sonatype

For Better Security, Stop Wasting Developer Time

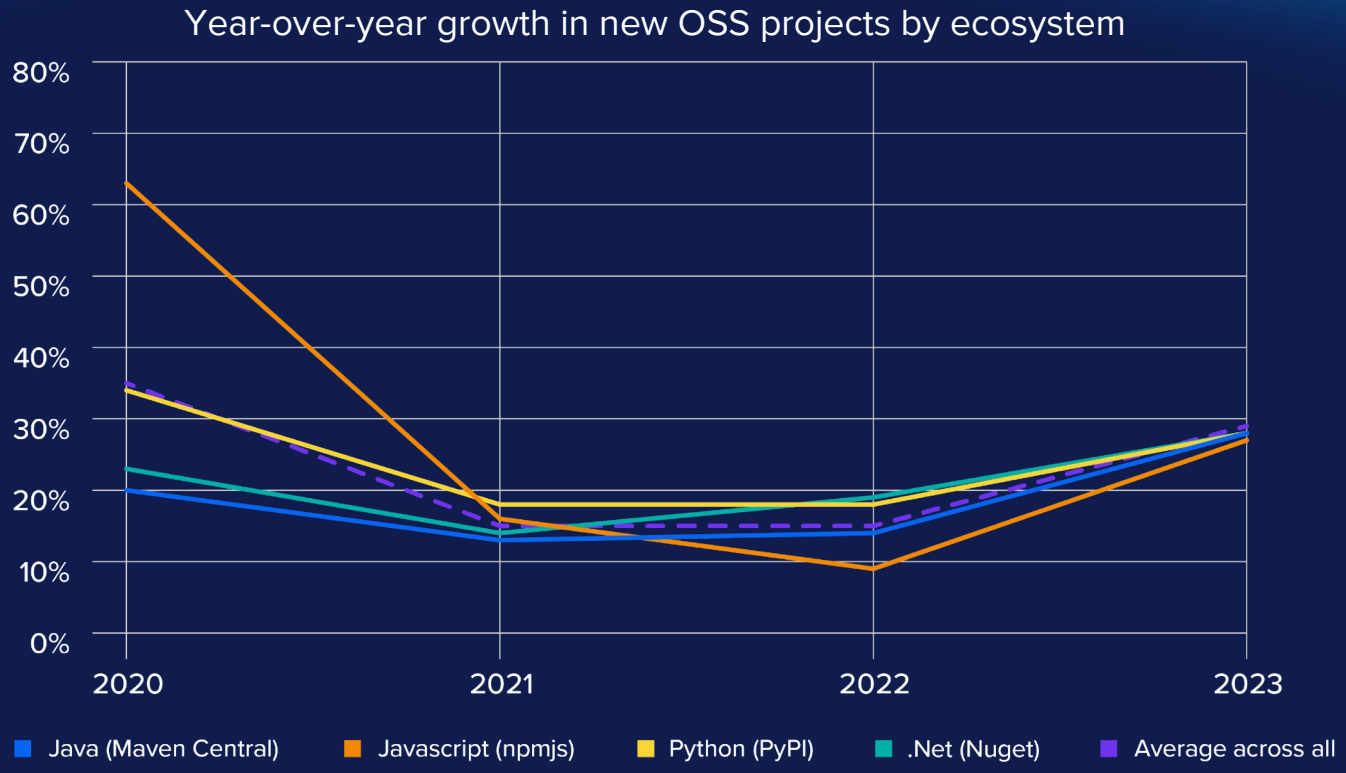
9th Annual State of the Software Supply Chain

Dr. Stephen Magill,
VP Product Innovation, Sonatype

2023: A Year of Innovation

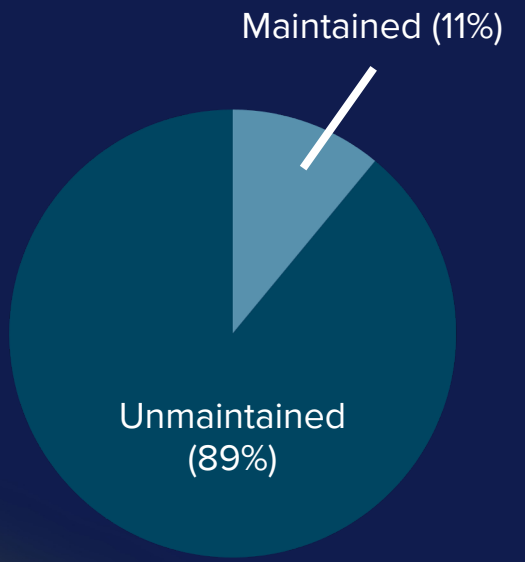
sonatype

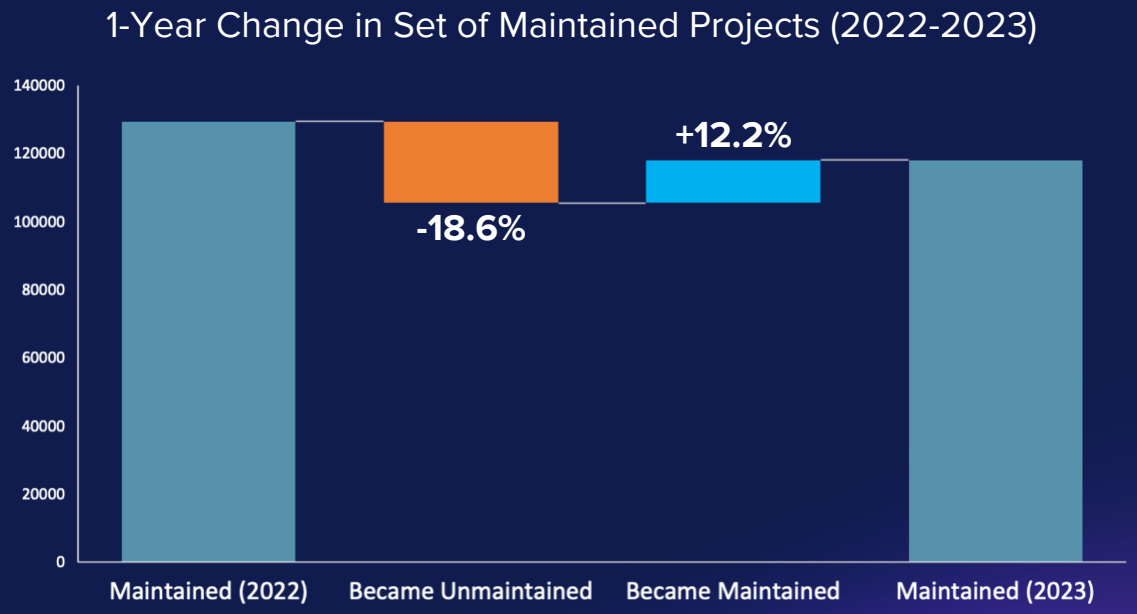
New OSS Project Growth Rate Is Recovering



sonatype

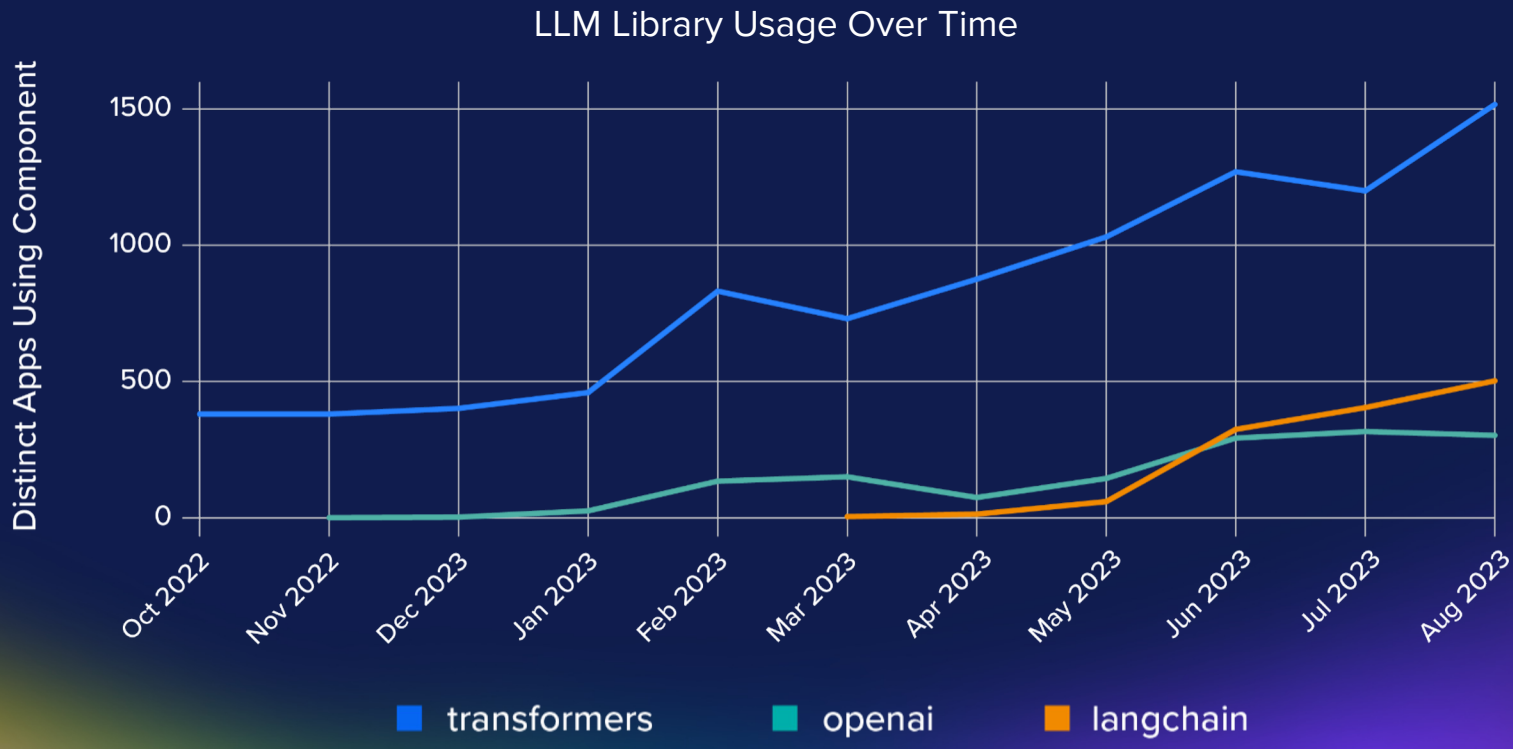
Maintained Projects





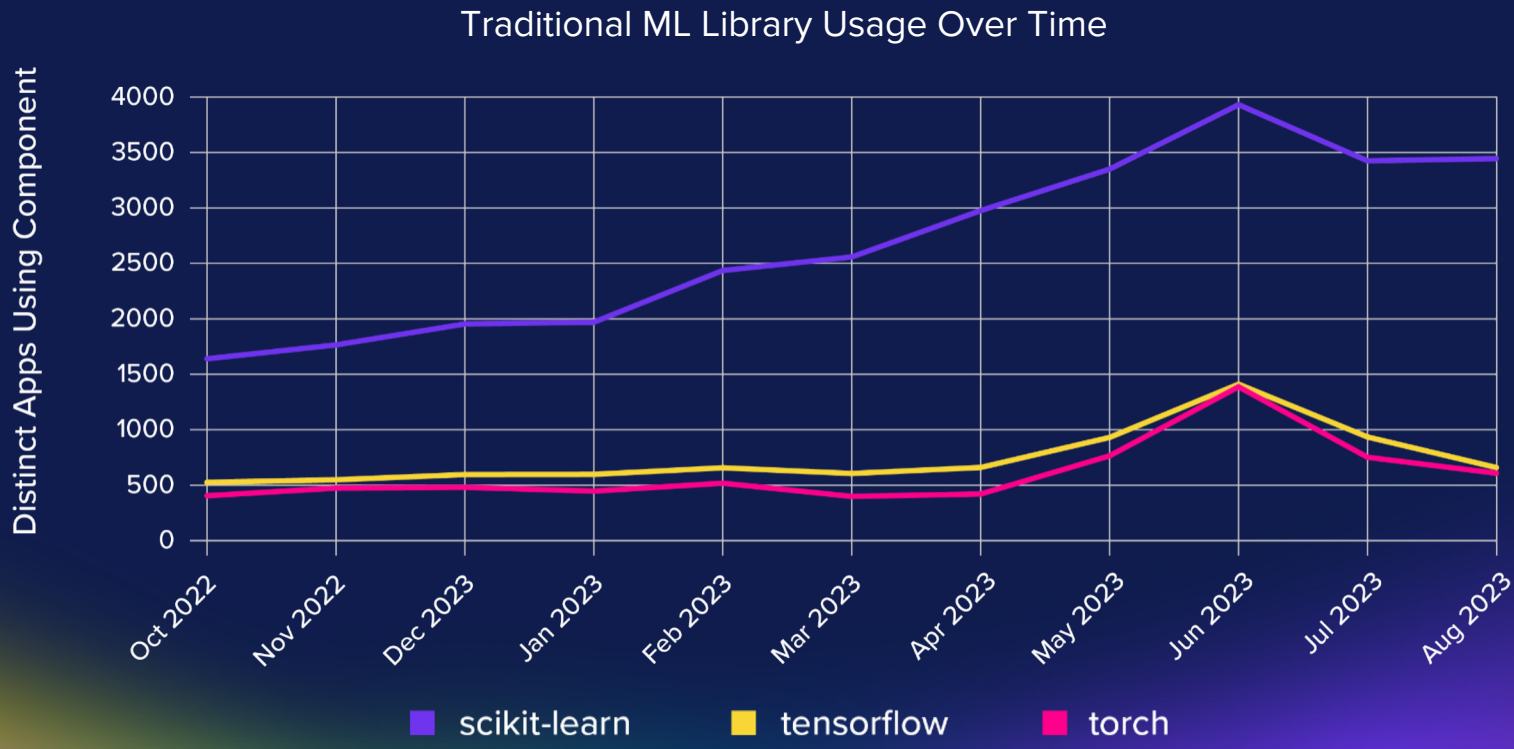
sonatype

Demand for LLM Libraries Is Growing



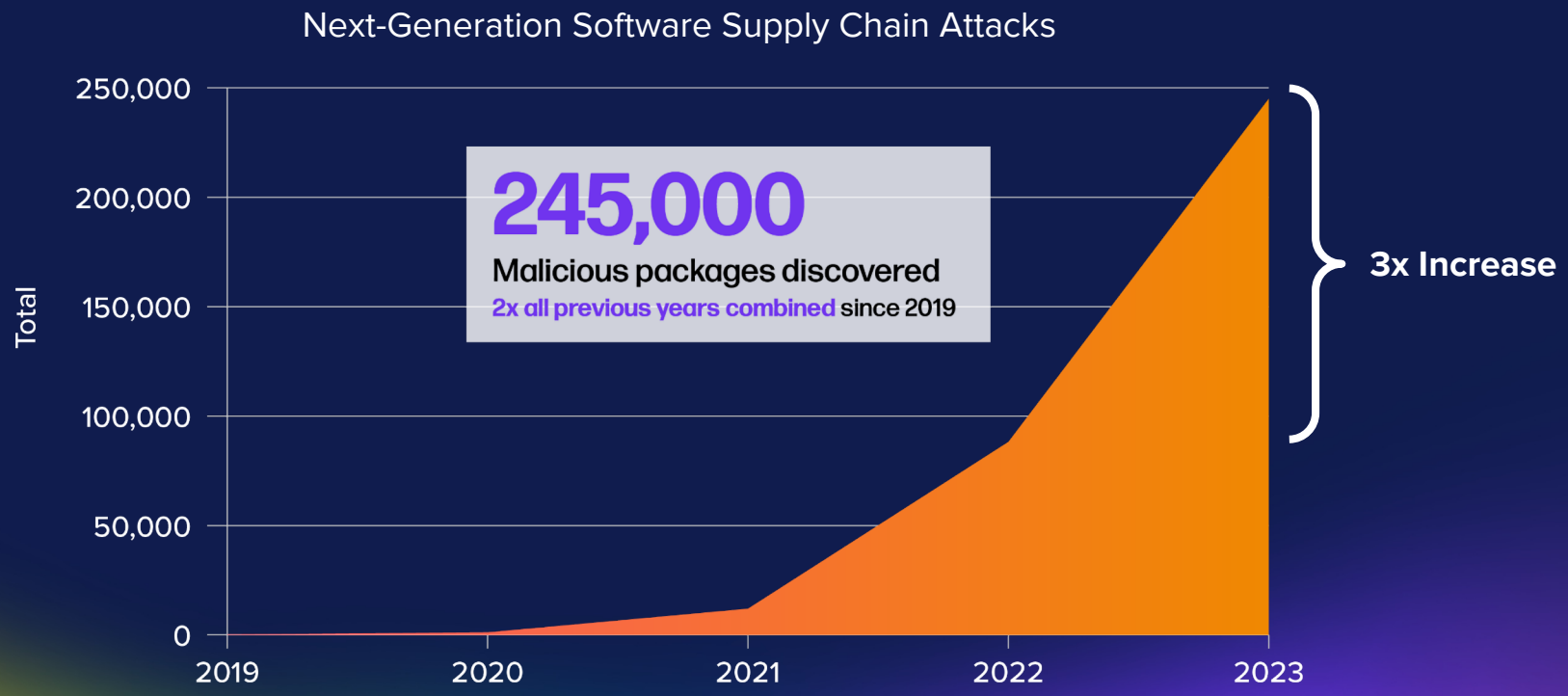
sonatype

Demand for ML Libraries Broadly Is Also Growing



sonatype

Attackers Are Also Innovating



sonatype

Challenges To Harnessing Innovation

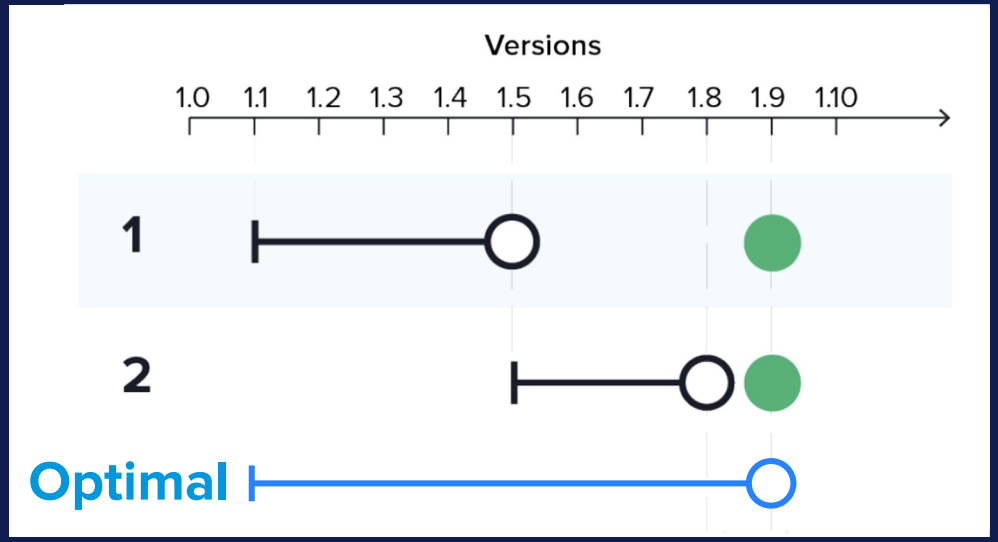
sonatype

150 Dependencies (avg Java project)

x 10 Releases Per Year (avg per dependency)

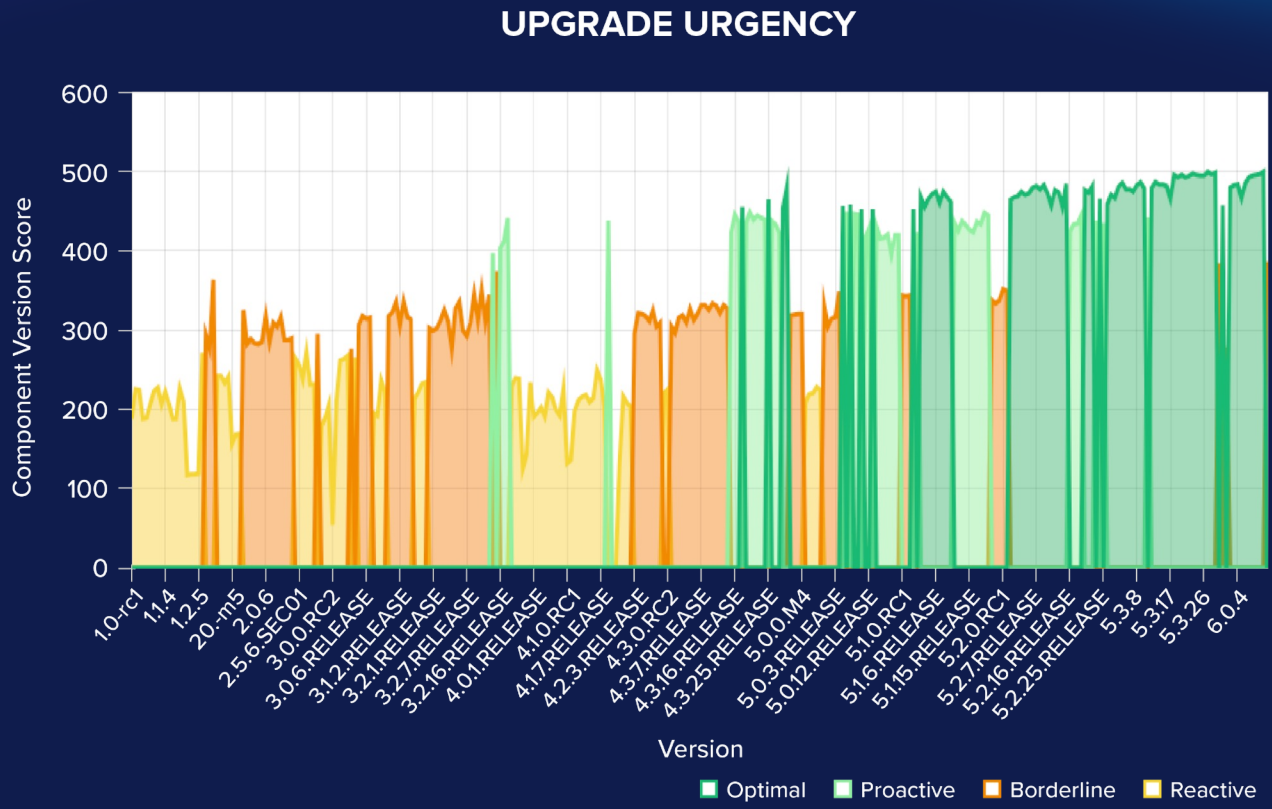
1500 Updates To Consider 😱

Inefficient Upgrades Waste Time



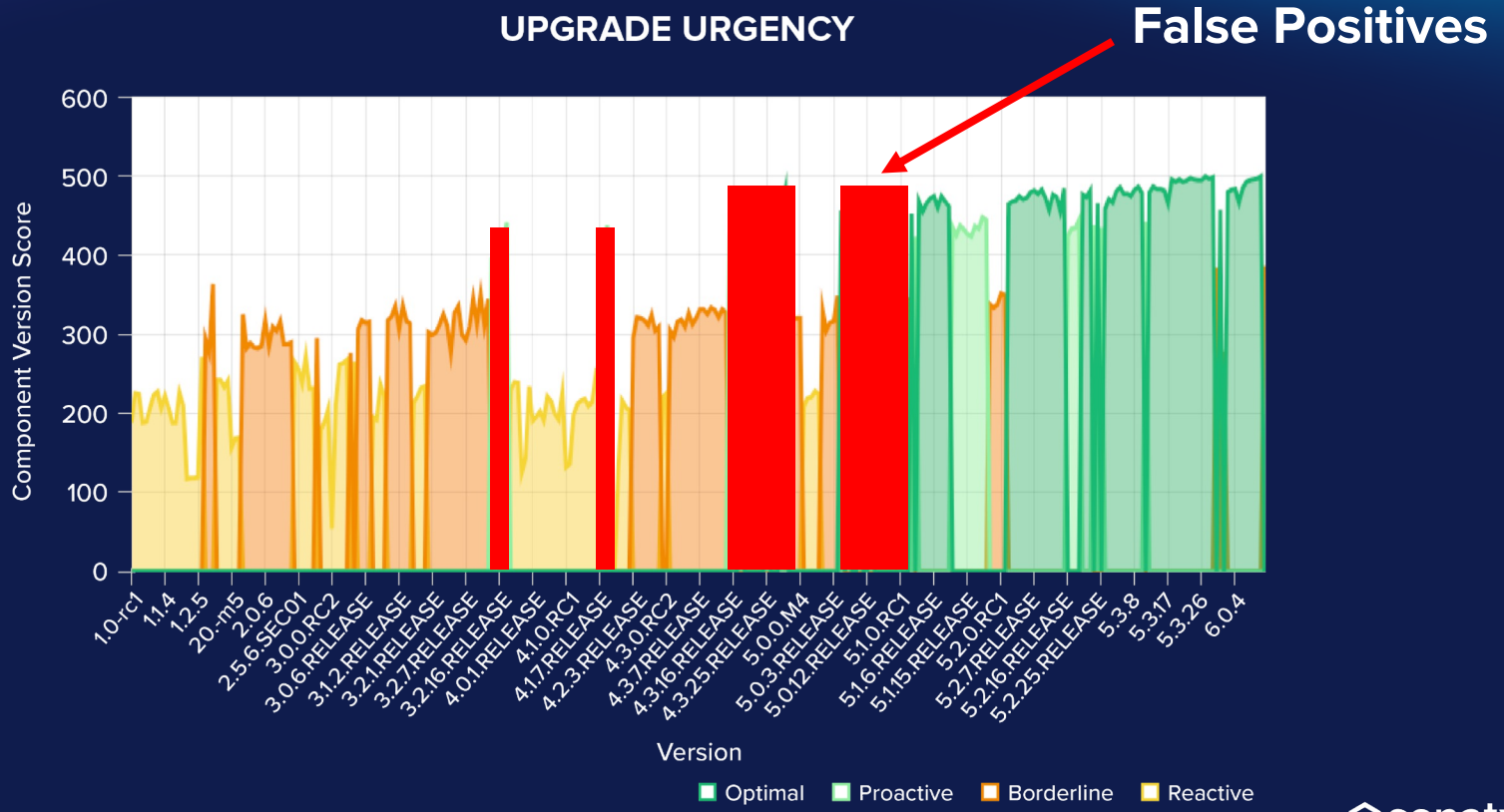
The average downloaded Maven Central component has 10 superior versions available.

Only Certain Versions Need Attention



sonatype

Only Certain Versions Need Attention



sonatype

Saving Effort When Upgrading

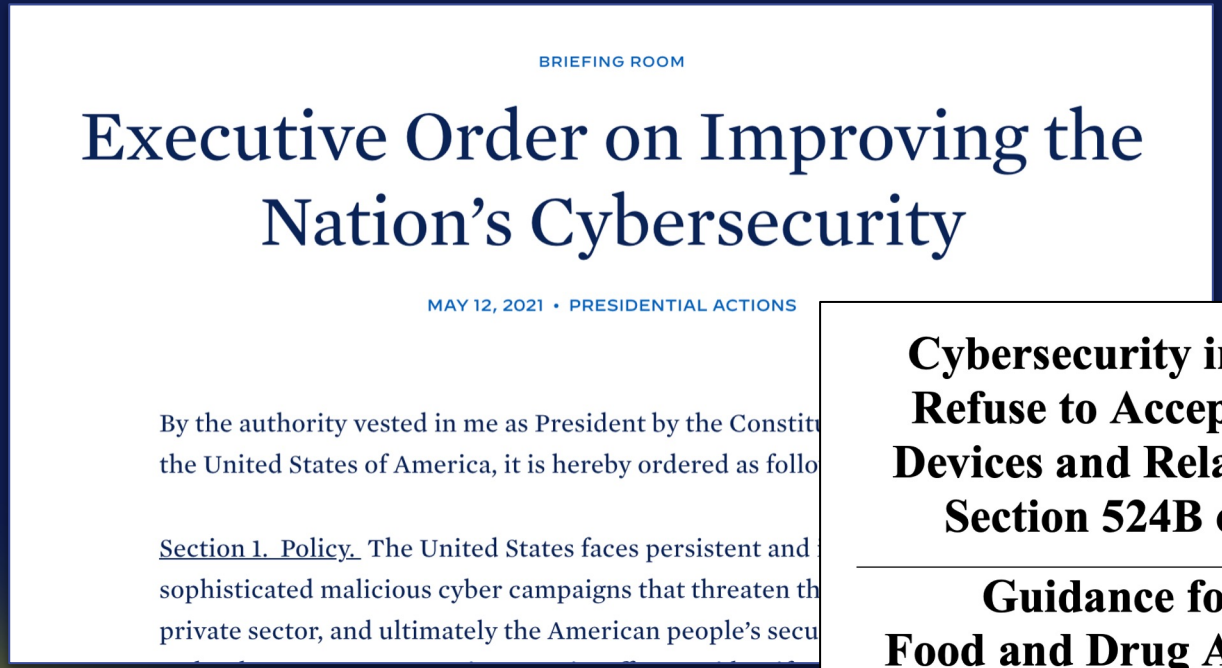
1. Use vulnerability scanners with a low false positive rate.
2. Choose the optimal version when upgrading.

Combined: 1.5 months of time saved per dev team per year.

Stop Wasting Developer Time

sonatype

Regulations Are ~~Coming~~ Here



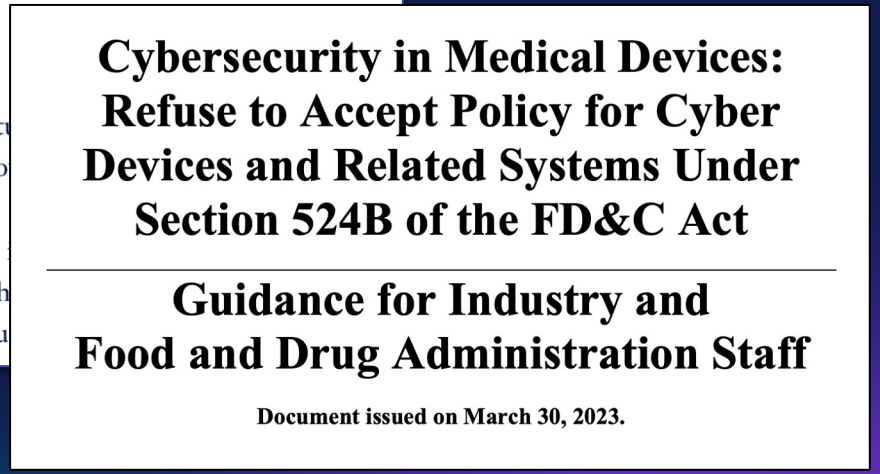
BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitu
the United States of America, it is hereby ordered as follo

Section 1. Policy. The United States faces persistent and
sophisticated malicious cyber campaigns that threaten th
private sector, and ultimately the American people's secu



Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act

Guidance for Industry and Food and Drug Administration Staff

Document issued on March 30, 2023.

sonatype

SBOM Requirements Are Spreading

sonatype

"Never let a good crisis go to waste."

- Winston Churchill

Stop Wasting Developer Time

sonatype

Thank You! (and read the full report!)

sonatype