FORTRA™

CASE STUDY (Digital Guardian)

Defending Formula 1 R&D Data

About The Customer

Formula 1 racing is competitive on and off the track. Teams invest heavily for faster, more reliable cars, and any advantage they can find. Sensors measure temperature, pressure, and acceleration. The information is sent via telemetry to engineers at the track and the team's research center.

This data is confidential to the teams and automotive sponsors. Small changes to the vehicle can increase speed, or improve cornering. In a sport where seconds separate winners from losers, data is king. Concerned that competitors were attempting to access their designs, the team decided to take steps to protect their competitive advantage.

The Business Challenge

The team's designs are developed and tested at their research center in Europe. Data is also on laptops at race venues around the world. The large amount of data processing equipment used required the team to travel with not only drivers and crewmembers, but also its own IT infrastructure.

Mobility also reinforced the team's decision to focus on protecting the data instead of the device. Data is what their competitors wanted. The customer needed to ensure that information from the research center and teams at race venues was available to authorized users while preventing exfiltration of information by electronic transmission or downloading to removable drives. All actions, even those authorized by policy, required monitoring and logging.

Critical Success Factors

- Unfettered access to data by authorized users
- The ability to block egress of data and record all authorized actions
- Enable their mobile IT infrastructure to travel to races worldwide while securing IP at these remote locations
- Support multiple data types, including CAD drawings, documents, spreadsheets, and scientific data
- Require users to justify actions when data was moved and log all responses

INDUSTRY

- Manufacturing

ENVIRONMENT

- 2,000 Windows and Linux workstations
- Sensitive engineering data
- Remote locations at 20 race venues around the world
- R&D locations in home country

CHALLENGE

- Remote IT infrastructure at 20 race venues around the world
- Remote workers who required internet access
- Multiple scientific applications and data types
- Sensitive data on hundreds of devices needed by users with legitimate data requirements
- Privileged users with root access to devices

RESULTS

- Visibility and control of data movement
- Identification of breach
- Evidentiary quality logs document data movement
- Perpetrator sentenced to prison
- Rival team fined $100 million

The Solution

For the race team, no data classification was required. They considered all data residing on their hardware as sensitive. Specific policies were created to address known egress risks, and Fortra™'s Digital Guardian®'s kernel level agents enforced those policies. The agents allowed authorized users to access information, while detecting attempts to move, copy, or otherwise misuse the data. Digital Guardian was deployed on all devices, including in the team's mobile IT infrastructure facility. Specific controls include block, log, report and alert on high risk activities, such as copies to removable devices, unloads to non-sanctioned cloud storage, or emailing.

If exceptions to these policies were required, Digital Guardian prompted the user with a form to acknowledge the risk associated with the exception, and provide a justification for their actions. This request, by itself, often dissuades users from engaging in risky behavior. In addition, the company required specific reports that were available out-of-the box with Digital Guardian. These included data discovery and investigative reports of attempts to hide, delete, encrypt, screen shot, or print sensitive data.

Data Types We Protect

CHEMICALS/ PHARMACEUTICALS

- Formulas
- Business Processes
- Supplier Contracts

AEROSPACE/AUTOMOTIVE

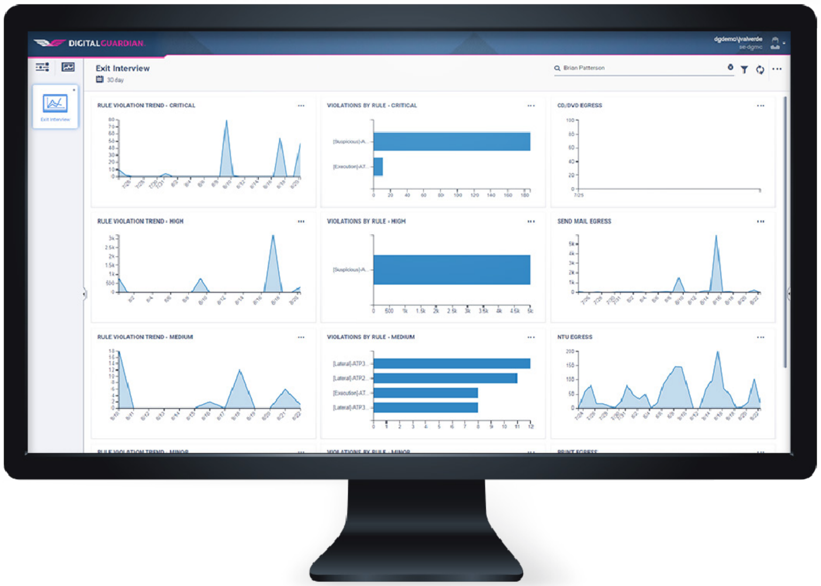
- Design Specifications
- CAD Drawings, Blueprints

ADVANCED ENGINEERING

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

CONTRACT MANUFACTURERS

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



The Results

Hundreds of pages of design information were discovered with a competitive team. Digital Guardian's advanced forensics and reports determined the identity of the employee who printed the documents. Further, Digital Guardian confirmed that at no time had another employee or contractor printed the document, or any portion of it.

With this evidence, the employee was dismissed and the rival team fined $100 million. Digital Guardian's evidentiary-quality logs were later used in legal proceedings, where the engineer was tried and sentenced to prison.

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.