VERA

VERA SECURITY SOLUTIONS BRIEF

SECURE SENSITIVE BOARD COMMUNICATIONS WITH VERA

Introduction

Organizations from multiple industries are tasked with implementing secure content collaboration tools, such as cloud storage solutions, and board portals and virtual data rooms (or deal rooms) to secure board books and other, confidential board information. These are necessary to enable use cases that involve key business roles, highly sensitive data and compliance requirements. There has been significant growth in demand for these tools, as well as an increase in regulations on data protection and privacy. In the past, organizations have secured board books and documents by deploying solutions like board portals and virtual data rooms, that can address their specific security requirements.

This brief explores the use cases and required capabilities of board portals and virtual data rooms, the challenges that organizations face with these tools, and VERA's solution to protect board books and other company documents in collaborative environments with strict security requirements.

Overview: Board Portals (BP) and Virtual Data Rooms (VDR)

Board portals and virtual data rooms are highly specialized solutions where companies can store sensitive information and share it with authorized users. Some BP and VDR tools allow secure collaboration among board directors and members, administrators, and management. These solutions might also include digital meetings, the ability to deliver digital meeting materials and board documents to mobile devices such as phones, tablets, and laptops.

BPs and VDRs provide basic features for secure access and collaboration. More specifically, VDRs are used to facilitate the due diligence process during M&A transactions, loan syndications, or private equity and venture capital transactions -- financial transactions that require the exchange of hundreds, or thousands, of documents.

However, these tools are not without significant challenges.

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, or where it's stored.

Challenges of Board Portal and Virtual Data Room Tools

SECURE COLLABORATION FOR INTERNAL AND EXTERNAL USERS

Current solutions, from board portals and virtual data rooms, and 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 secure collaboration. 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.

LACKS INTEGRATIONS WITH OTHER SOFTWARE AND REPOSITORIES

Board portals and virtual data rooms lack integration with Microsoft Office 365, SharePoint, Box, Dropbox, and others. They do not offer a development platform and are too narrowly focused on board-specific use cases when most organizations are highly collaborative and need the ability to work with multiple groups and departments. Companies need content security that enables multiple use cases, working across different platforms and tools.

NARROWLY FOCUSED, EXPENSIVE AND FRAGMENTED

It's common for most companies to invest in multiple point products that have a narrow focus so they can cover each use case. But, BP and VDR applications are often narrowly focused, expensive and fragmented. Complexity and support costs typically grow significantly over time with increased usage. And organizations often struggle to identify the best application among the myriad of different VDR and BP products in the market.

Secure Sensitive Board Communications with VERA

Board Documents in Preparation (or During) for Meetings

Employees and third-parties may sometimes struggle to adhere to company security policies, especially when productivity requires dynamic collaboration within and beyond the organization. In an enterprise environment, users work across many applications and leverage email, file shares, and the cloud to get work done. VERA allows internal and external (as well as third-party) collaborators to securely share and edit board documents, presentations, and spreadsheets regardless of how that content is accessed. This way, your users can maintain operational agility without risking security. By giving organizations central control over access, sharing and collaboration, policies follow the data and can be implemented globally and automatically across all users.

Enable Secure Collaboration

Not all business relationships are equal which means the level of access your partners have to your data should be carefully considered. 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.

View Any File Type from Any Device

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 control, management, and ownership over critical data, the platform must permit any kind of content type to be controlled and monitored consistently.

Secure Sensitive Board Communications with VERA

Data Protection After Board Meetings Are Completed

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 document, and take back control even if the files have 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.

Security, Compliance and Defensible Audit

VERA's dashboard enables you to track, monitor, and get reports on content usage after it leaves your chosen 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.

Seamless and Simple for End-Users

For every individual in your organization, we make it effortless to securely collaborate on board documents 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.

Summary

Most organizations are still distributing information to board members and directors through email, file sync tools, and sharing systems. But 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.

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, or where it's stored. It's imperative that you are able to secure sensitive board documents, no matter what device, person, cloud or application creates or receives that data, even if - and after - it falls into the wrong hands.

For more information about securing board documents with VERA, or to schedule a demo, please contact us at sales@vera.com.

VERA Security
Board Portal and Virtual Data Room Capabilities

Data Protection	• AES 256-bit encryption to any file type to ensure sensitive data can't be accessed by unknown parties. • Control access to sensitive files even after they have been shared with external users via cloud collaboration, email or other means. • Targeted access for users, groups, and domains.
Security Across Third Parties	• Remote deletion of board books and annotations from board members' PCs and tablets. • Access to shared documents can be revoked at any time, even after files have been downloaded. • Third parties can create and keep critical documents in a protected area, with governance such as document retention and audit trails. • Maintain control over access to sensitive files even after they have been shared with external users via cloud collaboration tools, email, or other means.
Secure Collaboration	• Compose documents, meeting agendas, minutes and other sensitive content using your preferred modern applications. • Internal and external parties can work and review sensitive files based on access controls and set policies. • Supports secure international collaboration, even where different data storage, protection, and privacy laws may apply.
Privacy and Compliance	• Granular visibility and centralized control; understand how your content is used, by whom, and proactively investigate unauthorized access attempts. • Policies can be customized to control users' actions such as print, download, view, restricting permissions to users and/or groups. • VERA logs every action taken by any user on a VERA-protected file. • VERA's detailed audit logs provide defensible proof against data breaches.

VERA Security
Board Portal and Virtual Data Room Capabilities

Document Productivity	• Access sensitive files from any device, at any time, from anywhere you are located. • Productivity is not sacrificed when working with secure files. • Board members can receive critical documents in preparation for meetings without concerns of data leakage or theft. • Third parties can create and keep critical documents in a protected area, with governance such as document retention and audit trails.
Flexible Deployment	• Pure SaaS deployment model. • Allows for a 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. • Integration with existing file share solutions such as Box, Dropbox, SMB, SharePoint and OneDrive.
Easy-to-use	• Automatic access and securing integration when leveraging the following file share repositories: Box, Dropbox, SMB, SharePoint and OneDrive. • Seamless access and editing of secure data in native applications via the VERA desktop client. • Intuitive onboarding to all supported platforms through HTML browser workflows.