The vast majority of today’s technology applications rely on open-source software (OSS), which can enhance innovation by leveraging the knowledge of the global OSS community. However, open source comes with cybersecurity vulnerabilities that bad actors are working to exploit. The vendor you choose for open-source security will determine the safety and outcomes of your applications built with OSS.

Here are the latest numbers on OSS usage, cyberthreats, data breaches, and vulnerabilities—and how Anaconda can help.

**Open-Source Security by the Numbers**

- **Python is the #1 most popular programming language, with 27% of global market share.**
- **96% of code bases contain open-source software.**
- **48% of code bases contain high-risk vulnerabilities.**
- **277 days (9 months) for security teams to identify and contain a breach.**
- **$9.4M is the average cost of a data breach in the United States.**
- **$1.4M is the average cost to remediate a ransomware attack.**
- **74% of data breaches are caused by human error, a common threat vector.**
- **25K common vulnerabilities and exposures (CVEs) were recorded in 2022.**
- **45% of software supply chains will be attacked by 2025.**
- **It takes an average of 30 mins to manually curate data for one CVE.**

Is your open-source pipeline secure?

Anaconda is your one-stop shop for trusted OSS packages. Leverage our expert-curated, up-to-date, policy-aware, open-source component software bills of materials (SBOMs), and enterprise-grade support to empower users and teams to securely innovate using open-source tools.