CUSTOMER SUCCESS STORY

DIGITAL GUARDIAN®

Leveraging Data Discovery to Drive Data Security

About the Customer

One of the largest U.S. non-profit corporations provides insurance, discounts, advocacy, and financial services to over 9 million members. The company understood the need to protect all of their members' personal information from theft or misuse, but became concerned with the effectiveness of their current solution for identifying where personal data was located and how it flowed throughout their organization.

The Business Challenge

The company, like all organizations providing insurance and financial services, depends on maintaining the trust of its members. This includes ensuring the security of members' personal information. While the company had not been breached, they were aware that sensitive information on millions of members was an attractive target for hackers. Some services require the company to collect Personally Identifiable Information (PII) from its members, including Driver License, Social Security, and credit card information; all potentially subject to regulatory compliance.

They first needed to identify where their sensitive data resided. In any organization, identifying sensitive data in both structured and unstructured form can be difficult. Documents, spreadsheets, data files, and images must be evaluated to determine whether they contain sensitive information. The company's job was made more challenging by the differing standards used by each individual state and territory for assigning driver license numbers. Unlike the consistent formats used by major credit card issuers, each state creates its own standard, ranging up to 17 alphanumeric characters.

Critical Success Factors

- Automatically identify and classify sensitive data in structured and unstructured forms, across the enterprise
- Watch, Learn, Implement - Help create useful policies by mapping the use of critical data in their environment prior to policy development
- Support multiple formats and rules used by states and territories for classifying driver information
- Support Windows, Mac, Linux, Citrix, and virtual environments

Industry

- Insurance & Financial Services

Environment

- 8,500 endpoints
- Windows, Linux, Mac
- Citrix Virtual environments

Challenge

- Locate and identify sensitive data in structured and unstructured forms
- Multiple data formats for driver license data
- Multiple egress channels, including network transfer uploads
- Inspect data at rest and in motion

Results

- Visibility to all sensitive data
- Clear controls to support club policies
- Protection of data at rest and in motion

Data Types We Protect

Banking

- Personally Identifiable Information (PII)
- Payment Card Industry (PCI DSS)

Insurance

- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Payment Card Industry (PCI DSS)

FInancial Markets

- Intellectual Property (IP): Deal Management Information, Trading Algorithms, Financial Modeling, IPO Plans, M&A Plans

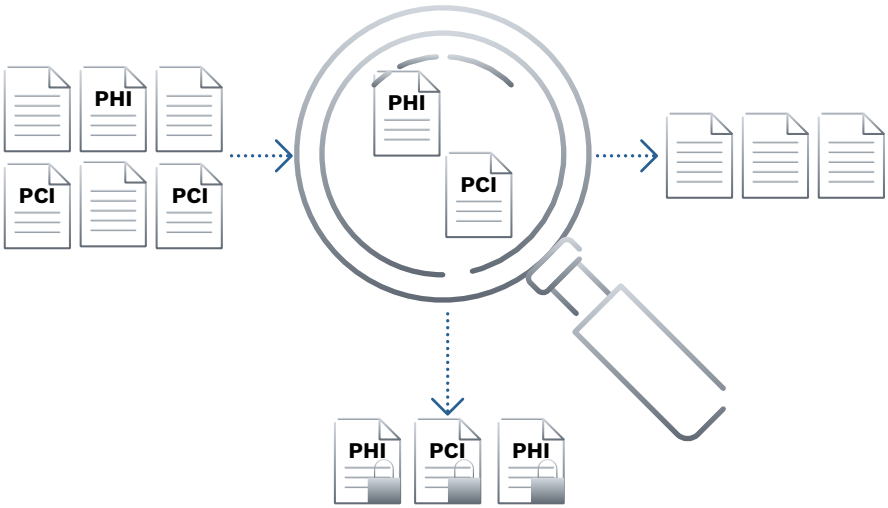
The Solution

The most critical feature of any data loss prevention solution is the ability to accurately locate and identify sensitive data, in all formats, wherever it resides. Manually classifying data is inconsistent and subject to human error. Digital Guardian worked with the company to understand the different rules used by each state and territory to create driver license numbers. The ability of Digital Guardian's automated classification to inspect content on-the-fly and support multi-factor rules, simplified PII identification while minimizing false positives and negatives. DG's endpoint agents automatically identified PII, providing the company with its first ever, verifiable map of the sensitive data in their environment, including how that data was used.

Once the company had visibility to its members' sensitive data, it then needed controls to ensure the data was handled properly. DG worked with them to design and document policies that protected PII from misuse while allowing legitimate use. Policies covering egress channels, including company email, web mail, file transfer services, and removable storage devices could be created and refined to support legitimate use but block unauthorized use, whether malicious or accidental. Warnings could be provided to users when legitimate, but risky use of data was required.

The Results

The company's evaluation pointed to Digital Guardian as the optimal solution. By providing a clear picture of where sensitive data resided and how it was used, sensible controls were put in place to enforce proper use of the PII. A rollout to over 8,500 endpoints will ensure that the members' trust in the company was well deserved.



About Digital Guardian

Installed Based

- Over 700 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

- Managed Security Program
- SaaS
- On-Premise

DIGITALGUARDIAN®