

Go Beyond Compliance to Reduce Cyber Risk and Insider Threat

BETHESDA, MD, UNITED STATES, December 10, 2020 /EINPresswire.com/ -- Data breaches make headlines every day and companies across the globe struggle to meet changing privacy regulations, such as the California Consumer Privacy Act (CCPA), the upcoming California Privacy Rights Act (CPRA) and of course, the General Data Protection Regulation (GDPR). Data security is very high on the list of corporate priorities with most concentrating on protecting databases containing personally identifiable information (PII). Sensitive information subject to privacy or industry regulations are not found or stored solely in structured databases, but in unstructured files like Microsoft Office documents, PDFs, images, and computer aided design (CAD) drawings. Companies create far more unstructured data and the same security controls used to protect structured databases are ineffective. This data contains not only PII, but Intellectual Property (IP) that in the wrong hands, could cost a business its reputation, competitive advantage, lead to financial losses, and even [litigation](#). Most organizations do not focus on this constantly growing invisible and largely unprotected area.

Trusted insiders have overtaken cyber-attacks as the greatest threat to business. You trust the people you hire to do their job, but mistakes happen. The trust model is no longer sufficient to protect sensitive data especially with the increase in working from home becoming more common. How do you fix this? By taking the guesswork out of the equation and automatically encrypting files containing sensitive data. Doing so ensures that even if a file is accidentally sent to the wrong person, it is protected.

A recent report by the Aite Group, Sensitive Data Everywhere: Find It, Classify It, Manage It, and Protect It, discusses how quickly and easily unstructured data in files grows, and why it's so important to include it as part of a data governance strategy. The report includes a case study of a global financial services organization that recognized the liability of not understanding and protecting its unstructured data inventory. The Impact Brief also provides guidance and recommendations based on the author's findings after interviews with ten (10) technology providers of data discovery, classification and protection solutions.

To read the entire report, click [here](#).

DEBORAH KISH
Fasoo Inc
+1 203-913-2484
deborahkish@fasoo.com

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/532425653>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2020 IPD Group, Inc. All Right Reserved.