Start with the Most Comprehensive Data Classification

Digital Guardian data classification can automatically locate and determine how the data is handled. Our comprehensive data classification solutions - from automated content and context-based classification to manual user classification - are optimized for regulatory compliance, intellectual property protection, and mixed environments.

By understanding what sensitive data you have, where it is, and how it’s used, you’re in a better position to apply the appropriate controls.

Deepest and Broadest Visibility

Gartner

The Most Comprehensive Data Classification Solution
Digital Guardian incorporates the full range of classification from fully automated to manual user classification. Digital Guardian’s unique, context-based classification can automatically identify and tag sensitive data even before you develop policies. Our automated content-based file inspection identifies, tags and fingerprints sensitive data for the lowest false positives. User classification empowers users to classify sensitive data based on business requirements. Each can be used singly, or combined to deliver the most comprehensive data classification solution.

The #1 Rated Technology by Gartner for IP Protection
Only Digital Guardian’s context-based classification provides the intelligence to classify unstructured data such as intellectual property (IP) automatically, as it is created or modified, based on the user, source, and application. It automatically adds a security tag to each individual piece of data that dictates customized permissions, taking into account the type, content, and/or author. It’s just one reason that Gartner rates us #1 for IP protection.

More Accurate DLP and Endpoint Detection & Response
Digital Guardian data classification is integrated into our Threat Aware Data Protection platform. That means that your organization’s classified, sensitive data is identified and tagged for both Data Loss Prevention (DLP) and Endpoint Detection & Response (EDR) use cases. This increases data protection efficacy as well as threat hunting and incident response efficiency by incorporating data sensitivity levels into alert prioritization.

Gartner Critical Capabilities for Enterprise Data Loss Prevention, 10 April 2017, Brian Reed, Deborah Kish
Key Benefits

Get Rapid Time to Value
Digital Guardian automated classification drives repeatability and predictability. It also speeds implementation time by enabling you to classify even before formal policy creation. And DG User Classification integrates natively in Office applications for minimal change in workflows.

Drive More Efficient Security
Digital Guardian classification organizes and prioritizes data, enabling organizations to proactively assign data protection resources to the most valuable data. This ultimately drives more efficient security.

Use Data Classification as an Enabler
"In effect, data classification enables a less restricted handling of most data by bringing clarity to the items requiring the elevated control."

- Gartner, Understanding Insider Threats Published: May 2, 2016, Erik T. Heidt, Anton Chuvakin

---

Digital Guardian's threat aware data protection platform safeguards your sensitive data from the risks posed by insider and outsider threats. By harnessing our deep data visibility, real-time analytics and flexible controls, you can stop malicious data theft and inadvertent data loss.