VERACODE

VOLUME 11

The State of Software Security
Industry Snapshot: Technology

Veracode's State of Software Security (SOSS) Volume 11 focused on how developer actions influence software security. It also looked at the impact that application attributes (their "nature") and the development environment (the "nurturing" of the app) can have on how quickly flaws are fixed. Our analysis uncovered key differences in software security between industries and found that these differences affect how quickly flaws were addressed, adding another dimension to our "nature vs. nurture" discussion. This infosheet provides a summary of the factors that shape software security for the technology sector.

Figure 1 describes how applications compare across industries in finding and fixing flaws. From left to right, the columns rank each industry by the proportion of applications with flaws, the proportion of applications with high-severity flaws, the percentage of flaws that are fixed, and the median speed at which flaws are fixed. In this figure, the technology sector is among the poorer-performing groups for applications with any flaws and for having high-severity flaws – though it's worth noting that all the groups are fairly close to each other in absolute percentages. When it comes to fixing flaws and the amount of time spent fixing flaws, technology firms fare better, occupying middle-of-the-road rankings for both attributes. Technology firms may start off a bit behind the pack, but they are doing well at fixing flaws and managing their security debt.

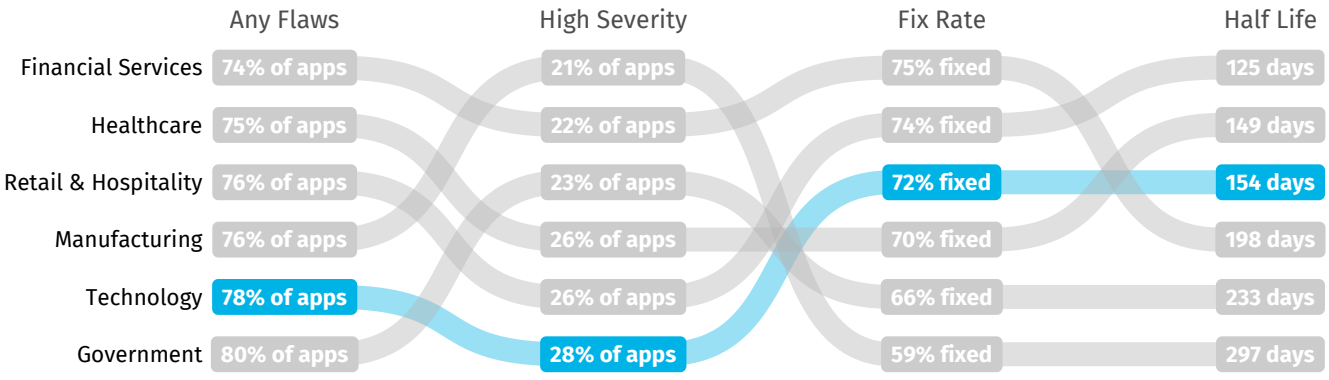

Figure 1: Values and rankings for key software security metrics by industry.

In Figure 2, we show a more detailed view of the flaw types discovered in applications. The left axis shows the overall prevalence of each flaw category across all sectors, and the right axis shows the prevalence of the category for the technology industry. This figure shows that the prevalence of these common flaw types is higher in this sector for every category compared to the overall rates. The data suggests that developers in the technology industry encounter issues related to information leakage and cryptography the most, which makes sense since many of the applications in this space collect and handle sensitive information.

In this year's SOSS, we see strong evidence that certain developer behaviors associated with DevSecOps yield substantial benefits to software security. In Volume 10, we discovered that teams scanning applications most frequently carry five times less security debt than infrequent scanners. In this volume, we see other developer actions also make a difference in fixing security flaws in software.

For example, we looked at the impact that application attributes and the development environment can have on how quickly flaws are fixed in software. There are some attributes that developers have no control over and others, such as best practices, that developers can influence.

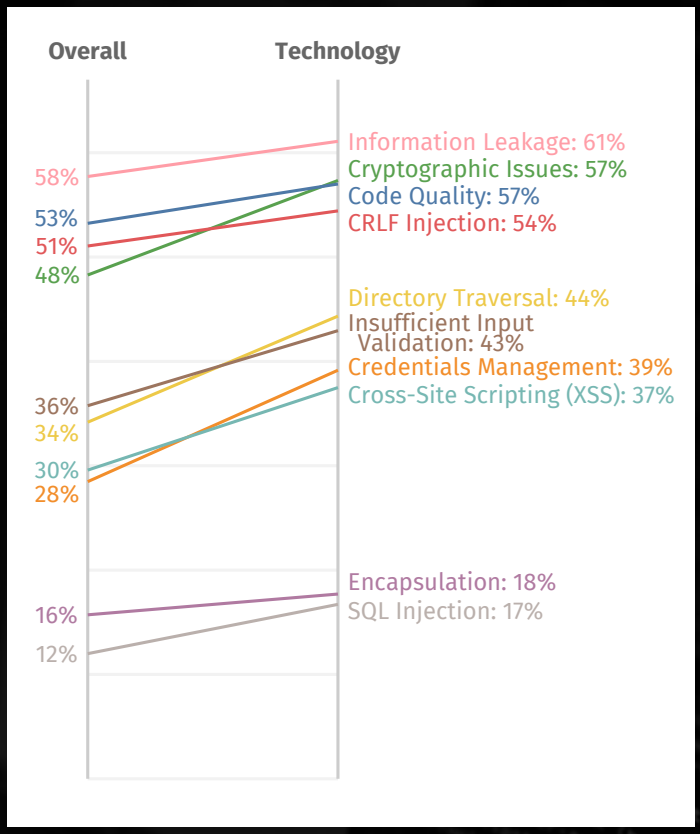

Figure 2: Prevalence of flaw categories in the technology sector

In Figure 3, we look at how technology companies compare with companies in other industries in their development attributes (nature) and utilizing helpful developer behaviors (nurture). The data shows that technology firms are all over the place for attributes. Going from left to right for attributes, technology firms in the SOSS don't have exceptionally old applications (perhaps the result of refactoring code and adopting new frameworks), tend to be smaller in size, maintain large and often complex applications, and have flaws spread throughout the application.

That makes sense intuitively, as sizes and types of applications vary widely across the technology industry. In contrast, technology firms tend to be pretty consistent in adopting DevSecOps behaviors, such as scanning frequently, using dynamic analysis, integrating security testing into the development process (using the API), and using software composition analysis. The only metric technology firms seem to rank poorly in comparison to other industries is the cadence of scanning – they are scanning frequently, but not consistently over time. There are bursts of frequent scanning over a short period of time, followed by a period of no (or little) scanning. This suggests that for many tech firms, security testing is still being saved for specific points after coding, perhaps just before a major release.

In the most recent SOSS, we see that certain factors are likely to lead to flaws getting fixed faster, and others lead to slower fixes. Industry is something developers don't have control over, so how does being part of the technology industry affect time to remediate flaws?

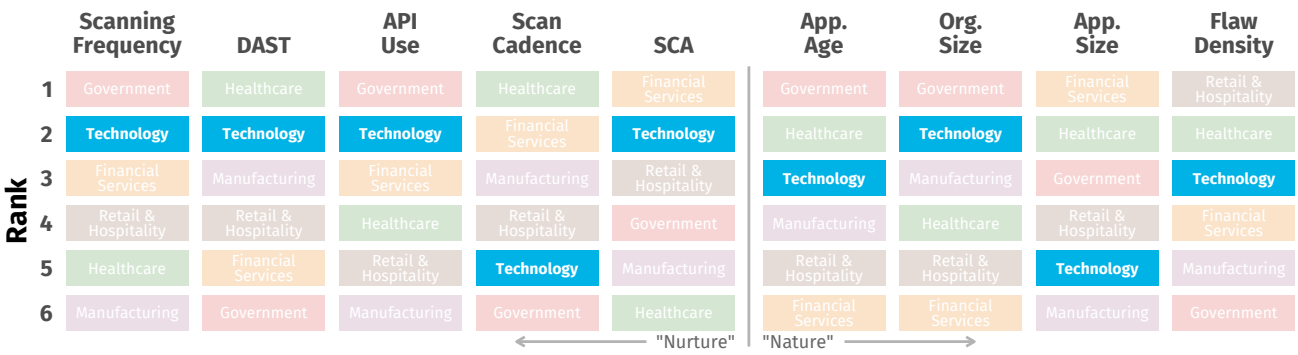

Figure 3:Relative ranking of the technology sector for attributes and actions associated with application security performance

Figure 4 shows that being in the technology industry means the firm is more likely to remediate flaws faster. Part of the reason may have to do with technology firms being more likely to frequently refactor their applications for better speed and performance, incorporating new frameworks and tools that have a side effect of addressing flaws. We see in Figure 3 that developers in technology firms utilize several DevSecOps behaviors and typically work in environments with several positive attributes. We clearly see the impact of that combination in Figure 4 as the data trends toward faster flaw remediation. It goes to show that even though developers can't control their environment, their actions can have beneficial results.

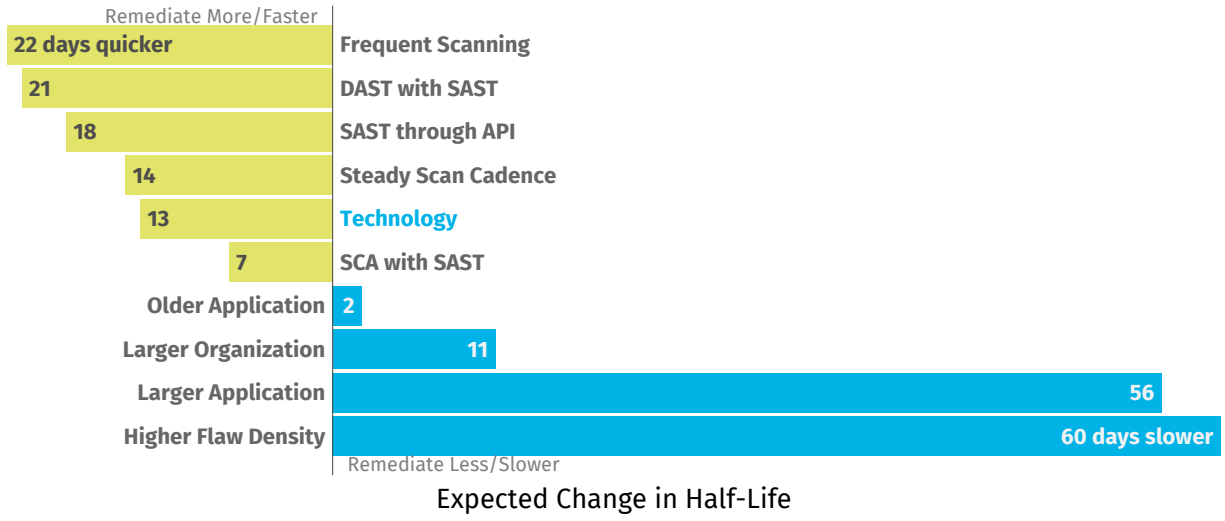

Figure 4: Remediation factors...