSS in production



A wide variety of types of OSS are in use

Naturally, we wanted to know the types of OSS companies are using. The heaviest hitters include: *operating systems* (83%), *runtimes* (79%), *database or cache* (75%), and *container orchestration* (65%). While there is a surprising amount of *OSS line of business software* in use (42% of respondents), the lion's share of OSS in the enterprise appears to be infrastructure- or development-related.



Because a majority of companies (83%) use open source operating systems, we asked respondents to EXCLUDE operating systems from consideration when answering the remainder of the survey questions.

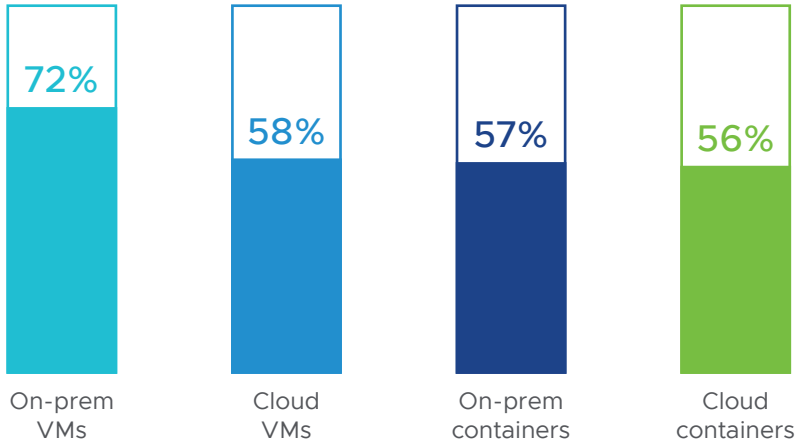
Deployments use both VMs and containers

When we asked where companies are deploying OSS, *on-prem VMs* were chosen by 72%. In addition, we saw: *cloud VMs* (58%), *on-prem containers* (57%), and *cloud containers* (56%).

This is an impressive showing for containers. This survey doesn't ask what percentage of applications organizations run in containers overall, but other estimates point to a figure of 5% to 15% for an average organization.

When compared by company size, large companies (>5,000 employees) are more likely to have deployed OSS in containers (62%)—especially *cloud containers* (65%)—versus companies with fewer than 1,000 employees (40% deployment for *on-prem containers* and 42% *cloud containers*).

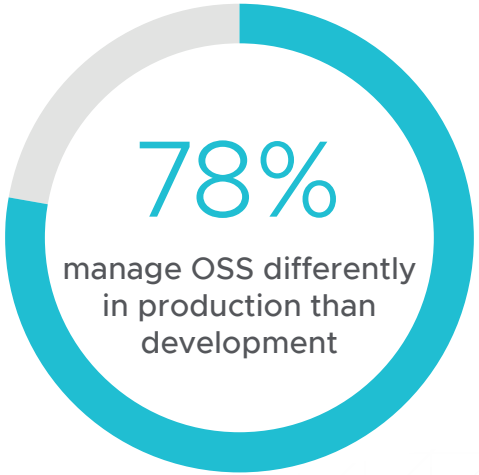
Where open source software is deployed



OSS is managed differently in production

For 78% of respondents, OSS in production is managed differently than OSS in development. Reasons given for the differences included: *internal security policy requirements* (55%), *internal IT policy requirements (other than security)* 46%, and *external security or compliance requirements* (43%). Vendor support for OSS used in production is seen as a requirement by 29%.

With security such a major concern, it's odd that companies have less—or at least different—security in development than production. Having different security tools in development adds complexity when moving to production, creating a weak link that could be exploited, as in *recent supply chain attacks*. Development should be just as secure as production.



Benefits outweigh the challenges

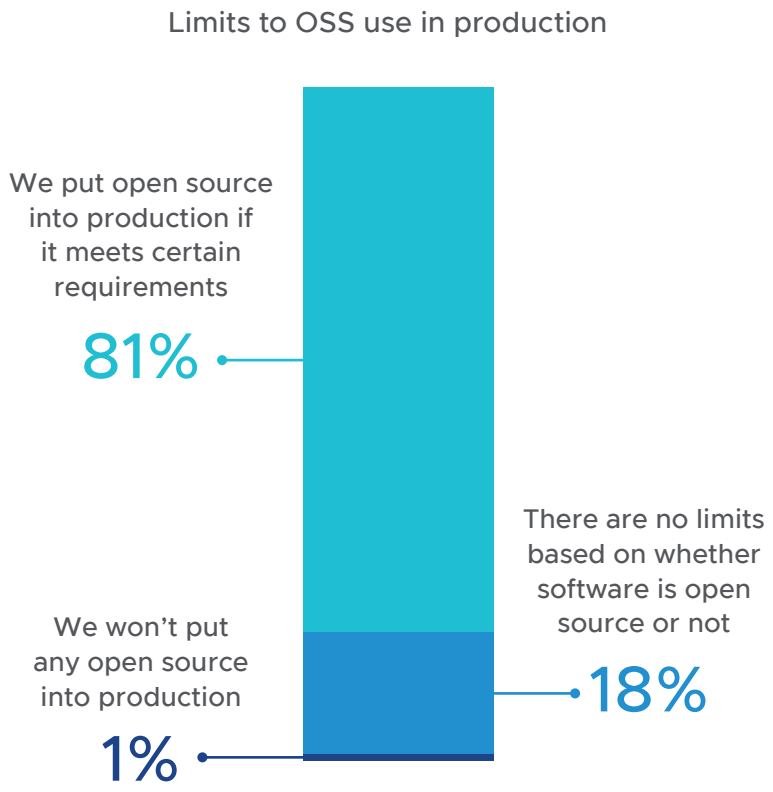
The organizations surveyed clearly believe that the benefits of using OSS in production outweigh concerns. Companies attempt to address continuing concerns by establishing specific requirements for OSS use but feel that risks remain, especially due to lack of visibility into patching, testing, and CVEs.

Benefits tip the scale toward OSS usage

Stakeholders saw the top benefits of OSS in production as: *reduced costs* (79%), *more flexibility* (63%), *benefit from a huge community* (58%) and *developer productivity* (45%). Given the overall level of OSS adoption, the benefits apparently outweigh the challenges: *dependency on community to fix bugs and patch vulnerabilities* (56%), *introduces security risks* (47%) and *no or unreliable SLAs for patches from community* (42%). These challenges come down to trust and reliability—or maybe trusting that OSS will be reliable. A fourth challenge, selected by 36% of stakeholders, was *licensing concerns*.

Company requirements limit OSS use in production

When asked about requirements for use of OSS in production, 81% of companies impose specific requirements, including: *open source license supports production use* (81%), *on our list of approved open source software* (53%), and *there is an option to purchase commercial support* (40%). The requirement for commercial support remains consistent across all company sizes, while large companies are much more likely to have a list of approved OSS options.

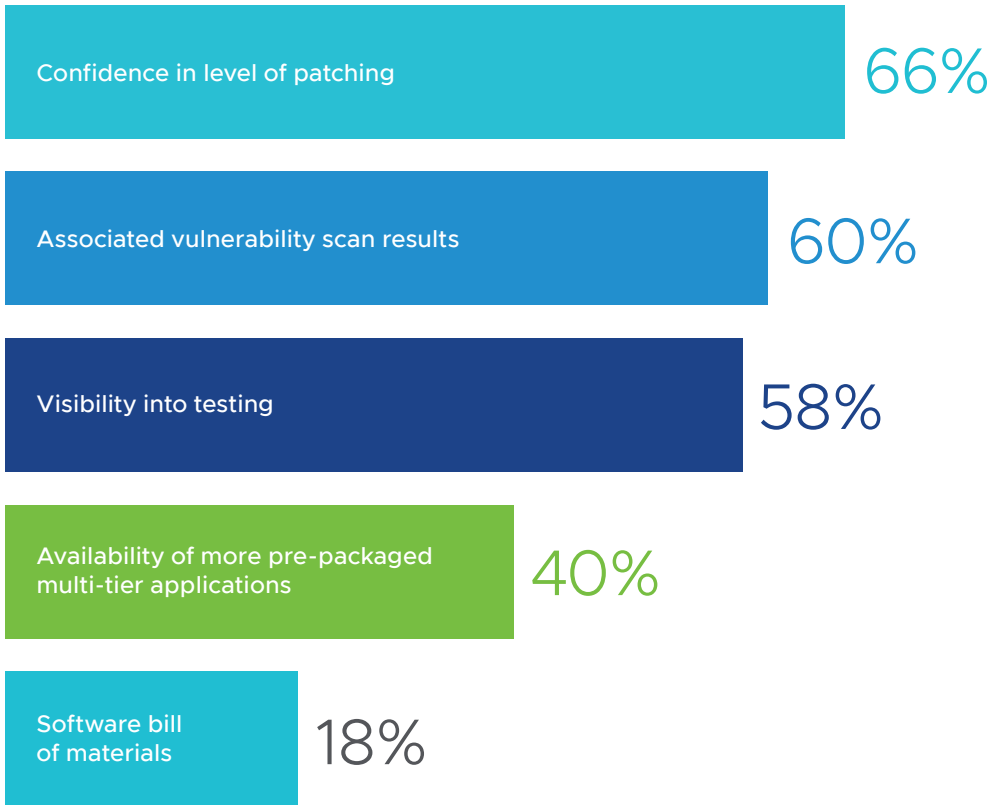


There's significant room for OSS improvement

When asked about areas for improvement, the top three options were: *confidence in level of patching* (66%), *associated vulnerability scan results* (60%), and *visibility into testing* (58%).

Respondents in DevOps roles expressed much more concern about *level of patching* (79%) and *vulnerability scan results* (77%) than the average.

Areas for OSS improvement



Packaging remains challenging and complex

Packaging OSS for enterprise use is a difficult and time-consuming task; 80% of respondents agree that *packaging isn't a technically difficult problem, but the devil is in the details and it is an inefficient use of time.* Tracking dependencies, lack of standardized procedures, and the involvement of too many teams—with too many tools—contribute to packaging challenges.

Too many challenges...

According to 91% of survey respondents, packaging OSS for production is challenging. The top bottlenecks included: *difficult to track vulnerabilities* (52%), *challenging to check if dependencies are compliant* (51%), and *difficulty tracking dependencies installed by package managers* (40%). Other notable concerns were: *can't always check sources reliably to know if we follow policies*, *highly manual and error prone*, and *time consuming and boring*.

Given these challenges, perhaps it's not surprising that more than half of respondents say that packaging OSS software has *more steps, checks and verifications* than commercial software. Two-thirds say that packaging OSS typically takes more than a day.

For the purposes of this survey, **packaging** is defined as the process of adapting OSS so it can be used internally. This could involve changing an application's configuration, building an application into a container, or changing the base operating system.

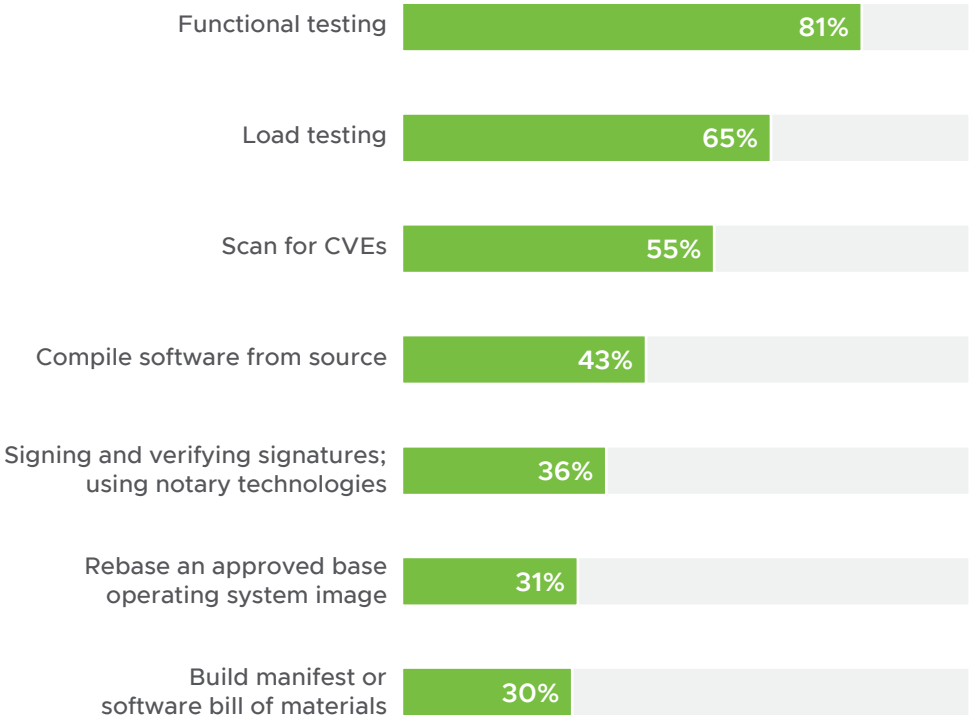
Too many tools...

Most OSS stakeholders don't appear to have a standard procedure or toolset for packaging OSS. One in ten organizations use no tools at all for packaging, while two-thirds of organizations use multiple types of tools to accomplish the job. A full 36% use three or more tools, ranging from configuration management such as Chef and Ansible to Docker tooling to Cloud Native Buildpacks and Packer.

It's notable that almost a third of organizations are using Cloud Native Buildpacks, which examine the source code, build it, and create a container image with all the required dependencies to run the application. It's an approach that makes the developer experience better and addresses most of the packaging challenges described in this report.

Too many tasks...

Most organizations perform many different tasks before OSS goes into production. The top tasks are centered around testing, including: *functional testing* (81%), *load testing* (65%), and *scan for CVEs* (55%). The full list is long.



And too many cooks

A final complication is that 65% of organizations have more than one team responsible for packaging OSS; some have as many as five teams involved. Developers have responsibility for packaging most often (67%) followed by IT Ops (64%). Involving multiple teams in what should be a straightforward process creates opportunities for mistakes, variability, and vulnerabilities. Controlling how software is packaged is a key part of DevSecOps, so standardizing on as few methods as possible—preferably just one—is recommended.

Is there an easier way?

If your organization faces any of the challenges described in this section, it's probably already clear to you that OSS packaging is an area where the right automation would go a long way. ***VMware Tanzu Build Service*** is designed to simplify the process of building containers from OSS and other source code. Optimized for Kubernetes, Tanzu Build Service automates container creation, management, and governance at enterprise scale. Cloud Native Buildpacks is at the heart of Tanzu Build Service, simplifying operations, boosting security, and reducing risks from CVEs.

Software Supply Chain Risks

Security remains the single biggest concern keeping companies from using OSS in production; 95% of respondents agree that *the software supply chain is a critical security risk that must be taken seriously.* Ownership of OSS security remains unclear, and organizations surveyed have an almost universal belief that better packaging capabilities are needed to manage OSS security risks.

Security concerns dominate

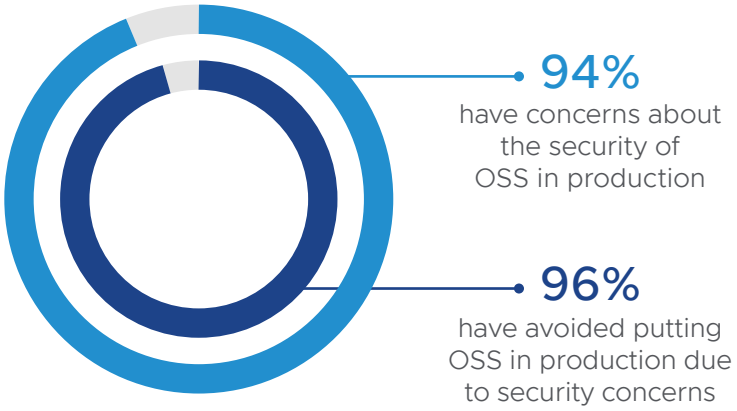
Almost all stakeholders surveyed (94%) have concerns about the security of OSS in production. Top risks selected were: *no guarantee that vulnerabilities will be remediated or patched* (63%) and *difficult to keep up to date on vulnerabilities so we can address them* (54%). Concerns such as these kept 96% of organizations from putting open source into production.

Ownership of security is unclear

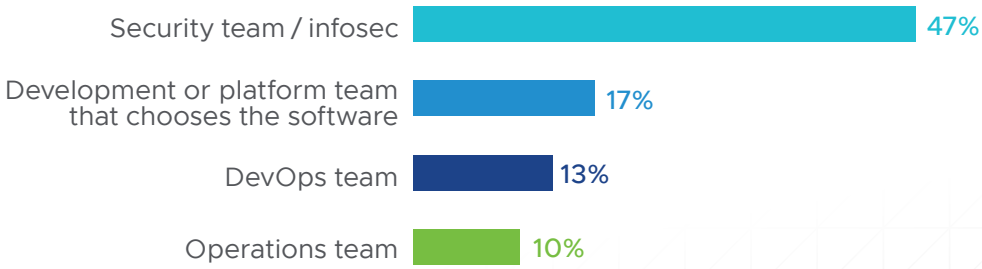
In slightly more than half of organizations, the security team is NOT ultimately responsible for validating and approving the security of OSS in production. Almost one in ten say there is no single owner.

Complicating matters further, more than half (54%) use different security tools for OSS than they do for other software at least some of the time.

Security concerns about OSS in production

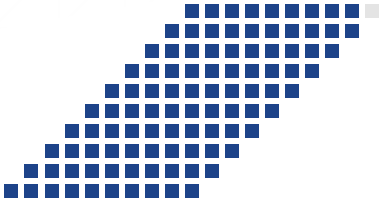


Responsibility for OSS security in production



Everyone wants better tools

Virtually all organizations (99%) would like better software packaging tools to help manage the security risks of the OSS supply chain. In particular, stakeholders appear to want tools that provide centralized visibility and control plus automation for tasks like CVE and virus scanning.



99%
want additional capabilities to reduce security risks in the software supply chain

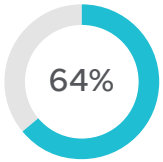
How can I increase the security of packaged OSS?

If you're using OSS software, you've probably been looking for tools to increase the security of your OSS supply chain. An earlier sidebar mentions *Tanzu Build Service*, which automates container creation, management, and governance and can help you adhere to strict compliance requirements, mitigate CVEs more efficiently, and gain control over app dependencies.

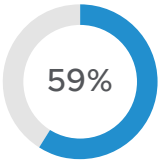
VMware *Tanzu Application Catalog* takes an alternative approach. Choose from an extensive OSS library and upload your golden image to receive a built, scanned and tested container. Create your own app catalog that gets automatically updated, so you always deploy the most secure stack. Developers spend less time worrying about config management tools and manual updates and more time writing code.

vmware

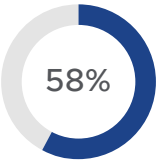
Capabilities that would help manage security risks



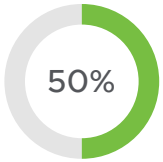
Immediate access to trusted security patches to applications or runtimes, dependencies, and operating system components



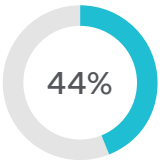
Centralized visibility to all scans to simplify security audits



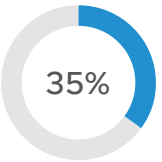
Automatic CVE and virus scanning for every container



Centralized metadata store that can be used to query dependency or versions when a new CVE emerges



Scalable and resilient support for key technologies and services



Vendor contribution to upstream projects

Summary and Recommendations

Open source software is seeing widespread use, with 95% of the enterprises covered in this survey deploying OSS in production. Stakeholders see significant benefits from open source use, including reduced costs, greater flexibility, and increased developer productivity. However, challenges exist. About half of all respondents are concerned about dependence on the OSS community for patches and bug fixes and also believe that use of OSS introduces security risks. Establishing and maintaining trust is vital for users of OSS.

In this survey, we wanted to understand two particular pain points in the OSS supply chain: packaging and security. According to 91% of survey respondents, packaging OSS for production remains challenging, and 94% have concerns about the security of OSS.

For too many organizations, OSS packaging remains a manual, time-consuming process. Two-thirds say that packaging OSS typically takes more than a day. Multiple tools may be required, and multiple teams are often involved. Security concerns have kept 96% of organizations from putting open source in production. Yet, in half of organizations the security team is not ultimately responsible for validating and approving the security of OSS in production. All organizations have a desire for better software packaging tools to help accelerate packaging tasks and manage the security risks of the OSS supply chain.

We don't want to imply that OSS is a "security problem" at all. We use, work on, and rely on OSS every day in our own business. The benefits of using OSS are clear. What these responses tell us is that establishing trust by focusing on packaging and security is vital for achieving those benefits. Managing how open source fits into your software supply chain is a requirement for modern IT.

So, how can enterprises maximize the benefits of OSS while avoiding packaging and security pitfalls? One option is to choose only OSS that's available with commercial support; 40% of organizations surveyed are bound by such a requirement. However, given the number and variety of open source projects, it's unlikely that there will be a supported option for every piece of software you want to use. Whether you build trust in OSS through commercial support or not, you need to establish and maintain that assurance.

The right tools can go a long way to address OSS supply chain, packaging, and security concerns for all OSS software. Automation not only reduces manual toil, it reduces the risk that vulnerabilities are inadvertently introduced. Cloud Native Buildpacks are one approach that addresses many of the packaging challenges described here.

VMware Tanzu has the capabilities to address your OSS challenges and concerns. *VMware Tanzu Build Service*—using *Cloud Native Buildpacks* as a foundation—automates container creation, simplifying operations, boosting security, and reducing risks from CVEs. *Tanzu Application Catalog* allows you to create your own OSS app catalogs of trusted projects. Components of these catalogs are automatically updated, so you always deploy the most secure stack—avoiding tedious packaging and security tasks. And finally, Tanzu application environments, including our Cloud-Foundry-derived *Tanzu Application Service* and Kubernetes-based *Tanzu Application Platform* (currently in beta), takes over packaging and security tasks from developers, allowing them to focus more attention on creating code.

Interested in talking to an expert about open source software strategies?

Get in touch >

Join us online:

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA
Tel 877-486-9273 Fax 650-427-5001 vmware.com

Item No: VMware_State_of_OSS_2021_eBook_v02_100121 10/21