CUSTOMER SUCCESS STORY

DIGITAL GUARDIAN®

Contextual Classification, Data Protection, and PCI-DSS Compliance

About the Customer

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), Payment Card Industry (PCI) standards, and other international regulations.

While the requirements for each 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. This organization decided it needed to improve protection of its credit card customers' data.

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), which require sensitive credit card information be controlled and protected.

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 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. PCI-DSS standards allow PAN to be stored, but only if encrypted. The company also wanted improved control over removable storage devices, such as USB memory sticks, to include automatic encryption and mandate the use of registered drives only.

Critical Success Factors

- Demonstrate and document regulatory compliance
- Automatic identification, classification and encryption of data
- Granular data access based on roles within organization
- Administrator can back-up sensitive data files, but not decrypt

Industry

- Financial Services

Environment

- 12,000 Windows workstations
- Regulated industry
- Global customer and employee base

Challenge

- Data on over 50 million credit card customers
- PCI-DSS, SOX, GLB 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 noncompany devices
- Classify existing data quickly and easily

Data Types We Protect

Banking

- Personally Identifiable Information (PII)
- Payment Card Industry Data Security Standard (PCI DSS)

Insurance

- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Payment Card Industry Data Security Standard (PCI DSS)

FInancial Markets

- Intellectual Property (IP): Deal Management Information, Trading Algorithms, Financial Modeling, IPO Plans, M&A Plans

The Solution

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. Digital Guardian enabled the bank to automatically encrypt sensitive files when moved to network file servers or written to removable drives. System administrators could still perform backups and other system maintenance, but were unable to decrypt sensitive data

The Results

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

Digital Guardian's ability to recognize and apply policies to different types of drives enabled the use of non-company owned devices by automatically encrypting sensitive data stored there. Those files could be decrypted only on workstations using Digital Guardian. Digital Guardian's comprehensive logging of information provided a complete forensic view for reporting.

About Digital Guardian

Installed Based

- Over 600 customers from across the globe
- Industries served: Business services, education, energy, financial services, government, healthcare, manufacturing, retail, technology
- Used by 7 of the top 10 patent holders

Discovery and Classification

- Endpoint, network, cloud and local data storage
- Content, context, and user classification
- Fully automated to fully manual classification
- Over 300 data types, over 90 languages

Educate and Enforce

- Monitor log, prompt, justification request
- Auto-encrypt, quarantine, move, block

Actionable Analytics

- System, user, and data level event visibility
- Analytics that filter out the noise
- Drag and drop incident management
- Right click remediation in real time

Operation System Support

- Full visibility, analytics and controls across multiple operating systems
- Mac
- Windows
- Linux

Deployment

- On-Premise
- SaaS
- Managed Security Program

DIGITALGUARDIAN®