VERACODE

VOLUME 12

The State of Software Security Industry Snapshot: Technology

Veracode's State of Software Security (SOSS) Volume 12 examines historical trends shaping the software landscape and how security practices are evolving along with those trends. The data collected from 20 million scans across half a million applications suggests that we're making good progress toward the goal of producing more secure software.

This SOSS snapshot provides a view of software security in the technology sector. We hope it brings the findings a little closer to home so you can better refine your application security (AppSec) program based on the most relevant data. Let's start things off with Figure 1, which provides some core comparative metrics for the state of software security in the tech industry.

Starting on the left, the technology sector owns the econd-highest rate across all flaws as well as the highest for the most severe flaws. The industry lands in the middle of the pack when it comes to the proportion of security flaws that are fixed, though there's little variation among industries here. It could be argued that tech firms have a higher proportion of applications and/or more complex applications to contend with, but that doesn't change that the first three columns reveal ample room for improving approaches for developing more secure code in the technology sector.

The rightmost columns rank industries according to how quickly they fix flaws once they're detected by three different types of scans. The technology sector boasts industry-leading fix times for flaws discovered by static analysis (SAST) and software composition analysis (SCA) scans and slips to the middle for dynamic analysis (DAST). That's a laudable accomplishment, but the number of days required to get to the halfway point shows there's still ample room for improvement.

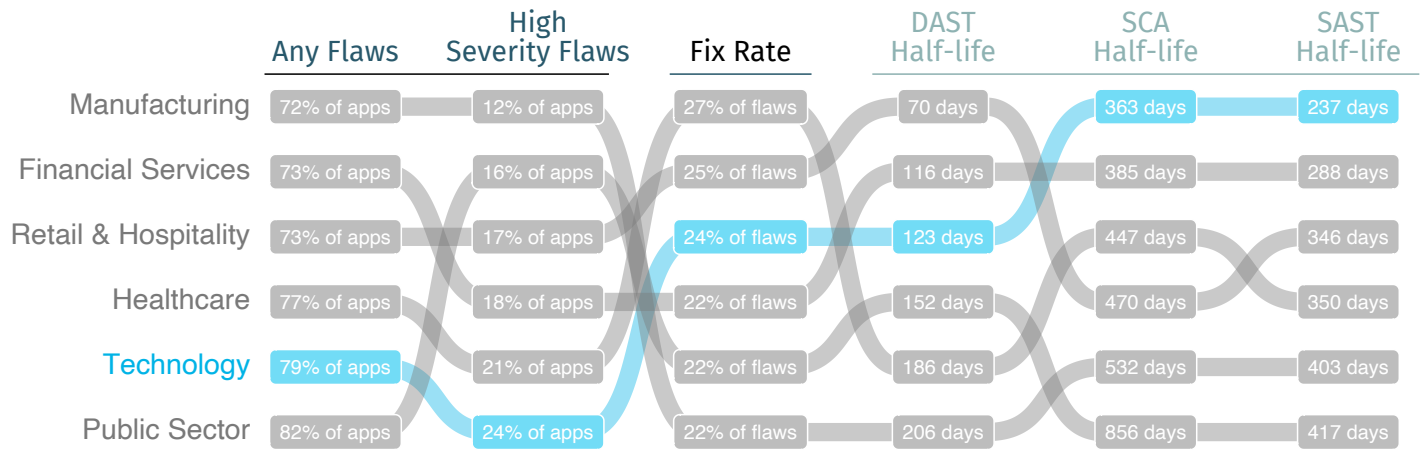

Figure 1: Values and rankings for key software security metrics by industry

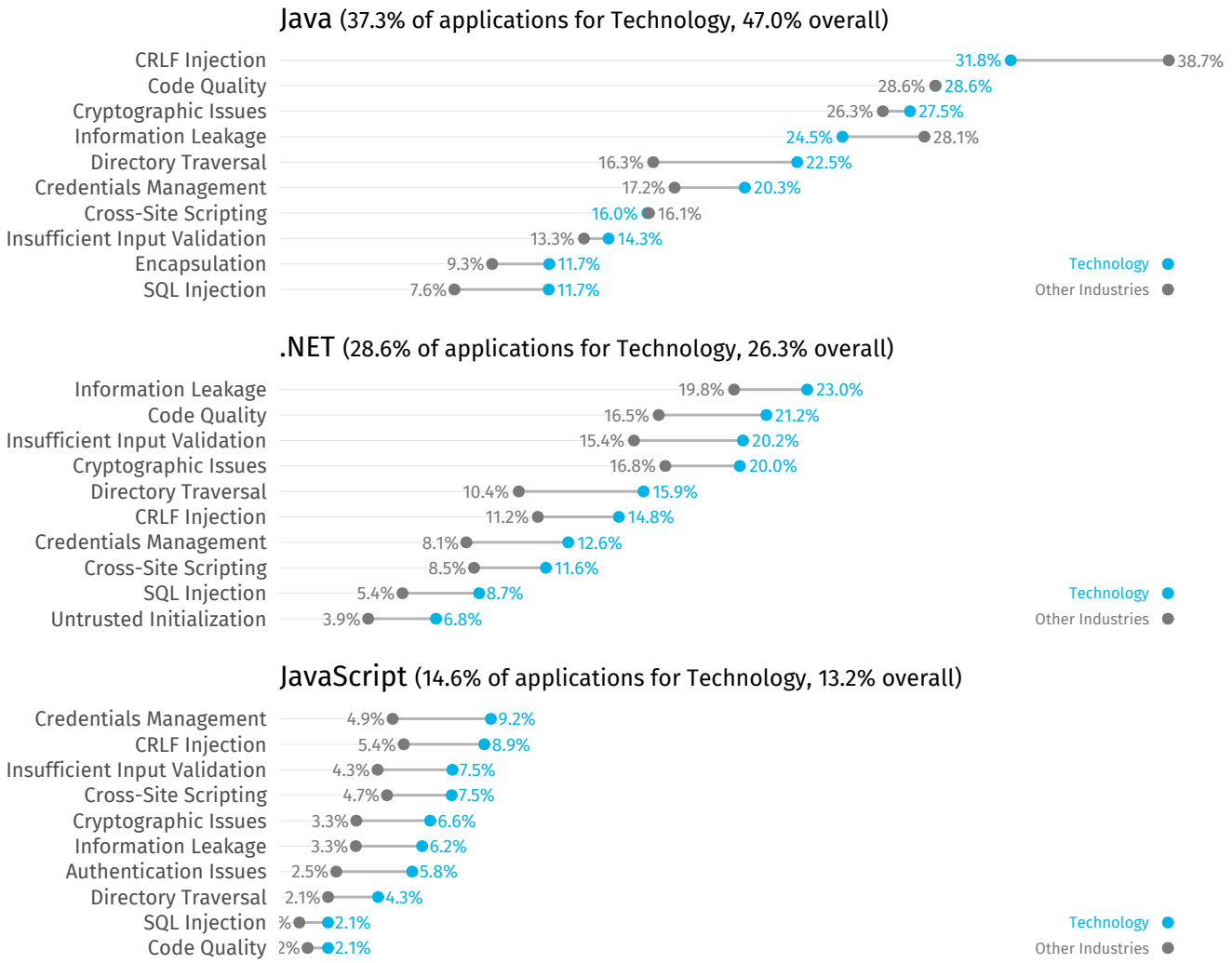

Figure 2: Most common flaws from static analysis in the technology sector.

Having compared overall flaw and fix rates, let's take a look at the most common types of flaws affecting applications. Because flaws found by SAST are very language-dependent, Figure 2 separates results by the top three programming languages used among applications in the tech sector. The chart makes it easy to determine whether technology firms (in blue) have higher or lower rates than the overall average (in gray) for each type of flaw. In general, the tech sector puts up higher rates across the board. There's a lot of information to digest here, so we'll leave you to develop your own takeaways.

Unlike SAST, DAST findings are largely consistent across languages, leading us to combine the findings into one chart. The technology industry follows a similar pattern to that of others in terms of which flaws are commonly vs. rarely identified by dynamic analysis. Cryptographic issues and information leakage exhibit the highest disparity in favor of tech firms, perhaps indicating developers are more savvy on data protection challenges. That's good to see.

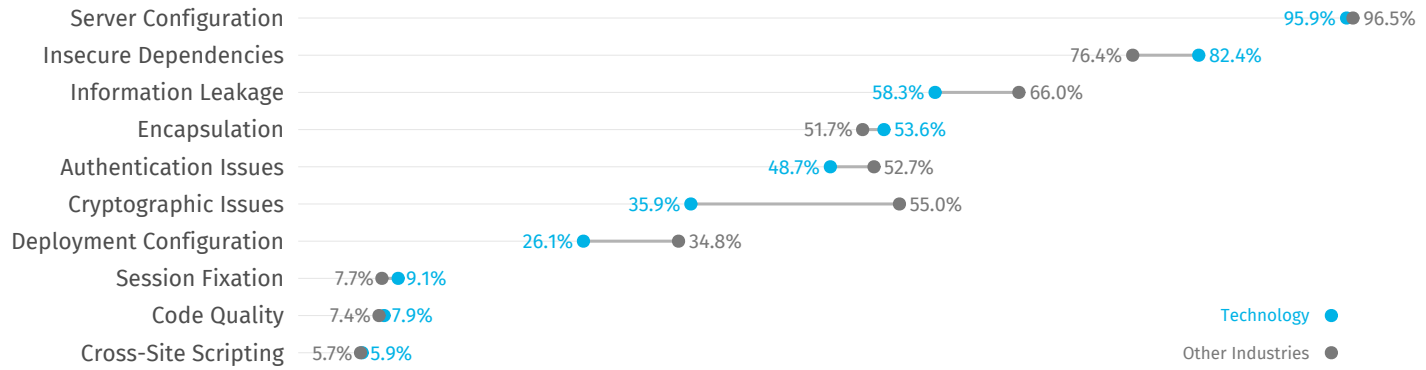

Figure 3: Most common flaws from dynamic analysis in the technology sector.

Next, we'll offer a few charts that expand on the half-life stats presented back in Figure 1. The number of days required to fix half the flaws in an application is a simple, benchmark-worthy stat, but what if you're curious about the comprehensive lifecycle of software security issues? Good news – Figure 4 enables exactly that using a method known as survival analysis!

Triangulating any point along the survival curve gives the percentage of flaws still "alive" after a period of time following discovery (e.g., 40 percent still unresolved after one year). For the most part, tech firms appear to be performing comparatively well here. They're about three months ahead of other sectors according to SAST. Tech gains an early lead addressing flaws found via DAST, but loses that lead around the one-year mark.

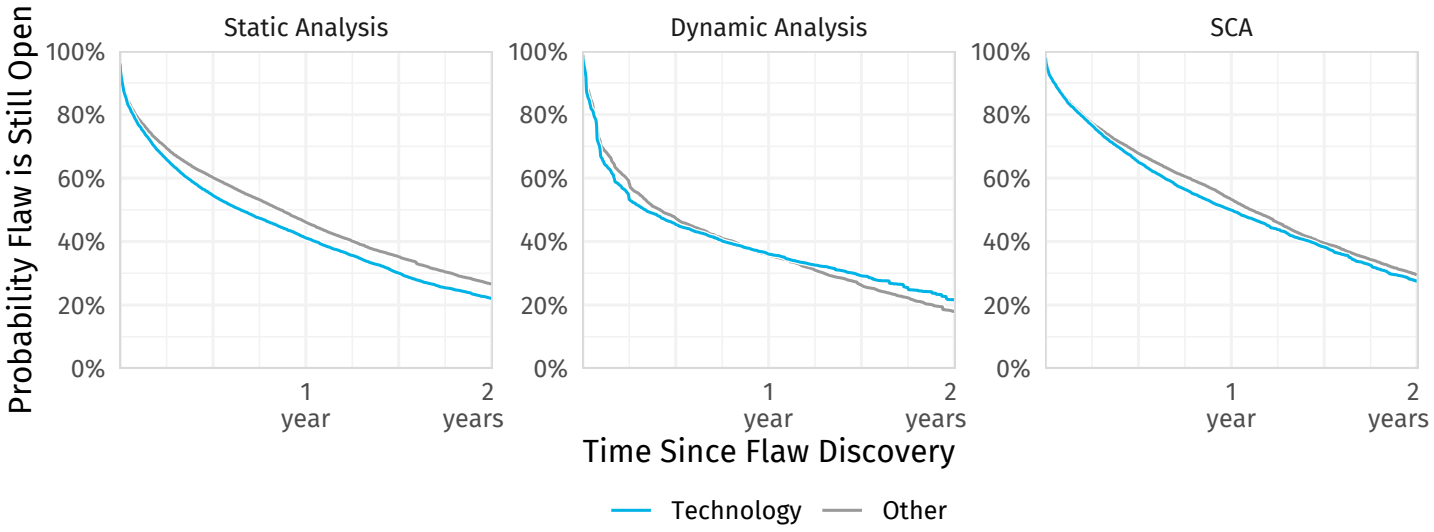

Figure 4: Two-year flaw survival rates for applications in the technology sector.

Flaws in third-party libraries found through SCA stick around longer for all industries, with about 30 percent still unresolved after two years. The technology sector tows the line for the first three months, but then quickens the pace of addressing vulnerable libraries to stay about a month ahead of the cross-industry average.

Speaking of vulnerable libraries, you're probably aware that the software supply chain is kind of a big deal these days among software security professionals. The last set of charts in this snapshot show the extent of flaws in third-party code discovered via SCA. Java applications exhibit the highest ratio of vulnerable libraries, but that's trending down over time. The same can be said for the other languages, which is a welcome ray of sunshine in an otherwise gloomy realm of software security. Here's to increasingly clear skies in the years to come!

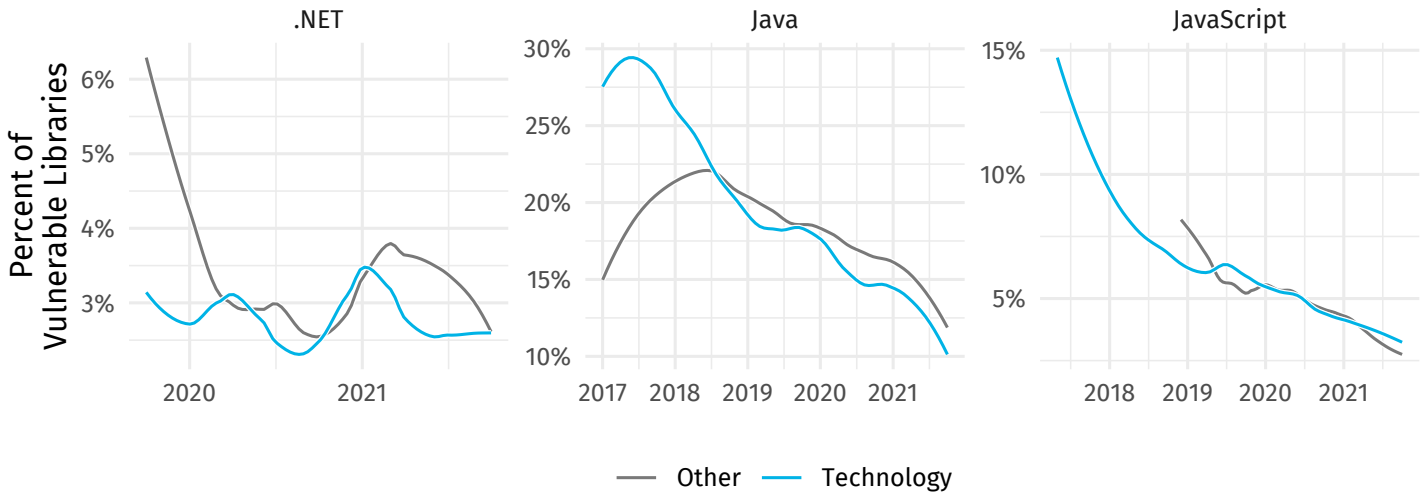

Figure 5: Proportion of vulnerable libraries used by applications in the technology sector.