KuppingerCole Report

EXECUTIVE VIEW

by Graham Williamson | February 2015

TITUS Classification Suite

by Graham Williamson
gw@kuppingercole.com
February 2015

Content

1 Introduction

Sharing information securely is becoming increasingly important within companies, be it to protect intellectual properly, meet regulatory requirements for privacy or simply to avoid embarrassing leaks of proprietary information. While it is easy to stop access to documents and files, it is much harder to manage sharing such information. Shared Information Security is a topic within Cyber Security that deals with providing intelligent access control to protected resources; and it is of prime importance to most organizations today.

The typical questions facing companies are:

- Which of my corporate information is sensitive?
- How can controls be placed on unstructured data?
- What should be monitored?
- How can security be achieved without sacrificing productivity?

As companies increasingly embrace digital methods of conducting business these questions become more important. This means that steps must be taken to understand the data being used and shared within the organization and processes must be put in place to mitigate the risk of inappropriate data disclosure or data loss. *TITUS Classification Suite* provides tools to assist this task.

A necessary component of such information sharing is document and data classification. TITUS has operated in the email and document classification market for a number of years and has built an enviable reputation in controlling access to restricted documents, particularly in the Microsoft environment, enjoying significant market share in classification of Microsoft Outlook email and Office documents. TITUS is also a major third-party software supplier for Microsoft SharePoint security implementations.

Once a document, or file, has been appropriately classified TITUS software is focused on appropriate sharing of the information. This means making user's access as easy as possible, emulating the user experience in un-protected environments, while ensuring: classified documents are not sent to persons outside the sharing community, they are not stored on open infrastructure and they are not accessed from inappropriate locations. In addition, since most organizations are now faced with the need to support access from their staff member's mobile phone or tablet, TITUS provides the tools to manage the download and display of restricted documents and files to such devices.

TITUS has over 2.5 million users across 60 countries in both commercial and public sectors, including several defense organizations, utilizing their products.

2 Product Description

TITUS Classification Suite consists of the following products:

- *TITUS Message Classification for Microsoft Outlook* is a purpose-built add-on to Outlook providing the capability to block an email being sent to an inappropriate recipient. For instance, a message classification of "confidential" will restrict the distribution of an email to recipients authorized to a confidential level. Furthermore, a sensitivity rating can be associated with an email; a message with a sensitivity of "Internal use" will not be able to be sent to external email addresses. Policies can also be established restricting sending internal documents to external companies or public domains. To assist users, visual markings are used to alert users to the sensitivity of a document and, depending upon corporate policy, a "send anyway" option can be provided so that legitimate business is not hampered.
- *TITUS Classification for Microsoft Office* is a tool to attach a classification to an Office document. A Word document, Excel spread-sheet, or PowerPoint presentation marked Confidential, for example, will only be accessible by someone with Confidential access rights. Adding "Internal use" sensitivity will further restrict its distribution. The product provides visual markings to alert users to a document's sensitivity and can even dynamically add a watermark to a document to encourage appropriate treatment of sensitive information.
- *TITUS Classification for Desktop* is a tool to apply classification metadata to common file types such as PDF, JPG and MPG4. By right-clicking on a file in Windows Explorer, users can apply the appropriate classification to a file.
- *TITUS Classification for Mobile* incorporates the *TITUS Docs* and *TITUS Mail* mobile applications that apply classifications and inhibit data loss. The apps provide the ability to separate personal data from corporate data on smartphones and tablet devices and establish an encrypted document container that is subject to administrator control. This allows an organization to manage access to, and deletion of, corporate data files on external devices. The application can also be configured to delete documentation after a set expiry date or after a period of inactivity. The application also observes the RMS restrictions placed on mail attachments.

TITUS Classification for Mobile

The mobile apps bring Titus' classification expertise to mobile devices. The product comes with an easy-to-use management interface whereby global settings for document expiry, disabling attachments and geo-fencing can be set-up and individual controls on document classifications can be established. For instance, safe recipients can be set-up for Secret documents and print restrictions can be placed on restricted documents. The management GUI provides a set of standard policies that can be implemented to define the treatment of classified documents. TITUS is also working with Mobile Device Management (MDM) software suppliers to support the tool.

The *TITUS* Mail mobile application provides a standard email client for mobiles but with a difference. Emails can be displayed with color-coded classifications to allow quick determination of a message's classification level. For instance Secret documents could be colored red, Confidential documents blue,

and un-restricted documents green. In the event that a user attempts to send a restricted email to another user who is not entitled to receive restricted content, the send functionality will be inhibited and a message box will be displayed on the screen; the email will not be transferred to the recipient's device by the mail transport agent.

The *TITUS* Mail app fully implements the classification policy established by components of the Enterprise Suite. For example, if a policy has been set which limits a document to "restricted", for example, the mail transport agent email will only transfer the sender, subject line and classification level to the recipient's mobile device. The body of the email will indicate that the display of the full text is prohibited on the mobile device and needs to be viewed on the desktop.

The app also incorporates "geo-fencing" which allows the software to restrict access to data depending on the geographic location of the device. For instance, a user might be able to access a document while in North America but if the device is activated in China the document would not be displayed.

The Classification Task

TITUS has built significant expertise in classification technology and the related procedures within an organization and tools are provided to assist in the classification task.

Classifications are stored within email or document files as persistent metadata, these classifications are then used to control how users can store or send the files, effectively providing a DLP solution. There are three basic ways in which classifications can be assigned to documents and the selected approach should recognize the culture within the organization. For hierarchical organizations with a command and control structure a classification system can be imposed and staff will adapt to its use. For organizations with a flatter structure and a more co-operative approach the classification system must accommodate the way people work and indeed it might vary between departments.

An *automated classification* system will use specific rules to automatically assign a classification to a document. This might be based on the user's security level and the context of the document i.e. sensitive project documentation will be restricted to the members of the specific project group.

With a *guided classification* system a document's classification is automatically suggested, based on a set of rules. The user can choose to accept or override the suggested classification.

The *user-driven classification* system leaves the classification task up to the user and will identify documents based on the user's selection. Different classification methodologies can be employed based on the user or group membership. For example, one group may be required to classify, another group could have automatic classification, and yet another group set for discretionary classification.

Policy Management

TITUS Classification Suite offers a single tool with which to manage policies within the classification components. A competitive advantage for TITUS is their expertise in classification management and ensuring it is matched to the policies that the organization requires. TITUS will assist clients in determining the "policy pattern" that best matches the culture of the company, or each business unit within the company, and will assist in encoding these requirements via the policy management tool. Conditionality can be factored into the policies so that multiple decision paths can be evaluated before ensuring that the correct classification value is applied.

Reporting and Analytics

Current plans for *TITUS Classification Suite* include reporting features to allow management to monitor events and trends, identify possible policy violations and provides the ability to integrate metrics into dashboard technology. The system monitors activity against normal behavior and alerts on events such as classification downgrades, documents exported to Dropbox or classified documents sent to external recipients. Behavioral analytics is used to notify of anomalies and alarm on trends.

3 Strengths and Challenges

The strength of the *TITUS Classification Suite* is the way it brings together email, Office documents, the desktop and mobile applications under a single management environment to provide data loss protection across company resources. TITUS' professional services bring the expertise to inculcate a document security culture throughout an organization. By requiring staff to adopt a classification system, deploying access policies across the organization and overtly displaying a document's classification on smart devices and in emails, companies will enhance their approach to protecting corporate data. Users are encouraged to value company information and adopt proper document handling procedures to prevent disclosure of protected data to unintended recipients.

TITUS Classification Suite allows organizations to deploy a secure communications and document repository environment identifying intellectual property and trade secrets in emails and documents and engaging the user in the classification and protection of the company's soft assets by warning or preventing users from sending classified material outside the group or company. TITUS can identify sensitive material by classification keywords, PII data such as social security numbers or PCI data such as credit card numbers. The ability to dynamically add headers, footers or watermarks to documents to increase user accountability when handling their company's restricted information is particularly innovative. Compliance with worker privacy policy is also accommodated by the ability to restrict content monitoring to work-related documents.

The components in *TITUS Classification Suite* are focused on preventing compliance violations by stopping mistakes before they happen. Users are given immediate feedback on actions that would contravene policy so that they can avoid violations or justify exceptions.

There are several challenges for TITUS. Currently the *TITUS Docs* mobile app is a viewer only and cannot be used to set or modify document classifications. *TITUS Docs* will display a document's classification and will apply the appropriate policies to the display of a restricted document. Note: while the application utilizes AES-256 encryption which will be observed while the document is managed within *TITUS Docs*, if it is sent via email or copied to a cloud repository the protection provided by *TITUS Classification Suite* will be lost. RMS protection is observed by *Titus Docs* and such settings are persistent when a document is copied or emailed.

On the desktop, *TITUS Classification Suite* is Microsoft-centric and will fully satisfy most organizations with low-to-medium security environments.

While product enhancements are being developed, for organizations with mixed environments with Linux servers and open doc files there will be some challenges to deploy a cross-environment document security regime. For high-security environments such as pharmaceuticals or defense establishments, combining *TITUS Classification Suite* with a purpose-built security framework i.e. network protection or gateway devices may be warranted.

Some organizations wanting a comprehensive secure shared information environment will want to augment the TITUS solution in order to provide DLP controls to data-in-motion and data-at-rest in server-based repositories. TITUS does closely integrate with a number of DLP solutions, notably McAfee and Symantec DLP, making them easier to use and improving their effectiveness.

Two specific areas in which enhancements are being made are: reporting analytics and policy management.

Strengths	Challenges
• Well-defined balance between protecting and sharing corporate documents and data. • Longevity in the document classification marketplace and reputation for strong access control. • State-of-the-art mobile application to protect documents in a BYOD environment with enforced data segregation. • Strong professional services offering to assist customers to configure their required classification system. • Automated RMS-based classification to manage content and recipients extended to mobile devices • Centralized policy management via the TITUS Administration Console	• *TITUS Classification Suite* is a comprehensive package requiring cross-organization cooperation for an effective deployment. • Stronger email management to allow TITUS Classification for Mobile to protect an outgoing mail using Microsoft RMS is planned. • TITUS is currently focused on the Microsoft market; users will experience shortcomings in cross-domain environments.

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden| Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com