KEEPER

業界レポート：ゼロトラストセキュリティ

ゼロトラストの5つの柱とKeeperの対応策

FedRAMP

FIPS 140-2


AWS GovCloud

連邦政府機関は、2024会計年度末までにゼロトラストセキュリティのフレームワークを採用することが求められておりサイバーセキュリティに対するアプローチを根本的に転換する必要があります。ネットワーク内部のユーザーやデバイスに信頼を与える境界ベースのセキュリティモデルに依存する代わりに、連邦政府機関は「決して信頼せず、常に検証する」アプローチを採用しなければなりません。そのためには、既存のセキュリティ慣行の包括的な評価と見直し、新しいテクノロジーとソリューションへの投資、職員の再教育が必要となります。ゼロトラストの目標は、攻撃対象領域を減らし、不正アクセスを防止し、脅威をより迅速に検知して対応し、最終的には連邦機関が管理する機密データやリソースをより確実に保護することです。

Keeper Security Government Cloud (KSGC) パスワードマネージャーと特権アクセス管理はFedRAMP認定を受け、企業向けのパスワード、シークレット情報、特権アクセス管理を1つの統合プラットフォームで提供します。KSGCは、連邦政府機関がゼロトラストセキュリティフレームワークを構成する5つの柱すべてに対処するのに役立ちます。

アイデンティティの柱

KSGCはゼロ知識認証と承認モデルでアイデンティティの柱をサポートします。アイデンティティはKeeper内で完全に管理することができます。当社のプラットフォームは、既存のゼロトラストアイデンティティプロバイダに完全に統合することが可能です。Keeperのセキュリティモデルは、保管庫、デバイス、記録レベルでの継続的な検証やリアルタイムの機械学習分析を含む、いくつかの高度な認証方法をサポートしています。

デバイスの柱

Keeperのソリューションは、デバイスセキュリティの常時監視、デバイスベースのアクセス制御、検証とデータアクセスでデバイスの柱をサポートします。KeeperはAzureの条件付きアクセスポリシーのような既存のデバイス管理ツールと連携します。当社のプラットフォーム内に保存された情報は、デバイスレベルでローカルに暗号化および復号化されます。データを保護し、ゼロトラストモデルをサポートするために、デバイスレベルで楕円曲線（EC）暗号化技術が利用されています。

ネットワーク環境の柱

Keeperのソリューションは、完全に分散されたイングレス/エグレスマイクロパーミッター、機械学習ベースの脅威保護、ゼロ知識暗号化、および記録レベルのアクセス制御により、ネットワーク/環境の柱をサポートします。情報は、256ビットAESレコードレベル暗号化とデバイスレベルEC暗号化を使用して静止状態で暗号化されます。デバイス上のKeeper デジタル保管庫とKeeperクラウド間のネットワーク通信はTLS 1.3で保護され、さらにMITM攻撃、ブルートフォース攻撃、列挙攻撃などの攻撃ベクトルから保護するために、送信レベルの暗号化レイヤーが追加されています。

アプリケーションワークロードの柱

Keeperのソリューションは、アクセスが継続的に許可され、アプリケーションワークフローに強力に統合されているアプリケーションワークロードの柱を最適化します。デフォルトでは、KeeperはVPN接続なしでインターネット経由でアクセスすることができます。管理者はアクセスコントロールポリシーを通じて、ユーザーロールアクセシビリティを管理することができます。

KeeperのARAM（Advanced Reporting and Alerts Module）機能は、リアルタイムアラートまたはその他の脅威ベースのアクションをトリガーすることができる何百ものイベントタイプをカバーする遠隔測定データを機関に提供します。

データの柱

Keeperのソリューションはゼロ知識暗号化でデータの柱をサポートします。ゼロ知識は最高レベルのプライバシーとセキュリティを保証するフレームワークです。暗号化と復号化は各ユーザーのデバイス上で行われます。256ビットAESと楕円曲線暗号を組み合わせることで、Keeperはユーザーの情報があらゆるレベルで安全で安全であることを保証します。当社の完全な暗号化モデルについての詳細を読むには、当社のドキュメントポータルをご覧ください。

Keeper Security Government Cloud (KSGC) は、ゼロトラスト・サイバーセキュリティで政府機関を保護します。

Keeperは業界で最も長いSOC 2認証とISO 27001コンプライアンスを保持しています。Keeperはゼロ知識、ゼロトラストパスワードマネージャー、シークレットマネージャー、特権アクセスマネージャー、リモートデスクトップゲートウェイです。Keeperに保存されたすべての情報は、エンドユーザーのみがアクセス可能です。このプラットフォームは、従業員のパスワード慣行を完全に制御することができます。IT管理者は組織全体のパスワード使用を制御し、ロールベースのアクセス制御を実装することができます。

KSGCでICAMの要件を満たす

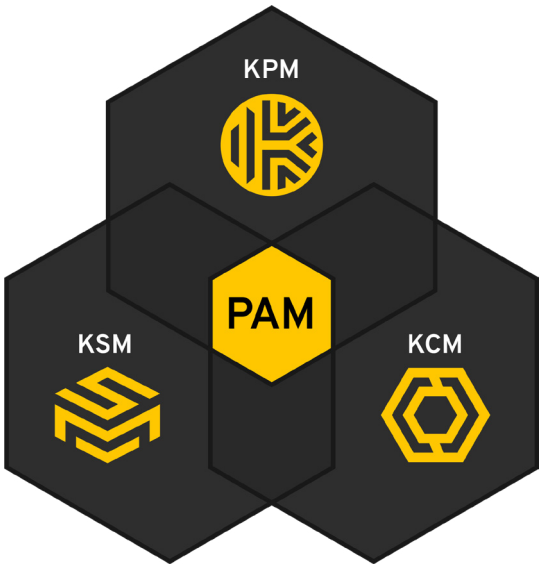
KeeperPAMは、必要な機能だけで、データ漏洩を防止するための組織の主要なペインポイントと要件に対応します。

- 費用対効果。最小限のITスタッフで管理できる単一プラットフォーム。
- 迅速なプロビジョニング。シームレスに導入でき、わずか数時間であらゆる技術やアイデンティティスタックと統合します。
- 使いやすい。統一された管理コンソールとモダンなUIで、すべての従業員がすべてのデバイスタイプで使用できます。

パスワードと認証情報を保護
Keeperのユニークなセキュリティアーキテクチャは、迅速な導入と使いやすいソリューションでデータとシステムを保護します。組織全体でパスワードを安全に保存、共有、管理します。

安全なリモートアクセスを簡素化
VPN不要で、どこからでもリモート接続を安全に管理できます。

コンプライアンスと監査の合理化
組織の認証情報と機密情報へのアクセス許可をオンデマンドで可視化します。



KEEPER PASSWORD MANAGER

組織は、パスワードとパスキーの安全な管理、保護、発見、共有、ローテーションを、完全な制御と可視性で実現し、監査とコンプライアンスを
簡素化します。

KEEPER SECRETS MANAGER

APIキー、データベース認証情報、アクセスキー、認証情報などのインフラストラクチャの機密を保護する、完全に管理されたクラウドベースのソリューションを提供します。

KEEPER CONNECTION MANAGER

エージェントレスリモートデスクトップゲートウェイを提供することで、VPNを必要とせず、特権セッションの即時管理、リモートインフラストラクチャアクセス、RDP、SSHキー、データベース、Kubernetesによる安全なリモートデータベースアクセスを実現します。