



# Data Visibility, IP Protection, and Reduced IT Complexity



## About the customer

The process of bringing new drugs to market is a complex, costly, and regulated process, billions of dollars and years are tied up until an organization can realize any revenue. This company is understandably protective of its intellectual property; losing it could erode their competitive advantage, or allow others to file for patents preemptively. The company needed visibility into how Research and Development scientists handled sensitive IP.

## The Business Challenge

For each new drug produced, pharmaceutical companies require hundreds of researchers, scientists, and clinical trial organizations to work together efficiently. Time limits on patent protection means any delays in time-to-market causes measurable erosion in revenues and profits. Any solution that helped monitor and control this company's IP must not impede the productivity of the users or slow development.

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.

## Critical Success Factors

- Gain visibility into how R&D use sensitive data
- Enhance worker productivity while protecting data
- Visibility into data egress
- Protect data after it is moved between users and applications

## Industry

- Manufacturing (Pharmaceuticals)

## Environment

- 95,000+ Windows workstations
- Internal and external parties accessing IP
- Time sensitive product development process

## Challenge

- 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

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

## Data Types We Protect



### Chemicals/Pharmaceuticals

- Formulas
- Business Processes
- Supplier Contracts



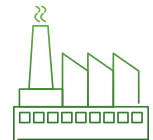
### Advanced Engineering

- Source Code
- Designs
- R&D Data
- Supplier Contracts



### Aerospace/Automotive

- Design Specifications
- CAD Drawings, Blueprints



### Contract Manufacturers

- Customer IP
- Component List
- Business Processes
- Customer Contracts

## The Solution

Digital Guardian 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. The InfoSec team could 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

Scientists, researchers, and contractors had uninterrupted access to the data they needed, and the InfoSec team had complete visibility into where data was created, how it was used, and where it was located. Formulae, research results, and other data extracted from systems were automatically classified, while Digital Guardian monitored all movement and use. Classification was so effective, the company reduced the number of applications handling critical data by 80%, reducing complexity and lowering overhead.



Digital Guardian Sales Partner

Request your personalized demo:  
[www.EPCUSA.net](http://www.EPCUSA.net)

**1-303-703-3609**