CUSTOMER SUCCESS STORY

Multinational Banking Company

FINANCIAL SERVICES

Industry

- Financial Services

Environment

- 12,000 Workstations
- Windows

Challenges

- Data on over 50 million credit card customers
- PCI-DSS compliance
- Removable storage devices required
- Mask some data, while leaving other data visible
- Automatic classification of data using content inspection

Results

- Visibility into location and use of all PCI regulated information
- Contextual and content-based classification of data
- Compliance with PCI requirements for PAN encryption based on data usage
- Removable device support with automatic encryption on non-company devices
- Classify existing data quickly and easily

DIGITALGUARDIAN™
by VERDASYS

Contextual Classification, Data Protection, and PCI-DSS Compliance

A multinational banking and financial services company, with over 50,000 employees worldwide, was subject to a wide range of regulatory requirements. In addition to Sarbanes-Oxley (SOX), Graham, Leach, Bliley (GLB), and Payment Card Industry (PCI) standards in the US, they were subject to international regulations such as the EU Data Protection Directive.

While the requirements for each standard vary, all focus on protecting information. The frequent news regarding data breaches and stolen credit card information made it clear that security had to be a priority. When this organization decided it needed to improve protection of its credit card customers' data, it called Digital Guardian.

THE BUSINESS CHALLENGE

With over 50 million credit card customers around the world, the company was subject to the Payment Card Industry Data Security Standards (PCI-DSS). The standards require that sensitive credit card information be encrypted at rest, and that access to the information is controlled.

The latter requirement can be complicated. Credit card information includes the account holder's name, address, social security number, and Primary Account Number (PAN). Most of the bank's employees should be blocked from viewing any of this sensitive data. However, some employees required access to social security numbers, others only needed access to PANs. Still others needed access to both.

The company also wanted improved control over removable storage devices, company-supplied devices, such as USB memory sticks, included automatic encryption. They wanted to ensure that all sensitive information stored on other devices would be encrypted as well.

The company required a solution that would allow each employee group to access appropriate data from their workstations using their local network, VPN, or thin client terminals such as WYSE or Citrix. PCI-DSS standards allow PAN to be stored, but only if encrypted. Section 3.3 of the standards further states: "Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN."

DIGITAL GUARDIAN FACTS

Customers

- Over 250 customers
- Inlcudes 130 of the Global 2000 and government agencies
- Used by 7 of the top 10 patent holders
- Over 2.1 Million endpoints protected
- Only solution to scale to 250,000 agents

Information Discovery and Classification

- Context-based data awareness
- Content inspection
- User classification
- All content is tagged with permissions
- Permissions persist through reuse, renaming
- Over 300 data types
- 90 languages

Response Options

- Monitor, log, report
- Prompt, justify, and report
- Block and report

Supported Platforms

- Desktop/Laptop
- Server
- Network
- Virtual
- Supports devices on network and off network

Supported OS

- Microsoft Windows®
- Linux
- Mac OS X®

Deployment Models

- On Premise
- Managed Security Program (MSP)
- Hybrid MSP

DIGITALGUARDIAN™
by VERDASYS

www.digitalguardian.com

CRITICAL SUCCESS FACTORS

- PCI-DSS compliance
- Automatic identification and classification of sensitive data
- Protection of all critical data on network file servers
- Allow administrators to back up files containing sensitive data such as PAN and social security numbers, but not decrypt them

THE SOLUTION

The Professional Services team from Digital Guardian worked with the bank to identify key processes and applications. They chose to use both context and content-based automatic classification of data.

Contextual data awareness helps classify data by understanding information about the data file or email message. Digital Guardian's contextual awareness is thorough, accounting for variables including the application used to create the data, who created/edited the data, the storage location/repository, or the email message sender, recipient, or subject.

Digital Guardian's content inspection technology directly inspects the data to identify confidential information in over 300 data formats and 90 languages . In this case, the goal was to identify social security numbers, PAN, and other personal information.

With data classification addressed, Digital Guardian endpoint agents could monitor all user actions and enforce controls, including:

- Automatically encrypt sensitive files when those files are moved to network file servers
- Prevent decryption of PCI PAN and/or SSN data by unauthorized users, including system administrators with root privileges
- Automatically encrypt all sensitive data written from workstations to authorized removable storage devices

THE RESULTS

Using Digital Guardian provided the customer with complete visibility into the location and use of all information subject to the PCI-DSS. The endpoint agents classified data appropriately, both online and offline, and ensured that policies were enforced with the appropriate controls.

Digital Guardian's ability to recognize and apply appropriate policies to different types of removable devices enabled the use of non-company owned devices by automatically encrypting sensitive data stored on those devices. This ensured that the files could be decrypted only on workstations using Digital Guardian.

Automatic encryption also protected sensitive data if a laptop or removable drive was lost. Digital Guardian's comprehensive logging of information both at rest and in motion provided a complete forensic view for reporting.