VERA

VERA PLATFORM FREQUENTLY ASKED QUESTIONS (FAQ)

What is VERA's origin? Can you tell me about the company?

Vera was founded in 2014 by data security experts who realized that in today's highly collaborative world, there is no perimeter. We're solving the problem of helping IT and security teams control information as it's shared beyond their borders, and especially when it's "in use " when it's in others' hands.

We're headquartered in Silicon Valley and have secured venture financing from notable investors, including Battery Ventures, Sutter Hill Ventures, and Capital One Growth Ventures.

How is VERA different than traditional DRM tools,like Microsoft RMS or AIP?

Traditional digital rights management (DRM) tools are limited by the file types they support (only Office and PDFs), an inflexible framework that requires a client at all times, and the difficulty of implementation and use for business users. VERA is a data security platform that can secure any file type, provides a seamless end-user experience and gives admins complete control of their information anywhere the file travels, whether or not the recipient has a VERA client in place.

How is VERA different than traditional DLP products?

DLP products scan and process data to prevent sensitive information, including PII and PHI, from leaving the organization. Once that data leaves the network, DLP products cannot track or dynamically revoke access if sensitive information is leaked from the company. It can be either network or endpoint-based, each having their own unique benefits and challenges. DLP technologies have traditionally been prone to false positives, and as such, some of their best use-cases are for controlling very predictable and structured content in very specific situations. For example, DLP might be used for ensuring that credit card numbers do not leave the Cardholder Data Environment of network. However, as content and locations get more complex, DLP can develop problems very quickly.

How is VERA different than a CASB product?

CASBs have proven to be highly valuable to enterprises on a variety of fronts. At their core, a CASB is able to extend security policy to an enterprise's cloud applications in much the same way a traditional firewall would protect on-premise applications. What we see is that a CASB can lose control over data after it has been accessed. Users can still copy the content, store it in insecure personal drives, share it with other parties, or have it compromised by malware or attackers. While a CASB can help illuminate an application blind spot, it does not ensure that data itself remains safe.

This is where VERA compliments a CASB product.

VERA protects unstructured data, and a CASB allows you to fulfill the gaps in structured data. From an unstructured data perspective, when VERA encrypts a file in Box, it can break some of the functionality of Box, namely search. You can use a CASB to protect the file as it's sent to Box, and gives the ability to use that file while it's unencrypted, so you have the benefits under their infrastructure. However, when that file starts to egress and leave the company, that's when the CASB would call on the VERA API to extend their protection, encrypt the files, and maintain that ownership of the file, once it leaves the protection of the CASB sphere.

What file types does VERA secure?

VERA is a content-agnostic platform, so we can secure any type of file, including; PDF, XLS, PPTX, JPEG, PNG, MP4, XLSM, DOC, DOCX, XLSX, TXT, JPG, BMP, AVI, CSV, PPT, RTF, GIF, MOV, WMW, including CAD/CAM files used in the manufacturing industry. Please see the VERA RFP Guide for more information on coverage.

What operating platforms are supported by VERA?

VERA supports Windows, Mac OS, iOS (iPad and iPhone), Android, and Surface.

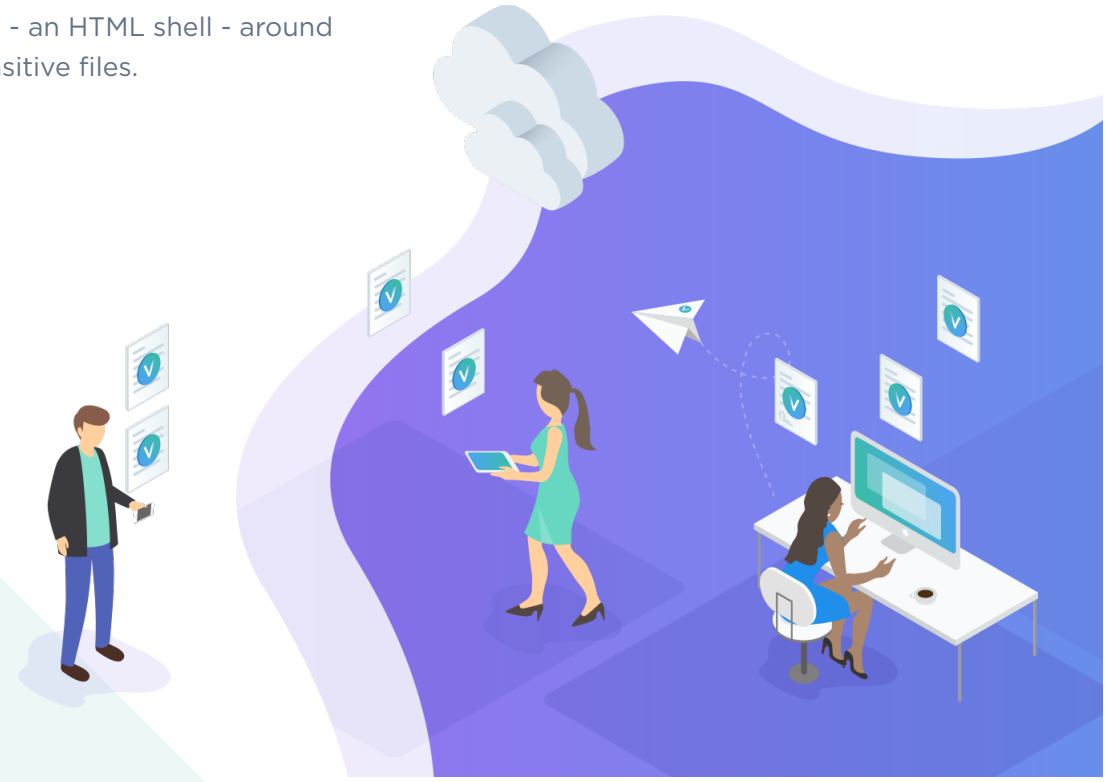
How does VERA's encryption work?

VERA is a secure shell - an HTML shell - around each of your most sensitive files.

Vera's encryption:

1. Encrypts the file with AES 256-bit encryption
2. Enforces access control (who has access to it?)
3. Allows you to control what people can/ cannot do with your information (disable printing, copy/paste, and others)

As people open your file, this sends a request to the VERA cloud, which confirms whether or not that person has access and what their rights are to the document. For more information, please see the VERA security architecture and the RFP Guide.



How can I be sure that VERA does not see or store my data?

The VERA Cloud Platform manages the policy and controls for each customer, or tenant on the platform, and securely manages the processes of creating keys, enforcing access policies and aggregating events and activities for audit and reporting purposes. No customer data or content is stored on the VERA Cloud Platform.

How does VERA work with file share tools?

VERA integrates with Box, Dropbox, and SharePoint. If your organization uses one of these content repositories, you can set up VERA to automatically encrypt the files placed in a designated folder. For publication of view-only files, you can set up a simple rule to establish this process. For more involved collaboration, the installation of a Share Connector enables you to map Box/Dropbox/SharePoint roles to VERA roles to ensure that the right people get the right access.

For SMB file shares, you can use the VERA integration to automatically secure content stored on SMB file shares in your organization. Users just drag-and-drop files into the designated folder. VERA automatically applies the restrictions defined for that folder.

How does VERA work with content management systems?

VERA operates independently of most content management systems. Therefore, incorporating VERA into your content management processes involves encryption and access from outside of the repositories. Though this means users need to extract files from content management in order to view and edit, you can automate the security of this content using the VERA SDK.

What is Activity Logging?

VERA captures file-related events, enabling you to see who is accessing your content and what they are doing with it. The Syslog integration is also available for incorporating VERA logs into your organization's logging server.

How does VERA confirm my identity? Authenticate me?

VERA supports several authentication methods, including; Microsoft Active Directory and ADFS as well as Azure Active Directory; Oauth via Google; SAML-based Single Sign-on (SSO) authentication from various Identify Providers (IdP) including Okta, Ping, OneLogin, and Centrify. integration is also available for incorporating VERA logs into your organization's logging server.

Do viewers need to download an application or a plugin to view files?

No. With VERA, viewers do not need to download any client to view files. Authentication (if you require it) can simply happen in the browser. Once a user is authenticated, protections can be applied and viewing of files will simply happen in the browser. You can also give the ability for users to download the file if you wish as well. There are lots of options.

This allows recipients external to the organization the ability to easily access data without having to install any plugins or clients and within their default browser. Authentication is controlled in multiple ways for external users. One example is simply doing email authentication, this is where the user would receive a second verification email.

Users inside the organization usually have the VERA client installed on their endpoint (iOS, Android, Windows, macOS). This allows them to easily access secure files in native applications without having to add any additional steps. Users with a client can also easily manually secure data in multiple ways. This, however, is usually managed through automation by the admins and does not require a client.

Can I update user permissions after I have shared or sent information?

Absolutely. VERA can update recipient rights, even after information has been shared. The VERA admin or file owner can dynamically update the user permissions in bulk (e.g., everyone that has access to the file), or change access controls for specific individual recipients.

Does VERA work with network shares, Box, Dropbox, SharePoint, etc?

Absolutely. VERA has native integrations with Box, Dropbox. What this means is that any file dropped into a VERA secured Box/Dropbox folder is automatically protected with VERA, and we inherit the permissions and access controls from Box/Dropbox. If the file ever leaves Box and Dropbox, VERA permissions stick to the file to make sure it's protected, anywhere it travels.

What's the difference between access control and file security? How does VERA provide "data in use" protections?

Access control is the list of people that can and cannot access your information. VERA security goes a step further allowing you to control your data when it's in others' hands. VERA protects your data as others use it – so you can restrict printing, disable copy/paste, enforce time restrictions – and those protections travel with the file, anywhere it travels, anywhere it's stored.

How does offline access work? If I'm on a plane, how do I authenticate?

First and foremost, IT admins can decide whether or not to grant offline access to files and set how long the file can be offline before requiring that someone re-authenticate with VERA. If you're on a plane, you can open and access secure information easily, as long as you have been granted access and you've authenticated to the VERA cloud before moving offline. Note: offline access requires having a VERA native app installed. To access the web-based experience (browser view), you need to be online.

Can you kill a file or revoke access if the user is offline?

Yes. If a user wants to do anything malicious with a file, they'll have to log back online to email or share it. Once VERA revokes access for a user and that user logs back online, they won't have access to the file. If the user remains offline for an extended period of time, at some point (set by the Admin) they'll be timed out of the app. VERA will force the user to log back online to authenticate, and once they do, access will be denied.

Can you turn off the map feature?

Yes. This is a feature that can be disabled on the VERA dashboard.

Can I use geo-fence my data? Can I use VERA to prevent users in other countries from accessing corporate data?

While VERA provides insight into where your data is accessed, we can't restrict access based on location or set rules preventing users from accessing the data in certain countries. However, you can always dynamically change access to users and revoke or update their access at any time, no matter where in the world they happen to be.

How do you secure file metadata to remain HIPAA compliant?

VERA stores meta-data but our servers never store the content of your files. We are currently working on encrypting meta-data at VERA.

How do you index files for journaling requirements? What happens if the SEC needs secured files for an audit?

Journaling is a compliance requirement where financial services firms have to log and retain any information pertaining to investments. Journaling software needs to be searchable. The concern for firms is that if VERA is encrypting files, how do we search them in the journaling software? VERA can save two copies of the file and send the unsecured copy of the file to journaling software

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.

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.

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.

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.

For more information about Vera, or to schedule a demonstration for your organization, please visit us at **www.vera.com** or find us on Twitter **@veratalk**