Rational. software

IBM

# DTCC leverages IBM Rational AppScan software to help protect its financial transactions.

## Overview

- ***Challenge***
  *To create security-rich applications that could handle the clearance and settlement of more than US$1 quadrillion in securities transactions per year, DTCC needed to implement rigorous security practices as part of its application development process.*
- ***Solution***
  *DTCC educated its application developers on building security into the Web application development lifecycle, and the company leverages IBM Rational® AppScan® software to identify, analyze and remediate security issues from early development through live deployment.*
- ***Key Benefits***
  *DTCC is able to perform automated security, compliance and integration testing on its Web-based applications, while adding 225 new applications per year, improving its developer productivity and speeding time to market for new applications.*

The Depository Trust & Clearing Corporation (DTCC) provides custody and asset servicing for more than 2.5 million securities issued from the United States and 100 other countries and territories. In addition, DTCC is a leading processor of mutual funds and insurance transactions, linking funds and carriers with their distribution networks. The company employs approximately 450 application developers to create products for its customers, who include brokers, dealers, institutional investors, banks, trust companies, mutual fund companies, insurance carriers, hedge funds and other financial intermediaries.

To create security-rich applications capable of handling the clearance and settlement of more than US$1 quadrillion in securities transactions per year, DTCC needed to implement rigorous security practices as part of its application development process. Attacks against organizations storing confidential personal and financial information are on the rise—plus, they are becoming increasingly sophisticated. Because DTCC creates and modifies so many Web applications each year, it quickly became critical that the company implement comprehensive Web application security vulnerability testing practices—particularly for projects determined to have a high security risk.

DTCC sought to deploy an information security program across its entire organization. The company's corporate information security (CIS) department recognized that sound security practices required not only the right technology, but also an education program to help developers and users better understand how to protect and secure company assets.

***DTCC leverages IBM Rational AppScan software to help protect its financial transactions.***

**Key Components**

*Software*

- *IBM Rational AppScan*

### Turning to IBM

The CIS group began by recruiting security team leaders for each development team across the company's different development platforms; then the group provided those leaders with six weeks of training on security-rich application development. Once the training was complete, the team leaders rejoined their teams as security experts, passing on best practices, coaching and support.

To identify application security issues and report them to the development team for remediation, the CIS group needed to deploy a vulnerability management tool. Jim Routh, chief information security officer (CISO) at DTCC, found that AppScan software provided the functionality the company needed. "We did very thorough, extensive and competitive analysis of secure application development and vulnerability assessment tools, and use them as the cornerstone of our information security practice," he explains. "AppScan was chosen because it really met all our requirements nicely, and we'd also gotten good results from using it in the past."

AppScan software helps address the security and compliance of Web applications throughout the software development lifecycle. DTCC uses AppScan to scan its Web applications, test for security issues and develop actionable reports and fix recommendations. The application also helps the company maintain confidence in its production environments by providing continuous auditing for known vulnerabilities and by reporting on compliance-related issues. The scanning capabilities of AppScan, combined with its advanced remediation recommendations and a comprehensive reporting system, help simplify ease of use. As a result, DTCC has been able to enhance developer and security team productivity, facilitate security compliance management and protect its Web application infrastructure.

"We turned to AppScan as our tool of choice for end-to-end security vulnerability assessment of the applications and code for high-risk applications," says Routh. "That assessment was conducted by a dedicated team of integration testers addressing high-risk and complex applications. AppScan is so comprehensive in its ability to identify and help remediate vulnerabilities that it serves as an industrial-strength assessment tool for our corporate information security team to oversee the secure application development process."

*"AppScan is so comprehensive in its ability to identify and help remediate vulnerabilities that it serves as an industrial-strength assessment tool for our corporate information security team to oversee the secure application development process."*

*—Jim Routh, CISO, DTCC*

**Facilitating better integration testing**

DTCC also leverages AppScan vulnerability assessment capabilities to automate advanced integration testing. Some of the company's Web-based applications pull files off a database server, either the company's mainframe or another server, and leverage those files to complete the workflow of the application. Such integrations are critical to the company's operations, yet are often difficult to scan for vulnerabilities. AppScan enables DTCC to perform Web application vulnerability security scanning by performing real-world usage tests, checking for vulnerabilities where application code is used by multiple products, and monitoring Web-based service interactions.

"The security and reliability of our product is what DTCC's business and reputation are dependent upon, so our focus was first upon how to make our application developers smarter and more skilled in information security as it applies to application development," comments Routh. "When first implementing vulnerability management, if it's done properly you'll actually find more vulnerabilities over time. The numbers don't decrease, because that's part of the maturity curve. Eventually the vulnerabilities do go down, as they have now for us. But the real key is that we have the education in place and now implement security early in the application development lifecycle, so we have less overall vulnerabilities to manage."

> *"The real key is that we have the education in place and now implement security early in the application development lifecycle, so we have less overall vulnerabilities to manage."*
>
> *—Jim Routh, CISO, DTCC*

**Tailoring education to each employee**

So far, Routh finds that the company's efforts are paying off. "My perspective is that one of the most strategic tools a CISO has is education and awareness," Routh states. "We implemented employee education and awareness to teach them that any network access, Web use or device connecting to the DTCC network can have security risks or vulnerabilities—or be compromised. The more knowledge people have on best practices and the implications for information security, the better their decision-making ability, and the easier my job becomes."

> *"The more knowledge people have on best practices and the implications for information security, the better their decision-making ability, and the easier my job becomes."*
>
> *—Jim Routh, CISO, DTCC*

Every person in the company required different levels of and approaches to training, depending on their job and day-to-day business functions. In the process of educating key stakeholder groups within DTCC, the CIS team recognized that application developers had the greatest need for education. Like many organizations, DTCC had devoted a lot of time to addressing its perimeter security, but it had done less to address potential application vulnerabilities.

"My charter mandate for the application development security program, and the foundation of our entire information security program, was not just to better secure our code, but to better educate all 450 application development professionals on best practices for creating secure applications, and apply information security controls throughout the entire application development lifecycle," says Routh.

With the developers better educated and now building increasingly more security-rich code, DTCC is realizing impressive value from its AppScan software investment. And the application provides even more value for DTCC's systems integration group, which uses AppScan to perform security testing across platforms in a specialized way, creating a kind of derailment tool the group can use to test DTCC's most critical applications and live Web deployments.

**Building more secure applications from the ground up**

Today, DTCC application developers are trained and certified on security-rich application development lifecycle and security best practices. Dedicated experts regularly perform vulnerability assessments with AppScan, the company's tool of choice for highly complex applications. Security is designed and built into more than 225 new applications per year, right from development throughout the lifecycle of the application. DTCC feels that the AppScan solution has stabilized its processes and practices, providing industrial-strength vulnerability assessment and remediation for its high-risk and complex applications.

**For more information**

To learn more about IBM Rational AppScan software, contact your IBM representative or visit:

**ibm.com**/software/rational/offerings/testing/webapplicationsecurity



IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
12-07


RAC14015-USEN-00