CUSTOMER SUCCESS STORY

DIGITAL GUARDIAN®

Enabling Employees to Protect Sensitive Client Information

About the Customer

The company is a multinational human resources consulting firm with about 29,000 employees worldwide. The firm specializes in human resource services for temporary and permanent jobs, including contract staffing of professionals and senior managers.

The Business Challenge

Professional staffing relationships are built on trust, with both candidates and clients, and the responsibility of maintaining confidentiality for thousands of job openings, and the privacy of millions of candidates. In a competitive environment, maintaining trust can be the difference between success and declining margins and revenue. The new director of privacy and security at the company understood this well. When he became concerned about confidential information on candidates and clients being leaked through poor security habits, he began to look for solutions.

The company collects and maintains confidential information on candidates and salaries, including Personally Identifiable Information (PII) subject to regulatory requirements. Protecting this information from attackers and inadvertent disclosure required a comprehensive, but flexible security solution.

The director's task was complicated by separate IT infrastructure in each of its 1,000+ offices, and differing privacy requirements in each jurisdiction. In addition, they operated with a lean IT team and capital budget, therefore could not take on workload for deploying and managing new tools. A managed solution was required, but one that would not adversely affect the culture of trust within the organization.

Critical Success Factors

- A low impact on staffing and CapEx delivery model with proven reliability was imperative, along with support for analysis of activity and alerting when thresholds were passed.
- The solution needed to support the company's culture of trust and provide feedback to users in a positive manner.
- Granular visibility to inappropriate actions - down to individual users - was required in case of breaches and to inform actions if needed.
- Security and risk decisions must support business goals and objectives

Industry

- Business Services

Environment

- Enterprise Deployment across 10,000 workstations in over 1,000 locations
- Internal users; Privileged users
- Sensitive employer and candidate information

Challenge

- Lean IT team; seamless integration with a 3rd party IT vendor
- Provide positive user feedback
- Reporting for enterprise-wide data movement and granular visibility
- Provide evidence to corporate leadership that policy violations existed and could be handled in a positive manner

Results

- Visibility into movement of expected data (PII), and unexpected data (media files).
- Business-wide alignment on value of data visibility; controls for appropriate use policies.
- Immediate improvements in employee awareness of sensitive information
- Self-policing by employees

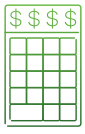
Data Types We Protect

Business Consulting

- Client Data – PII, PHI
- Product Roadmaps
- Go to Market Strategy
- M&A Data
- Business Processes

Technology Consulting

- Source Code
- System Architecture
- R&D Data
- Personal Information (PII, PHI)
- Login Credentials



Bookkeeping, Taxes and Accounting

- Customer Data (PII)
- Financial Data
- M&A Data
- Tax Data

The Solution

Only Digital Guardian's Managed Security Program (MSP) could provide the full-service deployment and support the company's staff required, along with automated classification and enforcement options.

Digital Guardian's MSP consultants worked with the company to understand their appropriate use policies for different data classifications and transform those into rules that could be enforced automatically, or simply provide reminders to users of appropriate policies.

Digital Guardian automatically classified data based on the source of the data (e.g., HR systems) and the content of the data (e.g., social security numbers and other PII). Automatic classification removed the burden of manually classifying each document or piece of content manually and helped better comply with regulatory standards.

The Results

Starting with deployment in a single office, Digital Guardian's MSP team monitored the company's activities to identify those which violated policies. The initial focus was preventing sensitive data exiting the company; losing PII through email or downloads. The initial policy violations they found, however, were for the opposite problem. Unauthorized copywrite-protected data was entering the company as employees used the corporate network to download movies. This presented risk in terms of copyright violations as well as the introduction of malware. The company's risk team was able to present the evidence of misuse in aggregated form purposely, to not disclose individuals who violated the policy. This and other policy violations served as a learning tool and did so without embarrassing individual employees.

Digital Guardian allowed the company to identify and deter activity not in alignment with acceptable use policies, while treating individuals as the valued employees they were. Presenting Digital Guardian "prompts" to users before a policy violation was completed provided ongoing reminders, allowing users to "self-correct". Employee awareness for the handling of sensitive information improved immediately and the number of policy violations dropped precipitously in just two months.

> *"With Digital Guardian we had the enterprise wide visibility to go from just a hunch to confirmation. We used this confirmation to drive changes within the organization to better protect our client's valuable information."*
>
> **- Director Enterprise Risk and Security**

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®