VERA

VERA SECURITY SOLUTIONS BRIEF

THE VERA SOFTWARE DEVELOPMENT KIT (SDK)

Highlights

VERA offers two ways to integrate VERA features with other applications:

- VERA SDK
- VERA REST APIs

The VERA SDK is intended for executing VERA features locally. The VERA REST APIs enable remove execution, which requires sending files to the VERA server.

Data-Centric Security

Data-centric security is the ability to secure data through its entire life cycle, everywhere it travels, no matter who has it or where it's stored. The goal is to protect confidential data at the point of its greatest vulnerability – when it's being used in others' hands, and as it travels outside our perimeters into unmanaged domains, devices and applications.

Introduction

Many organizations have needs for file security and access control that cannot sufficiently be met with "off the shelf" solutions. As a result, they often build their own custom ("homegrown") applications to achieve their desired objectives.

However, the administration of these custom applications can become expensive. For example, new business requirements or compliance mandates may dictate that a new policy has to be created or updated in the custom application to accommodate the change. This process is expensive and limits the organization's ability to respond rapidly in their business environment.

The Solution

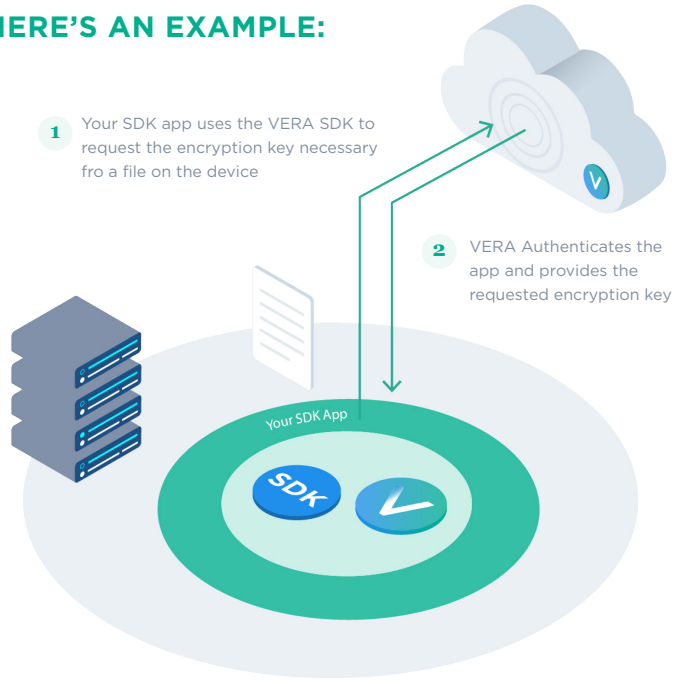
The VERA Desktop SDK enables you to programmatically execute the following tasks on a device: you can secure files, unsecure files, give access to a file for specific users, groups or domains, revoke access to a file for specific users, groups or domains, and revoke access to a file for all users.

Using the VERA SDK is the best way to integrate VERA features with your own scripts or applications.

How it Works

Downloading the VERA SDK to a device is like installing a smaller version of the VERA client with a programmatic interface. The VERA SDK interacts with the VERA tenant to retrieve the encryption keys and other data necessary to complete basic tasks on files stored on the device. Your custom app drives the interaction through command-line calls to the SDK.

HERE'S AN EXAMPLE:



The VERA SDK Local Execution

Execute the following tasks on a device:

- Secure a file
- Unsecure a file
- Give access to a file
- Revoke access to a file for specific users
- Revoke access to a file for all users

SDK allows for integration into 3rd party applications such as web apps, DLP, classification, and DMS.

Desktop SDK Use Cases

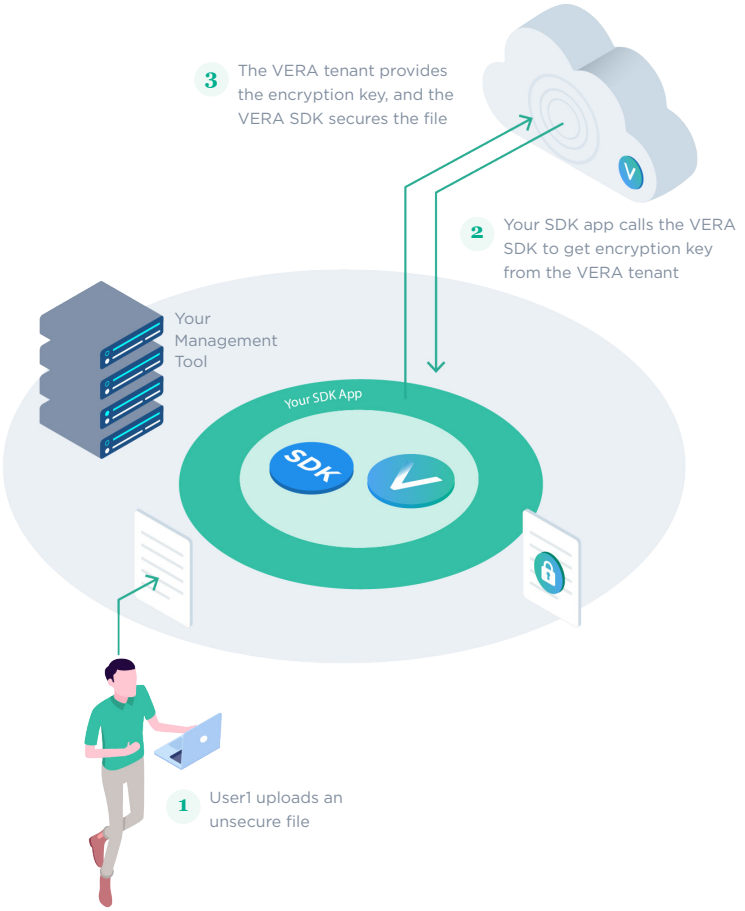
Before you begin to plan your Desktop SDK integration, there are some basic points to consider: 1) the SDK needs to be local to the files you are working with; 2) a secure file is protected even from your internal apps until you unsecure the file.

Securing on Upload

Securing files when they are uploaded to an internal system is a common use case. Because a secure file is both encrypted and wrapped in a proprietary HTML shell, your internal applications will not recognize the secure file as having its original file type.

Always-on File Security

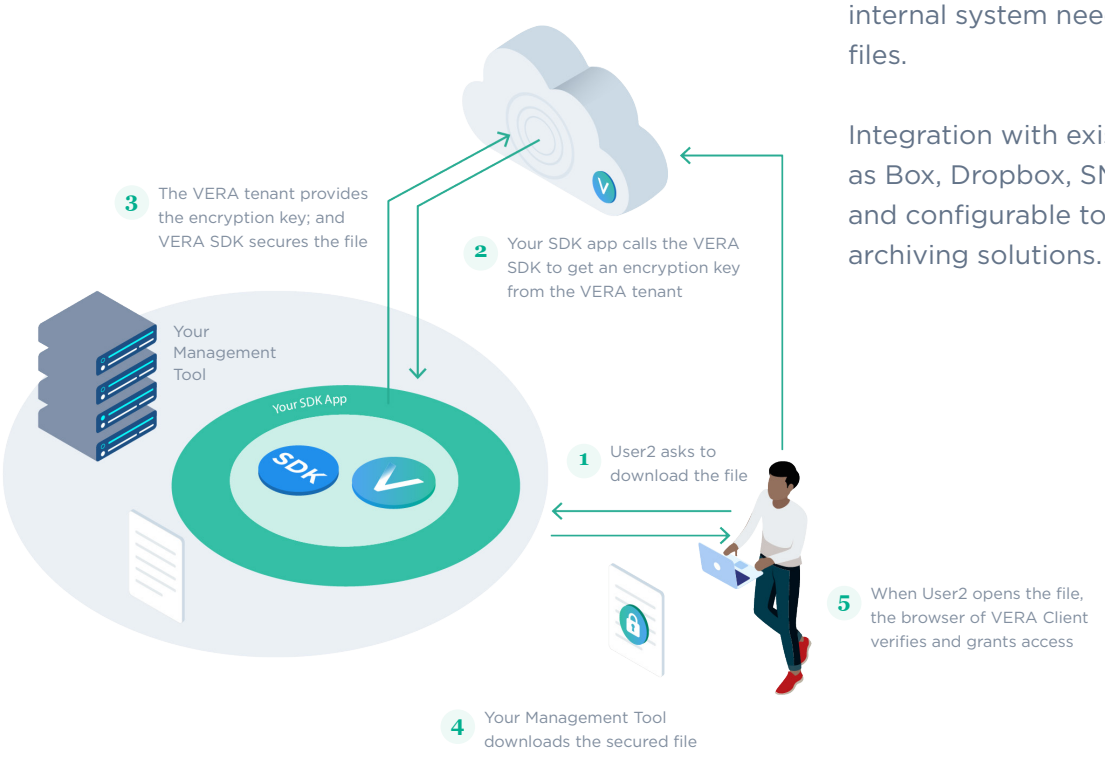
- Dynamically control user file permissions
- Permission management is external to the file
- AES 256-bit encryption to any file type
- Granular visibility and centralized control
- Understand how your content is used, by whom, and proactively investigate unauthorized attempts
- Policies can be based on a number of pre-defined parameters including file location, name, type, securer, sender, recipient, group or other pre-existing permission structures.



Securing on Download

Some organizations prefer to store unsecure files, securing them only when a user chooses to download them. This model works well if an internal system needs to operate on the stored files.

Integration with existing file share solutions such as Box, Dropbox, SMB, SharePoint and OneDrive, and configurable to work with enterprise email archiving solutions.



Desktop SDK and Third-Party Access Control

VERA provides a third-party access feature to enable your Desktop SDK app to use a separate database for authentication and policy mapping. You might use this feature if you have an established internal database that governs which users have access to which files.

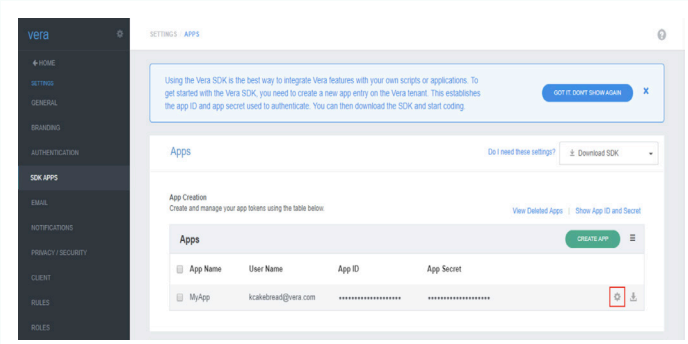
Active File Protection

- Apply AES-256 Encryption to any file type to ensure sensitive data can't be accessed by unknown parties.
- Granular visibility and centralized control; understand how your content is used, by whom, and proactively investigate unauthorized access attempts.
- Policies can be based on a number of pre-defined parameters including file location, name, type, securer, sender, recipient, group, or other pre-existing permission structures.

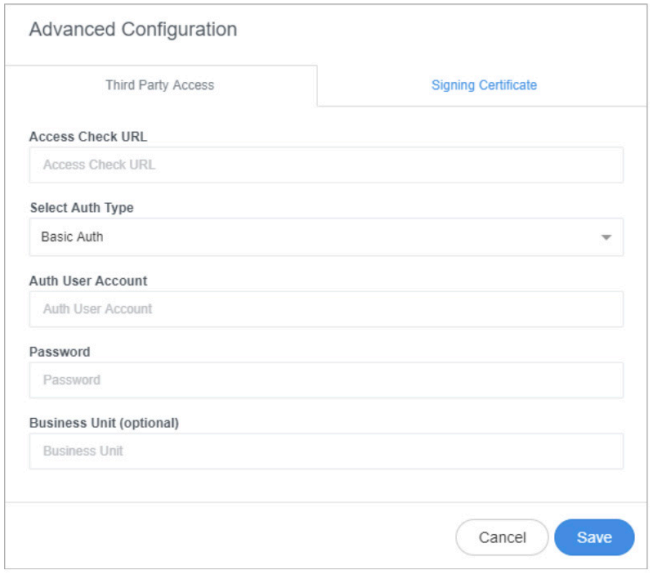
Setting Up Third-Party Access

To set-up third-party access, you need to add information to your SDK app entry on the VERA tenant:

Go to Settings > SDK Apps



Click on the settings icon for your app entry



Using a Second Factor for Your SDK App

VERA provides the option of using a certificate as a second factor for authenticating your SDK app. You can configure the certificate by uploading the public key in the VERA Admin Portal. Your SDK app would then need to use the certificate to validate interactions.

About Vera

The VERA platform enables businesses of all sizes to effectively protect any kind of data, and then track, audit and manage the policies securing it in real-time, no matter where it travels, or where it's stored. It's imperative that you are able to secure sensitive files, no matter what device, person, cloud or application creates or receives that data, even if it falls into the wrong hands.

For more information about securing your data with VERA, or to schedule a demo, please contact us at sales@vera.com.

Supported Environments

PLATFORM	C++	JAVA	.NET/C#
Windows 64 bit	✓	✓	✓
macOS	✓	✓	
Ubuntu Linux 64 bit	✓	✓	
CentOS Linux 64 bit	✓	✓	
RedHat Enterprise Linux	✓	✓	