vera
by HelpSystems

事例 *(サイバーセキュリティ)*

Pokémon VERAを活用し、知的財産と個人情報のセキュリティを確保

メディアやエンターテインメントは、新しいコンテンツを市場に投入し、既存の製品を進化させるために、サードパーティーとの高度なコラボレーションを必要としています。Veraは、機密性の高い知的財産を含むファイルを暗号化して追跡することで、ワークフローを停滞させることなく、サプライチェーン全体の情報交換を保護します。

事例概要

- ポケモンGOからの個人特定可能情報（PII）の流入を確保する。
- サプライチェーン全体でのセキュアなコラボレーションを可能にする。
- クラウドアプリケーションを通じて共有される情報を強力に暗号化します。

Pokémon GOは2016年のサービス開始時に爆発的な人気を博し、現在も高いアクティビティを誇っています。発売から2年後には、1日のアクティブユーザー数が500万人、ダウンロード数は8億を超えました。

拡張現実ゲームの一夜の成功により、ポケモンの小さな情報セキュリティチームは、ユーザーの個人識別情報（PII）が流入し、プレッシャーにさらされることになりました。

ポケモンの情報セキュリティチームは、エンドユーザーの個人情報の保護に加え、同社のテレビアニメシリーズ、映画、ホームエンターテイメント、Webサイトに関連する知的財産の保護にも責任を負っています。

新製品の発売と販売促進を成功させるために、この企業は社員と外部の関係者の間で機密性の高い知的財産を共有することに依存しています。リッチメディアファイル、ゲームデザイン、新しいキャラクターのアイデアを安全に共有し、長時間の制作プロセスで大量のコラボレーションと動的な編集を可能にする方法が必要でした。

複雑化するセキュリティ要件に対応するため、ITチームはセキュリティを自動で業務に組み込むことを望んでいました。今日のモバイルワークでは、従業員が企業情報にアクセスする手段や場所を制限することは、もはや現実的な選択肢ではありません。ボーダーレスなIT環境という新しい現実に直面し、リモートワーカーやモバイルワーカーに権限を与える、より柔軟なデータセキュリティのアプローチが必要でした。

セキュアなサードパーティコラボレーション

- Veraは、企業が拡大したチームや第三者と安全にコラボレーションすることを可能にします。.
- 機密情報がどこでどのように共有されるかにかかわらず、機密情報を保護します。
- クラウドコラボレーションツールとのシームレスな統合。
- センシティブなデータの移動先を360度可視化。

ユースケース#1：ユーザーの個人情報（PII）の保護

Pokémon GOをはじめとするゲームでは、名前や場所など、機密性の高いユーザーデータが大量に発生します。州や連邦政府、国際的なデータ保護規制がますます厳しくなる中、ポケモンの情報セキュリティチームは、社内システム間で移動するデータへのアクセスを制御する監査可能な方法を必要としていました。

ポケモンがVeraを導入したのは、個人情報を含むファイルを暗号化し、そのファイルがどこに移動したかを追跡するためです。各ファイルは、Vera Platform内で保護された固有のキーで暗号化されています。セキュリティポリシーは、これらのファイルにアクセスできる担当者と、その担当者がこの情報を使って実行できるアクションを定義します。

許可されたユーザーは、暗号化と復号化が舞台裏で行われ、データにアクセスするためにエージェントをダウンロードしたり、プラグインをインストールしたりする必要がありません。Veraの技術は、中間者攻撃から保護し、悪意のあるアクターによる個人情報への不正アクセスを防止します。

監査ログはVera Dashboardから閲覧でき、情報へのアクセスに成功したものも失敗したものもすべて表示されます。これにより、情報セキュリティチームは規制への準拠を証明し、すべてのPIIを確実に管理することができます。

ユースケース#2：知的財産の安全な共有

Pokémon GOなどのゲーム GenPokémonの社員は、SharePointやDropBoxなどのクラウド・コラボレーション・プラットフォームを使って、組織のチームと情報のやりとりを行っています。サードパーティ セキュリティチームは、自分たちの環境内での情報管理には自信がありましたが、機密ファイルがネットワークを出た後に悪人の手に渡る危険性を認識していました。従業員が業務上頼りにしている情報共有を制限するのではなく、クラウドプラットフォームに保存されている知的財産や外部デバイスにダウンロードされた情報を管理する方法を必要としていました。

Veraでは、ポケモン環境の外でもデータを追跡できる暗号化機能により、ドキュメントレベルでのセキュリティ確保が可能になりました。デザイナーは、新しいアートワークを第三者に送ることができますが、その際、ユーザーのアクセスや、転送やコピーなどのアクションをコントロールすることができます。

ポケモンでは、一般的なクラウド共有アプリケーションとの統合を活用し、迅速かつシンプルな展開を実現しました。DropBoxなど外部で共有されるファイルの暗号化を自動化することで、ユーザーの導入に伴う問題を回避し、どのアプリケーションやデバイスに存在するデータであっても企業データを保護することができるようになりました。

アクティブなファイル保護により、使用中も常にファイルの内容が安全であることを確認します。これは、Veraの特許であるAlways-on File Securityを使用し、アプリケーション層とシステム層間のすべてのコールをキャプチャすることで実現されます。また、きめ細かな可視化と集中管理により、コンテンツが誰にどのように利用されているかを把握し、不正なアクセスの試みを未然に調査することができます。さらに、ファイルの場所、名前、種類、セキュリティ担当者、送信者、受信者、グループ、その他の既存の権限構造など、多くの事前定義されたパラメータに基づいてポリシーを設定することができます。

成功するセキュリティ文化を育てる鍵は、従業員が安全な方法で行動し、業務を遂行することをできるだけ容易にすることです。
Veraはそれを支援するツールの一つです。"

「ポケモンのような国際的なブランドにとって、社員やパートナーがより自由に、そして安全に情報を共有できるツールを持つことは、非常に強力です。社員はVeraを活用して、より速く、より効果的に仕事をこなし、時代の最先端を走っています。"

- ポケモン社 ジョン・ヴィスネスキー氏

Bottom Line

ポケモンの情報セキュリティチームの戦略は、第一にビジネスイネーブラーとして、第二にセキュリティの専門家として活動することです。データをロックダウンしたり、チームのコラボレーションを制限したりするのではなく、人々の生活を便利にし、より効果的に仕事をこなせるようにするデータセキュリティソリューションが必要だったのです。

Veraを使用することで、ユーザーには見えない方法で機密情報の暗号化を自動化し、一般的なコミュニケーション・プラットフォームとシームレスに統合することができたのです。セキュリティチームは、データが社内外を問わずどこに移動しているかを明確に把握し、その使用方法を細かく制御できるようになりました。

これにより、組織の生命線である知的財産を保護し、組織内を移動するユーザーの個人情報を確実に保護することが可能になりました。Veraのソリューションの柔軟性により、セキュリティチームは、ファイルの種類、ストレージプラットフォーム、場所に関係なく、データが保護されているという安心感を得ることができました。

その結果、デザイナー、財務担当役員、トーナメント主催者など、社内の多様なチームがセキュリティを犠牲にすることなく、スピーディーに仕事をこなせるようになったのです。

アクティブファイルの保護

- AES-256暗号をあらゆる種類のファイルに適用し、機密情報が第三者にアクセスされないようにします。
- きめ細かい可視化と集中管理：コンテンツの利用状況を把握し、不正アクセスを未然に防げます。
- ファイルの場所、名前、種類、セキュリティ担当者、送受信者、グループ、その他既存権限構造など、多くの事前定義されたパラメータに基づくポリシーが可能です。

セキュアなサードパーティコラボレーション

- ユーザーフレンドリーなアプローチは、従業員全体の安全なプラクティスの採用を増加させます。
- 社内外のチーム間の安全なコラボレーションを促進します。
- 自動化と簡単な導入により、多忙な情報セキュリティチームに負担をかけない。