CUSTOMER SUCCESS STORY

Multibillion-Dollar Global Financial Services Firm

FINANCIAL SERVICES

Industry

- Financial Services

Environment

- 10,000 endpoints protected
- Windows 7

Challenges

- Maintaining confidentiality of M&A information and 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

DIGITAL GUARDIAN®
Formerly VERDASYS

Data Protection, Open Access, and Business Enablement

A multi-billion dollar, international financial services organization had a problem. 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, include GLBA, SOX, and PCI.

While it prides itself on its open culture and commitment to providing employees with wide access to information, the company recently failed an SEC audit. It needed to get control of its information, understand how data is being used, and ensure that employees treat all information in accordance with corporate security policies and regulatory standards.

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 analysis supporting each individual deal is highly confidential. Even the formulas in spreadsheets are considered a competitive advantage and a closely guarded secret.

The data created or acquired from these M&A's includes market analyses, financial history and forecasts, draft transaction terms and conditions, and correspondence with key personnel. Data types include documents, spreadsheets, emails, and graphics. All are stored on file shares, with a separate share for each deal. This links a user's rights to a device with all information on that device.

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.

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

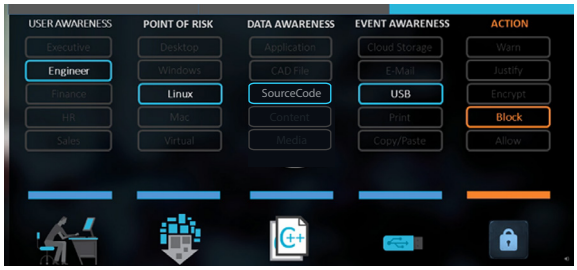
- On Premise
- Managed Security Program (MSP)
- Hybrid MSP

DIGITAL GUARDIAN®
Formerly VERDASYS

www.digitalguardian.com

THE SOLUTION

Digital Guardian worked with the customer to understand its information needs while meeting its security goals. Digital Guardian provides a granular solution that could identify and provide appropriate data to each user, while protecting the confidential information of each deal.



Digital Guardian's Context-based Data Awareness capability automatically classified and tagged all Investment Banking data in the file shares. This prevented incorrect manual categorization, and simplified segmenting data for each individual deal.

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.

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 the use of the data. By using data classification to control access, as opposed to device settings, system administrators could perform all maintenance and updates to the company's devices, but not copy, move, or open confidential files.

Digital Guardian's tags, at the meta data level, also 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 spreadsheet formula, if a user copies a section of the document, saves it under another name, or saves it in a different file format, that new document will have the same rights and restrictions of the original spreadsheet.

Digital Guardian was deployed in "Monitor" mode, so that users saw no change in workflow, blocking, or prompting. However, Digital Guardian's forensics-quality logging monitored and recorded all actions. When suspicious or prohibited events occurred, the internal incident response team received real time alerts for quick investigation and follow-up.

The company increased productivity, improved security, and addressed shortcomings cited in the SEC audit. With the value of Digital Guardian firmly established in the Investment Banking group, use expanded into additional business units.