FORTRA

DATASHEET (FORTRA DLP)

Comprehensive DLP for Rapid Deployment and Results

Today's most successful businesses are digitizing virtually every aspect of their operation. That's led to dramatic influx in data across the enterprise landscape and in turn, the value of sensitive data that's collected, processed, stored, and needs to be protected by organizations.

Data loss prevention (DLP) is a time-tested solution that ensures your organization's most sensitive data is properly protected. These days, however, changing release schedules and evolving operating systems, applications, and browsers can cause legacy enterprise DLP solutions to be woefully inefficient. Organizations using software from DLP providers who spend too much time, effort, and budget troubleshooting, and not enough time delivering meaningful data protection, are doing themselves a disservice. New entrants touting "DLP-lite" and "next-generation DLP" as a solution to the inefficiencies of traditional DLP often gloss over the compromises inherent in "DLP-lite." With lite- or no-agent architectures and little-to-no endpoint controls, what you gain from an "easy install" and lightweight endpoint agents, you lose opening your organization to an increased risk of data leakage and loss.

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

How We're Different

Three pillars form the foundation of Fortra's more efficient, industry-leading data protection architecture.

Fast Deployment and Results

Fortra DLP lets organizations see critical results quickly thanks to a series of out-of-the-box dashboards and an integrated rapid start up. Powered by AWS, Fortra Data Loss Prevention available as a SaaS deployment can help organizations reduce overhead and cost with added simplicity and speed – as well as reduced customer burden. Get immediate visibility to DLP actions and threats to sensitive data egress without having to allocate employees to maintaining complex infrastructure.

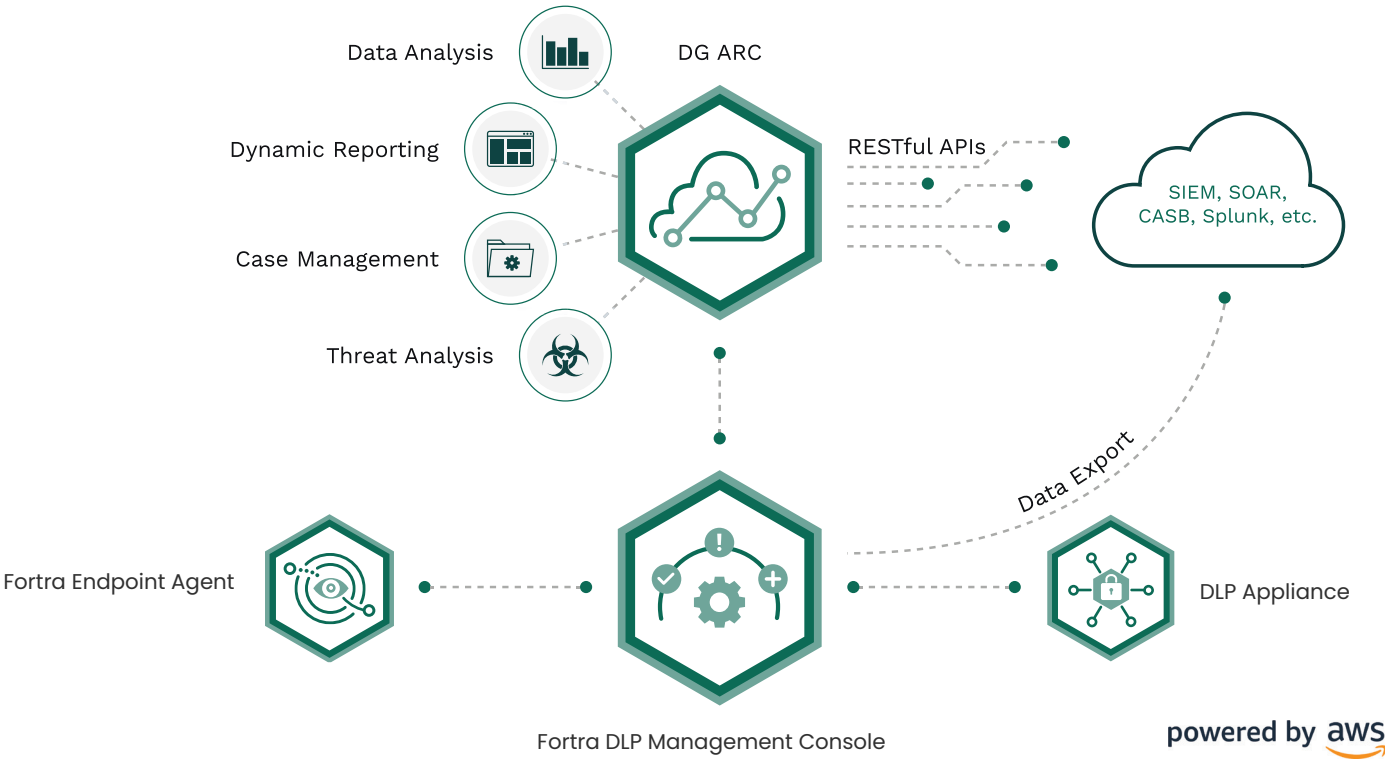
Cross Platform Coverage

Get coverage for your hybrid environment, including your corporate network, traditional endpoints, and cloud applications running on Windows, Mac, and Linux operating systems. Employing an enterprise DLP solution that supports less than complete visibility across the three most popular operating systems and how data can be manipulated across them can leave big gaps in your data protection program.

Comprehensive Controls

With Fortra DLP, organizations can choose from a wide variety of controls based on the sensitivity level of a file to secure their valuable data, including the ability to protect, monitor and outright block actions. Often, "DLP-lite" solutions will tell you that sensitive data has been compromised, but only after the data has been exfiltrated. By guiding users to the right security step, and giving soft and hard limits on allowed data actions, organizations can educate users while guarding against serious risk. Pre-built policies can also help support compliance efforts while ensuring sensitive data doesn't get out in the first place, no matter how it is modified or where it goes.

Fortra DLP



Fortra DLP is unique among DLP solutions in its ability to support both a "top-down," use case-based approach (focused on known data types or user groups) or a "bottom-up," data risk discovery approach. Our "bottom-up" approach enables you to gain visibility even before you create policies by showing you where sensitive data is located, how it flows in the organization, and where it is put at risk.

Fortra Endpoint Agent

Delivers the deepest visibility available on the market. Our agent captures and records all system, user, and data events – on or off the network.

- Noninvasive, context-aware protection
- Automatically blocks and controls only those behaviors that pose a threat
- Monitors structured and unstructured data, applications, and data movement
- Applies policies based on user role and usage rights

Analytics & Reporting Cloud

Provides fast and intuitive visibility to DLP actions, analytics, workflows, and reporting. Running on AWS, Fortra DLP's analytics and reporting cloud correlates and analyzes system, user, and data events from endpoint agents and network appliance to provide the visibility and context you need to identify and remediate insider and outsider threats.

- Behavioral-based rules and contextual intelligence deliver a complete view of risks to sensitive data, whether human or business process driven
- Visual presentation of Fortra DLP's data usage insights
- Modern, SaaS UI – click, drag, drop, pivot, filter
- Case and incident management made easy – communicate, collaborate, and aggregate
- Right-click response - real-time updates and controls

Network Appliance

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

- Web and email network DLP — single deployment or global distribution
- Discovery — locate, classify, and remediate sensitive data
- Inspection includes keywords, regular expressions, dictionaries, file metadata (type, size, name), and file category

Management Console

Enables configuring and deploying agents, managing policies, alerts, and reports.

Technology Partners and Integrations

Fortra DLP has developed custom applications and leverages APIs to integrate with the products you already own. Technology and partnership integrations include:

Greater Deployed Efficacy

Fortra's Managed Services team can help deliver instant expertise and best practices, all customized to your data protection environment. Our security experts administer, run, and oversee your data security platform, acting as an added layer of support for your existing security team. While the lack of trained cybersecurity staff can pose a challenge to adopting data protection solutions, relying on Fortra's Managed Services team gives you a way to ensure threats to your sensitive data are stopped.

Fortra DLP starts up quickly and gives organizations immediate visibility into their data security, making it easier to see and block all threats to sensitive information. Available as a SaaS or managed service deployment, Fortra DLP performs across corporate networks, endpoints, and cloud applications to stop data theft. For 20 years, we've helped data-rich enterprises protect their most sensitive data and intellectual property without slowing the pace of their business.

Managed Security Program for Endpoint DLP

Our team takes care of hosting, setup, ongoing monitoring, analyzing, tuning, and maintenance of your endpoint DLP program.

What You Get

- Fully Managed DLP Infrastructure
- Automated Data Discovery and Classification
- Full Data Visibility and Control
- Incident Escalation
- Ongoing Improvement of Your Security Posture

Managed Security Program for Detection & Response

Our team uses the latest defense strategies and intelligence to hunt, detect, and respond to attacks in real-time.

What You Get

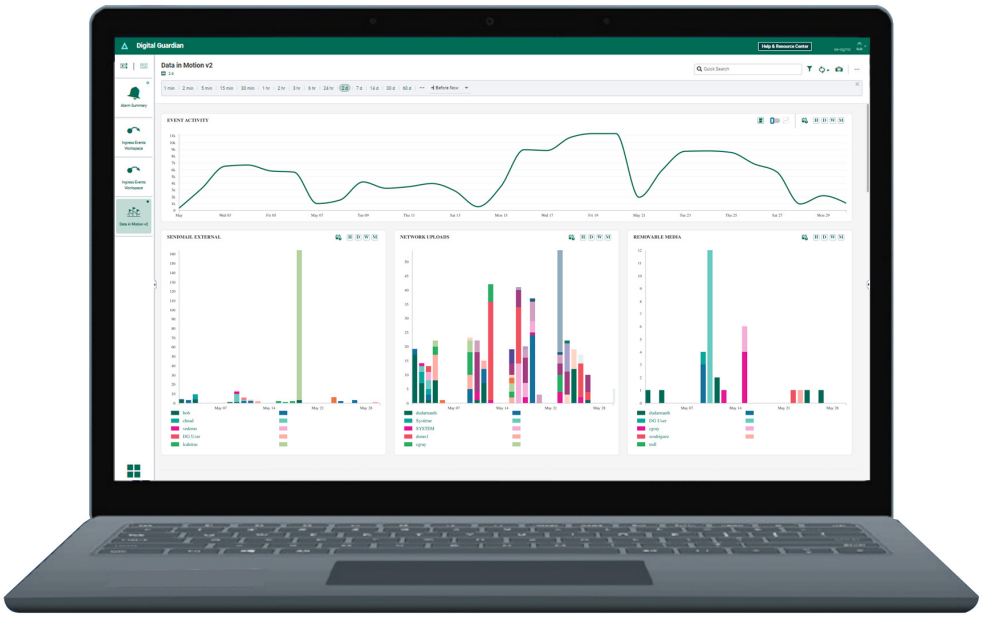
- Current State Gap Analysis
- EDR Policy Development, Maintenance & Updating
- Proven Cyber Experts with "Eyes on Glass" at Your Service
- Ongoing Threat Intelligence
- Cyber Threat Advanced Alerting and Reporting

Managed Security Program for Network DLP

Our team of experts host, administer, advise, and guide your program to discover, monitor, and protect regulated data.

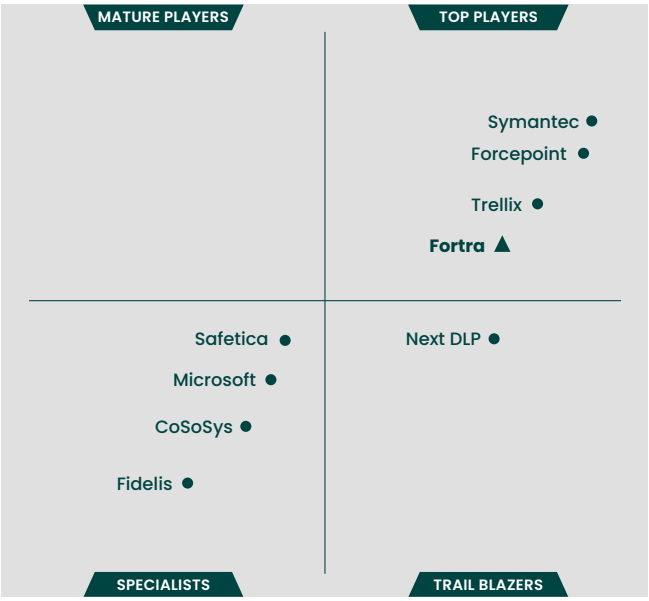
What You Get

- Active Directory and SIEM Integration
- Fully Managed Data Security Compliance Infrastructure
- Optimized PII and PHI Protection
- Alerting and Incident Escalation
- Ongoing Improvement of Security Posture



Industry-Leading DLP

Fortra DLP is regularly named a Forward Mover and Top Player in Market Quadrant for Enterprise DLP reports.



DLP Pricing & Packaging

Choose from three robust DLP packages to give you immediate data protection, adding coverage as you scale. Unlike "free" or low-cost DLP options, our pricing is simple and transparent, giving you foundational endpoint and cloud DLP capabilities with additional protection and value available at each higher tier. Enhance any package with additional features, managed services, support, and services.

FORTRA DLP PACKAGES	ESSENTIALS	ADVANCED	ELITE
ENDPOINT DLP			
Endpoint data discovery and classification	●	●	●
Endpoint agent for Windows, Mac, and Linux	●	●	●
Analytics and reporting cloud (ARC): 60-days retention and 1-year archive	●	●	●
DATA SECURITY POSTURE MANAGEMENT (DSPM)			
Applications for SaaS API security (data discovery and sharing controls)	5 included	Unlimited	●
Data detection	Standard, including keyword, regex, source code, access keys	Advanced, including EDM and OCR	●
Cloud DLP controls	Standard, including sharing controls, quarantine, data labeling, redact, mask, watermark	Advanced, including EDRM and data labeling with AIP, Fortra DCS, and Google	●
Data protection controls for email		●	●
Rest APIs for third-party integrations		●	●
Data in motion controls (shadow IT/AI, cloud tenants)			●
Data protection for unmanaged devices (agentless)			●
Adaptive risk controls (user, device, IP)			●
NETWORK DLP			
Network discovery		●	●
Web and email discovery		●	●
SUPPORT	**CORE**	**CORE**	**CORE**

AVAILABLE UPGRADES	
Product Add-Ons	• Live data retention in 30-day increments (max 120 days) • Archive data retention in 1-year increments (max 3 years) • DSPM historical data discovery service: retroactive scanning for existing data in SaaS applications • Optical character recognition (OCR)
Managed Services	Add managed services for endpoint
Service Add-Ons	• Quick Start Implementation Package* • Expert services: Core, Enhanced, Enterprise • Resident engineer support • Hourly professional services • Training: self-paced, public, or private • Upgrade your level of support **Required*
Support	• Enhanced Support • Enterprise Support