CUSTOMER SUCCESS STORY

Global 100 Technology Conglomerate

TECHNOLOGY

Industry
- Technology

Environment
- 9,000 workstations
- Virtual desktops
- Internal users on five continents
- Scientists, Engineers
- Manufacturing
- Privileged users with direct physical access to Citrix® server hardware.

Challenges
- 15 business units with separate requirements
- Custom, proprietary software storing and managing IP
- Multiple written languages
- Multiple privileges for the same piece of data, varying by user and use case

Results
- Classification of all data based on data context and content, even on proprietary systems
- Immediate visibility into all user activity, without impacting productivity
- Enhanced data sharing without loss of IP
- Written, recorded justification for movement of critical data by email or to removable devices
- Automatic encryption of critical files moved by email or to removable devices

DIGITALGUARDIAN™ by VERDASYS

Data Visibility, IP Protection, and Secure Partner Collaboration

This global 100 engineering and electronics conglomerate had recently suffered a loss of proprietary intellectual property. Their highly competitive market required constant innovation, and their workforce had expanded to thousands of scientists, engineers, and technicians on five continents. With IP valued at over $30 billion USD, they understood they were an attractive target for IP theft. Now it had occurred, with no proof of who was the perpetrator. The company began an initiative to control more closely its IP and trade secrets, and turned to Digital Guardian® for assistance.

THE BUSINESS CHALLENGE

The company was concerned that identifying critical data would be difficult. As a technology manufacturer, it used many types of software in the design process, including source code for its software, 3-D computer-aided design and simulation software, and proprietary applications developed by its own engineers. A custom-built repository stored the majority of the design documents used by research, engineering, and manufacturing. Classifying this data was critical, yet the software was not used outside of the organization, so integrations with commercial tools did not exist. In addition, with a global workforce, emails and text files could be in any one of several written languages. Traditional lexical scanners could not classify the output from these easily.

Controlling access and use of IP had obviously been an issue in the theft. However, the company's competitive advantage could be maintained only by making data freely available to authorized users. Multiple users required access to the same data, but with different privileges for how they could use the data. Building data silos for each user group was inefficient and difficult to maintain.

Finally, some users occasionally needed the ability to move critical data to business partners by email or removable media drives. Their existing policy required users to encrypt this data first, but was difficult to enforce. The company wanted to require anyone moving data, first to provide written justification for the action. If approved, the data should be encrypted and stored only on approved devices.

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

- Improve data sharing across a global workforce while preventing IP loss
- Classify data in multiple formats and languages quickly and accurately
- Enforce appropriate use of data by users with varying privileges
- Allow authorized users to move data via approved methods, but only with appropriate and recorded justification

THE SOLUTION

The first task was to discover and classify all data. With support for 90 languages, DigitalGuardian could work with each of the separate offices to ensure appropriate coverage and messaging. For their proprietary information repository and SAP systems, the customer used Digital Guardian's classification API to build their own automatic classification rules. This provided context awareness for data stored in those systems, and complemented Digital Guardian's Context-based Data Awareness and Content Inspection features. All of the organization's critical data was classified quickly.

Digital Guardian solution architects worked with the customer to build policies in the Digital Guardian Management Server that properly reflected data use policies. This included use of Digital Guardian's "Prompt" mode when risk could be introduced by a user's action. Prompt mode blocks the action, prompts the user to enter justification for the action in a displayed form, and records all actions in a forensic-quality event log. Prompting was used when a user attempted to:

- Copy classified files to removable storage devices, including USB drives CDs and DVDs
- Print classified files in hard copy or to a PDF file
- Attach classified files to SMTP/Outlook emails

In addition to prompting the user for justification and approval, Digital Guardian prevented the use of unauthorized devices by authorized users. Only company approved device types with authorized serial numbers were allowed, so that data could be tracked after removal. Finally, Digital Guardian encrypted the classified files automatically. With encryption applied, decryption was restricted to workstations that host the company's Digital Guardian agent.

THE RESULTS

Digital Guardian designed a solution for this organization that exceeded their requirements and expectations. It allowed authorized access to critical data without extra steps or latency. Desktop and server agents enforced policies at the endpoints, where data was most vulnerable.

Digital Guardian logged all activity, and its evidentiary-quality event logs allowed visibility into where all critical data was and how it was used. The customer eventually expanded their use of Digital Guardian to other divisions, more than doubling the initial deployment.