VOLUME 12

# State of Software Security

For the 12th version of the *State of Software Security* report, we leveraged the full historical data from Veracode services and customers. This accounts for a total of more than half a million applications that used a variety of scan types. All those scans produced 42 million raw static findings, 3.5 million raw dynamic findings, and 6 million raw software composition analysis findings.

**HERE'S A SNAPSHOT OF WHAT THE DATA SHOWS ABOUT THE STATE OF SOFTWARE SECURITY TODAY.**

## 01 The Number of Apps Scanned Has Tripled

Organizations are scanning triple the number of applications per quarter than they were scanning a decade ago.



NEW APPLICATIONS PER ACCOUNT

WEEK APPLICATION FIRST SCANNED
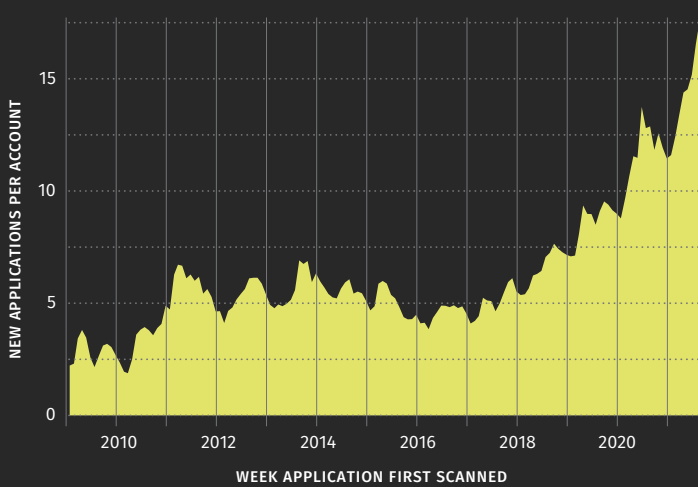
## 02 Microservices

In 2018, roughly 20 percent of applications incorporated multiple languages. This year, less than 5 percent of apps used multiple languages, suggesting a pivot to smaller, one-language applications or microservices.

2018 **20%**

2021 **< 5%**
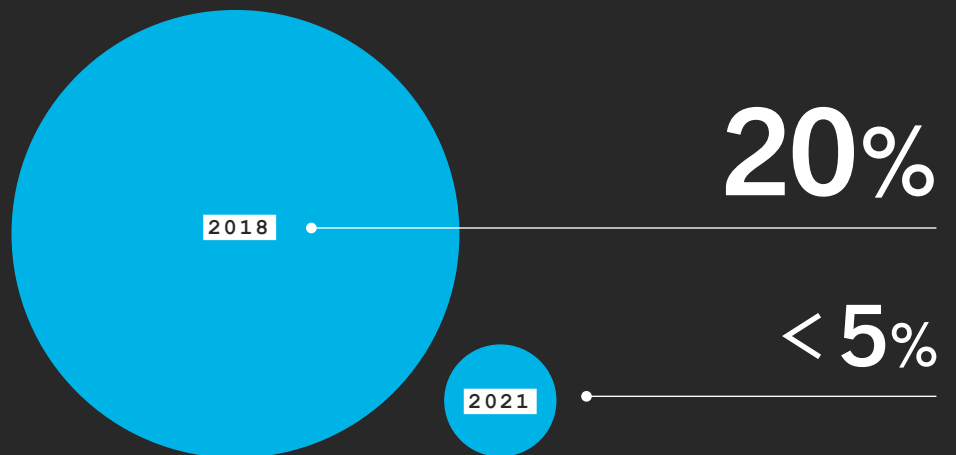
*JavaScript, Python, and .NET have seen declines in app sizes, indicating a trend toward more microservices.*

## 03 Scan Cadence

Continuous testing and integration, which includes security scanning in pipelines, is becoming the norm.

**20x** increase in median scan cadence from 2010 to 2021

2010    2021

## 04 Multiple Scan Types

We've seen a 31 percent increase in the use of multiple scan types between 2018 and 2021, with much of that gain coming from organizations using the full suite of static, dynamic, and SCA scans.

**31%** increase in the use of multiple scan types
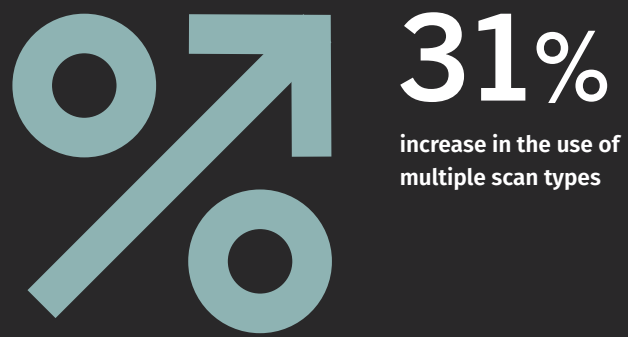
## 05 Flaw Prevalence

Over the past four years, the percent of libraries with known flaws dropped from 35 percent to less than 10 percent.

2017

2021

*Percent of libraries with known flaws dropped*

**The trend across all applications is a general reduction in flaw prevalence.**



PERCENT OF APPLICATIONS

Any Flaws
OWASP
CWE / SANS Top 25
High Severity
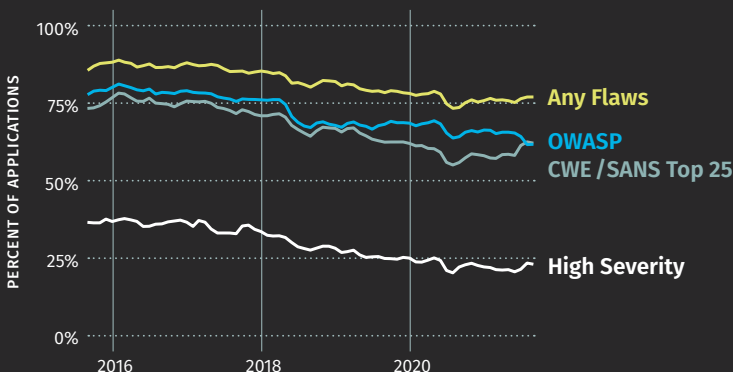
## 06 Open Source

**77%** of flaws in third-party libraries remain unfixed after three months

On a positive note, there is a noticeable improvement in time to remediation for third-party flaws. Back in 2017, it would take over three years to get to the 50 percent (half-life) closed point, and now it takes just over a year.

SOFTWARE COMPOSITION ANALYSIS



HALF-LIFE
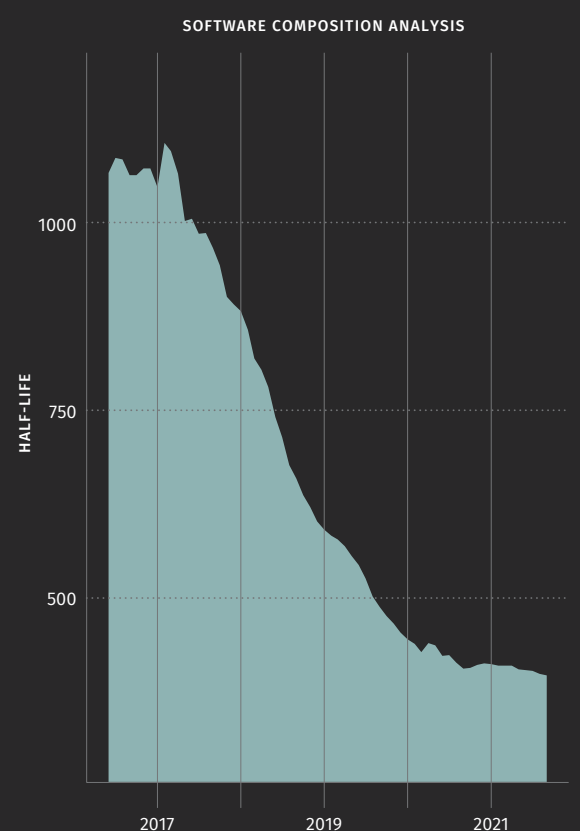
## VERACODE

Learn more at **www.veracode.com**, on the Veracode **blog** and on **Twitter**.

## 07 Veracode Security Labs

On average, organizations with Veracode Security Labs training decrease their time to fix 50 percent of flaws by 35 percent.

**35%** decrease in the time it takes for organizations to fix flaws