



Start Secure. Stay Secure.™



End2End - No Security Disconnect Here

CASE STUDY

How one of the world's largest managed service providers of mobile data and content services mitigated its software development risk-and slashed the time it took to spot Web application vulnerabilities from days to minutes.

Background

Mobile content and information services are ringing sales. More businesses than ever are delivering wirelessly-enabled applications and services as the thirst for more services and information targeted toward smart phones and wirelessly-connected PDAs parallels the sales of these devices. Consumer demand for mobile data services also grows unabated, with spending, according to the Yankee Group, of \$111 billion for mobile services last year. Nearly \$6 billion of that was for wireless data services, a figure that Yankee anticipates will reach \$14 billion within two years.

And End2End Holdings Ltd. is in the thick of it. The European-based business-to-business managed services provider's reach for mobile data and services and content extends from New Zealand to The Americas. Its unique service delivery infrastructure hosts, manages, and delivers to mobile operators, portals, media companies, and other content providers the ability to launch custom mobile data services and content. The company helps power the mobile data delivery needs for more than 55 mobile operators in 20-plus countries. Its customers include Lycos Mobile, MSN, Sony NetServices, and Vodafone.

Through its ability to decrease its customers' capital expenditures on development and content development by 60 percent, End2End makes it possible for clients to quickly reach ROI on their mobile data initiatives. One of the most critical aspects of End2End's capability to do just that exists within its ability to create applications that are both highly available and secure.

Manual Testing Processes and Tools Proved Troublesome

As part of its services, End2End provides an application and services platform CDS (Content Download Solution) for each of its customers. The platform consists of a download engine, a content management system, a customer care and administration module. The platform runs on either BEA WebLogic or Apache. The company is increasingly adopting the Agile principle of code development, which attempts to mitigate risk through the development of software in short time spans called iterations, in which mini-increments of large applications are produced within a few days or weeks and tested. According to Jes Beirholm, information security manager at End2End, each iteration, which can be considered a software project in itself, undergoes stringent quality assurance and security testing.

Until last year, the company's development team relied heavily on manually testing its iterations with a handful of both commercial and open source security and quality assurance testing tools. But the process wasn't proving as effective as Beirholm needed. For instance, the reporting capabilities of the tools varied greatly, and they provided inconsistent results in how they described identical flaws and the potential development problems they uncovered. This, explains Beirholm, forced team members to waste enormous stretches of time as they combed through the various reports to normalize test results for reporting. In addition, the number of false-positives these tools reported "created even more work" as the team labored to determine if they were just looking at "ghosts" within the results, or if their tools uncovered real software issues that needed to be remedied.

"These tools would simply collect banner information and "shout" vulnerabilities at us, simply because we were running Apache, or whatever application, as part of the project. Too many times, the vulnerabilities they 'found' just didn't exist," he says.

Of course, that's too much waste for a company that's growing and constantly on the move. Just this past spring, End2End rolled out a local delivery infrastructure in the U.S. to provide more robust mobile delivery capabilities in North and South America. Since at any time, the company's development team can have 50-plus software iterations underway, "our team has to be able to move very quickly, very dynamically, and follow a continuous life-cycle of application development," says Beirholm.

That's why it was crucial that the company find a more effective way to find and fix security flaws as part of its application development process. While Beirholm and the company's team of developers were able to develop secure and available applications and services, "we were missing the ability to provide and monitor our security controls effectively," he says. "It's a question of having tools that probe for the right things, and verify actual vulnerabilities in an intelligent way."

Efficient, Accurate Security Testing Through WebInspect™

To find those tools, Beirholm surveyed the market and turned to FortConsult. That's when he learned more about SPI Dynamics and its WebInspect product, which "encompassed the features we need to conduct our risk-based testing," says Beirholm.

Beirholm says WebInspect provides the testing "richness" needed to assure that End2End is delivering to its clients the most secure applications and services possible. "That's one of our goals, and we know that we get to this level of quality with WebInspect," he says. Much of that quality is derived from SPI Dynamics' SecureBase -the world's largest and most comprehensive database of application-layer vulnerabilities. SecureBase contains 4,400-plus unique Web application vulnerabilities, threats, and security checks, compiled by SPI Labs.

It didn't take long before WebInspect became a vital part of End2End's development process. Beirholm says the sheer number of tests WebInspect is capable of conducting, and the fact that it's continuously updated to be able to spot both known and unknown vulnerabilities within the Web application layer, is "very, very vital for us. WebInspect has given us the ability to go the extra mile with our security efforts. While in the past we would have found potential security issues, without the help of WebInspect we weren't able to resolve such issues efficiently."

The automated testing, accuracy, and depth of WebInspect has slashed the enormous amount of time that it used to take the company to find and verify security flaws. Prior to deploying WebInspect, testing took about a week to ferret through potential vulnerabilities, classify their severity, and verify whether they were "ghosts" or actual weaknesses that needed to be remedied. "Today that's done in about 20 minutes of scanning and application exploration with WebInspect. That's a very, very big gain on ROI."

"When talking about security and automated security tools, one of the biggest enemies is the false positives. The amount of knowledge that you need to be able to go into depth of analyzing the false positives to verify requires a high level of expertise, but it is also extremely time consuming," says Beirholm. "The drop in false positives has meant a great deal to us," he adds.

Because End2End tests its applications as often as twice a month, even after they've been deployed into production, the newfound efficiency has made it easier for the company to remain proactive when it comes to the development of its Web applications. "With WebInspect, we're able to make sure that we stay ahead of potential security issues and that our customers are provided the most thoroughly tested services and applications possible," says Beirholm.

That's critical, because each year End2End's clients conduct customer-based audits that detail End2End's development and security process and procedures. "When we discuss application development with our customers, security questions always come up," he explains. Those questions are answered in part by End2End's thorough use of WebInspect as a critical component of its risk management process. "That's what they want to see verified when they do audits," he says.

For application development management and testing, End2End relies on Mercury TestDirector and QuickTest Professional. Beirholm says he soon will integrate WebInspect with his Mercury applications. That combination will give End2End a common platform to conduct its security and application quality testing. By centralizing Web application and security testing, the company's development team will attain even higher levels of effectiveness.

While the need to build speed, accuracy, efficiency, and security into the development process exists for any company, it's especially critical for a nimble and fast-growing company such as End2End. "Efficiency is the name of the game here," says Beirholm. "We couldn't be market leaders without the aid of automated testing tools like WebInspect."

