



Digital Insight

The RSA® Data Loss Prevention (DLP) suite helps a leader in online banking extend their Deep Defense strategy.

Acceleration

As an added layer of their Deep Defense strategy, Digital Insight leverages RSA DLP Endpoint to accelerate and enhance their ability to locate and remediate company data stored across a dispersed computing environment. Utilizing the Top Risk Snapshot feature Digital Insight can proactively prioritize scanning and remediation efforts.

“We have seen continued growth in the performance and ease of use of the product since its development and now conduct regular scans using RSA® DLP Endpoint to locate data.”

Scott Mackelprang
Vice President of Security and Compliance
Digital Insight

To remain competitive in today's market and help strengthen customer relationships, mid-market financial institutions increasingly look to the online channel as a means of attracting, retaining and serving their customers. Through online banking, customers are able to manage their finances, apply for loans and complete a variety of transactions, including pay bills, access statements, view and order checks and transfer funds. However, managing an in-house online banking solution can inflict significant technological

and economic tolls on a financial institution. Enter Digital Insight: the largest on-demand provider of online banking in the United States with more than 1,750 client banks and credit unions. The company's on-demand solutions enable financial institutions to bring industry leading functionality, products and services to their end users with greater technological and economic benefits than a financial institution could achieve alone.

The Challenge

Given online banking's rapid growth, nothing is more important to a financial institution and its online users than the peace of mind knowing that all front and back end processes and transactions are secure. Maintaining this level of security requires many layers of defense spread across systems, operations, the architecture, and third party partnerships. In short, it requires a “deep defense”.

For more than a decade, Digital Insight's Deep Defense has incorporated numerous layers that prevent, detect, correct and report security threats for its financial institution clients who trust the company to protect them and give their users peace of mind. As part of this Deep Defense architecture, the company has implemented some of the strongest, state-of-the-art security policies and procedures to ensure the highest level of information security throughout its organization. Retinal scan identification is used for access to Digital Insight's secure data centers, strict security-based personnel policies including background checks are routine, and a team of security specialists provide 24/7 company-wide support. In addition, a SAS 70 Type II audit (the more stringent of the SAS 70 audits) of Digital Insight's policies and procedures is performed yearly by Ernst and Young to measure the effectiveness of the company's policies and procedures.

While every available safeguard was being taken, Scott Mackelprang, vice president of Security and Compliance at Digital Insight, desired a means to further enhance the company's ability to manage company data stored across the company's dispersed computing environment.



The Security Division of EMC



The Solution

“Digital Insight became one of the first early adopters of the RSA DLP Endpoint product (formerly Tablus Content Sentinel). It was at that time an important, ongoing relationship between the two companies began. “RSA DLP Endpoint showed potential at the onset,” noted Mackelprang. “Our main requirements during the initial testing were that the solution needed to be extremely accurate, scalable and offer the highest performance. In particular, precision was critical because it has one of the biggest impacts on the ongoing total cost of ownership of the solution. We also needed a product that would scan and complete analysis of the various and disparate locations and servers in a timely manner. RSA DLP Endpoint is able to execute a distributed scan across all networked computers to analyze content in place, without adding a client to the machine. This can cut the time required to scan 10,000's of computers from months to hours.”

Digital Insight maintains more than 100 interfaces to core processing platforms and more than 175 technology partners, enabling the company to effectively integrate hundreds of products and services with the core systems of its financial institution clients. The company monitors the security and reliability of all of these technology interfaces from within its own data center, which adheres to the highest standards. “We not only must proactively find problems and fix them for our own business and our clients' benefit, but also because we must demonstrate again and again to our auditors that we're maintaining the highest possible security standards,” said Mackelprang.

The Results

RSA DLP Endpoint helped Digital Insight to better locate and remediate data and to measure the company's compliance with internal regulations. The company also utilizes the 'Top Risk Snapshot' feature to prioritize remediation activities. “Digital Insight carefully evaluated the marketplace before deploying the initial release of the solution as an additional layer of security within our data center, and we have evolved our use of the product over the last year,” noted Mackelprang. “We have seen continued growth in the performance and ease of use of the product since its development and now conduct regular scans using RSA DLP Endpoint to locate data.”



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA, and the RSA logo are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC is a trademark of EMC Corporation. All other trademarks mentioned herein are the property of their respective owners. ©2007 RSA Security Inc. All rights reserved.

DIIN CP 1107