

LEVERAGE MODERN COLLABORATION SECURELY:

HOW TO PROTECT SENSITIVE FILES IN BOX, DROPBOX AND SHAREPOINT

Introduction

Modern enterprises collaborate extensively with third-parties, working on proposals, contracts, and housing customer data, intellectual property, and financial reports. Cloud collaboration vendors such as Box, Dropbox and SharePoint enable productivity improvements and convenience for knowledge workers and greatly facilitate information-sharing with external users. This is exactly why businesses are making the strategic move to the cloud.

However, these modern collaboration technologies can present significant security risks. Users often lose visibility and control once files are uploaded to the cloud. In addition, organizations may have already made significant investments in these tools but aren't able to utilize them because they simply can't secure the data that's put into them. Not only is this a waste of money but it can create productivity issues for both internal and external users. This can also lead to "Shadow IT", where employees use their personal Dropbox or Box accounts to store company information. And that's a huge risk.



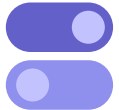
“Vera is geared towards users that already have accounts with Dropbox, Box, Google Drive, and OneDrive but need a way to maintain privacy control of those documents.”

- Ruth Reader, Venturebeat



Secure all your data

Whether your business handles large CAD files, standard Microsoft Office documents, or rich media content like videos, Vera is a content agnostic solution and can secure all forms of data. This means, your business can secure any file type with access policies and dynamic data protection to extend security beyond where they're stored in the cloud. Our most sophisticated teams leverage the Vera SDK/API to build data security into their home-grown applications and secure custom files.



Granular access controls

Not all business relations are equal which means the level of access your partners have to your data shouldn't be the same. Assign access rights and specific permissions that determine how collaborators interact with your files. From full collaboration rights that allow editing, to time-restricted viewing that prevents offline access, gain granular control over how your files are consumed.



360-degree visibility

Vera's dashboard enables you to track, monitor, and get reports on content usage after it leaves your cloud repository. See who's opened your files, monitor whether they've been forwarded and update access permissions in real-time, even after the file has been shared externally. Get full audit trails and activity logs on your organization's content and centrally manage all your confidential files, including email attachments and content that never make it to the cloud.



Active File Security

Realized you sent the wrong file, or a close collaborator is now a former partner? With Vera's real-time access control, instantly revoke access to any Vera-protected file, and take back control even if it's been downloaded, copied, or shared online. Whether an employee leaves or a project with external contractors is completed, change or take back access rights to files with a single click, on any platform or device.



Integrates with your ecosystem

its simple and consistent interface, Vera works across devices and operating systems without impacting the Box or Dropbox user experience. Seamlessly integrated with Box and Dropbox, Vera operates in the background to maintain existing workflows. From the moment files are uploaded to Box or Dropbox, Vera automatically secures your files, giving you a powerful data security fabric for your entire ecosystem and extended enterprise.

ADDITIONAL FEATURES



100% Agentless Edit-in-Browser

According to industry surveys, over 80% of enterprise business users see security as a hurdle to productivity and innovation. Historically, that's the challenge with security solutions. By adding clicks, installs, and friction to workflows, security tools frequently slow down end users and hinder productivity. That's why Vera has always championed a seamless user experience that doesn't sacrifice usability for security. Without downloading any agents, enabling plug-ins, or registering new accounts, users could access and consume Vera-protected files from any device and have an "agentless" experience. However, editing secured files required a lightweight agent.

Vera completely eliminates the friction between security and collaboration and offers the first 100% agentless experience for file security. Without any downloads, users can collaborate on secure files with access controls and dynamic data protections. From time-sensitive documents to highly collaborative presentations, securely move work forward with edit-in-browser.

Vera's dynamic data protection give organizations the power to secure all their mission-critical data and persistently control access to that data, regardless if a teammate forwards it or an external collaborator downloads it. Vera's edit-in-browser capability provides the same level of strong data security and access controls, but in an entirely agentless experience. Now, users can create, share, access, and edit Vera-protected files without ever downloading an agent for an unmatched level of usability and security.



Seamless and Simple for End-Users

Employees struggle to adhere to company security policy especially when productivity requires dynamic collaboration within and beyond the organization. In a complex enterprise environment, employees work across many applications and leverage email, file shares, and the cloud to get work done. Vera's agentless experience allows employees and their external collaborators to securely edit documents, presentations, and spreadsheets regardless of how that content is accessed. This way, your employees can maintain operational agility without risking security.



Centralization of policy management and administration is critical, ensuring that copies of documents or edited versions do not lose the original's security.



Collaboration with Zero Slowdown

The web browser is the tool every organization depends on and the network that connects employees, teams, and external partners. By offering the ability to edit-in-browser, Vera facilitates collaboration in a secure environment. Editing Vera-protected files in the browser allows users to collaborate across and beyond the organization with zero slowdown. Vera's browser-based editing experience provides an unmatched native experience and eliminates any barrier to secured content. That way, employees experience zero slowdown but operate in a secure browser-based editing experience.

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.



The Bottom Line

When sharing files internally and externally using cloud collaboration tools, it's important to have three core components—strong encryption, real-time access control, and hosted policy management.

The moment your documents are uploaded to your chosen cloud collaboration tool, Vera encrypts the files and assigns rights that travel with each individual document. No matter where your content travels – to client sites as an email attachment, to a local desktop or elsewhere in the cloud, only users with the right credentials can open your files in and beyond your cloud collaboration vendor.

For more information about Vera or to schedule a demo for your organization, please visit us at www.vera.com or find us on Twitter [@VeraSecurity](https://twitter.com/VeraSecurity)