

# FORTRA



WHITE PAPER *(Digital Guardian)*

## Digital Guardian Technical Overview



## Table of Contents

1. Introduction	3
2. How We're Different	3
3. The Four Requirements for Successful Data Protection	4
4. Digital Guardian Cloud-Delivered Security Architecture	7
5. Digital Guardian Modules	11
6. Data Protection Controls	15
7. Technology Integrations	18
8. Deployment Models	19

## Introduction

Today's most successful enterprises are instrumenting and digitizing virtually every aspect of their business. This change is dramatically increasing the value and volume of sensitive data that must be protected.

Enterprise data loss prevention (DLP) is a time-tested solution that ensures your organization's most sensitive data is properly protected. However, the rapid release schedules and accelerating changes in operating systems, applications, and browsers can cause many traditional enterprise DLP solutions to be woefully inefficient. Organizations using software from DLP providers who aren't keeping up are spending too much time, effort and budget troubleshooting, and not enough time delivering meaningful data protection. New entrants are touting "DLP-lite" as a solution to the inefficiencies of traditional enterprise DLP, though they often gloss over the big compromises inherent in "DLP-lite". With lite- or no-agent architectures and no endpoint controls, what you gain from an "easy install" and lite-agent, you lose in increased risk of data leakage and loss.

You need a better way to protect the data that matters most to your organization without the inefficiencies of traditional enterprise DLP or the data protection compromises of "DLP-lite."

## How We're Different

Three pillars form the foundation of our more efficient, no-compromise data protection architecture.



### Cloud-Delivered Data Protection

Traditional enterprise DLP's inefficiencies start with the requirement to throw loads of datacenter servers and people at the DLP problem. No-compromise data protection delivers greater effectiveness and higher performance through a more efficient cloud-native, multi-tenant architecture. Powered by AWS, Digital Guardian's data protection has been cloud-delivered since 2017, enabling you to cut data center costs, and allocate more people to insights instead of infrastructure.



### Cross Platform Coverage

Windows, macOS, and Linux are the three most common operating systems in the global enterprise. Employing an enterprise DLP solution that supports less than all three platforms leaves big gaps in your data protection program. Using "DLP-lite" that disregards the nuances of how data can be manipulated across operating systems (copy/paste, save-as, print screen, etc.) results in large blind spots. Digital Guardian is alone in investing in feature-rich enterprise visibility and controls across the leading operating systems, browsers, and applications.



### Flexible Controls

No-compromise data protection allows organizations to choose from a wide variety of controls based on the sensitivity level of a file ranging from monitor and report, to user justification, to outright blocking an action. "DLP-lite" is absent the concept of control. "DLP-lite" software will tell you sensitive data has been compromised, but only after the data has been exfiltrated. Our no-compromise protection provides you with the controls to make sure that sensitive data never gets out in the first place - no matter how the data is modified or where it goes.

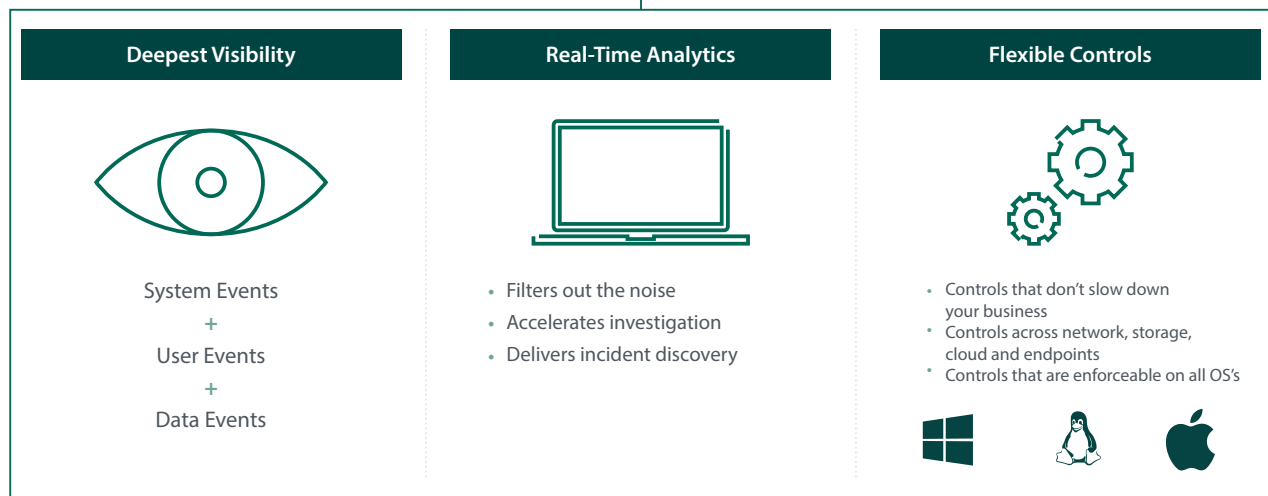
## The Four Requirements for Successful Data Protection

Regardless of the type of attack and the type of data, effective data protection relies on four capabilities:

- Visibility to all data, all the time
- Analytics to understand and manage risk
- Controls to enforce data protection policies
- Consolidated view into all threats to sensitive data

Only Digital Guardian provides all four of these capabilities to find, understand, and secure sensitive data assets and stop data theft or abuse from both insiders and outsiders and better manage risk from a consolidated platform.

### Consolidated view into all threats to sensitive data



### Deepest Visibility

Visibility to all your data, and an understanding of what it represents, is the most critical aspect of protecting your data. This is the foundation for successful data protection programs. Visibility must include data events, user events, and system events, across endpoints, databases or shares, network traffic, and cloud storage. Without this comprehensive view intelligent decisions around data protection cannot be made.

- **Data Events** focus on the file or document level, with awareness of both content and context of the data. These include moving files from one location to another via email, uploading or downloading files over the network, or local USB usage.

***Each of these three areas can deliver insights, but the combination of data, user and system event visibility provides context into data movements, the context you need to protect sensitive data from all threats, internal or external.***

- **User Events** focus on what each individual or process is actively doing with sensitive data. Digital Guardian understands who users are, their role in the organization, the tasks applications or processes can perform, and which policies apply to each. This includes keyboard or terminal commands such as cut/copy/paste, as well as the use of applications like file transfer tools, or uploading documents via the network.
- **System Events** are what happens outside of direct user intervention and are initiated at the operating system level. System events can be expected and trusted, such as the process of Adobe launching a .PDF file. They can also be unexpected and potentially malicious, like an Adobe launch prompting rogue processes to modify registry settings, or a PowerShell launch.

Each of these three areas can deliver insights, but the combination of data, user and system event visibility provides the full context needed to protect sensitive data from all threats, internal or external.

## Real-Time Analytics

System, user, and data events each mean something. By combining them, Digital Guardian sees the risky activity targeting sensitive data, within the noise of normal activities, and can stop it at the time of use, or abuse. This intelligence speeds the discovery of incidents while accelerating the investigation process and simplifying compliance. The enterprise wide view provides the full timeline of events and a defensible chain of custody in the logs to show document movement.

Digital Guardian provides real-time detection of advanced threats, forensics, incident management, and risk reduction to protect data from unauthorized use. Endpoint Detection and Response (EDR) solutions identify, in near real-time, patterns that indicate the presence of malicious software, system compromise or malware that mimics user behavior in attempting to exfiltrate sensitive data. Digital Guardian utilizes predefined rules developed by our security experts to prevent attackers from gaining access to enterprise computers, custom rules are easily created.

Digital Guardian's breadth and depth of monitoring and control capabilities make it an ideal platform to drive incident response and investigations. Digital Guardian records event forensics by time, user, system, application, file type, file classification, and network operation. These correlated events are bundled, hashed, time-stamped, and cryptographically signed at the point of use for investigative analysis. Further, for compliance driven requirements, the deep visibility supports the full picture of all sensitive data movement and demonstrates the compliance posture of the organization.

## Flexible Controls

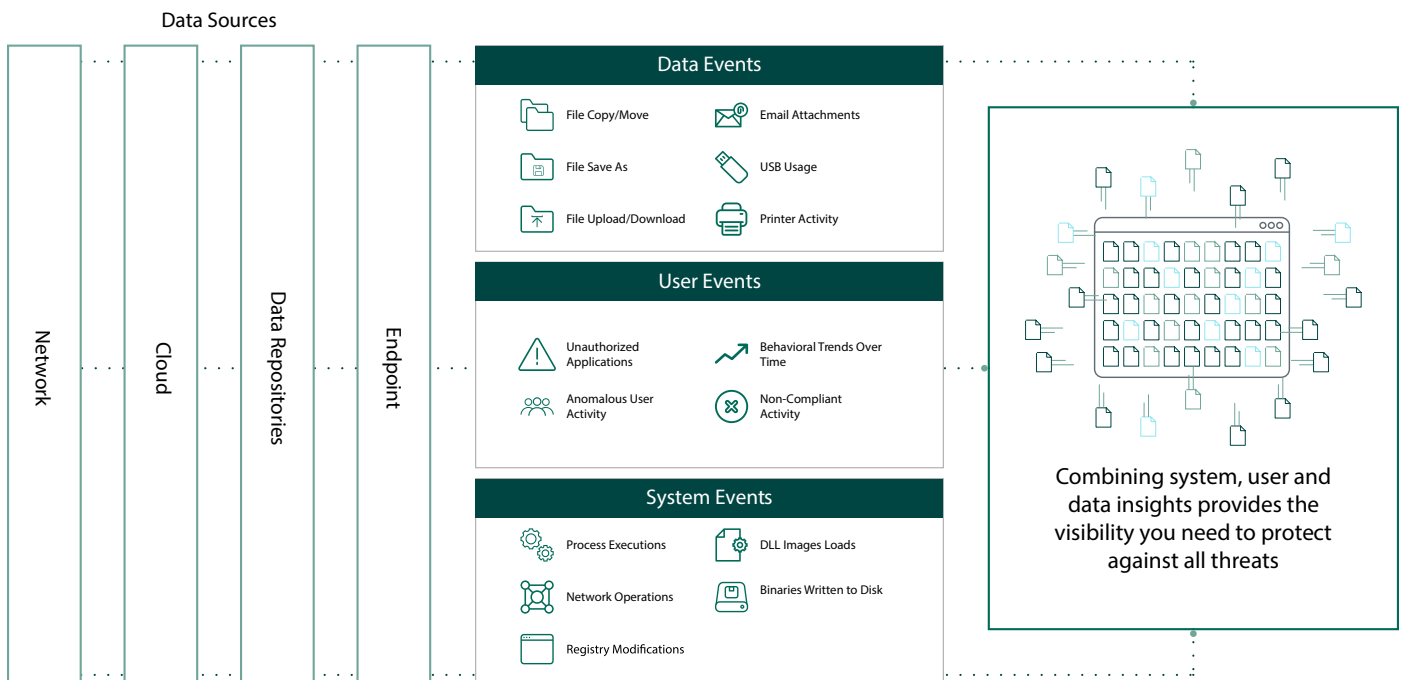
Policies are a way of translating data protection goals into consistent and actionable rules applied throughout the business. Digital Guardian's flexible controls enforce policies on and off your corporate network for the data protection you need without impacting workflows.

Controls include the ability to alert both information security teams and users to potentially risky data usage in real time. Prompts allow users to justify their actions, and are recorded for auditing purposes; information security teams immediately see data movements and can track when data is at risk or automatically block these actions. Additionally, data can be automatically encrypted or quarantined as needed to maintain data security and support compliance efforts. All activity is tracked and maintained in evidentiary-quality logs. These controls work across the following egress channels:

- Network
- Web
- Data Repository
- Cloud
- Endpoint

When a user accesses data, Digital Guardian acts based on classification of the data, the context of the action, and the applicable policy(s). If the action is allowed by policy, Digital Guardian is silent. If the action violates an organizational policy, Digital Guardian can apply a wide range of controls to data usage based on data content, context, user, application or system process, and risk type. The controls range from logging silently to actively blocking activity. DG can monitor and log without blocking when a patient’s data is sent to the insurance company, but block when that same data is sent to a personal Gmail address.

Data control policies are built in the Digital Guardian Management Console then deployed to sensors for enforcement. Digital Guardian monitors all actions on endpoints, traffic on the network, and data in cloud storage for coverage throughout the extended enterprise. Policy control options can be applied automatically based on user, risk condition, and other operating variables. The resulting matrix delivers comprehensive coverage for all data use and data egress to prevent data loss.

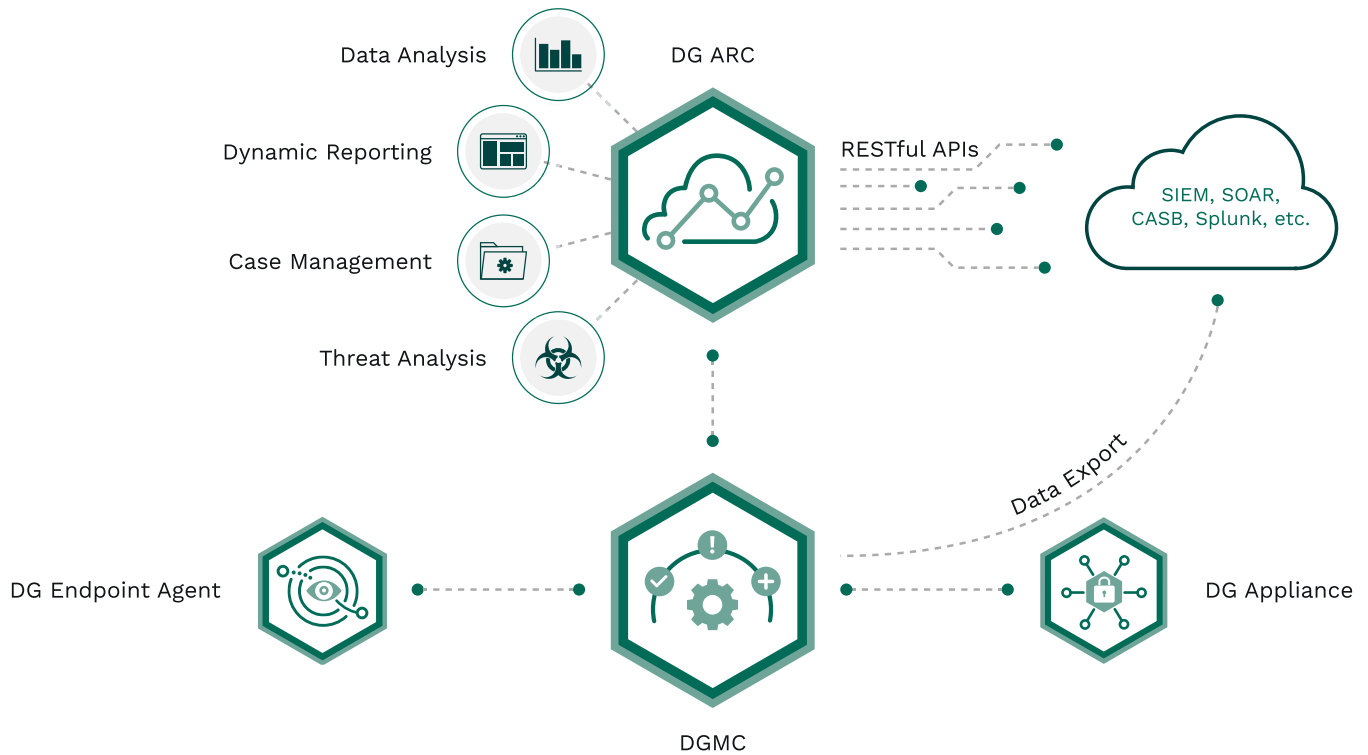


### Consolidated View into all Threats to Sensitive Data

Digital Guardian is responding to the need to do more without adding complexity by consolidating data protection solutions. By converging DLP and EDR, you can consolidate and simplify your security program, going from multiple tools to one agent managed with one console. In addition to traditional insider focused DLP, Digital Guardian extends into a broader awareness of threats, combined with the forensic artifact collection and behavior analytics required to fully assess the risks to your data. Our cloud-delivered Data Protection Platform detects threats and stops data exfiltration from both well-meaning and malicious insiders as well as external adversaries

## Digital Guardian Cloud-Delivered Security Architecture

Digital Guardian delivers granular visibility, real-time analytics, and flexible controls through a consolidated, cloud-native platform for data protection. It is comprised of three primary components: event collection sensors, functional modules, and the cloud infrastructure.



### Event Collection Sensors

Digital Guardian's data collection sensors provide full visibility into endpoint actions, network traffic, and cloud apps. The Digital Guardian Agent and Digital Guardian Appliance see sensitive data as it is created, used, or moved and complement each other to deliver the most complete visibility, analytics, and controls for data protection from inside and outside threats.

### Digital Guardian Agent

The key to Digital Guardian's endpoint visibility and control is its kernel-level agent. The agent provides oversight of system, user, and data event activity to protect sensitive data. By integrating at the kernel, the agent can monitor and control events, processes, and data from within the operating system. The agents maintain awareness of all operations and data, and can apply appropriate controls to each data item prior to allowing execution of an operation. When a user accesses data, agents act based on classification criteria of the data in question, evaluate appropriate usage, and then apply protection policies or prompt the user to modify or justify actions. Agents operate autonomously, with full knowledge of all systems, services, and executables, without relying on a connection to the management cloud.

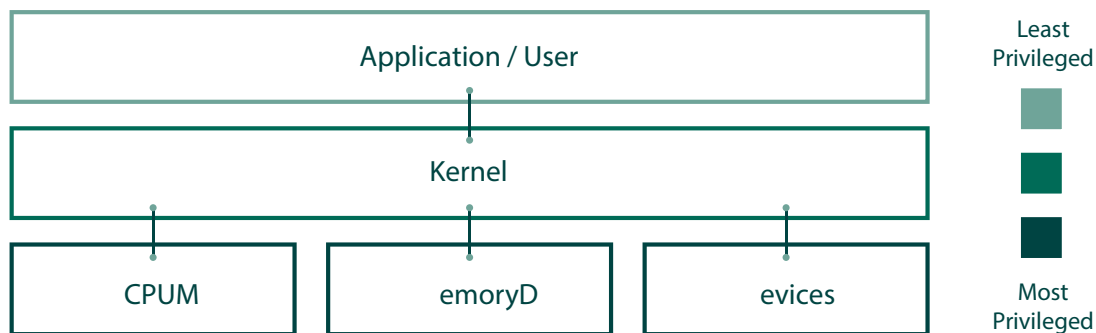
Digital Guardian data protection endpoint agents are available for laptops, desktops, servers, and virtual environments. The agent provides full visibility, controls, and analytics for the following operating systems:



## Digital Guardian Kernel Level Agent for The Deepest View Into your Data

Digital Guardian integrates directly into the kernel for a simple reason; it is the only way to have full visibility to all events on a device. Preventing data loss at the endpoint requires visibility to all the protected data, at all times, on and off your network, and visibility to all of the different ways one could attempt to steal or leak sensitive information.

To better protect sensitive information wherever it resides requires an understanding of the content of the data (e.g., data considered sensitive or subject to regulatory standards such as PCI-DSS or HIPAA), the role and privileges of a user, system, or process accessing the data (what actions are allowed and by which users), and the context of how the data is being used. In other words, an understanding of every action on every piece of data by every user, application, or process. This can only be achieved by leveraging the power of the kernel. On a computer, the kernel manages all requests and system calls to the CPU, memory, and input/output devices (e.g., mouse, keyboard, disk, and USB drives). By integrating in the kernel, Digital Guardian's agent provides the deepest visibility possible, and enforces policies by leveraging the kernel to control access to input and output devices, or applications such as email, peer-to-peer networks, and external storage/sharing.



## Protecting the Agent

A knowledgeable attacker will attempt to defeat controls by compromising the defensive application. To defend against all adversaries, one must protect the agent itself. Digital Guardian addresses this two ways.

### Tamper Resistance

Digital Guardian executables are protected from termination and are self-monitoring; an attacker cannot kill, debug, or inject code into our processes. All components are signed, signatures are verified on start-up and update.

Self-monitoring ensures that DG is running and that rules are active. When started, the DG Service initializes an Agent on the device (this executable is hidden from view). Periodically, the Agent checks the Service to ensure the Service is running, communicating with the Service Control Manager, and set to automatic restart. If any of those conditions are not met, the Agent will restart the Service, and a new Agent will be initialized.

The Digital Guardian platform also knows when an agent it expects to see is no longer reporting to the management console and logs this condition.



## Stealth Mode

When the Stealth configuration option is enabled, Digital Guardian hides all related processes and files to thwart attempts to find and bypass the agent. Agent processes are never visible in the Task Manager, Activity Monitor, or other applications that enumerate running processes. In addition, all Digital Guardian files and folders are hidden on the file system. Registry entries are also protected to prevent viewing or modifying entries, or changing an entry's security attributes.

## Ensuring Compatibility

Digital Guardian has partnered with Microsoft to ensure that, upon release of new versions of Windows, Digital Guardian will deliver compatibility and interoperability. Digital Guardian receives pre-release, development builds of Windows for testing and Microsoft provides Azure-hosted VM's and dedicated engineering staff to support the development process.

## Digital Guardian Appliance for the Most Accurate Data Protection

Digital Guardian appliances monitor and control network communications to prevent sensitive data from leaving the organization's control. Network appliances are designed to protect data at rest and in motion with minimal overhead. Utilizing a network Switch Port Analyzer (SPAN) or intelligent traffic aggregator, appliances monitor all network traffic and enforce policies. Digital Guardian appliances monitor and control all communications channels — including email (SMTP), web (HTTP/HTTPS), File Transfer Protocol (FTP), Secure Sockets Layer (SSL), and applications such as webmail. Appliances can be deployed as either physical or virtual machines.

The appliance architecture consists of specialized sensors that monitor the full TCP stack and can provide policy protection enforcement for both inbound and outbound connections. The appliance's scalable architecture provides flexible deployment options; single network appliances can perform multiple functions from network monitoring and enforcement to discovery of data stored in various repositories. Appliance capabilities may be decoupled and deployed across multiple locations reporting into a single DGMC management platform. The Digital Guardian appliance works across:

- **Network** - Supported Protocols: all TCP/IP communications
- **Storage Repositories** - Discovery and Fingerprinting: Windows CIFS & SMB, NFS
- **Databases** - Discovery and Fingerprinting: MS SQL, Oracle, MySQL, DB2, Sybase, Informix, PostgreSQL
- **Cloud** - Discovery and Fingerprinting: Box, O365 (OneDrive), Egnyte, Citrix Fileshare, Accellion

## Accurate Data Classification and Protection with the Digital Guardian Appliance

The goal in identifying sensitive information is often to prevent the inadvertent release of "known information" such as employee social security numbers, patient identifiers, or customer credit card numbers. A 10-character string may represent a patient record, but it may also be a phone number or just a random string. To minimize false positives and false negatives in common formats, DG's Database Record Matching (DBRM) provides a fast, reliable, and accurate method to identify matches to the actual data in question.

***In a side by side comparison with a competing solution, the traditional methods without DBRM missed at least 87% (650/750) of real PHI, while still producing 94% (1700/1800) false positives.***

DBRM uses mathematical hashes to find, categorize, and tag sensitive data. Starting with a training set, DBRM generates a unique, one-way hash for each record; a digital “fingerprint” for each specific data element (e.g., patient record number, social security number, account ID). It then inspects target data such as emails, web postings, uploads to cloud storage, or removable media, generates hashes to identify exact matches of the fingerprints of known sensitive data. Adding a 2nd hashed database element (e.g., a patient’s name) and requiring the 2 hashed elements to exist near to each other reduces false alarms to negligible rates.

## Digital Guardian Modules

The event collection sensors communicate bi-directionally to the next layer in the architecture, the modules, to deliver superior data protection. The modules include, Analytics, Workspaces, Management Console, and Applications.

### DG Analytics

Digital Guardian Analytics is an advanced analytics, workflow and reporting cloud service. DG analyzes events in context, leveraging streaming data from Digital Guardian endpoint agents and network sensors, providing the deepest visibility into system, user, and data events. That visibility powers security analyst-approved dashboards and workspaces to enable data loss prevention, managed detection & response and user entity & behavior analytics from a single console.

DG Analytics packages over 150 man-years of data defense techniques into over 100 behavior-based rules. Anomaly detection with advanced statistical models and machine learning filter the noise and identify events that warrant additional investigation by your IR and security teams.

### DG Workspaces

Information needs vary with roles. DG’s SaaS solution has workspaces and workflows preconfigured based on our experience protecting organizations against data loss. Our information security experts, threat hunters, incident responders, and security leaders developed workspaces to guide security professionals to the events that matter when identifying anomalous and suspicious insider and outsider activity. Analysts can easily drill down to follow an event and determine next steps or create custom dashboards, reports and workspaces. Real-time reports provide the information your team needs to make better decisions. Regardless of your role, the tools and information you need are ready and customizable as your needs evolve.

### DG Management Console

The Digital Guardian Management Console (DGMC) is your web-based configuration and management hub within our platform. It enables you to set up and deploy agents and policies across your global deployment. Policies configured in the DGMC are distributed to and enforced by the agents and appliances.

### DG Applications

Digital Guardian delivers protection from internal and external threats on the endpoint, over the network, and into the cloud. Our comprehensive suite of data protection applications lets you find, understand, and protect your organization while supporting regulatory compliance.



## Applications

- **Data Discovery** – Find the sensitive data in your organization and view how it is used.
- **Data Classification** – Classify structured and unstructured data based on content, context, and user input.
- **Data Loss Prevention** – Monitor and control data usage to stop sensitive data from leaving your network and support compliance.
- **Endpoint Detection and Response** – Detect, investigate, and mitigate suspicious activities and behaviors at the endpoint.  
Powered by Digital Guardian Managed Security Program.
- **Cloud Data Protection** – Stops the loss of data in cloud applications such as Office 365.

## Data Discovery

Data visibility is the foundation to data protection. Digital Guardian Data Discovery uses automatic, configurable scanning of local and network shares using specific inspection policies to ensure all data at rest is discovered, wherever it is located. Pre-configured templates speed discovery of PHI, PCI, and PII data while customized templates deliver flexibility for other data types and emerging regulations. DG's DBRM "fingerprinting" can be used to minimize false positives and false negatives, adding efficiency to data discovery.

DG Data Discovery brings immediate value to organizations. When an initial scan completes, managers receive alerts for any data identified in a location that violates policy, including a detailed list of the files, their location(s) and the specific policy violated. These documents can also be automatically quarantined to address compliance or security policies. Data discovery is extended to the cloud through integrations with leading cloud storage providers to scan repositories, enabling encryption, removal, or other automated remediation of sensitive data before the file is shared in the cloud - data that is already stored in the cloud can be scanned and audited at any time.

## Classification

Many organizations find the task of understanding what constitutes critical data, where it resides, and how it is used overwhelming without the use of intelligent automation. Digital Guardian addresses this by providing automated classification of data, and then applying classification tags to the data, tracking its use, and preventing its misuse.

By understanding the sensitivity of each piece of data, organizations achieve greater control without affecting business processes. Digital Guardian supports automated content classification for over 300 file types and 90 languages, including structured and unstructured data types.

Digital Guardian's integrated classification engine can simultaneously identify, tag, and manage sensitive data in real time according to policy. Digital Guardian manages and enforces data policies from discovery forward, without needing to connect to a centralized clearinghouse to confirm a file or email's sensitivity.

Digital Guardian classifies data upon its discovery, access, creation, movement, or revision, and a classification tag is appended securely to its host file or email. Classifications can be permanent or updated with changes to content. Three methods are available for classifying data: Context-based, Content-based, and User-based. Digital Guardian’s ability to combine automated and manual methods when classifying data enables an auditing process that minimizes inaccurate policy enforcement.

Classification Method	Description
Context-Based Classification	Automatically classify data based on attributes such as application, user, or location stored.
Content-Based Classification	Automatically classify data based on specified keywords, patterns, dictionaries, or digital fingerprint.
User-Based Classification	End users manually classify based on their knowledge about the data.

This combination of technology-based and user-driven decisions provides balance and ensures the right policies are enforced on the right data. Digital Guardian incorporates the classification into alerts, elevating events targeting high value data to drive immediate action. By providing this multi-faceted approach, organizations can classify their data with the highest accuracy while providing automation and controls to stop data theft.

## Data Loss Prevention

- **Endpoint DLP**

Digital Guardian’s data-centric approach combines complete visibility to all sensitive data, with automatic classification tagging that travels with the data and granular control of all data movement enforced by kernel-level agents on endpoints. This allows DG to control the use of data even if it has been copied to another file format through manipulation or screenshots.

Whether the data is structured or unstructured, Digital Guardian knows where it is and how it is being used. DG understands the context of how sensitive data is used, seeing at the system, user, and data level. When data is used according to policy, Digital Guardian is invisible to end users, allowing access and use of data. When policies are violated, or actions are attempted that could put sensitive data at risk, DG can apply a wide range of controls, from warnings to hard blocks.

- **Network DLP**

Digital Guardian Network DLP can be configured and deployed to monitor and control movement of sensitive information via the network, email, or web. It works by inspecting all network traffic for sensitive information, then enforcing company policies to protect that information from misuse. Pre-configured policies for data covered by regulatory standards are bundled with Network DLP, including PII, PHI, and PCI. A policy wizard provides the flexibility to create customized policies, ensuring you protect what matters most to your organization and supporting compliance needs. Reports provide a detailed picture of sensitive and regulated data for audits.

The Network DLP appliance can be deployed as a physical machine, a virtual machine, or as an image in cloud services like Microsoft Azure to monitor and protect all communication channels, including email, Web, File Transfer Protocol, Secure Sockets Layer, and applications such as webmail, blogs, and social media.

## Endpoint Detection and Response

Digital Guardian Endpoint Detection and Response (EDR) provides protection from multiple attack sources using the same agent as DG DLP. Digital Guardian’s behavior-based rules automatically detect and block attacks - ransomware, malware, malware-free attacks and other suspicious data movements. It stops threats even if there are no IOC signatures. Wherever in the kill chain – entrance, lateral movement, installation, command and control, or exfiltrate – DG EDR provides the needed context of data movements to enable faster and more accurate determination of the attack, its motivation and impact. DG EDR is delivered as a managed service as part of our Managed Security Program.

## Cloud Data Protection

DG Cloud Data Protection extends your enterprise data protection visibility and policies to sensitive data in the Office 365 ecosystem and other leading cloud storage platforms such as Box. Digital Guardian Cloud Data Protection integrates with cloud storage providers to protect sensitive information before it moves to the cloud. DG Cloud can scan repositories for sensitive data, then apply controls before the file is shared in the cloud. Data that is already stored in the cloud can be scanned and audited at any time. Automated encryption or file quarantine can address compliance violations immediately.

## Cloud Infrastructure


Our purpose-built SaaS infrastructure enables you and your team to focus more time, energy, and resources on identifying and mitigating risks to your sensitive data and less time on acquiring, building and maintaining the infrastructure.

This service leverages the scalability, data visualization and ease-of-use security analysts need. Centralized reporting in the cloud removes storage limitations and gives you the ability to aggregate, analyze and query system, user and data related events across the network and endpoints over longer periods of time.

## Data Protection Controls

Digital Guardian policies travel with the data and enforce company policies on and off the network. Controls can be enforced on endpoints, applications, email, the web, and data repositories. Administrators can set up incident management workflows to automate any response actions when policy violations occur.

Policy actions for both Endpoint Agents and Network Appliances range from logging to hard blocking of actions, in every case Digital Guardian creates a detailed log of the event. The range of options includes the following:

- 
- **Log** – User is unaware of any action; Digital Guardian creates a detailed log of the action, but allows user to proceed.
  - **Alert** – User is unaware of any action; Digital Guardian generates an alert that this may be a high priority event but allows action
  - **Prompt** – User is aware of action; on-screen prompt alerts user to potential risky behavior, but allows user to proceed
  - **Justify** – User is aware of action; on-screen prompt alerts user to potential risky behavior, but allows user to proceed if they provide a justification
  - **Block** – User is aware of action; on-screen prompt alerts user to potential risky behavior, but does not allow user to proceed
  - **Encrypt** – User can either be aware or unaware based on preferences; documents are automatically encrypted prior to completing action, typically email or transfer to storage repository
  - **Quarantine** – User can either be aware or unaware based on preferences; documents are automatically removed to a secure quarantine and a place holder is left in its place.

Agent based inspection understands the content and context of the data and occurs on the Windows, Mac, or Linux endpoint, as well as Citrix VDI.

Digital Guardian appliances monitor network and web traffic via either a Switch Port Analyzer (SPAN) or Test Access Point (TAP) to provide instant visibility into policy violations and report incidents involving sensitive information. The appliance includes an inline Mail Transfer Agent (MTA) to integrate with local mail server for email inspection and control. Digital Guardian leverages the APIs of cloud storage providers to inspect cloud content. This allows Digital Guardian to analyze traffic before files are shared in the cloud. Information that is already stored in the cloud can be audited at any time with the same remediation action.

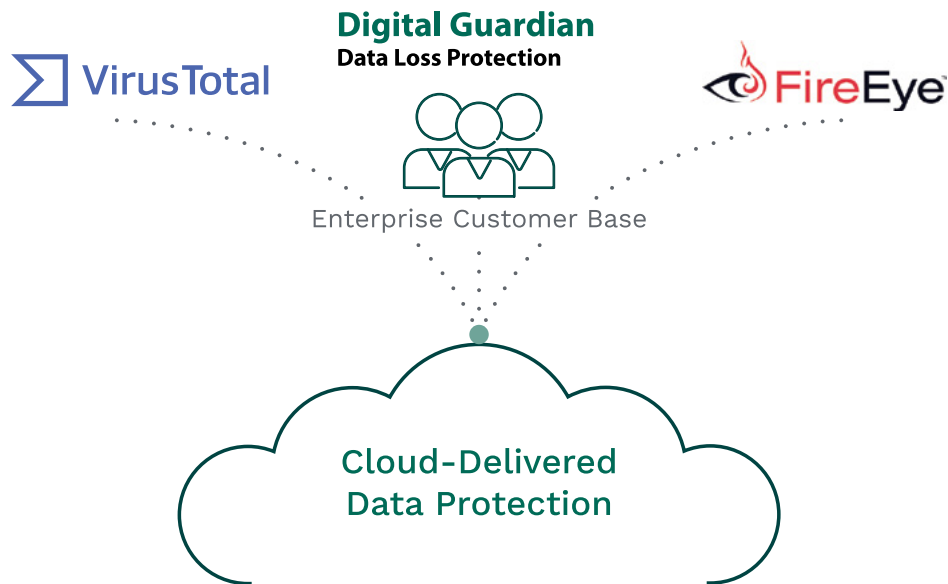
## Application Control

Advanced threats often introduce and spawn new processes to affected devices. Digital Guardian can detect these malicious applications, block execution or access to protected data, and alert Incident Response in near real time. Digital Guardian provides organizations with the ability to control which applications run in their environments, and what actions those executables and processes can take with data. Digital Guardian understands the function of each application, and prevents applications from being coopted to perform data movements that would compromise security.

With Digital Guardian, organizations can block unknown executables and ensure that only approved applications are used. This includes legitimate, but undesirable applications such as peer-to-peer networking or chat applications, as well as unknown software that may be malicious. Administrators can enforce the use of specific browsers with controlled settings, including limiting internet access to the company's network proxy or VPN.

## Threat Intelligence Feeds

Threats to sensitive data can come from both well-funded state sponsored actors as well as individuals, each group researches tactics, techniques, and procedures to increase their chances of success. This evolution of the threat landscape requires organizations use all available resources to keep their information security programs relevant. For customers subscribing to Digital Guardian's Managed Detection and Response, three separate sources of threat information are available.



## Digital Guardian Customer Intelligence

The DG Advanced Threat team is continuously diverse, global researching and analyzing malware campaigns along with targeted attacks to our customer's environments. In the event new, unique, or otherwise novel threats are identified, those risks are mitigated via indicator blacklist feeds or with new rules written by our team of cybersecurity experts. All DG MSP customers gain immediate access to these new rules to help protect their sensitive data from the evolving threat landscape.

## Virus Total

Digital Guardian can send process data in the form of MD5, SHA1, or SHA256 hashes to VirusTotal to identify viruses, worms, trojans, and other kinds of malicious executables and content. VirusTotal scans the hashes to identify suspicious content and provide information back to DG. Security teams can analyze the scan data to determine whether it poses a threat to the enterprise and take appropriate action.

DG makes VirusTotal data available for reports on:

- The total number of scans performed on a given application
- The number of positive matches returned for a given application
- The percentage of positive results returned for a given application

## FireEye

The FireEye platform is a virtual execution engine used to identify and block cyber-attacks in real time. FireEye-generated Indicators of Compromise (IOC) describe malware and attack methodologies. Digital Guardian receives FireEye Indicators of Attack describing attack methodologies, and converts the (IoC) into rules for endpoint agents to confirm the extent of an infection, quickly contain that infection, and block new infections.

## Technology Integrations

Digital Guardian complements an organization's security programs, and integrates with other solutions for enhanced alerting, security and forensics.

## Security Information and Event Management (SIEM)

SIEMs allow organizations to aggregate data related to events on endpoint systems and servers, and to correlate those with network and other log source data such as file integrity monitoring, audit and vulnerability information. Digital Guardian provides visibility across data in motion, at rest, and in use adding value to SIEM implementations by enabling new use cases in the areas of insider threats and external attackers. Digital Guardian SIEM partners are Micro Focus ArcSight®, IBM QRadar®, McAfee, and Splunk.

## Network Security

Network security solutions detect external threats and network attacks by working in conjunction with Digital Guardian. Digital Guardian partners with Palo Alto Networks and FireEye to provide a comprehensive security solution on both the network and endpoint. Suspicious files on endpoints can be delivered to the network systems for detonation and analysis before they execute, or to VirusTotal for examination.

## Email Security Encryption

Digital Guardian delivers an integrated and automated way to detect sensitive information and automatically apply encryption to outbound messages to simplify secure communications. Digital Guardian partners with Cisco and Micro Focus.

## Cloud Access Security Broker (CASB)

Netskope, Bitglass and Digital Guardian are proven industry leaders committed to ensuring that enterprise customers get best-of-breed sensitive data protection. Together, they address complex compliance requirements originating from privacy laws such as GDPR, HIPAA, and other regulations and work on premises, in the cloud, and across endpoints, whether users are remote or working from mobile devices. Enterprises can safely enable the cloud for their workforce and provide the industry's broadest data loss prevention coverage with the deepest contextual visibility and adaptive access control. A consistent data protection policy from the endpoint to the cloud is the result.

**Boldon James**  
Data Classification

 CISCO

 FireEye

 IBM

 McAfee

 MICRO FOCUS

 Microsoft

 palo alto NETWORKS

 splunk >

 bitglass

 zscaler

 netskope

## Deployment Models

Organization experience challenges either deploying security solutions or successfully running the solutions over the long term. They are generally related to:

- Security team resource limitations
- Maturity of IT and security organization
- Enterprise wide buy-in
- Lack of a programmatic approach

With years of experience deploying DLP and EDR solutions across global enterprises and a proven deployment methodology, Digital Guardian can help any organization achieve its compliance and security data protection goals quickly and maintain value over time.

The priorities (compliance, security, budget) and resources of each organization are unique, and evolve over time. To support this, Digital Guardian offers flexible deployment options. Customers can deploy as a SaaS or as a Managed Security Program.

## Software as a Service (SaaS)

A successful security initiative requires a combination of the right technologies, people, and processes. While some companies can build and maintain these resources internally, for many others, leveraging external expertise and infrastructure can bring better results. DG's Software as a Service (SaaS) solution leverages the Digital Guardian Data Protection Platform to provide this in a package that results in more effective security, simpler management, and better economics.

Digital Guardian's SaaS solution provides customers with the analytics, workflow and reporting analysts require for threat aware data protection, without the need to deploy and manage the associated hardware and software. This removes storage limitations and gives you the ability to aggregate, analyze and query system, user and data related events across the network and endpoints. You get big data security without investing in a big data infrastructure.

## Digital Guardian's SaaS delivery model provides:

Better utilization of scarce security resources. Let your people focus on higher value, strategic actions while DG manages your infrastructure.

- **Simpler Audits** – DG's SOC is managed to meet SSAE 16 standards, including ongoing investments in people and processes. Defenses are monitored 24x7 by staff years of security experience.
- **Faster Time-to-Value** – No need to order hardware or set up a new SOC. DG is ready when you are and can deploy when you are.
- **Elastic Scalability** – A primary benefit of a cloud architecture is the ability to scale up (or down) on a moment's notice. Instead of ordering new hardware, testing updates in a development environment, rebalancing servers, and training new personnel, the DG cloud scales on demand. Adding endpoints anywhere in the world is simple.

## Managed Security Program

Digital Guardian's Managed Security Program (DG MSP) provides all the benefits of Digital Guardian's best-in-class solutions for regulatory compliance, data loss prevention (DLP) and managed detection and response (MDR), without the overhead and direct costs of managing data security solutions. Digital Guardian launched the industry's first Managed Security Program for DLP to address the global shortage of trained security talent.

***Digital Guardian launched the industry's first Managed Security Program for DLP to address the global shortage of trained security talent.***



Digital Guardian utilizes a SaaS model and hosts all hardware and software at a secure SSAE 16 certified data center.

DG MSP benefits include:

- **Fully managed data protection infrastructure:** Digital Guardian deploys, hosts and manages data protection infrastructure including: data classification; policy rules, alerts and controls; event forensics; risk analytics.
- **Instant access to security experts:** The Digital Guardian MSP team has deep, practical experience implementing mission-critical data security, risk, and incident response and compliance programs.
- **Immediate risk awareness and mitigation:** You receive instant alerts and escalations of insider/outsider threats and noncompliant activities. You access live and configurable dashboards to gain real-time insights into sensitive data location, usage and threats. Incident review is scheduled per your requirements.
- **Fast deployment:** Digital Guardian MSP can be deployed and operating in full production mode in 90 days or less using our proven methodologies that help you achieve actionable results fast.



#### About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at [fortra.com](https://fortra.com).