

Identify Sensitive Data and Prevent Data Leaks

User-driven security to enhance McAfee® data loss prevention

The interoperability between TITUS Document Classification software and McAfee Data Loss Prevention (DLP) further reduces your risk of data loss by capturing end users' inherent knowledge about the sensitivity of documents and making that information available to McAfee host and network-based DLP as visual classification labels and corresponding metadata. By empowering users to classify information sensitivity, you don't have to rely solely on automated content scanning to determine what is sensitive. The originator, who knows the content best, can proactively indicate that the information is sensitive, enabling more intelligent and accurate DLP decisions.

McAfee Compatible Solution

TITUS Document Classification v3.3 and McAfee Data Loss Prevention 9.

Benefits

- Identify sensitive data
- Lower false positives
- Increase user awareness
- Apply classification schema
- Improve policy enforcement
- Improve productivity and search

One of the biggest challenges for IT security departments is how to take the guesswork out of identifying sensitive data. Organizations like yours generate various types of sensitive data. Regulated data includes traditional personally identifiable information (PII) and Payment Card Industry (PCI) data, such as Social Security numbers and credit card numbers, which are subject to regulation. McAfee Data Loss Prevention can readily identify this content through regular expressions and keywords. Other sensitive content, however, is more difficult to identify, as it may not contain known words, patterns, or the end users' context. This high business-impact information is inherently more difficult for DLP solutions to identify. By combining TITUS Classification with McAfee Data Loss Prevention, you can create rules and controls around regulated or sensitive data that are contextually important and help you make informed decisions to prevent data loss.

Classification Enables Controls

Important considerations in securing information are an understanding of what information is truly sensitive, who that information can be shared with, and how to safely handle it.

Individuals who create content generally have a good understanding of how their information should be handled. TITUS Classification solutions assist users with applying visual classification labels quickly and consistently which can prevent mishandling. These tools also provide guidance to for users who are unsure of policy and allow them to apply machine-readable metadata containing information regarding data sensitivity. Once applied, this classification metadata is a powerful asset, as it remains with the content and can be used to enforce security controls.

Consistent TITUS data classification metadata allows McAfee Data Loss Prevention to be even more effective, as it provides a source context for data that might otherwise not be structured. Once the McAfee Data Loss Prevention reads the TITUS classification metadata, additional policies can be enforced to block or allow sensitive information accordingly.

McAfee Data Loss Prevention Interoperates with TITUS Document Classification

Whether it is data in motion, data in use, or data at rest, no DLP solution can always identify the sensitive information created by your end users. Consider abbreviations, euphemisms, typos, and abstract concepts: how can you accurately identify and prevent the inappropriate movement of this type of sensitive data?

“The TITUS Document Classification solution complements McAfee Data Loss Prevention, and the joint solution provides our mutual customers greater control over managing the movement of their sensitive documents.”

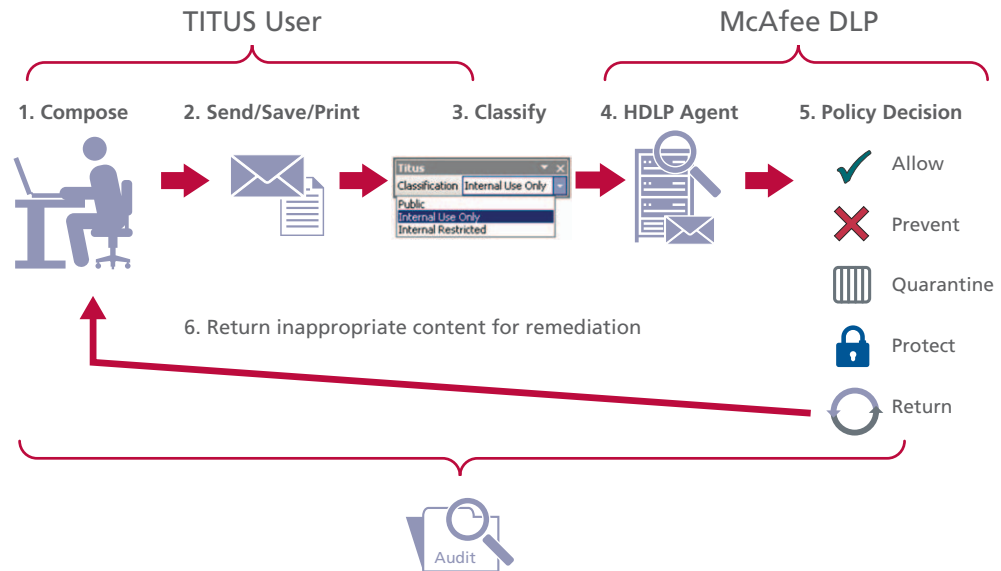
—Ed Barry, Vice President of McAfee Security Innovation Alliance.

TITUS Classification solutions are effective, easy to use, and easy to deploy enterprise-wide. Users are prompted to identify the sensitivity of data within their familiar Microsoft Office and Outlook environment. Once users identify the sensitive data with a classification label, TITUS will apply that label visually to the document with a header, footer, and watermark so others in the organization can clearly see the information is sensitive. Additionally, TITUS will embed metadata that McAfee Data Loss Prevention can read to help make informed policy decisions, such as whether to encrypt the content, or to keep it internal to the organization.

The joint McAfee/TITUS solution increases user awareness and responsibility by encouraging users to review what they are about to send and by helping them prevent transgressions of company policies. Applying specific labels takes the guesswork out of identifying sensitive data and ensures that it is shared securely. For example, if a document has a TITUS Classification label that reads “Internal Only”, McAfee Data Loss Prevention can block copying it to a removable USB memory device, thus ensuring better control of information assets.

“Working with McAfee will allow us to provide customers with a complete approach to DLP at all stages of the information lifecycle.”

—Tim Upton, President and CEO of TITUS.



About TITUS Classification Software

TITUS is a leading provider of security and compliance software that helps organizations share information securely while meeting policy and compliance requirements. Our solutions enable military, government, and large enterprises to raise awareness and meet regulatory compliance by visually alerting end users to the sensitivity of information.

TITUS Classification solutions include leading message, document and file classification, and labelling software. TITUS Document Classification interoperates with McAfee Host Data Loss Prevention, enabling customers to add user-driven classification to further protect sensitive and confidential information right at the desktop.

About McAfee Data Loss Prevention

McAfee Data Loss Prevention delivers the highest levels of protection for sensitive data, while greatly reducing the cost and complexity of safeguarding business-critical information. McAfee data protection is delivered through our low-maintenance appliance and the McAfee ePolicy Orchestrator® platform, for streamlined deployment, management, updates, and reports.

