VMware Tanzu®

The State of the Software Supply Chain: Open Source Edition 2022

Presented by: VMware

vmware®

Introduction

Given the significant vulnerabilities that have turned up in both commercial and open source software (OSS) over the past year—and the continued growth in cyberattacks—the software supply chain is receiving increased scrutiny from companies of all sizes. Our inaugural 2021 report explored risks and opportunities in the OSS supply chain at large companies. This year, we've opened the survey to companies of all sizes. This report highlights some of the unique concerns and challenges that smaller companies face, in addition to those of larger operations.

Companies continue to choose open source software for reasons such as cost efficiency (75%), flexibility (57%) and community support (54%), and this year's survey finds that OSS is fulfilling those expectations. However, the past year hasn't been all smooth sailing for OSS adoption. Fewer respondents say they are deploying OSS in production this year than last year—90% versus 95%—due to management challenges (44%), support concerns (38%) and lack of trust in OSS technology (34%). Significant opportunities exist to improve OSS packaging and the security of OSS in production.

This Report is Divided into Four Sections:

Open Source Software Fulfills its Promise

Benefits closely match user expectations

Open Source Software Headwinds

Production use has decreased this year

Security Risks Dominate

A notable uptick in risks across the board

Tools, Tasks and Teams

Optimizing OSS packaging is becoming essential

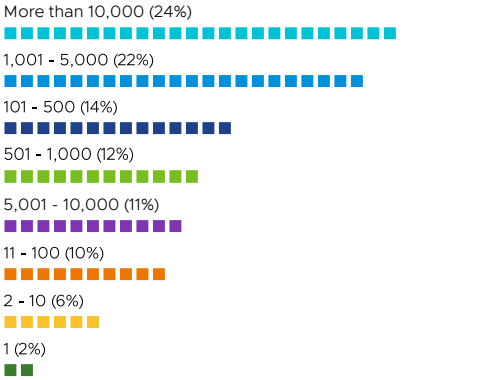
Demographics

VMware commissioned Dimensional Research to conduct this study to understand the experiences and attitudes of technology professionals responsible for OSS. Our study surveyed a mix of professionals in IT development and operations roles, including technology executives, team managers and individual contributors. While last year's survey focused on companies with 500 or more employees, this year's survey was expanded to include companies of all sizes. We've also more than doubled the number of respondents, reaching 1,198 OSS stakeholders from a wide range of industries and job levels.

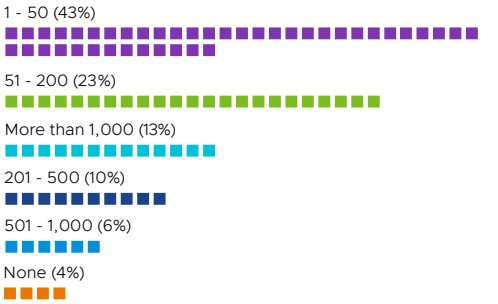
The companies sampled lean toward the software technology industry (18%). Other major sectors represented this year include financial services, healthcare, telecommunications, manufacturing and education—each making up 9% of the total.

When asked about infrastructure, 32% said they operated mostly on-prem, 38% were evenly split between on-prem and cloud while 30% were mostly or entirely in the cloud. DevOps has been adopted by 80% of companies surveyed, with 38% having a "mature" DevOps organization. DevSecOps has been adopted by 62% of companies with 26% saying they have a "mature" DevSecOps program.

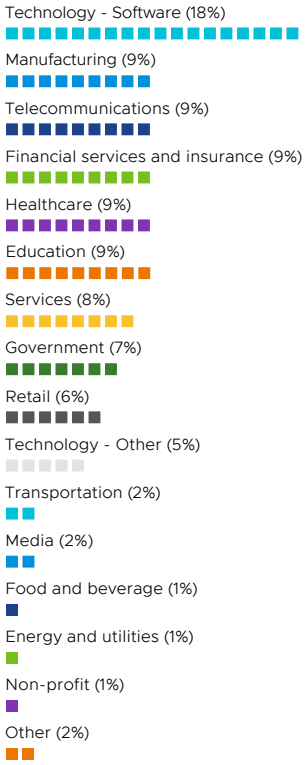
COMPANY SIZE (NUMBER OF EMPLOYEES)



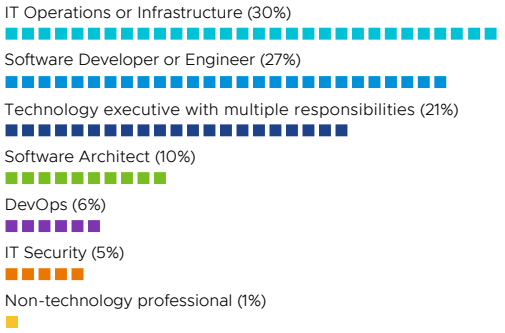
NUMBER OF SOFTWARE DEVELOPERS



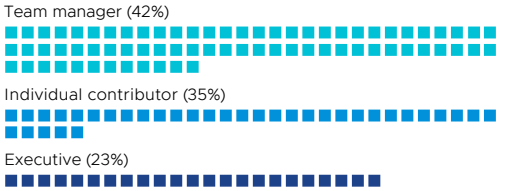
INDUSTRY



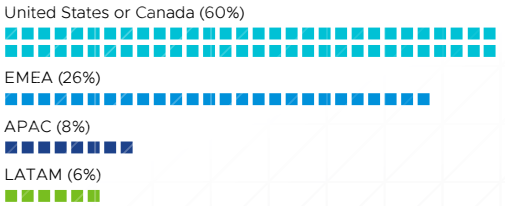
ROLE



JOB LEVEL



REGION



Open Source Fulfills its Promise

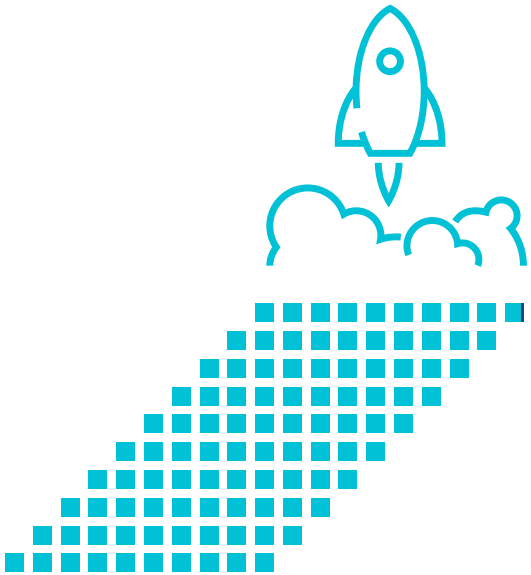
In the technology world, it's rare for the real benefits of new technologies to match expectations. In the early days of public cloud, for example, many companies moved operations to the cloud expecting to cut costs only to find that—although there were many benefits—cost reduction was rarely one of them. For OSS, there's a close correlation between expectations and benefits—especially when it comes to costs.

(Almost) Everyone is Benefitting From Open Source

This year, 99.8% of stakeholders using OSS in production report that their organizations benefit from OSS. Five benefits were selected by 50% or more of respondents: *cost efficiency* (chosen by 76%), *increased flexibility* (60%), *support of large user community* (54%), *developer productivity* (52%) and *technical team can work with preferred technology* (51%).

Small Companies Experience the Same Benefits

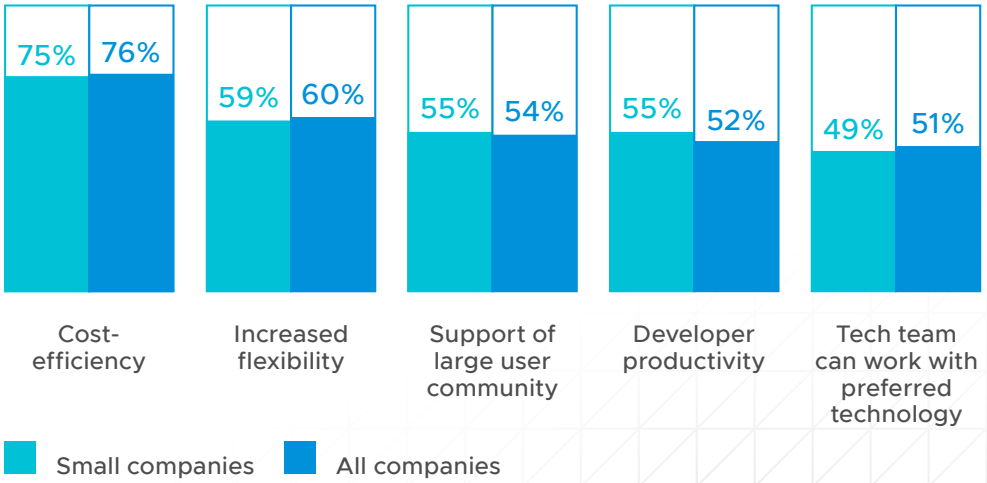
When we zero in on the smallest companies (those with 100 or fewer employees, accounting for just under a fifth of all companies sampled) we see that they recognize the same benefits as their larger brethren: *cost efficiency* (75%), *increased flexibility* (59%), *support of large user community* (55%), *developer productivity* (55%) and *technical team can work with preferred technology* (49%). Overall, these results are surprisingly close to those for the total sample. Small companies recognized *developer productivity* as a benefit 3% more often (55% vs 52%), the largest deviation.



99.8%

benefit from using open source

Benefits of OSS

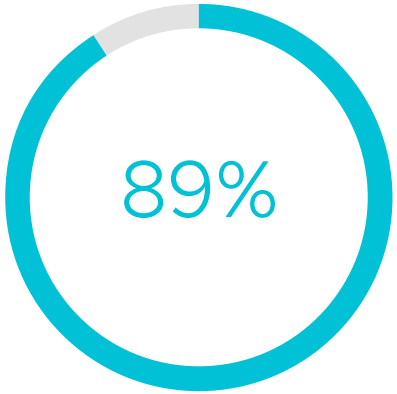


OSS Expectations Align Closely with Actual Benefits

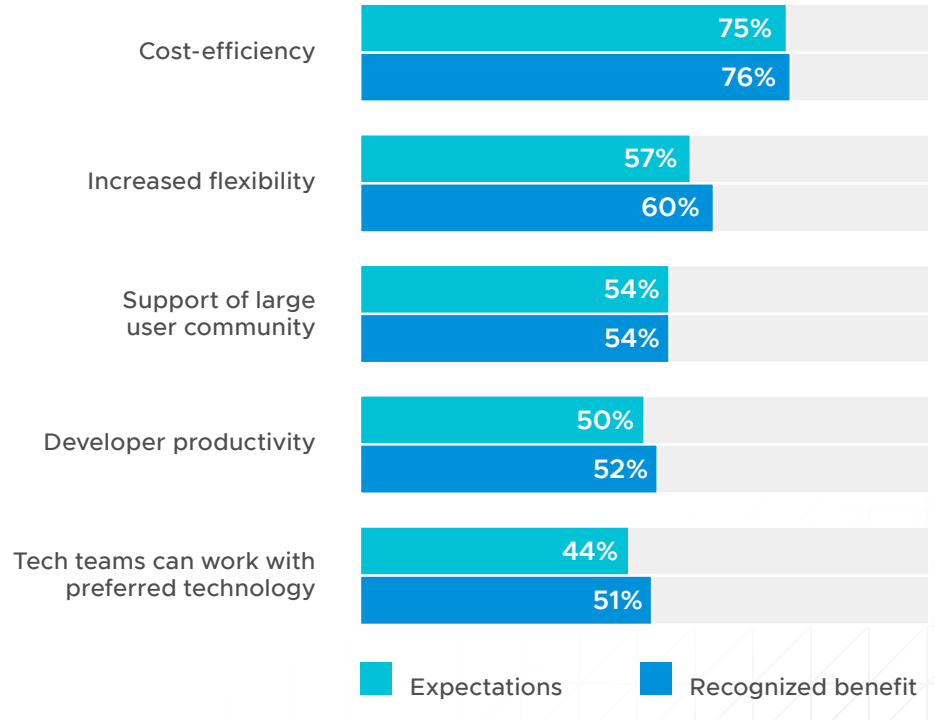
Sometimes, you learn a lot by asking the same question from slightly different angles. This year, in addition to asking, *"What benefits does your organization realize from running open source software in production?"*, we also asked the question, *"Why does your organization use open source software?"*. This allowed us to understand how closely the reasons for choosing OSS match the reported benefits, and the answer is VERY CLOSELY. There's a strong correlation for each of the top five benefits.

In particular, 75% said that *cost efficiency* was a **reason** for using OSS, while 76% said it was a **benefit** of using OSS. While OSS can be free to use, many question whether the "all in" cost of owning and operating OSS is favorable. This survey demonstrates that in real-world production environments, companies find OSS to be cost efficient.

When we look specifically at respondents that selected cost efficiency as a reason for using OSS, almost 9 in 10 (89%) also recognize it as a benefit.



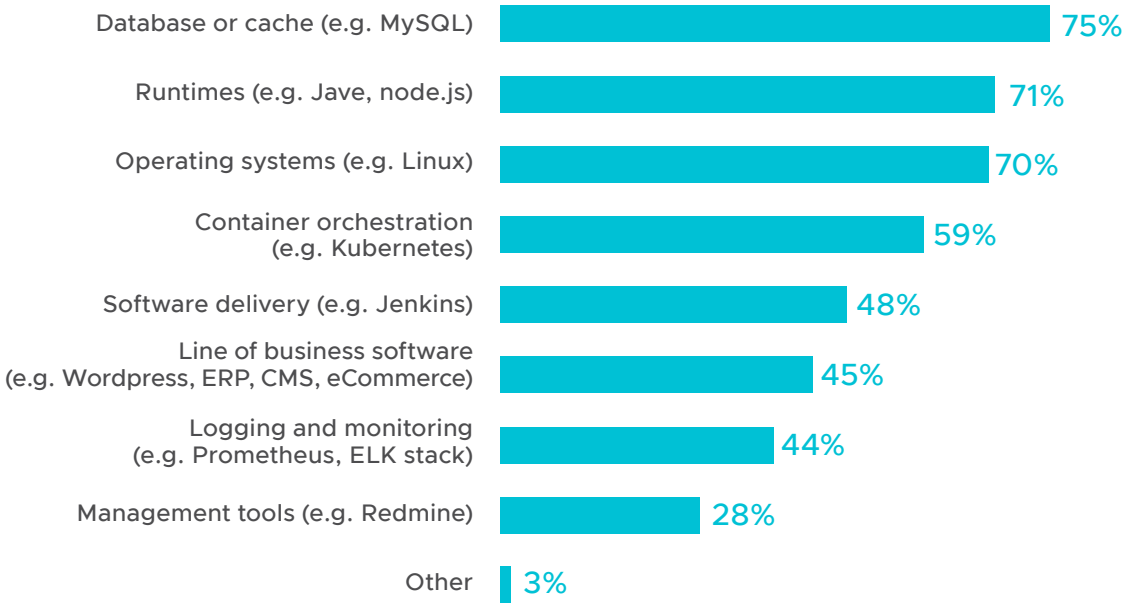
9 out of 10 stakeholders who said *cost efficiency* was a reason their organization used OSS recognized cost efficiency as a benefit



A Wide Variety of OSS is in Use

Naturally, we wanted to understand if there were any big changes in the kinds of OSS companies are using. The heaviest hitters this year included: *database or cache* (75%), *runtimes* (71%), *operating systems* (70%) and *container orchestration* (59%). There is also a significant amount of OSS *line of business software* in use (45% of respondents).

Smaller companies use a different mix of OSS. In particular, they are far less likely to use OSS for *container orchestration* (35% vs 59%), *software delivery* (31% vs 48%) and *logging and monitoring* (33% vs 44%). Small companies are far more likely to use open source *line of business software* (57% vs 45%), including solutions for ERP, CMS, eCommerce and WordPress.



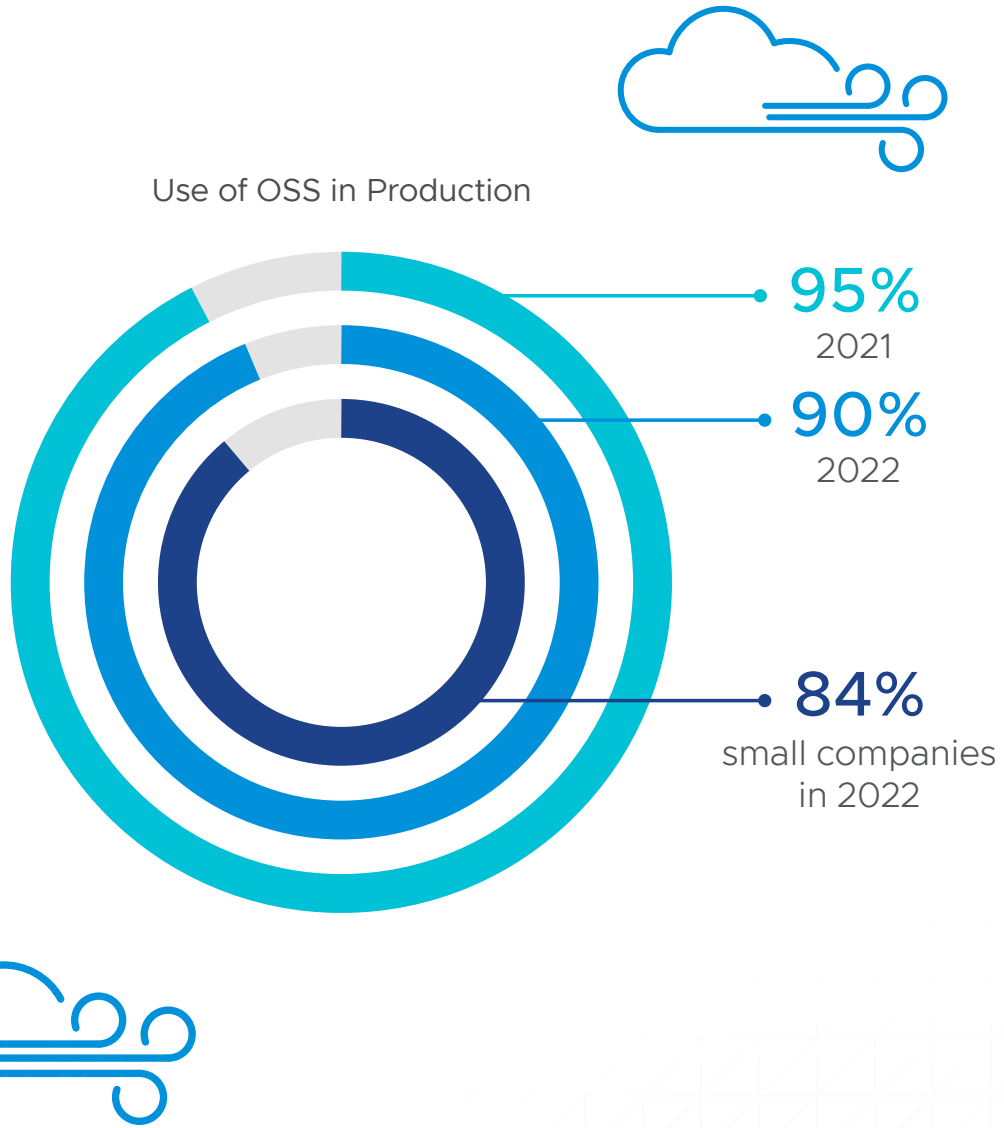
Because a majority of companies (70%) use open source operating systems, we asked respondents to **EXCLUDE** operating systems from consideration when answering the remainder of the survey questions.

OSS Headwinds

While the organizations surveyed clearly benefit from using OSS, this year's study also makes it clear that there are significant headwinds to OSS adoption, and some trends are moving in the wrong direction.

5% Fewer are Using OSS in Production

This year, 90% of respondents report using OSS in production, a drop of 5 percentage points versus last year (95%). Even if we exclude companies with less than 500 employees to ensure an apples-to-apples comparison (since last year's survey didn't include companies smaller than 500 employees), the decline is 4 points. Just 84% of small companies (*100 employees or fewer*) use OSS in production.



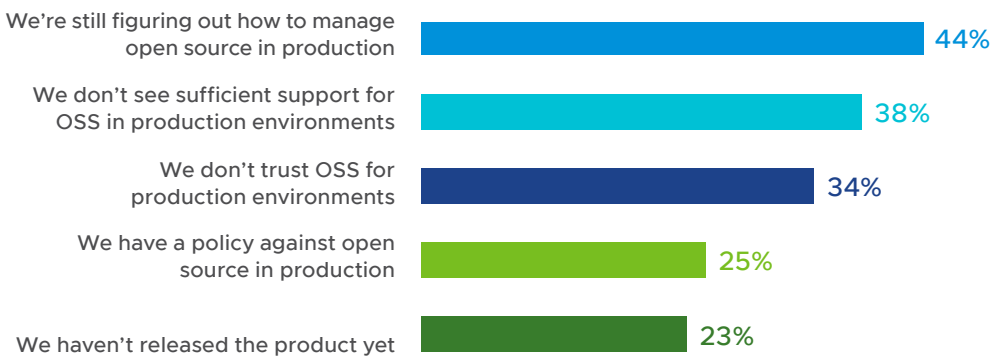
Biggest Headwinds are Management, Support and Trust

When we asked what was keeping a growing fraction of stakeholders from production deployment, many (44%) selected *we're still figuring out how to manage OSS in production.* However, 38% chose *we don't see sufficient support for open source software in production environments,* and 34% chose *we don't trust open source software for production environments.*

Last year, 46% of respondents selected *we have a policy against open source software in production.* This year, that number declined to just 25%. This dramatic change is not just an artifact of the inclusion of smaller companies. Only 35% of stakeholders from companies with *more than 10,000 employees* now have a policy against open source. These are the companies you might expect to be most cautious and policy-bound.

Thus, ironically, fewer companies have a policy against using OSS in production versus last year, yet fewer are actually putting OSS in production.

Why Hasn't Your Organization Deployed OSS in Production?

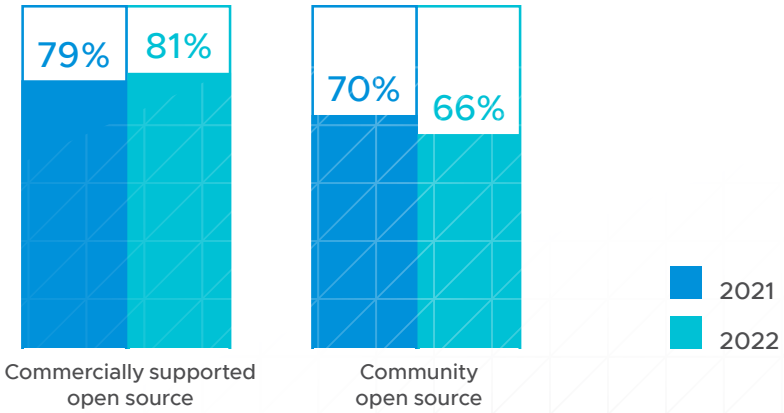


A Slight Trend Towards Commercially Supported OSS

Given the clear concerns about management, support and trust, you might expect to see greater adoption of commercially supported OSS. This is in fact the case. Of companies with more than 500 employees, 81% are using *commercially supported open source* versus 79% last year, while 66% are using *community open source* versus 70% last year.

Companies with *fewer than 100 employees* are much more likely to use *community open source* (79% vs 70% overall) and much less likely to use *commercially supported open source* (57% vs 75% overall). You might expect that smaller companies would benefit most from commercial support, suggesting that the cost of support is inhibiting small companies from choosing it.

Use of Commercially Supported OSS Increased, While Community OSS Declined (Companies with 500+ Employees)



Security Concerns and Risks Dominate

Security concerns and perceived risks increased this year, discouraging more companies that use OSS in development from using it in production. Almost all stakeholders surveyed have concerns about production use of OSS. Two of the top three concerns involve security and the OSS community, while the top two security risks identified pertain specifically to security vulnerabilities.

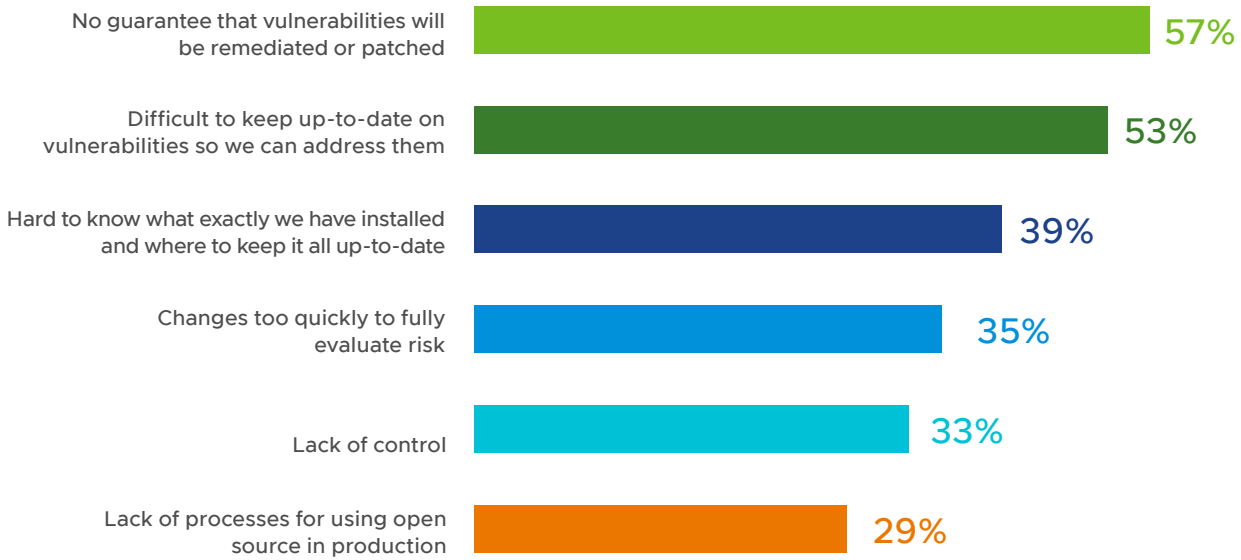
Concerns About OSS in Production are Dominated by Security (Again)

This year, 94% of respondents expressed concerns about running OSS in production, with security concerns dominating the list. The top three concerns are all security related, and all show a substantial increase versus last year. *Dependency on community to patch bugs and fix vulnerabilities* tops the list at 61%, up from 56% last year, followed by *increased security risks* (53% vs 47% last year) and *lack of SLAs for patches from community* (50% vs 42%).

Security Concerns on the Rise

When asked specifically about the security risks of OSS in production, most risks show an uptick since last year. The risks with the largest increases were *lack of good processes for using OSS in production* (+14 percentage points) and *hard to know what exactly we have installed and where to keep it all up-to-date* (+7%).

What Concerns Do You Have About the Security Risks of Open Source Software Deployed in Your Production Environment



Take Advantage of Trusted OSS to Increase Security and Streamline Operations

Given all the production concerns and security risks associated with OSS, it can make sense for organizations to take advantage of customizable, pre-packaged OSS from a trusted source, eliminating significant toil, risk and worry. **VMware Application Catalog** helps you streamline development with a continuously maintained and verifiably tested catalog of open source containers **and** virtual machine images. Choose from an extensive library of OSS that automates patches, upgrades and dependency management. VMware Application Catalog increases convenience for developers and inspires confidence for operators.

Visit the **VMware Application Catalog page** to learn more.

Tools, Tasks and Teams

In 2022, packaging OSS remains difficult and time-consuming, with processes dominated by too many tools, too many tasks and too many teams. For companies using or considering the use of OSS, this is a key area where optimization—either by choosing better tools or by finding commercial sources—may provide significant benefits.

State of Packaging

Last year's report found that too many tools, too many (manual) tasks and too many teams were involved in packaging OSS at most companies. Little has changed this year.

Tools. 70% of companies use two or more tools, with 36% using 3 or more. The most common behavior appears to be the use of two tools at 34%.

Tasks. A large number of tasks are performed before OSS goes into production, including *functional testing* (performed by 68%), *load testing* (52%), *scanning for CVEs* (48%) and *building a software bill of materials* (34%). Companies with *100 employees or fewer* are less likely to perform these tasks: *functional testing* (57% vs 68%), *load testing* (37% vs 52%) and *scanning for CVEs* (34% vs 48%).

Teams. Packaging tasks remain split between *Development* (60%), the *DevOps team* (60%), *IT operations* (47%) and *Platform operations* (27%). Once again, multiple teams appear to be involved in OSS packaging. As company size increases, the burden of packaging shifts from *Development* (declines from 65% to 55%) to the *DevOps team* increases (from 46% to 66%).

To improve OSS packaging in the coming year, companies should consider vesting responsibility for packaging in a single team, automating tasks, and consolidating packaging tools.

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. Similar packaging processes are also used by companies that offer commercially supported OSS, and by independent software vendors (ISVs) that include OSS as part of a commercial software package.

Almost Everyone Packages Their Own OSS

The vast majority of organizations surveyed (95%) are directly involved in packaging open source software. When asked to select the methods used for packaging, 56% chose *we use software the community has already packaged*, and 55% selected *we package open source software internally.* Much less popular were *we have a service provider that packages open source software* (28%) and *we purchase pre-packaged open source software* (28%). Given the difficulties with packaging, you might expect the last two options to gain in popularity. We'll ask this question again next year and see if there's a trend.

Companies with 100 employees or fewer are less likely to *package open source software internally* (47% vs 55%) but also far less likely to purchase pre-packaged open source software (17% vs 28% overall).

of respondents are involved in packaging OSS

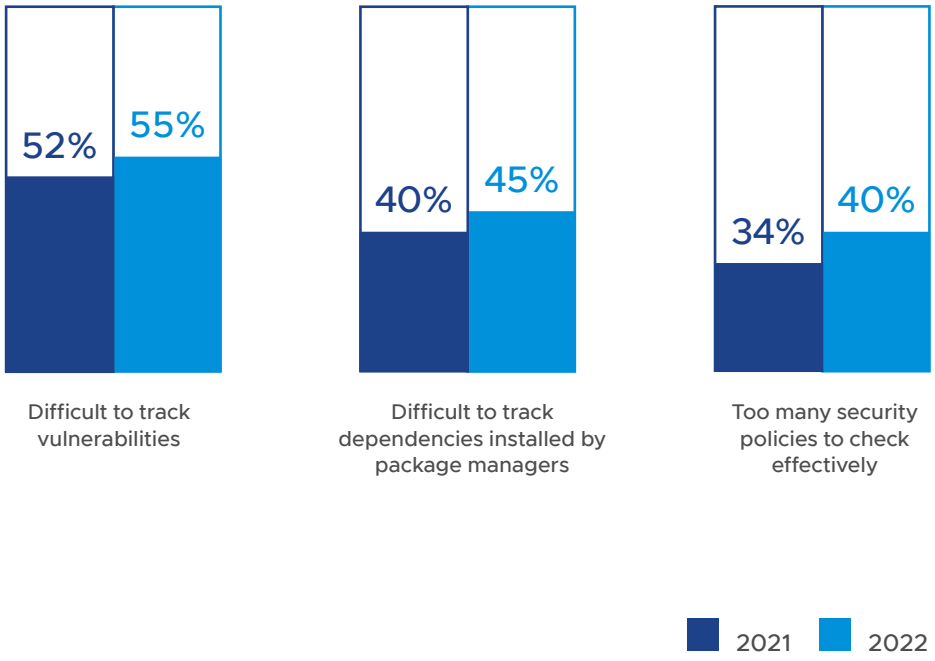
What Methods Does Your Organization Use for Packaging Open Source Software?

Packaging Challenges Are on the Rise

When we compare packaging challenges this year versus last, challenges have risen across the board. *Difficult to track vulnerabilities* increased by 3 percentage points from 52% to 55% of respondents. *Difficult to track dependencies installed by package managers* rose from 40% to 45%, and *too many security policies to check effectively* increased from 34% to 40%.

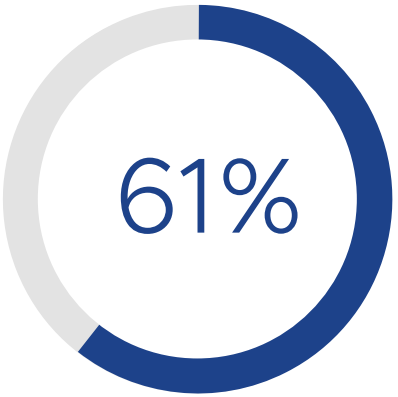
Almost a third (29%) of respondents said that the whole process of packaging OSS was *time consuming and boring.*

Packaging Challenges Increased Across the Board (Companies with 500+ Employees)



Critical Security Patches Take Too Long

A side effect of all the complexity associated with packaging OSS is that it takes significant time to deploy critical security patches. Almost two thirds (61%) take *more than a day* to deploy a critical security patch; 12% require *more than a week*. This is an area where small companies perform notably better. Almost half of the companies with *100 or fewer employees* can deploy a critical patch in *less than a day*, and almost a quarter (24%) can get the job done in *a few hours or less*.



take more than a day to deploy a critical security patch

Everyone Wants Better Security

When asked about software packaging capabilities that would improve security, the top three were *immediate access to trusted security patches to applications or runtimes, dependencies and operating system components* (60%), *centralized visibility to all scans to simplify security audits* (55%) and *automatic CVE and virus scanning for every container* (51%).

Which of These Capabilities for Software Packaging Would Help Manage the Security Risk of the Software Supply Chain?

One Packaging Tool to Rule Them All?

Organizations are finding it more and more complex to package and deliver OSS. It's a massive challenge for any organization that needs to control its software supply chain and adhere to industry standards and best practices. Companies would benefit greatly from a single, platform-agnostic service to build images.

VMware Image Builder automates the packaging, verification and publishing of customized and secure OSS images. It enables ISVs, large enterprises and smaller companies to move faster when building applications, while ensuring security and compliance.

VMware Image Builder allows you to:

- Build fully functional solutions in the desired format
- Validate your package on multiple platforms—including GKE, AKS, EKS, VMware Tanzu Kubernetes Grid and VMware Cloud. Verification includes automated functional and verification tests, health checks, CVE scanning and container scans using the latest generation tools
- Seamlessly publish packages onto Helm and OCI registries

To learn more about VMware Image Builder, read the **VMware blog**.

Summary and Recommendations

Open source software is a critical element of the software supply chain in companies of all sizes. While OSS is clearly fulfilling stakeholder expectations for cost efficiency (76%), increased flexibility (60%) and developer productivity (52%), significant concerns and risks have reduced the number of companies that are willing to deploy OSS in production environments this year from 95% to 90%. Given the rapid increase in cyberattacks against organizations worldwide, it's not surprising that two of the top three OSS concerns involve security, while the top two OSS security risks pertain specifically to the ability to identify and address vulnerabilities.

It's important to keep in mind that the sample for this survey consists of companies that are already using OSS, either in development only or in development **and** production. It's possible and even likely that the chilling effects of these concerns are far greater in companies that are considering OSS but haven't pulled the trigger.

OSS packaging is essential to ensure the security of the OSS supply chain, but it has become a significant source of complexity and concern. Packaging capabilities including *immediate access to trusted security patches* (60%), *centralized visibility to all scans* (55%) and *automatic CVE and virus scanning* (51%) would go a long way in addressing the packaging concerns of stakeholders.

While OSS offers clear and compelling benefits, better approaches to packaging security are needed. There are two approaches that companies can consider that will improve the security of OSS operations:

- **Integrated packaging tools.** Packaging tools can reduce complexity by integrating and automating tasks such as functional testing, CVE scanning and publishing to repositories.
- **Pre-packaged OSS.** Choosing OSS packaged by a trusted source removes a lot of the uncertainty around security and eliminates the risk of CVEs. Updates become available quickly as new CVEs are found.

Given the wide variety of OSS available, it may be necessary to use both approaches to meet the entirety of your OSS needs. These building blocks can significantly increase developer velocity when combined with an end-to-end developer platform.

VMware Tanzu has the capabilities to address your OSS challenges and concerns. VMware Image Builder automates the packaging, verification and publishing of customized and secure OSS images, ensuring security and compliance. VMware Application Catalog helps you streamline development with a continuously maintained catalog of open source containers and virtual machine images. Components in these catalogs are automatically updated, so you always deploy the most secure stack while eliminating tedious packaging and security tasks. Tanzu Application Platform is a flexible, end-to-end development platform that integrates packaging and security.

Simplify and Secure the Software Supply Chain to Increase Developer Velocity

Making your developers and DevOps teams responsible for the intricate details of packaging and security can be a recipe for disaster. Your software supply chains should automate and secure the path to production, using a shift-left methodology that applies best practices automatically. **Tanzu Application Platform** offloads manual packaging and security tasks, allowing your teams to focus more attention on delivering the best possible code.

The software supply chains used by Tanzu Application Platform automate and secure the processes for building, testing and delivering software to production across multiple Kubernetes clusters and multiple clouds. When a developer commits code, the Tanzu Application Platform supply chain is triggered, including automated testing, source scanning, signing and image scanning. These steps eliminate manual toil and increase the quality of software that uses OSS components. A software bill of materials (SBoM) is automatically generated, making it simple to determine which OSS packages are used by which workloads. When a base package is updated, Tanzu Application Platform automatically rebases and updates your software, so you never miss important security updates.

To learn more about Tanzu Application Platform, visit **tanzu.vmware.com/tap**

VMware Tanzu®

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

Get in touch

vmware®