VERACODE

SOSS VOLUME 10 INDUSTRY SNAPSHOT

Technology

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 Technology sector.

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

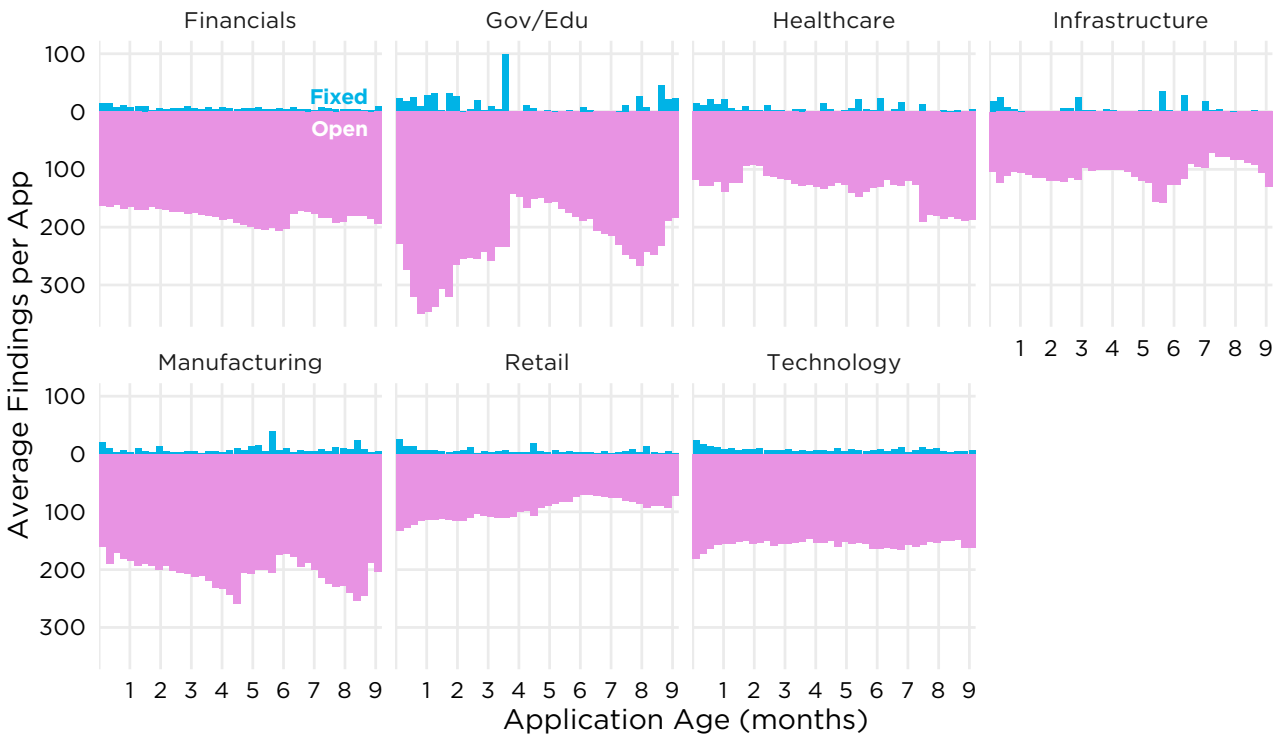
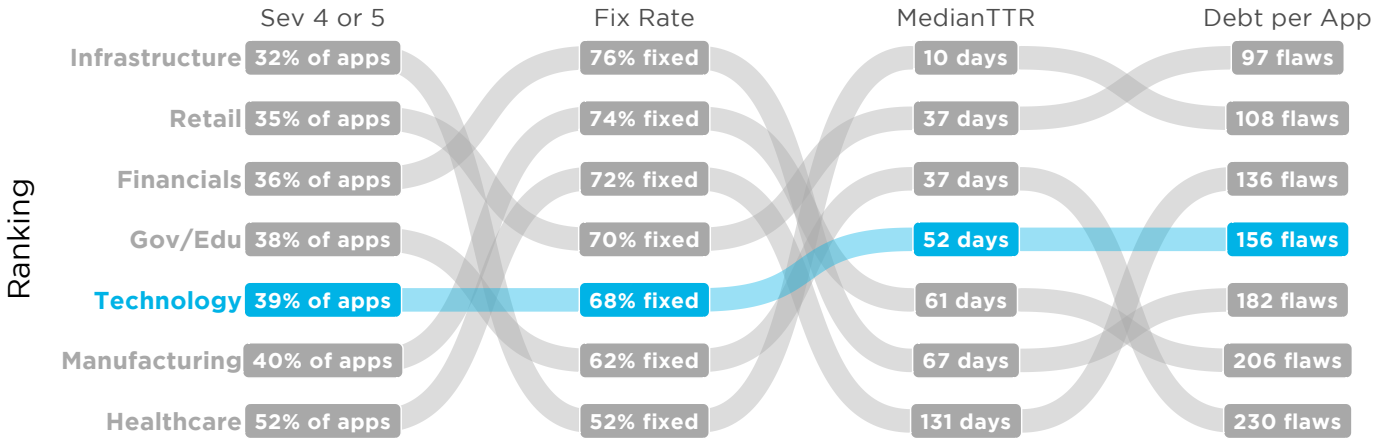


Figure 1 models the mechanics of security debt in a typical application. The dark blue bars on top correspond to weekly flaw closures. The pink area tallies the average number of unresolved flaws carried over each week. Per the figure, the Technology industry doesn't carry the highest amount of debt, but it's not the lowest either. Worth noting, the average amount of security debt for tech firms appears to be holding steady over the sample period.

Figure 2 ranks the Technology 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.

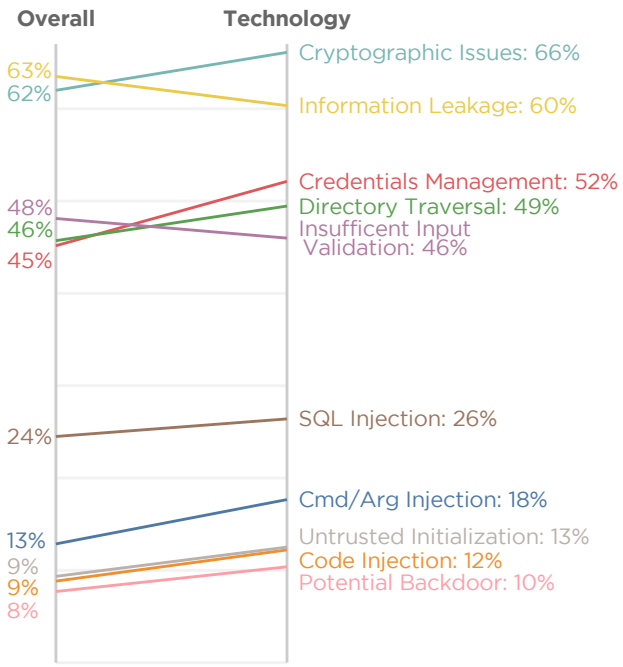
Figure 2: Values and rankings for key software security testing metrics by industry



Source: Veracode SOSS Volume 10

Tech firms occupy middle-of-the-road rankings in all columns of Figure 2. While we'd love to see them top the charts across the board, there's something to be said for consistency. Maintaining an even debt-to-income ratio certainly beats continually digging the hold deeper.

Figure 3: Prevalence of flaw categories in the Technology sector



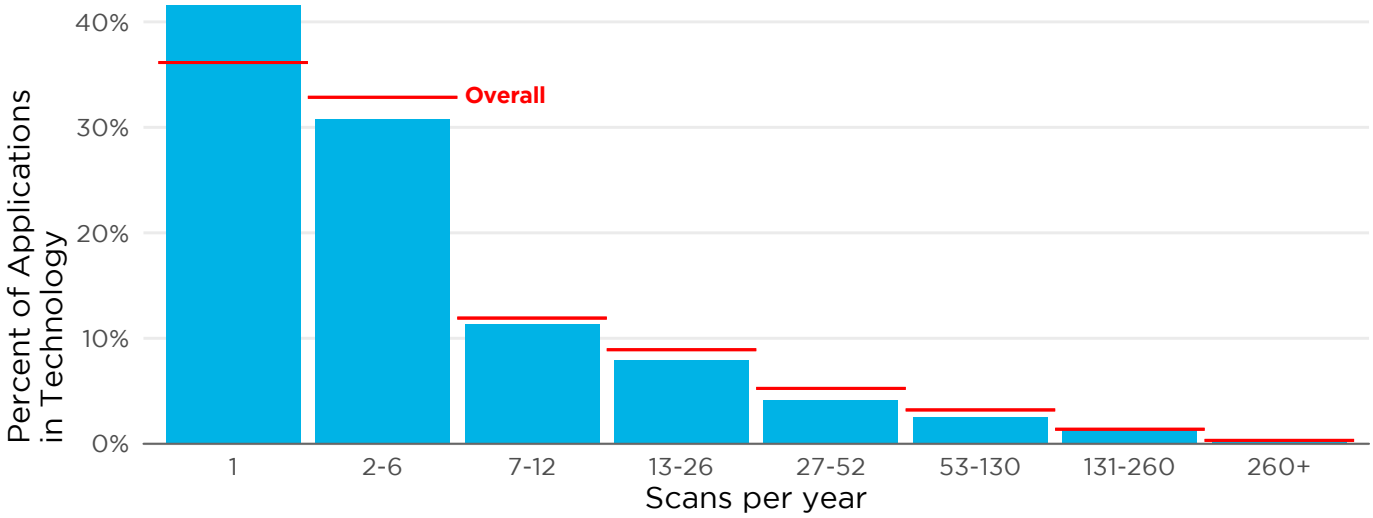
Source: Veracode SOSS Volume 10

A more detailed view of flaws discovered in 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 the Technology sector.

Despite the consistency shown by tech firms in the previous charts, the overall pattern of Figure 3 is that of increasing prevalence among the top flaw categories. In particular, issues related to crypto and credentials appear to challenge developers. This is intuitive, since many applications developed by tech firms authenticate users and collect sensitive information.

The preceding figures give us an informative snapshot of how Technology 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 Technology compare? Figure 4 has the answer.

Figure 4: Frequency of application security scanning in the Technology 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 skews a little higher for the Technology sector due to a higher-than-average percentage of one-time scans. The blue bars fall below the red overall mark in each frequency bin extending to the right, indicating that firms in the Technology sector generally scan less frequently than other industries.