



CASE STUDY

Human Services Organization Harnesses Fortify SCA

THE ORGANIZATION | The New York State Office of Temporary and Disability Assistance (OTDA) is responsible for supervising a wide range of programs that provide assistance and support to eligible families and individuals. These programs enhance the economic security of low-income working families, assist work-capable public assistance recipients in achieving entry into the workforce, assist individuals with priority needs other than work-readiness in accessing appropriate benefits and services, enhance child well-being and reduce child poverty.*

THE CHALLENGE

New York, the Empire State, is the third largest state in population. The volume of residents who require the types of assistance OTDA programs provide is also considerable. These program services are administered by local agencies across the state—including the New York City area. To better serve these agencies and constituents, OTDA application initiatives have leveraged the efficiency and accessibility of the Internet.

Web-based applications can pose significant information security risk for organizations. Ninety percent of the programs OTDA manages require the collection of private, personal and sensitive information (PPSI), such as Social Security numbers. Other agency applications support the transfer and disbursement of funds. Data and money represent the perfect targets for cyber criminals.

OTDA must also comply with myriad federal and State information security mandates, including the Federal Information Security Management Act (FISMA), the New York State Information Security Breach and Notification Act and New York State Cyber Security Policy.

“Information security risk management is a critical component of our agency’s strategic goals, policies and processes,” said OTDA Information Security Officer (ISO), Deborah Snyder, “We go to great lengths to ensure every member of our workforce understands that handling and protecting PPSI properly is part of their individual, everyday responsibilities.”

Security as an Integral Component of Software Development

In the past, OTDA did not have a standard protocol for their development teams to follow in building security into agency applications. Recognizing that her agency could do more to identify and manage software security risk, Snyder had the foresight to implement a Secure System Development Lifecycle (SSDLC) process roadmap. Through the joint efforts of the ISO and IT, development teams received specialized training and guidance on security threats, mitigation controls, secure coding principles and code analysis and testing practices. OTDA is currently implementing a standards-based secure development and assurance process that all applications must follow to be approved for production. The use of code scanning tools and code reviews are key features of this mature, risk-based process.

Building Security In

OTDA evaluated a number of code-scanning solutions and selected Fortify products to support automated security testing based on their fit with agency technical requirements. “Fortify stood out because it offered a full suite of products that enabled OTDA to implement a comprehensive application security strategy,” said Snyder.

Factors considered included a large and complex code base, multiple applications and development methodologies, Internet-facing business objectives; secure system development life cycle and enterprise architecture initiatives, and the desire to automate source code security scanning and analysis tasks. The intuitive nature, ease of use, analysis speed and developer feedback and education offerings provided by Fortify were key to developer acceptance and adoption. The reinforcement of secure coding principles and practices, ability to identify and address vulnerabilities early in the development process, security risk metrics and reporting features garnered management support. Fortify’s clear commitment to customer feedback and support, and willingness to work with our implementation and development teams to successfully implement these tools in our development environment, also stood out as an added value.

*For more information, see <http://www.otda.state.ny.us/main/programs.asp>

“Fortify stood out because it offered a full suite of products that enabled OTDA to implement a comprehensive application security strategy.”

— *Deborah Snyder*
OTDA Information
Security Officer

OTDA development staff uses Fortify Static Code Analyzer (SCA) to routinely evaluate existing and in-development code to identify potential security vulnerabilities. Earlier and more efficient code remediation enables OTDA to quality assure and deploy secure applications that meet the needs of their users and constituents more securely and with less time. Time-consuming manual code reviews are a thing of the past. Fortify SCA provides 100% line-of-code (LoC) coverage for reviewed applications throughout the SSDLC. With consistent, accurate reviews and virtually all instances of reported issues detected, the resulting application code presented to review teams is cleaner with no coding issues. Fortify’s Real-Time Analyzer (RTA) will help OTDA monitor and protect Web applications while remediation is underway.

Utilizing Fortify as part of their SSDLC has also helped OTDA to achieve compliance with federal and state security-related mandates requiring secure development processes, routine reviews and vulnerability assessment.

The resulting increased levels of security are helping OTDA assure PPSI is properly safeguarded and providing increased peace of mind for the agency and its constituency.

Deploying a Runtime Application Shield

OTDA will also protect applications in production using Fortify’s Real Time Analyzer as an effective means to shield applications until they have undergone in-depth source code review. With RTA in place, OTDA can automatically identify critical Application Programming Interfaces (API) within the application and insert guards into the bytecode at these locations. Once an application has been deployed, OTDA can monitor activity and respond in a variety of ways, including blocking the user entirely, posing a challenge response question, alerting a key administrator or performing more sophisticated actions such as communicating with a router to delay the user’s requests.

About Fortify

Fortify Software’s Business Software Assurance solutions protect companies and organizations from today’s greatest security risk: the software that runs their businesses. Fortify reduces the threat of catastrophic financial loss and damage to reputation as well as ensuring timely compliance with government and industry mandates. Fortify’s customers include government agencies and Global 2000 leaders in financial services, healthcare, e-commerce, telecommunications, publishing, insurance, systems integration and information technology. For more information please visit us at www.fortify.com.



FORTIFY SOFTWARE INC.

MORE INFORMATION IS AVAILABLE AT WWW.FORTIFY.COM

2215 BRIDGEPOINTE PKWY.
SUITE 400
SAN MATEO, CALIFORNIA 94404

TEL: (650) 358-5600
FAX: (650) 358-4600
EMAIL: CONTACT@FORTIFY.COM