A New Dawn for Data Loss Prevention

Data Loss Prevention is More Important Than Ever

**HERE'S WHY WE'RE REINVENTING IT.**

In the past few years Data Loss Prevention (DLP) has seen a major resurgence, and that's expected to continue. According to Gartner, by 2020 85% of organizations will have implemented DLP, up from 50% today. But Digital Guardian is challenging the security industry to expand their thinking about data loss prevention.

A DLP solution that is limited to protecting data from well-meaning or malicious insiders is no longer sufficient. The demand for data protection within your enterprise continues to grow, as does the variety of threats challenging your security team. Given today's evolving threat landscape and shortage of security talent, security professionals should demand vendors do more.

**REPLACE 3 TOOLS WITH 1**

Our purpose-built, cloud-native architecture utilizes streaming data from DG endpoint agents and network sensors to provide deep visibility into system, data and user events. That deep visibility powers security analyst-approved workspaces that provide information security analysts, incident responders and threat hunters with the context they need to identify, respond to and remediate threats to your sensitive data faster and more efficiently - regardless of the threat.

This unified solution delivers the product consolidation CISOs must demand. Our platform puts your most sensitive information assets at the center of all data protection, activity monitoring and endpoint detection and response activities.
The Digital Guardian Data Protection Platform

DG CLOUD
Reduces overhead, friction and cost while delivering the most comprehensive data protection available today.
- Immediate time-to-value — no hardware, additional software or configuration required
- Drives down cost and complexity
- Instant scalability

DG ANALYTICS
Correlates and analyzes system, user and data events from endpoint agents and network sensors to provide the deep visibility and context needed to identify and remediate ALL threats
- 100+ behavior-based rules
- Anomaly detection with advanced statistical models and machine learning

DG WORKSPACES
Enables InfoSec Analysts, Incident Responders and Threat Hunters to:
- Surface the real threats and real risks
- Pivot and drill-down to investigate
- Drag and drop to create a complete timeline
- Right click to remediate in real time

DG MANAGEMENT CONSOLE (DGMC)
Enables configuring and deploying agents, and managing policies, alerts, and reports.

DG ENDPOINT AGENT
Delivers the deepest visibility available on the market. It captures and records all system, user and data events - on or off the network.
- Unique context awareness or controls blocks only those behaviors that pose a threat to your organization
- Full OS support – Windows, MacOS, Linux, VDI – the broadest and deepest system coverage available

DG NETWORK APPLIANCE
Protects data at rest and in motion with low overhead. Our physical or virtual appliances classify, monitor and control sensitive data across your networks, storage repositories, databases and cloud applications like Office 365.

DG APPLICATIONS
Solutions that meet the broadest range of data protection use cases.
- DG Data Discovery – get visibility and auditing of potentially vulnerable data
- DG Data Classification – leverage the most comprehensive classification including content, context and user-based
- DG Data Loss Prevention – stop sensitive data from getting out of your organization
- DG Cloud Data Protection – stop loss of data in cloud applications such as Office 365
- DG Endpoint Detection & Response – detect, investigate, and mitigate suspicious activities and behaviors at the endpoint
- DG User & Entity Behavior Analytics – detect anomalies in user behaviors indicative of a threat

DG INTEGRATIONS
Digital Guardian has developed custom applications and leverages APIs to integrate with the products you already own. Integrations include:

Microsoft, IBM, Splunk, Boldon James, Ciscos, Micro Focus, Box, Citrix
Platform Benefits

Analytics that Filter Out the Noise
Digital Guardian monitors the most comprehensive set of events about your systems, users and data, quickly filtering through potential anomalies. It only triggers alarms for the high fidelity events that warrant additional investigation by InfoSec and/or SOC Analysts.

Drag and Drop Incident Management
Analysts can simply drag and drop to create new incidents, add events or alarms. It’s easy to add comments and artifacts. A timeline automatically builds out as you investigate an incident and work towards remediation, accelerating response time.

Security Analyst-Approved Workspaces
DG's experienced threat hunters and information security analysts developed workspaces to guide security professionals to the events that matter for identifying anomalous and suspicious insider and outsider activity. Analysts can easily drill down to follow an investigation and determine next steps or to create custom dashboards, reports and workspaces.

Right Click Remediation in Real Time
Security analysts can blacklist processes across the enterprise from virtually any screen for real time remediation of threats identified during incident response or threat hunting. Remediation options include blacklist, scan, warn on launch, send to VirusTotal, and more.

Choose Your Deployment Model

Manage Security Programs
Digital Guardian’s Managed Security Programs act as a remote extension of your team and offers data protection as a managed service. Our security experts will host, administer and run your data security platform. These 24x7 global analyst teams that live, eat, and breathe data protection will help you contain insider and outsider threats before sensitive data gets out of your organization. Data loss prevention, advanced threat protection or compliance, we’ve got you covered.

SaaS
The Digital Guardian infrastructure is available as a software service hosted and managed by Digital Guardian, enabling you to focus more resources on identifying and mitigating risks in your enterprise. This cloud-delivered platform was built using the latest web technologies to provide the scalability and ease of use security analysts have come to expect from SaaS tools.

On Premise
For customers desiring to host their management console on premise, Digital Guardian provides a simple direct integration with our cloud platform.
Digital Guardian provides the industry’s only security platform that is purpose built to stop data theft. Our platform performs across the corporate network, traditional endpoints, and cloud applications, buttressed by a big data cloud service, to make it easier to see and block all threats to sensitive information. For almost 15 years it has enabled data-rich organizations to protect their most valuable assets with a choice of on premise, SaaS or managed service deployment. Digital Guardian’s unique data awareness combined with behavioral threat detection and response, enables you to protect data without slowing the pace of your business.

A Recognized Leader. Just ask Gartner.

Digital Guardian is the only Enterprise Data Loss Prevention Gartner MQ Leader exclusively focused on data protection.

Gartner
Magic Quadrant Leader

OFFICE LOCATIONS

Corporate HQ
860 Winter St., Suite 3, Waltham, MA, 02451 USA
Phone 781-788-8180
Fax 781-788-8188

Washington DC Area
12030 Sunrise Valley Dr., Suite 110, Reston, VA 20191
Phone 703-956-2358

California
2101 Tasman Dr., #210
Santa Clara, CA 95054
Phone 408-716-4200
Fax 408-716-4201

United Kingdom
11 Leadenhall Street EC3V 1LP London
United Kingdom
Phone +44(0)207-469-0940

Japan
Mayapada Shiodome Plaza
8F, 2-11-4 Higashi-Shimbashi, Minato-ku, Tokyo, 105-0021, Japan
Phone +81-3-6435-6207
Fax +81-6435-6204

India
Stone Ridge Centre 4th Floor, Survey No: 12 & 13
Opp. Google, Kondapur Main Road, Hyderabad - 500084
Phone +91-40-4868-7872
Fax 781-788-8188