CUSTOMER SUCCESS STORY

# Fortune 100 Manufacturer

MANUFACTURING

**Industry**
- Manufacturing and Consumer Goods

**Environment**
- Enterprise deployment across 50,000 internal systems
- External deployment across 7,000 partner systems

**Challenges**
- Allow cross-functional access to data while maintaining control over confidential IP
- Integration of systems across internal and external users in India, China, Europe, and the Americas
- Real-time, automated data classification
- Reliance on third party scientists requires IP to sit outside corporate network

**Results**
- Sensitive IP is available only on Digital Guardian-secured devices
- Secure Outsourcing - Critical data is shared with external partners without loss of IP
- Automated data classification
- Data use policies communicated and enforced worldwide

DIGITALGUARDIAN™ by VERDASYS

## IP Protection, Secure Outsourcing, and Maximized Operational Efficiency

A $30 billion manufacturing and consumer goods organization needed help quickly. With over 60,000 employees and research and development resources worldwide, their extensive intellectual property (IP) allowed them to compete profitably in a competitive market. Then, a senior research scientist left to join a competitor. In preparing to do so, the scientist downloaded over 20,000 sensitive documents from the corporate network, and took at least 150 of those documents to his new employer. The organization estimated the cost of the data breach at $400 million.

## THE BUSINESS CHALLENGE

The staggeringly high number illustrates the high cost of stolen IP. The event prompted an initiative to introduce risk management measures to guard against an incident of this kind happening again.

The project, initially conceived as a response to a single incident and type of threat, grew to a review of data security throughout the value chain. This included all geographic and functional divisions, with data from research and development, through engineering to manufacturing, including sourcing and distribution.

## CRITICAL SUCCESS FACTORS

- Safeguard critical research while allowing authorized employees full access to engineering and manufacturing IP, whether in files or application databases
- Provide secure collaboration with third party scientists, manufacturers, and other business partners
- Enable secure and streamlined communications with remote offshore manufacturing locations

Simply locking down the information would not work. The company's competitive edge depended on ready access to this information to drive efficiency and collaboration. Due to the scale and complexity of the company's operations, any slowdown of the product development lifecycle would be unacceptable. The organization was not willing to sacrifice operational efficiency for security. They needed both.

# DIGITAL GUARDIAN FACTS

### Customers
- Over 250 customers
- 130 of the Global 2000 and government agencies
- Used by 7 of the top 10 patent holders
- Over 2,100,000 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

- Protect IP flowing through complex, internal and external communication channels, on and off the corporate network
- Classify data in real-time based on content and context, and apply it to the organizational data risk taxonomy
- Centrally administer organizational data security policy, allowing for risk appropriate action (e.g. blocking, warning, encryption, logging) based on classification of incident
- Create virtual "trust communities" that allow free and efficient collaboration between secured parties
- Maximize operational efficiency while introducing a previously unachievable level of data security

## THE SOLUTION

**Start with Secure Offshore Outsourcing**
Work with a new design partner in China provided an opportunity to run a pilot program of Digital Guardian. The company was extremely concerned about potential overseas IP loss, and viewed external parties as high-risk egress points for confidential data.

After evaluating operating environments and potential risk factors, Digital Guardian was used to build actionable and risk-aware information usage policies and controls. Sensitive IP would reside only on 25 Digital Guardian secured workstations. Those workstations did not have the authority or ability to transmit IP to any machine in Taiwan that lacked a Digital Guardian Agent, and were only permitted to send information back to machines in the US corporate headquarters also secured by Digital Guardian Agents. This created a virtual community of trust, and contained information by governing its use at the endpoint. Aggressive policies regarding device control (USB drives) and printing of confidential IP were also deployed. In less than two months, the team built a full pilot deployment to safeguard corporate intellectual property.

## THE RESULTS

Building on the success of the pilot, the team expanded their use of Digital Guardian to 5,000 workstations across five divisions in the US and China. The team used Digital Guardian's powerful data discovery capabilities and deployed the endpoint agents in monitoring mode to gain an accurate understanding of data flows within their organization. They then monitored and logged potentially risky actions (e.g. FTP to an outside destination) over 30 days to complete a detailed risk analysis and build an appropriate series of risk-aware data security policies. The new policies used content and contextual analysis to classify confidential data in real time, and, based on that classification, take risk appropriate actions. The result was a realization of the company's dual objectives – secure data interchange with minimal end user interruption and maximum operational efficiency.

Based on the success achieved through this expanded deployment, the organization rolled out Digital Guardian enterprise wide, which today safeguards data on over 50,000 internal workstations and 7,000 partner machines. The manufacturer is currently reaping the benefits of vastly safer operations, greater data security awareness, and improved collaboration from design to manufacturing.

Copyright © 2014 Digital Guardian, Inc. All rights reserved. Digital Guardian and Security's Change Agent are trademarks of Digital Guardian, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.