ENDPOINT PRIVILEGE MANAGER

Windows、Linux、macOSの各エンドポイントに対応したエンドポイント特権管理により、最小権限アクセスを徹底し、恒常的な管理者権限を排除するとともに、プロセスレベルおよびマシンレベルでのジャストインタイム (JIT) アクセスを実現します。

強固な特権アクセス制御は、組織がセキュリティ体制を強化し、業務効率を確保し、規制遵守を実現するために不可欠です。

Keeperエンドポイント特権マネージャーは、軽量エージェントを用いて恒常的な管理者権限を削除し、必要な場合にのみポリシーに基づいた一時的な権限昇格を可能にすることでエンドポイントを保護します。本システムは、オプションの承認ワークフローや多要素認証 (MFA) の適用を組み合わせたJITアクセスにより、柔軟にカスタマイズ可能なセキュリティポリシーを実現します。

特権操作は、各セッションごとに自動的にプロビジョニングおよび解除される一時アカウントを使用する方法、標準ユーザーアカウントに対して一時的に権限を昇格させる方法のいずれかで実行可能です。組織では、自社のセキュリティ体制や業務要件に応じて、最適な方法を選択できます。

Keeperエンドポイント特権マネージャーは、Windows、macOS、Linuxの各環境に対応しており、すべての特権昇格アクティビティを記録して監査やコンプライアンスに活用できる中央ダッシュボードを通じて可視化を実現します。

Keeperエンドポイント特権マネージャーの利点

セキュリティ

恒常的な管理者権限を排除し、承認されたアプリケーションに対してのみ必要なときに一時的な (ジャストインタイム) 権限昇格を許可することで、攻撃対象領域を減らし、セキュリティを強化します。

コンプライアンス

特権の使用に関する包括的な監査証跡を提供し、管理アクセス制御の記録を通じて規制要件の遵守を確保します。

運用効率

日常的な管理作業に対する承認を自動化することで、ヘルプデスクの負担を軽減します。

ユーザー体験

承認されたアプリケーションに対する特権の自動昇格により、ユーザーはIT部門の対応を待つことなく必要な作業を実行できます。

拡張性

一元化されたプラットフォームから数多くのWindows、macOS、Linuxのエンドポイントに対して、最小特権ポリシーの効率的な適用と特権アクセスの管理を実現できます。

監査性と可視性

昇格アクティビティや承認、エンドポイントポリシーの適用状況を可視化し、詳細なログとSIEMツールとの連携によって迅速なインシデント対応を可能にします。

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

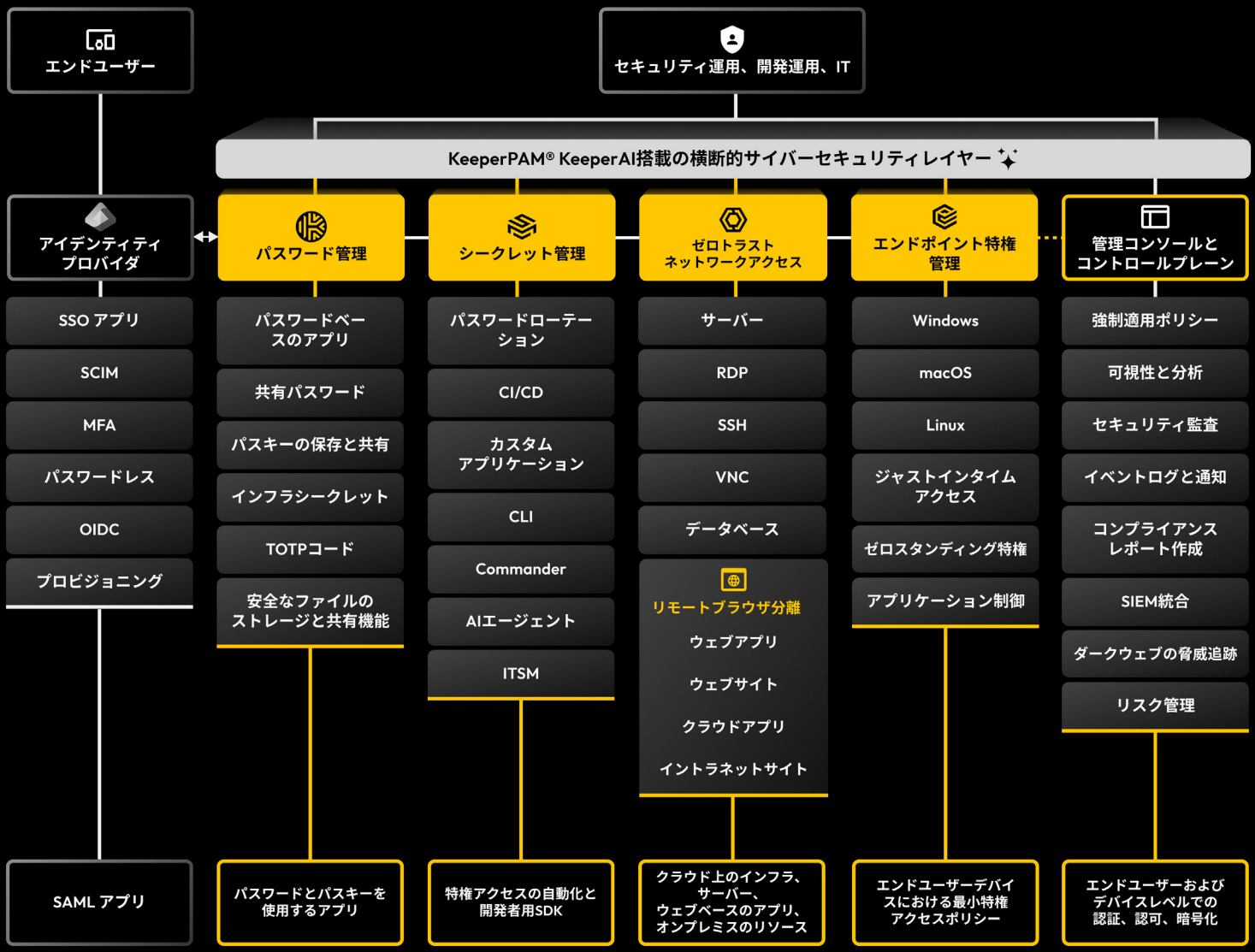
Keeper Securityは、世界中の人々と企業に革新的なサイバーセキュリティを提供し、安全なデジタル社会の実現を支えています。

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



ゼロトラストをエンドポイントに拡張

エンドポイント特権マネージャーは、エンドポイント上での権限昇格を直接制御することで、KeeperPAMのゼロトラストアプローチを拡張し、PAM全体のソリューションが持つセキュアな接続機能を補完します。KeeperPAMプラットフォームの他の機能が「ユーザーがどのようにシステムへ接続するか」を保護するのに対し、エンドポイント特権マネージャーは「接続後にユーザーが行使できる管理者権限」を統制します。

Keeperによる特権昇格の仕組み

1. **ポリシー**：アプリケーションやプロセスが特権昇格を要求すると、Keeperエージェントは該当するポリシーを確認します。
2. **承認**：承認が必要な場合、リクエストは管理コンソールまたはコマンドラインインターフェース (CLI) を通じて管理者に送信されます。
3. **多要素認証オプション**：承認が不要な場合は、多要素認証の設定に応じて、特権昇格が自動的に実行されます。多要素認証の適用はオプションです。