CUSTOMER SUCCESS STORY

Luxury Sports Car Manufacturer

MANUFACTURING

Industry

- Automotive

Environment

- 2,000 Workstations
- Windows®
- Linux®
- Remote locations at 20 race venues around the world
- R&D locations in home country

Challenges

- 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

- Blocked data movement
- Identification of breach
- Evidentiary quality logs could determine:
- Who printed the data
- Which printer was used, and when
- That no other person had ever printed the document, or segments of the document
- Perpetrator sentenced to prison
- Rival team fined $100 million

DIGITALGUARDIAN™
by VERDASYS

IP Protection, Incident Response, and Forensics

Formula 1 racing is competitive on and off the track. Automotive companies spend millions of dollars on research used in these advanced vehicles. Sensors measure engine temperature, oil pressure, air pressure, acceleration, and g-force. The information is sent via telemetry to engineers at the track and the team's research center.

This data is extremely confidential to the teams and automotive sponsors. Small changes to the vehicle can increase speed, or improve cornering and handling. 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. They called on Digital Guardian®.

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

DIGITAL GUARDIAN FACTS

Customers

- Over 250 customers
- Inlcudes 130 of the Global 2000 and government agencies
- Used by 7 of the top 10 patent holders
- Over 2.1 Million 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

THE SOLUTION

For the race team, no data classification was required. They considered all data residing on their hardware as classified.

Specific policies were created using the Digital Guardian Management Console to address known egress risks, and 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, with the following controls:

Digital Guardian Kernel-level Agents

On a computer, the kernel manages all requests and system calls to the CPU, memory, and input/output devices such as print drivers, disk, and USB drives. By integrating at the kernel level, Digital Guardian agents monitor and control data from within the operating system, on or off the network.

- Identify, log, report, and alert on high risk activities, including those by privileged users such as system administrators
- Block all writes, edits, and copies to removable storage devices
- Log all legitimate uses of data, including printing
- Block network transfers to cloud, email, or instant messaging applications
- Prevent the installation and execution of specific applications

If exceptions to these policies were required, Digital Guardian could prompt the user with a form to a) acknowledge the risk associated with the exception, and b) provide a justification for the exception. This action, 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:

- Data Discovery based on parameters such as user, data item, or device, and including hidden, password-protected, and encrypted files. Discovery reports can provide listings of all relevant files and discovered file information, and allow organizations to know precisely where their critical data resides.
- Investigative Reports detailing data authorship, and any attempts to hide, delete, protect, encrypt, copy, cut, paste, print, or screen capture data.

THE RESULTS

The company's initial assumption was correct. Hundreds of pages of design information were discovered with a competitive team. Using Digital Guardian's advanced forensics and Investigative Reports, the company determined the identity of the employee who printed the document. The reports also pinpointed the date and time the document was printed, and the physical printer used. 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.