case study

Deploying DLP and Encryption

in Financial, Government, Healthcare, and Insurance Verticals

DLP case study

Proven DLP Results in the Banking Industry

1

The Situation

A company with two hundred distributed offices which offers IT Services to small, local banks needed to provide a cost-effective solution to filter spam and viruses from incoming email and protect sensitive data in outbound email. Because banking information is particularly sensitive, the data loss prevention solution needed to be in strict compliance with banking regulations. The major regulations that the company faces are: SOX, PCI, PII, and several state specific regulations.

Technical Challenges

The customer needed to be able to offer systems to their customers that were scalable, reliable, and cost-effective. It was critical that the company could provide strong data loss prevention solutions to the banks they supported. In addition, because the company supported different banks, they needed to be able to tailor the solutions for different banks. However, it was equally important that the banks would be able to run reports that demonstrated their compliance with strict regulations. Some of the regulations that they face are SOX, PCI, PII, and state specific regulations.

The Cisco Advantage

Cisco IronPort was able to provide the company with a comprehensive email security solution that was not only cost-effective, but scalable.

Cisco IronPort has partnered with RSA – the leader in data loss prevention (DLP) technology – to provide an integrated data loss prevention solution on the Cisco IronPort Email appliance. The RSA DLP solution includes more than 100 pre-defined policies to ensure compliance with U.S. and international regulations, so tailoring solutions for different companies is simple.

Because the solution is integrated on the Cisco IronPort solution, it is also easy to run reports on the data loss prevention policies to ensure that the banks are in compliance, whether in the cloud or on the appliance. Administrators can access real-time and scheduled reports to view the top DLP email violations by policy, severity, and senders. In addition, the message tracking capabilities enable administrators to search for messages with specific DLP violations. These two tracking systems allow banks to provide evidence of the effectiveness of their DLP solution.

Building a Trusted Relationship

The Situation

The customer, with dual headquarters in Washington, DC and Charleston, WV, is a $7.5 billion holding company with one hundred and thirteen full-service banking offices in West Virginia, Virginia, Washington, DC, Maryland, and Ohio. The customer was seeking a data loss prevention (DLP) and encryption solution to bring their company into compliance with banking regulations.

Technical Challenges

The customer had an existing Cisco IronPort Email Security appliance, but they wanted to review all the leading vendors for encryption and DLP solutions available in the marketplace. The company was seeking the best product to meet specific infrastructure, feature, and budgetary requirements.

The Cisco Advantage

While the company was reviewing a wide range of solutions, it became clear to them that Cisco IronPort was able to build on their existing infrastructure with the least impact while delivering the best solution. The customer had an existing Cisco IronPort Email Security appliance in their network, so adding encryption and DLP solutions was a matter of upgrading and enabling features. Because RSA DLP strategies are deployed as more than 100 pre-defined policies, deployment is a matter of selecting and applying the correct policy. The customer was already satisfied with their inbound email security solution, so deploying outbound security with the same trusted brand was also appealing to them. Finally, the customer was pleased that Cisco IronPort worked closely with them to provide strategies for their future DLP requirements. Because Cisco IronPort was not only the best and easiest solution, but also a dedicated partner, the customer chose to deploy Cisco IronPort's Email DLP solution.

DLP case study

Expanding Coverage While Lowering Costs

3

The Situation

The customer supports email services for a county government, including the county Police Department. The customer needed to employ both encryption and data loss protection (DLP) solutions for all their employees in order to protect sensitive government data.

Technical Challenges

The customer was seeking an affordable solution for both their encryption and DLP needs, and they wanted to expand coverage to include all of their employees. They had an existing encryption solution with Zix, but they were hoping to replace it due to the exorbitant cost and the limited deployment. At the existing rate, the county could only afford to enable encryption for a small fraction of their employees, and they had no existing DLP solution.

The Cisco Advantage

The customer was happy to discover that Cisco IronPort could offer a combined solution for DLP and encryption because they had successfully deployed other Cisco products in the past and were very satisfied with the experience. The customer performed an onsite evaluation, and they were impressed with the DLP catch rate and reporting capabilities. Cisco IronPort has partnered with RSA, whose DLP solution has a high catch rate and a low rate of false positives. In addition, Cisco IronPort implemented a DLP violation report, making it simple to track and regulate DLP activity. Administrators can access real-time and scheduled reports to view the top DLP email violations by policy, severity, and senders.

Not only was the customer satisfied with the catch rate and performance, but they were pleased with the cost structure. Using Cisco IronPort's encryption and DLP solution, they were able to enjoy considerable savings over the competitors. Using the Cisco IronPort solution, the customer was able to deploy the DLP and encryption solution for all of their users at a rate lower than the competitors'.

DLP case study

Improving Communication in the Health Industry

4

The Situation

A large regional healthcare organization maintains an integrated system of health care services and facilities providing quality health care from emergency admissions to in-patient hospitalization and leading-edge surgery to rehabilitation and home care. The customer needed to implement both encryption and data loss prevention (DLP) solutions to identify and protect sensitive personal health information (PHI).

Technical Challenges

Already having deployed a Cisco IronPort Email Security appliance in their network for many years, the customer was extremely satisfied with their inbound email security. With compliance concerns and patient health information being sent via email, additional requirements were discovered to implement outbound security in the form of email encryption and DLP solutions. This new technology was sought to allow doctors to communicate securely with other doctors, insurance companies, and patients.

The Cisco Advantage

Completely satisfied with their implementation of the Cisco IronPort Email Security appliance for inbound protection, the customer expressed interested in researching Cisco's DLP and encryption solutions because of confidence and trust in the Cisco brand.

After researching solutions, the customer was quickly impressed that Cisco could provide such a complete and consolidated email security for their needs. The exclusive endorsement of Cisco IronPort's outbound email encryption and data loss prevention heightened the industry validation of the solution as the right and best one for the business.

The company was particularly pleased that Cisco IronPort had partnered with RSA because of their leadership and expertise in the data loss prevention industry. With predefined templates and a low rate of false positives, this functionality further differentiated the solution from the competition. Now running Cisco IronPort's DLP solution with their infrastructure, the customer can now communicate with confidence to outside doctors, insurance companies, and patients to in a protected and confidential manner.

Easy Integration Now and in the Future

5

The Situation

The company is a full-service financial services firm, providing comprehensive financial advice and service to individual, corporate, and institutional investors. The company had an existing Google Postini email security solution but was seeking a data loss prevention (DLP) solution to meet regulatory compliance requirements.

Technical Challenges

The customer was seeking a best-of-breed DLP solution to address particular regulations that were implemented in Pennsylvania and Massachusetts. The customer also needed to address general compliance issues for GLBA, Sarbanes-Oxley, PCI, HIPAA, and others. Lastly, the customer wanted assurance that they would be able to address future compliance requirements using solutions that could fully integrate with their existing infrastructure.

The Cisco Advantage

While researching DLP solutions, the customer was impressed with the best-of-breed performance provided by RSA's DLP integration with the Cisco IronPort Email Security appliance. Although they were not looking for a new email security solution, they discovered that it would be far more economical to buy the Cisco IronPort Email Security appliance and bundle email security and data loss prevention on a single appliance. They discovered that the combined solution not only improved their email hygiene, but it would save them a significant amount of money over the course of the deployment. The Cisco IronPort Email Security appliance could be easily integrated into their current infrastructure, and the bundled RSA DLP provided the best-of-breed DLP solution they were seeking.

The customer was particularly pleased to learn that Cisco IronPort Email DLP solutions are built into more than 100 pre-defined policies. This meant that different policies could be easily deployed as regulatory requirements change over time.

Finding a Single Platform

The Situation

A large life insurance company with 500 subscribers needed to consolidate their email security solution. The company wanted to work with a single vendor who could provide a solution for inbound email security and outbound scanning, data loss prevention, and encryption.

Technical Challenges

The company was seeking a single solution for encryption, data loss prevention, and inbound email security and they strongly preferred to work with a single vendor. The company placed a strong emphasis on the need for a data loss prevention solution that ensured they could meet their compliance requirements.

The Cisco Advantage

When the customer reviewed the landscape of different solutions, they found that there were many vendors who had a good solution to one of their problems, but very few companies who could offer best-of-breed performance on all three solutions. The customer eventually selected Cisco IronPort's Email Security appliance because of strong performance in email security, encryption, and data loss prevention.

Cisco IronPort was able to consolidate the company's email gateway, giving the customer simplicity in deployment and usability. Because data loss prevention was a key deliverable, the customer chose to deploy a Cisco IronPort Email Security appliance with an integrated RSA Email DLP solution. They were impressed with the simplicity and accuracy of the data loss prevention deployment. With the click of a button, the company's administrators could enable pre-defined RSA Email DLP policies that were designed to handle not only government regulations such as US-focused HIPAA and UK-focused Data Protection Act, but also include non-government regulations such as the Payment Card Industry Data Security Standards (PCI DSS).

The customer was also pleased that they encountered few false positives, which is a frequent problem with data loss prevention solutions. RSA Email DLP's pre-defined policies are created by RSA's Information Policy and Classification Research Team, who use sophisticated content analysis techniques specifically tuned to eliminate false positives and maximize catch rate.