CUSTOMER SUCCESS STORY

Global Pharmaceutical Company

HEALTHCARE

Industry
- Pharmaceuticals

Environment
- Over 95,000 Workstations
- Windows

Challenges
- Widespread distribution of critical data
- Third-party partner organizations
- Contractors and independent researchers
- Worker productivity is critical
- Application data must be protected when moved to other applications

Results
- Greater worker productivity and improved data protection
- Reduced complexity in managing IP
- Full visibility to all critical data throughout the organization
- Automatic, contextual classification of data
- Classification is maintained during data use, and propagated to derivative documents

DIGITALGUARDIAN™ by VERDASYS

Data Visibility, IP Protection, and Reduced IT Complexity

The pharmaceutical industry is research intensive. Companies spend millions of dollars and several years developing new drugs and conducting clinical trials. A company can cannot begin to recover this investment, through sales, until after approval from the Federal Drug Administration (FDA), or similar organizations in other countries.

This company is understandably protective of its intellectual property (IP). It exists in several forms, including documents, spreadsheets, and scientific applications. Losing this information would erode their competitive advantage, or could allow others to file for patents preemptively. In both cases, the monetary loss could exceed tens of millions of dollars.

When the company decided it needed better visibility into how Research and Development (R&D) scientists handled sensitive IP, Digital Guardian was there to help.

THE BUSINESS CHALLENGE

For each new drug produced, pharmaceutical companies require hundreds of researchers, scientists, and clinical trial organizations to work together efficiently. Delays in time-to-market erode revenues and profits. Any solution that helped monitor and control this company's IP must not impede the productivity of the users.

The scientific applications used by R&D professionals were an important repository for IP. The data resulting from these included specific formulae that may be required in other documents and data. The company required that information to remain confidential, even when moved between documents, inside or outside the original application environment.

Finally, the organization relied heavily on third party individuals and organizations, with whom it shared critical data. Independent scientists would work on projects, and independent organizations were required to conduct clinical trials. IP shared with these partners must be protected.

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

- Gain visibility into what R&D scientists are doing with sensitive data
- Enhance worker productivity while protecting data
- Protect data after it is moved between users and applications

THE SOLUTION

Digital Guardian personnel worked with the customer to identify sources of IP. This included four discrete applications used by R&D. Digital Guardian profiled these applications and configured its context-based, data awareness functionality to classify data on and from these systems as "sensitive" automatically.

Digital Guardian understands data and tracks its use throughout its lifecycle. Digital Guardian classifies data upon its discovery, access, creation, or revision, securely appending the classification tag to its host file or email. This tag persists throughout the life of the data. If a formula is copied from one document to another, or attached to an email, the tag propagates to the new document, providing continuous tracking and protection.

Since the customer's initial objective was visibility into data use, Digital Guardian was deployed in Monitor mode. In Monitor mode, actions are not blocked. Instead, Digital Guardian's kernel-level agents track every action, including copy, paste, email, and even printing. This allows users to conduct business as usual, while providing the company with complete visibility to all data use and movement.

When data exited each of the critical applications, it was classified and tagged appropriately. Digital Guardian agents on each server and workstation recorded data use and movement in evidentiary-quality event logs for reporting.

THE RESULTS

For the first time, the customer had visibility into how its scientists used critical information. Scientists, researchers, and contractors had uninterrupted access to the data they needed, and Digital Guardian allowed complete visibility into where data was created, how it was used, and where it was located, at all times.

Formulae, research results, and other data extracted from systems were automatically and appropriately classified, while Digital Guardian agents monitored all movement and use on endpoints. Classification was so effective, the company was able to reduce the number of applications handling critical data by 80%, reducing complexity and lowering maintenance and support costs.