

Customer Profile

Microsoft

The RSA® Data Loss Prevention (DLP) suite helps a technology leader discover sensitive data

Acceleration

The RSA DLP Datacenter product helps Microsoft to accelerate compliance with regulatory requirements and gain insight into data trends without disrupting business operations and IT resources. RSA DLP Datacenter has provided Microsoft with the performance, scalability and accuracy needed to discover and remediate sensitive data across thousands of file shares and SharePoint sites.

AT A GLANCE

Business challenge

- Adhering to Payment Card Industry (PCI) and Sarbanes-Oxley regulatory compliances
- Securing Intellectual Property such as source code, strategic plans and operational information

Solution

- RSA® Data Loss Prevention Datacenter with its distributed architecture and scanning capabilities, enables them to scan all data stored across their full set of file shares and SharePoint Sites

Results

- Rapid scans of 12TB of file system data and 120,000 SharePoint Sites make continuous content discovery a reality
- With a false positive rate of less than 1%, they know recorded incidents are genuine

For a global corporation like Microsoft, the biggest challenge it faces in preventing data breaches and complying with privacy regulations isn't so much a technical data protection issue - the company does, after all, have on staff many of the world's top IT security minds. Rather, the problem is one of content



sprawl. “Before we could do anything, we knew we had to locate our sensitive information and measure compliance to the policies already in place,” explains Olav Opedal, security program manager at Microsoft. “The problem was, we had approximately 30,000 file shares containing nearly 12 terabytes of data and more than 120,000 SharePoint sites needing to be scanned and analyzed. How do you get that done in a short time frame and without causing enormous disruption to your business operations and IT resources? This was the impetus behind our Information Classification and Data Handling project.”

BUSINESS CHALLENGE

As a level 1 processor of credit cards, Microsoft clearly had to tackle the Payment Card Industry (PCI) Data Security Standard as part of its content security initiative. The PCI standard requires companies that accept card payments to put in place strong controls to restrict access to cardholder account information and take steps to protect stored data.

Also, as with all publicly traded companies, Microsoft is subject to Sarbanes-Oxley and its stringent rules on securing financial information. With these two regulations, Microsoft's compliance challenge was pretty clearly defined. In terms of its overall information security policy, however, Microsoft had to consider intellectual property as well, which considerably broadened the scope of its Information Classification and Data Handling project.

“Source code, strategic plans, operational information and other kinds of sensitive business information are all types of intellectual property that we needed to secure,” asserts Opedal. “Of course, some kinds of information are more



The Security Division of EMC



sensitive than others - customer data, source code and corporate financial data were clearly the most important for us. This is why rather than trying to secure our information according to the specific regulation, we took the approach of classifying all data in our managed IT space into one of three categories: High Business Impact, Moderate Business Impact or Low Business Impact.”

With the basics of its strategy coming into focus, the question for Microsoft became: how to gain a better understanding of the risks posed by its information storage and data handling practices? Opedal and his team realized that they had to gain insight not just into specific files, but overall data trends.

“We built a risk model,” explains Opedal, “the purpose of which was to quantify the level of risk from our data. We decided to start with HBI - which encompasses all of the most important intellectual property and information regulated under PCI and SOX - then move on to target other areas. To execute our HBI strategy, we needed a way to scan any managed space where sensitive data could be stored to ascertain the nature of what we had out there. This was a content discovery challenge. That’s where RSA DLP Datacenter (formerly Tablus Content Sentinel) came in.”

SOLUTION

The parameters Microsoft developed for its Information Classification and Data Handling project dictated the stringent criteria for judging content discovery solutions. With enormous data loads and thousands of locations to scan, enterprise scalability, performance and accuracy were all top considerations. Management and operations were also at the head of the list.

Microsoft executives needed to know that they could handle security threats and incidents quickly and securely, and be able to document remediation efforts in order to maintain audit trails in compliance with PCI and SOX. “Content identification is not one of those problems that you can simply throw a lot of hardware at and get the kind of performance you need,” observes Opedal. “The unparalleled accuracy and unique features of RSA DLP Datacenter - such as incremental processing - made it the only viable choice for discovering all our sensitive content.”

Microsoft implemented RSA DLP Datacenter, which takes a revolutionary approach to content discovery with its distributed architecture and scanning capabilities, enabling them to scan all data stored across their full set of file shares and SharePoint sites. This is a vital capability in organizations, such as Microsoft, that have a vast amount of stored data.

To boost performance of this scanning process, Opedal opted to use the product’s Grid Processing capability, enabling him to specify a set of servers at each location to process the scan. The servers are automatically provisioned and automatically load balance the content analysis work for fastest processing. Microsoft is also leveraging the patentpending incremental scanning technology for ongoing scans. This enables them to regularly scan and analyze files and directories that are new, modified, moved or renamed.

“We really needed the performance, scalability and the highly precise content detection capabilities that only RSA DLP Datacenter could provide,” says Opedal. “Grid processing and incremental scanning were essential for Microsoft given the volume of data that we store. Also, RSA DLP Datacenter generates matched files with an accuracy rate consistently at or above 98%.”

The industry-leading accuracy of RSA DLP Datacenter incorporates the most advanced content analysis techniques, accuracy, and performance.

RESULTS

As a result, Opedal and his team were able to scan 12TB of file system data and a 120,000 SharePoint sites in a matter of nine days while still maintaining the highest levels of precision. Ongoing incremental scans of just the new, modified, moved or renamed data across those same 120,000 SharePoint sites takes less than 5% of the time it took for the original scan, making continuous content discovery a reality.

Further, with RSA DLP Datacenter, Microsoft is keeping the costs of its information security operations as low as possible. In planning the data discovery project, the team set a baseline that a single compliance officer or security advisor could handle approximately 250 incidents per day. “The false positive rate is lower than 1%, so we know that the incidents our compliance staff have to review are genuine,” explains Opedal. Without RSA DLP Datacenter, we’d have to hire and train a lot more staff and face a far higher total cost of ownership.”

RSA DLP Datacenter has given us a better understanding of the location of our high impact business information, and enables us to protect against the proliferation of that data - something of paramount importance for all of us here at Microsoft.



“Content identification is not one of those problems that you can simply throw a lot of hardware at and get the kind of performance you need. The unparalleled accuracy and unique features of RSA® DLP Datacenter made it the only viable choice for discovering all our sensitive content.”

Olav Opedal
Security Program Manager Microsoft



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

The Security Division of EMC

RSA, the RSA logo, and SecurID 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. ©2003-2007 RSA Security Inc. All rights reserved.

MICRO_CP_1208