Titus policy engine brokers

Vera encryption

titus by HelpSystems

JOINT SOLUTION BRIEF

Employees send emails, create documents, and upload files to internal servers and cloud applications every day—and the volume of data is growing exponentially. How can you ensure that sensitive data remains secure without burdening your end users with time-consuming and confusing workflows?

The best way to protect sensitive data is to restrict access to these files to only a select group of individuals. Identity Management solutions can define groups based on a number of parameters—department, role, security clearance, region, office location, etc. The question is, how does your data protection solution know how to treat any particular file?

Titus works to provide a foundation for encryption

It can be difficult to protect data when you don't know what you're protecting. A data classification solution with robust identification capabilities is the first step in securing data effectively. Titus works with existing workflows in the following ways to provide a basis for effective rights management.

- **Titus works where your users work** to identify and classify emails and office documents (Word, Excel, PowerPoint), at the point of creation where context availability is at its highest.
- **Titus works where your data** is by applying data identification technologies and classification to data in file shares and cloud repositories.
- **Titus works with the data you use every day** by providing users the ability to classify any file via an intuitive interface right from their desktop

No matter how data is classified, machine-readable persistent metadata is applied. It is this Titus Metadata that unlocks the potential of the VERA encryption solution.

Titus classification & Vera encryption

Company policy might determine that a sensitive file, classified by Titus as Restricted, must be encrypted before it can be shared via email or stored in the Cloud. The Restricted classification triggers the Vera Client to automatically encrypt the file, without any input required by the user. Titus embeds unencrypted classification metadata in the header of the encrypted file, resulting in a protected file with machine readable classification information.

The file is now encrypted, but other security products like DLPs, CASBs, etc. are still able to read the metadata that contains the data classification value.

VERA

About **Vera**

Vera is the data-centric security solution leader enabling businesses of all sizes to secure, track and share any kind of data, no matter where it's stored or located.

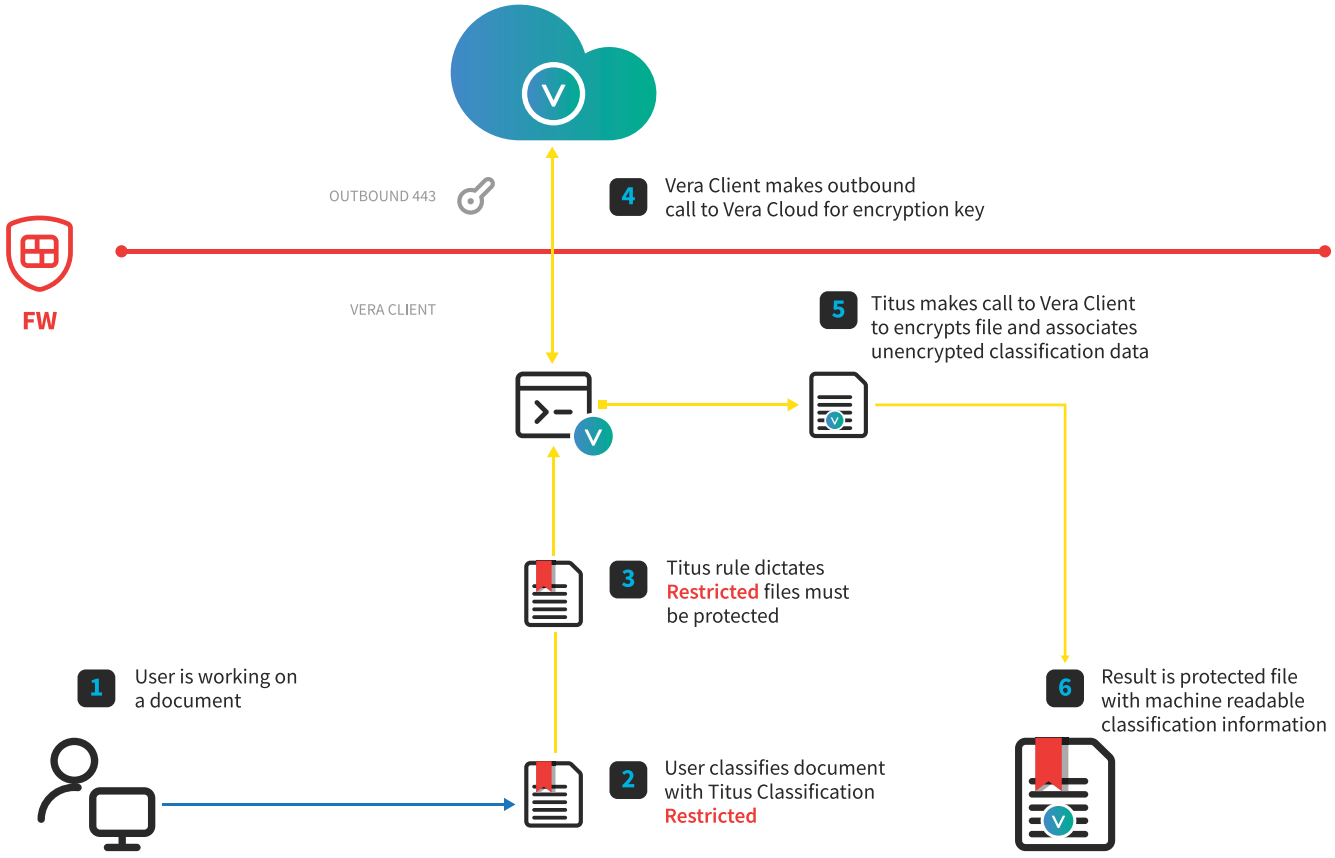
With robust policy enforcement, strong encryption and strict access controls, Vera's data-centric security solution enables employees to collaborate freely while ensuring a high level of security, visibility and control.

For more information, visit www.vera.com.

Titus policy engine brokers **Vera encryption**

Benefits

Titus' enterprise-grade classification solution embeds rich metadata into emails, files, and documents, helping organizations understand what data they have. The metadata offers partners in the security ecosystem visibility into classification and sensitivity levels or all files.



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.

JSB-Titus-policy-engine-brokers-VERA-07/20