

SOSS VOLUME 10 INDUSTRY SNAPSHOT

Infrastructure

Veracode's State of Software Security (SOSS) Volume 10 focused on the topic of security debt, defined as the amount of unaddressed flaws that accumulate in software over time. The report revealed about half of application teams added to their security debt, a little over a quarter paid it down, and a

quarter maintained a steady balance. As you might suspect, our analysis showed that debt profiles differed substantially among industries. This infosheet provides a summary of factors that shape the debt profile exhibited in the chart below for the Infrastructure sector.

Figure 1: Comparison of fix capacity and security debt by industry

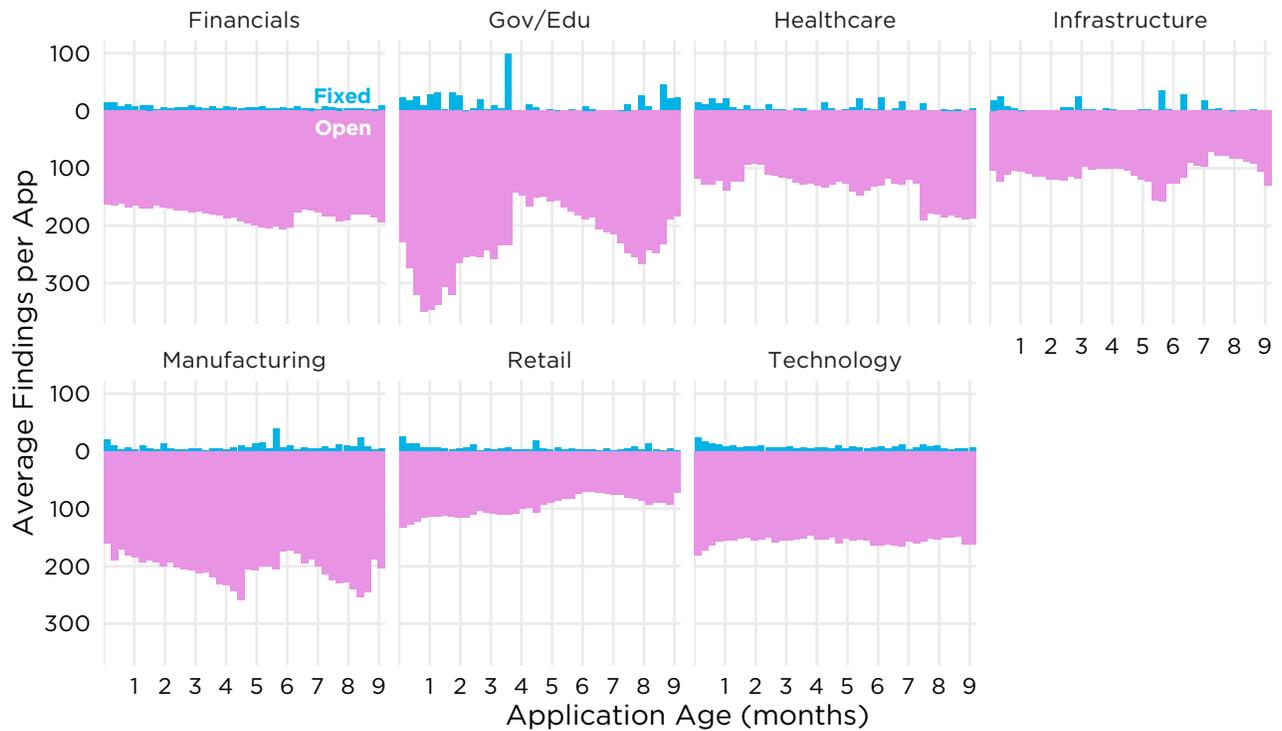
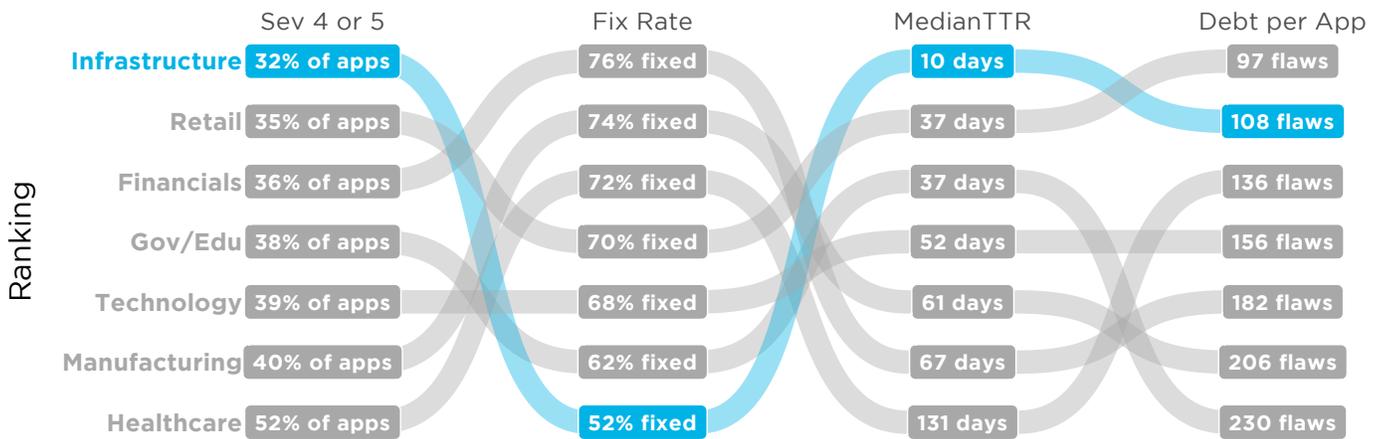


Figure 1 models the mechanics of security debt in a typical application. The dark blue bars on top correspond to weekly flaw closures. The pink area tallies the average number of unresolved flaws carried over each week. Per the figure, the Infrastructure industry carries a relatively low amount of debt that doesn't appear to be growing during the period. That's an impressive feat given what we see in other industries.

Figure 2 ranks the Infrastructure sector according to several key measures from our software security testing over the last year. Proceeding from left to right, the columns shed light on debt creation, starting with the proportion of applications with higher-severity (level 4 or 5) flaws, the percentage of those flaws that are fixed, the median speed at which those flaws are fixed, and the average amount of unfixed flaws (debt) per application.

Figure 2: Values and rankings for key software security testing metrics by industry

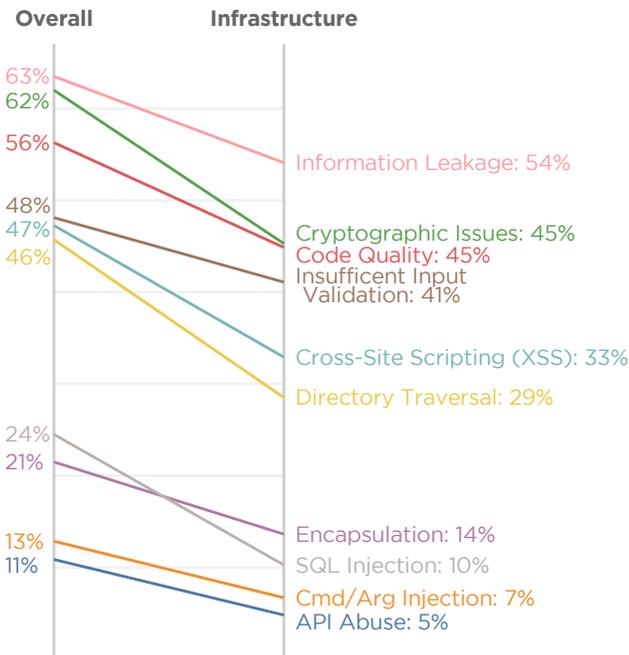


Source: Veracode SOSS Volume 10

Infrastructure firms rank at or near the top in three of the four columns in Figure 2, which probably helps explain that low balance of security debt witnessed in Figure 1. Most impressive is the 10 days typically required to fix severe flaws.

That’s almost 4X faster than any other industry, and 13X faster than the MedianTTR for Healthcare! The caveat to that feat is the Infrastructure sector only fixes half of their severe flaws. At least they’re fast when they do fix.

Figure 3: Prevalence of flaw categories in the Infrastructure sector



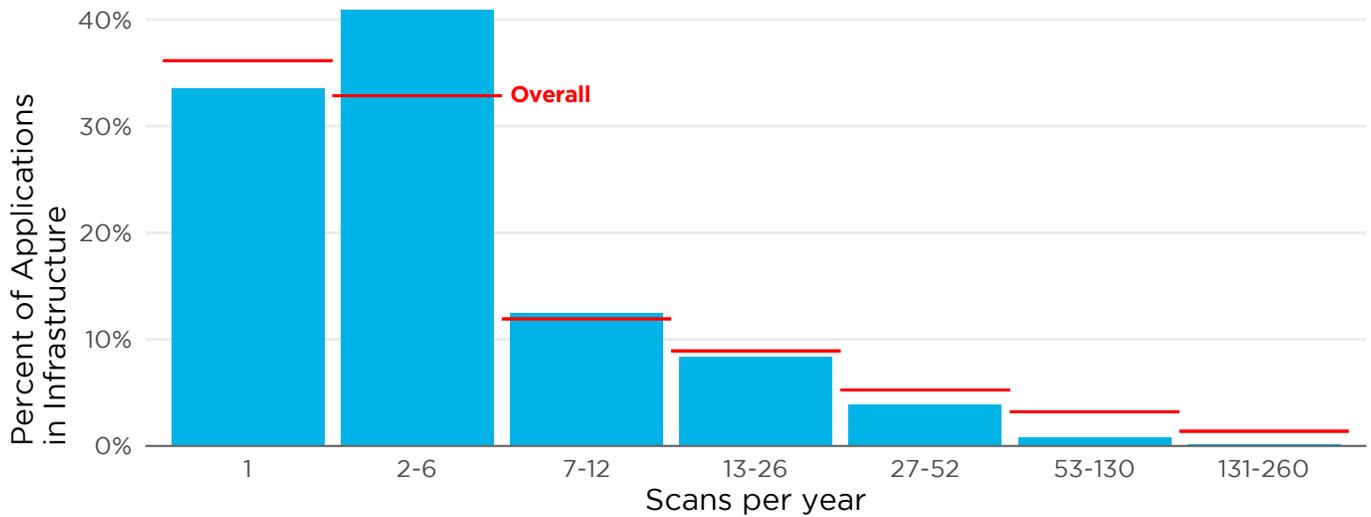
Source: Veracode SOSS Volume 10

A more detailed view of flaws discovered in Infrastructure applications can be found in Figure 3. The left column marks the overall prevalence of each category across all sectors and the right traces the comparable statistic for Infrastructure.

We see significant numerical shifts in Figure 3, but the relative ranking among categories remains mostly static. It’s worth noting that Infrastructure is the only sector in which flaw prevalence decreases across the board. That’s laudable but not entirely unexpected in light of the lowest ratio of severe flaws seen in Figure 2.

The preceding figures give us an informative snapshot of how Infrastructure performs in key software security measures, but they don’t tell us much about what’s driving those outcomes. Over the last two years, our research in the SOSS has uncovered strong evidence that practices in keeping with a DevSecOps approach yield substantial benefits to development teams that employ them. In Vol. 9, we discovered that the most active DevSecOps programs fix flaws more than 11.5x faster than the typical organization. The most recent SOSS found that teams scanning applications most frequently carry about 5X less security debt than infrequent scanners. So, how does Infrastructure compare? Figure 4 has the answer.

Figure 4: Frequency of application security scanning in the Infrastructure sector



Source: Veracode SOSS Volume 10

All industries show a skewed distribution for scanning frequency, with about 80 percent of applications scanned 12 times per year or less. That ratio remains for the Infrastructure sector, but does vary somewhat. Comparatively fewer

Infrastructure applications are scanned just once (that's good). Curiously, the proportion of applications tested over 52 times annually lies well below the overall average.



READ THE FULL REPORT
[VERACODE.COM/SOSS](https://veracode.com/soss)

VERACODE

Veracode is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development life cycle, before they can be exploited by hackers. Our complete set of offerings helps customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets — whether that's software they make, buy, or sell.

Veracode serves more than 1,400 customers across a wide range of industries, including nearly one-third of the Fortune 100, three of the top four U.S. commercial banks, and more than 20 of Forbes' 100 Most Valuable Brands. Learn more at www.veracode.com, on the Veracode blog, on Twitter and in the Veracode Community.

Copyright © 2019 Veracode, Inc. All rights reserved. All other brand names, product names, or trademarks belong to their respective holders.