

Defining a Data Security Program

In 2006, a billion dollar relationship management and outsourcing service provider completed an extensive enterprise-wide risk assessment and found that securing sensitive client data was ranked as being one of the top three risks facing the company. Furthermore, a growing number of clients were including in their service level agreements (SLA) the requirement to prove their data was being processed and managed in compliance with the Payment Card Industry (PCI) regulator requirements. The internal risk assessment concluded that an estimated \$250M of annual revenue could be at risk if the company suffered a data compromise or was unable to show PCI or other regulatory compliance around client data. To address both issues the company implemented an enterprise wide information risk management initiative with the primary objectives of:

- Enhancing data security and privacy across the global enterprise to include overseas call centers and a growing number of “work at home” agents
- Assuring regulatory compliance including PCI compliance on appropriate data across end points, servers, storage and applications
- Establishing an information/data security competency through people, process and technology

The strategic goal of the new risk management initiative was to increase the company’s competitive advantage for their outsourced service offerings by providing advanced data security capabilities and practices for their clients. This would in turn increase the protection of the company’s corporate brand by minimizing the possibility of a data loss incident while increasing shareholder value through a more competitive service offering. The challenge was to find the right mix of process, people and technology to successfully manage the vast amounts of sensitive data (over 2000 terabytes) entrusted to the company by their clients ensuring that data is appropriately monitored, secured and controlled.

Solution Deployment

- 50,000 Plus Software Agents
- Centralized, Policy Driven DLP

Use Cases

- PCI Compliance
- Policy Based File and Email Encryption
- USB/Mobile Device Protection
- Actionable Data Classification

Company Snapshot

- Global leader in outsource business process operations
- Workforce of over 75,000
- Provides IT, Process and HR outsourcing services to Fortune 1000 companies
- Processes and maintains large amounts of sensitive data for hundreds of clients

Deploying a Data Security Program

The new data security program began with a thorough data controls assessment in which all data related business processes were defined, mapped and vulnerabilities were identified. The result was the creation of a series of top-down, risk based reports defining areas of deficiencies and giving each area a risk criticality rating. At the same time, the team set out to define and implement PCI controls across three major customer care platforms in order to meet compliance requirements. The project involved over 100 staff members representing subject matter experts throughout the company, each being tasked with specific responsibilities across each business process and application platform. The results of both projects were then presented to the executive management team and included recommendations on policy and process changes as well as investments in technology and personnel in order to mitigate all risks. Critical to the success of the program would be:

- The ability to monitor sensitive data movement and implement security controls across the tens of thousands of end points including servers, workstations, desktops and laptops where client data is put at risk
- The need to encrypt sensitive data as it moves across and is stored on end points, including an alternative to whole disk encryption, is due to the sheer volume of host systems involved
- The requirement to centrally and easily define, build, implement and manage the security controls that would discover, classify, monitor and enforce data security policy across the global system
- The flexibility across general security policies to define and classify specific data and implement appropriate security controls separately for each client
- Extensive reporting that offers visibility into security control effectiveness, data usage and regulation compliance

Measuring for Success

The security team recognized that to succeed in a program of this scale and complexity they would need to implement a robust data security process that would identify new and changing risks, implement mitigating controls, make end users accountable for their actions and alert security managers immediately and accurately to potential data compromise incidents. This process needs to be continuous and have the ability to improve as it was forced to deal with new and unknown threats. The team also recognized that this process could not be achieved without investing in a data security technology platform that would become its foundation, being able to meet all critical program requirements, scale to the global enterprise and be flexible enough to meet new and unknown threats in the future.

After extensive research across many security and data management vendors, the company selected the Verdasys Digital Guardian solution as the technology foundation for their enterprise security program. Digital Guardian met all program requirements and offered the promise of a high level of data containment in an easily managed and highly scalable technology foundation.

Deployment and Program Rollout

The Digital Guardian solution was initially deployed to 5,000 desktops, laptops and workstations used to support various client programs. This early deployment enabled the data security team to begin monitoring the flow and usage of data across all of the newly protected end points.

The result was the creation of the first “top-down” data risk evaluation in which the company had visibility in data usage risk in terms of the sensitivity of the data as well as the riskiness of the process it moved through. The results surprised the data security team as it became clear that many of the assumptions about data movement and usage were incorrect and that many existing data security policies were inadequate and even increased risk. After existing security policies were updated, the first data security controls were successfully deployed. Initial controls would warn users to improper behavior and block certain high risk activities.

The deployment then rolled out to another 30,000 end-users located in over 60 different geographic locations. As data security policies and business process were aligned to accommodate both increased data security and higher client regulatory requirements the team began to aggressively deploy end-user prompts and warnings to deter risky behavior and offer real-time training on governance policies. These data security controls severed to increase end-user accountability and over the first 3 months a 93% drop in risky activities was recorded.

Today, the IT team finds that 2 FTE's easily cover the 50,000 post deployment users. These managers conduct continual risk analysis, policy and control improvement with line of business managers, compliance report updating and management, incident response management as well as the management of the Digital Guardian architecture and follow on updates.

The Digital Guardian Solution

Digital Guardian, through its integrated framework and multi-function agent, is the only data security solution that delivers:

- Real-time and background multi-function scanning and data classification of sensitive data on laptops, desktops and servers across the extended enterprise
- Enterprise-wide visibility into sensitive data location and usage
- Policy enforcement that leverages not only identity and activity, but also data classification, context and content analysis
- Risk appropriate responses to user activities including policy driven warnings, blocking and alerting, as well as automated file and email encryption

Digital Guardian allows your business to put sensitive information to work while ensuring its usage is governed, controlled and audited. Customers who are serious about data security chose Verdasys Digital Guardian.

“The ability to continuously audit sensitive data use and implement real-time, risk-appropriate controls for provable secure outsourcing is a key competitive advantage in the IT outsourcing, business process outsourcing, and call center business.”

SVP, Information Security

Verdasys provides enterprise software solutions that are the foundation of our customers’ global data security strategy. With greater than 1 million security agents deployed at over 120 of the world’s leading organizations, Verdasys is the proven leader of global data security solutions for information protection and compliance.

Verdasys headquarters is located in Waltham, MA, USA, with offices in London, Munich, Rome, Madrid, Athens, Tel Aviv, Tokyo, Osaka, Taipei, Singapore and Shanghai.

© 2008 Verdasys, Inc. All Rights Reserved. Verdasys, the Verdasys logo, Digital Guardian, and the Digital Guardian logo are trademarks of Verdasys, Inc. All other logos are the property of their respective owners. The content of this document is subject to change without notice. V5.0 09-29-08

Corporate Headquarters

404 Wyman Street
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

WWW.VERDASYS.COM