FORTRA™

CASE STUDY (Digital Guardian)

Data Visibility, IP Protection and Secure Partner Collaboration

About The Customer

A global 100 engineering and electronics conglomerate had recently suffered loss of proprietary IP. With IP valued over $30 billion USD, and a workforce of thousands of scientists, engineers, and technicians on five continents, they understood they were an attractive target. Their current systems were unable to stop the breach or identify the perpetrator.

The Business Challenge

The company used multiple applications both commercial and proprietary in the design process, with a custom-built repository storing most of the documents. Classifying data was critical, yet the software wasn't used outside 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 languages - traditional scanners could not classify these easily.

The company's competitive advantage could only be maintained by making data freely available to authorized users, and multiple users required access to the same data, but with different privileges. Building data silos for each group was inefficient and difficult to maintain.

Finally, some users needed the ability to move data to business partners by email or removable drives. Encryption was required, but difficult to enforce. The company wanted anyone moving data to provide written justification, and if approved, the data would be encrypted and stored on approved devices.

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, but only with appropriate and recorded justification

INDUSTRY

- Technology

ENVIRONMENT

- 9,000 workstations and virtual desktops
- Users on five continents
- Scientists, Engineers, Manufacturing users
- Privileged users with direct physical access to server hardware

CHALLENGE

- 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 data based on context and content, even on proprietary systems
- Visibility into all user activity, without impacting productivity
- Enhanced data sharing without loss of IP
- Written, recorded justification for movement of critical data
- Automatic encryption of critical file movement

The Solution

The customer's first task was to discover and classify all data. With support for 90 languages, Fortra™'s Digital Guardian® could work with each of their offices to ensure appropriate coverage. For their proprietary information repository and SAP systems, the customer used Digital Guardian's classification API to build their own auto-classification rules. This complemented Digital Guardian's built-in context-based data awareness and content inspection features for a comprehensive data classification foundation.

Digital Guardian worked with the customer to build policies that properly reflected data use policies. This included use of a "Prompt" mode when risk could be introduced by a user's action. Prompt mode blocks the action, prompts the user to enter justification in a form, and records all actions in a forensic-quality event log. Prompting was implemented when a user attempted certain actions for copying, printing or attaching classified files.

In addition to prompting, Digital Guardian prevented the use of unauthorized devices. Only company approved devices 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 Digital Guardian agent.

Data Types We Protect

INTERNET & ADVANCED TECHNOLOGY

- R&D Data
- Customer Contracts
- Source Code
- Patents

SAAS

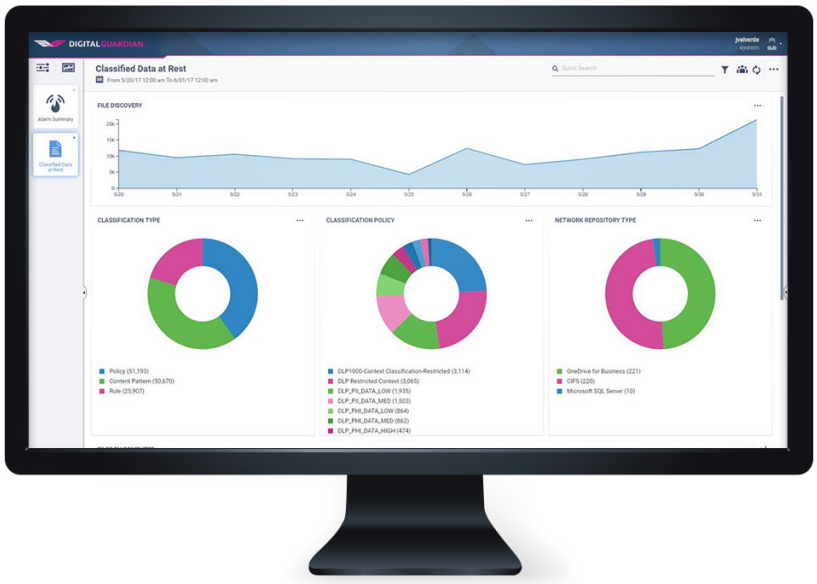
- Personally Identifiable Information (PII)
- Source Code
- Login Credentials
- Business Processes

SOCIAL NETWORKS

- Login Credentials
- Personal Information such as Pictures, Profile Data

TELECOMMUNICATION

- Personally Identifiable Information (PII)
- Privacy Data
- R&D Data
- Network Design
- Patents



The Results

Digital Guardian's solution exceeded the organization's requirements and expectations. It allowed authorized access to data without extra steps or latency, and desktop and server agents enforced policies at the endpoints, where data was most vulnerable. Evidentiary-quality event logs allowed visibility into where all data was and how it was used.

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.