





VERA SECURITY CASE STUDY

VERA SECURES DESIGN FILES OF LARGE FOOTWEAR AND APPAREL MANUFACTURER

Teams are laser focused on protecting the organization’s competitive edge and R&D—product designs, manufacturing specifications and supplier contracts—but to ship successful products, the business must share highly confidential information throughout the supply chain and to employees who may not necessarily be with your company forever.

CASE STUDY OVERVIEW

-  Protect the Company’s pre-release story and product data against leakage and loss.
-  Enable “on-the-fly” protection of files within cloud collaboration tool, Box.
-  Provide a frictionless experience for all users.
-  Seamless integration with the Company’s existing DRM, DLP and CASB tools.

Introduction

A large footwear and apparel manufacturer (“the Company”), headquartered in the United States, was challenged with protecting highly sensitive design files and intellectual property as those files moved internally within the organization, as well as when they were sent to partners and third-parties in different countries. The Company is global, with over 50,000 employees worldwide. These employees work in an agile environment, on different platforms, including Windows and Mac, and use a multitude of file types, including Adobe Illustrator, making security a potentially complicated and challenging endeavor. The Company’s security teams must balance between two competing demands: securing intellectual property and enabling employee collaboration as well as high-speed production efficiency.

This case study outlines three separate use cases describing how the Company currently uses Vera to secure highly sensitive design and product schematics and intellectual property.

DATA-CENTRIC SECURITY

Data-centric security is the ability to secure data through its entire life cycle, everywhere it travels, no matter who has it or where it's stored. The goal is to protect confidential data at the point of its greatest vulnerability—when it's being used in others' hands, and as it travels outside our perimeter into unmanaged domains, devices and applications.

OVERCOME LIMITATIONS OF TRADITIONAL TOOLS

-  Vera secures any kind of file, at rest and in use.
-  Designed for work: Transparent experience, no agents required.
-  Protects data anywhere it travels, on-premise or in the cloud.
-  Gives you total control of your data - even offline.

Use Case #1: Secure Cloud Collaboration

One of the user requirements was that the file security solution chosen by the Company must integrate easily with Box. Cloud collaboration often enables productivity improvements and convenience for knowledge workers, and greatly facilitates information-sharing with external user. However, these modern collaboration technologies can present security risks that the Company's teams knew they needed to address.

If data ever leaks or is downloaded from Box, Vera's security sticks to the file anywhere it goes, making sure only authorized parties are working with the Company's information. From a technical standpoint, Vera decouples the keys from the cloud collaboration tool vendor and provides optionality for key location to be hosted in the Vera service or on-premise. This ensures that the cloud collaboration tool vendor's employees cannot access sensitive files. This also protects against being unaware that sensitive files have been accessed as the result of a subpoena.




Use Case #2: "Man-to-Machine" SDK

As the Company progressed and saw immediate success in their deployments, they decided to upgrade to enterprise licenses and leverage the Vera SDK/API. This was done to weave and build data security into their home-grown and custom applications. With the Vera SDK, machine generated files and custom designs uploaded and shared from home-grown systems or third-party apps are automatically secured - which gives the Company a powerful data security fabric for their entire ecosystem and extended enterprise.



"Vera was the only company that could secure all file types, including atypical files such as Adobe Illustrator, and work with multiple platforms. Our users have a seamless experience, so their workflow isn't hindered, and we're actively looking to expand our deployment across more areas of the Company."

ACTIVE FILE PROTECTION

-  Apply AES-256 Encryption to any file type to ensure sensitive data can't be accessed by unknown parties.
-  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.

Use Case #3: Active File Protection

If the Company needed to send images to retailers in advance of new releases and campaigns, it was important that those images never show up prematurely online or in any other unauthorized way. With Vera, the Company is able to watermark, and prevent screenshots of their designs, as well as control the actions users can take on those files, such as view, edit, print and copy/paste.

This active file protection makes sure that file content 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.

The Bottom Line

Ultimately, the Company chose Vera because it was the only one that could secure a multitude of complex file types on both Windows and Mac, as well as integrate into their existing environment and security stack including Data Loss Prevention (DLP), Digital Rights Management (DRM) and their Cloud Access Security Broker (CASB). It was very important that everything "played nice together", as well as the ability to communicate with their SIEM. Now, the Company is able to secure their intellectual property and design schematics without disrupting workflows and collaboration internally, as well as with partners and third-parties.