データシート

Keeper Security Government Cloud

KSGCパスワードマネージャーと特権アクセスマネージャーは、FedRAMPとStateRAMPの認定を受けており、AWS GovCloudで利用可能です。

課題

脆弱で盗まれたパスワード、認証情報、DevOps の秘密情報が、データ侵害の主な原因です。ほとんどの組織では、こうした脅威を可視化できず、すべての従業員、すべてのデバイス、アプリケーション、システムにわたってセキュリティのベストプラクティスを実施する方法がありません。このため、IT 管理者には一連の課題が生じます。

01

政府機関は、サードパーティのソリューションを購入する際、複雑な規則と厳格なコンプライアンスを遵守しなければならない。

02

オンプレミス、オフプレミスを問わず、デバイス、クレデンシャル、シークレットが分散ネットワークに接続されるにつれ、攻撃対象は飛躍的に拡大している。

03

分散リモートワークやマルチクラウドコンピューティングといった最新の働き方は、従来のITの境界線を時代遅れにし、すべての人のリスクを増大させている。

04

従来のサイバーセキュリティ・ソリューションは、その性質上、サイロ化されており、可視性、セキュリティ、コントロール、コンプライアンス、レポーティングにおいて重大なギャップを生み出している。

これらの中核的な課題に対処しない組織は、データ侵害、コンプライアンス違反、業務摩擦のリスクが高まります。

解決法

Keeper Security Government CloudパスワードマネージャーとPAMはFedRAMPとStateRAMPの認定を受けており、ゼロトラストセキュリティフレームワークとゼロ知識セキュリティアーキテクチャを維持しています。これにより、組織は認証情報と暗号化キーの完全な管理と制御を保証します。

KSGCは、お客様のチームと組織に人間中心のサイバーセキュリティソリューションを提供します。多要素認証（MFA）のようなパスワードセキュリティのベストプラクティスを採用し、SSOと統合してセキュリティギャップをなくすシンプルで効果的な方法を従業員に提供することで、機関のサイバーセキュリティを向上させます。

Keeperでハッキングされないための対策を

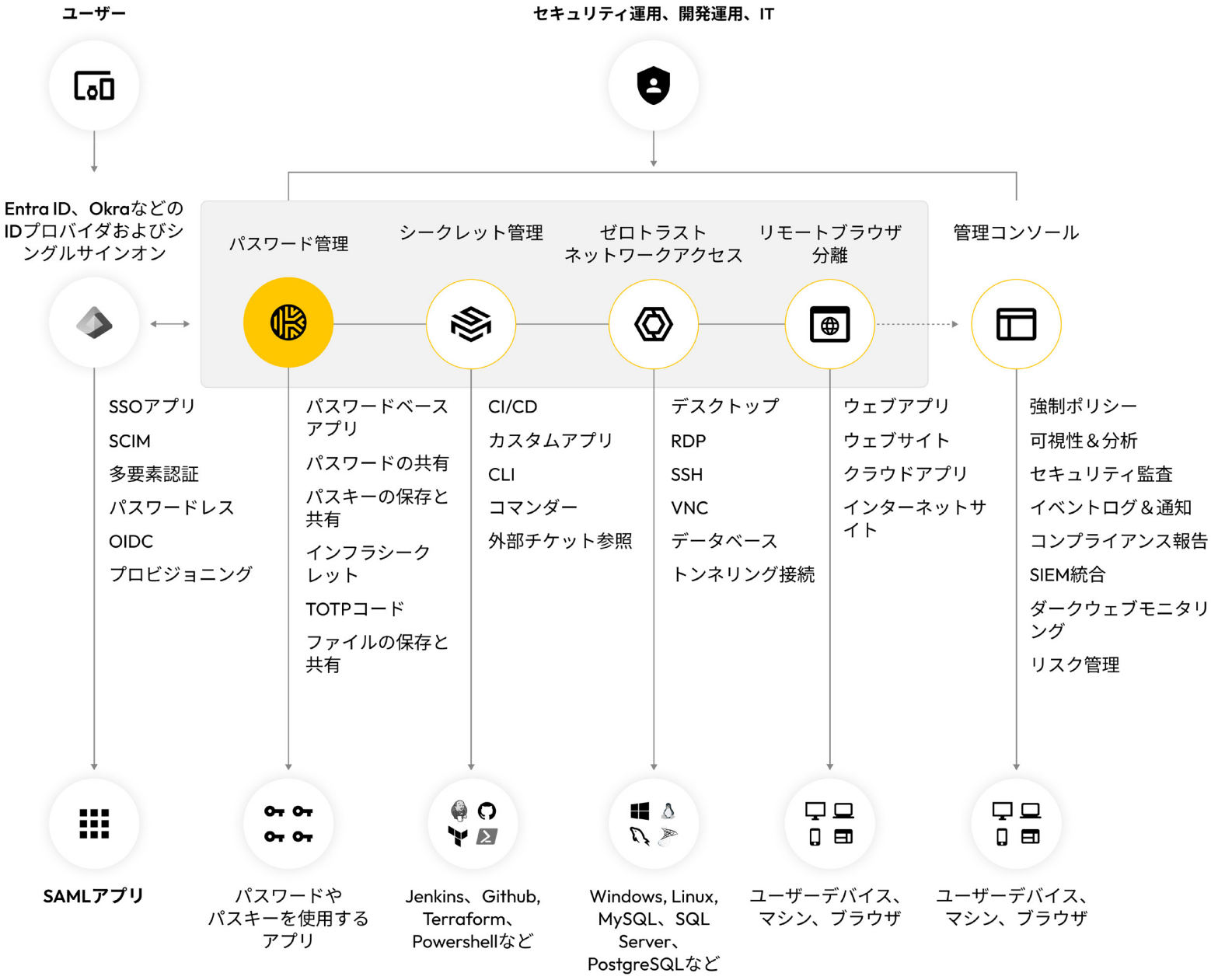
詳しくはこちら
keepersecurity.com

デモのリクエストはこちら
keeper.io/demo

弊社について

Keeper Securityは、世界中の人々と組織のためにサイバーセキュリティを変革しています。Keeperのリーズナブルな価格で使いやすいサイバーセキュリティソリューションは、ゼロトラストおよびゼロ知識セキュリティの基板上に構築され、すべてのデバイスにおけるすべてのユーザーを保護します。Keeperは、何百万という個人と数千の組織に信頼されています。業界随一のパスワード管理、パスキーとシークレット管理、特権アクセス、安全なリモートアクセス、および暗号化メッセージにおけるリーダーです。

Keeper特権アクセス管理プラットフォーム



組織バリュー

- ランサムウェアや認証情報関連のサイバー攻撃を防ぐ
- あらゆる場所からあらゆるデバイスのあらゆるユーザーを保護
- ゼロトラストのセキュリティとポリシーで組織を強化し、ゼロトラストの義務に対応
- 既存のシングルサインオン(SSO)展開を強化・拡張
- パスワードセキュリティのベストプラクティスを導入するためのシンプルで効果的な方法を従業員に提供し、ヘルプデスクやITチームのパスワード関連チケットの負担を軽減
- 認証情報の保管とアクセス管理
- シークレット管理
- シングルサインオン (SSO) 統合

主要機能

- 特権アカウントの認証情報管理
- セッション管理、モニタリングとレポート
- ICカード認証
- FedRAMP、StateRAMP認定
- 業界のコンプライアンスとレポート