FORTRA™

GUIDE *(Data Protection)*

Data Protection Technical Overview

Table of Contents

Introduction

Your business is not static, nor is the data that drives it. The volume and value of sensitive data being created is growing and changing by the minute, leaving it at risk of loss or theft. With hybrid work environments making remote collaboration a reality of daily business, and companies choosing to migrate technology to the cloud for both cost-saving and efficiency purposes, enterprise data protection solutions are more important than ever to protect data regardless of where it's located, or how it's used.

Data classification, data loss prevention (DLP), and secure collaboration are mature solutions that have been around for decades, and ensure your organization's most sensitive data is properly protected from the point of creation, to outside the organization. However, the rapid release schedules and accelerating changes in operating systems, applications, and browsers can cause many traditional data protection solutions to be woefully inefficient. Organizations who are using data protection solutions from providers who aren't keeping up are spending too much time, effort, and budget troubleshooting, and not enough time delivering meaningful data protection. New market entrants tout "easy" solutions to data protection, but often gloss over the big compromises their solutions will lead your organization to take.

You need to be entrusting your data protection to best-of-breed solutions who will work to fit your business requirements, and not the other way round.

How/Why We're Different

DLP that provides the highest level of visibility across the entire extended enterprise.

Traditional enterprise DLP's inefficiencies start with the requirement to throw loads of data center 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. Because Digital Guardian DLP lives at the kernel level, users have the ability to inspect far more data, as well as achieving the highest level of flexibility in embedded classification, giving the greatest visibility of what's happening to data across the environment.

Data Classification allows you to understand, prioritize, and improve data protection programs.

Digital Guardian, Titus, and Boldon James Data Classification solutions apply visual and metadata labels to ensure data is protected and controlled wherever it travels. From user-driven, to entirely automated, our solutions are fully flexible and customizable to meet your data protection requirements. Our multi-layered approach to policy and label design allows for the most specific/detailed policy and enforcement that your organization requires, with the ability to apply policies to most data types, including PDF, CAD, design documents, and more.

Secure Collaboration encrypts and controls access to files wherever they travel.

Secure collaboration makes it easy to securely share files externally with third parties, providing you control over file access and protection outside your organization. Fortra attaches powerful encryption, security, and policy directly to the data itself, giving you granular control over your data, no matter where it goes. User onboarding and collaboration has never been easier. Simply adding an email allows a user to securely collaborate instantly, without having to adjust Active Directory, or other user processes to get going. Meanwhile, we make it just as easy to remove access as it does to give access, maintaining the seamless user experience that highly productive teams demand.

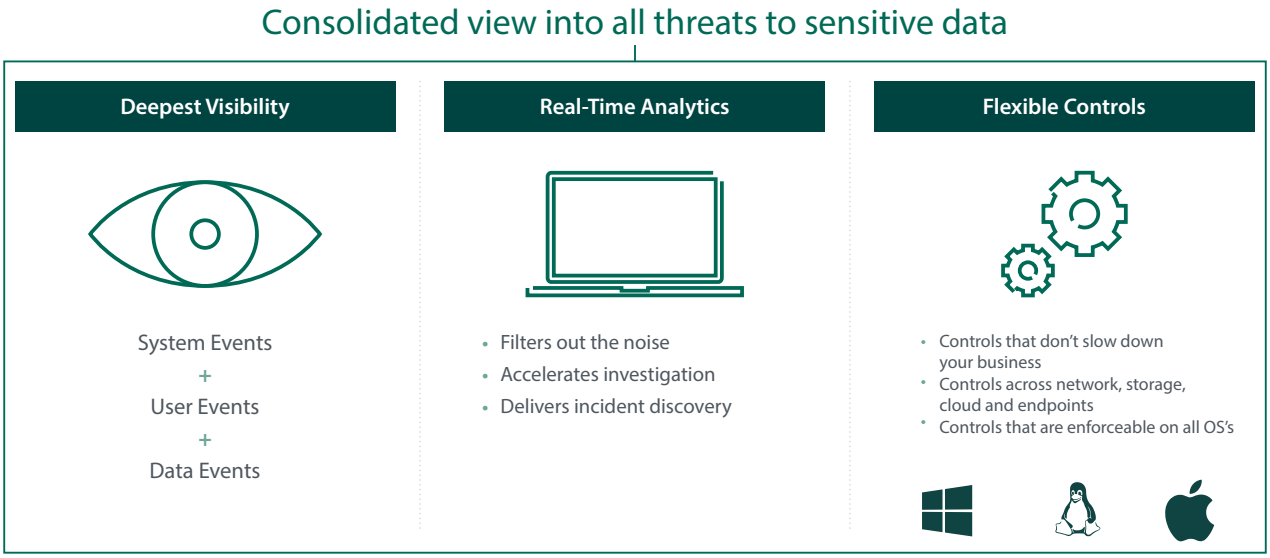
The Key Requirements for Successful Data Protection

The plethora of data security solutions available for use within an ever-changing landscape can make data protection seem like a daunting and complex task. Regardless of the type of data and the subsequent threats, there are some key requirements for successful data protection that should be focused on:

- Using solutions that solve data protection use cases end-to-end, not just within embedded technology
- Keeping things as simple as possible – from administrator level right through to end users
- Using a suite of integrated solutions which drives a full data protection program with ease
- Ensuring you have the deepest visibility to all data, in all locations, and activities, at all times

Fortra's leading data protection offering combines data classification along with data loss prevention and digital rights management to deliver data protection throughout the entire data lifecycle.

These solutions not only combine to give you the broadest spectrum of data protection, but provide a 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, and is the foundation for successful data protection programs. As the saying goes, how can you protect your data if you don't know what you have? Which is where a data classification solution is crucial. Our solutions apply visual and metadata labels to ensure data is protected and controlled wherever it travels. Visibility must include data events, user events, and system events, across endpoints, databases or shares, network traffic, cloud storage, and external sharing. 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.
- **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, the reporting capabilities we provide see 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.

Our reporting capabilities enable end users with the ability to access, design, and manage dashboards and reports effectively, while monitoring activities. When key data classification events happen, i.e. a document is created or sent, events are generated by the classification software and consolidated into the reporting database. There are numerous events and examples of these events include, but are not limited to:

- A user sends an email with a selected label value
- A user saves a document with a selected label value
- A user saves a document, or sends an email, without selecting a label value
- A user continues to send an email message that contains a policy violation after reviewing warning
- A downgrade or upgrade of a classification level was prevented or allowed
- The usage of a classification application on identified computers

Our data loss prevention reporting 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.

The breadth and depth of our monitoring and control capabilities make it an ideal platform to drive incident response and investigations. Event forensics are recorded 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

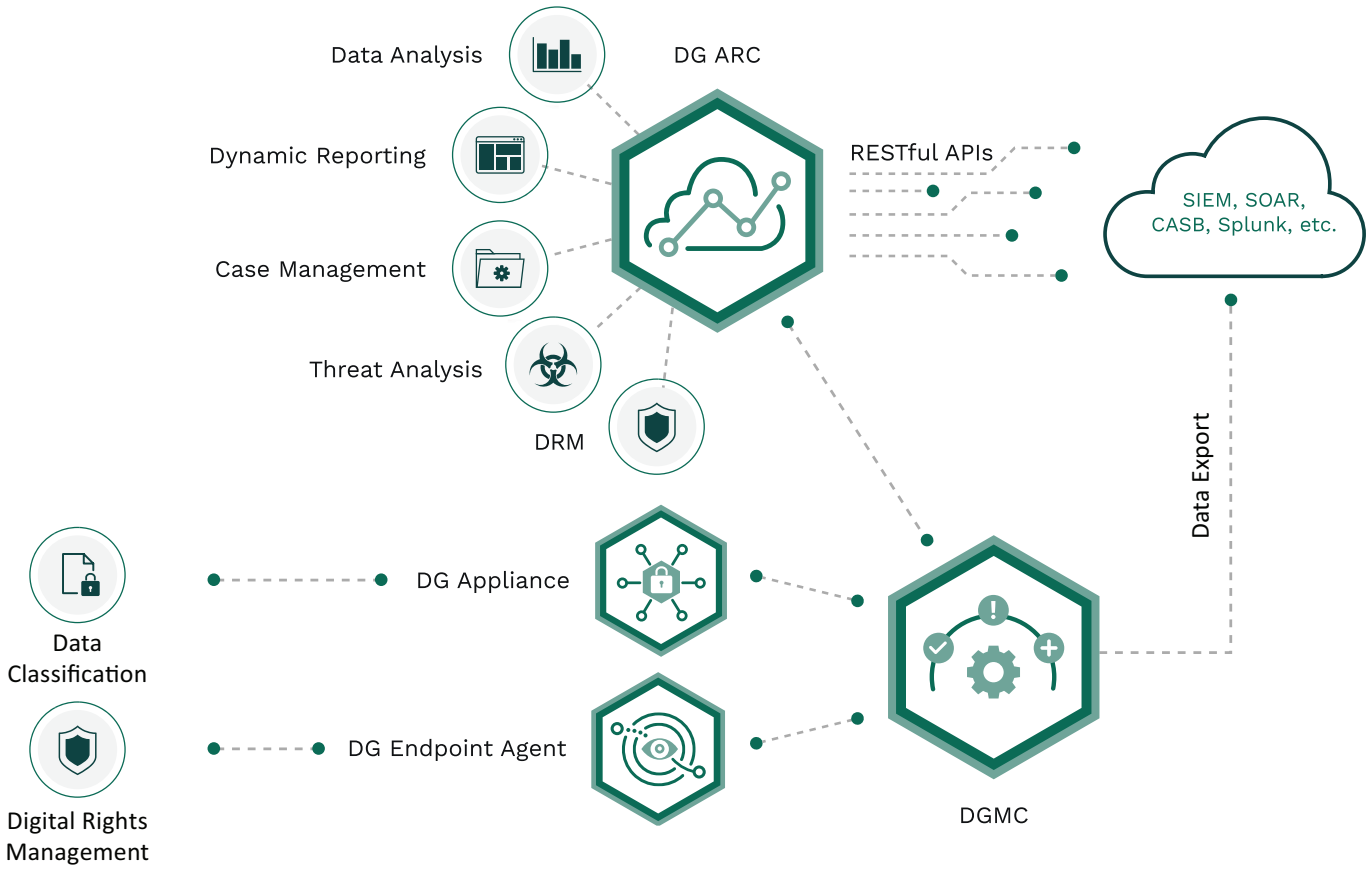
Policies are a way of translating data protection goals into consistent and actionable rules applied throughout the business. Fortra's data protection solutions all offer fully flexible and customizable solutions to enable policy enforcement on and off your corporate network for the data protection you 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

Fortra Data Protection Security Architecture

Fortra delivers granular visibility, real-time analytics, and flexible controls through consolidated data protection solutions.



Fortra Data Classification

Modern data classification solutions combine visual labeling with labels applied to the file's metadata to protect and control use. These labels enhance the performance of third-party technology solutions to determine how a piece of data should be treated, handled, stored, and finally disposed of.

Data classification streamlines the load when it comes to handling data, as well as enhancing data security and compliance – making your investment in security applications work harder. Once data has been classified, organizations can confidently continue their data security journey.

The Benefits of Data Classification

Having a comprehensive data classification solution is critical if your organization:

- Needs to comply with statutory, regulatory, contractual, or mandated compliance regulations
- Is motivated to protect intellectual property (IP)
- Wants to understand where sensitive data is stored and where it is sent
- Has been recommended to do so by an internal or external auditor
- Wants to bolster its security ecosystem and get better return on investment for other data security solution sets

Fortra's data classification solutions provide all these benefits and more.

Delivering the Broadest Data Classification Capabilities

VISUAL MARKINGS

Header/Footer Watermark

Subject line
First line of email body

METADATA

Machine-readable metadata
Pre-defined document properties
Custom document properties

X-headers

Drives downstream data protetion technology, including DLP, CASB, rights management, encryption, and more

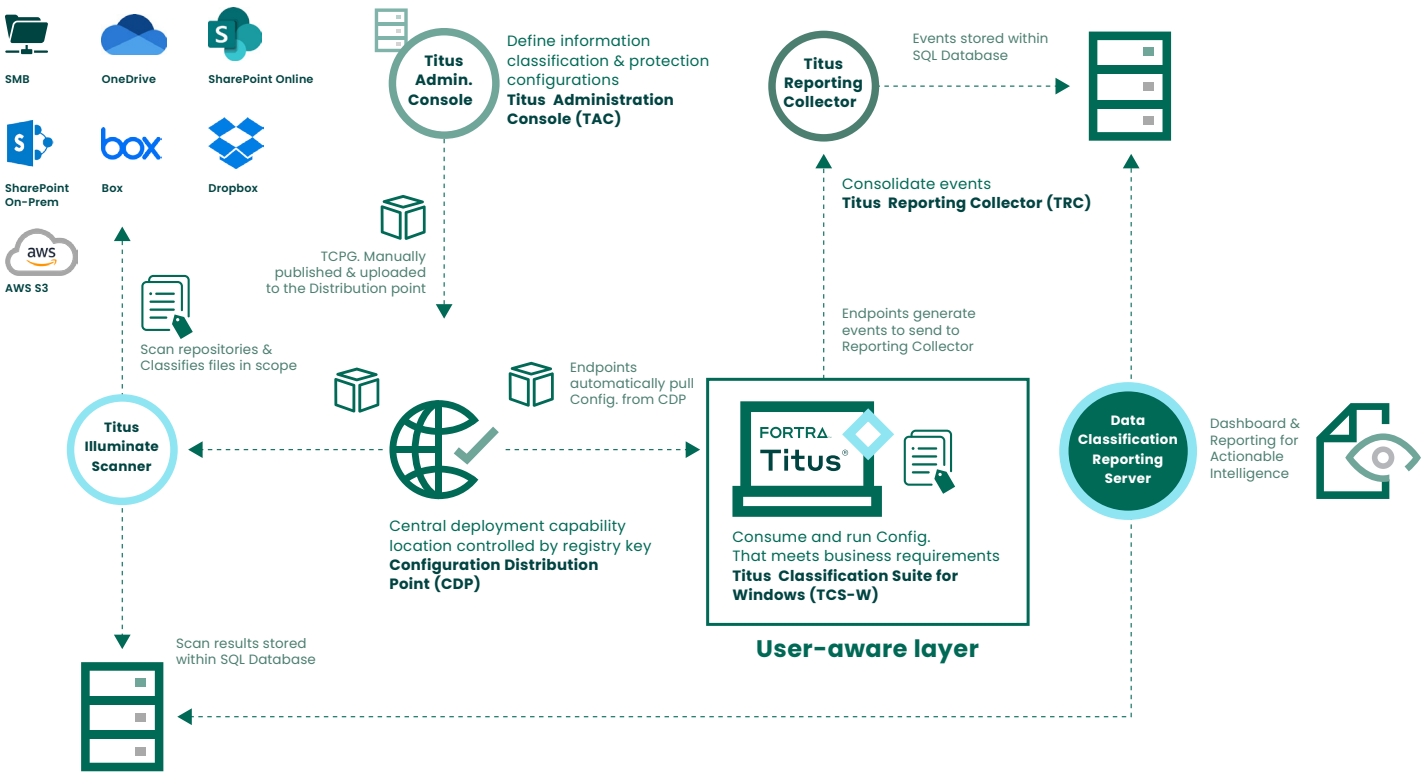
USER AWARENESS

Machine-readable metadata
Pre-defined document properties
Custom document properties

The key capabilities of our leading data classification solutions are:

- **Visual markings**
  Custom visual markings to inform users about the sensitivity of your business content. Visual markings enable end-users to see and understand the sensitivity of the content they are handling. The solution also allows users to remove visual markings on a per-document basis when they are not appropriate.
- **Metadata**
  Custom metadata, including custom document properties and email X-headers, to help drive other data security solutions such as Digital Guardian endpoint DLP.
- **User Awareness**
  Enhanced data security user awareness by enabling your users to classify emails and documents quickly and easily within the Microsoft application they are using.
- **Machine Learning**
  The Data Detection Engine leverages traditional Machine Learning technology, advanced Deep Learning technology, and Smart Regular Expression(Regex) queries to scan the content of emails and documents to detect sensitive information, including Personally Identifiable Information(PII), Personally Identifiable Financial Information(PIFI), and Protected Health Information(PHI).
- **Reporting**
  The Fortra Data Classification Reporting Server delivers dashboards and reports that provide administrators and managers insight into the way that the classification applications are being used in their organizations.

Titus Classification Suite: On-Premise Infrastructure



The main components of the Titus on-premise setup are:

- **Titus Administration Console**
  The Titus Administration Console is a web-based application that allows you to create and target Data Classification Configurations to Active Directory users and groups within an organization. The console uses SQL Server to host the configuration details. The console is supported on Windows Server 2012 R2 and later, and SQL Server 2014 and later. The final action of using the Admin Console is to publish a Titus Configuration File (TCPG).
- **Endpoint applications such as TCS Windows**
  Endpoint applications such as TCS Windows extend Microsoft Office applications with Data Classification capabilities use the TCPG file to present labelling values and make policy decisions. The TCPG file can be made available either as part of the install process, or via a file share or web server location. See later sections for an overview of the various endpoint applications.
- **Data Detection Engine On-Premise**
  The Data Detection Engine (DDE) Server On-Premise includes multiple Docker containers provided by Titus. After these Docker containers and the DDE installation package are installed, an Administrator can create policies on the Titus Administration Console that use the DDE Custom Condition and deploy these configured policies to Titus Illuminate and Titus Classification Suite (TCS) for Windows end users. These policies call the DDE Server to scan for sensitive information in emails and documents and apply policy rules and actions. The DDE Server is supported on Windows 2019 and later, and Redhat 8.5.
- **TCS Reporting Subsystem**
  Each of the endpoint applications may send event information to the Titus Reporting Collector machine. This information is passed with a RESTful API to a system that has Microsoft Message Queuing (MSMQ) configured. MSMQ will provide the events to a local SQL Server version 2014 or later.
- **Illuminate Scanner**
  The Illuminate Scanner is a data-at-rest application that can scan content for sensitive terms and subsequently apply a classification value to the content. Illuminate supports scans of:
  - File shares
  - SharePoint Online and on-premise
  - OneDrive
  - Box
  - Dropbox

  Illuminate runs on Windows Server 2012 R2 or later. It also utilises a SQL Server (2014 or later) to contain the outcome of the scans.
- **Fortra Data Classification Reporting Server**
  The Fortra Data Classification Reporting Server is a web-based application that runs on Windows Server 2016 or later. The Reporting Server utilises a SQL Server (2016 or later) that hosts the dashboards and reports. The Reporting server uses SQL database connections to report upon:
  - TCS Windows events or,
  - Illuminate scan results.

Titus Classification Suite: SaaS Infrastructure

The main components of the Titus SaaS setup are:

- **Policy Manager**
  The Titus Policy Manager is a web-based application that allows you to create and target Data Classification configurations to Active Directory users and groups within an organization. Policy Manager is hosted in the Titus SaaS Cloud. Future versions of Policy Manager will be able to run on-premise. The Policy Manager allows the configuration of:
  - TCS Windows endpoints
  - Office add-in
- **Classification for Office Add-in**
  The Titus Office Add-in ensures that Microsoft 365 Outlook emails and Word/Excel documents are classified before they are distributed. Classification labels are fully customizable to meet internal and regulatory marking standards. Titus Classification can be used to indicate any type of information; common applications include data sensitivity (for example, Public, Confidential) and department (for example, HR, Finance). Users add classifications with a simple and intuitive interface.
- **Data Detection Engine SaaS**
  The Data Detection Engine (DDE) Server SaaS is available to the Google Workspace and Office add-in applications. The DDE Server SaaS can scan for sensitive information in emails and documents and help apply policy rules and actions.

Data Classification Applications

TCS Suite

The TCS Windows Suite is a number of COM add-ins that extend Microsoft Office 2010 SP2 or later (32-bit or 64-bit) including Outlook, Word, Excel or PowerPoint, providing the ability to classify emails and/or documents.

TCS for Mac

The TCS for Mac Suite is an add-in that extends Microsoft Office Outlook, Word, Excel or PowerPoint 2016, providing the ability to classify emails and/or documents. The supported platforms are macOS 11,12 or 13.

Titus Mail for iOS

Titus Mail for iOS allows users to classify emails and meetings through an Apple mobile device application. The color-coded classification labels and the Data Classification user experience can be customized on the Mobile Administration Tool. With an intuitive, familiar user interface and interoperability with Microsoft Exchange, Titus Mail for iOS is easy to deploy and use. Titus Mail for iOS is supported on the iOS 14, 15 and 16 platforms, and the iPad OS 14 and 15 platforms.

Data Loss Prevention by Digital Guardian

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 Digital Guardian Agent is key to endpoint visibility and control. The agent provides oversight of system, user, and data event activity to protect sensitive data. The agent integration provides visibility at the file, network, and application levels, meaning 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:

Protecting with 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 in 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 Tagging 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, also known as Exact Data Matching (EDM), 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 second hashed database element (e.g., a patient's name) and requiring the two 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 analyses 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 & behaviour analytics from a single console.

DG Analytics packages over 150 man-years of data defence techniques into over 100 behaviour-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 behaviours 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 and 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. Digital Guardian's DBRM "fingerprinting" can be used to minimize false positives and false negatives, adding efficiency to data discovery.

Digital Guardian 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.

Tagging

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 tagging of data, and then applying 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 1500 file types and 90 languages, including structured and unstructured data types.

Digital Guardian's integrated tagging 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. Data tagging can be permanent or updated with changes to content. Three methods are available for tagging data:

- Context-based
- Content-based
- User-based

Digital Guardian's ability to combine automated and manual methods when classifying data enables an auditing process that minimizes inaccurate policy enforcement.

This combination of technology-based and user-driven decisions provides balance and ensures the right polices are enforced on the right data. Digital Guardian incorporates the tags into alerts, elevating events targeting high value data to drive immediate action. By providing this multi-faceted approach, organizations can tag 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 the product 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. The software 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 Digital Guardian 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 – Digital Guardian EDR provides the needed context of data movements to enable faster and more accurate determination of the attack, its motivation and impact. It is delivered as a managed service as part of our Managed Security Program.

Cloud Data Protection

Digital Guardian 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. The solution integrates with cloud storage providers to protect sensitive information before it moves to the cloud. It 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, analyse and query system, user and data related events across the network and endpoints over longer periods of time.

Digital Guardian Secure Collaboration

Fortra secures sensitive data through its entire lifecycle, everywhere it travels, no matter who has it or where it's stored. Secure collaboration can help you protect confidential data at the point of its greatest vulnerability—when it's being used by others, and while it travels outside your perimeters into unmanaged domains, devices and applications. Built on a scalable, easy-to-integrate platform, Digital Guardian Secure Collaboration attaches encryption, security and policy directly to the data itself, giving security practitioners and IT teams the power to control it, no matter where it goes.

Secure Sensitive Data Used by Employees

Secure and track any file, on any device. With a single click, protect documents, presentations, videos or images with AES 256-bit encryption and granular access policies that travel with the file. And with a simple, consistent interface on every platform, Fortra promotes secure behavior and dissuades your employees from choosing risky, insecure workarounds.

- Report on which internal users can access sensitive files and any failed attempts.
- Control sensitive files at any time, even after file is emailed, shared, or if it resides on a terminated user's device.
- Control sensitive files in core authoring applications (e.g., view, edit, print, copy/paste, watermark).

Leverage Modern Collaboration Securely

Box, Dropbox and SharePoint enable productivity improvements and convenience for knowledge workers, and greatly facilitate information-sharing with external users.

- Control access to sensitive files even after they have been shared with external users via cloud collaboration tools, email, or other means.
- Standardize on a sanctioned cloud collaboration tools without risking vendor's access to sensitive files.
- Employees and external users can collaborate securely via cloud apps.

Mitigate Compliance Risks

Regulatory bodies continue to implement rules and penalties related to maintaining privacy and security. Organizations must achieve a state of continuous compliance while allowing business to be executed.

- Files containing PII, PCI or PHI can only be accessed by authorized users.
- Audit trail of all successful and unsuccessful attempts to access sensitive files.
- Ability to revoke access to sensitive files, even if they are shared with unauthorized users.
- Your teams have the option to leverage our SDK and REST APIs to encrypt, track and revoke access to files.

Active File Protection

File content is always secure, even while in use:

- Apply AES-256 Encryption to any file type to ensure sensitive data can't be accessed by unknown parties.
- Granular visibility and centralized control; understand how your content is used, by whom, and proactively investigate unauthorized access attempts.
- Policies can be based on a number of pre-defined parameters including file location, name, type, securer, sender, recipient, group, or other pre-existing permission structures.

Flexible Deployment Options

Increase overall security of file data by integrating Digital Guardian Secure Collaboration into your own applications:

- Pure SaaS deployment model.
- Allows for hybrid model where infrastructure for protecting/viewing files and key management can be deployed on-prem.
- VPC option in AWS for customers with high security postures.
- SDK allows for integration into 3rd party applications such as web apps, DLP, classification, and DMS.
- Integrate with ID management solutions such as Okta, Google, AD, LDAP, etc.
- Integration with existing file share solutions such as Box, Dropbox, SMB, SharePoint and OneDrive.
- Configurable to work with enterprise email archiving solutions

File Activity Tracking

Easy-to-use web-based portal for expansive in-product auditing:

- File access, duration, location, actions
- User login, file access and actions
- Device type, information, and access
- System events (admin and connector activities)
- Syslog support
- CSV export

The Digital Guardian Secure Collaboration Security Architecture

Fortra's secure collaboration platform enables businesses of all sizes to effectively protect any kind of data, and then track, audit and manage the policies securing it in real-time, no matter where it travels. With Fortra, it is possible to secure data no matter what device, person, cloud or application creates or receives the data, even if – and after – it falls into the wrong hands.

Our unique security model follows your data wherever it goes. For every individual in your organization, we make it effortless to securely collaborate with anyone, no matter which tools they choose to use. For IT and Security practitioners, Vera provides powerful management and oversight in a cloud-based platform that can coordinate and monitor activity independent of where content is stored.

Our secure collaboration architecture is designed to address the challenges created by today's highly collaborative, cloud-based and mobile-centric work environment. Based on the assumption that traditional perimeter - and endpoint-based security solutions are ineffective ways to protect your enterprise's data, Fortra provides flexible, transparent data security that is:

Storage, Transit, and Data-Agnostic: Due to the highly collaborative nature of business, it is not safe to assume that enterprise data resides solely in controlled systems. A better approach is to design a system that can operate securely, independent of how information is shared or stored. And, to ensure the control, management, and ownership over critical data, the platform must permit any kind of content type to be controlled and monitored consistently.

Data-Centric and Policy Driven: Secure cloud platforms permit the centralization of policies that govern the management of sensitive enterprise data. By giving organizations central control over access, sharing and collaboration, policies follow the data and can be implemented globally and automatically across the entire organization.

Designed for Flexibility, Adoption, and Compliance: In a complex organization, data security is improved through adoption and compliance, and the fastest path to these goals is through useful, flexible and consistent user experiences. Securing data must be simple and transparent, and there must be as little friction as possible for collaborators receiving secured data - no matter what platform.

The Secure Collaboration Architecture

To address these three requirements and deliver a highly available, flexible and confidential security system that can serve both large and small businesses alike, Fortra incorporates three primary components in its platform architecture: a secure cloud platform, a set of end-user clients, and a web-based administration dashboard.

Digital Guardian Secure Collaboration Cloud Platform

The central component of the service is the cloud platform. The Digital Guardian Secure Collaboration Cloud Platform manages the policy and controls for each customer, or tenant on the platform, and securely manages the processes of creating keys, enforcing access policies and aggregating events and activities for audit and reporting purposes. No customer data or content is stored on the Cloud Platform.

End-User Clients

The end-user clients on mobile devices, Windows PCs, and Apple OS X desktops facilitate the encryption, decryption, and policy determination for everything secured by Vera. Through each endpoint, we can transparently confirm identity, protect new data as it is created, enforce policy restrictions, and ensure the secure transmission of keys and policy to and from the Cloud Platform. An end-user client permits IT teams to centrally manage access on devices both in and outside the enterprise's control.

Secure Cloud Policy Management

A key tenet of the Digital Guardian Secure Collaboration security model is that our platform never stores customer content or application data in any way. The primary information that lives in the Cloud Platform are the policy definitions and encryption keys, separated logically for each customer. All communication between the cloud platform, device clients and the administrative Dashboard is secured in transit and at rest with at least SSL 2.0 (though TLS 1.2 is preferred) and AES 256-bit encryption. Each secured document is encrypted with a unique key that is secured within the Cloud Platform. These keys are transmitted securely via TLS/SSL to the clients which form a trusted key space on the end user's device. Audit logs for every successful and unsuccessful access request to a document are recorded. Keys are not stored locally on the endpoint unless the policy owner specifically grants that privilege for offline or time-bound access. Additionally, End-User Clients protect the enterprise against man-in-the middle attacks from custom or forged certificates.

To decrypt and access a protected file, the opposite occurs - a request for a decryption key is sent via the client to the Cloud Platform via TLS/SSL for the specific file. That request is verified against the user permissions and policy restriction for the document, and if access is confirmed, the client is given access to decrypt the file. In the absence of a client, the end user will be given the choice to view the secure file via a browser interface. All access information, including time, identity, action and location are logged for the Dashboard and audit trail. Centralization of policy management and administration is critical, ensuring that copies of documents or edited versions do not lose the original's security. The system will maintain the integrity of the original. As a result of this design, Fortra employees and engineers cannot see customer content, unless the individual has been expressly granted access by a content owner. As a result, customers in even highly regulated industries trust Fortra with their most sensitive data.

Consistent, Transparent User Experiences

One of the reasons employees have not adopted traditional data and content security solutions like RMS and DRM is that they require users to change the way they work. Document-specific settings are disruptive to the process of getting work done and serve as impediments to adoption. People need instant, seamless access to their information, on any device, and at the same time, IT needs to ensure that critical information is protected. With Digital Guardian Secure Collaboration, IT can deploy a non-invasive, passive client that manages the application and enforcement of policies invisibly in the background on every user's device. A user with the client installed can open, edit, and share information however they choose without impacting their efficiency or effectiveness. For a user in-policy, opening a secure document is no different than opening any other file. Fortra provides native clients for Windows and Apple OS X desktops and laptops, as well as mobile applications for iOS, Android, and

Windows 8 tablets. The client is designed with the concept of "smart defaults" in mind, giving users the right nudges and indicators to secure important content as it is created. For access to secured documents away from a trusted device, Fortra also provides a web-based document viewer that supports read-only access to content. For desktops, Fortra also integrates with popular email clients like Outlook and Apple Mail, allowing users to protect attachments, apply policies, and share information directly from an email.

The Digital Guardian Secure Collaboration Policy Badge

An important element of the secure collaboration ecosystem is the Policy Badge, the user experience element that clearly demonstrates a user's access permissions and any policy restrictions on a document. When a secure document is opened, the client overlays a Policy Badge on the document that shows what restrictions are enforced. These policies can be set broadly, or on a per-document basis, and allow end users and administrators to prescribe granular permissions to documents, including the ability to limit copy/paste functions. Finally, all Digital Guardian Secure Collaboration access points, whether web, mobile or desktop, are integrated with enterprise identity and permissions management tools like Okta and Active Directory, further improving access and transparency in the system. By allowing customers to authenticate users to Digital Guardian Secure Collaboration agents with their existing corporate directory service, Fortra streamlines and simplifies the login, access, and provisioning of accounts.

Policy, User, and Content Administration (Dashboard)

The Digital Guardian Secure Collaboration Dashboard is the central console where our customers aggregate, analyse and take action on all the activity around their data. Returning to the fundamental assumption that perimeter and endpoint security are not enough to protect an organization's sensitive information, Fortra gives both end users and IT administrators full visibility and control over all their content, no matter where it is stored or how it is transmitted.

Through the Dashboard, an admin can manage access controls, set and update policies, oversee users and activity, and run audit reports. The web-based dashboard provides full visibility and management and aggregates event data in a simple, powerful dashboard.

The Dashboard also allows an administrator to centrally view all policies in effect by the organization and can also update those policies in real time. This is a critical capability, allowing an admin to instantly revoke access or adjust permissions to documents that have already left the organization's control. An IT admin can also manage user accounts, control groups, create new policies, and view all files secured.

Beyond simple administration and management, the Dashboard is a powerful analytics and SIEM tool. The Dashboard provides analytics on user adoption, policies in place, and attempted (and more importantly, unsuccessful) accesses to content. In tandem with the end-user clients, this console also can provide insights into attempts to tamper with a client or endpoint in an effort to gain unsanctioned access to information.

Thank you for reviewing Fortra's Data Protection capabilities. We look forward to helping you solve data protection challenges. If you have any question, please get in touch with Fortra on our website.

FORTRA™

Fortra.com

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.