vera
by HelpSystems

VERA SECURITY WHITEPAPER

TOP 10 USE CASES OF VERA'S DATA-CENTRIC SECURITY PLATFORM

Secure Files in Cloud Collaboration Platforms

With Vera, you can secure any type of file in cloud collaboration tools such as Box, Dropbox, and SharePoint. Using Vera's integrations with these platforms you can seamlessly plug granular control capabilities into these applications to ensure that only authorized parties could access sensitive information. Security policies follow the file allow IT security teams to define granular usage rights that controlled how files were used and distributed, even once they were stored on devices outside of your network. You can then track any file and use granular controls to prevent unauthorized access and revoke privileges at any time.

If data ever leaks or is downloaded from these collaboration solutions, Vera's security sticks to the file anywhere it goes, making sure that only authorized parties are working with your company's information.

WITH VERA YOU CAN CONTROL:

WHO
Who has access to your files (unauthorized access attempts with a full audit trail)

WHAT
What they can/cannot do with them (e.g., edit, view only, block copy/paste, add watermark)

FOR HOW LONG
How long collaborators can access (e.g., automatic time expiration, retention rules, granular revoke access capabilities)

AUDIT
Audit authorized (and unauthorized) access attempts with a full audit trail, anywhere your files travel Gives you total control of your data – even offline.

Secure Sensitive Board Communications

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.

Protect Manufacturing CAD/CAM Files

Many companies in the manufacturing, technology and biotech sectors store sensitive patents, trademarks, customer information and processes across multiple storage platforms - both on-prem and off-prem. Vera has built comprehensive integrations to all of these storage systems to automatically secure any file uploaded or downloaded from those platforms. That way, your employees work exactly the way they normally would, and Vera works seamlessly behind the scenes to protect your IP —everywhere it moves.

You can also leverage Vera's audit capabilities to understand exactly who is accessing R&D throughout the supply chain, track all access attempts (authorized or not, and obtain granular metrics on usage and adoption.

Your CAD/CAM files of product designs, manufacturing specifications, and other documents containing supplier contracts, are all critical to maintaining your organization's competitive edge. And these documents might be stored in a number of different places and platforms. But with multiple stakeholders, shifting production schedules, and a global supply chain, how do you balance keeping up with fast-paced collaboration without losing control over how your data is used?

Vera lets you control how your information is being used, even after it leaves your organization or goes offline. Whether you're sharing manufacturing plans through cloud services like SharePoint Online Box or Dropbox, or over local file shares, Vera ensures only authorized partners can access it. With Vera's dynamic data protection, you have the power to revoke access to any file, anywhere it goes, should you stop working with a vendor.

Secure Sensitive Human Resources Documents

One of Vera's biggest use cases involves securing sensitive employee data, such as human resources documents, payroll information, and recruitment data, among many other types of data in human resources departments. A fast-growth semiconductor manufacturer, faced the challenge of securing sensitive personnel files that were being shared across the business, in multiple locations throughout the world. Specifically, the manufacturer was recruiting top talent from across the globe, in order to grow the business and drive continued product innovation. This required files on candidates and new employees to be shared freely amongst different internal teams, which included personally identifiable information (PII), including names and social security numbers.

Ultimately, Vera was chosen to secure the HR and recruitment files that contained personally identifiable information (PII). Rather than restricting the methods through which users can collaborate and view data, Vera's security is attached to the file itself, allowing teams to work freely across internal applications, email and cloud sharing platforms such as Dropbox, Box, and SharePoint. Authorized users were able to view this information easily – without downloading any agents or plug-ins.

Protect Brand and Asset Data

The media and entertainment industry relies on high levels of protection for their intellectual property, as well as secure collaboration with third parties, to bring new content to market and evolve existing products. By working behind the scenes to encrypt and track files containing sensitive intellectual property, Vera secures the exchange of information across supply chains without negatively impacting workflows.

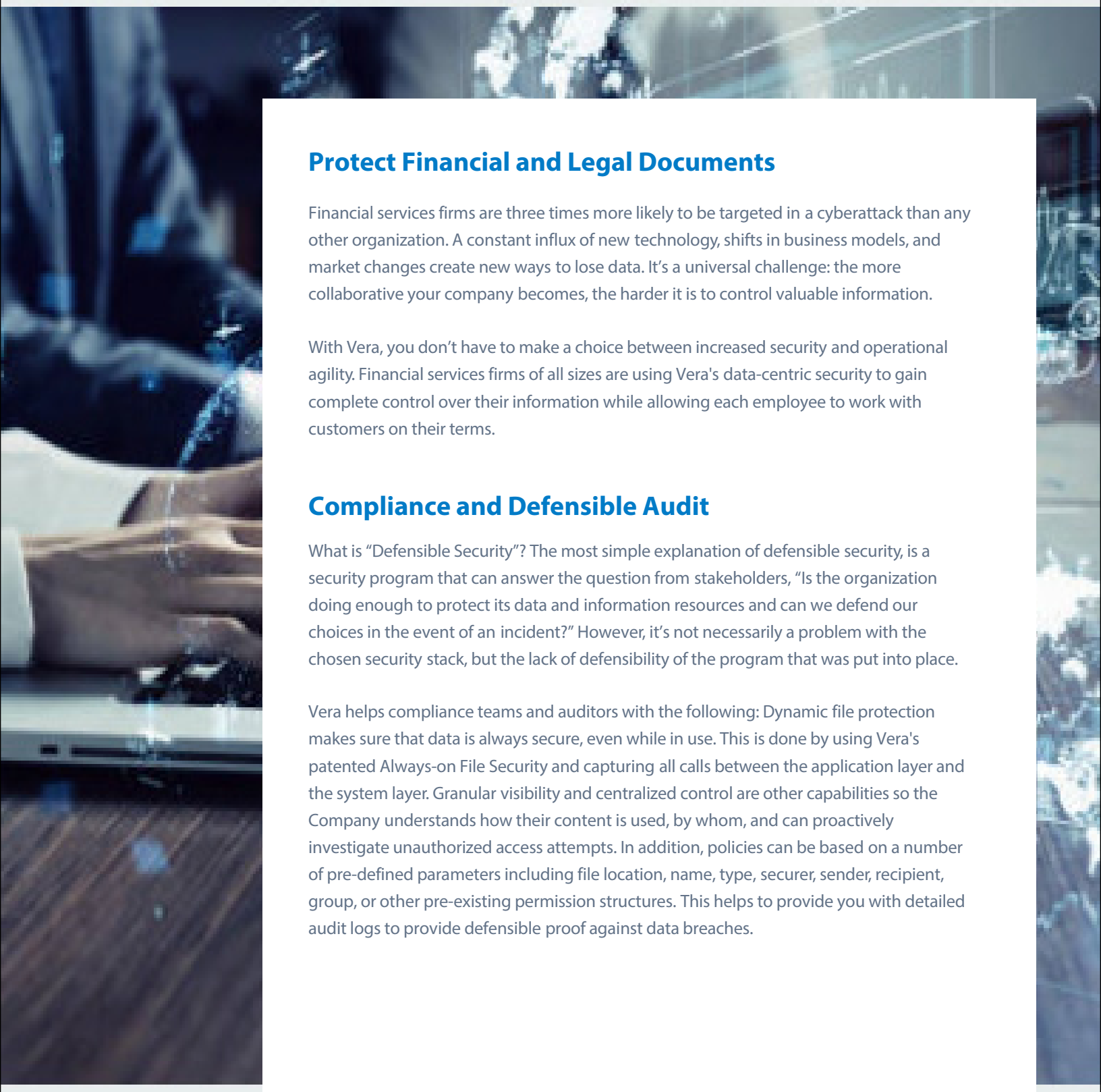
To successfully launch and promote new products, media and entertainment companies often rely on sharing sensitive intellectual property among employees and external stakeholders. They need a secure way to share rich media files, game designs, scripts, and screenplays, or new character ideas, allowing for mass collaboration and dynamic editing over the entire production process.

With Vera, you can secure at the document level using encryption and granular access control permissions that follows that data outside your environment. Collaborators can send information to third parties while retaining control over user access, including which actions are permitted, such as forwarding or copying.

Secure Top Secret Biotech and Pharmaceutical Formulations

Bringing new medical technology to market is a long and complex process, requiring everyone from the administrative staff to R&D to sales and marketing to follow exacting compliance guidelines. Every day, you share privileged information, valuable IP, and regulated documents within and beyond your firm.

With Vera, you have the ability to watermark, track, and report on the secure distribution of controlled documents, even after they've left your organization. As the pressure to innovate faster and accelerate the approval process mounts, protect the security of your data and the future of your business with Vera. Vera's dynamic data protection gives you total control over your sensitive data so only approved parties access your files, no matter where they're stored or when they're accessed, and the confidence that you can revoke access at any time.



Protect Financial and Legal Documents

Financial services firms are three times more likely to be targeted in a cyberattack than any other organization. A constant influx of new technology, shifts in business models, and market changes create new ways to lose data. It's a universal challenge: the more collaborative your company becomes, the harder it is to control valuable information.

With Vera, you don't have to make a choice between increased security and operational agility. Financial services firms of all sizes are using Vera's data-centric security to gain complete control over their information while allowing each employee to work with customers on their terms.

Compliance and Defensible Audit

What is "Defensible Security"? The most simple explanation of defensible security, is a security program that can answer the question from stakeholders, "Is the organization doing enough to protect its data and information resources and can we defend our choices in the event of an incident?" However, it's not necessarily a problem with the chosen security stack, but the lack of defensibility of the program that was put into place.

Vera helps compliance teams and auditors with the following: Dynamic file protection makes sure that data is always secure, even while in use. This is done by using Vera's patented Always-on File Security and capturing all calls between the application layer and the system layer. Granular visibility and centralized control are other capabilities so the Company understands how their content is used, by whom, and can proactively investigate unauthorized access attempts. In addition, 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. This helps to provide you with detailed audit logs to provide defensible proof against data breaches.

Extend the Protection of Cloud Access Security Brokers (CASB)

CASBs have proven to be highly valuable to enterprises on a variety of fronts. At their core, a CASB is able to extend security policy to an enterprise's cloud applications in much the same way a traditional firewall would protect on-premise applications.

Vera protects unstructured data, and a CASB allows you to fulfill the gaps in structured data. From an unstructured data perspective, when Vera encrypts a file in Box, it can break some of the functionality of Box, namely search. You can use a CASB to protect the file as it's sent to Box, and gives the ability to use that file while it's unencrypted, so you have the benefits under their infrastructure. However, when that file starts to egress and leave the company, that's when the CASB would call on the Vera API to extend their protection, encrypt the files, and maintain that ownership of the file, once it leaves the protection of the CASB sphere.

Vera + CASB gives organizations a chance to open up their ruleset so they can be more flexible and still stay secure. With any system, you can lock down information such that it becomes difficult for employees to do their jobs. This is one of the more powerful things Vera offers when we work with CASB solutions - we can give customers the best of both worlds.

Vera + CASB Capabilities

Content Inspection and Apply Policy

Documents residing in a OneDrive folder are sensitive. CASB can run DLP on those files and detect sensitive content. A policy has been defined to protect sensitive documents in Vera, and the CASB solution protects the document by calling the Vera API to encrypt the document.

Inherit App Permissions

Documents in Box folders that are shared for collaboration with external parties are also protected by Vera + CASB solutions. When the CASB detects sensitive documents, Vera policy is executed and the permitted users are inherited from the Box folder collaborators. For example, users that have view-only rights get a policy that is different from the policy that is applied to users that have read-write permissions.

Revise Vera Policies Based on Content

When documents are already protected, the CASB can decrypt the content to be able to apply DLP on the document. When the content scanning is complete and the CASB determines that the Vera policy should be escalated, the CASB will re-apply a new Vera policy based on the sensitivity level of the document.

Visibility and Analytics on Protected Documents

When customers use the CASB's analytics engine to report on Vera protected content, they can see that certain documents are protected with Vera. Administrators can run reports on protected vs. non-protected documents to understand the risk exposure.

Bonus:

The Vera Software Development Kit (SDK)

Many organizations have needs for file security and access control that cannot sufficiently be met with "off the shelf" solutions. As a result, they often build their own custom ("homegrown" applications to achieve their desired objectives.

However, the administration of these custom applications can become expensive. For example, new business requirements or compliance mandates may dictate that a new policy has to be created or updated in the custom application to accommodate the change. This process is expensive and limits the organization's ability to respond rapidly to its business environment.

The Vera SDK enables you to programmatically execute the following tasks on a device: you can secure files, unsecure files, give access to a file for specific users, groups or domains, an revoke access to a file for all users. Using the Vera SDK is the best way to integrate Vera features with your own scripts or applications.

SUMMARY

Vera's dynamic data protection platform is the intelligent, seamless and proactive solution that many firms leverage to secure all corporate data through its entire life cycle. This protection cannot be stripped off the file the moment it's downloaded or opened by a recipient. Your team is empowered to always enforce your company's security control and usage policies on highly sensitive files, even after data is shared outside of your team, downloaded, duplicated or moved to unmanaged domains.

In the event of a breach, whether from an outside actor, intentional misuse, negligence, or just smart people making an honest mistake, Vera gives you the tools to update or revoke access, instantly, to all copies of the file or specific users or vendors.

To learn more or to schedule a demo, please contact us at sales@vera.com.

vera
by HelpSystems

www.vera.com

About HelpSystems

HelpSystems is a people-first so tware 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.