



# For Better Security, Stop Wasting Developer Time

9th Annual State of the Software  
Supply Chain

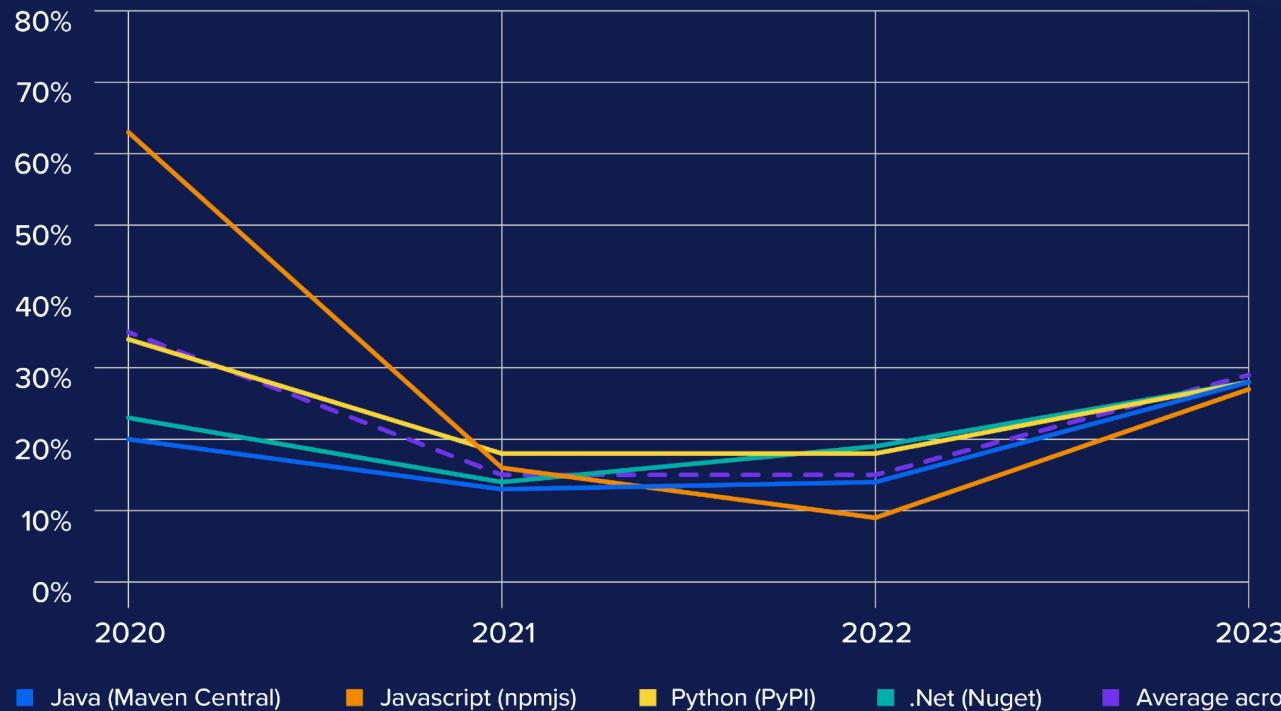
Dr. Stephen Magill,  
VP Product Innovation, Sonatype



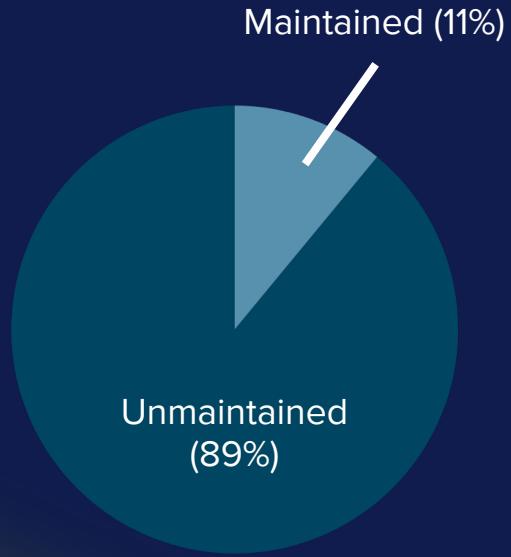
# 2023: A Year of Innovation

# New OSS Project Growth Rate Is Recovering

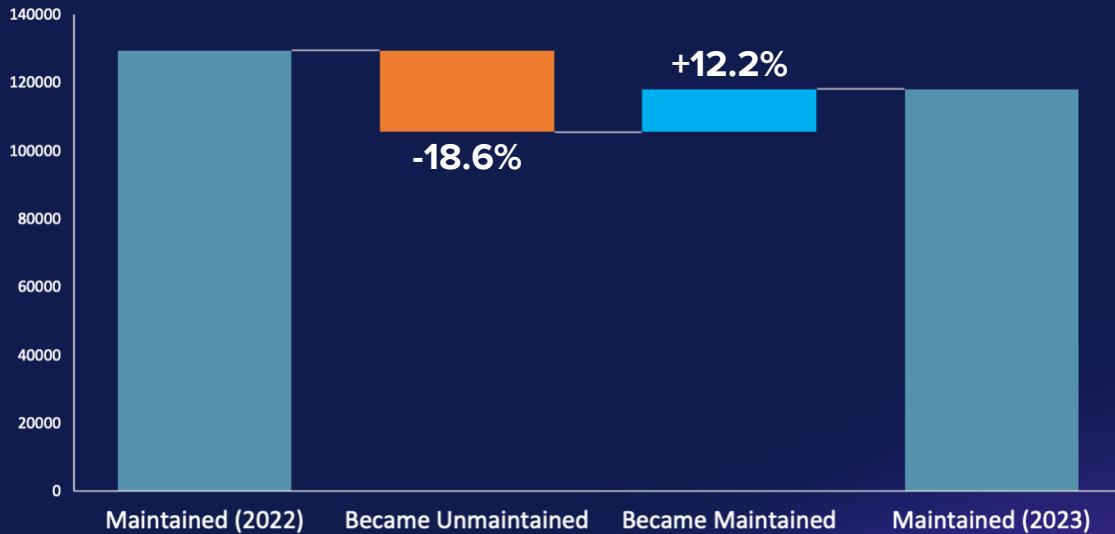
Year-over-year growth in new OSS projects by ecosystem



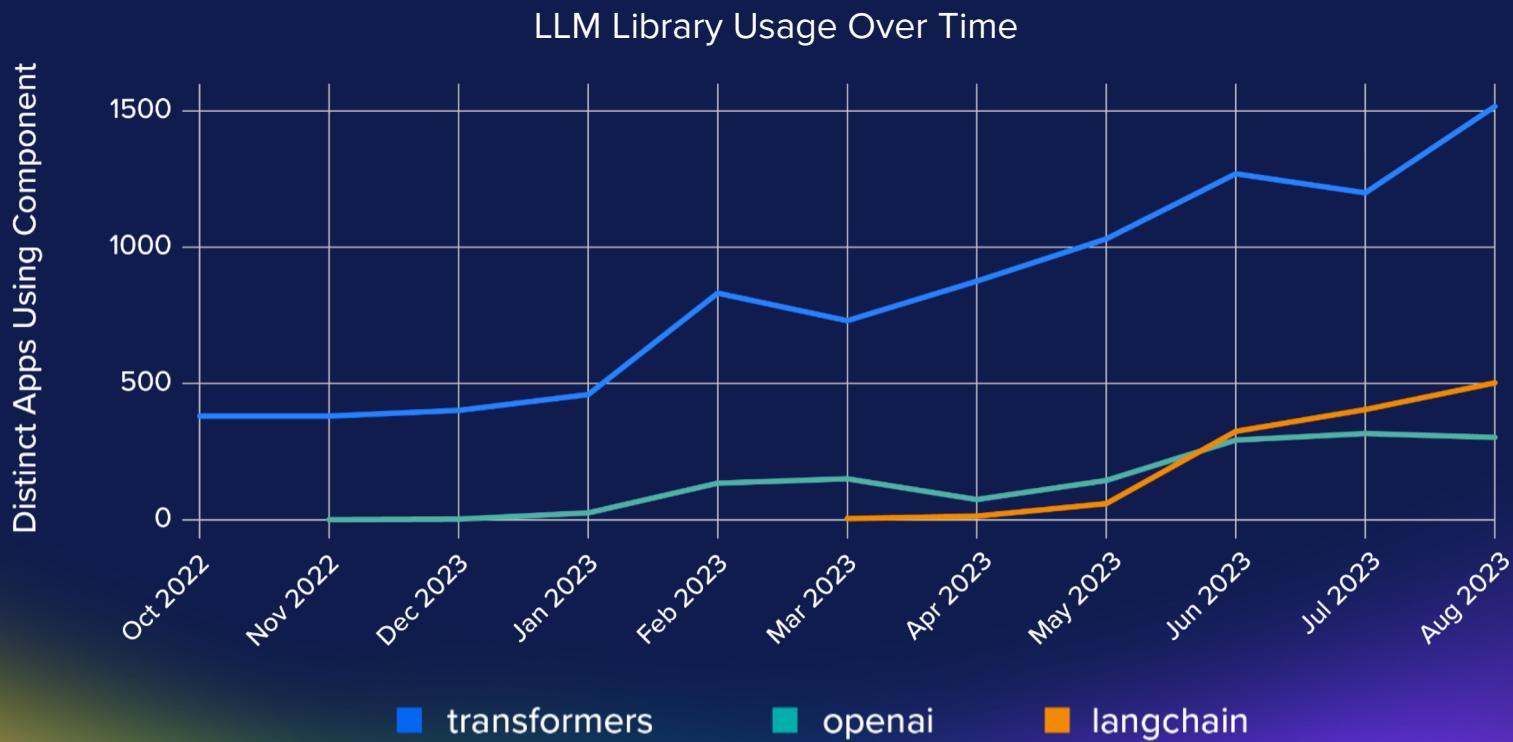
# Maintained Projects



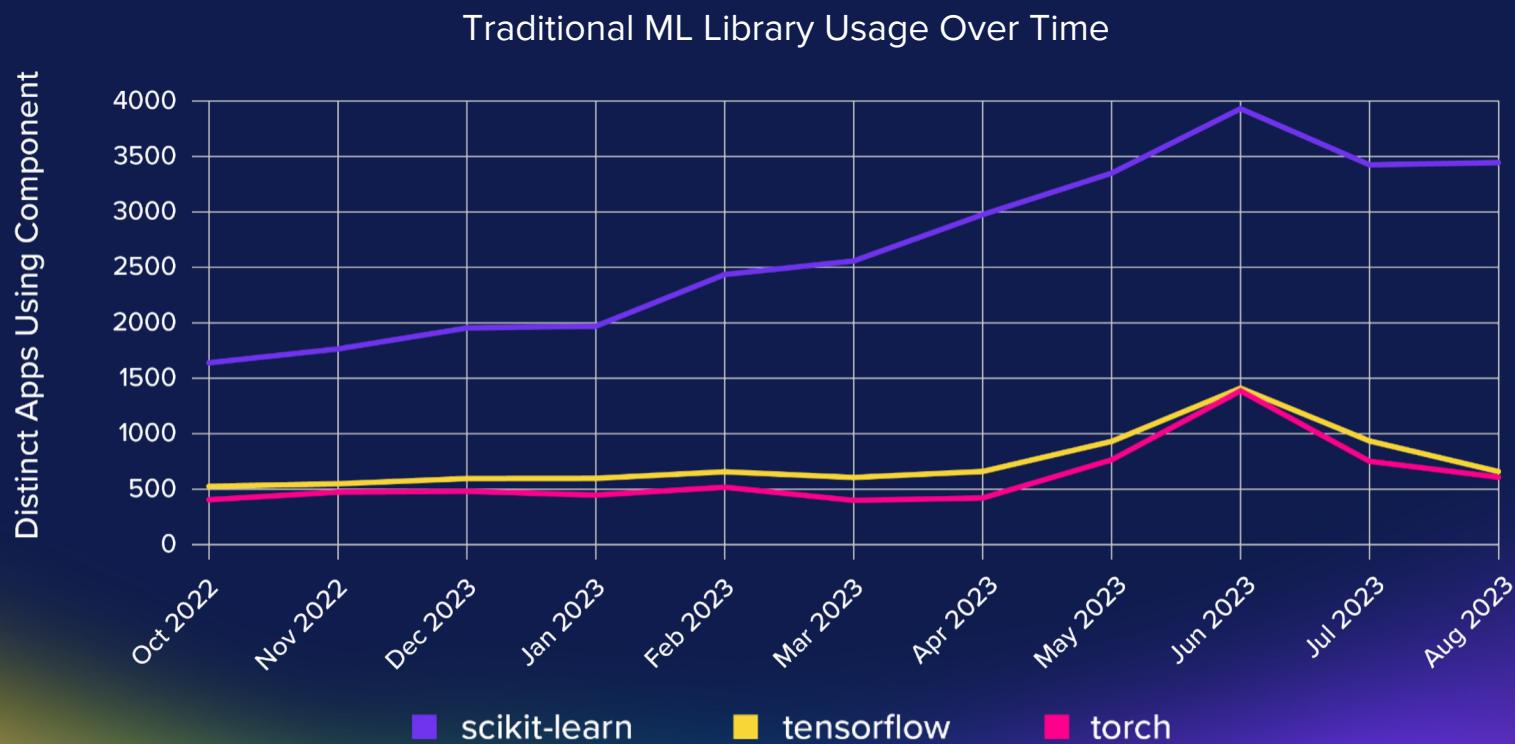
1-Year Change in Set of Maintained Projects (2022-2023)



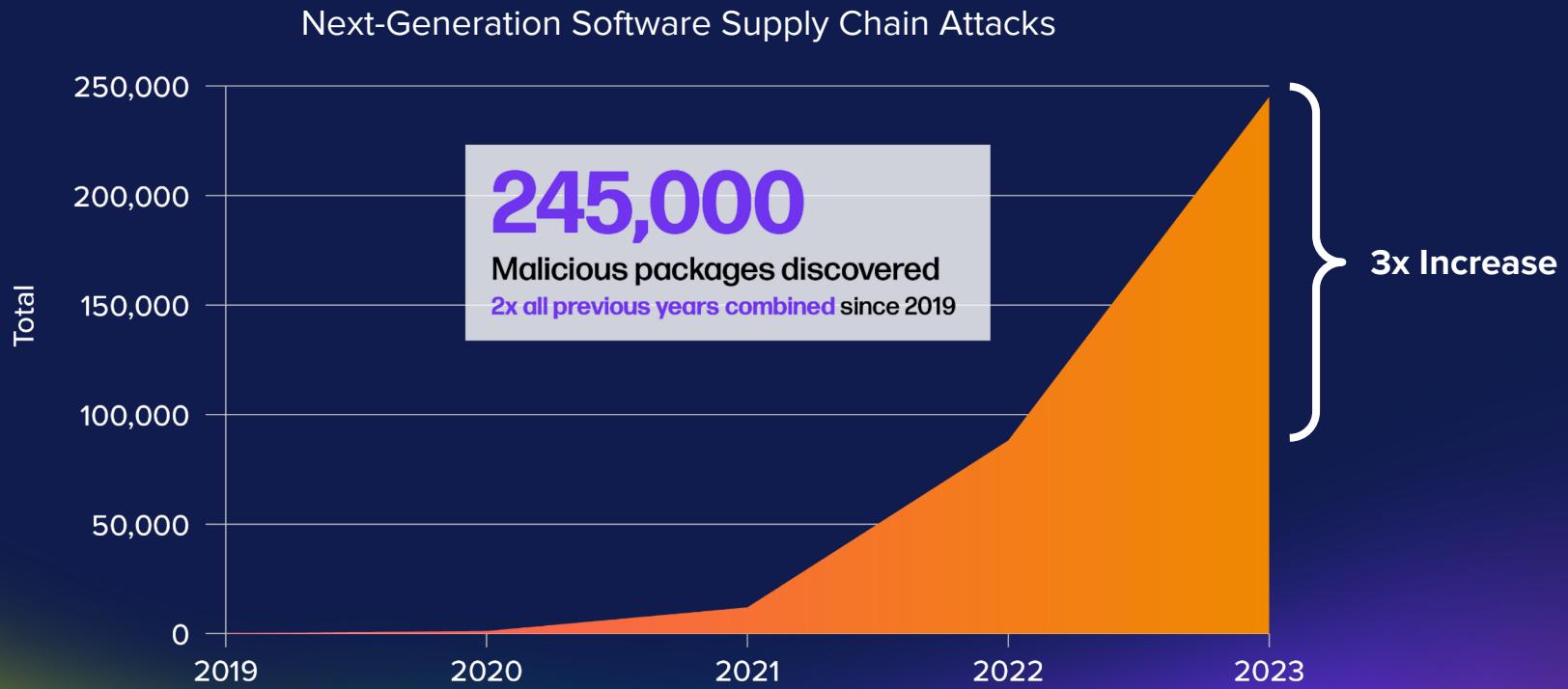
# Demand for LLM Libraries Is Growing



# Demand for ML Libraries Broadly Is Also Growing



# Attackers Are Also Innovating



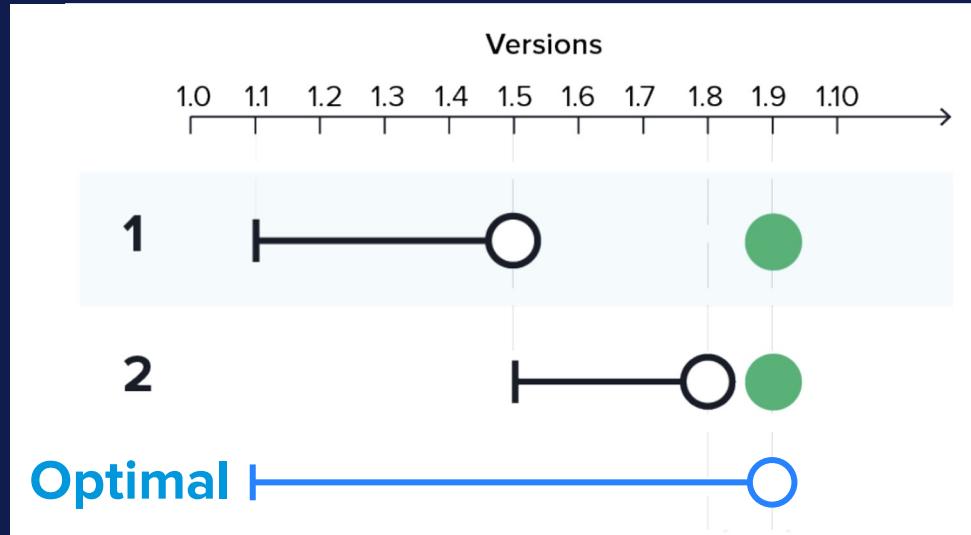
# Challenges To Harnessing Innovation

**150 Dependencies** (avg Java project)  
**x 10 Releases Per Year** (avg per dependency)

---

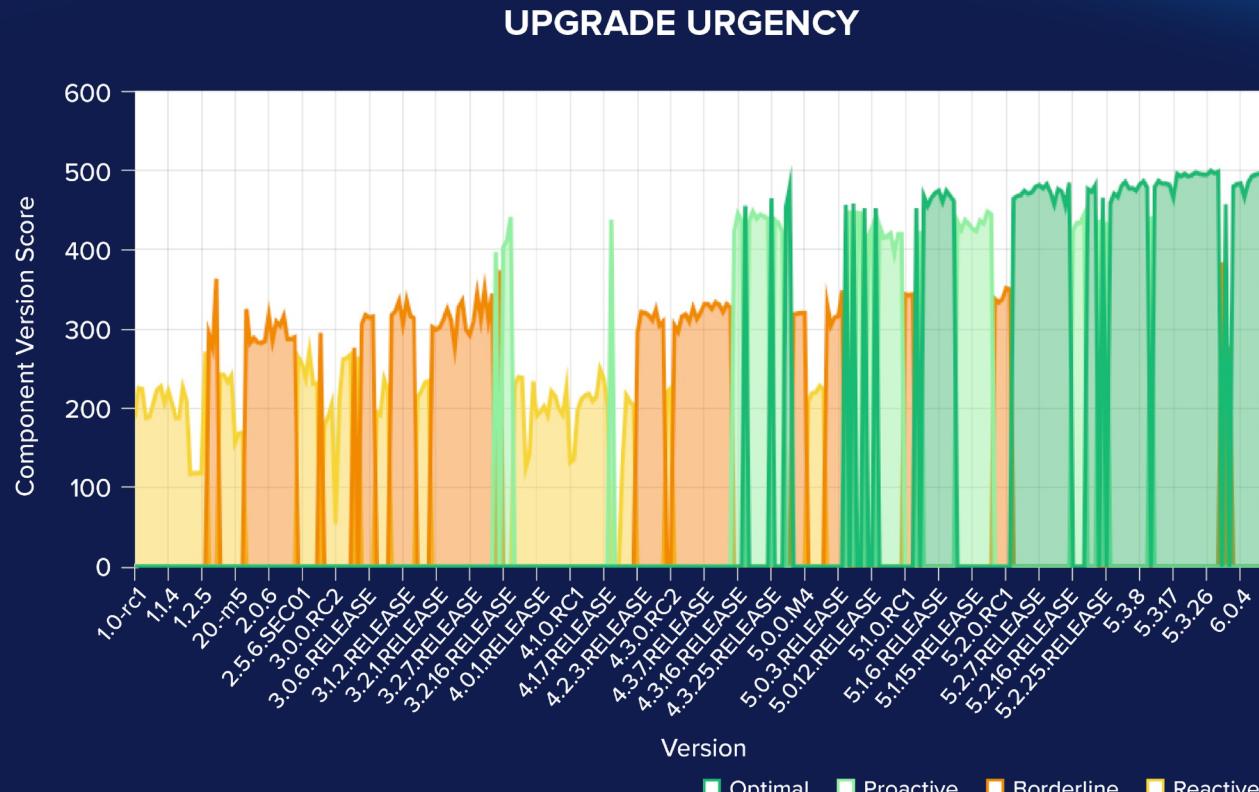
**1500 Updates To Consider** 😱

# Inefficient Upgrades Waste Time

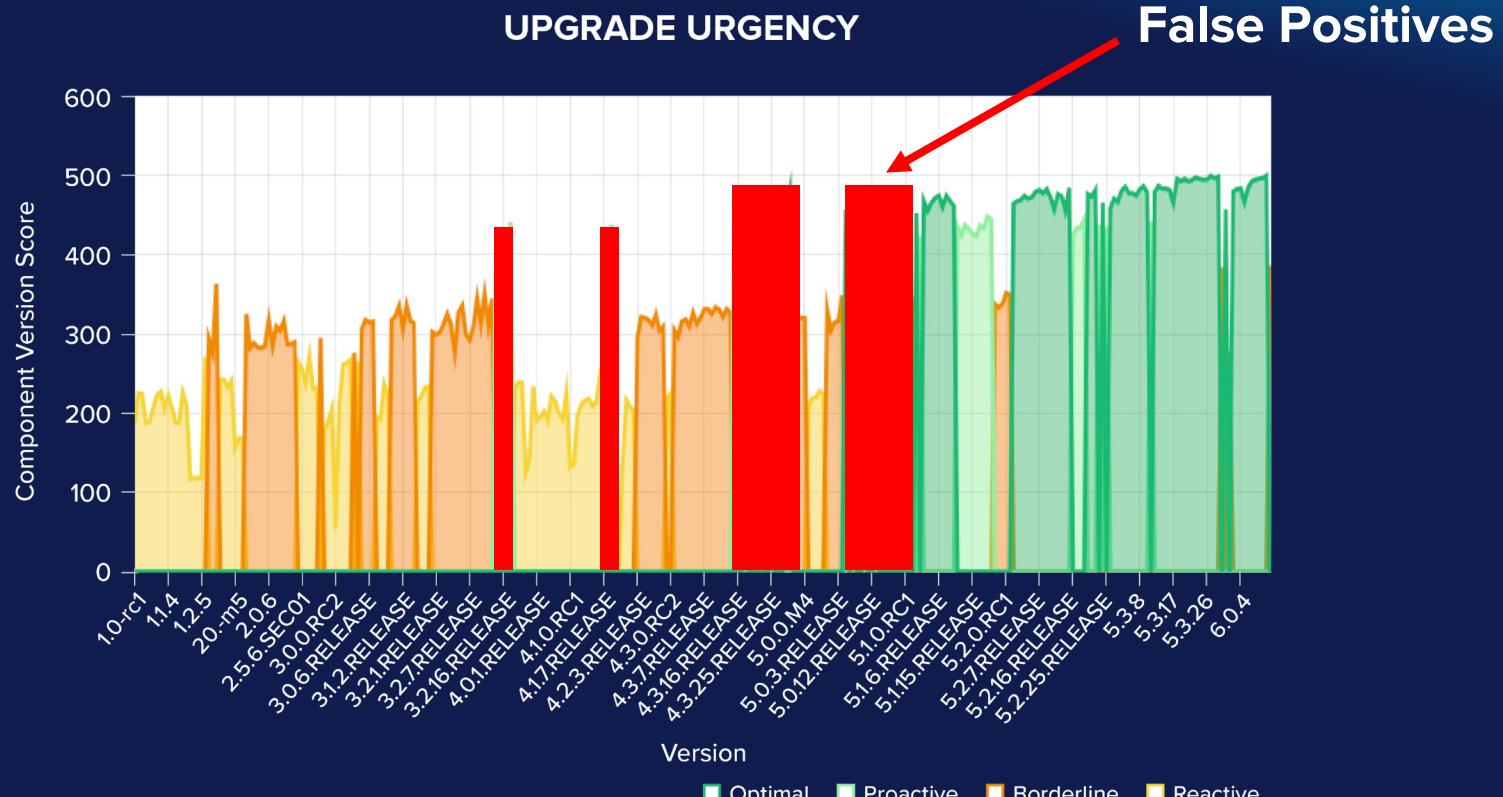


The average downloaded Maven Central component  
has 10 superior versions available.

# Only Certain Versions Need Attention



# Only Certain Versions Need Attention



# 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

# 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 Constitution and Laws of the United States of America, it is hereby ordered as follows:

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

### 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.

# SBOM Requirements Are Spreading



■ somewhat disagree   ■ disagree   ■ strongly disagree   ■ somewhat agree   ■ agree   ■ strongly agree



“Never let a good  
crisis go to waste.”

- Winston Churchill

# Stop Wasting Developer Time

# Thank You! (and read the full report!)

Understanding Open Source Adoption: Insights from the 9th State of the Software Supply Chain Report.

Download the Full Report

Introduction

Open Source Supply, Demand, and Security

Open Source Security Practices

Modernizing Open Source Dependency Management

Software Supply Chain Maturity

Establishment and Expansion of Software Supply Chain Regulation and Standards

**9th Annual**

# State of the Software Supply Chain

Sonatype's industry-defining research on the rapidly changing landscape of open source, software development, and software supply chain security

sonatype