



# Protecting Call Center Data from the Endpoint to the AWS Cloud

## About the Customer

This global leader in workforce management engagement relies on customer interactions and the billions upon billions of data points they generate. Collecting the data points is one thing, but to deliver meaningful, predictive, and personalized results requires a platform that can analyze these and spot the trends among the broad data pool.

## The Business Challenge

To deliver upon the promise of personalization at scale the organization must gather, understand, and leverage “customer moments,” each of these often contains sensitive information that must be protected. The more data they can gather, the better the ability to foster customer trust and loyalty but the more they must ensure it is protected from loss or theft. In the words of their CISO,

*“We understand that we are entrusted with deep insights into our customers, we must treat that information with the utmost care or risk losing the trust of our customer.”*

The Information Security team realized how critical it was to the business to deploy a data protection program but needed a solution that could see all their data and stop high risk behavior before an incident without excess complexity. Finally, they needed to show rapid return on their security investment both to protect sensitive data and satisfy financial metrics.

## Critical Success Factors

- Complete data visibility and protection from endpoints to the cloud
- Emphasis on source code protection
- Granular controls from “Log” to full and automated “Block” of the highest risk activities
- Multi-OS, browser, and application support
- Low overhead and immediate value

## Industry

- High Tech

## Environment

- Blend of intellectual property and PII
- 7,500+ endpoints
- Heterogeneous mix of OSs, browsers, and applications

## Challenge

- Constantly evolving pool of data from customer interactions
- Windows, Mac, and Linux endpoints
- Lean IT and IS staff
- Need granular data protection controls

## Results

- Simple purchase and rapid deployment
- Instant visibility into all data movement from endpoint to cloud
- DG, powered by AWS, meant no on-site HW or SW to support DLP

## 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 customer chose Digital Guardian to help them discover and protect the expanding pool of what they deem sensitive data today and enable them to expand their data protection program as their data patterns evolve. The SaaS deployment option, powered by AWS, allowed Genesys to spin up their DLP program quickly without any on-site hardware or associated software. Further simplifying the process was the AWS Marketplace, they purchased the Digital Guardian platform without a lengthy contract negotiation process due to previously agreed-upon terms.

The organization deployed the Digital Guardian platform to over 7,500 machines, a mix of Windows, Mac, and Linux endpoints. DG's multi-platform coverage was a key factor for Genesys as their data spans multiple operating systems, browsers, and applications both off the shelf and custom built. Of particular interest to Genesys was their source code as it was checked out and worked on by remote engineering teams. Digital Guardian was the only DLP vendor that could provide the full coverage for their diverse environment.

With endpoint to cloud visibility the customer could build policies based on how data actually moved throughout the organization. They applied the policy controls they needed to all their data, ranging from logging actions to automated blocking with far more accuracy. The controls flexibility enabled them to stop the actions they deemed the highest risk, while allowing, but still tracking, all others.

## The Results

- Simple purchase, rapid deployment & minimal complexity
- Instant visibility into all data movement across 7,500 endpoints
- Protection of source code for both on site and remote employees
- Accurate policies built from actual data flows
- Reporting to show highest risk areas and track improvement

“*... The Digital Guardian Data Protection Platform provides us with deep visibility and flexible controls, enhancing the protection our data and IP. Additionally, the ability to purchase the platform from AWS Marketplace enabled us to avoid lengthy contract negotiations and streamline the procurement process.*”

*Chief Information Security Officer*

## 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

### 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 Windows, Linux, and Mac operating systems

### Deployment

- SaaS
- Managed Security Program

