Case study

SAP uses HP Fortify to help produce secure applications

World's largest business software company relies on HP's static analysis solution to efficiently scan critical Java code

Industry
Enterprise application development

Objective
Perform static analysis on application code written in Java, C#, JSPs, and other languages to identify and remediate vulnerabilities early in the software development lifecycle

Approach
Deploy HP Fortify Software Security Center (SSC) and HP Fortify Static Code Analyzer (SCA) across the decentralized development organization and implement mandatory static analysis for application code

IT matters
- Enhanced developer awareness of secure coding practices
- In-depth training for developers on HP Fortify software tools and processes
- Eclipse plug-in to facilitate instantaneous security checks during code development
- Detailed, line-of-code guidance on fixing identified vulnerabilities
- Ability to customize HP Fortify software to meet specific customer requirements
- Expert on-site consulting to assist with pilot projects and product customization

Business matters
- Protection of SAP and its customers against software-related financial losses, business interruption, and damage to corporate brand through enhanced application security
- Reduced cost to repair as a result of identifying and remediating vulnerabilities early in the software development lifecycle
- Ability to efficiently perform static analysis on new applications and previous revisions, with more than 178 million lines of code scanned to date

"HP Fortify software is important in realizing our Product Security Strategy, because it helps us detect vulnerabilities early in the development lifecycle. This is essential for us, because the earlier we find vulnerabilities, the more efficiently we can repair them. I can definitely say that HP Fortify software has helped SAP in producing more secure code."

– Uwe Sodan, TIP Security, Engineering Excellence and Education, Code Analysis Team Manager, SAP

Strong code analysis solution

Headquartered in Walldorf, Germany, with locations in more than 130 countries, SAP AG is the world leader in enterprise software and software-related services in terms of revenue. To maintain its pre-eminent market position, SAP is committed to providing customers with the highest quality software solutions. This means going beyond simply ensuring that applications perform as designed, by integrating risk and security management into the development part of SAP's Idea2Market (I2M) process. HP Fortify software is a key element in this program.

SAP's Product Security Strategy mandates static code analysis during product development to help ensure that all applications are secure and resilient against cyber threats, thereby protecting customers—and the company itself—against financial losses through software malfunctions, loss or damage of intellectual property, or business interruption. SAP uses its own static analysis tool for applications written in the proprietary ABAP language; but for Java, the most common programming language at SAP after ABAP, the company decided to leverage third-party expertise. SAP chose the industry leader and has now fully integrated HP Fortify software into its development lifecycle.

The HP solution stays busy. "I estimate that we have around 80 million unique lines of Java code," says Uwe Sodan, TIP Security, Engineering Excellence and Education, Code Analysis Team Manager at SAP. "Furthermore, because we need to maintain older versions of many applications, we often scan a given product multiple times. We always scan the newest version, of course; but whenever we find something that needs to be repaired, we need to consider how many older versions also require the fix." As of 2012, SAP had performed static analysis on approximately 178 million lines of code using HP Fortify software.

HP Fortify at work

At SAP, static code analysis of applications written in Java, C#, JSPs, and a number of other programming languages has been designed and implemented together with HP Fortify and is based on the HP Fortify Software Security Center (SSC) and HP Fortify Static Code Analyzer (SCA) solutions.

HP Fortify Software Security Center helps leading organizations to manage security risk by ensuring that software—whether it is built for the desktop, mobile, or cloud—complies with internal and external security mandates. With advanced static and dynamic security testing capabilities and an integrated framework for proactive security management, HP Fortify SSC helps to identify and mitigate risks within the development process and legacy applications and throughout the entire software development lifecycle. Although SAP's development groups are decentralized, the company can consolidate and track all results within HP Fortify SSC.

HP Fortify Static Code Analyzer is part of the HP Fortify SSC solution and uses award-winning static analysis to provide far-reaching vulnerability detection in source code. HP Fortify SCA pinpoints the root causes of security vulnerabilities in source code, prioritizes results sorted by severity of risk, and provides detailed, line-of-code guidance on how to fix vulnerabilities. HP Fortify SCA helps organizations ensure that their software is trustworthy, reduce the cost of finding and fixing application vulnerabilities, and establish a foundation for secure coding best practices.

"We have a central group at SAP that is responsible for product security standards," explains Sodan. "Our Product Security Strategy is targeted at enabling our decentralized development teams to create secure products through central guidance; the security requirements are part of the nonfunctional requirements that are centrally collected, maintained, documented, and rolled out. We have testing measures throughout the development lifecycle, and static analysis is mandatory. For this reason, HP Fortify software is an essential component of our business success."

Support from HP Services is a valuable part of the overall solution. "We leveraged the expertise of on-site resident consultants for two years, and that was very helpful to us," says Sodan. "They taught my team to understand the HP Fortify software, not only in terms of the tool, but also in terms of processes." SAP continues to use HP Fortify consulting services for help with specific projects. "They recently helped us with two pilot projects, which were challenging in the amount of findings and the architecture," Sodan continues. "We also plan to provide some dedicated Custom Rules training, working with members of HP Fortify's security research team. These are really in-depth experts, and we continue to learn a lot from them."

Good things

Asked what he values most about the HP Fortify software, Sodan identifies a number of positive features. "For one thing, it has very good security coverage," he says. "It also comes with collaboration capability in the HP Fortify Software Security Center that is important for us. We want a central infrastructure where we can store all the scan results, in order to protect the data and control the access to it; at the same time, we want to have it deployed in such a way that the different development teams can easily work on the results. HP Fortify software fits our development model very well."

Another significant advantage is the ability to configure HP Fortify software to meet specific customer needs. "This covers both the sorting and prioritizing of results, as well as tuning," explains Sodan. "Using the Custom Rules feature, we can create our own rules and modify the behavior of the tool to adapt it to our proprietary libraries, interfaces, platforms, and frameworks." As developer efficiency is one of SAP's primary goals, the HP Fortify solutions have been enriched with SAP custom rules and fix recommendations. Sodan adds that good documentation on how to interpret findings, coupled with detailed guidance on fixing vulnerabilities, further enhances the value of HP Fortify software in the SAP development environment.

A driving factor in the use of HP Fortify software is the need to comply with SAP's Product Standard Security Requirements. "All software must avoid cross-site scripting, SQL injection, path traversal, memory corruption, XML entity, buffer overflow—the list goes on and on," says Sodan. "We also typically refer to the OWASP Top 10 and the CWE/SANS Top 25 vulnerabilities. This is the scope we cover using static analysis, and any SAP product must be free of these vulnerabilities. We count on HP Fortify software to help us meet these stringent requirements, protecting both our customers and our corporate brand." Even as threats become more sophisticated and targeted, static code analysis enables SAP to stay ahead of the game by identifying and mitigating vulnerabilities before they can be exploited.

Customer solution at a glance

HP Solution

- HP Fortify Software Security Center (SSC)
- HP Fortify Static Code Analyzer (SCA)

HP services

- On-premise training and consulting services

Fix it early

SAP has fully integrated HP Fortify software into its development lifecycle and, while hard metrics are not yet available, the cost benefit is clear. "The most expensive fixing is when a bug makes it all the way into production, and a customer or an external security expert reports it back to us," says Sodan. "According to different studies, the cost of fixing vulnerabilities in already-released software versus during the development lifecycle is a ratio of about 100 to 1. This is why we consider it so important to check our code as early as possible."

Nearly a thousand developers at SAP are active HP Fortify software users. "It's not every Java developer, but we target at least one or two in each development team," explains Sodan. The Eclipse plug-in for HP Fortify SCA is especially useful in this environment. "This plug-in enables developers to perform instantaneous checks, so they can improve the code directly in the process," says Sodan. "I also like the integration between the plug-in and the central server; once people understand how it works, they can use the scan results directly in their normal development environment. That's a good thing."

SAP has a comprehensive security response feedback process. Any potential vulnerabilities that are reported externally are fixed as part of the security response process; then, an additional feedback step analyzes the vulnerability pattern to determine whether it can be detected using static analysis. If the answer is yes, and if the affected code is in Java or one of the other languages for which SAP uses HP Fortify, a root cause analysis investigates whether the vulnerability was not yet in the scope of the scan or if some adjustment to the tool is needed. This feedback process enables SAP to continuously adjust and optimize its usage of HP Fortify software.

"In terms of the number of different programming languages that HP Fortify covers, as well as the number of different check categories corresponding to vulnerability types or patterns, I think the solution is quite complete," concludes Sodan. "HP Fortify software is important in realizing our Product Security Strategy, because it helps us detect vulnerabilities early in the development lifecycle. This is essential for us, because the earlier we find vulnerabilities, the more efficiently we can repair them. I can definitely say that HP Fortify software has helped SAP in producing more secure code."

Learn more at
hpenterprisesecurity.com

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document