KEEPER® + HLG HENSLEY LEGAL GROUP, PC INJURY LAWYERS

ケーススタディ

ヘンズリー法律事務所、Keeperの包括的なパスワード管理ソリューションで機密情報を保護

背景

1998年に設立されたヘンズリー法律事務所 (Hensley Legal Group, PC) は、インディアナ州インディアナポリスに拠点を置く、確かな実績を持つ人身傷害専門の法律事務所です。同社は、人身傷害、車両事故、社会保障障害事例を専門としており、顧客が適正な和解や判決を得られるように支援しています。インディアナ州に所在する複数のオフィスで、思いやりのある法的代理人の提供に専念するとともに、「ヘンズリー・ケアーズ」などのイニシアチブを通じて、地域社会への貢献も積極的に行っています。

業種
法務 (法律事務所)

従業員
150人以上

ソリューション
Keeperパスワードマネージャー

- エンタープライズ
- BreachWatch®
- 高度なレポートとアラート
- コンプライアンスレポート
- シルバーサポート

課題

インディアナ州で成長を遂げている人身傷害専門法律事務所のヘンズリー法律事務所では、社内全体のパスワードセキュリティ管理の問題が深刻化し、対応が困難になっていました。Keeperを導入する前は、従業員が個人のメールアカウントを使用したり、メールやMicrosoft Teamsなどの安全でない手段を使用してパスワードを共有するなど、パスワードの管理に一貫性がありませんでした。

以前は、従業員のパスワードの使用状況やセキュリティの可視性が限られていました。従業員によっては、以前勤務していた法律事務所や個人アカウントのパスワードをそのまま再利用することが多く、セキュリティ侵害のリスクが懸念されていました。そうしたことから、パスワード管理を改善し、社会保障番号や医療記録などの機密性の高い顧客データを保護するためのソリューションが必要とされていました。

パスワード管理における実情 - Keeperを導入する前は、パスワードを個人アカウントとビジネスアカウントの両方で、共有スプレッドシートや共有フォルダに保存するなど、一貫性がない状態でした。この方法では、特に共有アカウントや重要データを扱う場合に、セキュリティ上のリスクや業務の効率性が失われる原因となっていました。

コンプライアンスと倫理上の考慮事項 - 人身傷害を専門とする法律事務所であるヘンズリー法律事務所では、機密性の高い医療記録や個人情報を扱っており、機密性の高い顧客データを保護する倫理的責任を十分に認識していました。こうした背景から、パスワードセキュリティに積極的に取り組み、データ、ファイル、顧客情報を安全に保護したいと考えていました。

クラウドへの移行に伴うセキュリティリスクの 増加 - クラウドベースのインフラに移行したことで、どこからでもシステムにリモートアクセスできるようになりました。しかし、それにより、認証情報を安全なソリューションで適切に管理していない限り、不正アクセスの可能性が高まることを意味しました。そのため、この新しい環境でパスワードやパスキーを保護し、機密性の高い案件情報を保護するための包括的なソリューションの必要性を認識しました。

> **クラウド移行後、確実にパスワードを管理できるソリューションが必要でした。Keeperのサポートは素晴らしく、セットアップ手順も分かりやすいものでした。**
>
> **ライアン・クレイカー | IT&インターネットマーケティング担当ディレクター**

Keeperソリューション

ヘンズリー法律事務所では他のパスワード管理ソリューションも検討しましたが、優れた機能、セキュリティインフラ、ITプロバイダとの試用期間中の良好な体験を理由に、Keeperの導入を決定しました。

既存システムとのシームレスな統合: Keeperを選択した主な要因は、シングルサインオン (SSO) でのMicrosoft Azureとの**統合機能**でした。SSOを活用することで、Keeperプラットフォームにアクセスする際に個別のパスワードが不要になり、その結果、使いやすさもセキュリティも向上しました。また、Keeperの**ブラウザ拡張機能**をすべてのブラウザに導入し、どのデバイスからでも簡単にパスワードを管理できるようにしました。

パスワード管理の一元化: Keeperへの移行は簡単でした。Keeperのインポートツールを使用して、チームのスプレッドシートに保存されていたパスワードをKeeperボルトへと移行しました。また、Keeperの**BreachWatch®**機能を活用して脆弱なパスワードを特定して改善することで、保存されている認証情報がすべて高い安全基準を満たしているようにしました。

役割に応じたアクセス制御 (RBAC): Keeperでは、役割に応じたアクセス制御 (RBAC) を活用して共有ルールをきめ細かく設定するなど、組織全体のセキュリティポリシーとコンプライアンスの遵守を支援します。組織内での役割を設定することで、管理者のプロビジョニング作業が効率化し、さらに特定のルールを利用することで最小特権アクセスを維持しつつ組織のセキュリティ態勢を強化できます。

ユーザーへの導入とトレーニング: Keeperは使いやすく迅速に導入できるように設計されており、あらゆる規模の組織に対応可能なパスワードマネージャーです。Keeperの**ドキュメントポータル**では、詳細な手順とシステムのベストプラクティスを含む膨大な情報を公開しており、管理者がKeeperを導入する際にご活用いただけるようになっています。エンドユーザー向けには、使用法ガイドと**トレーニング動画**をご用意していますので、従業員の高い導入率につながります。

最高水準のセキュリティ: Keeperのゼロトラストおよびゼロ知識セキュリティアーキテクチャは、情報の保護とデータ漏洩のリスクの軽減に優れており、デバイスレベルの楕円曲線暗号 (ECC) と多層暗号化 (ボルト、フォルダ、レコードレベル)、多要素認証と生体認証、さらにFIPS 140-3で検証済みのAES 256ビット暗号化およびPBKDF2が組み合わされて活用されています。Keeperは業界で最も長い間**SOC 2とISO 27001**に準拠しているだけでなく、FedRAMPおよびStateRAMPの認証も取得しています。

> **何よりも従業員がパスワードを知る必要がなくなったことで、フィッシングやハッキングのリスクが大幅に低減しました。**
>
> **ライアン・クレイカー様 | IT&インターネットマーケティング担当ディレクター**

組織への効果

Keeperの導入で、組織全体の安全性と効率性が向上するなど、劇的な効果がありました。主な向上点としては、以下が挙げられます。

セキュリティとデータ保護の向上: Keeperの堅牢なセキュリティアーキテクチャにより、従業員がパスワードを覚える必要がなくなったことで、セキュリティが劇的に改善しました。Keeperを使用することで、パスワードは自動的に生成され、安全に保存されるため、従業員はフィッシング攻撃などのサイバー攻撃の脅威から保護されます。

Keeperはパスキーにも対応しており、ボルトに保存したパスキーを用いて簡単に認証できるようになりました。ITチームでは現在、全従業員のパスワードの複雑さやその取り扱い方について完全に可視化できるようになり、BreachWatch®によるダークウェブモニタリング機能でセキュリティに対する脅威を監視できるようになりました。これにより、すべての認証情報が不正アクセスから確実に保護されるようになりました。

実装とサポートの容易さ: 組織全体へのKeeperの導入作業はスムーズに進みました。ITチームにとってセットアップ手順がわかりやすかっただけではなく、Keeperのサポートチームからは導入期間全体を通して十分なサポートが得られました。

100人を超えるユーザーを以前のパスワード管理方法から移行させるのは難題でしたが、包括的なトレーニングとリソースのおかげで、スムーズな移行が可能となりました。また、新入社員に対しては、入社初日からKeeperをデフォルトのパスワード管理ツールとして使用するため導入プロセスは簡素化されました。

従業員の入社時と退職時の処理を効率化: Keeperを使用することで、ITチームでは新入社員の入社時や従業員の退職時に認証情報を手動で共有する必要がなくなりました。Keeperの共有フォルダ機能により、人事上の変更に迅速に対応し、パスワードを更新するだけでなく、転送や共有も安全に行えるようになりました。

> **従業員が退職する際には、その従業員のパスワードを共有フォルダに転送することで、チーム全体のパスワードをリセットすることなくアクセスを管理できます。**
>
> **ライアン・クレイカー様 | IT&インターネットマーケティング担当ディレクター**

コラボレーションの向上: 弁護士とケースマネージャーの間で認証情報を安全に共有できるようになったことで、部門間のコラボレーションが強化され、セキュリティを損なうことなく複数のアカウントを管理しやすくなりました。Keeperを組織全体に展開することで、業務効率が大幅に改善されました。

ポジティブなフィードバックとユーザーの導入: Keeperの使いやすいインターフェースのおかげで、高い導入率が実現しました。その結果、パスワードに関連したヘルプデスクチケットが大幅に減少し、安全かつ組織的なパスワードおよびパスキー管理が可能になりました。

Keeperパスワードマネージャー

ほとんどの企業では従業員のパスワードの利用状況が可視化されておらず、サイバーリスクが高まっています。パスワード管理を改善するには、パスワードの利用状況とコンプライアンスに関する情報が不可欠となります。Keeperでは、究極のセキュリティ、可視性、コントロール機能でこの問題を解決します。

データは、Keeperのゼロ知識セキュリティアーキテクチャと最高水準の暗号化技術で保護されます。ゼロ知識とは、ユーザーだけが自分のマスターパスワードと暗号化キーを知っており、それを使って情報を暗号化・復号化できる仕組みです。

Keeperは操作性に優れ、導入も簡単です。事業の規模に関係なくお使いいただけます。また、Active DirectoryおよびLDAPサーバーと連携させると、プロビジョニングとオンボーディングを効率的に行えます。**Keeper SSOコネクト®**はFedRAMPおよびStateRAMPの認証を受けており、既存のシングルサインオンソリューションとの連携を実現します。

Keeperは組織の成長に合わせて拡張できるようにデザインされています。役割別の権限設定、チーム間共有、部署別監査、管理権限の委任などの諸機能で組織の成長を支援します。**Keeperコマンダー**のAPIにより現在使用中のシステムだけでなく将来使用するシステムにも統合が可能です。

ビジネスでの活用事例: Keeperパスワードマネージャー

- パスワード関連のデータ漏洩やサイバー攻撃を防止
- パスキー対応で手間のかからない認証を実現
- コンプライアンスの強化
- 従業員の生産性の向上
- パスワードポリシーの遵守
- ヘルプデスクにかかるコストを削減
- 迅速な導入でトレーニングを削減
- 従業員のセキュリティに対する意識と行動が向上

Keeperについて

Keeper Securityは、次世代の特権アクセス管理で、世界中の人々と組織のためにサイバーセキュリティを変革する製品を開発しています。Keeperのサイバーセキュリティプラットフォームは、ゼロトラスト・ゼロ知識セキュリティを採用しており、使用するデバイスにかかわらずすべてのユーザーを保護します。Keeperは、多くの個人ユーザー、企業や組織から信頼を得ており、パスワード管理、シークレット管理、特権アクセス、リモートアクセス、暗号化メッセージで業界をリードしています。詳しくは、KeeperSecurity.comをご覧ください。

Keeper は世界中の何千もの企業と何百万もの人々から信頼され、愛されています。

G2
Enterprise Leader

PCMag
Editor's Choice

App Store
最高評価の生産性

Google Play
1000万以上のインストール