Raymond James Financial Strikes a Balance with Security, Compliance, and Access

The Challenge

As a leader in the financial services industry with a worldwide IT infrastructure, Raymond James Financial recognizes the importance of managing their event logs in meeting the strict requirements imposed by external regulations and internal policies. The challenge was in finding a single solution that could meet the firm's data collection, storage and reporting requirements. Scalability was also an issue, as the company's IT infrastructure supports approximately 5,000 financial advisors across 2,100 locations throughout the United States, Canada and internationally.

"Our first requirement was to collect events from remote locations so we could more effectively respond to those events, whether they were security or systems related," said David Bryant, team leader of Information Security Operations at Raymond James Financial. "In addition, it's important for us to report on those events for compliance reasons."

Bryant also wanted to integrate directory management with event management. "As a security person, I want to know about anything that changes in Active Directory. Having this information available through the same console as other data helps ensure it is analyzed and used."

After conducting market research, Bryant found only one company that could meet the organization's needs. "Aelita (now a part of Quest Software) was the only company with a solution that met all of our requirements," he said. "In evaluating their technology, it was clear Aelita understood our needs from both the event log management and security perspectives. That made their InTrust product a very attractive solution."

The Solution

InTrust is an integrated event log management solution that allows Raymond James Financial to effectively collect, store and report on the vast amount of event data found across its distributed environment.

With InTrust, Bryant and his team are able to collect event data automatically from multiple sources. They set up the product to collect the data as frequently as five times a day. InTrust's StoreMore technology then compresses and stores the data. The StoreMore technology, unique to InTrust, allows Raymond James to keep more data available for analysis than any other product on the market. Then, using the Reporting Console, Raymond James generates the reports they need, either for auditors, for compliance reasons, or for use within the IT Department. InTrust is also set up to notify the team of suspicious activity within their network, making it a very valuable operational asset from a security perspective.

Overview

"It's always a balancing act – we have to balance the need for security and auditing with the business need for access to data. InTrust helps us maintain that balance with a secure, well audited, yet accessible, environment."

David Bryant
Team Leader of Information Security
Operations, Raymond James Financial

ROI

- One-day setup process saved time and money
- Increased ability to comply with various regulations
- Increased security through daily e-mail updates
- Intuitive, easy-to-use interface eliminated need for user training

Benefits

- Increased confidence in compliance with internal and external regulations
- Provided means to collect event data from multiple sources
- Improved system security through powerful monitoring tools
- Keeps more data available for analysis

Environment

- 5,000 end users
- 2,100 locations throughout the United States and internationally
- InTrust running on 300 servers with plans to extend coverage

QUEST SOFTWARE®

APPLICATION MANAGEMENT | DATABASE MANAGEMENT | **WINDOWS MANAGEMENT**

Evaluating the Technology

Before deploying the solution companywide, Bryant wanted to make sure it could meet the real-world requirements of his network. So he evaluated InTrust on 125 production servers for a period of nine months.

"The product was easy to set up and use, and worked as advertised," said Bryant. "It had all the reports we needed, and the user interface was intuitive enough that I didn't even have to use the documentation to get started. We set it up one day and were viewing reports the next."

After a thorough evaluation in real-world conditions, Bryant extended the license for InTrust to 300 servers. Now that InTrust has been deployed in the production environment for more than three years, plans are underway to extend its coverage corporate-wide to 600 servers.

Results

"This product is one of our main sources compliance reports, security information and alerting," said Bryant. "As part of our regulatory response, we need to show due diligence as far as tracking and investigating what users are doing. InTrust is key to our compliance with both internal and external requirements. As a financial services firm, we must comply with NASD and SEC regulations, as well as meet the needs of our internal auditors."

Bryant also receives a daily e-mail from the system summarizing activity over the previous 24 hours, including suspicious log-on attempts. In addition, information for one of the company's divisions is extracted and used to create a custom report that is automatically e-mailed to the relevant department in PDF format.

"We do a lot with the information InTrust gives us," Bryant said. "We use everything the report tells us, some things on a daily basis, and some for quarterly self-audits and an annual external audit. If our internal auditors want to look at a report at any time, a paper copy is on the shelf – it's right there. We're one of the few departments that can say that.

"We view this product as a security and audit tool first," Bryant said. "Just having the system in place has made our internal audit team confident that we are doing the right things to protect our network," Bryant concludes. "It gives us capabilities we didn't have, and has become an important part of our overall systems management and security infrastructure. It not only helps us monitor policy compliance, it makes users more aware of their activities in regard to compliance because they know we have this capability.

"But the information being collected is useful in other ways," Bryant adds. "For example, we plan on rolling out the Reporting Console to our operations and engineering groups, and they are very excited about having access to the information it can deliver. Through the console, they will be able to easily access Exchange statistics, server error logs, server crashes and the wealth of other data we are now able to consolidate, analyze and archive.

"It's always a balancing act – we have to balance the need for security and auditing with the business need for access to data," Bryant added. "InTrust helps us maintain that balance, with a secure, well audited, yet accessible, environment."