

Introduction to managed open source

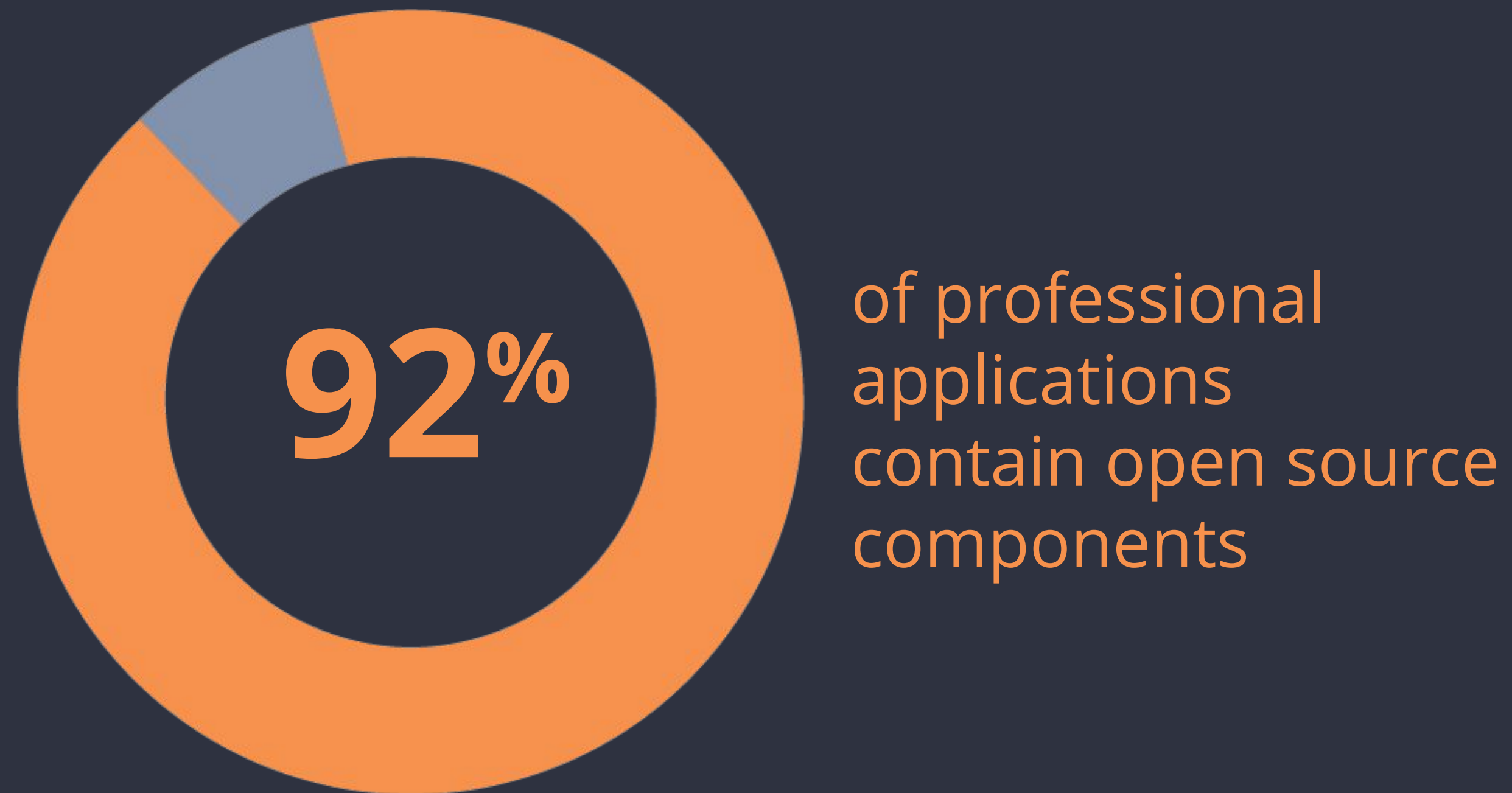
TIDELIFT

Managed Open Source

A way for application development teams
to offload the complexity
of managing open source components.

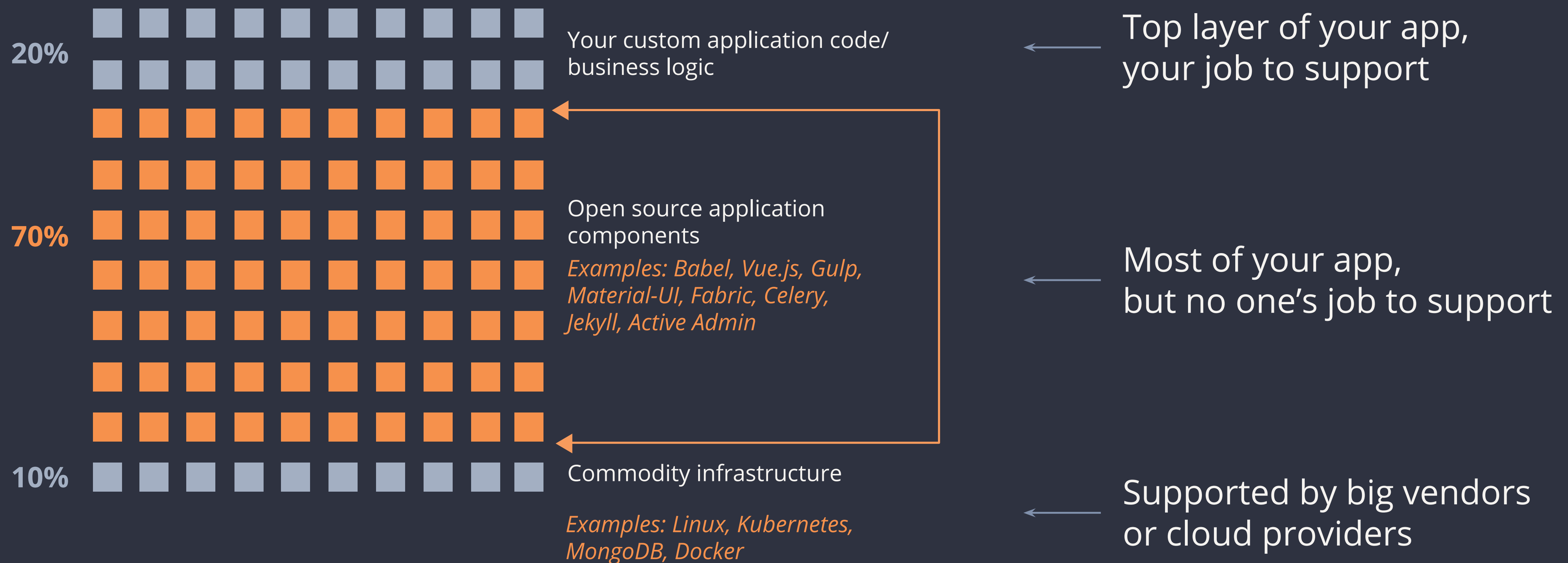
Save time. Reduce risk.

Open source = the modern development platform



- It is fundamental to the development process and essential for building applications
- It is a blessing (productivity boost) and a curse (dependency hell and other maintenance headaches)

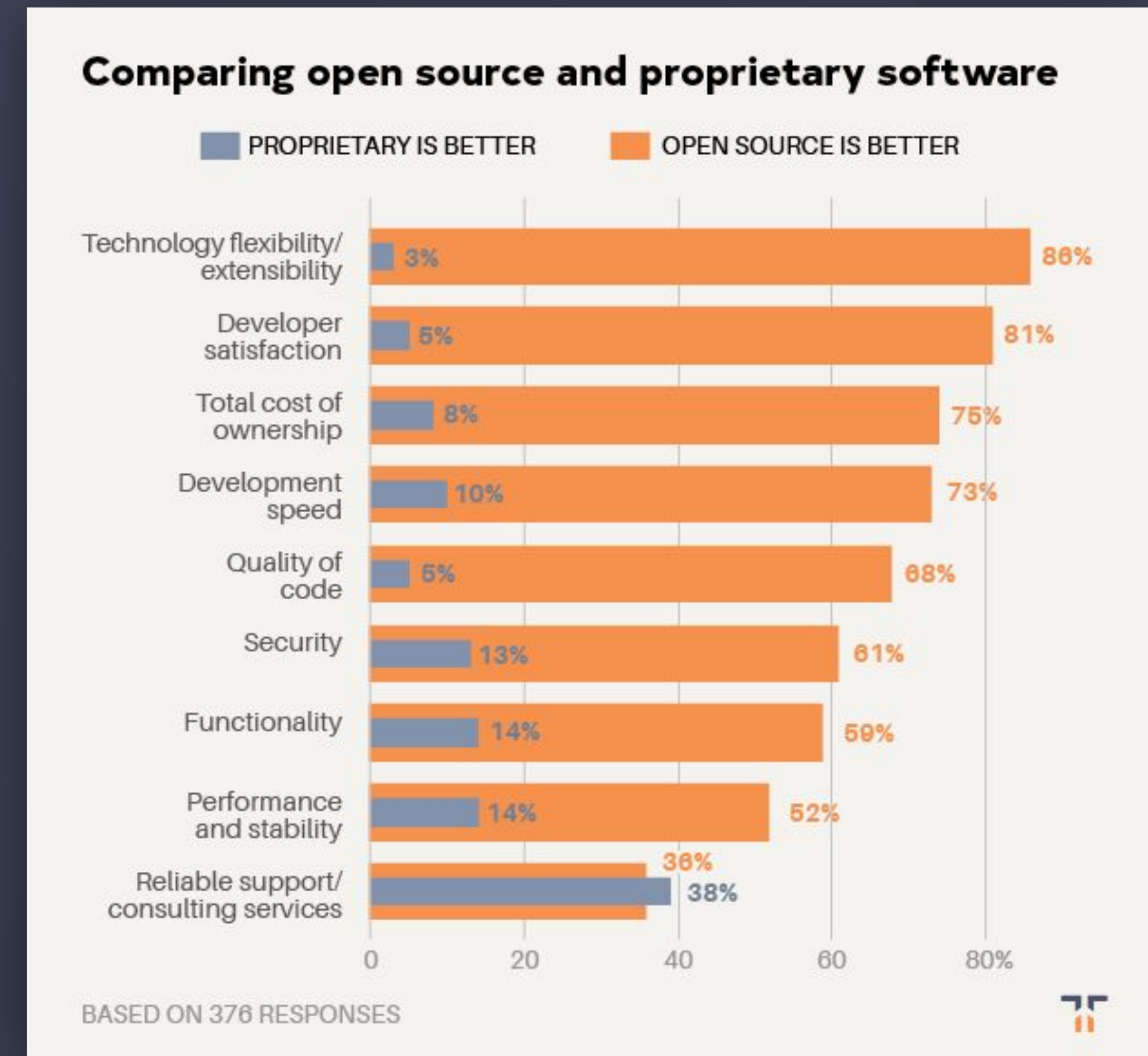
Most applications are built on top of a foundation of 70% or more open source code



Who's supporting the 70% of components you use to build your apps?

Historically, reliable support for open source is the only pain reported by many development teams.

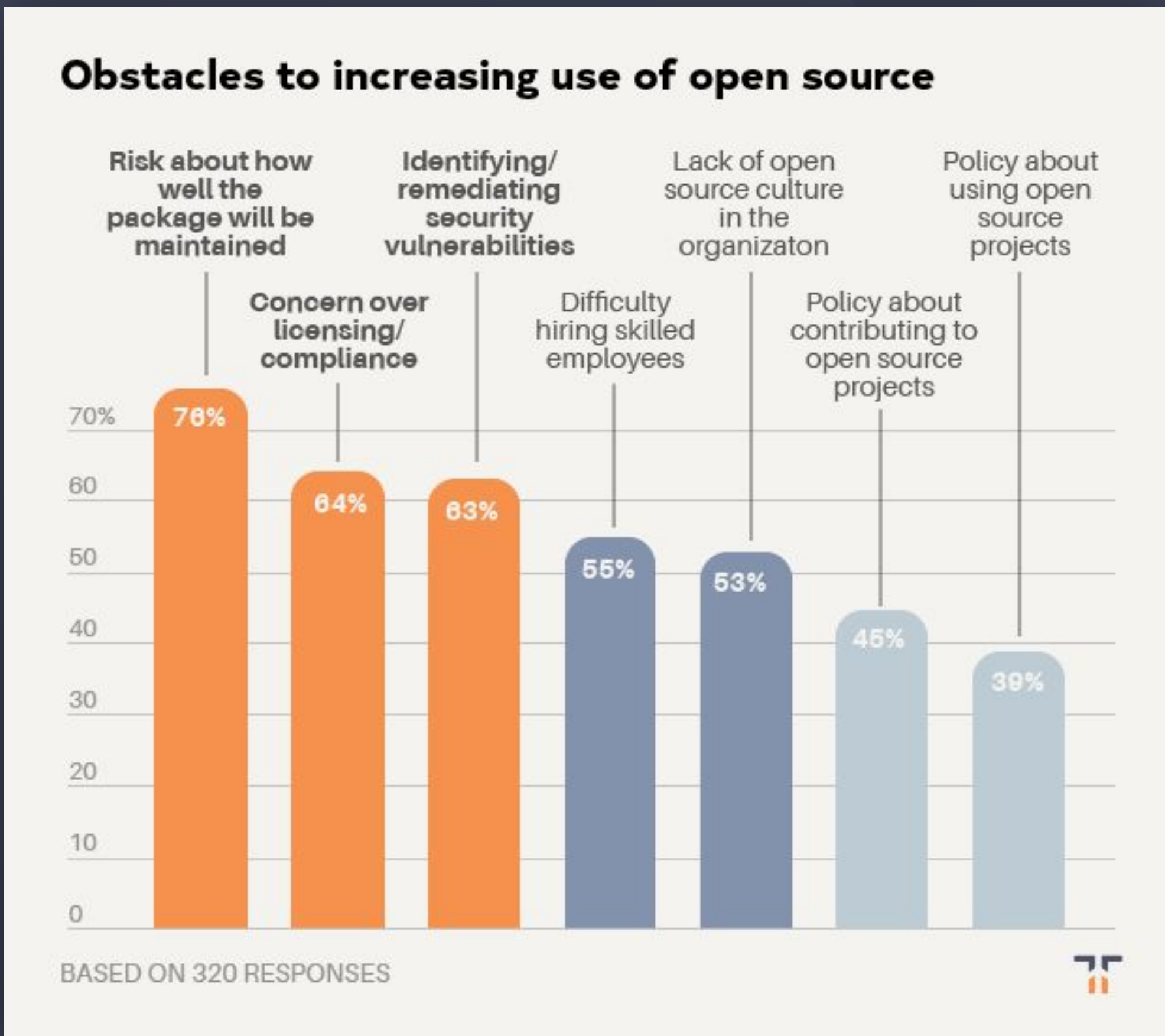
Open source outclasses proprietary software in every other category.



The big three support challenges: maintenance, security, and licensing

In multiple surveys, the biggest obstacles for development teams using open source have been remarkably consistent:

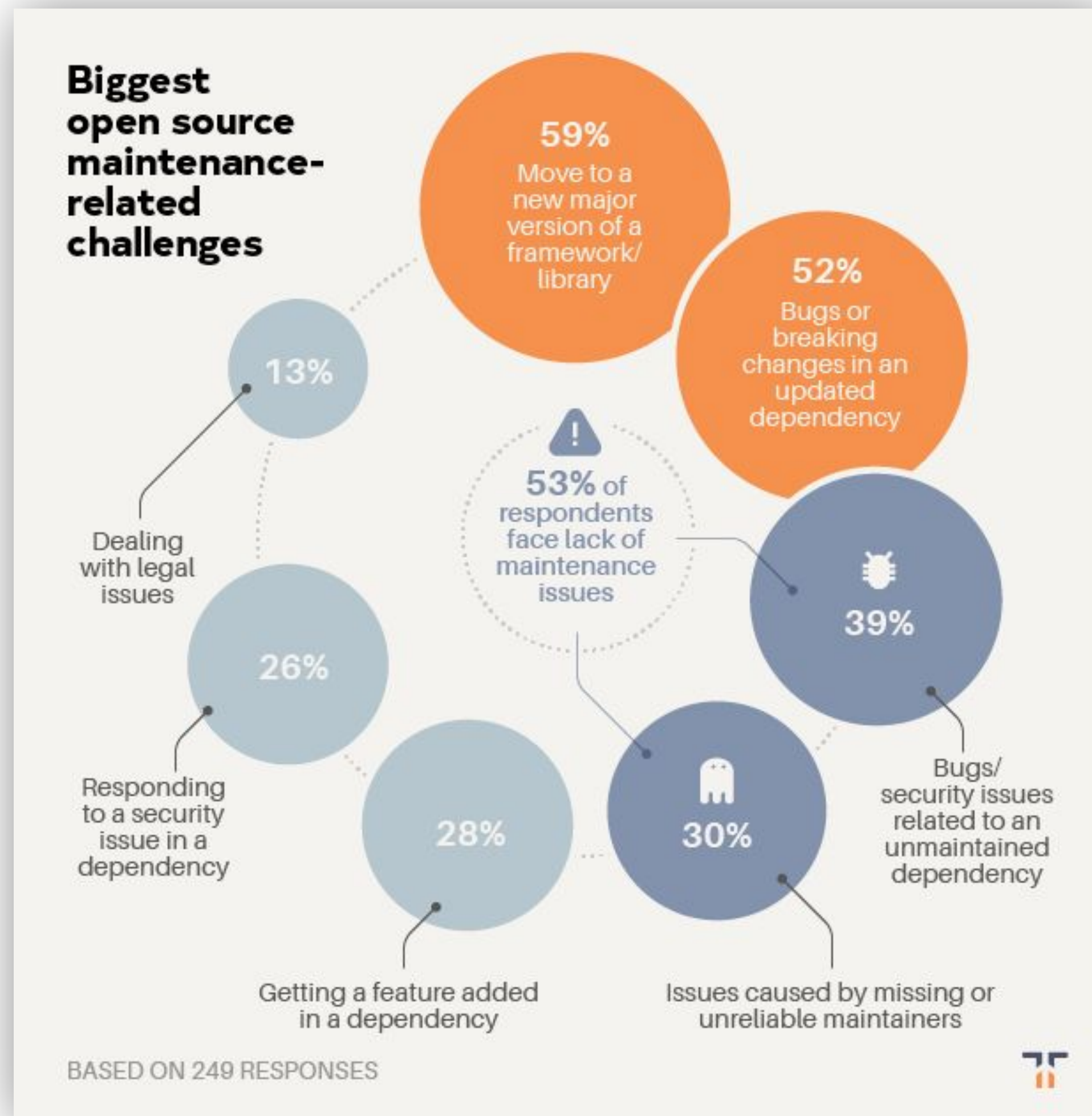
- Maintenance
- Security
- Licensing



Unmanaged open source drains productivity

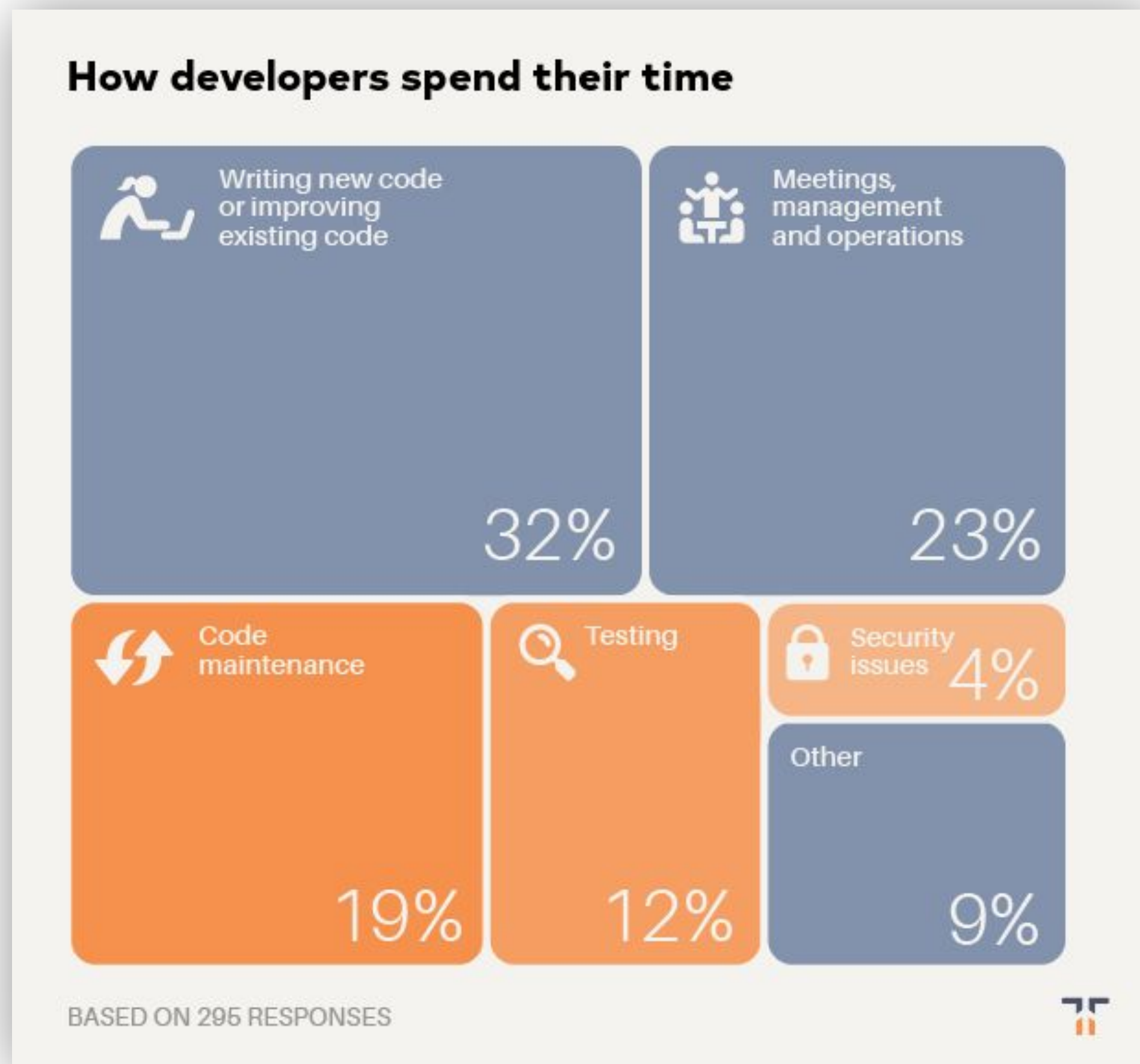
Biggest maintenance challenges include **moving to a new major version of a framework or library** and **bugs or breaking changes** in an updated dependency affecting their software supply chain.

Over half of development teams regularly face **challenges related to poorly maintained open source dependencies**.



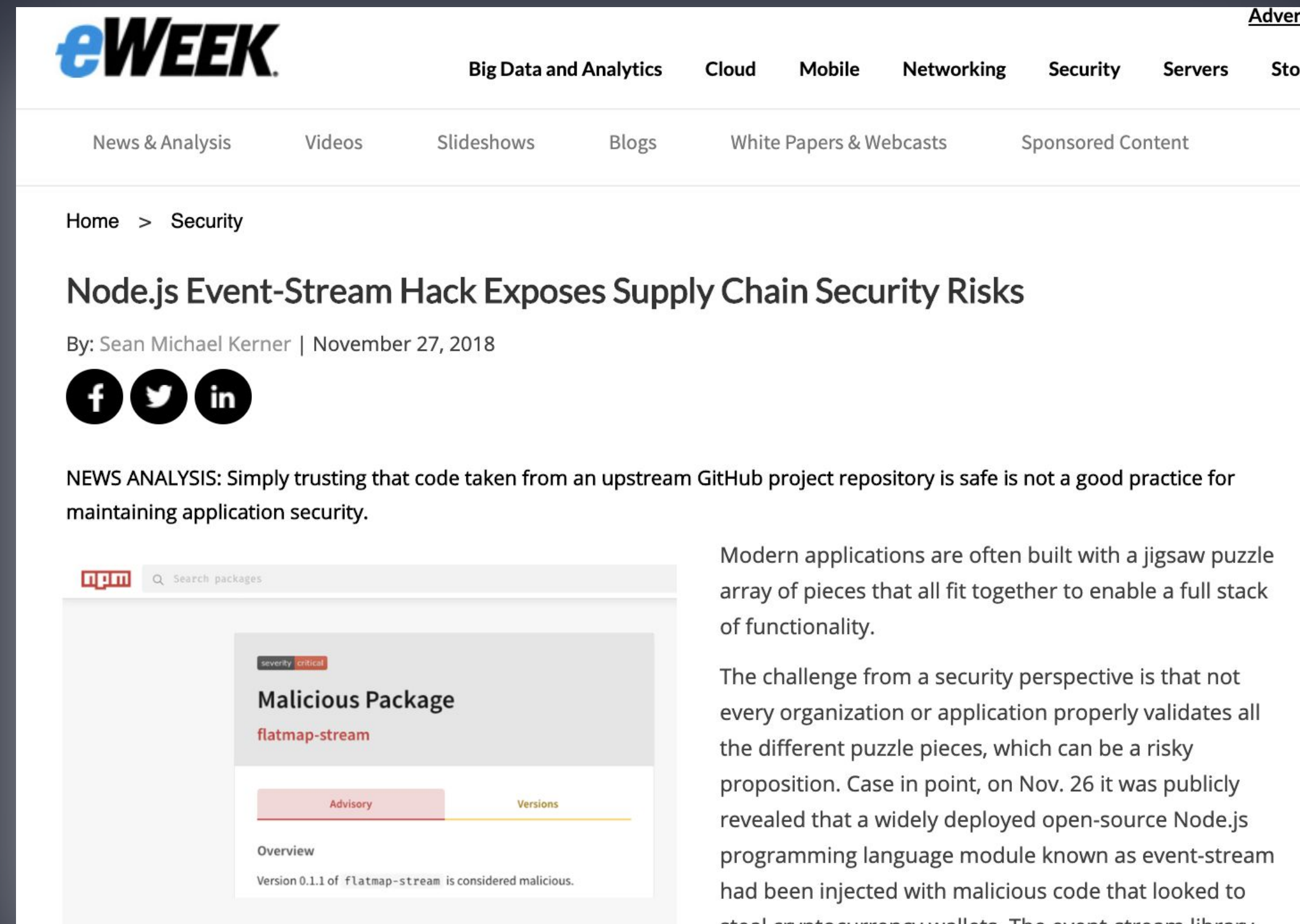
While taking up valuable time that could be spent writing code

Developers spend more time on **code maintenance, testing, and security** issues than they do **writing code**.



What can happen when code isn't professionally maintained?

One example: event-stream, an npm package with over 100 million downloads and no active maintainer, is taken over by a malicious actor trying to steal bitcoin.



The screenshot shows a webpage from eWEEK. The navigation bar includes links for Big Data and Analytics, Cloud, Mobile, Networking, Security, Servers, and Storage. Below this is a secondary navigation bar with News & Analysis, Videos, Slideshows, Blogs, White Papers & Webcasts, and Sponsored Content. The article title is 'Node.js Event-Stream Hack Exposes Supply Chain Security Risks' by Sean Michael Kerner, dated November 27, 2018. It features social media icons for Facebook, Twitter, and LinkedIn. A 'NEWS ANALYSIS' section states: 'Simply trusting that code taken from an upstream GitHub project repository is safe is not a good practice for maintaining application security.' An inset image shows the npm package page for 'flatmap-stream', which is marked as 'Malicious Package' with a 'severely critical' advisory. The advisory text reads: 'Version 0.1.1 of flatmap-stream is considered malicious.' The main text of the article discusses how modern applications are built with a jigsaw puzzle of dependencies and how a security perspective challenge arises when not all pieces are properly validated. It mentions a case where a widely deployed open-source Node.js module, event-stream, was injected with malicious code to steal cryptocurrency wallets.

Other horror stories

EQUIFAX



heartbleed

How can
development teams
using open source
address these issues?

AND UTILIZE OPEN SOURCE TO ITS FULL POTENTIAL

A historical analogy: life before cloud computing?

15 years ago if you were launching a new SaaS app you would need to:

- Rent space from a reputable hosting facility
- Buy and install servers to ensure your app has appropriate backup / failover
- Configure all of the software you need on those servers
- When something goes physically wrong with a server, drive or fly to the hosting facility, swap it out, install software updates, etc.

Today, same scenario:

- AWS or another cloud provider takes care of hosting, you take care of your app

Yet when it comes to the numerous open source components our apps rely on, today **development teams still carry the burden themselves.**

THE SOLUTION

The Tidelift Subscription

Managed open source for application development teams

The Tidelift Subscription is a managed open source subscription for application dependencies covering millions of community-led open source projects across JavaScript, Python, Java, PHP, Ruby, .NET, and more.

Save time. Reduce risk. Improve code health.



Enterprise-ready open source software— managed for you

Tidelift uses a layered approach to keep your open source dependencies trouble-free and enterprise-ready.

Tools. We provide tools to keep track of all the dependencies you use, flag issues, and enforce policies.

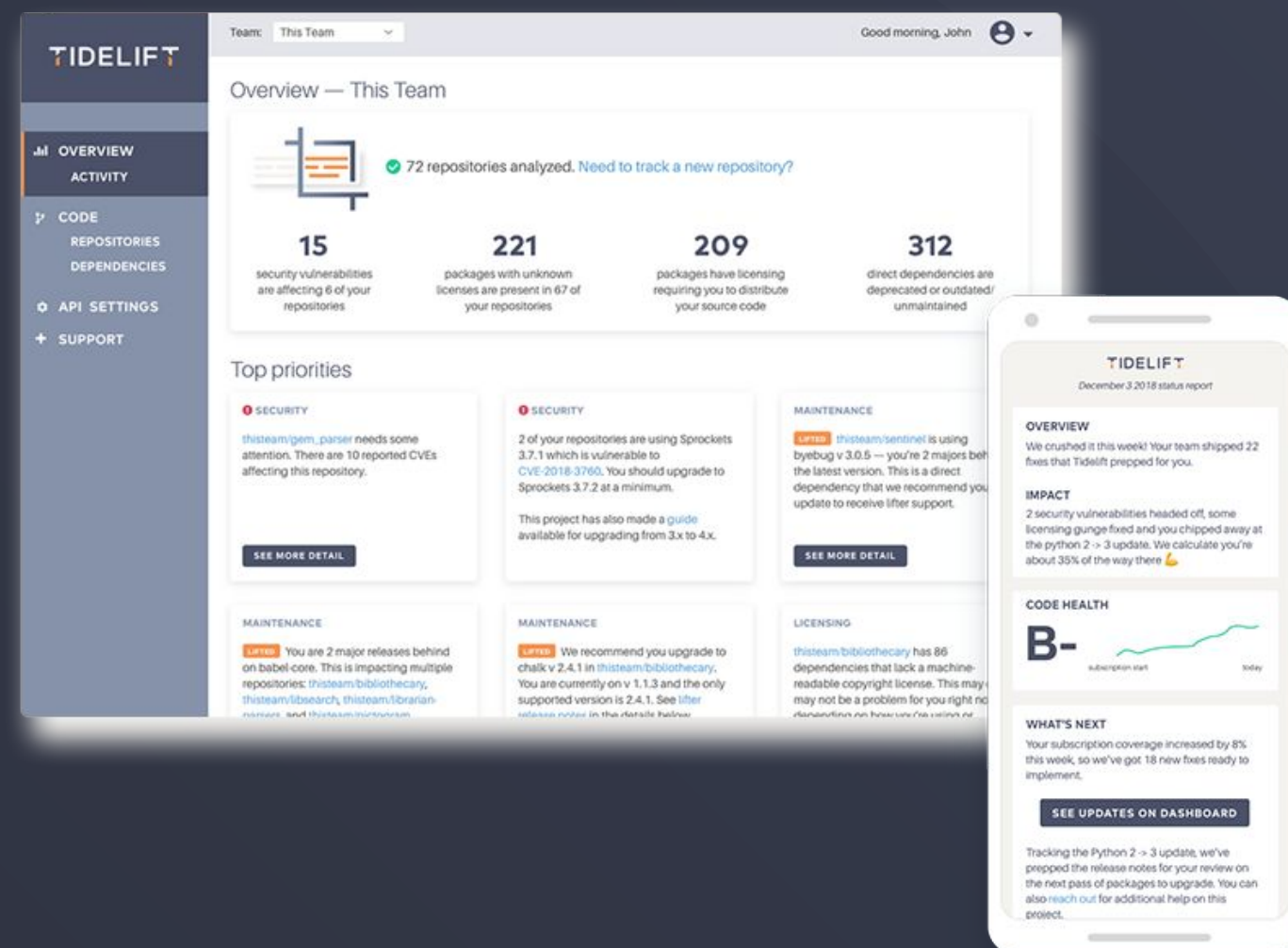
Management. We manage core, mission-critical packages on your behalf, including researching and resolving issues so you don't have to anymore.

Maintainers. We recruit maintainers for many important projects and pay them to proactively prevent problems and address the root causes of issues.

A managed open source subscription backed by maintainers

1

You purchase a managed open source subscription from Tidelift



2

Maintainers of the packages you use get paid and spend more time making their packages better



“This model helps us move closer to a future where many more maintainers like me can afford to work on their projects full time.”
—Evan You, founder of Vue

3

Which makes your apps perform better, while becoming more secure and reliable

Key benefits of the Tidelifft Subscription



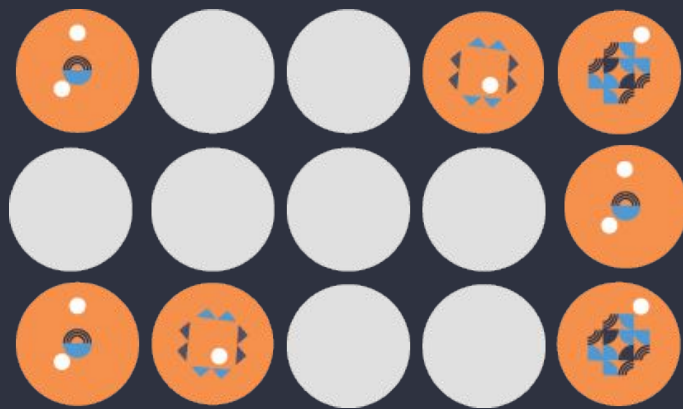
Security updates



Licensing verification and indemnification



Maintenance and code improvement



Package selection and version guidance



Roadmap input



Tooling and cloud integration



Security updates

Tidelift's security response team coordinates patches for new security vulnerabilities and alerts immediately through a private channel, to keep your software supply chain more secure.



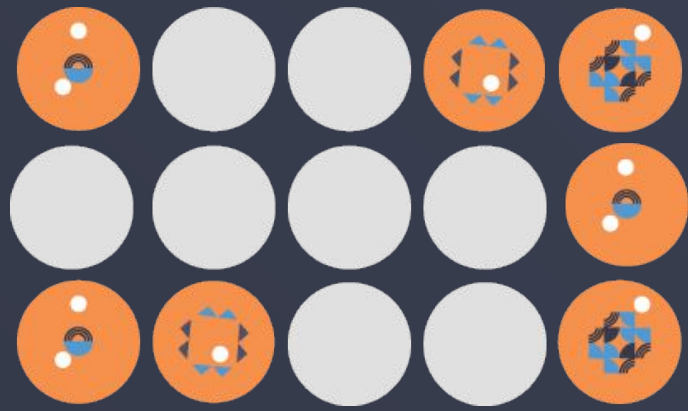
Licensing indemnification and verification

Tidelift verifies license information to enable easy policy enforcement and adds intellectual property indemnification to cover creators and users in case something goes wrong. You always have a 100% up-to-date bill of materials for your dependencies to share with your legal team, customers, or partners.



Maintenance and code improvement

Tidelift ensures the software you rely on keeps working as long as you need it to work. Your managed dependencies are actively maintained and we recruit additional maintainers where required.



Package selection and version guidance

We help you choose the best open source packages from the start—and then guide you through updates to stay on the best releases as new issues arise.



Roadmap input

Take a seat at the table with the creators behind the software you use. Tidelift's participating maintainers earn more income as their software is used by more subscribers, so they're interested in knowing what you need.



Tooling and cloud integration

Tidelift works with GitHub, GitLab, Bitbucket, and more. We support every cloud platform (and other deployment targets, too).

Bottom line:



All the capabilities you expect and require from commercial software.

But now, for all of the key community-led open source software you depend on.

The Tidelift Subscription covers application development in JavaScript, Python, Ruby, PHP, Java, .NET, and more



VUE



BABEL



MATERIAL-UI



FABRIC



DOCTRINE



NOKOGIRI



APACHE STRUTS



PILLOW



GULP



VUETIFY



CELERY



NUXT



MONGOOSE



BYTE-BUDDY



SLIM



CARBON



BYEBUG



MARSHMALLOW



CHERRYPY



PROXY-MANAGER



STANDARD



PRETTIER



PROMISEKIT



URLLIB3



CHALK



PARAMIKO



ACTIVEADMIN



MONOLOG



BEAUTIFUL SOUP



PROJECT LOMBOK

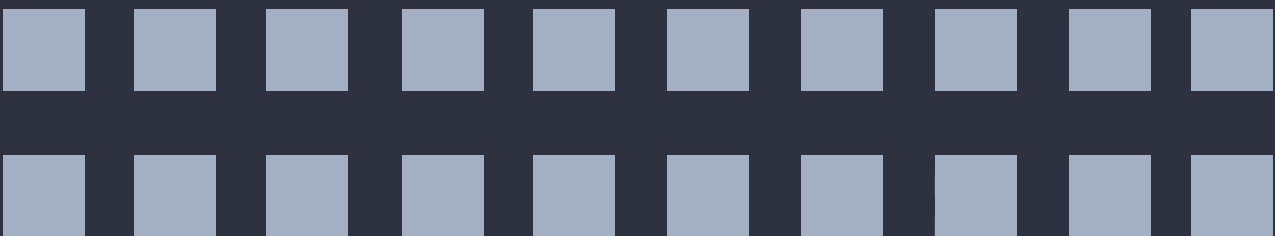


JODA-TIME

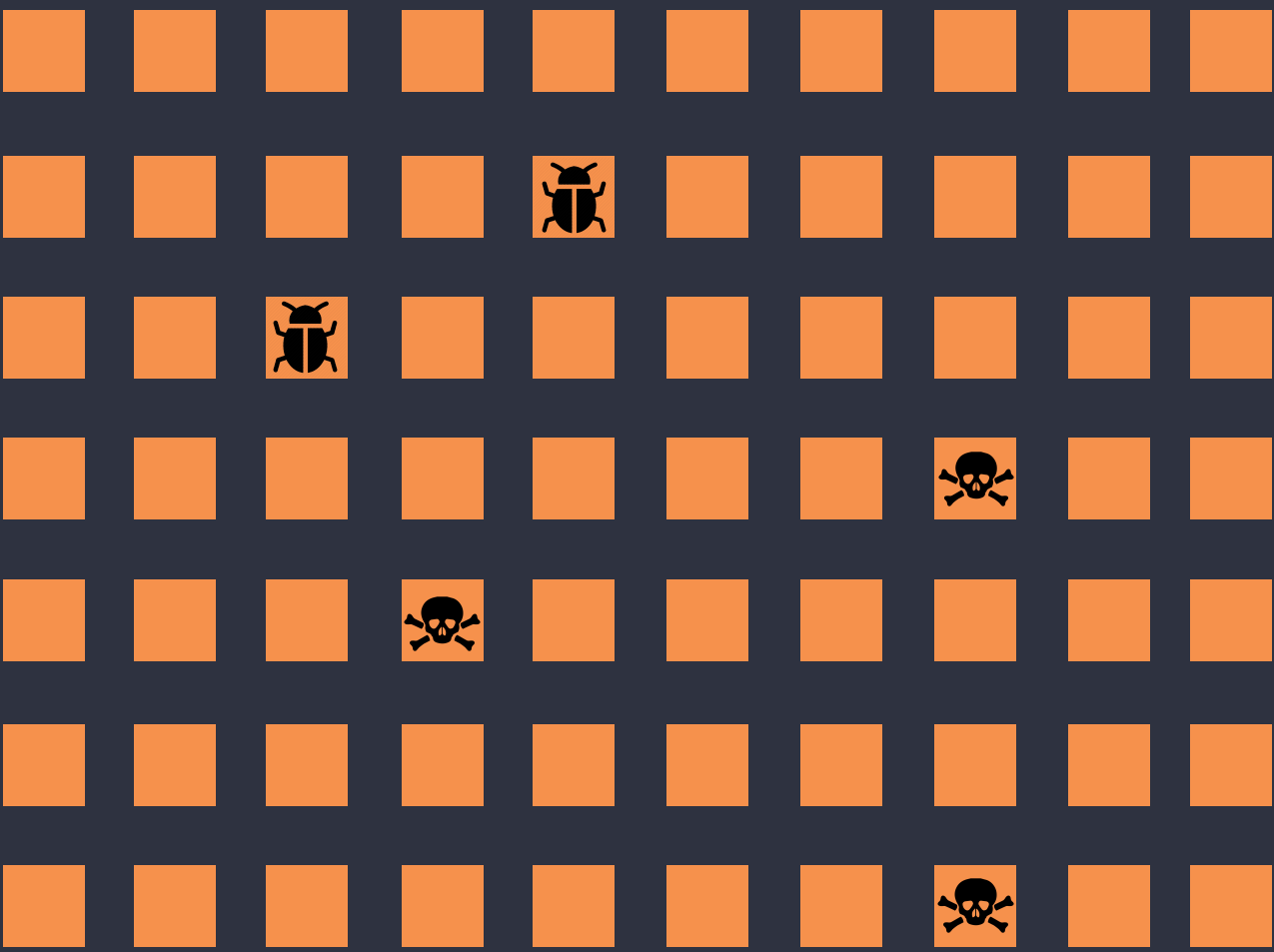
From unmanaged to managed open source

Your stack today

Your custom application code/business logic



Open source application components



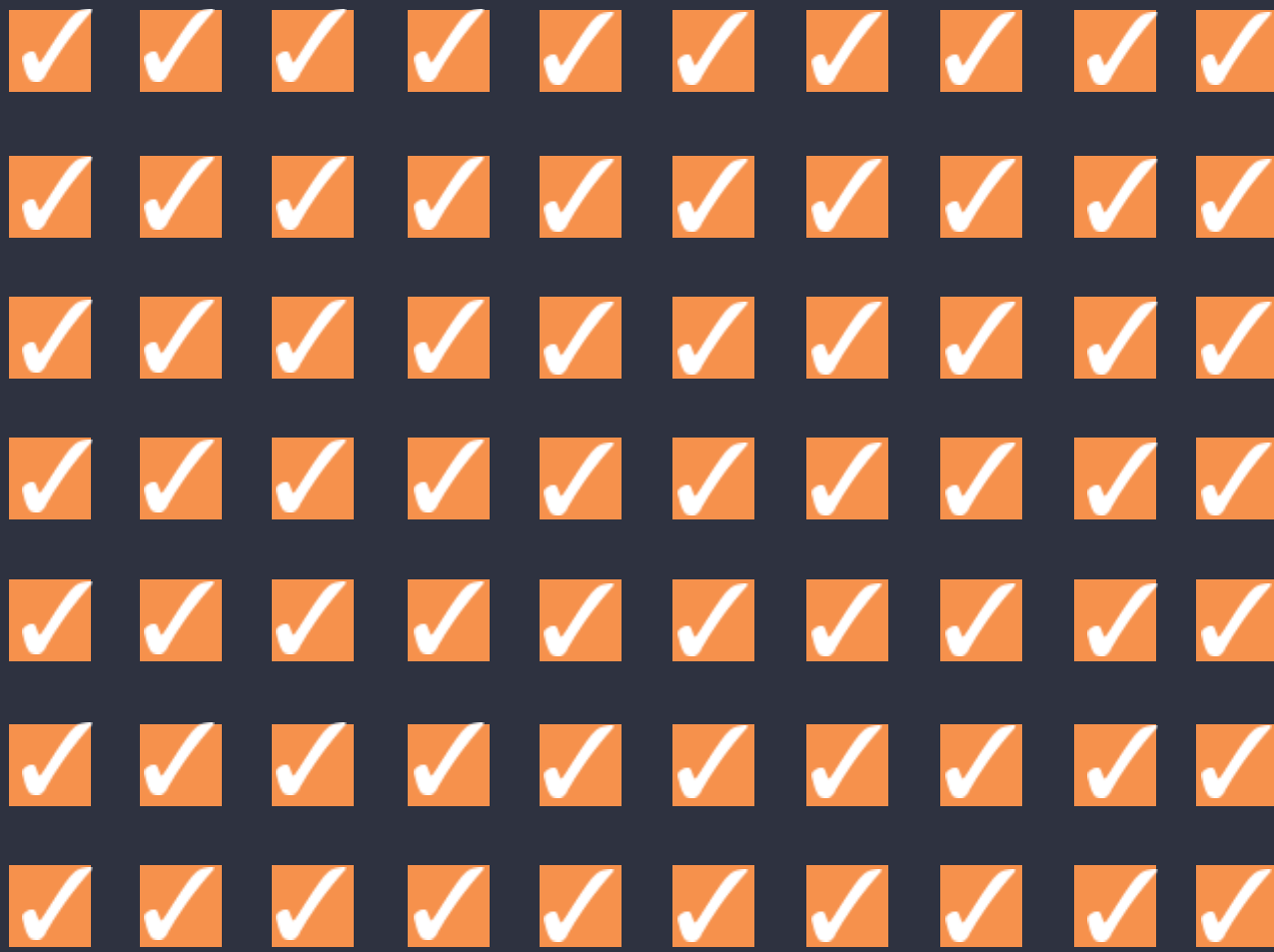
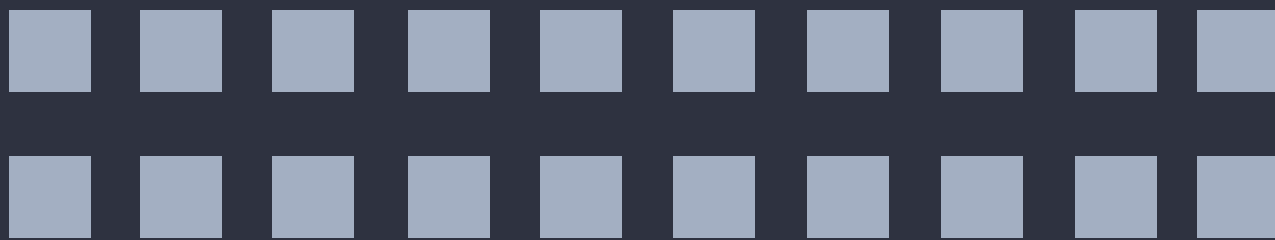
Commodity infrastructure



TIDELIFT

Managed open source subscription

Your stack with Tidelift



Managed open source backed by maintainers



Thank you