

FORTRA

SOLUTION BRIEF (Cybersecurity)

Combining Data Classification & Data Loss Prevention (DLP)

The Problem: Identifying the Data You are Trying to Protect

The need to keep sensitive data secure remains top of mind for organizations, however, risks associated with that data have grown increasingly in recent years. Many organizations struggle to keep up and create a security ecosystem that will protect their sensitive data and meet organizational needs. At the center of this problem is data security solutions that do not understand the data they protect – where it lives, how it is shared, and who is sharing it, what data truly is considered sensitive – and are therefore unable to work with the rest of a security ecosystem.

When software solutions do not understand the data they work with, current work processes become limited or stalled. In these cases, the risk of solutions being turned off, dialed down, or worked around creates expensive and unused organizational burdens, increasing the risk of sensitive data leakage. Ultimately, security solutions that don't understand the data they handle will fail to protect sensitive data.

The Solution: Get a Clear Picture of Your Data, Then Protect it Better

Organizations require solutions that tie seamlessly into the rest of their security ecosystem and understand both the data and the context of that data to be able to fully protect it. These solutions must work functionally and intelligently with existing work processes to be an added benefit to an organization and truly protect sensitive data.

The Fortra Solution

Together, Data Classification and Data Loss Prevention provide critical data protection that both understands the data you have and secures it as it is shared. Utilizing these two solutions within a security ecosystem allows organizations to:

Improve visibility for sensitive data:

With the use of data discovery methodologies, multiple utilizing machine learning, organizations can identify the data they possess on a deeper contextual level and pass on that information, or metadata, thorough a more interconnected security ecosystem. Because Fortra Data Loss Prevention and Classification solutions truly understand the data organizations are working with and can communicate that to the rest of a security ecosystem within an organization, data remains secure and compliant while providing visibility of policy violations.

Keep sensitive data private & secure:

With integrated Classification and Data Loss Prevention solutions, Fortra identifies sensitive data and uses easy-to-configure, but incredibly flexible policy to ensure it remains private and secure. Organizations can feel safe knowing that their data is correctly identified, no matter the infrastructure or point in the lifecycle of the data. In addition, an array of powerful hygiene controls protects the organization's sensitive data from external spyware and ransomware threats, without impacting day to day business processes.

Strengthen your data security ecosystem:

Fortra understands that most organizations have already begun their data security journeys. We are here to work alongside the parts of the security ecosystem organizations already possess, while utilizing methodologies and policies to ensure that an organization's current pieces of a solution perform to a higher standard, creating a more functional and robust ecosystem. Fortra Classification and Data Loss Prevention are the tools that augment organizations' security ecosystems intelligently and frictionlessly.

Titus

Data Classification

Titus, by Fortra, provides best-in-class data classification technology allowing you to identify and protect your sensitive data to clearly inform both your people and your policies on what information should be secured and how to handle it.

Key features:

- Leverages multiple data detection methodologies, including machine learning to best understand data.
- Provides the industry's most flexible and customizable classification metadata schema.
- Creates metadata that enables DLP and other solutions to make informed decisions around how to handle data, leading to a more efficient data security ecosystem.

Clearswift

Email Security

Clearswift, by Fortra, offers award-winning adaptive data loss prevention technology which prevents incoming cyber threats such as ransomware and minimizes the risk of sensitive data leaving the organization over email, web or cloud.

Key features:

- Rules, such as redact, sanitize, delete, encrypt, block, or monitor, are applied based on content and context provided by Data Classification.
- Automatic detection and removal of sensitive and hidden data, and active security threats as data enters an organization.
- Avoid unnecessary disruption and lower IT overhead costs by working jointly with Data Classification and other security solutions.

Let Us Help You Protect Your Data

Ready to add layers of protection to your data security defense?

Contact us at [Fortra.com](https://fortra.com) to schedule a consultation or talk to a solutions expert.

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.