KEEPER PAM

組織全体で可視性、セキュリティ、アクセス制御、コンプライアンスを実現

現在、多くの組織は、漏えいした認証情報、恒久的な特権、内部脅威、そして過度に複雑なPAMプラットフォームによるリスクの高まりに直面しています。サイバー攻撃は常に特権アカウントを狙っており、重要なリソースの保護は最優先事項です。

この問題に対処するため、多くの組織で複数のレガシーソリューションを利用していますが、それらは高額で、導入が複雑であり、統合も困難です。これらのレガシーソリューションは、あらゆる場所からあらゆるデバイスを使用しているユーザーを監視して保護するものではありません。攻撃対象領域を減らし、最小権限の原則を適用し、規制コンプライアンスを確保するには、特権アクセス管理にゼロトラストを活用することが必要不可欠となります。これにより、チームがハイブリッド環境やマルチクラウド環境に分散していても安全かつ効率的にアクセスできるようになります。

進化するインフラに対応する、最新のPAMソリューション

KeeperPAMを活用することで、サーバー、ウェブアプリ、データベース、ワークロードなどの重要なリソースへのアクセスを保護、管理できます。組織内のユーザーとデバイスはすべて安全な認証と認可を受けるとともに、強力なモニタリング、脅威検出、レポート機能によって保護されています。

KeeperPAMは、特許取得済みのクラウドネイティブかつゼロ知識プラットフォームとして、企業向けパスワード、シークレット、接続管理を、ゼロトラストネットワークアクセス、エンドポイント特権マネージャー、リモートブラウザ分離と統合します。

KeeperPAMの利点

マルチクラウド管理を実現

複数のクラウドプロバイダ、オンプレミスのワークロード、クライアント環境にわたるアクセスを1つのUIで一元管理。

すべての特権セッションを記録

SSH、RDP、VNC、データベース、ウェブブラウザセッションなど、あらゆるプロトコルで画面とキーボード操作を記録。
AIによる脅威検知と自動セッション終了機能を搭載。

すべてのシステムで多要素認証を強制適用

クラウドおよびオンプレミスのインフラに多要素認証を追加。
ネイティブでサポートされていないリソースにも対応。

パスワードローテーションを自動化

オンプレミスおよびクラウドインフラ全体のサービスアカウントを保護。

制御されたジャストインタイム特権昇格

恒久的な管理者権限を排除し、ポリシーに基づく一時的な権限昇格をオンデマンドで許可。すべての特権操作はログに記録され、時間制限と多要素認証、承認ワークフローで保護。

コンプライアンスに準拠

詳細なログ、セッション記録、自動レポートで完全な可視化を実現し、監査に必要なデータへ即時アクセス可能。

詳細はこちら
keepersecurity.com

デモのご依頼
keeper.io/demo

パートナーに関するお問い合わせ
partners@keepersecurity.com

Keeper Securityについて

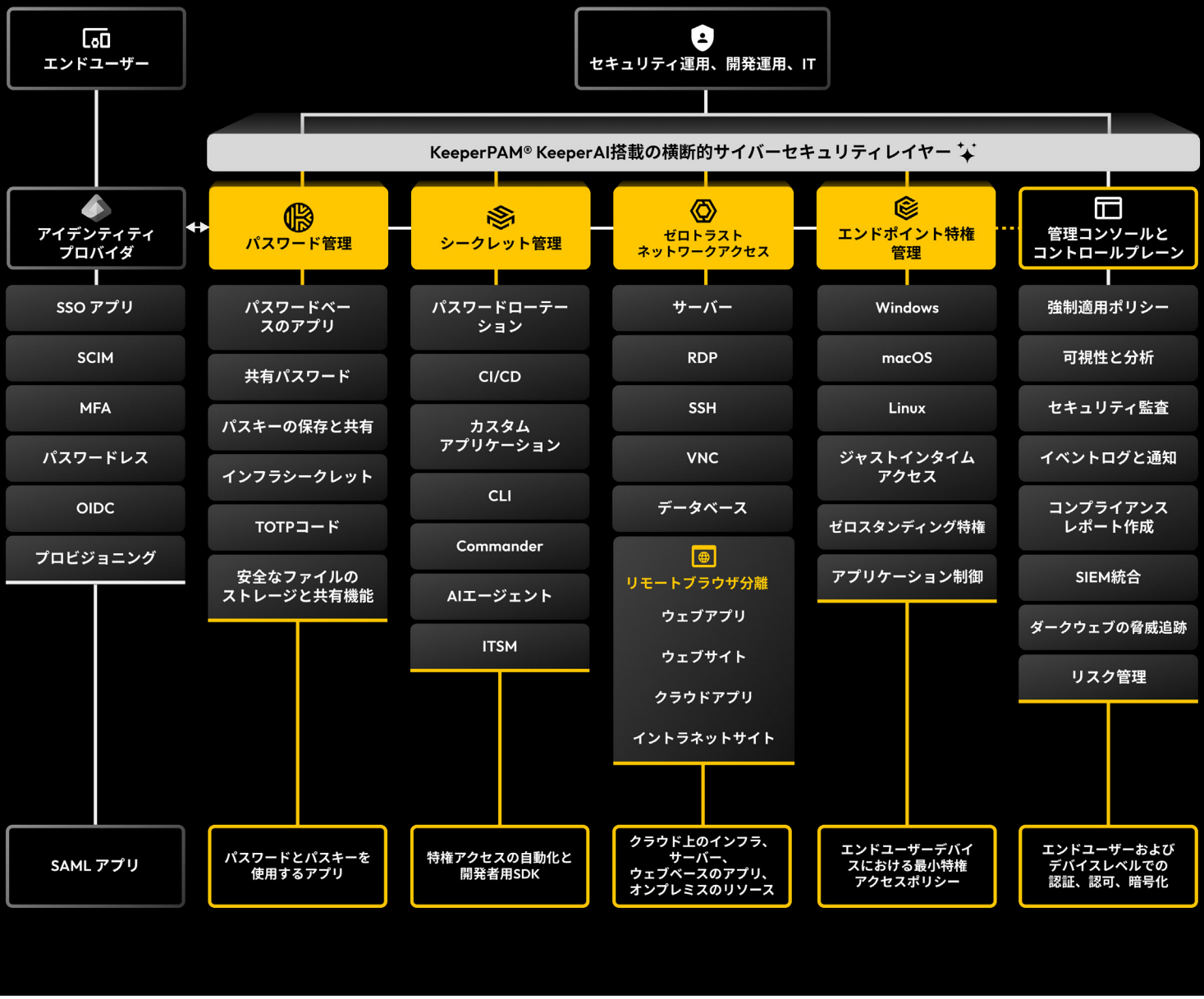
Keeper Securityは、世界中の人々と企業に革新的なサイバーセキュリティを提供し、安全なデジタル社会の実現を支えています。

直感的に使えるソリューションはエンドツーエンド暗号化で設計され、あらゆる場所・あらゆるデバイス・すべてのユーザーを確実に保護します。

Keeperは特権アクセス管理のグローバルリーダーで、その製品は個人から大企業まで幅広く導入されています。

KEEPER PAM

Keeper特権アクセス管理プラットフォーム



マルチクラウドおよび分散型リモートワーク環境向け次世代PAMプラットフォーム

KeeperPAMは、PAM機能をクラウドボルト (保管庫) に導入した初めてのソリューションです。保護されたあらゆるリソースへ安全にアクセスできます。KeeperPAMによりゼロトラストが実現し、組織のメンバーに永続的な権限が発生しないようになります。

プロビジョニング方式の設定、ロール (役割) やチームごとのきめ細かなアクセスポリシーの設定、SIEM、CI/CD、DevOpsツール、カスタムソフトウェアなどのIAMプラットフォームとの統合など、組織のニーズに合わせたカスタマイズが可能です。

KeeperPAMの導入方法

1. **ボルトを展開する** - Entra IDやOktaなどのシングルサインオンでKeeperを展開。SCIM、SAML、ADを通してプロビジョニング。
2. **エンドポイントエージェントを展開する** - Windows、macOS、Linuxの各システムにエージェントをプッシュし、ジャストインタイム権限昇格によってローカル管理者権限を制御可能。
3. **ゲートウェイを展開する** - 各環境に軽量ゲートウェイを導入し、エージェントレスアクセスと特権セッションを実現。
4. **ポリシーを設定する** - 職務に応じて多要素認証、ロール単位のアクセス制御、最小権限のポリシーを適用。