KEEPER SECRETS MANAGER

最新版規模に応じたシークレット管理 Keeperシークレットマネージャーの診断ガイド

効果的なシークレット管理と
ゼロトラストセキュリティの実現

はじめに

今日のクラウド環境と IT の仮想化環境は、組織が絶えず変化するユーザーの需要に合わせて対応し、これまでにない運用効率を実現し、厳しさを増しているサイバー環境においても競争力を維持することを可能にしています。企業全体で、クラウドソースへのアクセスがシームレスでユビキタスであることの必要性は、あらゆる数の部門やグループで同様に感じられています。たとえば、セキュリティスタッフやオペレーターには、API キー、データベースパスワード、証明書などのインフラ関連のシークレットをロックダウンするためのツールが必要ですが、開発者は、CI/CD パイプライン、構成、ソースコートあるいはソフトウェアのモジュール全体で認証情報を調整するためのメカニズムを必要としています。最後になりましたが、企業ユーザーは、パスワードや認証情報、ファイル、共有されたシークレットを合理化された使いやすいインターフェースに保存するための、適切なプラットフォームを必要としています。

適切に管理されない場合、こうした多様なエンタープライズのユースケースや、異種混合で分散されたインフラストラクチャの複雑さのために、シークレット管理プロセスが破損または無効になったり、攻撃対象領域が拡大したりします。これは、欠陥したセキュリティ体制の前兆としてよくあるものです。サイバー犯罪者にとって、特権認証情報とシークレットは驚くほど価値の高いターゲットです。実際、脅威アクターは、特権システムへの不正アクセスを得るために、誤って構成された可能性のあるサーバーやハードコーディングされたシークレットで漏洩したクラウド環境を故意に標的にしています。

以下では、管理ミスで発生したシークレットやキーの漏洩に関連する目立ったインシデントをいくつかご紹介します。

- 2022年4月、GitLab はクリティカルアップデートを発表し、アカウントにパスワードがハードコーディングされたことを報告しました。
- 2022年4月、Cisco は Cisco Umbrella クラウド型セキュリティサービスに対するクリティカルアップデートをリリースし、デフォルトの SSH キーを使用すると管理者の認証情報が盗難される可能性があることが明らかになりました。
- 2022年4月、Heroku および Travis-CI 0auth トークンがアップストリーム攻撃で盗まれたことを受けて、GitHub はハッキングされたことを発表しました。
- 2022年2月、ハードコーディングされたパスワードを含む重大なセキュリティ上の欠陥が、ネットワーキング企業の先駆者である Moxa の MXview ウェブベースネットワーク管理ソフトウェアで発見されました。

これらは、高度な技術を備えたセキュリティチームや DevSecOps プラクティス、最新のソフトウェア開発プロセスを導入している成熟した組織にとっても、適切なシークレット管理が困難であることを示す最近の例のごく一部です。

より優れたシークレット管理の必要性

管理が不十分なシークレットは、常に攻撃対象領域の増加や侵害のリスクにつながるため、シークレット管理を改善することは、すべての組織にとって継続的な基盤であるべきです。しかし、これは企業にとって規模を問わず複雑な問題です。シークレットは、多くの場合、組織全体に分散されて保存されているためです。

独自の社内ソリューションを構築している企業は、カスタム開発のアプリケーションにハードコーディングされたシークレットを持つ場合があります。さらに、シークレットが、プレーンテキストの設定ファイルや S3 バケット、CI/CD ツールあるいはプラットフォーム、ソースコードリポジトリ、個々の開発者ワークステーションなど、どこか別の場所に存在あるいは散在している場合があります。ほとんどの開発チームが、シークレットの管理と保護に関連するタスクへの取り組みに苦戦し続けているのも不思議ではありません 。

ハイブリッドおよびマルチクラウドの課題

ハイブリッド環境やマルチクラウド環境を既存のインフラストラクチャに統合することは、シークレット管理に関する問題をさらに悪化させることになります。シークレットが環境ごとにデータストア全体で複製され、共有されることになる可能性があるためです。管理者は、シークレットが使用された位置や過程を把握していない場合があります。さらに、クラウドベンダー間のニュアンスやクラウドスタックの違いにより、シークレットが更新あるいはローテーションされないことになる場合もあります（データベースパスワード、API キー、期限切れ証明書など）。その結果、企業は、クラウド環境全体のシークレットを調和させるために、生産システム全体を停止させる必要が生じる場合があるのです。

既存のソリューションは、これらの課題にさまざまな方法で対処します。しかしその多くは、結局のところ、ある課題を別の課題にすり替えるものであるため、組織が以前と比べて改善されたことにはなりません。たとえば、ソリューションの中には、シークレットを保存するためのホストされたボルトサーバーで構成されるものがあります。他には、ストレージエンジンやピアリング高可用性（HA）で構成され、必要な時にいつでもシークレットにアクセスできるものもあります。主要なソリューションの中には、インフラストラクチャでプロキシサーバーのインストールを規定しているものさえあります。それは、継続的な管理やメンテナンス、セキュリティの更新あるいはパッチ適用が必要な、脆弱でありうるサーバーを新たに展開することになるため、最終的には環境にさらなる複雑性をもたらす要件です。

Keeperシークレットマネージャー のご紹介

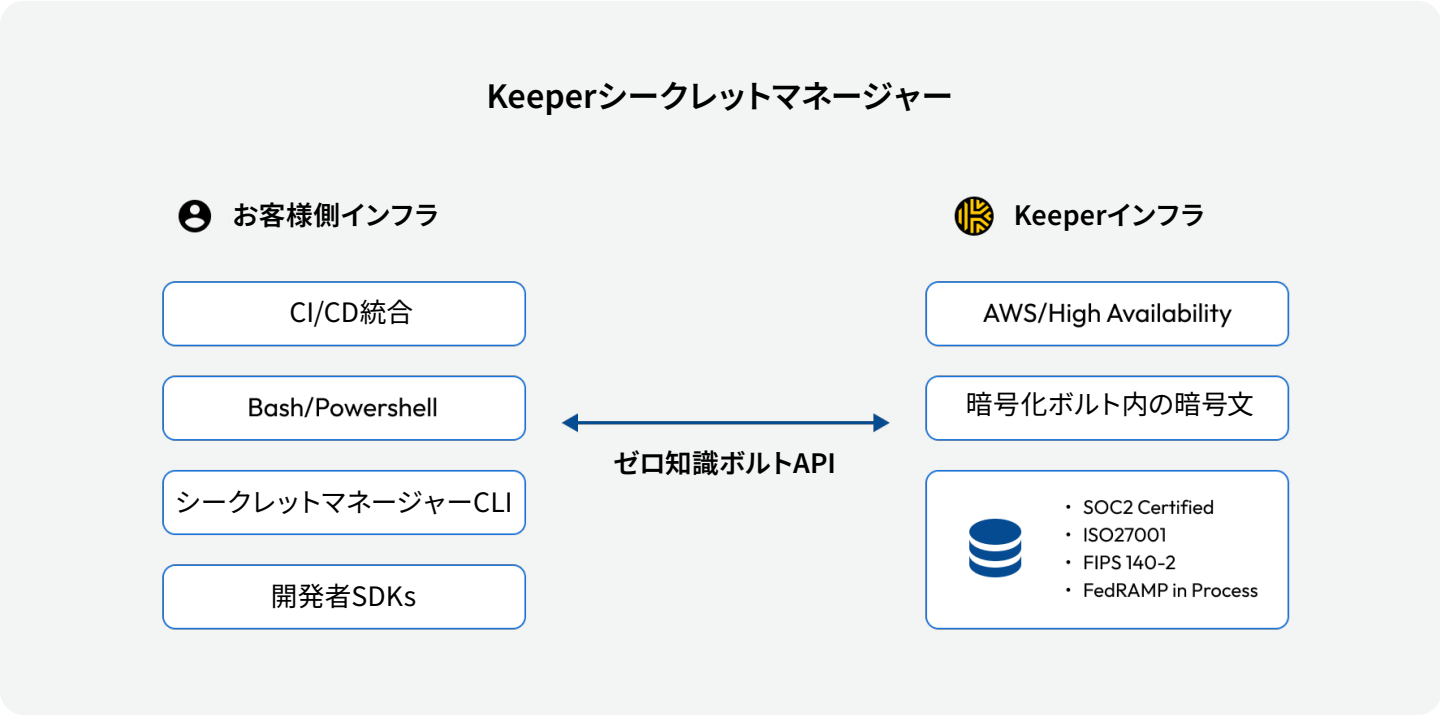
Keeperシークレットマネージャーは、このような懸念を念頭に置いて設計されており、あらゆる規模の企業が組織のニーズに合わせてシークレット管理プロセスを安全に拡張できます。さらに、Keeper のプラットフォームは展開が簡単で、既存のテクノロジーやソリューションとシームレスに統合するため、チームは使用中のビルドシステム内のシークレットへの動的なプログラムアクセスを簡単に作成および管理できます。ハードウェアへの追加費用の負担やエージェントによるソフトウェアのインストールは一切ありません。

Keeperシークレットマネージャーを使用すると、企業は独自のソフトウェアをホストしたり、新しいインフラストラクチャリソースを設定、構成、あるいは管理したり、複雑な VPC ピアリング要件を満たしたりする必要がなく、完全に管理されたクラウドベースのシークレットリポジトリにアクセスできます。Keeper は組織の環境やハードウェア、インスタンスへのアクセスを持たないため、企業はセンシティブデータが最小特権と最小知識の原則、つまり現代のゼロトラストアーキテクチャの基礎となる要素に準拠してい点で安心できます。

Keeperシークレットマネージャー の仕組み

Keeperシークレットマネージャーは、ゼロトラスト、ゼロ知識クラウドベースのモデルを使用して、チームによるシークレット管理プロセスの合理化を実現させます。インフラストラクチャシークレット（API キー、データベースパスワード、クラウドアクセスキー、証明書、SSH キー、サービスアカウントパスワードなど）は、256 ビット AES キーで暗号化されています。さらに、すべてのキーは AES と楕円曲線暗号化の追加レイヤーで保護されいます。楕円曲線暗号化は、復号化と暗号化に公開鍵と秘密鍵のペアを使用するものです。

もちろん、Keeperシークレットマネージャーと Keeper の SDK は、組織とそのユーザーに対してこれらのプロセスすべてを処理します。高度な暗号化はすべて舞台裏で行われるため、組織は暗号化を直接扱わずに済みます。



Keeperシークレットマネージャーでは、組織のすべてのサーバー、DevOps ツールやプラットフォーム、アプリケーション環境（開発、ステージング、生産エリアなど）、そしてソースコードは、暗号化された API エンドポイントと直接通信してシークレットにアクセスします。ゼロ知識ボルト API を活用することで、要求するデバイスはエンドポイントから暗号文を取得し、シークレットをローカルに復号します。

Keeperシークレットマネージャー - 機能と利点

ゼロ知識、ゼロトラストのセキュリティプラットフォーム

Keeperシークレットマネージャー は、Keeper のゼロ知識、ゼロトラストアーキテクチャをベースにしており、現在そして将来のクラウド環境で強力なセキュリティを維持します。認証され、承認されたユーザーのみが特権ファイルやシークレット、パスワードにアクセスできるようにするための管理プロセスは、組織がデジタル変革するにつれてより困難になり、データ環境はいっそう複雑になります。ゼロトラストとゼロ知識セキュリティモデルに重点を置く Keeperシークレットマネージャー を使用すると、認証されて承認されたユーザーのみが許可されたボルトにアクセス可能であること、そしてシークレットは組織の管理下で指定されたデバイスでのみ復号化が可能であることが保証されるため、組織は安心感を得ることができます。

ゼロトラストの概念

ゼロトラストの目的は、防衛体制を強化するために従来型の境界ベースのアプローチにとどまらないセキュリティモデルを組織に提供することです。この新しいクラウドベースのセキュリティモデルでは、信頼性が証明されるまで、すべてのエンティティは信頼できないものと見なされます。これは「最小権限の原則」とも呼ばれます。

ゼロトラストは、ネットワーク境界内のすべてのユーザーとデバイスを暗黙のうちに信頼するのではなく、トラストネットワーク境界モデルを完全に排除し、すべてのエンティティは漏洩されるものと仮定します。また、認証され承認されたすべてのエンティティは、目の前の仕事やタスクを実行するのに必要な最低限のアクセスのみ許可されることが求められます。これは最少特権および最小知識の原則として知られています。

ゼロトラストに準拠し施行することで、Keeperシークレットマネージャー は、盗まれたシークレットによって発生するセキュリティ侵害やデータ侵害を組織が防止できるようにするだけでなく、既存または計画されたゼロトラストアーキテクチャを補強し、ますます巧妙でユビキタスなサイバー脅威に備えたセキュリティへの取り組みに将来性を保証します。

回復力強化のためのゼロ知識

ゼロ知識セキュリティと暗号化は、ユーザーのみが保存されたすべての情報にアクセスできることを意味します。保護されたデータにはサービスプロバイダーでさえアクセスできません。従来のゼロ知識ではない環境の場合、サービスプロバイダー側でセキュリティ侵害が発生すると、顧客のすべてのキーやシークレット、ファイルは、たとえそれらが暗号化されていたとしても、悪意のある第三者が特権アクセスを得てしまう可能性があるのです。

堅牢な共有と監査

最も好ましいシークレット管理には、強力なセキュリティと合理的な共有および使いやすさのバランスが必要です。セキュリティを強化する際にユーザーフリクションが過度に発生すると、他の形式（ユーザーがキーやシークレットをローカルに保存するなど）でセキュリティのギャップが浮かび上がる可能性があるためです。たとえば、SSH キーと接続認証情報は、継続的に開発者が利用できるようにする必要がありますが、許可されていないユーザーからは積極的に隠され保護されています。このようなシナリオで発生する漏洩は、企業にとって壊滅的な打撃となる可能性があるためです。このため、堅牢なシークレット管理プラットフォームは、メール、SMS システム、またはローカルのキーストアを介した認証情報の公開を軽減する必要があります。

この目的のために、Keeperシークレットマネージャーは、堅牢な共有機能と SSH キーなどの認証情報を完全に管理制御することで、最適なシークレット管理プロセスを実施するとともに、ユーザーやチーム間での効果的なシークレット共有を可能にします。組織は、各エンティティがシークレットや認証情報を表示、編集、共有する能力に対し、完全できめ細かなコントロールを維持します。

センシティブな認証情報を含む各レコードの管理、処理および変更方法に対する可視性を維持するため、Keeperシークレットマネージャー は、管理者に高度な監査機能とレポートツールを提供します。シークレットがアクセス、使用、共有または編集されるたびに、変更イベントは管理者による将来の分析、レポート作成、監査のために記録されます。

統一のシークレット管理プラットフォーム

Keeperシークレットマネージャー は、シークレット管理に対して強力でありながらシンプルなクラウドネイティブアプローチを提供します。完全なゼロ知識暗号化とゼロトラストセキュリティを実現し、ホストされたサーバーやオンプレミスのインフラストラクチャは使用しません。

このソリューションにより、組織は、単一の管理ポイントを介してプロビジョニングやレポート作成、監査、ユーザー管理を行う統一されたプラットフォームでシークレットを統合できます。管理者は、インフラストラクチャ、コンテナ、および構築されたシステムにシークレットを統合したり、アクセスキーやパスワード、証明のローテーションの自動化を、すべて単一のインターフェイスで実現できます。Keeperシークレットマネージャー の一元管理コンソールは、アクセス権とアクセス許可の割り当てと管理に際して強力なアクセス制御を実施するための、役割に応じたアクセス制御（RBAC）を提供します。

DevOps や開発チームにとって、このプラットフォームは、ソースコードや構成ファイル、CI/CD システムに認証情報をハードコーディングするのではなく、直感的に操作できるユーザーインターフェースやコマンドラインインターフェース（CLI）を介してデバイスへのボルトシークレットのプロビジョニングを可能にすることで、シークレットのスプロール化を排除するのに役立ちます。チームメンバーは、数量無制限のシークレット、アプリケーション、環境を管理することが可能で、各エンドユーザーは、パスワード、認証情報、ファイル、その他の共有シークレットの保存や管理のために、暗号化されたプライベートボルトを割り当てられます。

無数にあるインテグレーション

Keeperシークレットマネージャー には、数多くの一般的なソリューションが**あらかじめ統合**されており、既存の技術スタックやツールを使用して稼働することは造作もないことです。つまり、追加のデバイスやハードウェアは必要ありません。

たとえば、広く普及している CI/CD プラットフォームやビルドツール（GitHub アクション、Jenkins、Azure DevOps、Docker、Kubernetes、Ansible、Terraform など）とのプラグインや、すぐに使える統合機能により、開発チームは Keeperシークレットマネージャー を既存の DevOps ツールチェーンやワークフローに簡単に組み込むことができます。Keeperシークレットマネージャー の SDK は、Java、JavaScript、Python、Go など、広く普及しているプログラミング言語で使用できるためです。Net や PowerShell の開発者は、わずか数行のコードでアプリケーションやソフトウェアのインターフェースを簡単に設計し、シークレットにアクセスして更新できます。また、セキュリティチームは、Keeperシークレットマネージャー を既存の SIEM や SOAR プラットフォームに簡単に統合し、詳細なイベントレポート作成、アラート機能、セキュリティインシデントのトリアージを目的としたセキュリティフォレンジックやアナリティクスを実現することも可能になります。

Keeperシークレットマネージャー と他製品との比較

Keeperシークレットマネージャー と他のシークレット管理製品との大まかな比較を以下に示します。

クラウドネイティブ機能

Keeperシークレットマネージャー は、フルマネージドのクラウドネイティブソリューションであり、無制限の拡張容量を備えています。ホスティングソフトウェア、複雑な VPC ピアリング要件、設定と管理のための新しいインフラストラクチャリソースは不要です。Keeperシークレットマネージャー は 100% クラウドベースで自己完結型であるため、いかなるメンテナンスあるいは維持管理も必要ではなく、機能するために組織の環境やハードウェア、インスタンスにアクセスするも必要ありません。

対照的に、競合するソリューションでは、お客様がオンプレミスやクラウド内で追加のサーバーをホストする必要や、拡張性を高めるためにより多くのサーバーが必要になる場合があります。また、ライセンスの制約により、閾値に達した場合にサービスの使用が制限されたり中断したりする場合もあります。

常時有効で利用可能な機密情報

Keeperシークレットマネージャー が構築された Keeper プラットフォームは、常に有効で API ベースのマネージドサービスアーキテクチャにより、何百万人ものユーザーや数千もの企業顧客をサポートします。どこからでも、どのデバイスでも利用可能です。Keeper を支えるバックエンドサービスは、HA を実現するために自動的に構築されており、お客様による設定や構成は必要ありません。

他のソリューションでは、ボルトを解除するための追加手順を踏んでから使用できるようになることがあります。HA を実現するために、複数のボルトサーバーやクラスタリング、ストレージエンジンの構成をお客様自身で行わなければならないことがよくあります。

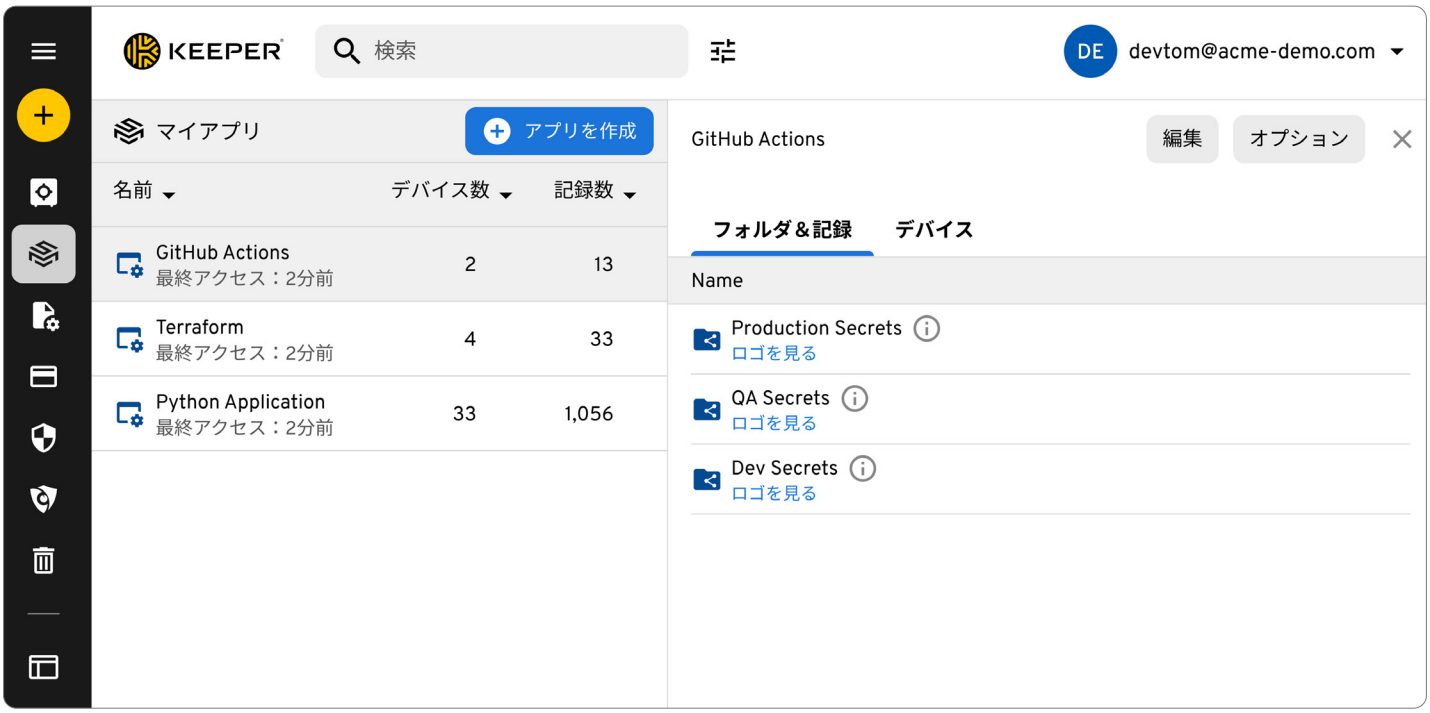
オンラインとオフラインの両方のモードで動作

Keeperシークレットマネージャー は、ボルト暗号文のキャッシングを通じて、オンラインとオフラインの両方で SDK とクライアントデバイスをサポートすることができます。

たとえば、Keeper へのオンライン接続や、SSO 経由でのログインができずにいるユーザーも、オフラインボルトへのアクセスを通じてシークレットにアクセスできます。ボルトのコピーをデスクトップやデバイスにコピーして保存することで、Keeperシークレットマネージャー は、ユーザーがオフラインで安全にシークレットにアクセスすることを可能にします。ユーザーがオンラインでログインするたびに、ボルトのミラーコピーが複製され、ローカルに同期されます。一方、ローカルのボルトデータは、ユーザーが提供するマスターパスワードでのみアクセス可能な暗号化形式で保存されます。他のシークレット管理ソリューションがこの機能を提供することはほとんどありません。もし提供している場合、リクエストは通常オンプレミスサーバーを介して送信されます。

SSL/TLS 暗号化内臓

Keeper ボルトサービスへのすべてのリクエストは、まず TLS 暗号化され、続いて中間者 (MITM) 攻撃を防ぐための 256 ビット AES暗号化レイヤーが追加されます。競合するソリューションでは、SSL 証明書を自分でプロビジョニングする必要があり、複雑なインストール手順が必要です。



ゼロ知識、ゼロトラスト

ゼロ知識暗号化モデルに従って、Keeperシークレットマネージャー は保存されたボルトデータを復号化することはできません。ボルトシークレットを取得後、ローカルに復号化できるのはお客様のデバイスのみです。これにより、お客様のみが自分自身のボルトにアクセスすることを可能にし、シークレットは、組織の管理下で指定されたデバイスのみで復号化されます。対照的に、市場に出回る多くのソリューションは、サーバー上で復号化する REST API やトラフィックデータを平文で使用しています。

Keeperシークレットマネージャー は、ゼロトラストをサポートするように設計されており、最小特権と最小知識の原則を遵守しています。また、特定のシークレットにアクセスするため、デバイスは厳密にスコープ設定されます。対照的に、多くのソリューションは、既存あるいは構成されたトラストモデルを上書きするための緊急アクセス機能を内臓しています。

クラウドベースのコンソール、レポート、アラート、統合

Keeper のクラウドベースのプラットフォームは、ユーザー、デバイス、およびレポート作成のプロビジョニングのための統合管理コンソールを提供します。さらに、Slack や Microsoft Teams、サードパーティーのアラートシステムとの統合により、アラートやイベントをグループやチャネルにプッシュすることができます。他のソリューションでは、これらの機能のサブセットが提供されることが多く、テレメトリは通常 SIEM に送信され、アラートと検出はすべて手動で構築または構成されます。これらのシステムの管理インターフェースは、一般的に、オンプレミスコンポーネントに直接アクセスすることが必要です。

マルチプラットフォームサポートとブラウザプラグイン

Keeper は、すべての主要なウェブブラウザ (Chrome、Safari、Firefox、Edge など) 用のプラグインを提供しており、Mac や PC デバイスでネイティブアプリを自動入力する KeeperFill® などの機能を備えています。対照的に、競合するソリューションには、ネイティブアプリやあらゆるウェブサイトにシークレットを自動入力する機能はありません。さらに、他のソリューションがブラウザ拡張機能を提供することは極めてまれで、たとえ利用可能であった場合でも、一般的にその機能は制限されています。

Keeperシークレットマネージャー のデスクトップアプリケーションは、Mac、Windows、Linux システム、および iOS、Android デバイスで使用できます。モバイルアプリ自動入力は、すべてのモバイルウェブおよびネイティブアプリでの自動入力を可能にします。対照的に、他のソリューションは通常、ボルトシークレットにアクセスするためのデスクトップアプリケーションやモバイルバージョンを提供しておらず、自動入力機能を備えていることはほとんどありません。

ダークウェブ監視

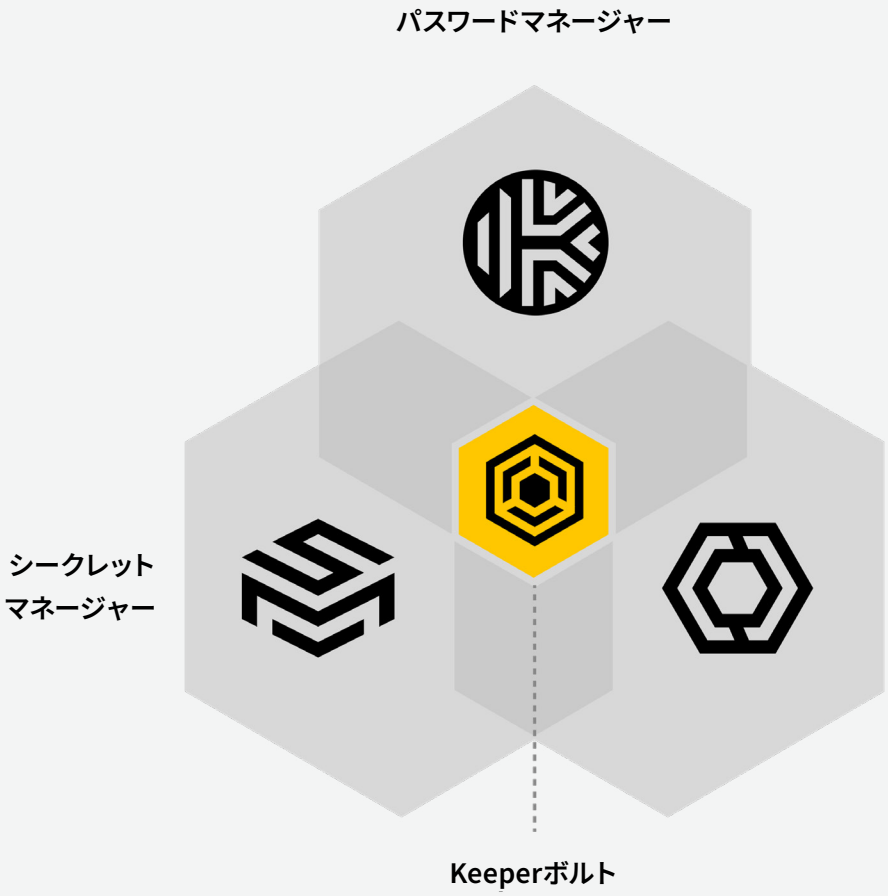
漏洩する可能性があるシークレットを積極的に監視することは、組織内のセキュリティ体制を強化するために不可欠です。この目的を達成するために、Keeper は保存されたシークレットのダークウェブ監視を目的とした、シークレットマネージャーボルトに BreachWatch を組み込んでいます。競合するソリューションには、侵害された機密情報をダークウェブで監視する機能はありません。

シンプルな価格モデル

Keeperシークレットマネージャー は、明瞭で費用対効果の高い価格モデルを提供しています。当社のソリューションは、1 ユーザー、1 か月あたりのライセンスで、1 年分が一括請求され、1 ユーザー、1 か月あたり 50 K の API コールが含まれます。

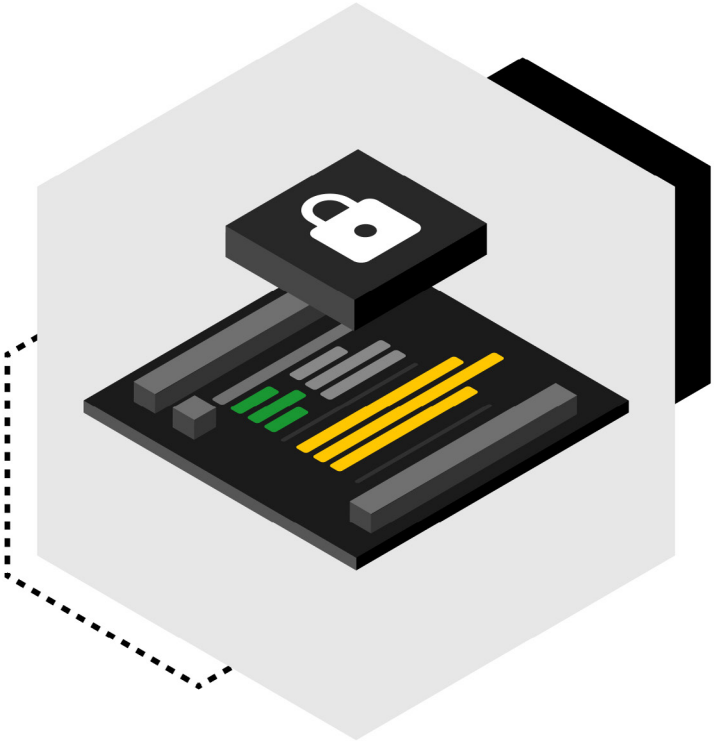
Keeper 製品のラインナップ

Keeperシークレットマネージャー は、世界で 100 万人以上のユーザーを保護するセキュリティソリューションのラインナップである、Keeper 製品ポートフォリオの一部です。他の製品には、Keeperコネクションマネージャー や Keeper パスワードマネージャーなどがあります。



結論

Keeperシークレットマネージャー は DevOps チームやセキュリティチーム、開発チームに対し、クラウドネイティブのゼロ知識、ゼロトラストのプラットフォームを提供しており、API キーやデータベースパスワード、アクセスキー、証明書、ユーザーパスワード、その他あらゆる特権データや組織シークレットなど、インフラストラクチャのシークレットを幅広く管理します。シークレットの安全を保つために何百万人ものユーザーや何千もの企業を支援している Keeper ソリューションの詳細については、Keeperシークレットマネージャー 製品ページをご覧になるか、今すぐ無料トライアルにご登録ください。



リソース

製品情報
https://www.keepersecurity.com/secrets-manager.html

ビデオの概要
https://vimeo.com/350220079

マニュアル
https://docs.keeper.io/secrets-manager/secrets-manager/overview

見積もりを取得
https://www.keepersecurity.com/request-quote.html

Keeper へのお問い合わせ
https://www.keepersecurity.com/contact