VERA

VERA SECURITY CASE STUDY

VERA SECURES BILLIONS WORTH OF INTELLECTUAL PROPERTY FOR FORTUNE 100 COMPANY

Large conglomerates face an uphill battle securing a wealth of sensitive information across internal siloes and expansive supply chains. Information security teams must ensure they have clear visibility into how data shared and retain control of critical files, without slowing down productivity.

COMPREHENSIVE DATA SECURITY

- AES 256-bit encryption protects highly classified files.
- Plug-and-play integrations into Box, Confluence and other applications.
- User-friendly web portal for extensive auditing capabilities.
- SDK and REST APIs provide simplified integration with custom apps.

IRM-as-a-Service

Accessing information rights management through a cloud platform revolutionizes the way that businesses encrypt, manage and govern their data security. Information security teams get visibility into data security across internal teams, divisions and external collaborators – without high costs or onerous deployment processes.

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 perimeters into unmanaged domains, devices and applications.

The Challenge

A multi-industry, multi-national organization of over 300,000 employees, (the "Company"), needed to secure intellectual property and other sensitive data being shared across a highly complex ecosystem. Internal divisions within the Company operated with distinct technology stacks, using the full range of internal and third-party applications to store and share data.

As an information-driven business operating at a large scale, it was critical that employees could effortlessly share sensitive files, such as product designs, across the supply chain to drive new developments. However, new products from high-value industries, such as aviation and software, represent billions of dollars of research and

development (R&D), therefore it was imperative that information sharing had strict security guidelines and enforcement.

The Company needed a single solution that could be leveraged by all divisions to secure and manage any type of file, on any application, wherever it traveled. They turned to Vera, to leverage its unique data-centric security to protect files at their source.

CASE STUDY 1:

CLOUD COLLABORATION PLATFORMS

The Company uses a range of cloud content management services, such as Box. Using Vera's integrations with these platforms they could seamlessly plug military-grade encryption capabilities into these applications to ensure that only authorized parties could access sensitive information.

Security policies which followed the file allowed the IT security team to define granular usage rights that controlled how files were used and distributed, even once they were stored on devices outside of the Company's network. The Vera dashboard allowed them to track any file and use controls to prevent unauthorized access and revoke privileges at any time.

CASE STUDY 2:

PROTECT CAD AND PRODUCT LIFECYCLE MANAGEMENT DATA

The Company recognized Vera's unique ability to protect the valuable intellectual property within computer-assisted design (CAD) files and leveraged its integration with Autodesk's Product Lifecycle Management system.

Teams needed to share confidential product designs with external parties without risking competitors or malicious actors accessing them. Vera's solution protects proprietary information throughout its entire lifecycle, with automated encryption which is transparent to authorized recipients.

The Vera Advantage

- Storage, transit and data agnostic, allowing one solution to secure complex ecosystems.
- Focus on flexibility, leading to high adoption rates and seamless user experience.
- Extends policy, data governance and compliance beyond traditional security perimeters.

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.

As a result, the information security team could enforce strict security permissions that stick to design files wherever they traveled to, securing the innovation that is the lifeblood of the Company.

CASE STUDY 3:

TWO-FACTOR AUTHENTICATION OF CRITICAL DOCUMENTS

Certain documents being shared by the Company with external partners were highly classified and required an additional layer of security. Vera supported this with policies that automatically triggered two-factor authentication confirming the identity of recipients, based on the sensitivity of the file. The Company worked with Vera to achieve the correct balance of user experience and security, protecting the most critical information without slowing down collaboration.

CASE STUDY 4:

PROTECT CUSTOM APPLICATIONS USING VERA SDK

The Company had a range of internal and custom-made applications being used widely by employees to store and share critical information. Using Vera's SDK, they could build encryption, file tracking, policy enforcement and access control into any application. As a result, they weaved security directly into the application stack - either when deploying a new application or retrofitting existing applications.

The Bottom Line

By partnering with Vera, the Company introduced encryption and information rights management across multiple divisions and use cases to greatly improve their data security posture.

The SaaS deployment model meant that employees could freely collaborate with internal and external partners, across the tools of their choice, including Box, Dropbox and Confluence.

The Vera dashboard gives the IT team unprecedented visibility into the state of data security across a large, multifaceted organization. Being able to monitor behavior and control access privileges gives the information security team peace of mind that they are enabling collaboration across the business, without exposing the business to risk.