FORTRA

**GUIDE** (Vera)

# The Vera Security Architecture

## Secure any Data, Anywhere.

At VeraTM, we believe that enterprise security perimeters are porous and data will travel. In a world of continuous productivity, collaboration across companies and services, and truly productive mobility, it's vital for organizations to confront this shift head-on by attaching security directly to the data itself.

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 how far it travels. Our belief is that it is possible to secure data no matter what device, person, cloud or application it travels to, even if – and after – it falls into the wrong hands.

**"Vera provides one of the most pivotal technologies eluding enterprise IT: A solution truly balancing strong security and simple user experience."**
- Nick Mehta, CEO, Gainsight

Current solutions, from on-premises 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 fully 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 simply extend these controls across platforms.

**Even for organizations with a clear cloud and data control strategy, this fragmentation of sources and sharing services drastically reduces the ability to monitor and control the spread of data.**

Moreover, all of this needs to be done with a focus on user interaction design. By making it simple and transparent to secure and share securely across any repository, companies can improve adherence to policy and dramatically improve their governance, security and data control posture.

Vera's unique security model follows your data wherever it goes. For every individual in your organization, we make it effortless to securely collaborate with anyone, no matter which tools they choose to use. For IT and security practitioners, Vera provides powerful management and oversight in a cloud-based platform that can coordinate and monitor activity independent of where content is stored.

## The Vera Architecture

To address these three requirements and deliver a highly available, flexible and confidential security system that can serve both large and small businesses alike, Vera incorporates three primary components in its platform architecture: a secure cloud platform, a set of end-user clients, and a web-based administration dashboard.

### Vera Cloud Platform

The central component of the Vera service is the cloud platform. 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.

### Vera End User Clients

The end-user clients on mobile devices, Windows PCs and Apple OS X desktops facilitate the encryption, decryption, and policy determination for everything secured by Vera. Through each endpoint, Vera can transparently confirm identity, protect new data as it is created, enforce policy restrictions, and ensure the secure transmission of keys and policy to and from the Vera Cloud Platform. An end-user client permits IT teams to centrally manage access on devices both in and outside the enterprise's control.

### Vera Dashboard

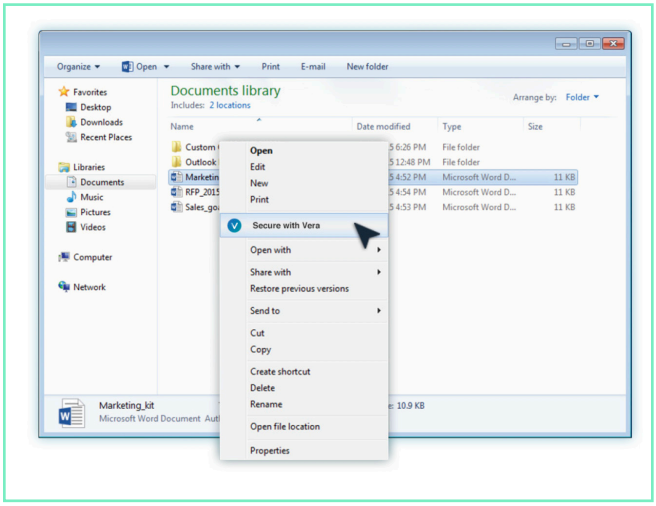
The Vera Dashboard gives both end users and administrators full visibility and control over all the activity around content, no matter where it is stored or how it is transmitted. Through the Vera Dashboard, an admin can manage access controls, set and update policies, oversee users and activity, and run audit reports on usage.

## Securing the Enterprise

Put together, these three components can secure, monitor, and control any type of enterprise data, on any platform. Currently, the Vera Cloud Platform and End User Clients support the encryption and policy management for content - the documents, objects and files most frequently collaborated on by employees.

When a new document is secured with Vera, the client on the employee's device requests a key from the Vera Cloud Platform. A unique key is created for that document, which identifies it in the Vera system and allows it to be associated with a policy and tracked across any repository or device. The key is stored securely on the Vera Platform, and any restrictions in the policy are applied to the document.

These policy restrictions include the ability to control a recipient's ability to Open, Edit, Copy, Share or Save a Copy of the file. All of these activities are logged and tracked by the cloud platform, and are aggregated for viewing in the Vera Dashboard.




## Data Security in Vera

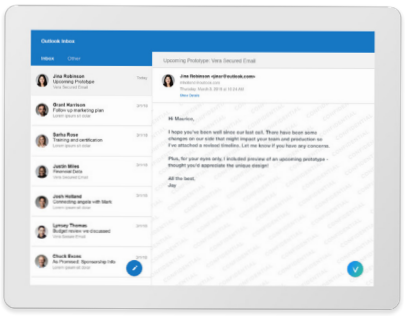
### Secure cloud policy management

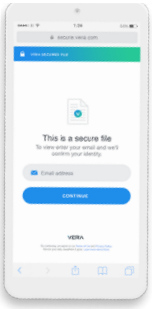
A key tenet of the Vera security model is that our platform never stores customer content or application data in any way. The primary information that lives in the Vera Cloud Platform are the policy definitions and encryption keys, separated logically for each customer. All communication between the cloud platform, device clients and the administrative Dashboard is secured in transit and at rest with at least SSL 2.0 (though TLS 1.2 is preferred) and AES 256- bit encryption.

Each document secured with Vera is encrypted with a unique key that is secured within the Vera Cloud Platform. These keys are transmitted securely via TLS/SSL to the clients which form a trusted key space on the end user's device. Audit logs for every successful and unsuccessful access request to a document are recorded. Keys are not stored locally on the endpoint unless the policy owner specifically grants that privilege for offline or time-bound access. Additionally, Vera End User Clients protect the enterprise against man-in-the middle attacks from custom or forged certificates.

To decrypt and access a protected file, the opposite occurs - a request for a decryption key is sent via the Vera client to the Cloud Platform via TLS/SSL for the specific file. That request is verified against the user permissions and policy restriction for the document, and if access is confirmed, the client is given access to decrypt the file. In the absence of a client, the end user will be given the choice to view the secure file via a browser interface. All access information, including time, identity, action and location are logged for the Dashboard and audit trail. Centralization of policy management and administration is critical, ensuring that copies of documents or edited versions do not lose the original's security. The system will maintain the integrity of the original.

As a result of this design, Vera employees and engineers cannot see customer content, unless the individual has been expressly granted access by a content owner. As a result, customers in even highly-regulated industries trust Vera with their most sensitive data.





## Consistent, Transparent User Experiences The Vera end user client

One of the reasons employees have not adopted traditional data and content security solutions like RMS and DRM is that they require users to change the way they work. Documentspecific settings are disruptive to the process of getting work done and serve as impediments to adoption. People need instant, seamless access to their information, on any device, and at the same time, IT needs to ensure that critical information is protected.

With Vera, IT can deploy a non-invasive, passive client that manages the application and enforcement of policies invisiblyin the background on every user's device. A user with the Vera client installed can open, edit, and share information however they choose without impacting their efficiency or effectiveness. For a user in-policy, opening a secure document is no different than opening any other file.

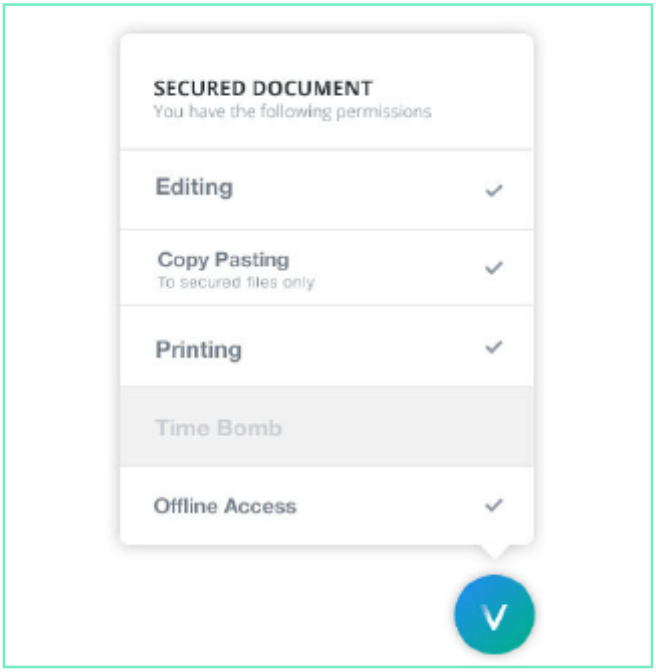
Vera provides native clients for Windows and Apple OS X desktops and laptops, as well as mobile applications for iOS, Android, and Windows 8 tablets. The client is designed with the concept of "smart defaults" in mind, giving users the right nudges and indicators to secure important content as it is created. For access to secured documents away from a trusted device, Vera also provides a web-based document viewer that supports read-only access to content. For desktops, Vera also integrates with popular email clients like Outlook and Apple Mail, allowing users to protect attachments, apply policies, and share information directly from an email.

## The Vera Policy Badge The Vera end user client

An important element of the Vera ecosystem is the Vera Policy Badge, the user experience element that clearly demonstrates a user's access permissions and any policy restrictions on a document. When a secure document is opened, the Vera client overlays a Policy Badge on the document that shows what restrictions are enforced.

These policies can be set broadly, or on a per-document basis, and allow end users and administrators to prescribe granular permissions to documents, including the ability to limit the copy and paste of information into, out of, or across protected files.

Finally, all Vera access points, whether web, mobile or desktop, are integrated with enterprise identity and permissions management tools like Okta and Active Directory, further improving access and transparency in the system. By allowing customers to authenticate users to Vera agents with their existing corporate directory service, Vera streamlines and simplifies the login, access, and provisioning of accounts.

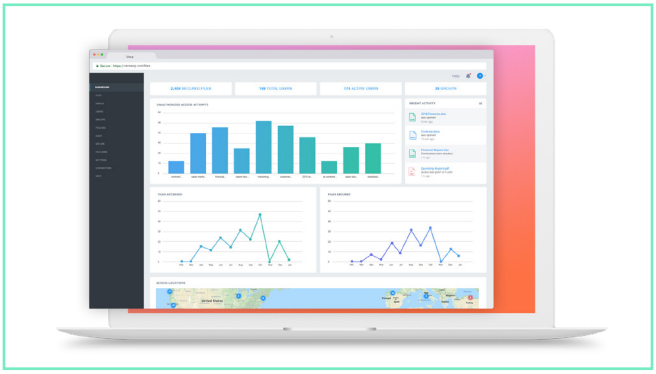


## Policy, User, and Content Administration
### The Vera Dashboard

The Vera Dashboard is the central console where Vera customers aggregate, analyze and take action on all the activity around their data. Returning to the fundamental assumption that perimeter and endpoint security are not enough to protect an organization's sensitive information, Vera gives both end users and IT administrators full visibility and control over all their content, no matter where it is stored or how it is transmitted. Through the Dashboard, an admin can manage access controls, set and update policies, oversee users and activity, and run audit reports. The web-based dashboard provides full visibility and management, and aggregates event data in a simple, powerful dashboard.

The Dashboard also allows an administrator to centrally view all policies in effect by the organization and can also update those policies in real time. This is a critical capability, allowing an admin to instantly revoke access or adjust permissions to documents that have already left the organization's control. An IT admin can also manage user accounts, control groups, create new policies, and view all files secured by Vera.

Beyond simple administration and management, the Vera Dashboard is a powerful analytics and SIEM tool. The Dashboard provides analytics on user adoption, policies in place, and attempted (and more importantly, unsuccessful) accesses to content. In tandem with the Vera end-user clients, this console also can provide insights into attempts to tamper with a client or endpoint in an effort to gain unsanctioned access to information.



## Conclusion

With a centralized cloud architecture that is content and storage agnostic, policy-driven and designed to adapt to modern work practices, Vera allows customers to provide consistent, auditable protection across all their critical content. And, by adopting Vera, organizations of all sizes and in any industry can maintain their existing investments in storage, collaboration, and communication and still improve their security profile.

Vera is a data and content security solution that enhances IT'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.

### With Vera you can:

- Enable employees to work in the tools of their choice, on their terms, without sacrificing security and control
- Extend policy, data governance, and compliance requirements beyond traditional security perimeters
- Secure enterprise data no matter which repository, cloud collaboration platform, or device it resides on
- Automatically apply policy transparently to information created by your organization
- Track, audit, and manage access to confidential information in transit and at rest

FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.