FORTRA™

SOLUTION BRIEF (Fortra)

Fortra Data Classification Suite (DCS)

HIGHLIGHTS

Fortra's Data Identification is an unobtrusive data protection solution that helps any organization mitigate risk and comply with multiple data regulations. This SaaS solution combines the DCS's Data Detection Engine (DDE) Engine and pre-configured cloud-based libraries of sensitive data terminology to evaluate data in context and accurately identify sensitive data within emails.

The Problem

Compliance regulations related to data are growing in number and complexity while IT and security solutions struggle to address these challenges, thus leaving major gaps. Due to these data regulations, organizations are required not only to understand the context and the value of the vast amounts of data that flow through email, but also protect and report on that data.

Accidental exposure of sensitive information could greatly and negatively impact the organization due to reputational, financial and legal exposures. Additionally, any proprietary information that is released could prove costly to an organization's long-term sustainability and strategy.

Most organizations are unable to pinpoint what data is sensitive, and the value of that data as it moves through the organization and beyond. The ability to identify sensitive data in motion through email will help minimize risk and provide a clear picture to leaders of the organization on how to create processes, reporting, and reduce compliance and risk exposure moving forward.

Other data detection solutions can fall short because they lack multiple methods of data detection, ultimately reducing the efficiency and value of an organization's security ecosystem. In addition, most solutions fail to offer a seamless user experience, both for the software administrators and endusers. On-premises solutions that require administrators to build policies can sometimes create burdens on the organization as well. This friction creates additional barriers to adoption and strong data protection.

The Solution

A data protection solution can help both administrators and end-users understand what qualifies as protected data – from customers' PII to their own IP – by accurately identifying sensitive data within emails.

This solution removes the burden on both administrators and end-users who currently struggle to understand what qualifies as sensitive data within an organization. The solution would leverage metadata to enable an interconnected and more robust security ecosystem, and should employ data detection methodologies, such as machine learning, that consider the context around the data. Ultimately, this creates the best understanding of the data at hand and therefore, what to do with it. All of this should be achieved with minimal friction by deploying pre-configured, cloud-based libraries of sensitive data terminology to reduce onboarding for the admin and increase automation for end-users.

How Fortra Can Help

Titus Data Identification is an unobtrusive data protection solution that combines the Fortra DDE and pre-configured cloud-based libraries of sensitive terminologies to evaluate data in context and accurately identify sensitive data within emails. Titus Data Identification provides many advantages to your organization's privacy program:

- **Keep Sensitive Data Private & Secure:** Fortra's Data Identification uses the Fortra's DDE to identify sensitive data. The solution applies rich, persistent metadata to emails, enabling organizations to take actions. The results include enhanced data security by identifying and truly understanding sensitive data and the context of that data within an organization.

- **Strengthen Your Data Security Ecosystem:** Organizations can use the rich, persistent metadata ortra's Data Identification applies to improve their overall data protection ecosystem, letting solutions such as DLPs make informed decisions about how to handle sensitive data.

- **Fast SaaS Delivery:** As a cloud-based solution leveraging machine learning to automate security, Fortra's Data Identification is unobtrusive to end-users and administrators. Undetected by end-users, this SaaS solution simplifies deployment, and Fortra's pre-configured cloud-based libraries of sensitive terminology allow organizations to be up and running faster.

- **Mitigate data risk:** Fortra Data Identification provides accurate understanding of sensitive data within email, from customer PII to organizational IP. This sensitive data can then be handled accordingly, with appropriate actions taken by the rest of an organizations data security ecosystem to mitigate risk.

Organizations require a solution that identifies their most sensitive data without disrupting how end-users do their jobs. In order to avoid increased complexity for administrators, the solution must integrate seamlessly with the rest of the security ecosystem and strengthen it by providing context and understanding of the sensitive data these organizations possess to mitigate risk. Fortra's Data Identification is a SaaS service that includes a robust data detection engine, keeps organizational data private and secure, and ensures both minimal implementation time and short time-to-value compared to other solutions available today.

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.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.