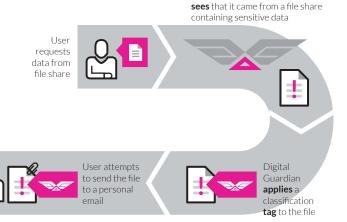**DIGITAL**GUARDIAN®
Data Loss Prevention

> CHOOSE THE INDUSTRY'S MOST COMPLETE DLP

Breaches are inevitable, losing data is not. **Digital Guardian for Data Loss Prevention** gives you everything you need – the deepest visibility, the fine-grained control and the industry's broadest data protection coverage – to stop sensitive data from getting out of your organization.

Digital Guardian for Data Loss Prevention is consistently a leader in the Gartner Magic Quadrant for Content-Aware Data Loss Prevention (DLP).

Digital Guardian offers unprecedented data visibility and control at the endpoint

User requests data from file share

Digital Guardian **sees** the file and **sees** that it came from a file share containing sensitive data

Digital Guardian **applies** a classification **tag** to the file

User attempts to send the file to a personal email

Digital Guardian **sees** the tag, **understands** the context, and **protects** by blocking the file transmission

CONTROL ALL DATA MOVEMENT AND TRANSMISSION WITH CONTENT AND CONTEXT-AWARENESS
- Set the DG agent to automatically prompt or block a user activity depending on the context, then log and audit the event for forensic analysis. Only Digital Guardian gives you full content inspection and context awareness that is data, user & event aware. Broader context enables more effective, real-time visibility & control.

ENFORCE DATA PROTECTION POLICIES ACROSS ALL EGRESS CHANNELS
- Set policies to automatically block, justify or automatically encrypt sensitive data in or attached to email, or files moved to removable drives or cloud storage.

STOP DATA THEFT – WITHOUT IMPACTING PRODUCTIVITY
- Design policies with fine-grained controls that won't block actions that comply with corporate policy so employees remain productive while the data stays safe. With Digital Guardian your data is made intelligent. Our software automatically blocks only those actions that pose a threat to your organization. Its unique, contextual awareness lets you minimize risk while maintaining the pace of your business.

DIAL-IN ADVANCED CLASSIFICATION OF SENSITIVE DATA ON ENDPOINTS
- Create and modify detailed classification and usage policies through full content inspection, context-awareness and user classification.

CONTROL DOCUMENTS ON MOBILE DEVICES WITH THE DG MOBILE APP FOR IOS
- Give your end users a secure document viewer for Microsoft Office, Apple iWork, and PDF documents on iOS devices. The DG Mobile App is classification aware and enforces policies consistent with DG agents to alert/notify, prompt or block users.
- Prevent unencrypted documents to be copied or redirected to another app, container, or other medium.

GET GRANULAR CONTROL OF ALL DATA MOVEMENT TO DEVICES/MEDIA
- Assign access permissions and encryption methods to removable devices or media including Non-Portable Encryption (access on network only) and Portable Encryption (self-contained for use on systems without an agent).
- Limit the types of files which can be transferred onto removable devices/media, and the amount of data which may be transferred by time interval (e.g., MB per day).
- Restrict data movement to devices/media by brand, model or serial number.

EXTEND YOUR DATA PROTECTION WITH DG ADD-ON MODULES
- Digital Guardian offers a suite of add-on modules that provide advanced encryption, extend your data protection to the network and more.

DIGITALGUARDIAN®
by **VERDASYS**

WHY DIGITAL GUARDIAN FOR DATA LOSS PREVENTION

1 BROADEST VISIBILITY AND CONTROL

Our solution offers the industry's broadest protection coverage, including Windows, Mac and Linux endpoints, recognizing both structured and unstructured files running on multiple systems. It's the only DLP solution that protects data on and off the network. With Digital Guardian, you have complete data visibility and control regardless of what users are running, what they're running it on, and whether or not they're on the network.

2 AUTOMATED CLASSIFICATION – WITHOUT PREDEFINED POLICIES

Most data loss prevention solutions require you to spend weeks or months identifying and classifying your sensitive data before protection starts. Digital Guardian begins as soon as you install it, proactively tagging and classifying PII, PCI and PHI data.

3 SCALES TO 250,000 USERS ON ONE CONSOLE

Digital Guardian is as robust as it is stable, designed to be easily and efficiently deployed across your entire user base. It's the only agent-based DLP technology covering 250,000 employees using a single management server. One of the largest and most respected companies in the world has deployed over 300,000 agents.

4 FLEXIBLE DEPLOYMENT

Only Digital Guardian offers complete data protection through an on premise solution, cloud-based managed service, or a hybrid of both. Our cloud-based managed services are the answer if you have more IP than IT. As an extension of your team, we'll expertly develop, deploy, and manage all of your policies enterprise-wide as if they were our own.

DIGITAL GUARDIAN PRODUCT PLATFORM

Digital Guardian is the only data-centric security platform designed to stop data theft.

DGMC
Digital Guardian Management Console

Your web-based command center. Deploy agents, create and manage policies, alerts and reports.

Advanced Threat Protection
Advanced threat detection, incident response and prevention that ensures security travels with the data.

Data Loss Prevention
Everything you need to stop sensitive data from getting out of your organization.

Data Visibility & Control
Out-of-the-box data visibility and device control.

DG Agent
The only endpoint agent compatible with Windows, Mac & Linux.

ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data-centric security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years we've enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

SHARE