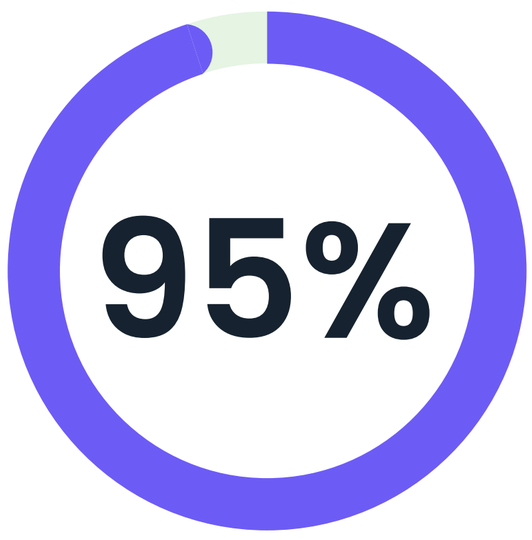
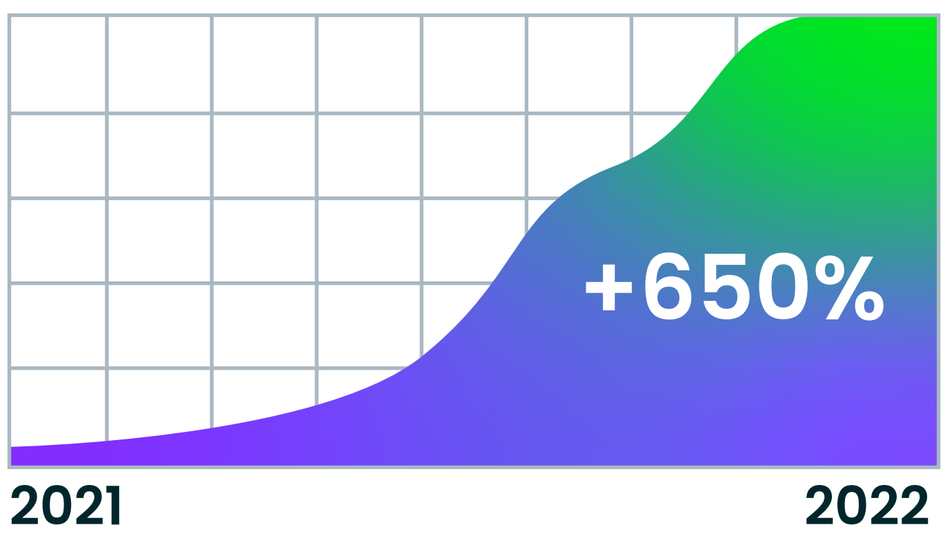
Open-Source Security by the Numbers

Cybersecurity attacks are on the rise. In our increasingly digital world, malicious actors have learned to take advantage of security flaws, also known as Common Vulnerabilities and Exposures (CVEs), to potentially put your organization's data at risk. Understanding the threat landscape is the first step to securing your open-source software pipeline.



of IT organizations rely on open-source software.

Source: The State of Enterprise Open Source



Cyberattacks aimed at open-source suppliers increased 650% last year.

Source: The State of Ransomware 2022

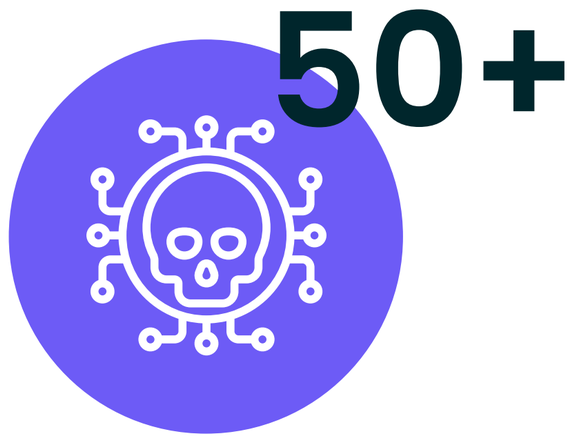
A single ransomware attack can cost over $1.4 million.

Source: The 2021 State of the Software Supply Chain Report

5.1

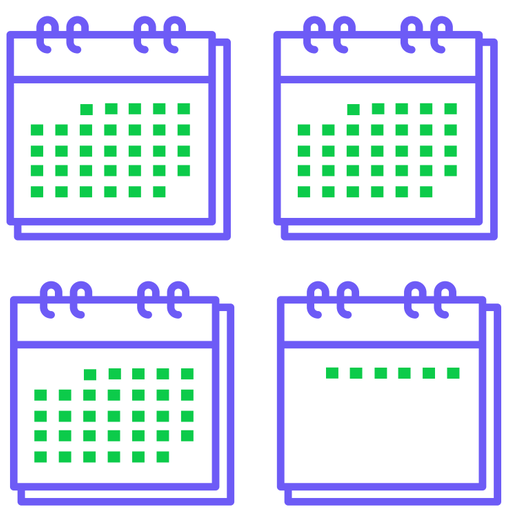
is the average number of outstanding, critical vulnerabilities in an application.

Source: Addressing Cybersecurity Challenges in Open Source Software



More than 50 CVEs are logged each day.

Source: Redscan analysis of NIST NVD reveals record number of vulnerabilities in 2021



The average amount of time to fix a vulnerability is 97.8 days.

Source: Addressing Cybersecurity Challenges in Open Source Software

More than half of organizations surveyed have no OSS security policy in place.

Source: Addressing Cybersecurity Challenges in Open Source Software

Is your open-source pipeline secure?

Anaconda is purpose-built to address open-source risk in your Python and R workflows. Contact us to learn how to secure your software supply chain today.

Contact Us >

ANACONDA.