FORTRA

DATASHEET (DATA LOSS PREVENTION + DATA CLASSIFICATION)

Stronger Together: Fortra DLP & Fortra Data Classification

The combined power of Fortra DLP and Fortra Data Classification delivers more accurate, more consistent, and more comprehensive data protection capabilities without adding excessive complexity and operational overhead.

The Problem with Siloed DLP and Data Classification Solutions

Data loss prevention (DLP) and data classification are two of the most foundational tools in any data protection program, but they're commonly deployed independently of one another. That disconnect creates real-world problems for everyday users and security teams alike.

DLP solutions are designed to detect and prevent sensitive data from leaving an organization's environment. But without classification context, DLP engines are left to infer sensitivity on their own, often relying on content inspection, pattern matching, and manually configured rules to make that determination. The result is a process that's tedious to manage, prone to false positives, and inconsistent across file types and channels. A document that a user has already identified and labeled as confidential may still be treated the same as an unlabeled file, meaning the intelligence embedded in that label goes unused.

Data classification tools, meanwhile, ensure sensitive information is identified and marked at the point of creation by applying persistent metadata labels that follow files and documents across their entire lifecycle. But classification labels without downstream enforcement are only half the equation. If your organization's DLP solution can't read classification labels, they function as informational markers rather than active controls.

INTEGRATION SUMMARY

HIGHLIGHTS

Fortra DLP and Fortra DCS work together to:

- Apply and read classification labels across all supported file types
- Import label schemas directly into the Management Console
- Easily build DLP rules triggered by classification labels
- Apply persistent metadata leveraged by downstream security tools
- Extend label-driven protection beyond endpoints
- Build a connected discovery-to-enforcement pipeline

When the two tools operate in silos, the gaps compound:

In general, organizations adopt DLP solutions to detect and prevent sensitive data from leaving an organization's environment. Some DLP tools, however, lack inherent data classification capabilities, instead relying on pattern matching, keyword detection, and/or manually configured rules to determine data sensitivity. These methods are prone to false positives, can present inconsistencies across file types and channels, and — with manually configured rules — are tedious to manage. In contrast, Fortra DLP uses both content and context to determine sensitivity and then applies labels based on specific business requirements, making it an effective data protection tool even in isolation.

With that in mind, even the most comprehensive DLP solutions have classification limitations. While native capabilities are convenient, in most cases, DLP-applied classifications aren't retained outside of the inspection points (e.g., endpoints), meaning labels aren't embedded in the files themselves. Ideally, a dedicated data classification solution would negate this limitation by applying persistent labels that follow files and documents across their entire lifecycle. The catch, however, is that some of these tools follow rigid classification schemas that lack flexibility, some can't apply metadata labels that inform downstream security tools, and many cause severe user friction — all of which undercut their added benefits. Fortra Data Classification, on the other hand, delivers deeper visibility over how and where sensitive data moves, flexible schema to meet specific and complex compliance demands, and persistent metadata labels that travel with your data — all with user-friendly policy guidance that reduces user friction and human error.

In short, while comprehensive DLP and data classification tools are effective on their own, they're most beneficial when used together. But even the most robust DLP and data classification pairings can experience gaps if their integration is lackluster:

Limited file type coverage - When DLP reads classification labels using document properties alone, coverage is often restricted to a narrow set of file types, leaving other file formats unprotected regardless of their classification.

Manual configuration overhead - Without a direct integration between classification and DLP policy management, teams must manually replicate classification schemas in their DLP policies — a time-consuming process that's prone to inconsistencies and policy drift as schemas change.

Inconsistent enforcement - DLP policies that operate independently of classification labels are limited to protecting data on the endpoints and channels where those policies are deployed. Similar to using a DLP tool's native classification capabilities instead of a dedicated classification tool, when sensitive files travel beyond those boundaries, the protection stops.

Our Solution

Fortra DLP and Fortra Data Classification are built to close these gaps — natively, cleanly, and without the manual overhead that comes with stitching together disconnected tools.

Deeper Integration & Broader Coverage

Fortra DLP's ability to read Fortra Data Classification labels natively via the Data Classification SDK provides customers with a meaningful step forward from reading labels through document properties alone.

DLP tools that read classification labels exclusively through document properties generally require additional XML configuration in DLP rules, and those labels can only be read from specific file types. With an SDK-based integration, DLP can now read classification labels from any file type that Fortra Data Classification supports, significantly expanding the scope of label-driven enforcement across an organization's environment. Furthermore, those leveraging Fortra DLP's Control Policy Manager can easily build DLP rules triggered by those same labels.

Additionally, Fortra DLP users can also import a Data Classification label schema directly into the DLP Management Console. Rather than manually recreating classification levels and categories as DLP policy conditions, administrators can import the schema in one step and ensure that DLP policies stay in sync with the organization's classification framework.

A Comprehensive Data Protection Program

Fortra DLP and Fortra Data Classification are designed to benefit organizations regardless of where they are in their data protection journey.

For existing Fortra Data Classification customers, adding Fortra DLP means that the classification labels already applied across your environment can now actively drive enforcement, leveraging metadata to prevent sensitive files from leaving your endpoints. Classification becomes the engine behind a more accurate, label-aware DLP program as opposed to merely a visibility and governance tool.

For existing Fortra DLP customers, adding Fortra Data Classification means your DLP policies gain immediate context. Data Classification converts sensitive content into labeled, metadata-tagged files that DLP can act on with greater precision, meaning you'll experience fewer false positives, simplify policy management, and extend protection beyond your endpoints.

These capabilities and their benefits also extend naturally to Fortra DSPM. DSPM can discover sensitive data across cloud and hybrid environments, and with Fortra Data Classification, it can automatically apply sensitivity labels upon discovery. Our endpoint DLP (eDLP) solution can then use those labels to enforce data-in-motion policies, helping to prevent classified data from leaving endpoints as a result of your security solutions working in silos.

Better Data Protection Starts with Better Integration

Whether you're looking to strengthen an existing DLP program, put your Data Classification labels to work, or build a comprehensive data protection program from the ground up, Fortra's integrated solutions give you the coverage, consistency, and control you need. Talk to a Fortra expert today.

CONTACT US

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.