



SOLUTION BRIEF (Data Classification)

Fortra's Data Classification Suite (DCS) for Windows

With the volume and speed of data being created and shared at an all-time high, your organization's sensitive information is likely in a myriad of locations including emails, presentations, spreadsheets, documents, PDFs, videos, and images. Should that data be exposed, it could have serious repercussions for your organization, such as reputation damage, loss of government contracts, regulatory fines, and the unauthorized disclosure of intellectual property.

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
- 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

What is Fortra's Data Classification Suite?

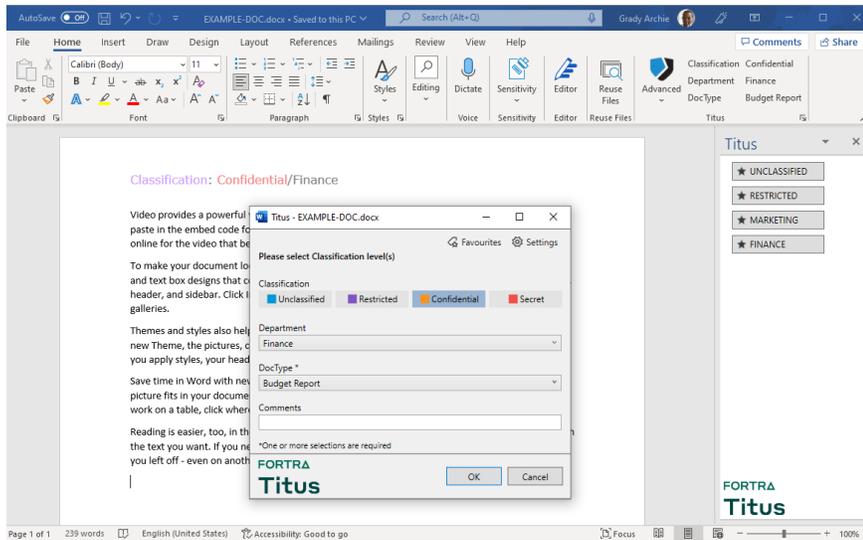
Fortra's Data Classification Suite (DCS) is an all-in-one data classification solution for Outlook, Office, and Windows desktop that informs both your people and your policies about what data should be secured and how it should be handled. You can find in-depth information for each solution included in TCS below:

- [DCS for Microsoft Outlook Datasheet](#)
- [DCS for Microsoft Office Datasheet](#)
- [DCS for Desktop Datasheet](#)

Secure Sensitive Data with DCS for Windows

By enabling users to classify emails, documents, and files, organizations can add structure and context to the vast amount of data created every day. This helps to prevent inadvertent disclosure of sensitive data, meet compliance requirements, and enhance infrastructure solutions such as archiving, [Data Loss Prevention \(DLP\)](#), [Secure Collaboration](#), and encryption. DCS for Windows unique and comprehensive data classification solution features include:

- Custom visual markings to inform users about the sensitivity of your business content
- Custom metadata, including document properties and email X-headers, to help drive other data security solutions
- Enhanced data security user awareness by enabling your users to classify emails and documents quickly and easily within the Microsoft application they are using
- Multiple layers and types of classification, such as single select, multi-select, and date controls, to provide a deeper level of granularity and security for your business content
- A fully customizable solution to meet the exact needs of your organization's data security policies
- High-end integrations with data protection solutions, including DLP and Secure Collaboration, providing end-to-end security
- The option for both fully automated and manual classification, and an approach in between, to meet your business needs as required



Apply advanced classification settings in Microsoft Office, Outlook, and Windows/File Explorer

Highlights

DCS for Windows enables organizations to ensure consistent and proper handling of sensitive data in Outlook, Office, and Microsoft Windows Explorer. The solution helps organizations:

- Classify files, documents, and emails
- Leverage metadata to enhance downstream security solutions
- Promote user awareness and accountability
- Identify information sensitivity
- Comply with regulations and policies

TCS v.2022.0 Features and Updates

DCS for Windows enables organizations to ensure consistent and proper handling of sensitive data in Outlook, Office, and Microsoft Windows Explorer. The solution helps organizations:

- Fully functioning integration between DCS and Microsoft Purview Information Protection (MIP) Sensitivity Labels. You can now map MIP Sensitivity Label values to DCS fields and values, so DCS users can process emails and documents from MIP users. When creating documents or sending emails, DCS will generate the equivalent MIP value, allowing MIP ecosystem functionality to operate.
- Our latest administration product, Policy Manager, is a web-based SaaS solution with a modern administrative interface used to configure DCS for Windows client.
- Improved autosave feature audits only when the user manually saves, vastly reducing the number of events in the event log.
- New custom interface branding. You can now replace the default Fortra logo with your organization's logo of choice.

Key Features and Benefits

KEY FEATURE	BENEFIT
Visual identification and markings	Visually identifies file sensitivity in Windows Explorer via a classification menu and customizable classification icons. In Microsoft Outlook, visual markings are applied in the email subject line and message body, and in Microsoft Office, visual markings are applied in the form of headers, footers, and watermarks to clearly identify information sensitivity.
Persistent metadata	Stores user classification selections with the email or document as per-sistent metadata that is maintained, even when transferring the file through email or to portable media such as USB drives. Classification metadata is also used to increase the accuracy and effectiveness of DLP, archiving, and perimeter security solutions.
Classify any file, email, or document	Enables users to classify and protect sensitive information and intellectual property contained in any file, including PDFs, videos, images, ZIP files, emails, calendar events, and design documents.
Classification selector	Provides simple, non-intrusive ways for users to identify the sensitivity of emails and documents with classification labels including: One Click Classification, classification via prompts, system-suggested, and automatic classification based on recipient, content, and other email attributes.
Ease of administration	Provides a centralized, web-based Administration Console for classification configuration and policy management across the Titus Classification Suite of products. Titus generates user activity logs that can be monitored and analyzed to measure the effectiveness of the security policies and detect anomalous usage.
Policy enforcement	Enforces policy in Office by comparing multiple properties about the information, author, document, and the action being performed. In Outlook, inspects emails for policy violations before the message leaves the desktop, providing instant feedback so that the sender can correct any problems.
Right-click classify	Provides a simple right-click classification menu that guides users when classifying single or multiple files in Windows ¹ .
Multi-platform support	Supports Outlook for both Windows and Mac, as well as Outlook Online ensuring the broadest possible coverage across the organization to mitigate risk of data loss.
Security enablement	Adds an extra layer of security by automatically applying Vera based on classification.

¹Available for Windows Desktop only



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.