titus
by HelpSystems

CASE STUDY *(Data Classification)*

Large Canadian Financial Institution

Enhances Data Protection Strategy with McAfee and Titus

When sensitive information gets into the wrong hands, the costs can be severe: fines, lawsuits, embarrassing headlines, loss of intellectual property, even risk to public safety. Using techniques such as data classification and content validation, Titus Classification Suite enforces policy and mitigates data loss - raising user awareness and preventing data breaches at the source.

Business Situation

One of the largest Canadian financial institutions was looking for a proven solution to enhance their data security best practices – specifically around the storing, handling, and sharing of sensitive information. They also had a specific requirement to improve employee awareness specific to data confidentiality and security. They were looking for a comprehensive solution that would more effectively safeguard data, and enable end users to easily identify and classify the sensitivity of emails and documents as they were being created and/or retrieved from corporate file-shares.

Enhancing DLP with Classification

After extensive research, this institution determined that the integrated information classification and data loss prevention solutions from Titus and McAfee would help them effectively protect and confidently share their most sensitive information. This large financial institution selected Titus Classification Suite to help their employees accurately and effectively identify and handle emails and documents. By implementing Titus Classification solutions at the desktop, they were able to address compliance requirements by raising user awareness and accountability as part of their usual workflow. Titus Classification solutions work in conjunction with a number of McAfee products, including McAfee DLP, McAfee Enterprise Security Manager, McAfee Email Gateway, and McAfee ePolicy Orchestrator.

Titus Classification

Titus Classification enables organizations to ensure consistent and proper handling of Microsoft Outlook email and Microsoft Office documents. Titus Message Classification ensures that every email is accurately classified when created, while Titus Classification for Microsoft Office prompts users to identify the sensitivity of every Word, Excel and PowerPoint document. Both solutions warn users of specific policy violations. User classifications are stored with the email or Office document as persistent metadata which can be used to increase the accuracy and effectiveness of McAfee DLP policies inside and outside the desktop and network boundaries.

> ***"Using Titus Classification in conjunction with McAfee DLP allows us to involve our end users and their knowledge of the information they create and handle in order to optimize data security management policies. We are striving to improve our data loss prevention practices while enhancing secure information sharing."***
>
> CISO
> Large Canadian Financial Institution

"Titus has been and continues to be an extremely valuable partner for McAfee. Our joint customers have come to rely on McAfee and Titus to provide them with greater control over managing the movement of their sensitive information. Together, Titus and McAfee have enjoyed great mutual success in developing new enterprise customers and helping them to effectively protect their most sensitive information."

Ed Barry
Vice President of Global Technology Alliances at McAfee

Titus and McAfee – Better Together

McAfee DLP can effectively identify most structured data, such as PII or PCI data (ie. social security numbers and credit card numbers), as well as specific regular expressions and keywords. Some sensitive content however is much more difficult to identify as it may not contain known words, patterns or the end users' context. The integration between Titus Classification and McAfee DLP reduces an organization's risk of data loss by capturing the data owner's intrinsic knowledge about the context and sensitivity of their documents and making that explicit information available to both users (visual classification labels) and to the McAfee host and network-based DLP in the form of corresponding metadata.

Additionally, using Titus Classification with McAfee Enterprise Security Manager provides real-time contextual analytics on potential suspicious activities occurring on the desktop and network. For example, network administrators are notified when multiple document classifications are downgraded or attempts are made to send these or other sensitive emails or documents to an external email address, different file-share, removable device, or unauthorized recipient.

About Titus

Titus solutions enable organizations to classify, protect and confidently share information, and meet regulatory compliance requirements by identifying and securing unstructured data. Titus products enhance data loss prevention by involving end users in classifying and protecting sensitive information in emails, documents and other file types – on the desktop, on mobile devices, and in SharePoint. Titus solutions are trusted by over 2 million users in 60 countries around the world. Our customers include Dell, Nokia, Dow Corning, Safran Morpho, United States Air Force, NATO, Pratt and Whitney, Canadian Department of National Defence, Australian Department of Defence, and the U.S. Department of Veterans Affairs.

titus
by HelpSystems
www.titus.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.