Solution Brief

Identify and Make Informed Security Decisions about Sensitive Data

Automated and user-driven classification enhances Intel Security's open and connected security ecosystem

The integration of TITUS Classification solutions with McAfee® Data Loss Prevention (McAfee DLP) greatly reduces the risk of data loss by capturing users' inherent knowledge about the sensitivity of information that they create, store, and share. These solutions work together to make that information available to Intel Security host- and network-based data loss prevention (DLP) and enable the DLP solutions to take action based on user classification labels and embedded metadata. Users are empowered to classify information, so organizations don't have to rely solely on automated content scanning to determine what is sensitive.

McAfee Data Exchange Layer unites the combined activities of both TITUS Classification and McAfee DLP. Event logs are transmitted to the McAfee Enterprise Security Manager to enable instant communication and collaboration for real-time situational analysis and to trigger corresponding actions if required

How does IT take the guesswork out of identifying sensitive data? Organizations generate a wide variety of information, including personally identifiable information (PII), Payment Card Industry (PCI) data, Social Security numbers, and credit card information, which are often subject to industry-specific regulations. McAfee DLP can easily identify this content through regular expressions and keywords. Other sensitive content, however, can be more difficult to identify, as it may contain many common words, vague patterns, or users' input or context. By starting with classification as the foundation of your data governance strategy and combining TITUS Classification with McAfee DLP, you can create rules and controls around regulated or sensitive data that may not otherwise be tagged as sensitive and is contextually important for your business. This capability helps you make even more informed decisions in your efforts to prevent data loss.

TITUS

McAfee COMPATIBLE

McAfee Compatible Solution

- TITUS Classification Suite 4.4
- McAfee DLP v9.3
- McAfee Data Exchange Layer 1.0
- McAfee Enterprise Security Manager v9.2
- McAfee® ePolicy Orchestrator® (McAfee ePO™) software, v5.1

Joint Solution Benefits

- Identify and secure unstructured data.
- Enhance DLP performance and reporting.
- Increase user awareness.
- Improve policy enforcement.
- Track user activity when handling sensitive information.
- Better threat and event response.

intel Security

Classification Enables Controls

An understanding of what information is truly sensitive, who that information can be shared with, and how to safely handle it is critical when you consider the sensitivity of certain types of information. People who create content generally have a good understanding of how their information should be handled. TITUS Classification solutions assist content creators by enabling them to apply visual classification labels quickly and consistently. TITUS also offers automated and suggested classification to aid users who are unsure of data security policies and to help with the application of corresponding machine-readable metadata. Once embedded into the content, classification metadata is a powerful asset tag that remains with the information regardless of where it goes and can be leveraged to automate data security controls, such as those contained in McAfee DLP. TITUS metadata allows McAfee DLP to be even more effective, as it provides a source context for data that might otherwise not be structured. Once McAfee DLP reads the TITUS classification metadata, additional policies can be enforced to block or allow sensitive information accordingly.

McAfee and TITUS Integration

Whether it's data in motion, data in use, or data at rest, most DLP solutions can identify all of the sensitive information created by end users. But consider abbreviations, euphemisms, typos, and abstract concepts. How can you accurately identify when this data is sensitive and prevent its inappropriate dissemination?

TITUS Classification solutions are effective, easy to use, and easy to deploy enterprise-wide, thanks to McAfee ePO™ software. TITUS Classification Suite includes solutions for email, Microsoft Office documents, and other file types, so virtually all types of unstructured information can be tagged and protected. Once users identify the sensitive data with a classification label, TITUS applies that label visually to the information, so that others in your organization can clearly see that the information is sensitive. Additionally, the metadata embedded by TITUS into the data can be read by McAfee DLP to help make informed policy decisions, such as whether to encrypt 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 violations of company policies.

By using TITUS Classification with McAfee DLP and McAfee Enterprise Security Manager, organizations can enhance valuable risk analysis capabilities. While McAfee Enterprise Security Manager is monitoring what is happening on the network in real time, TITUS Classification provides context to activities occurring on the desktop and network. For example, network administrators will be notified when email classifications are downgraded from "Internal Only" to "Public" and attempts are made to send to an external email address. This also occurs when Microsoft Office files previously classified as "Secret" are downgraded to a lower-level classification.

TITUS solutions seamlessly integrate with the most advanced and scalable security management software in the industry: McAfee ePO software. McAfee ePO software can be used to deploy TITUS solutions on the endpoint and to report deployment status across the enterprise. Applying specific labels and metadata takes the guesswork out of identifying sensitive data and ensures that information is shared securely. For example, if a document has a TITUS classification label that reads "Internal Only," McAfee DLP can block the ability to copy it to a removable USB device.

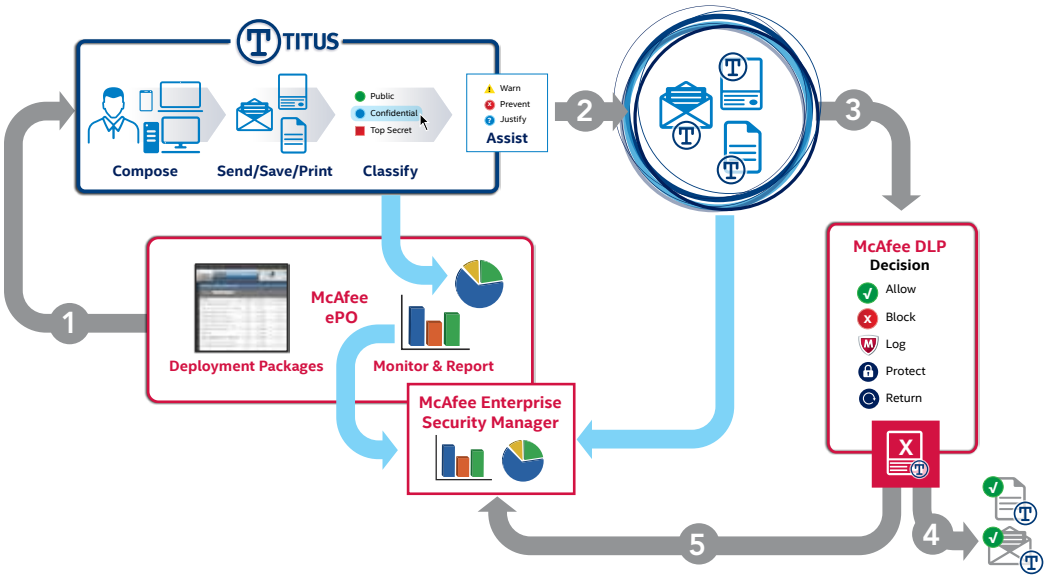

Figure 1. TITUS and Intel Security integration overview.

About TITUS Classification Solutions

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 DLP by classifying and protecting sensitive information in emails, documents, and other file types—on the desktop, on mobile devices, and in the cloud. For more information, visit **www.titus.com**.

About McAfee ePolicy Orchestrator Software

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

About McAfee Data Loss Prevention

McAfee Data Loss Prevention software 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 the McAfee ePO platform, for streamlined deployment, management, updates, and reports.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from Intel Security—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

About McAfee Data Exchange Layer

McAfee Data Exchange Layer is Intel Security's architecture for adaptive security. It is a real-time, bi-directional, communications fabric that allows security components to operate as one, immediately sharing relevant data among endpoints, gateways, and other security products, enabling security intelligence and adaptive security.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com