## Is VERA's performance to encrypt/decrypt impacted as information is shared worldwide? Is there a lot of latency to send a file from California to Sweden or South Korea?

VERA's secure shell is extremely light and only adds about 3% additional weight to the file. VERA only stores meta-data, which makes for a very lightweight wrapper. Our customers haven't experienced any latency sending files abroad.

## Does VERA physically store my data anywhere?

VERA does not store customer data or content. The information stored in the VERA Cloud Platform is limited to the encryption keys, policy definitions, user account information, and audit log data for the VERA Dashboard. VERA can't actually see the information inside your files. We separate the encryption keys from where the content is physically stored.

## What encryption standard does VERA use?

Data encrypted at rest by VERA is secured with AES 256-bit encryption. In transit, VERA employs TLS 1.2 and SSL 3.0 to protect customer data.

## If someone emails an encrypted document to someone who should not have access to it, at what point would we be able to see that happen in VERA?

Would we have any visibility when the email is sent, or would it trigger only when the recipient tried to open or work with the file?

VERA would be able to see the action when the recipient tries to open or work with the file.

## How do you prevent copy/paste, disable printing and enforce other data loss policies across files?

VERA sits between the operating system and the application layer. Think of it as a sandwich (OS–VERA–applications, e.g., Word). VERA can block commands the application sends to the OS -- blocking the ability to copy/paste, print, save, save as, etc.

## Where do the encryption keys live? Who stores the keys?

VERA stores the encryption keys, policies and usage rights in our cloud instance on Amazon Web Services (AWS), all separated logically for each customer. Note: we do offer customers the ability to manage their own keys with a local key store service.

## If VERA is subpoenaed, would you share my company's data?

One thing that's really valuable about our platform is that VERA separates security (encryption keys) from your content. Your content and your company's data is stored with you, and VERA only stores and manages those keys and usage policies. This means that if VERA is subpoenaed, we couldn't share your company's data because VERA doesn't have it. Assuming the subpoena is valid, and that it's a subpoena with a gag order forcing VERA to comply, the only thing we could hand over would be the meta-data (e.g., metadata includes the encryption keys, usage policies, permissions, file details, etc.).

## Where is VERA's instance located in the cloud?

VERA is located in one region (AWS US West 2/Oregon) mission-critical components span a minimum of two availability zones and VERA's data is distributed across three availability zones within the Oregon region.

## What happens if the VERA service is unavailable?

In the event VERA cloud service is unavailable, customers will receive notification of the outage condition and estimated time to resolution. Authentication will be unavailable until the situation is resolved, however, all offline policies will continue to be enforced.

## What happens if VERA's servers go down?

VERA runs across multiple AWS (Amazon Web Services) regions. We plan for both disaster and recovery  but have built a system for disaster avoidance. We do allow customers to manage their own disaster recovery scenario, take a copy of the key store and have a backup on-premises. Box and Dropbox, for example, do not allow for this type of on-premise solution.

## Does VERA have a public-private key model?

No. VERA uses a single, symmetric-key algorithm for both encryption and decryption. At VERA, the same key that encrypts a file is the key used by a recipient to decrypt it on his end.

## If I choose to move away from using VERA in the future, what does the process look like to unencrypt my files?

It is fairly straight-forward to remove VERA protections from any object, whether you are a current customer, or have decided to move on. Administrators and file owners have the ability to directly unsecure a file, individually or in bulk. Additionally, through the VERA API and SDK, large quantities of files in your applications and repositories can be restored to their earlier state. Also, using the VERA dashboard (which you can have access to for a fixed period of time after termination of a contract), you can easily locate the owners and last accessed locations of any file, making retrieval and unsecuring straightforward.

## How is VERA deployed?

VERA can be deployed automatically (admins deploy to end-user machines) or end-users can download VERA themselves. Either option is available to customers. If automatically, this would be a silent installation and management. For internal users, our VERA app can be silently installed via an MSI using your SCCM and/or MDM solution of choice. Users in this case never have to download anything.

## Is there an option if I want to manage my keys on-premise?

Yes. One of our deployment options allows customers to manage the keys on-premises though most of our customers deploy VERA as a cloud-based model.

## Does VERA offer an SDK?

Yes. VERA has a client-based SDK that allows security teams to weave in VERA data security capabilities into third-party apps and homegrown business applications. Our sales engineer can provide more detailed information.

# Summary

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 documents, no matter what device, person, cloud or application creates or receives that data, even if - and after - it falls into the wrong hands.

vera
by HelpSystems

To learn more or to schedule a demo, please please visit us at **www.vera.com**.