MICRO FOCUS

Customer Success Story

Security

# Acxiom

Acxiom boosts application security with Micro Focus® Fortify Static Code Analyzer. This leading data technology company leverages automated static code analysis to protect consumer information.

## Overview

Acxiom is a data technology company that works to enhance the targeted marketing capabilities of its clients—whether the marketing takes place via television, e-mail, Web-based advertising, or postal campaigns—by helping provide a strong, clear, immediate view of their end customers. Given the nature of its enterprise analytics business, the company is a particularly attractive target for hackers, and it explains why Acxiom works so hard to keep pace with evolving data security technology. IT Security Engineer Brenton Witonski runs the application security program for static code scanning within Acxiom's development engineering group. Part of the solution he relies on for this critical task is Fortify Static Code Analyzer (SCA), in conjunction with Micro Focus Software Security Center (SSC).

"We have always been at the forefront of ensuring data privacy and data security are in place at Acxiom and in our industry," says Witonski. "Acxiom works closely with key policy makers and regulators worldwide, pioneering innovative privacy solutions that have created the foundation for what are now standard practices in many industries. The emphasis on security and privacy at Acxiom is extremely high; where other companies need to fight to get their board engaged, Acxiom's board is regularly briefed and fully supportive of the overall security initiative. For instance, Acxiom was the first company in the world to appoint a chief privacy officer more than 20 years ago. Everything from physical security to software security and data privacy is taken extremely seriously."

## Challenge

As industry awareness of overall security risk grows, Witonski notes that static code analysis is becoming an increasingly critical tool in protecting applications and, by extension, the people who use them. Acxiom implemented Fortify SCA in November 2011. "We did a lot of research and looked at several different solutions," Witonski recalls. "But given Fortify's reputation, it was a no-brainer." In addition to the inherent capabilities of the solution, a key factor in the purchase decision was Acxiom's excellent relationship with Micro Focus through the years; the company was already using Micro Focus WebInspect for dynamic penetration testing with great success, as well as Micro Focus Application Lifecycle Management (ALM).

At first, Witonski and his team created PDF scan reports from Fortify SCA's Audit Workbench and sent them out to the developers, who worked off the reports to identify and resolve issues; subsequent screenings were then performed to get the releases out the door without material

acxiom

## At a Glance

- **Industry**
  Business Services
- **Location**
  United States
- **Challenge**
  Further enhance Acxiom's comprehensive security program by implementing static analysis of source code for key applications.
- **Products and Services**
  Fortify Static Code Analyzer (SCA)
- **Results**
  + Reduces risk—significant reduction in application vulnerabilities enhances the protection of consumer information and reduces the company's risk
  + Saves money, identifying and resolving issues early in the lifecycle with Fortify SCA is much more cost-effective than finding vulnerabilities post-release
  + Stays ahead of the bad guys; regular static code analysis helps the company stay one step ahead of increasingly sophisticated attack vectors

issues or vulnerabilities. Over time, Micro Focus SSC became the hub for vulnerability identification and analysis. Most recently, the team has started automating the process by integrating the security component into the Continuously Integrated Build Process (CIBP).

"CIBP is our internal build process for continuous delivery automation," Witonski explains. "When a developer checks in code, CIBP can automatically pull that code, create a build and compile, run metrics, perform a security scan, send the code to the delivery environment, and optionally kick off regression testing. Fortify SCA fits right into that process—we simply added a security module to CIBP to say, 'OK, at the time of the build we are also going to do a scan.' Essentially the developers can initiate their build, and within 10 to 20 minutes they can go to SSC and see the scan results. Fortify SCA is now fully integrated into our software development lifecycle."

## Solution

### Across-the-Board Value

When Witonski stood up Fortify SCA initially, he was surprised at the number of issues the first scan revealed. "It's always impressive to see what the tool shows us," he says. "It's like waiting for that gift on Christmas morning; you're like, 'What am I going to open up and see?' It's exciting to me as a security professional, because when I see the vulnerabilities that the tool has found— vulnerabilities that the natural process of development cannot find—it validates what we're doing. It is very satisfying that potential vulnerabilities are resolved before the release goes out."

There will never be a shortage of vulnerabilities, given the ever-changing threat landscape. "It is definitely an arms race when it comes to security," Witonski continues. "You've got the hackers and you've got the preventers, and the hackers are always finding new ways to attack. One of the values that Fortify brings is the ongoing research behind it, and the new rule packs we consistently receive to help us stay ahead."

Another key value is developer education. According to Witonski, one of the benefits of the Fortify software is the way it identifies each issue, provides a detailed description, and recommends ways to resolve it. "It is an important self-education opportunity, and I definitely see in subsequent development that the same issues are not being created as often," he says. "The developers and engineers are growing in their ability to program in a secure way, being able to identify 'Oh, that's what an SQL injection error issue is,' or 'You're right, I should not have a hard-coded password there.' As they learn over time to create more secure code, it's better for Acxiom and for the development staff as well."

Fortify SCA's broad language coverage is also important. In his engineering group, Witonski deals with more than 50 applications, consisting of hundreds of components, written in multiple languages, including Java, .NET, C++, and JavaScript. "The language coverage is essential, because if we were not able to scan all the different types of code, then obviously we would have a security gap," he says. "It is critical that both legacy and current source codes are covered. And as new codes are created and become prevalent, I feel confident that [Micro Focus] will continue to expand Fortify coverage to include them."

## Results

Has Fortify SCA made a difference at Acxiom? According to Witonski, the answer is an unequivocal "Yes." "The obvious benefit is the overall improvement in our security," he says. "We are able to identify and resolve issues before they get out into production, so we are definitely improving security across all our products." The visibility that Fortify SCA provides into Acxiom's software is also important. This visibility enables Witonski to see what types of vulnerabilities may be present, the frequency of the vulnerabilities, and the improvement over time in terms of producing secure code.

Another key benefit is efficiency. "We can identify, analyze, and resolve our issues far more efficiently with Fortify SCA than we ever could before," continues Witonski. "Without a tool like this, we would need a manual, labor-intensive, security code review process to analyze hundreds of thousands of lines of code, identify the issues, and communicate those issues to development for remediation. Fortify SCA allows us to identify and resolve these issues far more efficiently."

Fortify SCA makes it possible to find and resolve vulnerabilities early, and that's a good thing according to Witonski. "Within your development lifecycle, the closer you get to release, the more expensive and the more time-consuming it becomes to resolve any issues that are found," he says. "Now you're talking about opening tickets. The developer may already have moved on to another project, so he or she has to be brought back to work on the fix. The code has to be rebuilt, and all the testing has to be redone. There's a good chance that you will impact the release schedule, which could have negative consequences for the end customer. By contrast, if you can identify a security issue in the code during the normal development phase and fix it as part of the standard process, the cost is minuscule by comparison."

### Looking Forward

What does Witonski see coming at him in the future? One thing is sure: The security challenges will not abate. "I see that the vulnerabilities I'll be looking for and fighting against next year will be some that we face today, plus a whole new set of things that we can't even predict," he says. "It is a constantly changing

> "We can identify, analyze, and resolve possible issues far more efficiently with Fortify Static Code Analyzer than we ever could before."
>
> **BRENTON WITONSKI**
> IT Security Engineer
> Acxiom

Contact us at:
**www.microfocus.com**

landscape, with smarter adversaries and more sophisticated attacks. I think the result will be that many more companies and clients will require static code analysis as an integral part of contractual obligations and internal practice. Compliance bodies—the Payment Card Industry, or PCI, is a good example—will likely tighten their source code security requirements as well."

Fortify SCA is a powerful ally in the hard-fought and escalating battle against the hackers. "Being able to deliver applications that are more secure makes Acxiom a better software company," Witonski concludes. "We work extremely hard to ensure the highest levels of security, and Fortify has enabled us to add one more element to our overall program."