



Proactive Security Monitoring with RSA enVision® Platform

IANS WORKING KNOWLEDGE SERIES™

CASE STUDY

September 2008

Jim Routh
Chief Information Security Officer

Parthiv Shah
Director of Vulnerability Management

DEPOSITORY TRUST & CLEARING CORPORATION (DTCC)

About Depository Trust & Clearing Corporation (DTCC)

The Depository Trust & Clearing Corporation (DTCC), through its subsidiaries, provides clearing, settlement and information services for equities, corporate and municipal bonds, government and mortgage-backed securities, money market instruments and over-the-counter derivatives. It is the world's largest post-trade processing infrastructure.

In addition, DTCC is a leading processor of mutual funds and insurance transactions, linking funds and carriers with their distribution networks.

DTCC's depository provides custody and asset servicing for 3.5 million securities issues from the United States and 110 other countries and territories, valued at \$40 trillion. In 2007, DTCC settled more than \$1.8 quadrillion in securities transactions.

DTCC has operating facilities in multiple locations in the United States and overseas, including New York, London, Tampa and Shanghai.

DTCC is industry-owned by its customers who are members of the financial community, such as banks, broker/dealers, mutual funds and other financial institutions and increasingly operate both in the U.S. and overseas.

DTCC operates on an at-cost basis. All services provided through the U.S. clearing corporations and depository are registered with and regulated by the U.S. Securities and Exchange Commission (SEC). The depository is also a member of the U.S. Federal Reserve System and a limited-purpose trust company under New York State banking law, and monitored by the New York State Banking Department.

DTCC operates through six subsidiaries—each of which serves a specific segment and risk profile within the securities industry. Omgeo, DTCC's joint venture with Thomson Financial, provides global support for institutional post-trade processing in more than 40 countries.

For more information about DTCC, see their website at: www.dtcc.com.

Quick Read

DTCC:

- A family of companies that automates, centralizes, standardizes, and streamlines post-trade processes related to the safety of the capital markets.
- A highly regulated organization and environment.
- Key IT security challenges included responding to security audit and SEC security findings.
- Focus areas included privileged-user monitoring, monitoring of multiple login failures, and real-time alerts of behaviors that cause incidents.
- DTCC selected RSA's enVision platform as it best met their selection criteria, supported their platforms, provided easy and intuitive alerts, and had robust reporting.
- Deploying RSA enVision has improved DTCC's security monitoring and allowed DTCC to isolate security issues quickly and respond rapidly. It has made DTCC more proactive.

RSA enVision Platform:

- An information management platform for comprehensive and efficient transformation of event data into actionable compliance and security intelligence.
- Displays real-time events and correlates events across device types.
- Alerts against baseline anomalies and unusual privileged user activity.
- Maintains digital chain of custody with unaltered log data for data retention and forensic requirements.
- Automates compliance reports.
- Provides inbound and outbound IP traffic summaries.

Overview

As a regulated player in the financial services industry, DTCC is always looking at ways to improve its security monitoring. After reviewing the findings of security audits and SEC evaluations over a period of several years, the information security team wanted a more proactive approach to security monitoring. Actionable alerts about behaviors that pointed to potential security incidents were of particular interest.

After conducting internal research to define the organization's security monitoring requirements, DTCC drafted an RFP outlining key solution criteria. The goal was to find a solution to support DTCC's mix of legacy and newer systems, while enabling proactive monitoring across multiple layers (perimeter devices, middleware device log data, application logs, and workstation log data).

Among the solutions that DTCC evaluated, RSA enVision met or exceeded DTCC's RFP selection criteria. Since DTCC has implemented enVision, they have experienced numerous benefits. Although millions of events are identified each day, the information security staff receives actionable, real-time alerts and reports that quickly isolate anomalies and security events that require follow-up actions.

About Jim Routh

Jim Routh is DTCC's Chief Information Security Officer. He has over 20 years experience in information technology and information security as a practitioner, management consultant, and leader of technology functions and information security functions for global financial service firms. Routh was selected the 2007 Information Security Executive of the Year for the Northeast and is a member of the Board of Directors for FS-ISAC and the Wall Street Technology Association.

About Parthiv Shah

Parthiv Shah is the Director of Vulnerability Management in DTCC's Information Security group. He helped design and implement an enterprise-wide information security program for DTCC based on risk management best practice, COBIT, and ISO 27001 standards. Shah is a graduate of the City University of New York and has earned several information security certifications including ESCA, CISM, CISSP, and CCNA.

"It took us four to five months to define our requirements and to find the right solution."

"Security audits had identified many 'what-if' scenarios. To address these; we felt that we needed to do a better job with security monitoring."

Background

DTCC's subsidiaries provide clearing, settlement, and information services for every segment of the financial securities industry. Given the sensitive, financial information that DTCC processes, the organization is regulated by the U.S. Securities and Exchange Commission. As a result, information security is a top priority.

IT security is handled in a centralized manner at DTCC. The 28-person information security team addresses the security requirements of numerous legacy and new systems operating on a diverse set of platforms.

The Security Monitoring Challenge

Since DTCC's work is highly regulated, information security is of utmost importance. Through security audits and SEC evaluations, DTCC continues to update and enhance its security monitoring. Specifically, the organization focused on more robust monitoring of privileged user activity, multiple login failures, and other security-related events.

DTCC had traditionally followed a "passive" approach to security monitoring. The security team would only take action when notified of a potential breach. DTCC recognized that moving to a proactive approach would be a significant security improvement.

The company's vision was to understand and identify what behaviors might cause a security incident, and then proactively take steps to investigate and address any problems. The alert information would feed an existing and mature process for enterprise-wide security risk assessment. RSA enVision platform provides extensive automation of event information creating alerts and reports that enable the DTCC security staff to focus on analysis and risk assessment as opposed to log aggregation and manual review of log files.

Solution Requirements

DTCC's security team spent several months defining their requirements for a security monitoring solution and then developing an RFP. Their key selection criteria were:

- **Multi-platform support.** DTCC's IT infrastructure includes legacy and newer systems. It was critical to find a security monitoring product that could support all of the platforms used in the organization.
- **Support for multiple logging protocols.** With its diversity of systems, DTCC needed a solution that could support a variety of logging protocols, ranging from mainframe logs to Windows Active Directory to UNIX.
- **Event aggregation and correlation.** To interpret and analyze large amounts of security data, DTCC wanted a product that could aggre-

“A passive approach to security monitoring is always more dangerous than being proactive.”

- **Real-time alerts.** DTCC’s information security staff sought a security monitoring solution that would send proactive, real-time alerts.
- **Log integrity.** To support forensics, DTCC wanted a security monitoring solution that would retain the integrity of log files.
- **Privileged user monitoring.** A key requirement was the ability to determine whether privileged users had inappropriately accessed or jeopardized the integrity of data.
- **At least 60 days log retention.** DTCC needs to retain at least 60 days of log data. As a result, sufficient storage was an important consideration.
- **Superior reporting.** Reporting capabilities were critical, as security information would be shared within the information security team and throughout the organization.

Selecting RSA enVision® Platform

DTCC then conducted research (including speaking with Forrester, various financial firms, and market analysis) to create a “short list” of vendors to evaluate. This short list included:

- RSA enVision
- Cisco Security Monitoring Analysis and Response System (MARS)
- LogLogic

“We were looking for a vendor who was flexible enough to support our requirements.”

These vendors were evaluated against the key selection criteria, and DTCC spoke with customers of each of these vendors.¹

Cisco MARS and LogLogic didn’t meet several of DTCC’s selection criteria.

RSA enVision. The DTCC team concluded that RSA enVision met or exceeded all of their key criteria. They were struck by several aspects of RSA’s enVision solution:

- **Extensive platform and logging protocol support.** DTCC learned that enVision supported 70% of their system platforms. Almost all of the logging protocols that were used within DTCC were supported by enVision, including those of the older legacy systems.
- **Easy and intuitive alerts.** Proactive alerts were simple to create. DTCC’s security staff spent a minimal amount of time configuring and maintaining the system.
- **Robust reporting.** RSA enVision offered several hundred reports “out-of-the-box” and these reports could be easily customized.

“We no longer have uncertainty about the ‘what-if’ scenarios identified in our security audits.”

¹ In this IANS case study, DTCC shared its experience selecting and implementing an information security solution. However, in no way does DTCC or IANS provide an express or implied endorsement of any company or solution.

“We capture 85 million events a day in our logs. RSA enVision was the only product that enabled us to interpret that data in an efficient way.”

“RSA enVision enables us to find a needle in a haystack. The product points us to the area to look for the needle and sometimes it puts the needle right on top of the haystack.”

RSA’s Benefits for DTCC

The benefits that DTCC has realized due to implementing RSA enVision have been significant. They include:

- **Improved monitoring of privileged users and user authentication.** DTCC now has a better sense of privileged user and user authentication behavior. The security team can easily detect multiple unsuccessful logins. In one case, they found that there were tens of thousands of login failures in one day. Through an alert, the team was able to trace this issue to a user who had hardcoded his password in Windows.
- **Proactive, actionable alerts.** DTCC’s security staff has new insight into what types of actions may be required based on alerts from enVision. For example, if a user downloads a virus, enVision obtains information from the anti-virus application and sends an alert to a member of the IT staff. The alert identifies whether the virus has been eradicated, quarantined, or has not been addressed. Based on this information, the IT team knows what action must be taken.
- **Fast isolation of problems.** DTCC currently captures 85 million events per day through logs. The log data is normalized into 55 reports on a daily basis, and critical events are flagged through automated alerts. Instead of reviewing all the events, DTCC’s security and infrastructure subject matter experts are notified in near real-time about problems. This helps isolate issues quickly.

Next Steps and Lessons Learned

Looking ahead, DTCC will continue using RSA enVision for security monitoring. The team plans to work with RSA to build improved mainframe logging support into enVision.

In addition, DTCC would like to see more robust capabilities around privileged user monitoring. For example, it would be useful to see what commands a user executed after login.

As Routh and Shah reflect on DTCC’s security monitoring solution selection and implementation, they have two recommendations for companies embarking on a similar process.

- **Defining requirements first is crucial.** It took DTCC four months to research what they needed from a security monitoring application. Key questions to be answered include how long log data must be retained and which in-house systems must be supported by the product. The existing manual process for risk assessment enabled a better understanding of the actual business requirements for an automated solution.
- **A phased approach to implementation makes sense.** DTCC took time to understand the different sources of risk within the organiza-

“When it comes to implementation, only bite off what you can chew.”

tion. They then aligned their security monitoring implementation phases to the risks. The riskiest systems were monitored first then the less risky systems were brought online for monitoring.

About RSA

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle—no matter where it moves, who accesses it, or how it is used.

RSA offers industry-leading solutions in identity assurance and access control, data loss prevention and encryption, compliance and security information management, and fraud protection.

RSA is headquartered in Bedford, Massachusetts. For more information, contact the company at www.rsa.com.

About IANS

IANS is the premier membership organization for practicing information security professionals. IANS' mission is to provide key technical and business insights to help members solve their most pressing technical and professional challenges.

IANS achieves this mission through a broad offering of services provided to its members—insightful events, thought-provoking publications, best-practice research, and unique networking opportunities.

IANS is committed to providing its members with unbiased, relevant insights to increase their productivity and effectiveness as emerging technical leaders inside their organizations.