FORTRA™

CASE STUDY (Digital Guardian)

Defending Against a $400MM Breach

About The Customer

A $30b manufacturing and consumer goods company with over 60,000 employees relied on intellectual property to maintain their advantage in a competitive market. When a senior research scientist left, he downloaded over 20,000 sensitive documents and took at least 150 of those to his new employer. The organization estimated the cost of the data breach at $400 million.

The Business Challenge

Intellectual property can drive sustainable competitive advantage, but this makes it an appealing target. External parties look to steal this, and internal parties can be lured by monetary reward to aid in the theft. This incident highlighted the value and the risk of such a collection of intellectual property. Because the organization relied on a 60,000+ employee base and a network of 7,000 partners to develop and manufacture products, locking down the data would cripple the business. 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.

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 network. This included all geographic and functional divisions, with data from R&D, through engineering to manufacturing, as well as sourcing and distribution. The infosec team needed a way to, in real time, classify sensitive data without impacting workflows. This classification then needed to drive granular protection based on specific roles within the value network, including external parties. Further, the solution needed to scale to cover their global footprint while delivering the centralized visibility and control to the infosec team.

Critical Success Factors

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

INDUSTRY

- Manufacturing

ENVIRONMENT

- Enterprise deployment across 50,000 internal systems
- External deployment across 7,000 partner systems
- Suffered data breach by an insider
- Significant investment in intellectual property

CHALLENGE

- 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
- 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 content and context data classification
- Data use policies communicated and enforced worldwide

The Solution

Because of the critical nature of the data, the organization couldn't afford downtime, especially as they ramped for the holiday season. Work with a new design partner in China provided an opportunity to run a pilot program of Fortra™'s Digital Guardian® and adjust as needed for a global roll-out. The company was 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. They used content and contextual analysis to classify confidential data in real time, and, based on that classification, take risk appropriate actions. Sensitive IP would reside only on specific, Digital Guardian secured workstations. Those workstations did not have the authority or ability to transmit IP to any machine 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.

Data Types We Protect

CHEMICALS/ PHARMACEUTICALS

- Formulas
- Business Processes
- Supplier Contracts

AEROSPACE/AUTOMOTIVE

- Design Specifications
- CAD Drawings, Blueprints

ADVANCED ENGINEERING

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

CONTRACT MANUFACTURERS

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

The Results

Building on the pilot, the team expanded their use of Digital Guardian to 5,000 workstations across five divisions in the US and China, eventually expanding to 50,000 internal and 7,000 partner workstations. The customer gained an accurate understanding of data flows and created policies based on actual, not assumed, business processes. The result was a realization of the company's dual objectives – secure data interchange with minimal end user interruption and maximum operational efficiency.

About Digital Guardian

INSTALLED BASED

- Over 600 customers from across the globe
- Industries served: Business services, education, energy, financial services, government, healthcare, manufacturing, retail, technology
- Used by 7 of the top 10 patent holders

DISCOVERY AND CLASSIFICATION

- Endpoint, network, cloud and local data storage
- Content, context, and user classification
- Fully automated to fully manual classification
- Over 300 data types, over 90 languages

EDUCATE AND ENFORCE

- Monitor log, prompt, justification request
- Auto-encrypt, quarantine, move, block

ACTIONABLE ANALYTICS

- System, user, and data level event visibility
- Analytics that filter out the noise
- Drag and drop incident management
- Right click remediation in real time

OPERATION SYSTEM SUPPORT

- Full visibility, analytics and controls across multiple operating systems
- Mac
- Windows
- Linux

DEPLOYMENT

- On-Premise
- SaaS
- Managed Security Program

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.