vera
by HelpSystems

SOLUTION BRIEF *(Cybersecurity)*

Always-On File Security That Protects Data Anywhere

Today's organizations are collaborating outside their borders, now more than ever, working on proposals, contracts, and housing customer data, intellectual property, and financial reports that are critical to protect. But consider this – the minute you email or share a file or link, you lose control over how, when, and where that data will be used. You need a way to manage access in real-time, even when the data is in someone else's hands.

How Vera Can Help

Vera secures sensitive data through its entire life cycle, everywhere it travels, no matter who has it or where it's stored. We help you protect confidential data at the point of its greatest vulnerability—when it's being used by others, and while it travels outside your perimeters into unmanaged domains, devices and applications. Built on a scalable, easy-to-integrate platform, Vera attaches encryption, security and policy directly to the data itself, giving security practitioners and IT teams the power to control it, no matter where it goes.

Secure Sensitive Data used by Employees

Secure and track any file, on any device. With a single click, protect documents, presentations, videos or images with AES 256-bit encryption and granular access policies that travel with the file. And with a simple, consistent interface on every platform, Vera promotes secure behavior and dissuades your employees from choosing risky, insecure workarounds.

- Report on which internal users can access sensitive files and any failed attempts.
- Control sensitive files at any time, even after file is emailed, shared, or if it resides on a terminated user's device.
- Control sensitive files in core authoring applications, (e.g., view, edit, print, copy/paste, watermark).

Mitigate Compliance Risks

Regulatory bodies continue to implement rules and penalties related to maintaining privacy and security. Organizations must achieve a state of continuous compliance while allowing business to be executed.

- Files containing PII, PCI or PHI can only beaccessed by authorized users.
- Audit trail of all successful and unsuccessfulattempts to access sensitive files.
- Ability to revoke access to sensitive files, even if they are shared with unauthorized users.
- Your teams have the option to leverage ourSDK and REST APIs to encrypt, track andrevoke access to files.

Leverage Modern Collaboration Securely

Box, Dropbox and SharePoint enable productivity improvements and convenience for knowledge workers, and greatly facilitate information-sharing with external users.

- Control access to sensitive files even after they have been shared with external users via cloud collaboration tools, email, or other means.
- Standardize on a sanctioned cloud collaboration tools without risking vendor's access to sensitive files.
- Employees and external users can collaborate securely via cloud apps.

Active File Protection

File content is always secure, even while in use

- 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.

Easy-to-use

Virtually invisible to end users

- Seamless access for clientless viewing and editing in browser via the Vera HTML wrapper.
- Easy access and editing of secure data in native applications via the Vera desktop client.
- Intuitive onboarding to all supported platforms through HTML browser flows
- Integrated authentication for: AD, SSO and SAML solutions, Google, email and native Vera.

Flexible Deployment Options

Increase overall security of file data by integrating Vera into your own applications

- Pure SaaS deployment model.
- Allows for hybrid model where Vera infrastructure for protecting/viewing files and key management can be deployed on-premise.
- VPC option in AWS for customers with high security postures.
- On-Premise for Federal services and military
- SDK allows for integration into 3rd party applications such as web apps, DLP, classification, and DMS.
- Integrate with ID management solutions such as Okta, Google, AD, LDAP, etc.
- Integration with existing file share solutions such as Box, Dropbox, SMB, SharePoint and OneDrive.
- Configurable to work with enterprise email archiving solutions.

File Activity Tracking

Easy-to-use web-based portal for expansive in-product auditing.

- File access, duration, location, actions
- User login, file access and actions
- Device type, information and access
- System events (admin and connector activities)
- Syslog support
- CSV export

Any Device, Anywhere

Configurable rules-based engine that provides automated securing and access control for:

- Local desktop folders.
- Box, Dropbox, network shares, SharePoint and OneDrive repositories.
- Inherited access control and mapped permissions.
- Email attachments

vera
by HelpSystems

www.vera.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.