VERA

THE VERA SECURITY ARCHITECTURE

The industry has proven 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 embedding security directly in 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 where it travels. Our belief is that it is possible to 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.

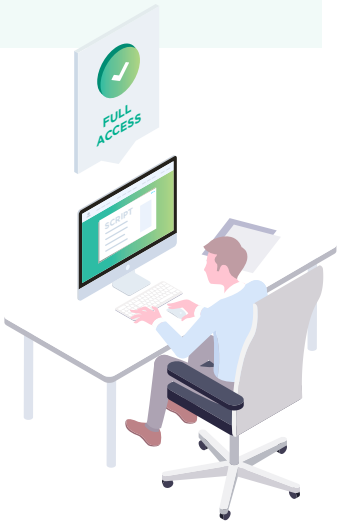
Current solutions, from on-premise storage to Enterprise Content Management (ECM) to modern enterprise sync and share tools -- like Box, Dropbox, and OneDrive -- can address different parts of this problem. But, none have the capability to protect the full lifecycle of enterprise content. Companies regularly 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.

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.

SECURE SENSITIVE DATA USED BY EMPLOYEES

Employees need access to various types of sensitive information in order to perform their duties and support business objectives. Organizations need to ensure that access to sensitive information is limited to the employees who need it in order to do their job.

- 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).



LEVERAGE MODERN CLOUD COLLABORATION SECURELY

Modern enterprises collaborate extensively with 3rd parties. Box, Dropbox and SharePoint enable productivity improvements and convenience for knowledge and greatly facilitate information-sharing with external users. However, these modern collaboration technologies present security risks. Organizations want to mitigate the security risks so they can realize the benefits.

- 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 tool without risking vendor's access to sensitive data.
- Employees and external users can collaborate securely via cloud apps.

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. This is an important and challenging objective.

- Files containing PII, PCI or PHI can only be accessed by authorized users.
- Audit trail of all successful and unsuccessful at tempts 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 the VERA SDK and REST APIs to encrypt, track and revoke access to files.

How We Do It

The VERA architecture is designed to address the challenges created by today's highly collaborative, cloud-based and mobile-centric work environment. Based on the assumption that traditional perimeter - and endpoint-based security solutions are ineffective ways to protect your enterprise's data, VERA provides flexible, transparent data security that is:

STORAGE, TRANSIT, AND DATA AGNOSTIC:

Due to the highly-collaborative nature of business, it is not safe to assume that enterprise data resides solely in controlled systems. A better approach is to design a system that can operate securely, independent of how information is shared or stored. And, to ensure the control, management, and ownership over critical data, the platform must permit any kind of content type to be controlled and monitored consistently.

DATA-CENTRIC AND POLICY DRIVEN:

Secure cloud platforms permit the centralization of policies that govern the management of sensitive enterprise data. By giving organizations central control over access, sharing and collaboration, policies follow the data and can be implemented globally and automatically across the entire organization.

DESIGNED FOR FLEXIBILITY, ADOPTION, AND COMPLIANCE:

In a complex organization, data security is improved through adoption and compliance, and the fastest path to these goals is through useful, flexible and consistent user experiences. Securing data must be simple and transparent, and there must be as little friction as possible for collaborators receiving secured data - no matter what platform.

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 CLIENT:

The end-user clients on mobile devices, Windows PCs and Apple OSX 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.

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

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. Document-specific 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 invisibly in 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

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 copy/paste functions.

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 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.

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.

Additional Features and Capabilities:

DYNAMIC FILE PROTECTION

- Dynamically control user file permissions
- Permission management is external to the file
- AES 256-bit encryption to any file type
- 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.

REAL-TIME ACCESS CONTROL

- Decoupled data and access control
- Real-time management for all file types
- Targeted access for users, groups and domains
- Access control is easily managed from desktop, mobile and browsers

FLEXIBLE DEPLOYMENT OPTIONS

- 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
- Integration with existing file share solutions such as Box, Dropbox, SMB, SharePoint and OneDrive Configurable to work with enterprise email ar chiving solutions