WSO2CON 2024

Does Open Source Still Matter?



Jonathan Marsh
VP Strategy, WSO2
9 May 2024

Yes!

But … let’s look deeper at the current environment

- Challenges addressed by Open Source
- WSO2’s Open Source policies
- New challenges to Open Source itself
- The future of Open Source

Challenges addressed by Open Source

Better software

- Transparency improves software development practices
  - More eyes on the code
  - Contributes back to human knowledge (human and AI training)
  - Wider set of constituents
  - Wider set of contributors
  - Open marketplace of ideas
  - Rewrote how software is written with decentralized tools and governance methods
- Reduced duplicative efforts
  - Freely build on best-of-breed components
  - Allow technical consensus to coalesce around best software
- Attracts geekiest developers

Cost & equity

- Software is necessary for modern societies
- Traditional software vendors may impose undesirable terms:
  - Unaffordable
  - No control over evolution, maintenance
  - Controlled by private entities
  - Controlled by foreign entities
- Open Source provides legal path to obtaining low-TCO software
- Maintains market pressure on proprietary software vendors

Software independence

- Open Source broke open the problem of “vendor lock-in:”
  - High prices
  - Unresponsive to evolution needs
  - Opaque quality & “abusive relationships”
  - Product lifecycle pressure (early EOLs)

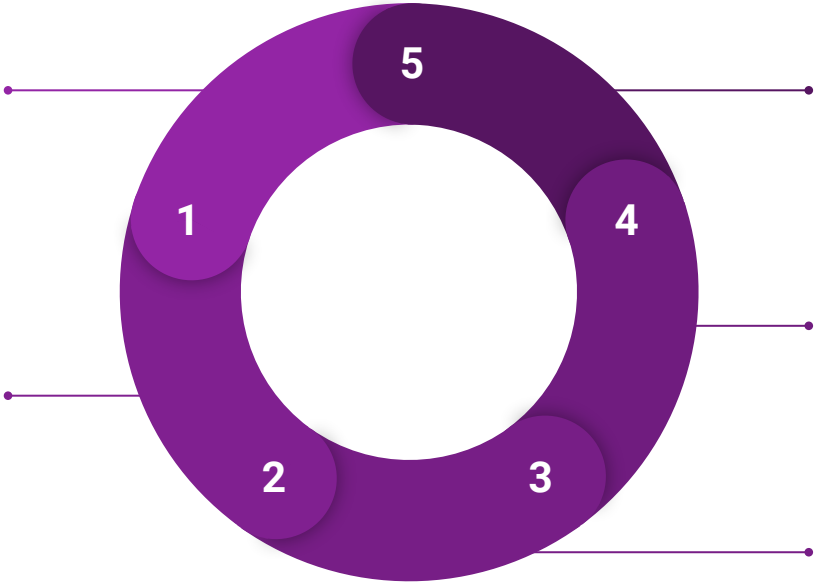
- Now governments are emerging as a more significant source of uncertainty
  - Data privacy and other software regulations
  - Trade restrictions
  - International sanctions
  - Snooping by “law enforcement”

WSO2's Open Source Policies

WSO2's extraordinary Open Source commitment

All downloadable products
SaaS offerings may differ

All enterprise features
No dual licensing



Critical security updates
On latest release only

Open process
Apache Way governance model

Permissive license
Apache 2.0

Why does WSO2 prefer Open Source?

- Ideological decision deeply embedded in company history and culture
- Increased employee equity
  - Establish personal reputation
  - Access to code after leaving the company
  - Exposure to a global community (contributors, users/customers)
  - Supports development of software talent beyond Silicon Valley-like hot spots
- Secures unique business advantages
  - Replaces expensive marketing with viral/word-of-mouth awareness
  - Benefits from open-source preferences (individual, institutional, regulatory)
  - Expectation of high value/low cost

WSO2's business model

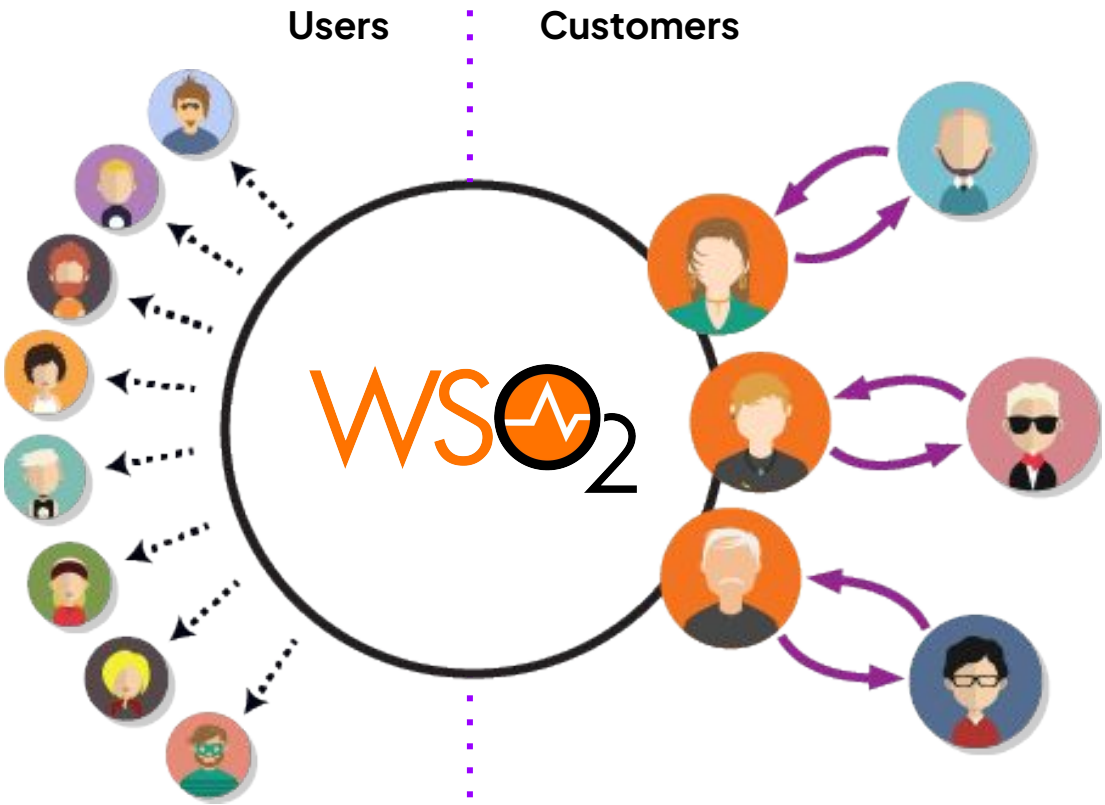


Image by Freepik

WSO2's business model

Users

- Community releases
- Regular releases with new features & bug fixes
- Critical security updates (only) on latest release (only)
- Community support (public, best efforts)
- DIY & community expertise



Customers

- Supported distributions & SaaS products
- Continuous updates on 3+ years of supported releases
- Security bulletins & updates, updates to supported releases
- Enterprise support (private, SLA)
- WSO2 expertise

Challenges to Open Source

Maintaining security in a decentralized system

The #XZ story:

- A compression library central to the linux stack was maintained by an overworked volunteer
- Nation-state hackers posed as open source developers to gain commit rights and assume effective control over the component
- After a year of productive participation the new committers inserted a very significant back door
- An alert developer/consumer at Microsoft identified degraded performance, located and reported the problem
- Worries remain that a loose system of decentralized volunteers is open to manipulation

See https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/

SaaS

- Strong trend towards SaaS for the last decade or more
  - Ease of trial
  - Low entry cost
  - Low maintenance effort
- On-premises still continues to grow
  - “Reshoring” SaaS to save money
  - Cloud native characteristics now more readily available on-prem (Kubernetes)
  - Competing regulatory regimes leading to a fragmented global market

Mega-cloud competition

- Smaller companies can face existential competition from Amazon etc. should they decide to offer a SaaS version of a popular open source product.

- Vendors moving towards “source-available” licenses to provide most of the full benefits of open source to MOST users, while precluding “predatory” use.
    - MongoDB, MariaDB, Cockroach Labs, Couchbase, Redis, Hashicorp, Elastisearch

Investment expectations

- Open source companies have not proliferated
- Low uptake from traditional VC investors
  - No playbook for success
  - Difficult to make quick returns
  - Hard to defend/monetize proprietary IP
  - SaaS is more attractive
  - Dual-licensing (i.e. not truly open) at best
- Value of open sourcing is often indirect
  - Preempt competition
  - Boost reputation
  - Leverage community to lower long-term costs

Increasing regulation

- US Cyber Trust Mark Act
  - Safety certification allowing consumers to choose safer products
  - Certification performed by independent labs
  - Voluntary - open source projects can choose whether to apply
- European Cyber Resiliency Act
  - Product safety regulation - software vendors may be penalized for for insecure software and sub-standard security processes
  - Requires self- documentation of security practices, ongoing responsive measures (i.e. security patches)
  - Applies to all software vendors with business in Europe, with global spillover
  - Also applies to open source software sponsored by vendors with business in Europe

Gift horse or trojan horse?

- Increased costs of releasing software
  - Formalized risk assessments
  - Documenting releases
  - Achieving zero known vulnerability goals
- Increased costs of maintaining software
  - Making security updates available freely
  - Promptly report security vulnerabilities to authorities
  - Committing to a product lifetime
- Increased financial risk
  - Penalties reaching millions of euros



Who pays for conformance costs?

- Software vendors
  - Higher prices for commercial products to subsidize open source
  - Where the open source is ancillary to a commercial product sale (e.g., tools)
  - Where the open source is a precursor to a commercial product sale (e.g., dual license)
- Open source foundations
  - Established open source foundations can provide systems and support for conformance.
  - Foundations are usually funded with pooled corporate dues and donations
- Governments?

The Future of Open Source (my predictions)

Entering a time of push and pull

- Waning globalization and waxing geopolitical instability will drive demand for software independence
- SaaS may peak in some areas - “reshoring” underway
- Open source can avoid traditional marketing saturation failures, with word-of-mouth awareness





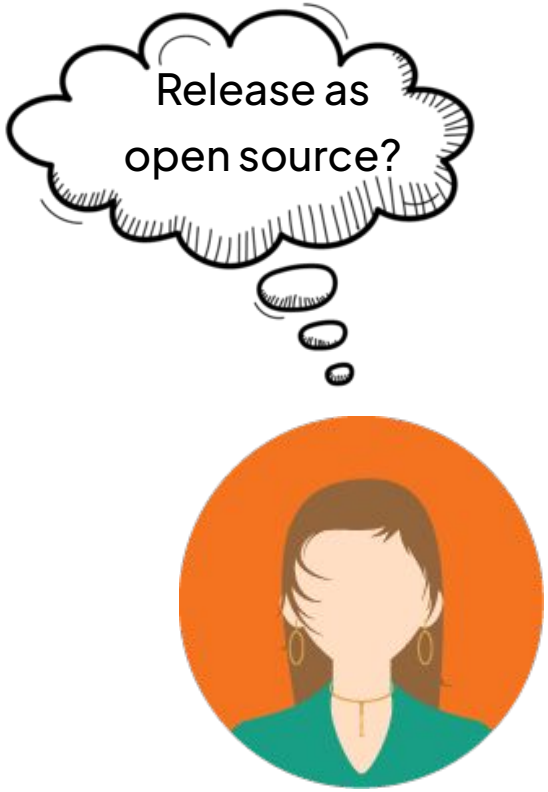
- Regulatory damage to “as-is” open sourcing
- Harder for companies to justify open sourcing in the face of increased obligations and liability
- Public funding is insufficient to fully support open source as a public good

Awareness of the need to treat open source as a public good

- OpenSSF (Open Source Security Foundation): defining and promoting repeatable security practices
  - https://openssf.org/

- Open Source Quality Institutes (OSQI): Tim Bray's idea for public funding for open source "commons" maintenance efforts
  - https://www.tbray.org/ongoing/When/202x/2024/04/01/OSQI

Developer quandary



- Fully conform, accept liability & maintenance obligations
- Don’t release at all
- Release as closed source/dual license
- Regional “open source” license variants
- Explore new revenue sources
- Minimize conformance costs

Less license purity

- Increased use of dual-licensing and source-available licenses (addresses the investment problem)
- Increased use of SaaS-prevention licenses (addresses the SaaS problem)
- Emergence of “as-is” licenses (addresses the un-funded mandate regulatory problem)



Return to Open Source Foundations (OSFs)

- OSFs will gain some special regulatory status
- Pools costs and mechanisms for satisfying regulatory requirements





Personal thoughts

- Open source will need your help!
- Be open to a diversity of open-source-adjacent licenses
  - Licenses that prevent direct competition by SaaS providers
  - “As-is” licenses
- Support open source as a public good
  - Support initiatives to provide public support
  - Expect more certification options
  - Recognize secure use of open source is a joint responsibility of developer and user
- Know your Open Source - examine the SBOM
- Expect somewhat less diversity and vigor in open source community
- Expect somewhat higher costs for commercial equivalents

Thank You!