CUSTOMER SUCCESS STORY

Energy Division of Fortune 50 Company

ENERGY

Industry

- Energy

Environment

- Over100,000 workstations
- Windows®
- Linux

Challenges

- Widespread distribution of critical data
- Multiple desktop and server environments
- Multiple data types, including scientific data, not easily recognized
- Support for authorized and privileged users, while preventing misuse of data

Results

- Visibility to all data use and movement
- Improved collaboration and reduced risk of data loss
- Automatic encryption of sensitive data in emails or on removable drives
- Improved user training on appropriate use through Prompt and Warn controls
- Detected and stopped an insider threat in first months of deployment

DIGITALGUARDIAN™
by VERDASYS

IP Protection, Secure Collaboration, and Massive Scalability

The global business unit of a Fortune 50 company faced a problem. The organization designed and manufactured energy generation machinery, and had invested millions of dollars in its intellectual property (IP). Scientists, engineers, and manufacturing personnel across the organization used the IP to create and maintain the company's competitive advantage.

The company had always relied on "trust-based" access control. This allowed open access to all information, without regard to an employee's need for the information, with the assumption that all employees were trustworthy. When a privileged user was caught attempting to steal proprietary data, it became obvious a "trust-based" system no longer worked. The company needed to gain control over their IP, and quickly. They called Digital Guardian®.

THE BUSINESS CHALLENGE

The company had over 40,000 employees in locations around the world who required access to the IP. Their infrastructure included desktops, laptops, Windows® Servers and Fileshares, as well as virtual environments. The IP was used in multiple applications, including specialized scientific and simulation software. Data types included new product design and engineering documents, process flow plans, manufacturing documents, and business plans.

Identifying and classifying the sensitive data presented a challenge. Manual classification of the data was impractical; it existed in too many forms and in too many locations. Manual classification is also subject to a user's judgment, and therefore inconsistent. More importantly, the attempted breach made clear the risk from malicious insiders. The solution had to provide automatic classification of data as it was created.

The company had previously relied on access control measures to protect data, but further restricting access to sensitive material was not possible. Employees needed the information to perform their jobs. The required solution had to provide authorized users with unencumbered access to IP, while monitoring data use to ensure compliance with corporate policies. In short, permissions for use needed to travel with the data.

CRITICAL SUCCESS FACTORS

- Enable knowledge workers to share sensitive data, by group and need, with teams across three continents

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

- Automatic encryption of sensitive data when shared by email or copied to a removable drive
- Fast alerting for Incident Response Teams and forensic reporting
- Allow users with elevated privilege to perform system maintenance without exposing critical data
- Scalability to deploy across 40,000 endpoints on multiple continents

THE SOLUTION

Digital Guardian worked with the company to identify systems where IP was created, used, and stored. Context classification was used for the discovery and automatic classification of files – as data was created – based on over 106 variables, including source application, server, file path, file type, and user identity. For some data types, content-based classification was used based on keywords, regular expressions, document similarity, and pattern or dictionary matching.

Digital Guardian provided the company with visibility to data location and use. Endpoint agents monitored the data and enforced the organization's policies in real time across the following channels:

- Files on local hard drives / USB devices
- Copying of data from specified file servers
- File uploads to Web/FTP sites
- Email attachments sent via SMTP and Outlook®
- Printing of documents to hard copy or PDF
- Files burned to CD / DVD

Digital Guardian provided the company with policy-driven, automated data controls to allow collaboration between business units, balanced against the risk posed by a specific activity, such as copying data to another drive. Data controls included:

- Blocking unauthorized access, while reporting such actions to the Incident Response Team
- Prompting users for justification prior to allowing actions that could introduce risk
- Warning users of unsafe actions, while reinforcing corporate usage policies
- Encryption controls to protect information prior to being moved to file shares and removable devices
- Automated alert escalation to senior managers and the Incident Response Team when data sensitivity class, amount of data, and/or user access type met critical policy violation definition

THE RESULTS

Digital Guardian was deployed initially across 40,000 systems on three continents. The company improved business and security processes, while protecting critical IP from compromise through poor procedures or lack of employee risk awareness. Within months of implementation an insider threat incident was identified and stopped. With Digital Guardian in place, the company continues to build its IP protection program and integrate it into their overall Corporate Information Risk, Governance and Training.