FORTRA™

CASE STUDY (Digital Guardian)

Open Access, Business Enablement, and Data Protection

About The Customer

A multi-billion dollar, international financial services organization had failed an SEC audit. With more than 200,000 employees in over 100 countries, and divisions in commercial banking, wealth management, and corporate investment banking, the firm was subject to a wide variety of regulatory standards, including GLBA, SOX, and PCI. While it prides itself on its open culture and commitment to providing employees with wide access to information, the company needed to get control of its information driving security and compliance.

The Business Challenge

The investment banking division of the organization investigates and evaluates possible mergers and acquisitions. Each of these strategic deals can be worth billions of dollars, and information and analytical models supporting each individual deal is highly confidential.

Investment bank professionals need unfettered access to all available information on each individual deal. At the same time, protecting confidential information from exposure and egress is a firm requirement. The sensitivity of the data requires that access to the information be limited to those employees with “need to know” privileges. “Privileged Users,” such as system administrators who manage the servers with root access, must be able to perform administrative tasks on those devices without being able to open, move, or change critical files.

Finally, to support the organization’s culture of openness, the organization could not allow blocking. Instead, they required immediate notification of suspicious or prohibited use of data, so the incident response team could quickly respond to and investigate the activity.

Critical Success Factors

- Global, open access to sensitive merger and acquistion data
- Flexible data discovery and classification
- Rapid visibility into data risks to support immediate incident response

INDUSTRY

- Financial Services

ENVIRONMENT

- 10,000 endpoints protected
- Windows
- Sensitive merger and acquistion documents
- Regulated data

CHALLENGE

- Maintaining confidentiality of merger & acquistion information
- Segregation of rights in an “open access” environment
- Privileged users with root access to the servers must not be able to view or move data
- Rights to individual data stores varies by user
- Multiple data types

RESULTS

- The investment banking team has free access to sensitive data, without concern for data loss
- The company maintains its culture of “open access”, while improving security over critical data
- Automated data classification that persists even when data is copied to another document
- Privileged users are able to maintain file shares without compromising data security

The Solution

Fortra™'s Digital Guardian® worked with the customer to understand its information needs while meeting its security goals. Digital Guardian provided a granular solution that identified and provided appropriate data to each user, while protecting the confidential information of each deal.

Digital Guardian's Context-based capability automatically classified and tagged all investment banking data in the file shares. This prevented incorrect manual categorization, simplified segmenting data by deal, and ensured all documents were classified. Digital Guardian's tags, at the metadata level, allowed the company to track and prevent unauthorized reuse of material. If a document is tagged as "Confidential" and restricted to a specific group, that classification persists and is "inherited" by derivative documents. For their confidential investment models, if a user copies a section of the document, any new document with that section will have the same rights and restrictions of the original document.

Classification also broke the previously rigid link between access rights to the file shares and specific documents. By implementing policies, members of each deal team were restricted to data related to their individual deals, based on the classification provided by Digital Guardian. Other users, even those with elevated access privileges, were prohibited by the same policies from accessing the data. The solution monitored and logged all user action, reporting prohibited activity immediately to the incident response team.

Data Types We Protect

BANKING

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

INSURANCE

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

FINANCIAL MARKETS

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

The Results

Digital Guardian allowed the organization to maintain its culture of "open access," while improving security over critical data. The investment banking team maintained immediate access to critical information, with strict control over data use. By using data classification to control access, system administrators could perform all maintenance and updates to the company's devices, but not copy, move, or open confidential files. The company increased productivity, improved security, and addressed shortcomings cited in the SEC audit.

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

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.