titus
by HelpSystems
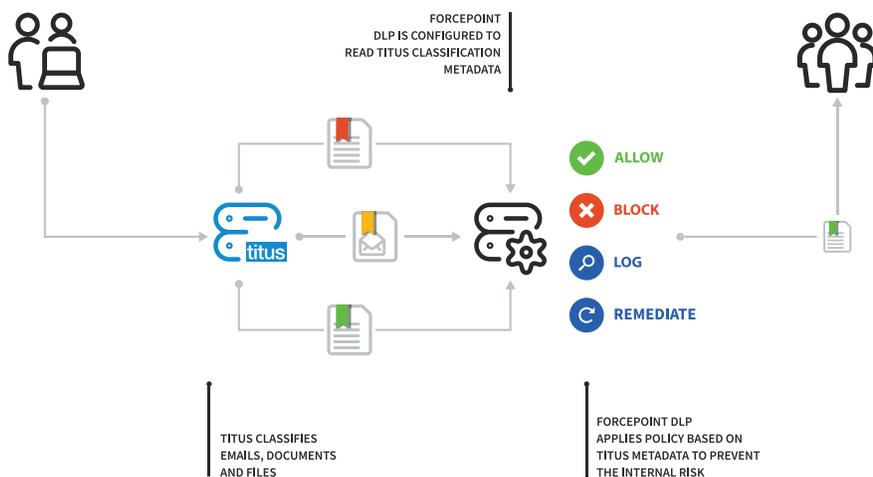
Titus Classification and **Forcepoint Data Loss Prevention**

Titus Classification solutions provide the perfect complement to Forcepoint DLP by involving end users directly in corporate DLP strategies. Titus promotes a culture of security by prompting users to stop, think, and consider the business value of the information they are creating and handling. When the information creator can proactively indicate the value of data, Forcepoint DLP is empowered with additional information, allowing for more dynamic DLP policy decisions and insider threat detection.

In order for organizations to effectively protect their most valuable information assets, it is imperative that they be properly identified. With solutions for email, documents, and other file types, Titus enables users to classify unstructured information they create and share. Involving users in the data identification process helps to foster a culture of security and emphasizes end user responsibility for information protection.

FORCEPOINT DLP IS CONFIGURED TO READ TITUS CLASSIFICATION METADATA

ALLOW
BLOCK
LOG
REMEDIATE

TITUS CLASSIFIES EMAILS, DOCUMENTS AND FILES

FORCEPOINT DLP APPLIES POLICY BASED ON TITUS METADATA TO PREVENT THE INTERNAL RISK

FORCEPOINT

About **Forcepoint**

Forcepoint is the global human-centric cybersecurity company transforming the digital enterprise by continuously adapting security response to the dynamic risk posed by individual users and machines. The Forcepoint Human Point system delivers Risk-Adaptive Protection to continuously ensure trusted use of data and systems. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries. www. forcepoint.com

Titus promotes user accountability by applying visual labels and watermarks which can be configured by the administrator to indicate the classification value as well as the active user's name, ensuring greater responsibility for the information even when printed or shared as a PDF.

The persistent metadata associated with Titus classifications provides Forcepoint DLP additional details about the files, documents and emails. This information can be used to enforce granular data security policies and prevent

Identify sensitive data and **prevent data loss**

accidental or malicious data leaks. For example, a user may have access to a specific folder on the network, but some of the content contained within the folder may be classified above their security access privileges. Forcepoint DLP policy Identify Sensitive Data and Prevent Data Loss will recognize the classification on the document and prevent the user from accessing that file, therefore avoiding a security policy violation.

Additionally, Titus Classification and DLP Discover can work together to classify your entire document archive. As DLP Discover audits legacy data and determines the value, Titus will apply the appropriate classification metadata to the file.

Titus Classification metadata makes it possible to more easily detect an insider with malicious intent. As data is shared, DLP Network and DLP Endtime Endpoint will validate that the classification applied by the employee is appropriate. For example, a user may deliberately classify a document containing valuable Intellectual Property (IP) as "Public" in order to bypass security. The Forcepoint DLP engine will verify the content before it is copied and locate the IP. Once identified as containing sensitive information, Forcepoint DLP will quarantine the document and, because the classification was set by the user to "Public," be alerted to the suspicious activity.

Together, Titus and Forcepoint enrich corporate security culture and enforce data security policies to prevent accidental or malicious data disclosure.

JOINT SOLUTION COMPONENTS

TITUS Classification Suite and Forcepoint DLP

- DLP Network
- DLP Discover
- DLP Endpoint
- DLP Cloud Applications

JOINT SOLUTION BENEFITS

- Reduce the risk of data loss and theft
- Identify sensitive data with greater accuracy
- Classify data-in-motion and data-at-rest
- Enable automated and user-driven classification
- Increase user security awareness and
- accountability
- Improve internal risk detection and response

---

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.