OpenSSL CONFERENCE

Who Pays for Open Source?

A first-party answer from the OpenSSL Corporation

Kajal Sapkota Business Development Manager & Commercial Lead, OpenSSL Corporation

OpenSSL Conference 2026 · Prague · The Křižík Effect

OpenSSL CONFERENCE

Who Pays for Open Source?

$2,000

Total donations the OpenSSL project received in 2013, the year before Heartbleed

At that time OpenSSL terminated TLS for roughly two thirds of websites.

OPENSSL OTHER PROJECTS

OpenSSL CONFERENCE

The assumed answer: nobody has to pay; altruistic individuals keep it running, and the companies relying on it are the exception.

What the records show: almost everyone depends, almost nobody pays. Heartbleed 2014 and xz 2024 are what that gap produces.

How I will answer it: OpenSSL's published git history, annual reports, and customer totals, checked against other projects.

1 **The question** and the two kinds of evidence

2 **Underpaid and overworked** Heartbleed 2014, xz 2024

3 **Who pays now** who pays, who does not, which answers fail

4 **What paying buys** commits, reviews, key-person risk

5 **Beyond OpenSSL** kernel, census, abandonment

6 **AI raises the price** of expert review

7 **What you can do** three options

OPENSSL = this project's own record: git history, annual reports, customer aggregates

OTHER PROJECTS = Linux kernel statistics, 23-project census, SAP and Copilot studies

STEP 2 OF 7 · UNDERPAID AND OVERWORKED

What happens when nobody pays?

Heartbleed 2014 · xz utils 2024

2014 to 2024: 10 years, different code, same cause

OPENSSL: HEARTBLEED, 2014

One de-facto full-timer. $2,000 a year in donations.
One under-reviewed patch, 2+ years in production.
~17% of trusted secure servers exposed.
Cleanup: mass certificate and key rotation, worldwide.

Sources: S. Marquess (Apr 2014) · Netcraft (Apr 2014) · shipped Mar 2012, found Apr 2014

XZ UTILS: BACKDOOR, 2024

One overloaded maintainer, openly asking for help.
Two years of trust-building, then a backdoor aimed at SSH logins (CVE-2024-3094).
Caught by one engineer chasing a 500 ms slowdown, weeks before the major distros.
2025: he still wrote 97% of all changes.

Sources: public disclosure, 29 Mar 2024 (A. Freund, Openwall) · sheets.works census (Oct 2026)

We were fortunate: Heartbleed put OpenSSL on the map, and funding followed. xz got a news cycle; its maintainer still works mostly alone.

Details for both incidents: appendix reserves

STEP 3 OF 7 · WHO PAYS NOW

So who pays today?

Customer totals, the commit log, the job boards

OPENSSL

OpenSSL CONFERENCE

Fifteen million users. One hundred payers. Five million dollars

15,000,000+ downloads of the OpenSSL Library in 2024, and it ships inside operating systems, clouds and devices beyond counting (Annual Report 2024)

Thousands of certified products: FIPS 140 and Common Criteria validations across the industry lean on these primitives (public validation listings)

~100 support customers (Annual Report 2025)

$5M: the entire 2025 funding of the Project's dedicated work (Annual Report 2025)

Renewal runs 86 to 88%, so the base is stable. The question for the room: is the bottom of this funnel the right size for what sits on top of it?

Source: OpenSSL Corporation Annual Reports 2024 and 2025 (openssl-corporation.org); each tier labeled with its source

OPENSSL

OpenSSL CONFERENCE

Together the three records show 218 organisations, about twice the customer list

~100

organisations hold OpenSSL support contracts today

customer records, Oct 2026 (totals only)

28

outside organisations landed commits in our repository, 2024 to 2026

status.openssl.org, top-20 tables

130

organisations identifiable across the ten OpenSSL Communities

membership titles, Oct 2026

218 distinct organisations in all. 7 both pay and commit · 34 customers sit in the Communities · 6 do all three: pay, build, govern.

Not a tech monoculture: **22 industries (medical devices, automotive, payments, utilities); 26 customers report revenue above $10B; together those reporting headcount employ ~5.0 million people** (customer records, aggregates only).

The perception is altruistic individuals. The measurable reality is this slide. And when it breaks, it breaks for all of them on the same day.

Sources: customer records (aggregate counts) · status.openssl.org · OpenSSL Communities membership (Oct 2026)

OPENSSL

OpenSSL CONFERENCE

Companies without contracts still invest: upstream in commits, or in-house in hiring

IN PUBLIC: OUR COMMIT LOG

28 outside organisations committed, 2024 to 2026.
7 hold support contracts. 21 do not.
Their engineering time lands on the upstream branch.
The 2014 pattern, as one vendor told NPR: we don't donate money, but our employees help with the code.

Source: status.openssl.org × customer records

IN PRIVATE: THE JOB BOARDS

LinkedIn: 300+ open roles require OpenSSL (count stopped at 300, 9 Oct 2026).
ZipRecruiter: 212. Dice: 41. Separate boards; never summed.
Every ad is a salary for working WITH OpenSSL inside one company.

Source: logged-in and public searches, 9 Oct 2026; floors

The commit log is companies already paying with engineers upstream. The job-board spend is real too, and it stays inside one company.

Sources: status.openssl.org cross-checked with customer records · LinkedIn, ZipRecruiter, Dice (9 Oct 2026) · NPR (2014)

Two popular answers that do not sustain the project

ANSWER 1: ASSUME SOMEONE MAINTAINS IT

Outside signals mislead: 46% of flagged Java repos were not actually end-of-life.
11 of 23 pieces of core software infrastructure run on one or two regular maintainers, among them zlib, sudo, bash and the time-zone database.
xz is where the assumption ends.

Sources: Lange (SAP), 6 Oct 2026 · sheets.works (Oct 2026)

ANSWER 2: HIRE YOUR OWN EXPERTS

Companies already do: 300+ open LinkedIn roles.
Internal experts work downstream, on your builds.
They do not review upstream changes, cut releases, or stop the next incident before it ships to everyone.

Sources: LinkedIn hand count (9 Oct 2026) · status.openssl.org

upstream OpenSSL master branch → your internal builds and patches

work flows downstream; almost nothing flows back up

Internal expertise rides on the upstream master branch. Only money and upstream contribution keep that branch alive.

Sources: Lange (SAP SE, 6 Oct 2026) · sheets.works (Oct 2026) · LinkedIn (9 Oct 2026)

STEP 4 OF 7 · WHAT PAYING BUYS

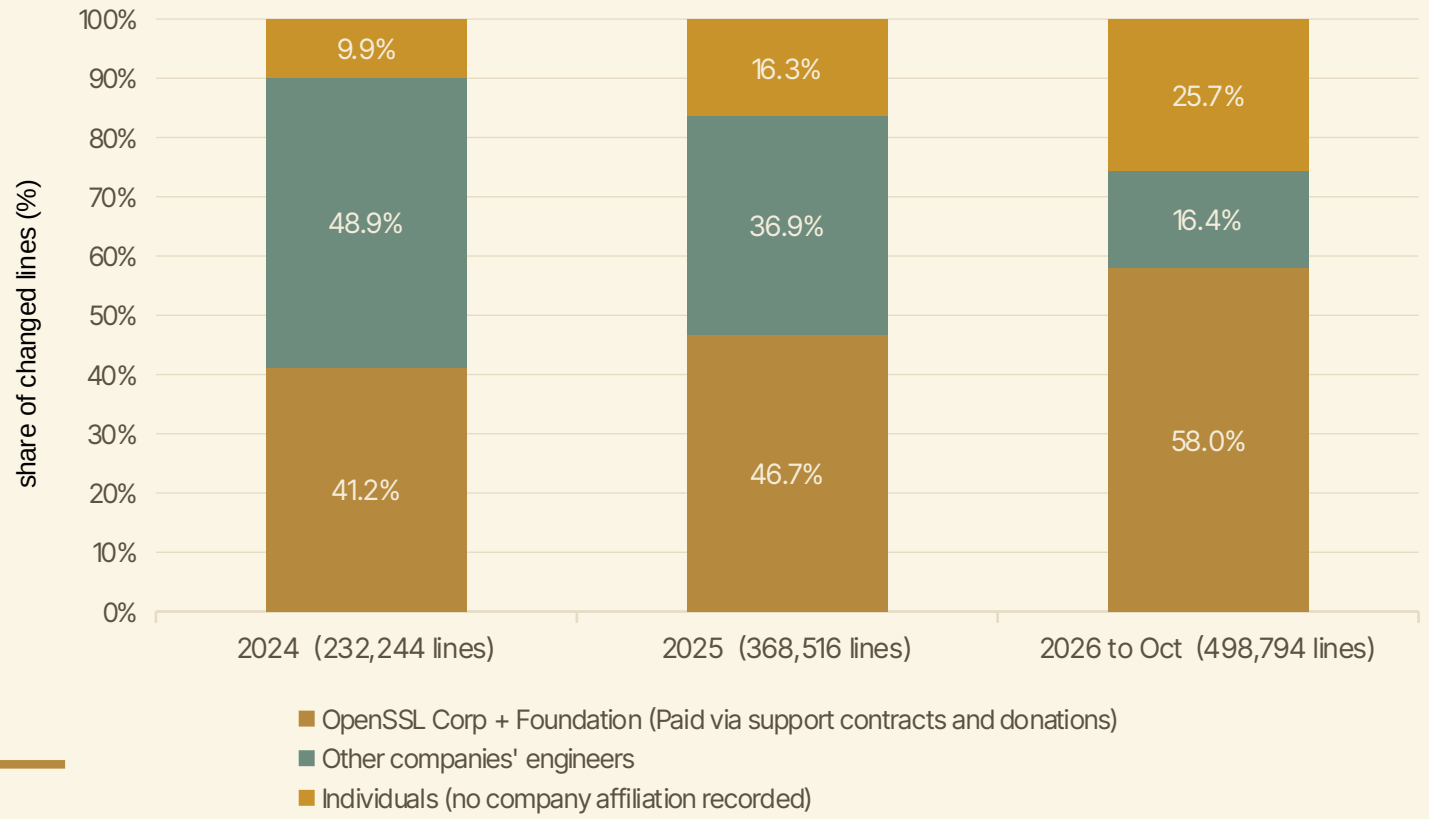
Does paying change anything?

Changed lines, reviews, key-person risk: status.openssl.org

OPENSSL

OpenSSL CONFERENCE

Four in five changed lines come from company-affiliated engineers



Company-affiliated total

90.1% · 83.7% · 74.3%

of changed lines in 2024, 2025, 2026; four in five across the three years

Individuals still matter, a tenth to a quarter of the volume. The point is not that volunteers vanished; it is that most of the work is done by paid engineers.

Buckets date from the 1 Mar 2024 restructuring; earlier years are not comparable and are not shown.

The abstract's claim, straight from the git history: this library is written overwhelmingly by paid engineers.

Source: status.openssl.org (built 2 Oct 2026); changed lines by contributor affiliation, as published; company attribution from the OpenSSL contributor directory. 2026 is a partial year.

OPENSSL

OpenSSL CONFERENCE

Writing is shared. Review is not

46.7%

of 2025's 368,516 changed lines were written by OpenSSL Corp + Foundation staff

status.openssl.org, 2025

98.5%

of recorded code reviews were carried by company-affiliated reviewers (10,404 of 10,561 Reviewed-by trailers, 2025; 97.7% so far in 2026)

status.openssl.org, Reviewed-by trailers

Review is the expensive, expert, unglamorous half of maintenance. Every change needs two reviewers; that rule is Heartbleed's legacy.

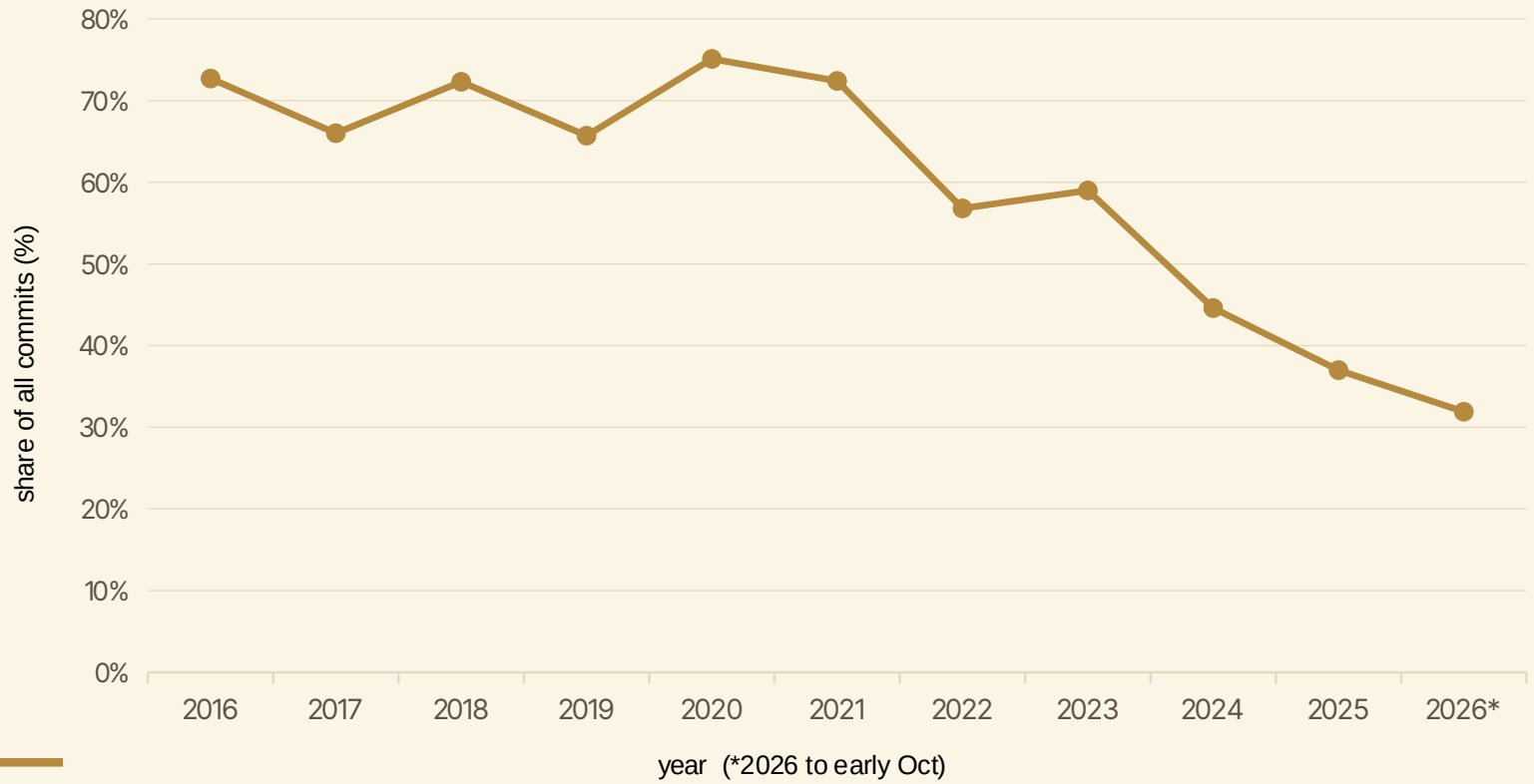
Volunteers write code. Almost nobody volunteers to review other people's code at scale.

Source: status.openssl.org (built 2 Oct 2026). Reviewed-by trailers are an OpenSSL convention; review shares are not compared across projects.

OPENSSL

OpenSSL CONFERENCE

The funded decade cut key-person risk in half



2016

5 people = 73%

of all commits

2026

5 people = 32%

of all commits, with more total output

Paying maintainers did not crowd volunteers out; it spread the work across more people. Key-person risk is a funding question, not a culture question.

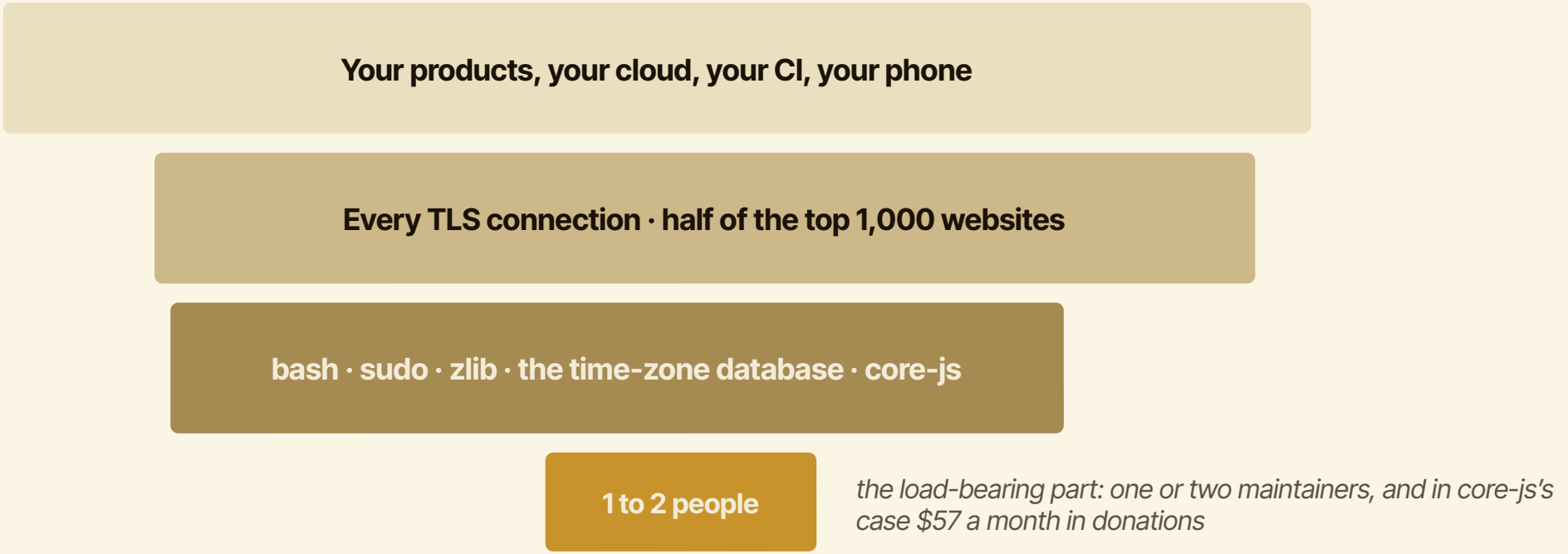
Source: status.openssl.org, yearly top-contributor tables (built 2 Oct 2026)

STEP 5 OF 7 · BEYOND OPENSSL

Is this just an OpenSSL story?

A 23-project census, the Linux kernel, and how enterprises detect abandonment

Billions of devices still rest on one or two unpaid people



the load-bearing part: one or two maintainers, and in core-js's case $57 a month in donations

Block sizes illustrative. The counts are real: 11 of 23 widely-deployed projects in last year's commit histories were maintained by one or two regular contributors.

Source: sheets.works, The people holding up the internet (Oct 2026); commit histories of 23 projects, Oct 2025 to Oct 2026

Funded open source is professionals. Unfunded open source is one or two people

WHERE THE MONEY IS: THE LINUX KERNEL

85%+ of kernel 6.18 changesets: developers with an identified employer.
Top by changesets: Intel 10.4%, Google 7.9%, Red Hat 6.3%, AMD 5.0%.
Unknown affiliation ~14%, and unknown does not mean unpaid.

Source: LWN kernel 6.18 development statistics, Nov 2025

WHERE IT IS NOT: THE LOAD-BEARING LONG TAIL

11 of 23 pieces of core software infrastructure: one or two regular maintainers.
The time-zone database behind ~4B phones: two people.
SQLite: four people. core-js: half the top 1,000 sites, $57 a month.

Source: sheets.works census, Oct 2026 (regular = 10+ changes/yr)

Context: 98% of audited commercial codebases contain open source (Black Duck OSSRA 2026, 947 codebases). The dependence is corporate everywhere; the maintenance often is not.

OpenSSL in 2013 was the right column. Funding moved it to the left. That is the whole argument in one slide.

Sources: LWN (Nov 2025) · sheets.works, The people holding up the internet (Oct 2026) · OSSRA 2026

Enterprises build models to detect abandoned open source projects

When maintainers move on, there is no reliable signal to the outside world. Status flags exist but are rarely set; sometimes the maintainer no longer has the credentials to set them.

So the consumers guess, at scale: SAP built a statistical model to detect end-of-life repositories in its own dependency stack, presented in Prague one week before this talk.

What did not predict survival: popularity, contributor counts, commit counts.

~3 years

of commit silence (1,089 days): the heaviest-weighted end-of-life signal in SAP's model (weight 0.26)

SAP model, 92 to 95% precision on ~430 Java repos

46%

of Java repos flagged unmaintained by OpenSSF Scorecard were not actually end-of-life, by manual assessment

same study; the outside signal is that noisy

Popularity does not show whether a project is alive. Paid maintainers who stay are the only signal a project controls.

Source: F. Lange (SAP SE), When Maintainers Move On, OpenSSF Community Day Europe, Prague, 6 Oct 2026

OpenSSL CONFERENCE

STEP 6 OF 7 · AI RAISES THE PRICE

What does AI change?

More submissions for the same reviewers, funded or not

AI made contributing cheap. Expert review stayed expensive

+5.9%

project code contributions after Copilot adoption

Song, Agarwal & Wen (GitHub data)

+8%

coordination time in the same projects

Song, Agarwal & Wen

+6.5%

more code reviewed by core developers after adoption

Xu et al. (2026)

−19%

core developers' own original-code output after adoption

Xu et al. (2026)

Two independent studies of GitHub Copilot in open source, same direction: **volume rises at the edges, and the cost lands on the experts in the middle, as review.**

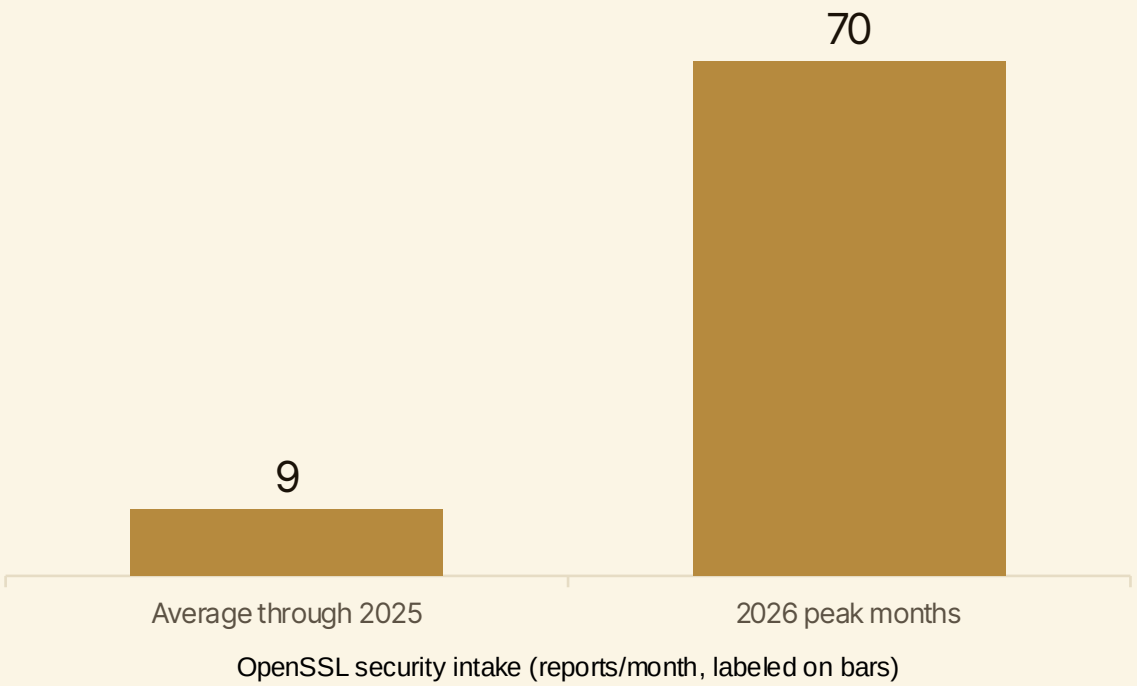
In OpenSSL's case, the core developers absorbing that review are the engineers the support contracts pay.

Sources: arXiv 2410.02091 (Song, Agarwal & Wen) · arXiv 2510.10165 (Xu et al.); full citations in the appendix

OPENSSL

OpenSSL CONFERENCE

Our security intake went from 9 to 70 reports a month



OpenSSL security intake (reports/month, labeled on bars)

400+

vulnerability reports received in the past 12 months

M. Caswell, Infosecurity Magazine, 2 Oct 2026

43

became published CVEs, roughly 1 in 10. The other 9 in 10 still consumed senior-expert time to disprove

same source

Filing a report is now nearly free. Assessing one is not. We absorb this with paid staff; unfunded projects face the same flood with nobody paid at all.

Source: Matt Caswell, OpenSSL Executive Director, Infosecurity Magazine (2 Oct 2026)

OpenSSL CONFERENCE

2014

One under-reviewed patch exposed a sixth of the web's secure servers. The fix: two expert reviewers on every change.

2026

AI multiplies the reports and patches those same reviewers must now assess.

Review is the product. The question was never whether open source code is free.
It is who pays the reviewers.

STEP 7 OF 7 · WHAT YOU CAN DO

What do you do with this?

Three options, all measured in this deck

Three ways organisations can pay for the review they rely on

(the part where I am the slide)

1

Buy the support you already rely on

Support contracts are 100% of what funds the dedicated engineering and review. ~100 customers carry it today; renewal runs 86 to 88%.

Source: Annual Reports 2024 to 25

2

Fund the commons directly

The Foundation channels sponsorships and public-interest money into the non-commercial side. Germany's Sovereign Tech Agency committed EUR 405,888 for 2025 to 26.

Source: sovereign.tech, public record

3

Put your engineers upstream

Oracle, Red Hat, Intel, IBM and others author real commits every year. In the 3.5 release, over half of substantive changes came from companies beyond our entities.

Source: status.openssl.org · release notes

None of these is charity. Each is cheaper than the alternative. Ask anyone who has maintained a private fork through three CVE cycles.

Sources: OpenSSL Corporation Annual Reports 2024 to 2025 · sovereign.tech · M. Caswell, Infosecurity Magazine (Oct 2026)

OpenSSL CONFERENCE

Open source is not free.

It is paid for by whoever shows up.

Kajal Sapkota · kajal@openssl.org · kajalsapkota.com

Data: status.openssl.org · openssl-forks-stats.pages.dev · openssl-corporation.org · full source list in the appendix

APPENDIX

Methodology and reserve slides

The 2014 answer: pool money, pay people, review everything

OpenSSL CONFERENCE

12 × $300k

Core Infrastructure Initiative founders: Amazon, Cisco, Google, IBM, Microsoft …

2

full-time OpenSSL developers funded for the first time

1st

complete security audit, by the Open Crypto Audit Project

2

reviewers now required on every change, the rule Heartbleed wrote

2013

$2k / yr

donations; one de-facto full-timer; volunteers carry everything

→

2014–2017

CII grants

pooled corporate money: two paid developers, first audit, review rule

→

2025

$5M / yr

support contracts only, zero donations, 21 staff, renewal 86%

"Public infrastructure without a tax base", Ed Felten's diagnosis that April. **Grants were the bridge. Support contracts became the tax base.**

Sources: CBC · Threatpost · Linux Foundation (2014) · Annual Reports 2024-25

Reserve: Two thirds of the web ran on software almost nobody watched or funded

USED BY EVERYONE

About two thirds of websites terminated TLS through OpenSSL. It shipped inside Android, routers, firewalls, clouds, and payment systems, mostly without anyone knowing it was there.

WATCHED BY ALMOST NO ONE

One de-facto full-time maintainer. About $2,000 a year in donations. No complete security audit in the project's history to that point.

KNOWN TO ALMOST NO ONE

The 2014 bug got a name, a logo, and a news cycle before most of the world had heard the maintainers' names. The internet met OpenSSL by watching it break.

Everyone used it free and expected it to always work. Everyone needs to eat; one unpaid person cannot carry this.

Sources: NPR, Apr 2014 · S. Marquess, Apr 2014

Reserve: April 2014: one missed review, and everyone patched at once

~17%

of the internet's trusted secure web servers exposed by Heartbleed

Netcraft estimate, Apr 2014

2+ years

the bug sat in production releases before discovery

shipped in OpenSSL 1.0.1, Mar 2012; disclosed Apr 2014

1

external contribution introduced it, merged after cursory review

project history

1

person worked on OpenSSL without other full-time employment

S. Marquess, Apr 2014

0

complete security audits in the project's history, to that point

S. Marquess, Apr 2014

First victims within days: 900 taxpayer SINs (Canada Revenue Agency), Mumsnet sessions. The failure was not cryptography. It was unfunded review.

Sources: Marquess (2014) · NPR · NBC News (Apr 2014) · Forbes Australia (2026)

Who the hundred are

OpenSSL CONFERENCE

>85%

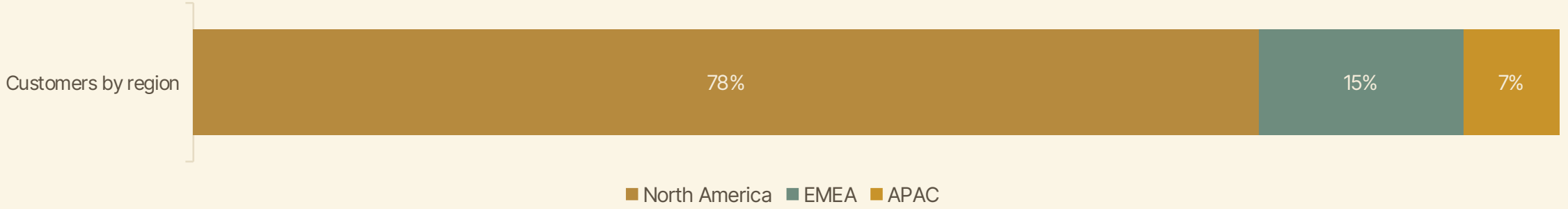
of customers are large businesses

>10%

have a market capitalisation above $100B

100%

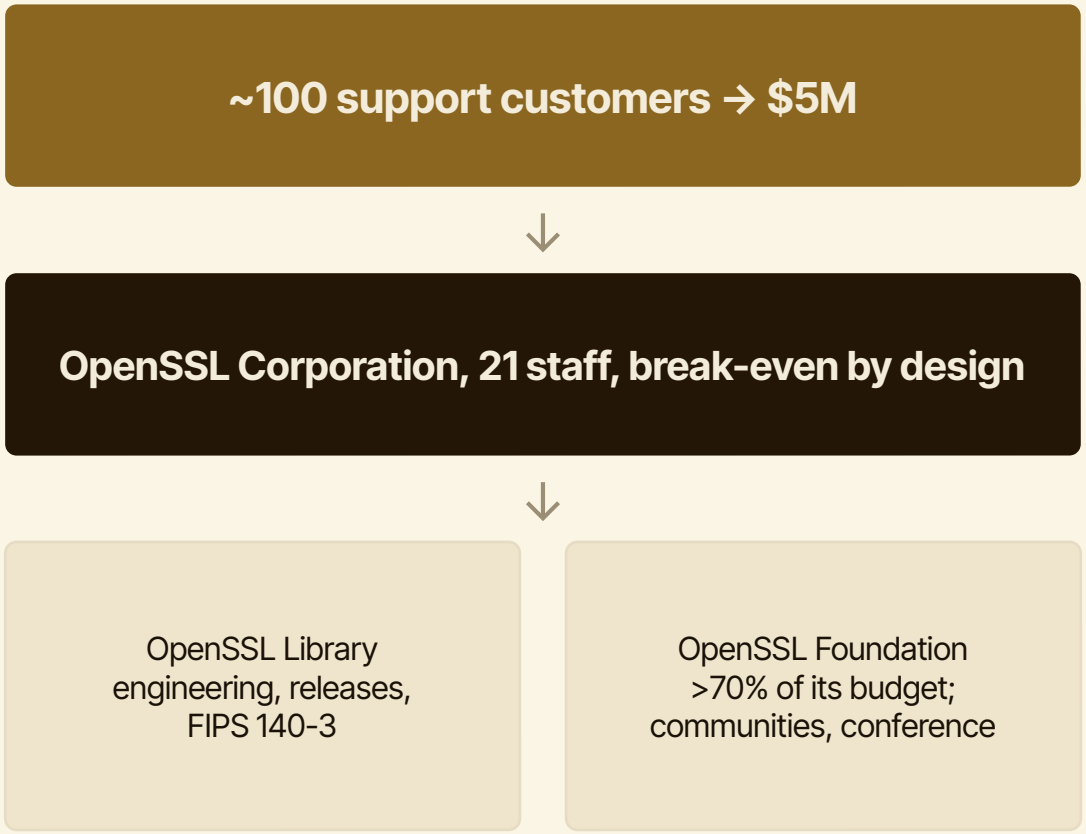
of 2025 revenue was support contracts, no donations, no sponsorships



The payers are giants. So are most of the non-payers.

Source: Annual Reports 2024–25

Where the money goes



What the $5M bought in 2025

- Releases 3.5 and 3.6: server-side QUIC; ML-KEM, ML-DSA, SLH-DSA post-quantum support
- FIPS 140-3: 3.1.2 validated; 3.5 submitted
- 4.0 in development, first major release in five years
- OpenSSL Conference: 400+ attendees from 30+ countries
- Jostle project funded; CI donated to cryptsetup; cryptlib and Bouncy Castle partnerships

“We cooperate by choice, not by force.”, Tim Hudson

Sources: Annual Report 2025 · Forbes Australia

Seven related libraries, seven funding models

OpenSSL CONFERENCE

Project	Funding model	Top funder share, 2025 commits	Top-5 contributor share
OpenSSL	Support contracts fund dedicated staff	50% (Corp + Foundation)	37%
BoringSSL	Single vendor (Google)	97%	87%
AWS-LC	Single vendor (Amazon)	96%	67%
wolfSSL	Commercial dual-licence vendor	92%	50%
Mbed TLS	Corporate steward (Arm + Linaro)	72% + 13%	71%
Bouncy Castle (Java)	Charity + commercial partner	60% + 34%	97%
LibreSSL (portable)	Volunteers + donations	100% individuals	95%
quictls	Community fork, wound down	82% of 211 commits	97%

Sources: status.openssl.org · openssl-forks-stats.pages.dev · LibreSSL = portable packaging repo only

2026: bug-bounty programs cut off submissions

OpenSSL CONFERENCE

22 Jan — **curl ends its six-year bug bounty** $86k paid for 78 valid vulnerabilities; by mid-2025 only ~5% of submissions were genuine

May — **Microsoft MSRC warns the industry** AI will raise the "pace and breadth of vulnerability discovery"

Sep — **Intel removes bug-bounty rewards** from its Intigriti program

5 Oct — **Google suspends its open source bounty intake** "a significant rise in automated submissions, the vast majority of which are not valid"

Also this year: RubyGems reports a tenfold surge; Homebrew bot-closes obviously AI-generated PRs. Measured across 294 repos and 2M+ PRs, volume rose while merge rates fell ("AI slop is DDoSing open source"). The common defences refuse submissions; the alternative is paying the people who review them.

Sources: BleepingComputer (5 Oct) · LiveWyer · LeadDev · arXiv 2607.04003 (appendix)

Reserve: the productivity story is less settled than it sounds

OpenSSL CONFERENCE

Measured: experienced maintainers

19% slower

with early-2025 AI tools on real issues in their own large repos, while believing afterwards they had been 20% faster. Randomized trial: 16 veteran maintainers, 246 tasks.

Measured: review tooling

4 days faster

average PR closure when AI drafts the PR summary for reviewers, across 200,000+ pull requests. AI pointed AT the review bottleneck helps; AI firehosed INTO it does not.

Sources: METR randomized controlled trial (Jul 2025; early-2025 tools, METR has since published updated data); Nattamai Kannan & Ramasubbu, SSRN 5106441 (2025)

Reserve: the sustainability trap, in full

OpenSSL CONFERENCE

294

repositories, 2M+ pull requests and issues analysed

↑ / ↓

PR volume rose through 2025 while merge rates fell

−18%

merge rate for one-time contributors vs the counterfactual

“AI slop is DDoSing open source” , and the common defences (refuse submissions, ban first-time contributors, auto-reject) protect this quarter's review capacity by giving up what makes open source open. The authors call it a sustainability trap.

The alternative to refusing submissions is paying the people who review them.

Source: Afroz, Miller, Menezes, Gilmour, Sarma & Feng, arXiv:2607.04003 (Jul 2026); 229-practitioner survey

Reserve: other project types, same pattern

OpenSSL CONFERENCE

- Linux kernel 6.18 (Nov 2025): 85%+ of changesets came from developers with an identified employer; Intel, Google, Red Hat and AMD top the table (LWN development statistics).
- Commit-history census of 23 load-bearing projects (sheets.works, Oct 2026): 11 are maintained by one or two regular contributors, including the time-zone database (~4B devices), zlib, sudo and bash. SQLite: four people, an estimated trillion-plus databases.
- core-js ships in roughly half of the top 1,000 websites; its maintainer reported $57 a month in donations (same census).
- bash: the line behind Shellshock entered in 1989 and was reported in 2014, a 25-year gap. Our Heartbleed sat 2+ years. Unwatched code ages the same way everywhere.
- Where public money now flows, it follows visible dependence: Sovereign Tech Agency commitments include log4j €596k, FFmpeg €438k, OpenSSL Foundation €405,888 (2025–26), OpenSSH €200k, curl €195k (sovereign.tech).
- The same census counts OpenSSL as the counter-example: 6 regular contributors in 2013, 32 in 2026, the funded decade (their definition: 10+ changes/year; our own ledger is status.openssl.org).

Universal dependence, handful-of-people maintenance, funding only where the dependence became visible.

Sources: LWN kernel 6.18 statistics (Nov 2025); sheets.works, “The people holding up the internet” (Oct 2026); sovereign.tech funding records

Context: enterprises run their AI on open source

OpenSSL CONFERENCE

94%

of organisations have adopted AI (Linux Foundation, 2025)

89%

of AI adopters build on open source in their AI infrastructure

$8.8T

demand-side value of open source software (Harvard research)

66%

of organisations run AI workloads on Kubernetes (CNCF, 2026)

3.5×

what firms would spend on software without open source

“strain”

CNCF's word for what machine-driven usage puts on open source systems

Sources: Linux Foundation, Economic & Workforce Impacts of Open Source AI (May 2025); CNCF 2025 Annual Survey (Jan 2026)

OpenSSL Communities: where users and payers organise

OpenSSL CONFERENCE

- Ten communities, 401 unique members: Large Businesses (144), Small Businesses (66), Distributions (45), Academics (43), Committers (35), Individuals (159), two advisory committees, General Discussion.
- 130 organisations identifiable across the communities, from Oracle, Red Hat, IBM, Intel and Cisco to PQShield, Chainguard and university groups on four continents.
- Business and Technical Advisory Committees give commercial users and technical leaders a formal voice in priorities and releases.
- Partner projects at this conference: Bouncy Castle, cryptlib, Jostle.

Governance that gives payers a voice is part of what makes paying rational.

Source: OpenSSL Communities platform membership data (Oct 2026); Annual Report 2025

Methodology and metric definitions

OpenSSL CONFERENCE

- Contributor data: status.openssl.org and openssl-forks-stats.pages.dev (both built 2 Oct 2026). Non-trivial commits by authored date, all branches; CLA-trivial commits, bots, imported/generated history excluded. Company attribution: OpenSSL contributor directory; corporate email domains plus curated lists for other projects.
- Review counts use Reviewed-by commit trailers, an OpenSSL convention; review metrics are not compared across projects.
- Affiliation buckets date from the 1 Mar 2024 restructuring; Individuals-vs-Companies trends are not charted across that boundary. 2026 figures are partial (to early Oct).
- Affiliation shares on the what-paying-buys slides use changed lines as published by status.openssl.org; the key-person chart uses commit counts, since per-person line totals are not published there. Share figures use ALL commits or lines as the denominator. The Annual Report's "two thirds of project-funded contributions" uses the funded subset, both are correct, with different denominators.
- Fork histories carry inherited upstream commits (AWS-LC ≤ 2019 = BoringSSL; quictls ≤ 2020 = OpenSSL); LibreSSL figures cover the portable packaging repo only.
- Job-posting counts (9 Oct 2026): LinkedIn 300+ open roles requiring OpenSSL (logged-in hand count, stopped at 300); ZipRecruiter 212 and Dice 41 (US), logged-out keyword searches. Point-in-time floors; boards overlap, so the counts are not summed; ads name OpenSSL only when the skill is essential.
- Financial and customer figures: OpenSSL Corporation Annual Reports 2024 and 2025 (public).

AI evidence: the full citations

OpenSSL CONFERENCE

- Xu, Medappa, Tunc, Vroegindeweij & Fransoo (arXiv:2510.10165, 2026): core devs +6.5% review, −19% own output after Copilot; gains to peripheral contributors; rework rises.
- Song, Agarwal & Wen (arXiv:2410.02091, GitHub data): contributions +5.9%, participation +3.4%, coordination +8%; timely merging still improved.
- Afroz et al., "AI Slop is DDoSing Open Source" (arXiv:2607.04003, 2026): 294 repos, 2M+ PRs/issues; volume up, merge rates down; one-time contributors −18.18% vs counterfactual.
- METR RCT (Jul 2025): 16 experienced maintainers, 246 tasks, 19% slower with early-2025 tools vs 20% believed speedup; METR published updated late-2025 data in Feb 2026.
- Nattamai Kannan & Ramasubbu (SSRN 5106441): Copilot-for-PR summaries, 200k+ PRs, ≈4 days latency via fewer required reviewers.
- ACM Technology Policy Council (Sep 2026, Garfinkel, Dykstra et al.): human assessment remains the bottleneck regardless of model quality.
- M. Caswell, Infosecurity Magazine (2 Oct 2026): OpenSSL intake 9 → up to 70 reports/month; 400+ reports, 43 CVEs in 12 months.

Full citations: data and press sources

OpenSSL CONFERENCE

- Primary data: status.openssl.org and openssl-forks-stats.pages.dev (both built 2 Oct 2026); OpenSSL Corporation Annual Reports 2024 and 2025 (openssl-corporation.org); OpenSSL Communities membership titles (Oct 2026); OpenSSL Corporation customer records (Oct 2026, aggregate counts only).
- Heartbleed era: S. Marquess, “Of Money, Responsibility, and Pride”, veridicalsystems.com (12 Apr 2014); NPR, “Who Should Pay To Keep The Internet's Locks Secure?” (Apr 2014); NBC News (Apr 2014); CBC (Apr 2014); Threatpost (May 2014); Linux Foundation CII announcements (2014).
- 2026 press and profiles: M. Caswell, Infosecurity Magazine (2 Oct 2026); Forbes Australia (21 Aug 2026); Authority Magazine (27 Aug 2026); BleepingComputer (5 Oct 2026); LiveWyer (Feb 2026); LeadDev (Feb 2026).
- Industry studies: Black Duck OSSRA 2026 (947 codebases); F. Lange (SAP SE), “When Maintainers Move On”, OpenSSF Community Day Europe, Prague (6 Oct 2026); LWN, kernel 6.18 development statistics (Nov 2025); sheets.works, “The people holding up the internet” (Oct 2026); Sovereign Tech Agency funding records (sovereign.tech).
- Job-posting counts: LinkedIn (logged-in hand count, stopped at 300), ZipRecruiter, Dice; all 9 Oct 2026.
- AI studies: full citations on the previous slide.