ANACONDA.

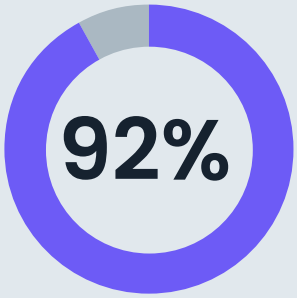
Govern Your Open-Source Pipeline with Anaconda

Open-source software (OSS) and its rich ecosystem have become essential to the modern technology stack. In 2023, most products and services fail to remain competitive without heavily depending on open-source components.

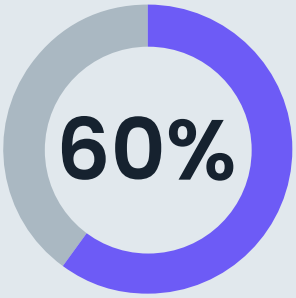
Even organizations in highly regulated industries are beginning to operate more like technology organizations. Increasingly, financial, healthcare, and government institutions are utilizing cutting-edge OSS to deliver differentiated and data-driven services.

OSS can introduce exploitable code and bugs even in the most fortified networks, however. Without comprehensive OSS protocols and policies in place, OSS vulnerability attacks can inadvertantly wreak havoc.

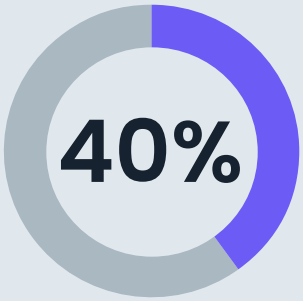
Anaconda offers OSS pipeline governance tools and best practices to help you and your organization stay one step ahead of the ever-changing cybersecurity landscape.



Applications containing OSS in 2022



Security teams miss critical alerts



Alerts lack actionable insights

↑ 650%

Increase in OSS cyberattacks in 2021

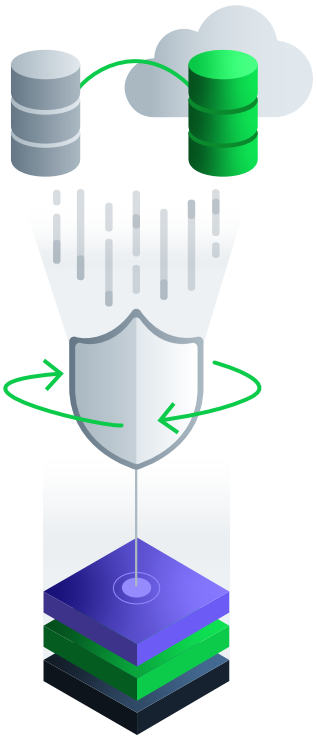
$1.4 million

Average ransomware remediation cost in 2022

Know where your software comes from.

Institutions need visibility into what packages, dependencies, and versions are being used across the organization. Open-source libraries can contain hundreds of artifacts and modules, and you simply cannot control what you don't know.

Distributing OSS from a centralized, trusted source is a top-down approach to reducing your overall attack surface. With access to Anaconda's trusted repository of over 8,000 privately built Python and R packages that feature SHA-256 encryption and verified dependency trees, Anaconda helps organizations mitigate and automate protection against the most common security attacks such as typosquatting, man in the middle, and dependency confusion.



Software Distribution

Trusted and public sources

Security Policy Filtering Engine

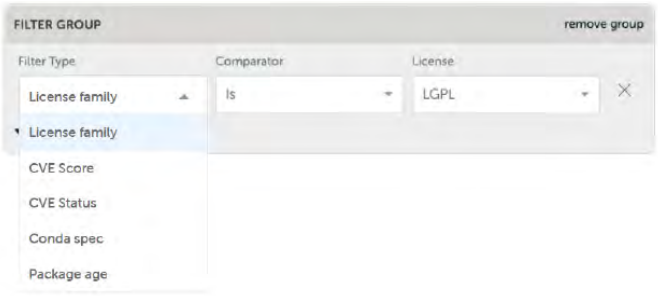
Filtered Channels

IT approved, developer ready

Be proactive, not reactive.

How much control does IT have over end-user OSS access across your networks? Just as knowing where your software comes from is important, so is knowing where it's being used and deployed.

Anaconda also enables institutions to govern OSS usage across their networks with a bottom-up approach. Pair tokenized access to Anaconda's trusted repository with an automated risk policy engine to proactively uncover—and block—unwanted security and licensing risks, whether deploying on premises or to the cloud.



Have an OSS remediation plan.

In addition to top-down and bottom-up approaches to securing your networks, institutions should also arm themselves against any unforeseen vulnerabilities with actionable information.

With Anaconda, security administrators can remediate vulnerabilities quickly with enriched, expertly curated package metadata. Enriched metadata can include vetted upper and lower impacted version bounds, impacted use cases and conditions, potential remediation tactics, and more.

CVE-2022-24288

Anaconda curated at: May 10, 2022

The "origin" parameter passed to some of the endpoints like '/trigger' was vulnerable to XSS exploit. This issue affects Apache Airflow versions <1.10.15 in 1.x series and affects 2.0.0 and 2.0.1 and 2.x series. This is the same as CVE-2020-13944 & CVE-2020-17515 but the implemented fix did not fix the issue completely. Update to Airflow 1.10.15 or 2.0.2. Please also update your Python version to the latest available PATCH releases of the installed MINOR versions, example update to Python 2.6.13 if you are on Python 2.6 (Those contain the fix for CVE-2021-23336 https://nvd.nist.gov/vuln/detail/CVE-2021-23336).

To learn more about Anaconda's governance, security, and compliance capabilities and to schedule a demo, visit anaconda.com/security-compliance.

With more than 35 million users, Anaconda is the world's most popular platform to develop and deploy secure Python solutions, faster. We pioneered the use of Python for data science, champion its vibrant community, and steward the open-source projects behind tomorrow's artificial intelligence (AI) and machine learning (ML) breakthroughs. Our solutions enable practitioners and institutions around the world to securely harness the power of open source for competitive advantage and groundbreaking discoveries. Visit anaconda.com to learn more.

ANACONDA.