KEEPER
Cybersecurity Starts Here

ケーススタディ

grand river Health

医療システムにおけるパスワード管理の問題を解決

KEEPER®

成長を続ける地域的なヘルスケアシステムは、ヘルスケアにおける厳格なプライバシーとセキュリティルールの中で、パスワードのロールベース許可を管理できる信頼性の高い方法を必要としていました。

課題

- データのプライバシーとセキュリティに関する厳格な要件
- 紙のパスワードリストが使えなくなった
- ヘルプデスクにパスワード関連の問い合わせが大量に発生

ソリューション

- ロールベースのパスワードマネージャー
- ゼロ知識セキュリティと 2FA による不正アクセスからの保護
- 組織体制やポリシーに合わせたカスタマイズが可能

結果

- より強固なデータセキュリティ
- 効率性の向上
- データアクセス制御の改善

© 2019 Keeper Security, Inc.

グランドリバー病院地区について

グランドリバー病院地区とは、コロラド州西部のライフル市を中心とした約 3800 平方キロメートルの地域で患者を診療する地域医療システムです。この地区では、550 人以上の職員と 100 人以上の提携医が、5 つの医療施設、長期介護施設、学生向け医療施設に勤務しています。

課題

1962 年に最初の病院を開設して以来、グランドリバー病院地区（GRHD）は、何百人もの従業員を雇用し、毎年何千人もの患者を治療する、地域にとって不可欠な存在へと成長しました。GRHD が拡大し、医療データのプライバシーとセキュリティの要件が高まるにつれ、情報技術（IT）部門は、組織のパスワード管理方法がもはや機能していないことに気づきました。

> **「プライバシーとセキュリティの要件が高まるにつれ、従来のパスワード管理方法はもはや機能しなくなりました。」**

「私たちは紙のマスターパスワードリストでは不十分なほど大きくなりました」と、GRHD ネットワークエンジニアの Daniel Wilson 氏は言います。「私たちのシステムはより複雑になっており、パスワードのロールベースの許可とそれらを安全に保つためのより優れた方法が必要でした。紙のパスワードリストでは対応しきれなかったのです。」パスワードのリセットも問題となっていました。多くの組織と同様、IT ヘルプデスクへの問い合わせの約半数はパスワードを忘れたことによるもので、多忙な Daniel 氏のスタッフには大きな負担となっていました。

Daniel 氏と彼のチームがパスワード管理ソフトウェアを検討し始めたとき、いくつかの機能の必要性を念頭に置いてました。セキュリティとロールベースの許可を筆頭に、パスワードを簡単にインポートとエクスポートする機能、すべてのプラットフォーム（特にモバイル）からのパスワードマネージャーへのアクセス、そしてオフラインでのパスワードボルトへアクセスする機能を求めていました。

Keeper のソリューション

Keeper の設定可能なロール、ロールベースの許可、管理特権は、組織階層にすべて従って割り当てることができるので、GRHD に完璧にフィットしていました。Daniel 氏と彼のチームは、ロールと責任に基づいたきめ細かなアクセス制御を通じて、従業員の許可を完全にカスタマイズすることができます。

> **「Keeper ソリューションは、ゼロ知識アーキテクチャで構築されています。」**

セキュリティ面に関しては、Keeper がすぐに目立ってきました。このソリューションはゼロ知識アーキテクチャに基づいて構築されており、ユーザー以外は記録にアクセスできないので、データを完全に制御することができます。Keeper では、ユーザーがボルトにログインする際に、ユーザーのデバイス上でだけ暗号化と復号が行われます。

Daniel 氏と彼のチームにとって、Keeper の二要素認証（2FA）も強力なプラス要素となっていました。Keeper は DUO Security と提携し、ユーザーがウェブサイトやアプリケーションにログインする際に追加の保護レイヤーを提供します。GRHD の IT 管理者は、あらゆる場所、あらゆるデバイスにおけるあらゆるユーザーのログイン試行をモニタリングし、不正アクセスを防止することができます。

Daniel 氏のチームは、Keeper が GRHD の厳格なセキュリティ基準をクリアしていて、優れたモバイルエクスペリエンスを備えた唯一のパスワードマネージャであることを知りました。従業員がどのデバイスやプラットフォームを使用していても、記録は自動的に同期され、オンラインとオフラインにおける完全なアクセスを提供します。Keeper ソリューションは、医療システムの組織構造とポリシーにサービスを適合させることで、GRHD の IT ヘルプデスクにかかってくるパスワードリセットを求める電話の負担を軽減することもできます。

© 2019 Keeper Security, Inc.

結果

Keeper パスワードマネージャーソリューションにより、GRHD は厳しい HIPAA 要件に対応でき、IT チームは組織の増加するスタッフのパスワードを簡単かつ効率的に管理することができるようになりました。「Keeper ボルトは、特権アカウントクレデンシャルのライフサイクルを安全に管理することができます」と Daniel 氏は言います。「新しい人が入ってきたら、IT 部門は必要なものへのアクセスを徐々に与えることができ、また、いつでも撤回することができます。Keeper は、パスワード、ウェブサイト、アプリケーションへのオンデマンドアクセスを従業員に提供し、クラス最高峰のセキュリティで GRHD と患者を保護しながら、従業員の生産性を向上させてくれます。」

影響

GRHD は地域の主要な医療機関として、患者のプライバシーと健康データを保護する責任を負っています。データ漏洩の 81 %が脆弱なパスワードによるものであることから[1]、強固で信頼性の高いパスワード管理は、患者の信頼を獲得し、良好な評判を維持するために不可欠です。

> **「脆弱なパスワードセキュリティは、データ漏洩の 80%以上につながる。」**

Keeper は GRHD にパスワード管理における実用的で拡張性のあるアプローチを提供したので、組織が成長しても貴重な情報を保護することができるようになりました。

Keeper について

Keeper Security は、企業やクライアント情報を保護するための最先端のパスワードマネージャーとセキュリティソフトウェアを開発しています。Keeper は、あらゆる業界のあらゆる規模の企業と連携し、データ漏洩のリスクを軽減し、データセキュリティとプライバシーを強化し、従業員の生産性を高め、サイバーセキュリティレポートとコンプライアンスを強化します。

Keeper Security の最先端のパスワードマネージャーとセキュリティソフトウェアの詳細については、**keepersecurity.com** をご覧ください。

[1] ベライゾンデータ漏洩調査報告書、2017年版

REV 6.25.19 © 2019 Keeper Security, Inc.