VERA

# VERA SECURITY RFP GUIDE FOR DATA-CENTRIC SECURITY

## AN EVALUATION GUIDE FOR SECURING SENSITIVE FILES

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. You can now secure data no matter what device, person, cloud or application creates or receives the data, even if – and after – it falls into the wrong hands.

Current solutions, from on-premise storage to Enterprise Content Management (ECM) to modern enterprise sync and share tools -- like Box, Dropbox, and OneDrive -- can address different parts of this problem. But none have the capability to protect the full lifecycle of enterprise content. Companies regularly store and share information across multiple repositories, and the daily course of business disperses that data across different systems, from CRM to ERP to HRM and even to financial systems. As organizations and individual workers become more continuously productive, IT and security teams need tools that can extend these controls across platforms. Moreover, all of this needs to be done with a focus on simplicity and user experience. By making it simple and transparent to secure and share securely across any repository, organizations can improve adherence to policy and dramatically improve their governance, security and data control posture.

This RFP guide is a comprehensive checklist to evaluate VERA's features and capabilities against your existing solution, or another solution you may be considering.

| BUSINESS PRODUCTIVITY APPLICATIONS | VERA | VENDOR |
|---|---|---|
| Microsoft Word | | |
| MS Excel | | |
| MS PowerPoint | | |
| MS Outlook | | |
| Windows Photo Viewer | | |
| Visio | | |
| Adobe Illustrator | | |
| Adobe Acrobat DC | | |
| Adobe Reader DC | | |
| Adobe Photoshop | | |

| CAD/CAM APPLICATIONS | VERA | VENDOR |
|---|---|---|
| Autodesk AutoCAD | | |
| Autodesk Inventor | | |
| PTC: Windchill Workgroup Manager | | |
| Creo Parametric + Windchill | | |
| Creo View + Windchill | | |

| OS PLATFORMS | VERA | VENDOR |
|---|---|---|
| Windows OS | | |
| macOS | | |
| Android | | |
| iOS | | |

| REPOSITORIES | VERA | VENDOR |
|---|---|---|
| SMB 2.0 | | |
| Box | | |
| Dropbox | | |
| Sharepoint on-premise | | |
| Sharepoint Online | | |
| OneDrive | | |

| ANY DEVICE, ANYWHERE | VERA | VENDOR |
|---|---|---|
| Support for latest versions of Windows OS and macOS | | |
| Native iOS and Android app | | |
| Support for all major browsers: Chrome, Firefox, IE/Edge and Safari | | |
| Ability to view sensitive files on mobile platforms | | |
| Ability to view sensitive files in browser | | |

| | | |
|---|---|---|
| Ability to edit on mobile platforms | | |
| Ability to edit sensitive files on browser | | |
| Dynamic access and permission management via all platforms | | |
| Linux support through browser interface | | |
| Push notification support to desktop and mobile platforms | | |
| Blackberry support via Dolphin browser | | |
| Works with existing MDM solutions with native support for Intune | | |

| GRANULAR CONTROL CAPABILITIES | VERA | VENDOR |
|---|---|---|
| Ability to restrict/grant access to sensitive files on any device | | |
| Ability to restrict/grant access to sensitive files to specific device | | |
| Ability to restrict/grant access while offline | | |
| Ability to restrict/grant access to sensitive files by specific users/groups | | |
| Ability to restrict/grant viewing of sensitive files by specific users/groups | | |
| Ability to restrict/grant access to files via remote connections | | |
| Ability to restrict/grant editing of sensitive files | | |
| Ability to restrict/grant printing of sensitive files | | |
| Ability to secure sensitive files automatically so that users continue to work in the same way as before without new/additional passwords | | |
| Automated ability to leverage data store ACLs to define access rights to sensitive files | | |
| Ability to decouple the encryption keys that enable access to sensitive files from cloud collaboration vendor | | |
| Ability to restrict/grant copying/pasting content from file to external location | | |
| Ability to watermark content | | |
| Ability to restrict/grant screen capture (native and third-party tools) | | |
| Ability to restrict/grant access in virtual environments | | |

| | | |
|---|---|---|
| Ability to restrict/grant access to files and usage for certain time periods | | |
| Ability to “time bomb” access to content | | |

| ACTIVE FILE PROTECTION | VERA | VENDOR |
|---|---|---|
| AES-256 encryption | | |
| Dynamically control user file permissions | | |
| Ability to make changes to access rules on sensitive files at any time - even after file is shared or if it resides on a terminated user’s device | | |
| Ability to revoke access to sensitive files in the event they are shared with an unauthorized user | | |
| Ability to report on failed attempts to access sensitive files | | |
| Permission management is external to the file | | |
| Targeted permission control for users, groups and domains | | |
| File permissions can be easily managed from desktop, mobile and browsers | | |
| Configurable, rules-based engine that provides automated security and access control | | |
| Automated securing and access control for local desktop folders | | |
| Automated securing and access control for Box | | |
| Automated securing and access control for Dropbox | | |
| Automated securing and access control for network shares | | |
| Automated securing and access control for SharePoint and OneDrive | | |
| Automated securing and access control for email attachments | | |
| Automated securing and access control for SDK app integration | | |

| POLICIES, FILE TRACKING AND DEFENSIBLE AUDIT | VERA | VENDOR |
|---|---|---|
| Easy-to-use web-based portal for extensive in-product auditing | | |
| Ability to validate that only authorized external users are accessing sensitive files | | |
| Audit trail of all successful and unsuccessful attempts to access sensitive files | | |

| | | |
|---|---|---|
| Ability to report on access and chain of custody on any sensitive file and its derivatives | | |
| Ability to customize policies | | |
| Ability to audit file access, duration, location and actions | | |
| Ability to audit user logins | | |
| Ability to audit device type, information and access | | |
| Ability to audit system events (admin and connector activities) | | |
| Syslog support | | |
| CSV export | | |

| FLEXIBLE DEPLOYMENT OPTIONS | VERA | VENDOR |
|---|---|---|
| Pure SaaS deployment model | | |
| Allows for hybrid model where infrastructure for protecting/viewing files and key management can be deployed on premise | | |
| VPC option in AWS | | |
| On-premise for federal services and military | | |
| Integrates with ID management solutions (Okta, Google, AD, LDAP) | | |
| SDK allows for integration into 3rd party applications (web apps, DLP, classification, and DMS) | | |
| Integration with existing file share solutions (Box, Dropbox, SMB, SharePoint, OneDrive) | | |
| Configurable to work with enterprise email archiving solutions | | |

| CONNECTORS FOR ENTERPRISE REPOSITORIES | VERA | VENDOR |
|---|---|---|
| Box Connector | | |
| Dropbox Connector | | |
| SharePoint Connector | | |

| | | |
|---|---|---|
| OneDrive Connector | | |
| Okta Connector for Single Sign-on (SSO) | | |

| END-USER DRIVEN FILE SECURITY | VERA | VENDOR |
|---|---|---|
| Intuitive, web-based administration | | |
| Native sharing of sensitive files | | |
| Ability to manually secure sensitive files by 'right-click secure | | |
| Ability to secure one or multiple sensitive files concurrently | | |
| Ability to secure sensitive files automatically so that users continue to work in the same way as before without new/additional passwords | | |
| Ability to have different access rights for users/groups for the same file | | |
| Intuitive onboarding to all supported platforms through HTML browser flows | | |
| Access and editing of secure data in native applications via client | | |
| Access for clientless viewing and editing in browser via the HTML wrapper | | |
| Automatic access for securing supported for attachments sent from Outlook and Mac Mail | | |
| Automatic access and securing integrations when leveraging the following repositories: Box, Dropbox, SMB, SharePoint and OneDrive | | |
| Integrated authentication for: AD, SAML, Google, email, and native | | |
| Seamless key exchange | | |

| PROFESSIONAL SERVICES AND SUPPORT | VERA | VENDOR |
|---|---|---|
| Project Kickoff and Team Alignment | | |
| Business Project Planning | | |
| Line of Business Deployment Planning | | |
| Technical Project Planning | | |
| Technical Architecture Review and Tech Team Engagement | | |

| | | |
|---|---|---|
| Administrator Training and Best Practices | | |
| Tenant Overview - Review with Solutions Architect | | |
| Tenant Configuration Checklist | | |
| Additional Services on Request | | |

## Glossary

| TERM | DEFINITION |
|---|---|
| Access Control List (ACL) | Defines who may open a file, but does not specify what they may |
| Admin Portal | The web portal used by VERA administrators and any other VERA users having a role other than User. |
| Administrator | A VERA user having any role other than User. |
| AES 256 Encryption | The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. |
| Application Programming Interface (API) | A programmatic interface to the VERA Server that enables operations on files transported to the VERA Server. |
| Authentication Configuration | Settings defined for an authentication provider to be used for VERA access. |
| Authentication Rule | Settings that determine under which circumstances an Authentication Configuration will be used. |
| AWS Customer Cloud | A configurable pool of shared computing resources allocated within your own AWS public cloud environment for a VERA deployment. |
| Browser View | Accessing a secure file using a web browser instead of using a compatible app. |
| Connector | A virtual appliance that integrates VERA features with a component of your data center. |
| Core Authoring Applications | We use the term “Core Authoring Application” to refer to applications that end users leverage to develop content. These tend to be more powerful, complex applications like Excel or CAD tools. Customers often require more granular control over specific actions in Core Authoring Apps beyond basic access control. VERA supported provides control over data in use for a number of Core Authoring Applications. See Core Authoring Applications Grid for details. |

| | |
|---|---|
| Dashboard | An Admin/User Portal page that provides important information about VERA users and secure files.do with the files. |
| Data at Rest | Files that are being stored on a writable media (Hard Drive, CD, DVD, USB, Cloud Storage) |
| Data in Transit | Files that are actively traversing a networked environment, email, etc. |
| Data in Use | Files data that is being accessed by a supporting application (Ex. A word document that is open within Microsoft Word) |
| Directory Connector (DC) | A virtual appliance that integrates Active Directory into a VERA system for authenticating VERA users. |
| Encryption | The process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot |
| Edit in Browser (EiB) | Accessing a secure file using a web browser instead of using a compatible app |
| Email Connector (EC) | A virtual appliance that integrates VERA features into your email flow in order to address eDiscovery requirements or support access to secure email from browsers and mobile devices |
| File Conversion | A virtual appliance that converts files to PDF for browser viewing |
| File Share Connector (FSC) | A virtual appliance that integrates VERA features with your organization's preferred file share technology. |
| GDPR | The General Data Protection Regulation ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU |
| Group | A set of VERA users to which you can grant secured file access. You can create local groups in the VERA Admin Portal or import groups from directory services, such as Active Directory. |

| | |
|---|---|
| HIPAA | The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage. |
| Key Store | The database in which file encryption keys are stored. |
| Local Key Store | A virtual appliance that manages the file encryption keys for VERA-secured files. |
| Local Rule | A setting that specifies automatic securing of files in specified folders on a VERA user's desktop. |
| NYDFS | The New York Department of Financial Services (NYDFS) was created by transferring the functions of the New York State Banking Department and the New York State Insurance Department into a new department to reform the regulation of financial services in New York to keep pace with the rapid and dynamic evolution of these industries, to guard against financial crises and to protect consumers and markets from fraud. |
| On-Premise | The act of installing part or all of the VERA environment within a customer maintained facility. |
| PCI | Payment Card Industry Data Security Standard is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment. |
| PHI | Protected Health Information - The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. |
| PII | Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered. |
| Policy | A collection of permissions that define what a user can do with a secure file. |
| Rule | A setting that specifies automatic securing of files. |
| Secure | Using VERA to encrypt a file, wrap it in a VERA HTML shell, and provide an optional policy to control what authorized users can do. |

| | |
|---|---|
| Sensitive Files | We use the term “sensitive files” to describe any file that contains sensitive or non-public information. This includes Intellectual Property (IP), customer data, patient health information (PHI) and personally identifiable information (PII). |
| Shell Doc | The HTML wrapper applied to files secured by VERA. |
| SMB | A protocol (also called Samba) for sharing files on the internet. |
| Software Development Kit (SDK) | A program that you install on a device to enable scripted operations on local files. The SDK performs the VERA Server interactions necessary for securing and unsecuring files |
| Tenant | A separate virtual computing environment in the VERA Cloud or another AWS environment. |
| Total Access Device | A Windows device designated as a location for escrow backup of VERA encryption keys. |
| Total File Access | A permission that enables a user to access all VERA-secured files. |
| Unstructured Data | In our space unstructured data refers to files that reside across a customers employee desktops, network file shares, and cloud collaboration services. |
| User Portal | Web app where VERA users can manage VERA-secured files. |
| User Role | A list of permissions that determines which portions of the VERA system a user is allowed to work with. |
| VERA Client | The VERA Client is the app installed on a user’s device for securing files and managing secure files. |
| VERA Cloud | VERA shared computing resources. |
| VERA for Files | VERA’s core product, which enables securing of files wherever they go. |
| VERA Server | The portion of a VERA deployment that controls VERA features and functions. |
| View in Browser (ViB) | Accessing a secure file using a web browser instead of using a compatible app. |
| Virtual Private Cloud (VPC) | This is a deployment model for VERA that allows our customers to host their own master tenant environment of VERA for use in their large enterprise environment or as a managed service. This is supported in AWS, where their term replaced VPC with AWS Customer Clou |
| Whitelisted App | An app that VERA allows to open a secure file. |

VERA

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.

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