DIGITAL GUARDIAN®

DIGITAL GUARDIAN

TECHNICAL OVERVIEW

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Digital Guardian is a leader in data protection and has protected sensitive data for over a decade including protecting the intellectual property in the world's largest and most innovative companies and the personal information of health care, financial services and other regulatory driven industries. Since our founding in 2002, our heritage is solving data protection problems and our only focus is protecting your sensitive data from loss or theft.

Sensitive data fuels the growth and sustainable competitive advantage of industries, this data has value outside of the control of your business. Whether via accidental disclosure or intentional data theft, the problem costs the global economy billions of dollars. How do businesses maintain their global operations and ensure unimpeded data flow to only the right people? Digital Guardian's data protection platform solves this problem.

Digital Guardian delivers the most complete data protection platform through the deepest visibility, real-time analytics, and flexible controls. These three pillars drive our Data Loss Prevention and Advanced Threat Protection solutions. The Digital Guardian platform delivers visibility at the system, user, and data level to understand threats to the data at the point of risk and prevent data loss. Our analytics help cut through the noise and let InfoSec professionals focus in on the threats that matter most, those impacting sensitive data. Finally, the flexible controls can act automatically, as needed, to enforce data protection policies.

Digitization across nearly every industry means the challenge to protect the growing pool of data is increasing. Digital Guardian, through our flexible deployment approaches gets your organization's data protection program operational on your schedule to protect the sensitive data your business needs.

We're the only security company 100% dedicated to protecting sensitive data from inadvertent loss and malicious theft.

INTRODUCTION

Threats to sensitive data occur every day. An employee downloads design information to a USB stick, then leaves to join a competitor. Hackers break into a healthcare system's network and steal millions of patient records. An employee inadvertently attaches a file with sensitive, customer information to an email and sends it externally. Protecting an organization's data against loss, theft or external attacks is a formidable task.

Further complicating the task, data no longer resides exclusively inside an organization's walls or control. In addition to living on the corporate network, it is on laptops and tablets used in remote offices, customer sites, and coffee shops. Data resides in the cloud and is shared with global business partners in the supply chain. Structured data such as client records and other personally identifiable information proliferates throughout your organization. Sensitive content exists in unstructured forms such as images, formulas, CAD drawings, audio and video files. The data explosion and sprawl makes it clear that organizations can no longer rely on traditional approaches (firewalls, AV, IPS) to defend their information.

"DIGITAL BUSINESSES REQUIRE A DATA-CENTRIC APPROACH."

"In this new reality, traditional perimeter-based approaches to security are insufficient. S&R pros must take a data-centric approach that ensures security travels with the data regardless of user population, location, or even hosting model"

(source: The Future Of Data Security And Privacy: Growth And Competitive Differentiation, Forrester Research, Inc., July 10, 2015)

Your organization relies on information, whether it is personal information used for identity theft or corporate IP valued by competitors, your data has value to those outside the organization. Protecting the data must be the primary goal of security professionals.

DIGITAL GUARDIAN – THREAT AWARE DATA PROTECTION

Digital Guardian built a threat aware data protection platform to monitor for and prevent the misuse, accidental disclosure, or theft of sensitive data across the extended enterprise. This threat aware data protection provides comprehensive data protection solutions and controls from both insider and outsider risks. Whether data is stored and used at the endpoint, accessed remotely from a shared server, stored in a database repository, copied to removable media, or attached to an email, Digital Guardian's threat aware data protection platform provides solutions for your sensitive data challenges.

Any effective data protection program requires that data is protected throughout its life cycle, from creation and access to usage to destruction. Digital Guardian will help you translate internal business and technical requirements to a fully operational data protection program. Digital Guardian's threat aware data protection platform can manage the data cycle and can protect data regardless of how the data is used or accessed. In addition, this threat aware data protection platform can provide proof that the data hasn't left your organization. Digital Guardian protects data regardless of the source of the attack. Digital Guardian's intelligent correlation detects patterns indicative of malicious software, system compromise and unauthorized user behavior. This allows Digital Guardian to log, alert, and retain activities to develop alert sequencing where a combination and/or sequence of indicators indicates malicious behavior.

Digital Guardian can trigger immediate alerting to the presence of an attack, quarantine compromised machines from the network, initiate the collection of artifacts required to support the forensic investigation and stop attacks in progress by killing a process. Digital Guardian can stop unwanted email or web posts and protect data improperly stored in local or remote repositories by moving the documents into secure location and encrypting content.

Our unique ability to protect sensitive data in use, in motion and at rest from both insider and outsider threats is a result of three distinct capabilities:

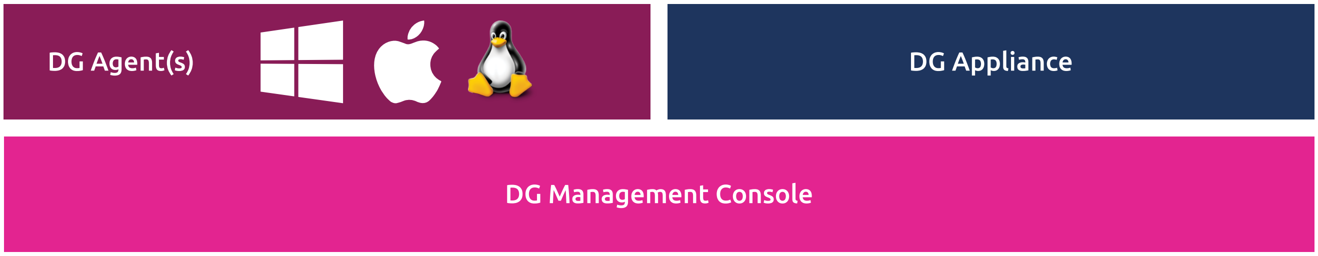
- **Deepest Visibility:** Digital Guardian sees and correlates system events, user events and data events at the endpoint, on the network, in the cloud and in databases.
- **Real-Time Analytics:** Digital Guardian filters out the noise allowing InfoSec to focus on the real threats, accelerating the investigation process and streamlining compliance.
- **Flexible Controls:** Digital Guardian acts at machine speed with controls that adapt to your business to stop data loss before it happens. These controls cover networks, endpoints and storage, on premises and in the cloud.

The platform is available from Digital Guardian through an on-premises deployment, cloud-based fully-managed solution, or a hybrid of both.

PLATFORM OVERVIEW

Digital Guardian's threat aware data protection platform uses a secure, flexible, and extensible architecture with centralized policy management to protect sensitive information. The Platform has three components: Management Console, Agent, and Appliance.

THREAT AWARE DATA PROTECTION PLATFORM



DG Agent(s)

DG Appliance

DG Management Console

DIGITAL GUARDIAN MANAGEMENT CONSOLE

The Digital Guardian Management Console (DGMC) is a web-based command center within the Digital Guardian data-centric security platform. It enables policy and report creation and management, as well as alert viewing and disposition. Policies configured in the DGMC are distributed to and enforced by the agents and appliances. The agents and appliances send event details back to the DGMC, which aggregates and analyzes the event data to provide alerts and consolidated reporting. These reports drive enterprise wide data visibility, improved data security, and simplified compliance throughout the organization.

Digital Guardian ships with predefined reports, dashboards, executive summaries, and usage trends. Reports can be modified as needed, or custom reports can be created. Predefined dashboards include:

- **Operational –** Provides summary information on the entire Digital Guardian system, including deployed agents & appliances, health status, events, report notifications, jobs scheduled & queued, and policies deployed.
- **Alerts –** Shows the total number of alerts generated by a rule or policy over a specific period.
- **Events –** Displays an overview of general data events across the enterprise, including total activity, activity by application, and activity by user.
- **Network –** Shows data-in-motion activity and policy violations for network, email and web.
- **File Inventory –** Reports on data-at-rest; a near real-time inventory of all classified files on a given computer.
- **File Discovery –** Provides information on discovery policy violations.
- **Email –** Displays an overview of all email activity across the enterprise.
- **Rule Violations by User –** Identifies trends for individual users or computers at day-level granularity.

DIGITAL GUARDIAN AGENT

The Digital Guardian kernel-level endpoint agent provides effective oversight of system, user, and data event activity to protect sensitive data. By integrating at the kernel, application and user level of the operating system, the Digital Guardian agent can monitor and control events, processes, and data from within the operating system. Digital Guardian agents maintain awareness of all operations and data, and can apply appropriate policies 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 their behavior. Agents operate autonomously, with full knowledge of all systems, services, and executables, without relying on a connection to the DGMC. Digital Guardian agents can be configured to mandate the use of private networks for data security.

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: Microsoft Windows, Mac OS, Linux and Citrix.

The agent provides full visibility, controls and analytics for the following operating systems:

- Microsoft Windows®
- Mac® OS
- Linux
- Citrix®

DIGITAL GUARDIAN APPLIANCE

Digital Guardian appliances monitor and control network communications to prevent sensitive data from leaving the organization's control. Utilizing a network SPAN or intelligent traffic aggregator, Digital Guardian appliances monitor all network traffic and enforce policies to ensure protection. Policy-based actions include: allow, log, prompt, move, block, encrypt, reroute, and quarantine. 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. Digital Guardian 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 for 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 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

DATA PROTECTION PILLARS

To provide the data protection needed in the digitizing enterprise Digital Guardian relies on three pillars:

- Visibility
- Analytics
- Controls

With these three capabilities, we deliver threat aware data protection to see, understand, and secure sensitive data assets to stop data theft or abuse from both insiders and outsiders.

DEEPEST VISIBILITY

You can't protect what you can't see, that just seems logical. Digital Guardian delivers the deepest visibility at the system level, user level, and data level. This visibility encompasses endpoints, databases or shares, network traffic, and cloud storage.

Digital Guardian sees data level events, those that focus on the file or document level. These include moving files from one location to another via email, uploading or downloading files over the network, or local USB usage. User level events focus on what the person at keyboard is actively doing to a document. This includes the use of applications like file transfer tools, or uploading documents via the network. System level events are what happens after the user performs an action and are initiated at the operating system level. These system events can be expected and trusted, such as the process of Adobe launching after the user clicks a .PDF file, but can also be unexpected, and potentially malicious, like that Adobe launch prompting rogue processes to modify registry settings, or a PowerShell launch. Digital Guardian sees these events as they happen and can intervene in real time, if needed, to prompt, encrypt, or block the action to protect your sensitive data at the endpoint, on the network, in databases, or in the cloud. Each of these three areas can deliver insights, but the combination of data, user and system event visibility provides context into data movement, the context you need to protect sensitive data from all threats, internal or external.

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

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 then delivered to the Digital Guardian Management Console for investigative analysis, and can be archived. 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.

REAL-TIME ANALYTICS

System, user, and data events all mean something; by combining them Digital Guardian can see the risky or malicious activity targeting sensitive data, within the noise of normal activities, and can see 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 search and reporting provides the full picture of events and a defensible chain of custody in the logs to show document movement. The detailed sequence of events including data, user, and system at the endpoint, on the network, in databases or in the cloud streamlines the investigative process allowing InfoSec to address gaps quicker and reduce the attack surface.

Digital Guardian provides real-time detection of advanced threats, forensics incident management and risk reduction to protect data from unauthorized use. Advanced Threat Protection (ATP) 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. Security administrators can also create custom rules to detect malicious attacks.

ATP module provides the following additional functionality within DGMC:

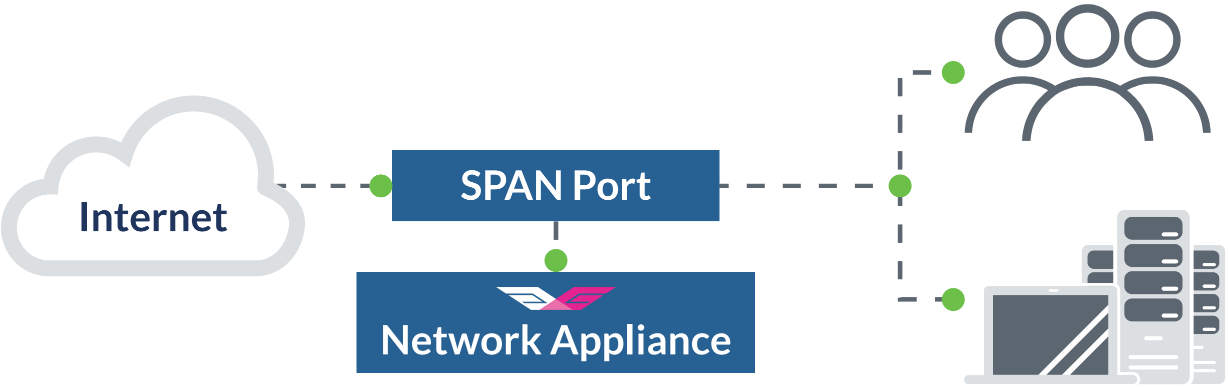
- File capture capability
- Threat protection report
- System and application process details
- Internal system scan report
- Third-party integration such as SIEM and NGFW
- Threat feeds

FLEXIBLE CONTROLS

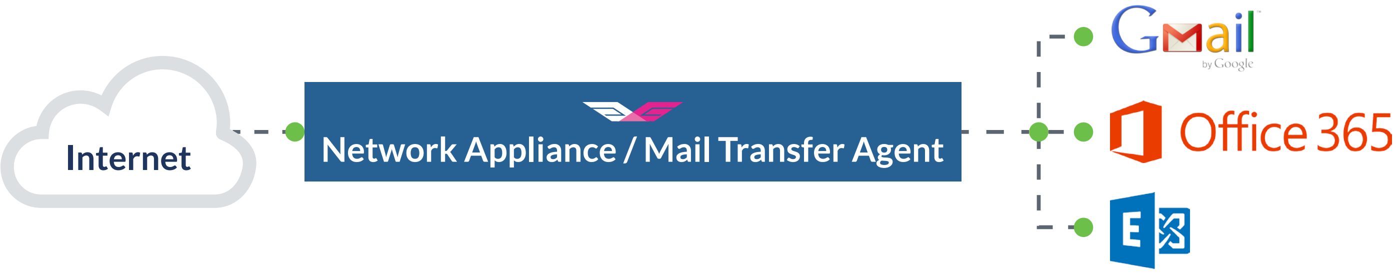
Digital Guardian's flexible controls, including log, alert, prompt, move, quarantine, block, or encrypt, deliver the situational granularity needed without impeding legitimate business. For example, DG controls can log without blocking when a patient's data is sent to the insurance company, but block when that same data is sent to a personal Gmail address. These controls work across the following egress channels:

- Network
- Web
- Data Repository
- Cloud
- Endpoint

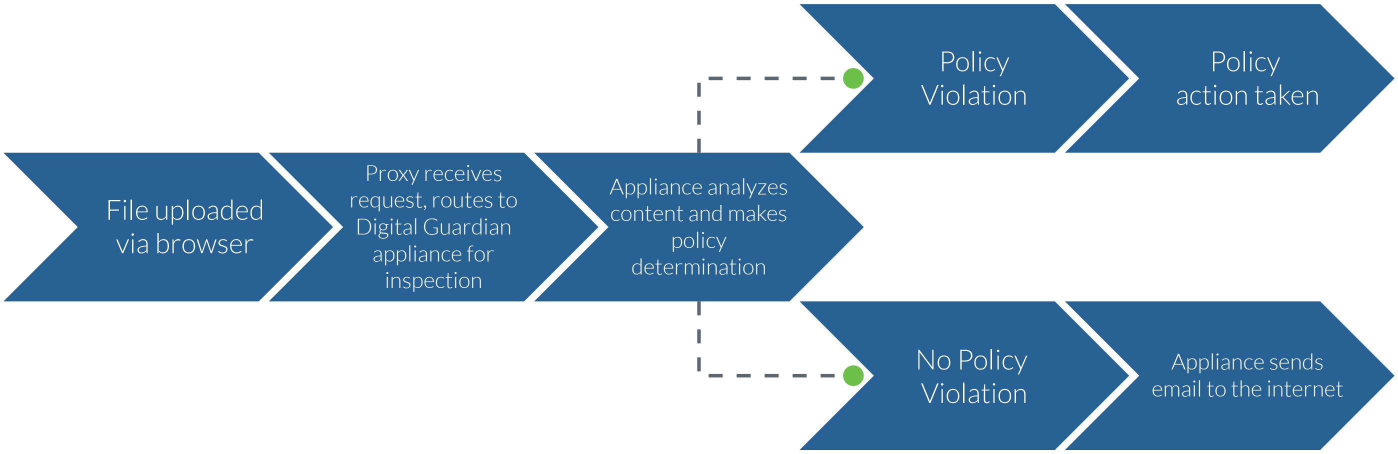
- **Network Monitoring & Control**
  Digital Guardian appliances monitor network traffic to provide instant visibility into policy violations and report incidents involving sensitive information directly into the DGMC. The appliances monitor and inspect traffic across any TCP protocols, identifying sensitive data and flagging policy violations. Network inspection is often a first step for an organization's compliance program as it doesn't impact user experience nor degrade network performance. This assesses the type and extent of data loss exposure before implementing security controls over user activity. Via either a SPAN or a TAP Digital Guardian appliances inspect network traffic for sensitive information and can then take appropiate actions to protect that content.



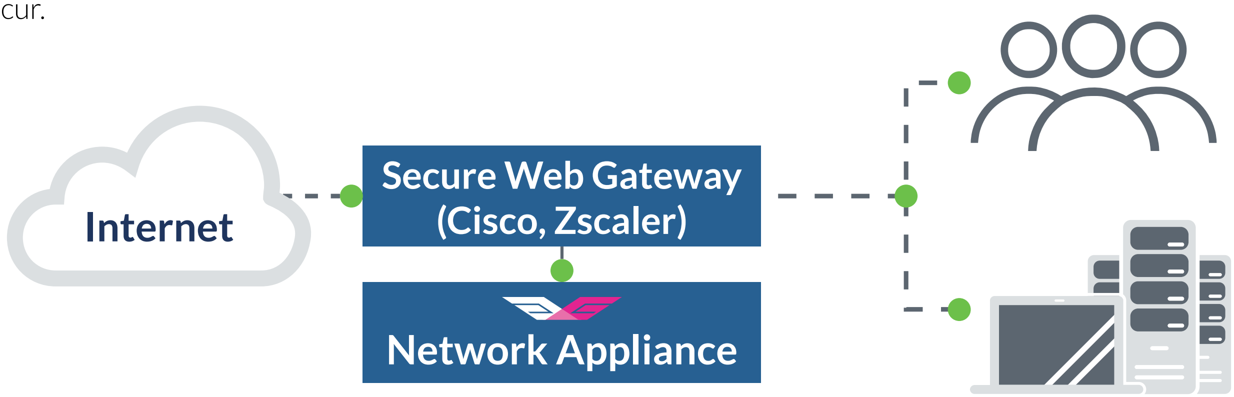
- **Email Monitoring & Control**
  Digital Guardian appliances incorporate in-line web inspection that integrates with a proxy server to provide policy-based web monitoring and control.



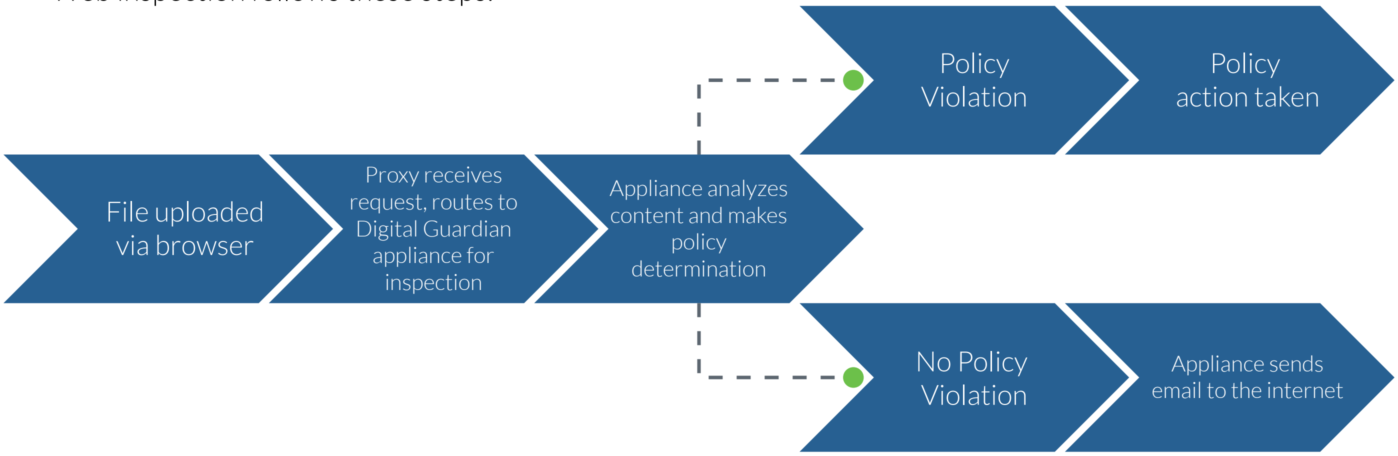
Administrators can setup incident management workflows to automate any response actions in the event certain policy violations occur. For organizations that require email encryption to secure sensitive email communication, Digital Guardian offers optional email encryption, providing seamless and secure integration with leading email encryption services from Cisco, ZixCorp, and Voltage Security. Policy-based email encryption as part of the solution offers greater accuracy and control than the limited DLP capabilities of message gateway solutions.


File uploaded via browser
Proxy receives request, routes to Digital Guardian appliance for inspection
Appliance analyzes content and makes policy determination
Policy Violation
Policy action taken
No Policy Violation
Appliance sends email to the internet

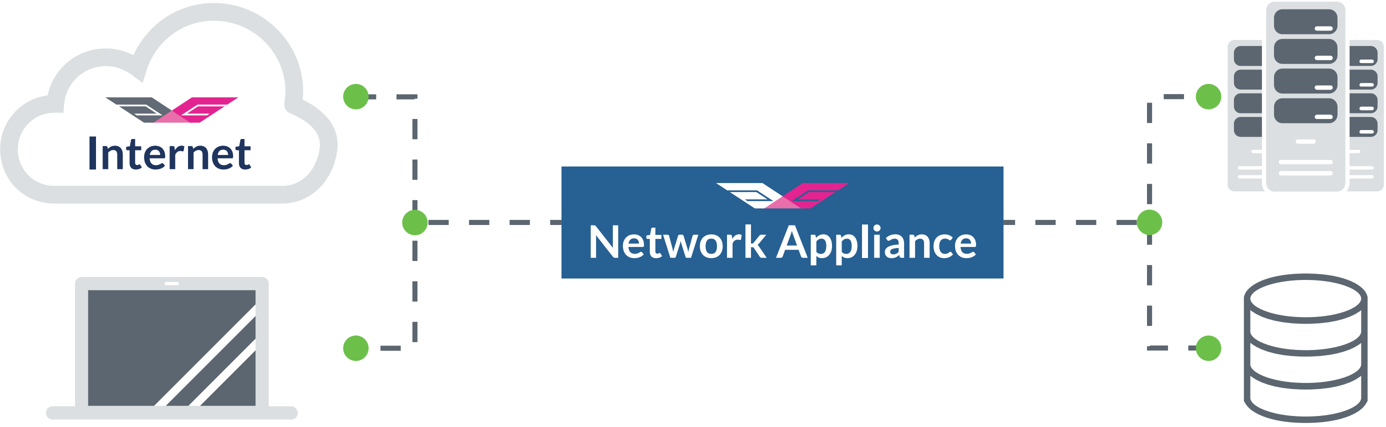
- **Web Monitoring & Control**
  Digital Guardian appliances incorporate inline web inspection that integrates with a proxy server to provide policy-based web monitoring and control. All traffic is inspected for sensitive content, administrators can setup incident management workflow to automate any response actions in the event certain policy violations occur.



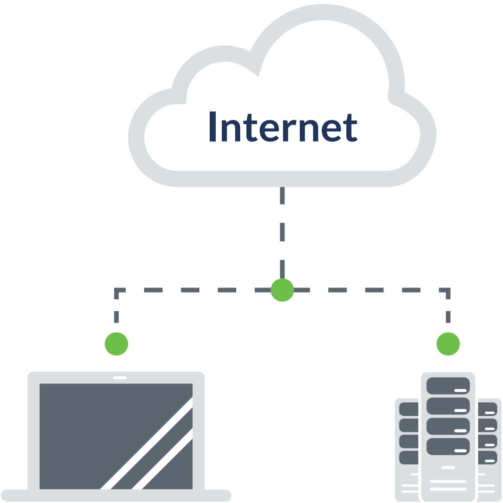
Web inspection follows these steps:


Policy Violation
Policy action taken
File uploaded via browser
Proxy receives request, routes to Digital Guardian appliance for inspection
Appliance analyzes content and makes policy determination
No Policy Violation
Appliance sends email to the internet

- **Data Repository and Cloud Storage Monitoring & Control**
  Digital Guardian appliances locate and identify sensitive data residing on endpoints, servers, network shares, and databases providing visibility and control of potentially unsecured sensitive information. Detailed audit logging and automatic remediation provide administrators with the information and controls needed to demonstrate compliance, protect confidential information, and reduce risk of data loss.



In addition to local repositories, 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. Automatic remediation actions include encryption, removal, or moving sensitive data that violates protection policies. Information that is already stored in the cloud can be audited at any time with the same remediation actions.



- **Endpoint Monitoring & Control**
  The Digital Guardian endpoint agent provides the deepest understanding of system, user, and data level events, and the granular controls to stop sensitive data from getting out of your organization without interrupting legitimate business activity. Once the policy is received from the DGMC, the agent operates without user impact and monitors user actions for policy violations, malicious operations, or correlation of multiple events.

  With Digital Guardian, organizations have visibility into all applications that run in the environment, and can control which applications run and what actions they can take. Digital Guardian understands the function of each application, and prevents applications from being co-opted to perform data movements that could compromise security and(or) compliance requirements. Organizations can block unknown executables and ensure that only approved applications and versions are used. Administrators can enforce the use of specific browsers or limit internet access to the company's network proxy or VPN.

  The Digital Guardian agent delivers the most comprehensive ability to protect sensitive data, regardless of whether the device is on or off the network. Digital Guardian allows organizations visibility and control into data at:

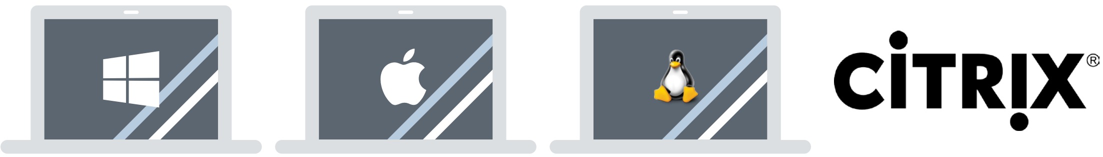
  - View/Open
  - Save/Save As
  - USB Transfer
  - Burn to CD/DVD
  - Delete/Recycle
  - Encrypt/Compress
  - File Create
  - Cloud Sync

  Only Digital Guardian allows organizations to see and control "Print Screen" and "Cut/Copy/Paste" operations to further protect sensitive data.

  Only Digital Guardian allows organizations to see and control "Print Screen" and "Cut/Copy/Paste" operations to further protect sensititve data.

  If the user action is allowed by policy, the agent is silent. If the user action violates policy, endpoint agents can apply a wide range of controls based on data content, context, user, application, system process, and risk type, including:

  - **Monitor –** Allows users to complete all actions without warning or blocking, while logging all user activity.
  - **Prompt –** Provides a warning to users that an activity violates policy.
  - **Block –** Prevents users and processes from performing the requested action.
  - **Classify –** Applies one or more tags to a file or email to track it throughout its lifecycle.
  - **Encrypt –** Allows encryption to be applied as needed to files stored on a removable drive.
  - **Alerts and Notifications -** Alerts or notifications automatically pop up on the end-user machine.



DATA PROTECTION AND TAGGING FOR DATA PROTECTION ACCURACY

Data classification is a process to categorize different types of information (data) based on various criteria driven by governance, compliance and (or) regulation frameworks (PCI, HIPAA, ITAR, SOX, GDPR), protection of intellectual property (IP) or simply based on business and information security requirements. There are a few basic questions organizations may ask to help define classification categories:

- What are the data types?
- Where is the sensitive data located and who is the owner?
- How is the sensitive data used and shared?
- How is the sensitive data governed?

Effective data protection requires an understanding of what is deemed sensitive. Understanding where and how sensitive data is used drives more informed security decisions. With more accurate classification incorporating user knowledge, security administrators can better protect all data.

After classification categories are defined, organizations typically end up with 3-5 classification definitions. For example, definitions may include: *restricted* for compliance data, *private* for internal data, and *public* for external data. Defining classification and how the data is handled is critically important. Classification categorization will be later used within protection policies so accuracy of data identification becomes an integral part of data protection solution. Digital Guardian can accurately and precisely identify sensitive files and provide audit information.

As part of the classification process, an organization may choose automated tools or manual processes to achieve data classification goals. Digital Guardian provides both automated and manual classification methods.

CLASSIFICATION PROCESS	DESCRIPTION
AUTOMATIC	Gathers information about the data and provide scalable data classification without user involvement.
MANUAL	Relies upon data users and owners to enhance automatic classification by leveraging their data knowledge.

Choosing classification method(s) depends on data type and business requirements. As an organization evaluates its classification needs, a single method for compliance data may provide the best results however a combination of methods to identify intellectual property data might work best.

Digital Guardian supports the following methods to classify and prioritize an organization's data:

CLASSIFICATION METHOD	DESCRIPTION
CONTEXT-BASED CLASSIFICATION	Automatically classify documents based on data or document 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 the data

This combination of technology-based and user-driven decisions provides balance and ensures the right Data Loss Prevention polices are enforced on the right data. Digital Guardian's Advanced Threat Protection 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.

CONTEXT-BASED CLASSIFICATION

Digital Guardian context-based classification uses metadata attributes such as user, system, location, or application to determine data sensitivity. Context-based classification gathers information about sensitive files without knowledge of actual data content. This process is flexible and extensible; it accommodates multiple data attributes and the relationship between them. This classification method becomes crucial if an organization is trying to protect unstructured sensitive files, where content based inspection alone may be inefficient.

Digital Guardian identifies and classifies sensitive data files such as engineering files, design documents, software source code, formulas, and other IP information with flexibility and accuracy. Digital Guardian was founded to solve a context based classification business problem and continues to develop this core capability. Digital Guardian context classification recognizes multiple data attributes, such as:

Digital Guardian was founded to solve a context based classification business problem and continues to develop this core capability.

- Identity of the user who created the data
- Network source and destination
- File type, name, extension, path
- Operation: read, write, open, save, copy, move, recycle, delete
- Drive type: fixed, removable, network
- Buffer: Copy, paste, print screen
- Application: Image Name, Parent process and version
- Email: To, From, CC, Body, Attachments
- Time of use
- 200+ other data attributes

CONTENT-BASED CLASSIFICATION

Digital Guardian can inspect, analyze and classify documents based on the specific content found within a document. To identify specific content Digital Guardian can utilize various techniques:

- **Keywords and Dictionaries**
  Digital Guardian can identify specific content based on keywords or collections of keywords (Dictionaries). Keywords can be associated with different industries, compliance, process terms, internal acronyms, project code names, and more. Keyword dictionaries require an understanding of the information being analyzed as well as common work arounds and misspellings. For example banking keywords would contain the following: bank, card, cvv, magnetic strip, account, routing number, but may also have magstrip, routing #, or other common variants.

- **Regular Expression (Regex)**
  Digital Guardian can identify specific content based on regex (a sequence of characters that define a search pattern) to validate specific combinations (patterns). Data that can be associated with repeatable patterns can be identified with regex. Regex requires an understanding of the data, how it typically appears, as well as the proper coding for accurate identification of sensitive data. For example VISA credit card numbers can be identified with the following regex “^(?:4[0-9]{12}(?:[0-9]{3})?”

- **Exact and Partial Record Matching**
  Digital Guardian can identify sensitive data based on matching the digital signature of that data. This matching process is granular and can be used for an exact data match (full match of actual data) or partial match (user determined % match). The process of matching to this signature is called Database Record Matching (DBRM). DBRM is a method of creating mathematical hashes of the actual data, then using those hashes to look for that identical data value when inspecting email, a file share, cloud repository, a web posting; anywhere that information would create a policy violation or pose a threat to data leaving an organization is flagged for action. The DBRM method can recognize and register a wide range of both structured (fields in databases or columns in spreadsheets) and unstructured data (document formats such as Microsoft Office, source code and PDF files) reducing false positives and false negatives.

The DBRM method can recognize and register a wide range of both structured (fields in databases or columns in spreadsheets) and unstructured data (document formats such as Microsoft Office, source code and PDF files) reducing false positives and false negatives.

USER CLASSIFICATION

Digital Guardian User Classification (UC) module powered by Boldon James complements automated data classification methods by allowing users to classify data manually. Empowering data owners to accurately identify their sensitive data can deliver a more effective approach to classifying data than using automated methods alone.

Digital Guardian integrates Boldon James Classifier Foundation Suite to provide:

- More accurate data protection
- Enterprise wide data visibility
- Security awareness throughout the entire organization

Data creators and users classify documents into predefined categories when they create, modify, review, or disseminate them. Adding this user-knowledge into the data classification program increases the level of involvement in and awareness of the importance of protecting sensitive data. Customized, visual markers and text can be added to documents or emails to remind users of the sensitive nature of the materials and meet compliance requirements.

Changes to a classification level can be flagged or logged to prevent intentional or unintentional data exfiltration. This assures that sensitive content remains visible to and controlled by Digital Guardian allowing organizations to monitor, analyze, and manage the entire data lifecycle.

DATA TAGGING AND INHERITANCE

Digital Guardian maintains classifications through classification "tags" that persist with the data throughout its lifecycle, or until the classification no longer applies due to a change in the data. For example, if a Microsoft Word document includes a list of credit card numbers, but otherwise contains no sensitive data, Digital Guardian could classify the document based on the presence of the credit card numbers. If a user deleted the credit card numbers, Digital Guardian would remove the classification when the user closed Microsoft Word.

Digital Guardian's tag inheritance enables classifications to follow the data. A child file automatically inherits classification tags from the source file. The tag will persist indefinitely, regardless of the number or types of file operations (For example: Embed in another file, compress). Persistent and inheritable tagging maintains consistent identification, usage auditing, and policy enforcement across files with common content. Changes to a classification level can be flagged or logged to prevent intentional or unintentional data exfiltration. This assures that sensitive content remains visible to and controlled by Digital Guardian allowing organizations to monitor, analyze, and manage the entire data lifecycle.

PRACTICAL APPLICATIONS OF DATA CLASSIFICATION

Data classification can help identify and protect different types of sensitive data. Digital Guardian adds automation to classification process to classify sensitive data and help protect organization's digital assets without user intervention. Manual, user-classification adds the knowledge workers direct touch with the data to the classification process. Below are examples of data classification use cases:

User-based Classification

- **What data to protect:** Patent files
- **Company information:** Law firm with remote end-users

How Digital Guardian can help: A law firm employs a team of geographically dispersed patent attorneys; they require remote access to sensitive client files along with administrative and general company documents. The firm requires that all patent documents be classified as "Restricted" to support the heightened data protection required. Due to the dynamic nature and wide variation of the information in these documents, content inspection would be difficult; user-based classification provides the accuracy needed. Lawyers can self-classify their patent files, while leaving general files unclassified. Digital Guardian sees the user-assigned classification and can protect this sensitive patent information, without the overhead of protecting all documents as if they were patent files.

Content / Context classification

- **What data to protect:** PII information stored in HR share
- **Company information:** Hospital

How Digital Guardian can help: A hospital stores health care records in an HR share along with other files that do not contain regulated, PHI information. The hospital must ensure that no sensitive PHI files are stored on local workstations, these files must remain on HR share. Content inspection is used to automatically classify files and protect sensitive PHI. If Digital Guardian determines the file as being from the HR share and containing sensitive PHI information, it will not be allowed to be saved elsewhere.

User / Content classification

INTEGRATION WITH OTHER SECURITY PLATFORMS

- **What data to protect:** Intellectual Property (chemical formulas and manufacturing processes)
- **Company information:** Manufacturing

How Digital Guardian can help: A manufacturing plant needs to classify their data to apply data protection policies to sensitive files containing valuable IP. The company relies upon proprietary chemical formulas and manufacturing processes to maintain their competitive advantage. The chemical compounds do not follow any predictable pattern nor do the internal manufacturing processes documents. Because these engineering documents are required to be stored on a specified server, context based classification will flag all documents on that server as "Sensitive" limiting what can be done with them.
Digital Guardian complements an organization's layered security programs, and integrates with several other solutions for enhanced alerting, security and forensics.

Security Information and Event Management (SIEM) – SIEM solutions allow organizations to aggregate data related to events on endpoint systems and servers, and to correlate those with network and other log source data: applications, databases, file integrity monitoring, system configuration, audit and vulnerability information. Digital Guardian provides visibility across data in motion, data at rest, and data in use and adds value to SIEM implementations by enabling new use cases in the areas of insider threats and external attackers. Digital Guardian SIEM partners are HP ArcSight®, IBM QRadar® and Splunk.

Network Security – Network security solutions detect external threats and network attacks. Digital Guardian integrates bi-directionally with network protection systems; by working in conjunction with Digital Guardian, network security adds a layer of protection against attacks. 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.

DEPLOYMENT OPTIONS

Many organization experience challenges either deploying DLP solutions or successfully running the solutions over the long term. Those challenges are generally related to:

- Maturity of IT and Security Organization
- Enterprise Wide Buy-In
- Lack of Thorough Planning
- Overextending the Security Team
- Long Term Execution

With years of experience deploying DLP solutions across global enterprises and a proven deployment methodology, Digital Guardian can help any organization achieve its compliance and security driven data protection goals. Our data protection platform and know-how ensure organizations can effectively protect their data.

The priorities (compliance, security, budget) and resources of each organization are unique, and may evolve over time. To support this, Digital Guardian offers three deployment options. Customers can run Digital Guardian as an on-premises solution, as a Managed Security Program hosted by Digital Guardian, or as a Hybrid Managed Security Program.

ON-PREMISES DEPLOYMENT

Deploying within your infrastructure allows organizations to leverage the investment in the business. The knowledge within the team is used to build, deploy, and manage the entire program with as much guidance from our professional services team as you need. Organizations use our patented and proven data protection platform to support advanced risk analysis and policy enforcement across virtually any business process. You have total ownership and control over your data protection program by hosting the infrastructure in your environment and managing and administering policies, rules, and reports. For organizations with or looking to build in-house expertise, an on-premises deployment makes the most sense.

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 advanced threat protection (ATP), 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 SAS-70 certified Type II data center. DG MSP benefits include:

- **Fully managed data protection infrastructure:** DG 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 DG 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:** DG 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.

HYBRID MANAGED SECURITY PROGRAM (HYBRID MSP)

Many organizations like the ability to manage their IT resources themselves, however security resources are often scarce and organizations need to focus on their most critical activities. For these companies, Digital Guardian offers complete data protection through a Hybrid MSP model.

Hybrid MSP allows organizations to focus on their core business and IT expertise and rely on Digital Guardian for security expertise. Customers' teams manage all hardware and supporting software on-site, so data never leaves the corporate environment. The Digital Guardian Managed Services team adds its security expertise to manage Digital Guardian, including developing and managing policies enterprise-wide.

SUMMARY

Digital Guardian delivers threat aware data protection to stop both insider and outsider threats. We do this through the deepest visibility, real time analytics and flexible controls, all of which can be delivered via multiple deployment options.

- **Visibility:** Digital Guardian delivers the deepest view into your data to show where it is, what it is, and when it is at risk; to go from reactive to proactive you need comprehensive visibility across the extended enterprise.
- **Analytics:** Digital Guardian helps you identify and focus on your sensitive data, driving information security effectiveness and regulatory compliance.
- **Flexible Controls:** The controls required to operate an effective data protection program range from logging all activities for better insights to blocking activities deemed too risky for the organization. Digital Guardian enables organizations to support user education and administrative actions to deliver effective data protection.
- **Multiple Deployment Options:** Organizations have different priorities when it comes to their data security program. For those investing in their information security team and infrastructure an on-premises deployment helps further leverage that investment. For organizations looking to have a team of security experts manage it for them, our industry first Managed DLP provides an instant InfoSec team. For organizations who have the infrastructure but need the expertise our hybrid approach fills the gap.

ABOUT DIGITAL GUARDIAN

Digital Guardian was founded in 2003 (as Verdasys) in reaction to a problem that had no solution at the time – insider theft of intellectual property (IP).

IP is typically unstructured data, so the founders had to solve the most difficult data protection use case first - effectively identifying and tagging unstructured data when it's in motion and in use on an endpoint. It's why Gartner Research has named **Digital Guardian #1 in IP protection** since the inception of the DLP Critical Capabilities report (a companion report to the Gartner Magic Quadrant for Enterprise DLP).

Since that time, in partnership with our customers, we've expanded our mission to deliver solutions that protect all sensitive data against all threats – internal and external. Our appliances enable organizations to meet compliance requirements for protecting personal information with little overhead and expand our coverage to Office 365 and cloud storage.

In response to customer challenges with hiring and retaining security talent, we launched the first data protection managed service and now manage more than 650,000 endpoints. To protect sensitive data from new and motivated adversaries we've created an advanced threat protection managed program. This program provides our customers the latest cyber defense strategies and the threat intelligence they need to stay ahead of cyber criminals.

We're the only security company 100% dedicated to protecting sensitive data from inadvertent loss and malicious theft.

DIGITAL GUARDIAN®

CORPORATE HEADQUARTERS
860 Winter Street, Suite 3
Waltham, MA 02451 USA
info@digitalguardian.com
781-788-8180
www.digitalguardian.com

SHARE