VERA

THE VERA PRODUCT

POKÉMON LEVERAGES VERA'S PLATFORM TO SECURE INTELLECTUAL PROPERTY AND PERSONAL INFORMATION

Media and entertainment rely on high levels of 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 slowing down workflows.

CASE STUDY OVERVIEW

- Secure influx of Personal Identifiable Information (PII) from Pokémon GO.
- Enable secure collaboration across the supply chain.
- Strong encryption of information shared through cloud applications.

SECURE THIRD-PARTY COLLABORATION

- Vera enables companies to collaborate securely with extended teams and third parties.
- Secure sensitive information regardless of how and where it is shared.
- Seamless integration with cloud collaboration tools.
- 360-degree visibility into where sensitive data travels.

Pokémon GO exploded in popularity when it was first launched in 2016 and continues to enjoy high activity levels. Two years after its launch, it saw 5 million daily active users, with over 800 million downloads.

The overnight success of the augmented reality game put the small information security team at Pokémon under pressure, with an influx of users' personal identifiable information (PII).

In addition to securing end-user PII, the Pokémon information security team is responsible for protecting intellectual property relating to its animated TV series, movies, home entertainment, and website.

To successfully launch and promote new products, the business relies on sharing sensitive intellectual property among employees and external stakeholders. They needed a secure way to share rich media files, game designs, and new character ideas, allowing for mass collaboration and dynamic editing over a lengthy production process.

With increasingly complex security requirements, the IT team wished to bake security into business operations in an automated fashion. They adopted Vera to enable seamless collaboration and protect data wherever it resided.

Use Case #1: Protect User Personal Identifiable Information (PII)

Pokémon GO and other games generate a great deal of sensitive user data, including name and locations. With increasingly strict state, federal and international data protection regulations, the Pokémon information security team needed an auditable way to control access to data as it moved across internal systems.

Pokémon deployed Vera to encrypt files which contained PII and track these files wherever they traveled. Each file is encrypted with a unique key that is secured within the Vera Platform. Security policies define which personnel can access these files, and the actions they can perform with this information.

For authorized users, encryption and decryption happens behind the scenes, with no need to download agents, or install plugins to access data. Vera's technology protects against man-in-the-middle attacks, preventing unauthorized access to PII from malicious actors.

Audit logs are available through the Vera Dashboard, showing all successful and unsuccessful attempts to access information. This creates a chain of custody, allowing the information security team to demonstrate compliance to regulations and ensure control of all PII.

Use Case #2: Secure Sharing of Intellectual Property

Pokémon GO and other games genPokémon employees use cloud collaboration platforms such as SharePoint and DropBox to move information between organizational teams and third parties. The security team was confident of controlling information within their own environment but recognized the risk of sensitive files landing in the wrong hands after leaving their network. Rather than restrict information sharing, which employees relied on to perform their jobs, the security team needed a way to retain control of intellectual property stored in cloud platforms or downloaded onto external devices.

With Vera, they could secure at the document level using encryption capabilities that followed data outside the Pokémon environment. Designers could send new artwork to third parties, while retaining control over user access and which actions were permitted, such as forwarding or copying.

Pokémon leveraged integrations with popular cloud sharing applications for swift and simple deployment. By automating the encryption of files shared externally through DropBox and other applications, they avoided issues with user adoption, securing enterprise data no matter which application or device it resides on.

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 key to growing a successful security culture is making it as easy as possible for your employees to behave and do their business in a secure manner. Vera is one of those tools that can help you do that."

"For an international brand like Pokémon, having the tools to enable employees and partners to share information more freely, and securely, is extremely powerful. Our employees are leveraging Vera to do their jobs faster and more effectively, keeping us ahead of the curve." - **John Visneski, Pokémon**

Bottom Line

The strategy of the information security team at Pokémon is to act as business enablers first and security professionals second. Rather than trying to lock down data, or restrict the ways that teams collaborate, they needed a data security solution that made people's lives easier and enabled them to do their job more effectively.

Using Vera, they could automate the encryption of sensitive information in a way that is invisible to users and integrates seamlessly with popular communication platforms. The security team got clear visibility into where data traveled, internally and externally, and gained granular control of how it was used.

This enabled them to protect intellectual property, which is the lifeblood of any organization, while ensuring that user PII is protected as it moved around the organization. The flexibility of the Vera solution gave the security team peace of mind that data is secured no matter what the file type, storage platform or location.

As a result, diverse teams across the company, including designers, finance executives and tournament organizers, could do their job at speed, without compromising security.

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.

SECURE THIRD-PARTY COLLABORATION

- User-friendly approach increases adoption of secure practices across the workforce.
- Facilitates secure collaboration across internal and external teams.
- Automation and simple deployment avoids burdening busy information security teams.