VERA

VERA SECURITY CASE STUDY

VERA SECURES SENSITIVE PERSONNEL FILES FOR FAST-GROWTH TECH MANUFACTURER

Remaining at the forefront of innovation in competitive high-tech markets is reliant on recruiting the best and the brightest from around the globe to drive ongoing product excellence. Fast business growth requires seamless sharing of personnel files to support recruitment, while protecting the personal data of recruits and employees located across the world, in a wide range of data protection jurisdictions.

CASE STUDY OVERVIEW

- Secure sensitive PII (personal identifiable information) used by recruiters, HR and the executive team.
- Enable secure use of Dropbox and other cloud collaboration services.
- AES 256-bit encryption of all PII without adding friction to end-users.
- Use auditing capabilities for deeper under standing of user behavior.

Privacy by Design

Vera's data-centric solution enables you to leverage the convenience and simple integration of a SaaS platform, safe in the knowledge that your data is kept 100% private. Vera stores encryption keys and policy data only, and never sees the content of your files or views application data. This allows you to safely leverage the Vera Cloud Platform to transform your data security.

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.

Introduction

A fast-growth semiconductor manufacturer, "the Company", headquartered in the United States, faced the challenge of securing sensitive personnel files that were being shared across the business, in multiple locations throughout the world.

Specifically, the Company 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.

This gave the information security team a challenge

– they needed to facilitate the sharing of sensitive information, without risk of unauthorized access to that information. As recruits were coming from across the globe, the Company needed to adhere to strict data protection laws in different geographical jurisdictions.

The Company had 2,000 employees and was growing fast and they needed to put in place processes that were fit for scaling up and hiring for rapid growth. They needed a solution that would solve the immediate issue of sharing recruitment candidate data, but also scale across the rest of the human resources department, as well as other departments that are exchanging sensitive product information with suppliers, partners and customers.

Use Case: Securely Share Personnel Files Containing Sensitive PII Across Teams

The Company needed a solution that did not impede the collaboration between different end-users and groups, both inside and outside the organization. In the past, when IT implemented a solution, unfortunately it proved cumbersome, and users resorted to using their personal file share accounts to get their work done. This is often referred to as “Shadow IT”. The IT department needed a file security solution that met their security requirements, as well as an end-user experience that eliminated most, if not all friction, between internal and external collaborators.

Ultimately, Vera was adopted in order to secure the HR and recruitment files that contained personal 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 in a completely seamless way – without downloading any agents or plug-ins.

ACTIVE FILE PROTECTION

- Deployed AES 256-bit encryption with secure communication of keys via TLS 1.2.
- Provided granular access policies that travel with the file and policies that can be updated in real-time.
- SaaS solution was quick to deploy and simple to integrate with existing technologies.
- Gave the ability to track, manage and audit access to all critical content.

THE VERA ADVANTAGE

- Data-centric protection that secures any file, anywhere.
- Active protection of data as it is used and shared, rather than locking data down.
- Storage agnostic solution that works across Box, Dropbox, Microsoft and on-premise applications.

However, administrators keep total control over who views, downloads, edits or forwards this information to ensure that this information is not compromised.

By making it simple and transparent to securely share these files across any medium, the Company was able to ensure adherence to policies and dramatically improve their governance, security and data control posture.

Solution Recap

The Company's information security team used Vera for a simple, user-friendly way to secure files and manage policies. Critical content is encrypted with a unique key that is secured within the Vera Platform. Keys are transmitted securely via TLS/SSL and used to identify that file, associate it to a defined policy and track it wherever it goes. When authorized personnel accessed the file, a decryption key was sent via the platform, in a way that is totally invisible to the user. All activities are logged and aggregated for viewing on a Vera dashboard.

Using Vera, the Company transformed internal data sharing of sensitive personal data, which supported an urgent mandate to recruit new talent in the semiconductor space. This supported rapid business growth and achieve the continued technological innovation that was the key to their success.
In addition, implementing Vera provided a new level of collaboration across different teams, including information security, HR, product development and the executive team, with better communication about how to fit security controls around end-user requirements. The auditing functionality in the Vera dashboard gave the IT team visibility into how users were consuming and sharing information on a day-to-day basis. As a result, they could ensure that data protection was designed around these behavior patterns, in order to facilitate seamless collaboration while retaining granular control of critical data wherever it travelled, which prevented unauthorized access.