FORTRA™

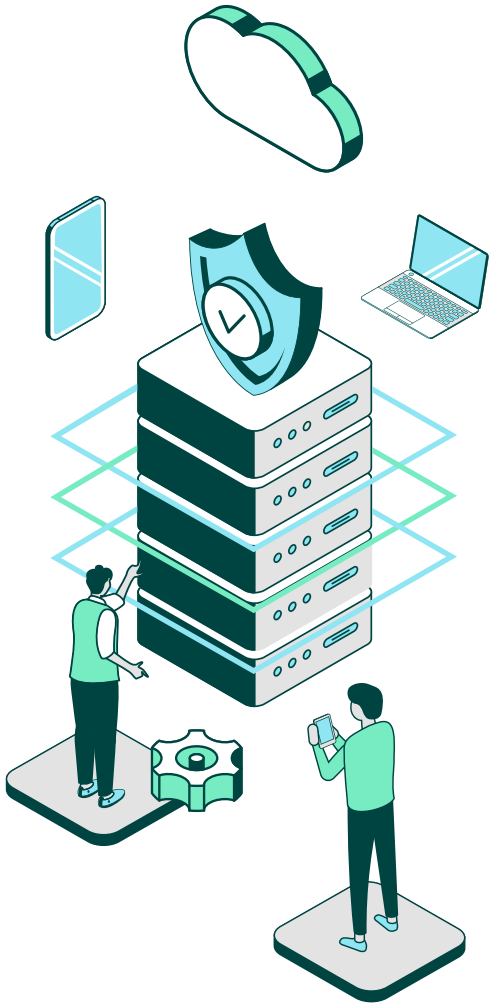
SOLUTION BRIEF *(Cybersecurity)*

Data Classification and Digital Guardian Secure Collaboration

Secure Sensitive Data Wherever it Goes

Employees send emails, create documents, and upload files to internal servers and cloud applications every day, and the volume of data is growing exponentially. How can you ensure that sensitive data remains secure without burdening your end users with time-consuming and confusing workflows?

Digital Guardian Secure Collaboration and Fortra's Data Classification Suite (DCS) integrate to provide an end-to-end solution to help organizations find, categorize, secure, and track the data they have. DCS combined with zero trust secure collaboration enables employees to work and collaborate more freely, both internally and externally, without having to worry about understanding what is or is not confidential and what needs to be encrypted.



The Challenges

In today's distributed enterprise, data is everywhere: in on-prem share drives, in the cloud, on desktop devices, and on employees' mobile devices. So, understanding what data you have, and where it's located, has never been more difficult—or more important. This becomes even more critical if that data is sensitive.

But how do you define what data is sensitive and what isn't? Almost anyone knows that personal information such as social security numbers, addresses, phone numbers, insurance numbers, personal health data, or bank account numbers is confidential. However, when it comes to company-specific information like business plans, product roadmaps, design files, product documentation, and intellectual property, it is not always as straightforward.

Collaboration outside your organization is a requirement of nearly every job role, and that means sharing sensitive data. Fortra helps protect all employees with secure collaboration tools.

IN TODAY'S TECH-DRIVEN WORLD, YOUR DATA IS EVERYWHERE.
Understanding what data you have and where it's located has never been more difficult—or more important. This becomes even more critical if that data is sensitive.

It's this type of information that typically presents the greatest challenge for organizations to deal with. Categorizing and protecting this data proactively, consistently, and accurately compounds this challenge, as failure to do so represents a real security risk. Likewise, context is crucial for accurate data classification and in the end, the most effective way to keep information protected is to employ a strategy based on a combination of people, process, and technology.

Data Classification: The Foundation of Effective Data Protection

Data classification is an integral part of the Information Lifecycle Management (ILM) process—so much so that data classification is really considered the foundation of any data security solution, both within the corporate firewall and in the cloud. You can't protect your data when you don't know enough about the contents of files to handle them properly. Once a user has created a file or an email, a classification solution scans the file to accurately identify the sensitivity of the data and apply visual labels and metadata that can be read by the entire security ecosystem. Then a policy engine determines what actions to take. The classification process can be guided (asking the user to confirm the recommended classification level), automated (applying the classification level automatically, without user input), or simply done manually.

Not only does data classification provide organizations with the ability to make more intelligent and conscious decisions about how data is used and handled, but in an age of growing regulatory compliance requirements, it is a critical tool in demonstrating compliance and remaining compliant.

Secure Collaboration: Control Over Your Most Sensitive Data

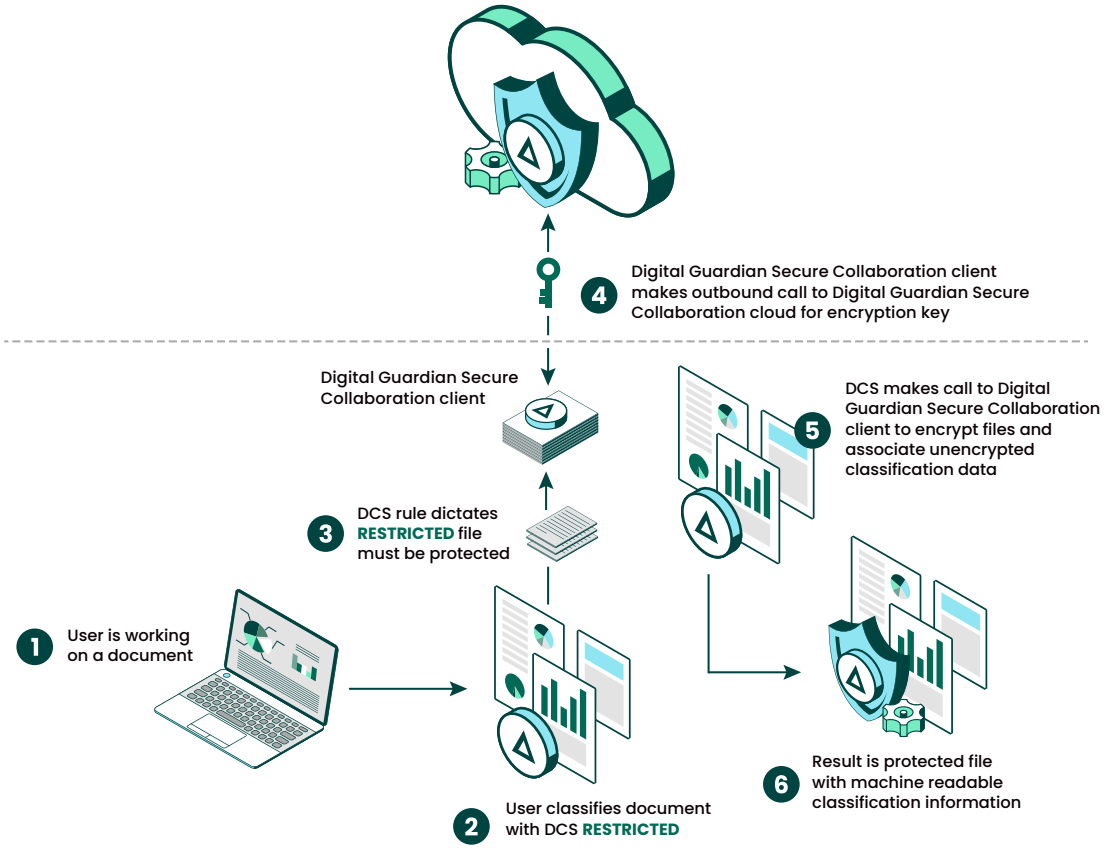
Secure collaboration solutions enable organizations of all sizes to protect their sensitive data by encrypting the file and then providing the ability to track, audit, and manage the policies securing the data anywhere it goes. So confidential data stays protected, no matter what device, person, cloud, or application it travels to.

Most importantly, a secure collaboration solution will ensure that your sensitive data is protected even when it travels outside of your organization. This is a must for industries or job functions (such as finance or legal) that frequently require external collaboration with information that would be most detrimental to the organization if a breach were to occur. Should our data fall into the wrong hands either accidentally or maliciously, secure collaboration will allow you to revoke access to the file in real-time.

In today's hyper-competitive business climate, the ability to maintain control of your data, manage who can access and modify your sensitive files, and track your intellectual property is critical. Fortra's solution provides the peace of mind that your security policies will stick with your most important data.

Digital Guardian Secure Collaboration and DCS integrate to provide an end-to-end solution to help organizations find, identify, categorize, analyze, secure, and track the data they have.

DCS Data Classification + Digital Guardian Secure Collaboration



How it Works

An organization might have a policy that mandates that any files determined by Digital Guardian Secure Collaboration to be **classified** or **sensitive** must be secured by Digital Guardian Secure Collaboration before they can be shared over email or via cloud.

In this scenario, once DCS tags a file with a "**Restricted**" classification, it then leverages secure collaboration to encrypt the file. Fortra encrypts the file, adding the access controls and any other specific policies that are tied to that "Restricted" classification. DCS also embeds unencrypted classification metadata in the header of the secured file, resulting in a protected file with machine readable classification information.

The file is now encrypted, but other security products such as a data loss protection software (DLP) or a cloud access security broker (CASB) are still able to read the metadata that contains the classification value.

Benefits

Digital Guardian Secure Collaboration and DCS together employ a powerful combination of best-of-breed classification and file-level security. This helps organizations to better understand and categorize the data they have, as well as secure that data wherever it travels. Both technologies also complement other security solutions used to protect data at rest and the flow of data, such as CASB and DLP. And since both solutions are a part of the Fortra Data Security Suite, you gain the advantage of working with a single vendor for all your data-centric security needs. All of this serves to dramatically improve an organization's overall security posture to protect against data breaches and having sensitive data fall into the wrong hands.

About DCS

DCS data classification enables organizations to truly understand what kind of data they possess, the value of that data, and how best to classify files in order to mitigate exposure to risk. With DCS, you can clearly and accurately classify emails, spreadsheets, presentations, and other file types using user selected, system-suggested, or automatically applied classification settings that are based on your unique data security policies. It is designed to empower employees to work confidently and productively, with the knowledge that their emails, documents, and sensitive information are all protected.

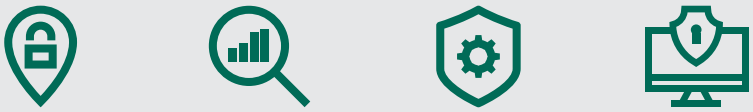
About Digital Guardian Secure Collaboration

Digital Guardian Secure Collaboration is a data and content security solution that enhances an organization's ability to protect, govern and manage the transmission of information without impacting employees, or the existing security choices the organization has made. Files secured can still be protected by gateways, firewalls, and endpoint technologies, but customers choosing secure collaboration can now extend these controls beyond the boundaries of their business.

With a centralized cloud architecture that is content and storage agnostic, policy-driven, and designed to adapt to modern work practices, Fortra allows customers to provide consistent, auditable protection across all of their critical content. Digital Guardian Secure Collaboration enables organizations of all sizes, in any industry to maintain existing investments in storage, collaboration, and communication while improving their security profiles.

DCS + SECURE COLLABORATION INTEGRATION

A POWERFUL COMBINATION of enterprise-grade classification and file-level security to dramatically improve an organization's overall security posture to protect against data breaches.



Want to learn more, or get a demo?
Get in touch with our team of experts **https://www.titus.com/request-demo**.

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.