CUSTOMER SUCCESS STORY

DIGITAL GUARDIAN®

Consolidated DLP and EDR for Internal and External Threats

About the Customer

At one of the world's largest data management companies, the value of proprietary information was always clear. It was the primary reason its customers used its solutions. This also included their own proprietary information; data which allowed it to compete effectively in a crowded market. With thousands of employees worldwide, the company recognized the risk to valuable IP from attacks originating both inside and outside the organization.

The Business Challenge

The company's data included source code, design documents, customer information, and internal financial records. They required a solution that would recognize the different types of data and apply appropriate controls, automatically. Manually classifying millions of documents, aside from being ineffective, was simply not possible.

The company started with Data Loss Protection, but also recognized the growing risk from outsiders using advanced techniques to gain a foothold in their environment, move laterally, and access confidential data. While adding Endpoint Detection and Response (EDR) was important, they needed a solution that would block malicious activity instead of simply generating alerts to security. They also sought a way to reduce complexity with a solution from a single vendor. With this eye toward consolidating agents on its endpoints, the company sought a single solution to address both insider and external threats across the enterprise.

Finally, whatever solutions they select must be available as a managed service through a trusted partner.

Critical Success Factors

- A single solution to address both insider and outsider threats across all egress channels
- A fully managed solution to alleviate internal staffing challenges
- Automatically identify and classify sensitive data for multiple data formats
- Support compliance efforts across multiple jurisdictions and protect critical IP
- Blocking prohibited actions instead of just providing alerts

Industry

- Technology

Environment

- 16,000 endpoints in over 50 countries

Challenge

- Internal and external threat protection without the complexity of multiple solutions, agents, and management consoles.
- A trusted partner to deploy, monitor and manage the solution
- Automatic classification of new and existing data to drive data protection accuracy
- Thousands of endpoints in hundreds of offices

Results

- MSP solution rolled out to over 16,000 endpoints within 6 months of initial deployment
- Single agent and interface for both insider and outsider threat protection
- A fully managed solution providing improved security with lower overhead.

Data Types We Protect

Internet & Advanced Technology

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

Social Networks

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

SAAS

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

Telecommunication

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

The Solution

The company issued separate RFI's for DLP and EDR. While they had previously licensed Digital Guardian's DLP solution, they were unaware of Digital Guardian's Consolidated DLP and EDR offering. Once provided information on this solution, it became clear they could address both external and internal threats with a single agent on the endpoints and a single management console. The subsequent competitive bake-off revealed Digital Guardian as the ideal partner.

Digital Guardian's MSP team translated the company's desired policies into a set of enforceable controls on every endpoint. This allowed the company to have full visibility to all data types and enforce controls to prevent data loss through printing/emailing documents or downloading to unauthorized devices. All without the overhead and learning curve of deploying multiple on-premises solutions. A single console for building, deploying, and monitoring DLP and EDR greatly simplified management and reporting.

Digital Guardian's automated classification eliminated any need to manually classify millions of existing documents, spreadsheets, and other files. Automatic classification assigns policies to data based on the source of the data (e.g., department, user, application, server) or on the contents of the data (e.g., PII, credit card information) to protect data from misuse and simplify regulatory reporting. This ensured a quick deployment for initial testing, and rapid time-to-value for the company.

The Results

An initial installation on 500 devices proved successful so quickly that within 6 months the company rolled out Digital Guardian's Managed Service Program to over 16,000 endpoints and servers. The ability to cover both internal and external threats through a single partner simplified and improved the company's security program, while reducing overhead.

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®