VERA

THE VERA-TITUS CLASSIFICATON INTEGRATION

Introduction

The VERA-Titus integration provides an end-to-end solution to help organizations find, identify, categorize, analyze, secure, and track the data they have. This enables employees to work and collaborate more freely, both internally and externally, without having to worry about having an understanding of what is and what is not confidential.

Data Classification Primer

Data classification is a subset of data management and is an integral part of the Information Lifecycle Management (ILM) process. Broadly speaking, it is a tool used for the categorization of data that enables organizations to better understand what types of data they have available, where that data is located, what are the different levels of access to that data, and what level of protection should be applied to that data. Likewise, in an age where there are multiple compliance and regulations to adhere to, data classification can help organizations gain more insight into their level of compliance.

Data classification represents the foundation of an effective information governance strategy. It provides organizations with the ability to make more intelligent and conscious decisions about how their data is used and handled by exposing the business value of that data.

The VERA-Titus integration provides an end-to-end solution to help organizations **find, identify, categorize, analyze, secure, and track the data they have.**

The Challenges

In today's distributed enterprise, data is effectively located everywhere - in on-prem share drives, in the cloud, on desktop devices, and on employees' mobile devices. So understanding what corporate data you have and where it's located has never been more difficult - or more important. This becomes even more urgent if that data happens to be sensitive in nature.

But how do you define what data is sensitive and what isn't? Almost anyone knows that information such as social security numbers, addresses, phone numbers, insurance numbers, personal health data, or bank account numbers are all confidential. However, when it comes to company-specific information like business plans, product roadmaps, design files, product documentation, intellectual property, it is not always as straightforward.

It's this type of information that typically presents the greatest challenge for organizations to deal with. Categorizing and protecting this data proactively, consistently and accurately compounds this challenge as failure to do so represents a real security risk. Likewise, context is crucial for accurate data classification and in the end, the most effective way to keep information protected is to employ a strategy based on a combination of people, process, and technology.
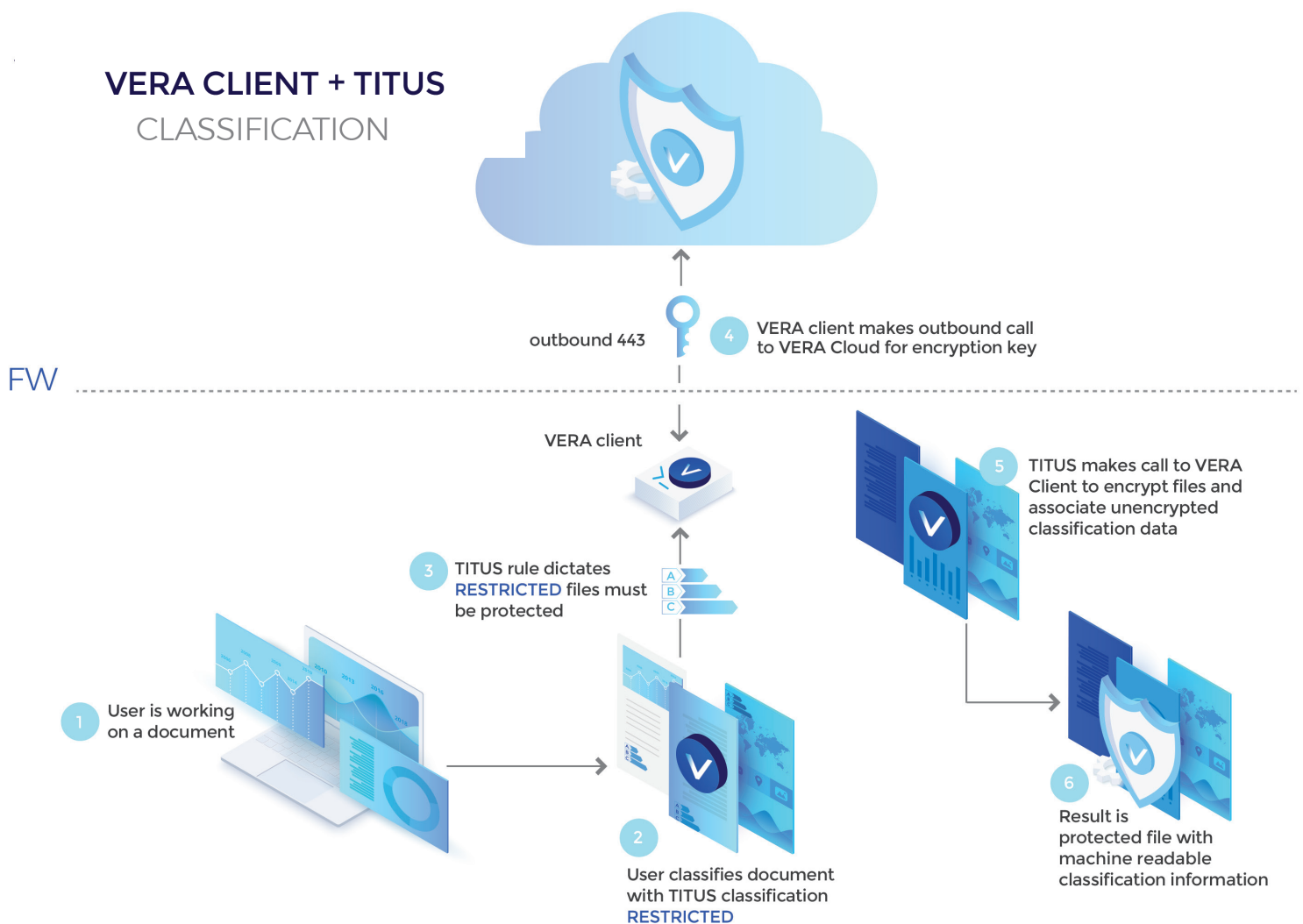
IN TODAY'S TECH-DRIVEN WORLD YOUR DATA IS EVERYWHERE.

So understanding what corporate data you have and where it's located has never been more difficult - or more important. This becomes even more urgent if that data happens to be sensitive in nature.

How it Works

A company might have a corporate policy that mandates that any files determined by Titus to be classified or sensitive in nature must be secured by VERA before they can be shared over email or via cloud collaboration solutions.

In this scenario, once Titus tags a file with a "Restricted" classification, it then leverages the VERA SDK to automatically call the VERA client to secure the file. VERA then applies encryption to the file and adds access controls along with a specific policy that correlates back to the classification applied. Titus also embeds unencrypted classification metadata in the header of the secured file, resulting in a protected file with machine readable classification information.

The classification metadata that gets attached to the secured document is important as it also enables other security products like DLPs and CASBs to read the metadata that contains th data classification value.

VERA CLIENT + TITUS
CLASSIFICATION

outbound 443

4 VERA client makes outbound call to VERA Cloud for encryption key

FW

VERA client

5 TITUS makes call to VERA Client to encrypt files and associate unencrypted classification data

3 TITUS rule dictates RESTRICTED files must be protected

A
B
C

1 User is working on a document

2 User classifies document with TITUS classification RESTRICTED

6 Result is protected file with machine readable classification information

Benefits

The VERA-Titus integration employs a powerful combination of enterprise-grade classification and file-level security. This helps organizations to better understand and categorize the data they have as well as secure that data wherever it travels. Both technologies also compliment other security solutions used to protect data at rest and the flow of data, such as CASB and DLP. All of this serves to dramatically improve an organization's overall security posture to protect against data breaches and having sensitive data fall into the wrong hands.

About Titus

Titus Classification Suite enables organizations to truly understand what kind of data they possess, the value of that data, and how best to classify files in order to mitigate exposure to risk. With Titus, you can clearly and accurately classify emails, spreadsheets, presentations, and other file types using user selected, system-suggested, or automatically-applied classification settings that are based on your unique data security policies. It is designed to empower employees to work confidently and productively, with the knowledge that their emails, documents, and sensitive information are all protected.

THE VERA + TITUS INTEGRATION

A **POWERFUL COMBINATION** of **enterprise-grade classification** and **file-level security** to **dramatically improve** an organization's **overall security posture** to **protect against data breaches**..

TRACK   **AUDIT**   **MANAGE**   **REVOKE**

About VERA Security

VERA is a data and content security solution that enhances an organization's ability to protect, govern and manage the transmission of information without impacting employees or the existing security choices the organization has made. Files secured by VERA can still be protected by gateways, firewalls and endpoint technologies, but customers choosing VERA can now extend these controls beyond the boundaries of their business.

With a centralized cloud architecture that is content and storage agnostic, policy-driven and designed to adapt to modern work practices, VERA allows customers to provide consistent, auditable protection across all of their critical content. VERA enables organizations of all sizes and in any industry to maintain existing investments in storage, collaboration and communication while improving their security profiles.

VERA

To learn more or to schedule a demo, please contact us at sales@vera.com.