VERACODE

VOLUME 11

The State of Software Security
Industry Snapshot: Healthcare

Veracode's State of Software Security (SOSS) Volume 11 focused on how developer actions can 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 factors that shape software security for the healthcare 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. Healthcare has the second-smallest proportion of applications with flaws but has a higher proportion of applications with high-severity flaws. Healthcare ranks fourth in how many flaws get fixed, but second in the median time to remediate flaws. The healthcare industry deals with a large amount of sensitive information and is highly regulated, and the data suggests that healthcare organizations move quickly to address security flaws in order to keep the security debt from getting too out of hand, compared to other industries.

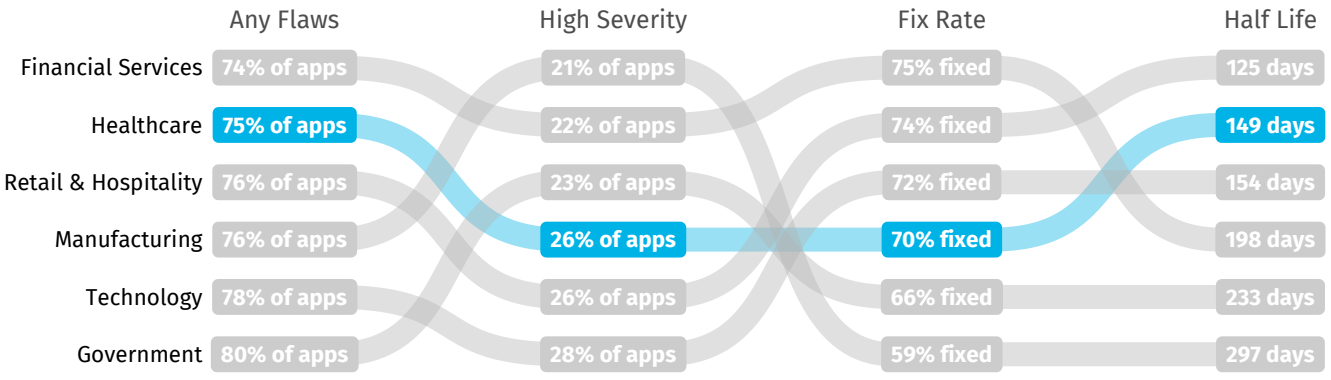

Figure 1: Values and rankings for key software security metrics by industry.

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 healthcare industry. We see some numerical shifts in this figure as the prevalence for flaw types trend lower in this sector compared to overall figures, suggesting developers in healthcare organizations do a better job handling these flaws, especially with issues related to information leakage and directory traversal. The rankings are fairly constant, and the data suggests that developers in healthcare organizations do a better job handling issues related to CRLF injection and cryptography – important things to worry about as more people rely on apps to manage their health.

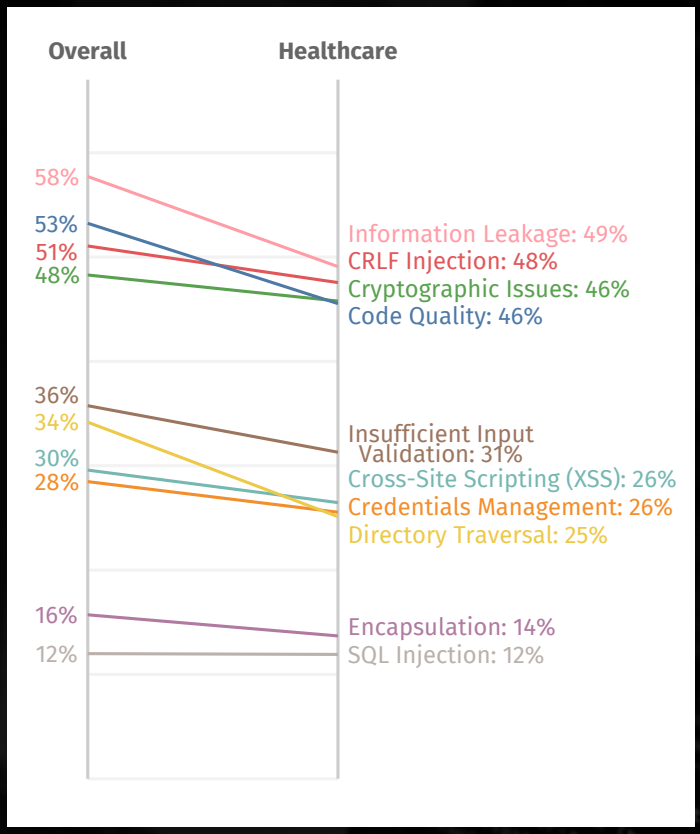

Figure 2: Prevalence of flaw categories in the healthcare sector

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 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.

In Figure 3, we look at how healthcare companies compare with companies in other industries in their development attributes (nature) and utilizing helpful developer behaviors (nurture). The data shows that developers at healthcare firms deal with a less challenging environment than other industries. Going from left to right for attributes, healthcare firms ranked second in application age, application size, and flaw density, and fourth in organization size. That means organizations may be a little on the large side, but applications are fairly new and not so large as to be unwieldy. The low flaw density means flaws are present only in certain parts of the application.

Like many organizations, healthcare firms are still trying to figure out DevSecOps, and the rankings show the adoption of secure coding best practices in healthcare firms are still uneven. Healthcare companies rank fifth in scanning frequency and fourth in integrating security into the development process. Despite scanning infrequently, it ranks first in scan cadence compared to other industries, suggesting that it is following a consistent, steady schedule of scans, most likely manually, but not frequently.

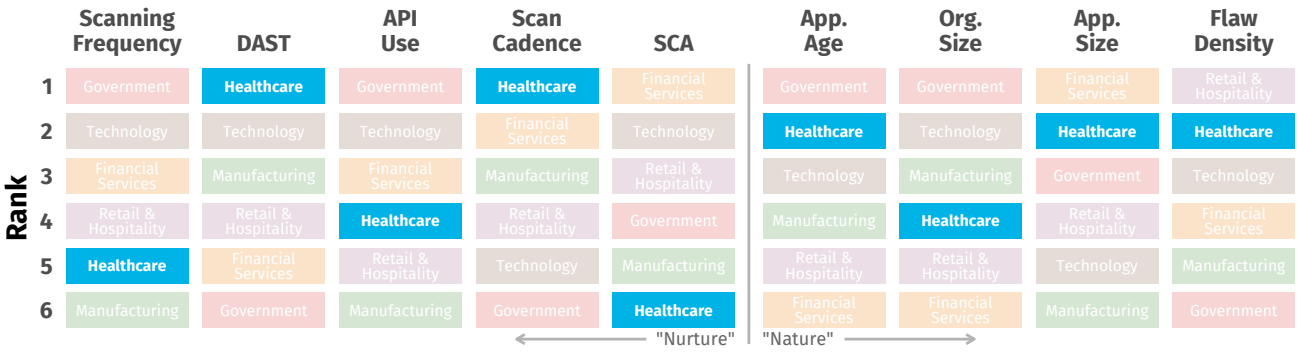

Figure 3: Relative ranking of the healthcare sector for attributes and actions associated with application security performance

Figure 4 shows us that being in the healthcare industry means the firm is more likely to remediate flaws faster. Part of the reason may have to do with the fact that healthcare firms are finding flaws they otherwise may not have found if they'd used only static analysis scanning technology. Healthcare firms are likely benefitting from the positive attributes in their environment, such as application size and flaw density. We can see how the positive attributes are helping healthcare firms remediate flaws faster and can only speculate how many more flaws would be remediated if developers changed their behaviors to integrate some of the best practices into their workflow.

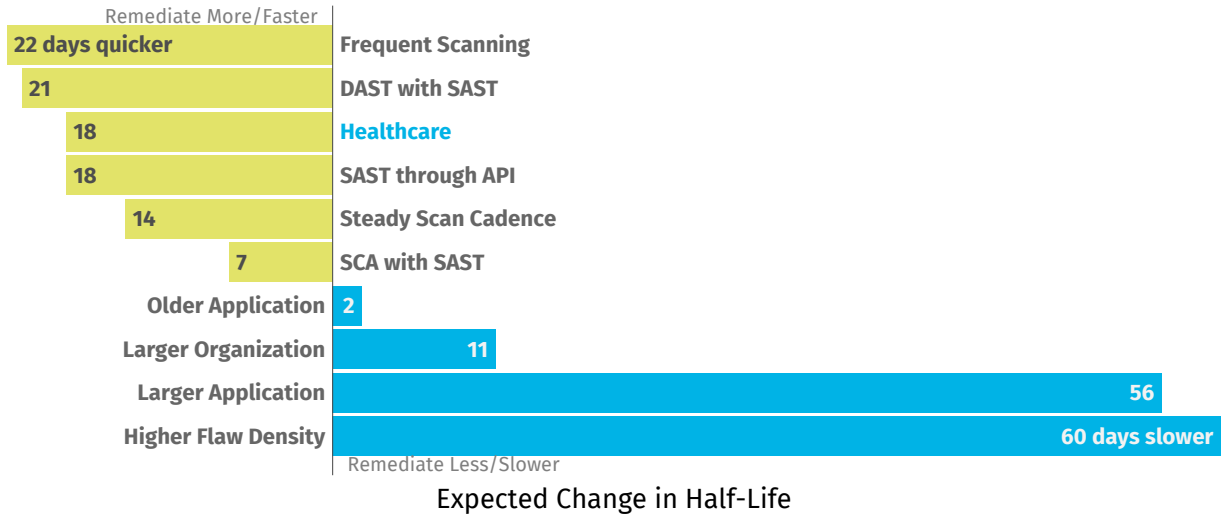

Figure 4: Remediation factors...

VERACODE

Veracode is the leading AppSec partner for creating secure software, reducing the risk of security breach and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities. Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode cloud platform has assessed more than 14 trillion lines of code and helped companies fix more than 46 million security flaws.

www.veracode.com **Veracode Blog** **Twitter**

Read the Full Report

TO LEARN MORE ABOUT SOFTWARE SECURITY, CONTACT US.