KEEPER
Cybersecurity Starts Here

シングルサインオン構成を強化し拡張する

DATASHEET

Keeper SSO Connect™

SSOは全てのアプリケーションを保護するわけではありません

企業はシングルサインオン（SSO）を採用していますが、その理由は、パスワード関連の労力を軽減し、パスワードを紛失した際のサポートデスク業務を最小限に抑え、効率を高めることができるからです。理論的には、ユーザーは複数のパスワードを覚える代わりに、1つのパスワードだけを覚えるだけで済みます。しかし、実際のSSOはそうはいきません。平均的な組織では約1,200のクラウドアプリケーションとサービスを使用しています。正確な数で言うと、小企業の数百から大企業の3,000以上まで様々です。これらのアプリケーションやサービスの多くは、SSOをサポートしていないか、あるいは、互換性のない異なるSSOプロトコルをサポートしています。

例えば、組織のアイデンティティ・プロバイダー（IdP）はSAMLプロトコルを使用しているが、従業員がOAuthを使用しているアプリケーションを業務で必要としている、ということがありうるでしょう。さらに、ほとんどの組織は、いまだ業務用のレガシーアプリケーションに依存しています。これらの古いアプリケーションはSSOを全くサポートしていませんが、重要なデータが含まれていたり、重要なビジネス機能を実行していたりします。そのため、従業員は古いアプリケーションを使い続けなければなりません。また、すべての最新アプリケーションがSSOをサポートしているわけでもありません。

従業員はパスワードをたくさん覚えておく必要があります。多数のサイトやアプリのパスワードを従業員の管理に任せることで、企業は情報漏えいの危険にさらされるのです。

SSOにはセキュリティ上の弱点があります

SSOには他にも欠点があり、特に、多要素認証（2FA）やロールベースのアクセスコントロール(RBAC)と組み合わせていない場合は、その欠点が顕著に現れます。例えば、以下のような欠点が挙げられます。

- SSOはシステムへのアクセスのみを制御し、個々のユーザーのアクセスレベルは制御しません。このため、管理者はロールベースのアクセスコントロールと最小特権を実現するための別のソリューションを導入する必要があります。
- ユーザーがパスワードを忘れると、1つのサイトやアプリのみならず、複数のサイトやアプリからロックアウトされる。
- サイバー犯罪者がユーザーのパスワードを盗んだ場合、1つのシステムのみならず、複数のシステムにアクセスされてしまいます。
- SSOは、管理者に、ユーザーのパスワードの習慣を教えてくれるわけではありません。そのため管理者は、単純なパスワードの使用、複数のシステムでのパスワードの使い回し、2FA をサポートするすべてのアカウントで 2FA を有効にしない、といった従業員の不適切なパスワード習慣を防ぐことができません。

Keeper SSO Connectはデータ環境全体でエンドツーエンドのパスワード保護を可能にします

Keeper SSO Connect はお客様の既存のSSO展開とKeeperパスワード管理システムをシームレスに結合する SAML 2.0 アプリケーションです。Keeper SSO Connectは、ゼロナレッジのパスワード管理、アプリケーションへの強制的なRBAC、およびユーザーのパスワードセキュリティの実践への可視性により、SSOを強化および拡張します。Keeperはデータセキュリティの複数のレイヤーを提供するので、SSO単体よりも攻撃者に対してはるかに強力な防壁を提供します。

Keeper SSO Connect は、Keeper のゼロナレッジボールトとシームレスに統合され、安全なパスワード、機密データ、ファイルストレージを提供し、共有機能と高度なセキュリティ機能を備えています。

Keeper + SSO = 100%のカバー率

Use Case	Keeper Enterprise	SSO Identity Provider
パスワードベースのアプリ	✓	✓
パスワードと機密情報の共有	✓	✓
データストレージの暗号化	✓	✓
ソーシャル・メディア・サイト	✓	✓
ネイティブアプリケーション	✓	✓
オフラインアクセス	✓	✓
SSHキーとSSL証明書	✓	✓
API認証情報	✓	✓
プライベートファイルの暗号化	✓	✓
ゼロナレッジ暗号化	✓	✓
SAMLベースのアプリケーション	✓ via Keeper SSO Connect	✓

[1] Dark Reading

既存のアイデンティティ・プロバイダー(IdP)との連携

パスワードマネージャーの中には、SSOやゼロナレッジ暗号化を全くサポートしていないものもあります。Keeper SSO コネクトは、Microsoft 365、Azure、ADFS、Okta、Ping、JumpCloud、Centrify、OneLogin、およびF5 BIG-IP APMなどのすべての一般的なSSO IdPプラットフォームと簡単かつシームレスに統合できます。

KeeperのPasswordセキュリティと暗号化プラットフォームを全員に展開しながら、SSOを拡張する。

Keeper SSO Connectは、ログイン認証情報だけでなく、独自の顧客データ、制限されたシステムへのアクセス認証情報、および機密文書を保存および暗号化するために使用できるゼロナレッジパスワードマネージャおよびデジタル保管庫とシームレスかつ容易に統合することにより、あらゆるSSOソリューションを強化します。

既存のIdPを介して認証するだけで、従業員は以下のような最高ランクのKeeperパスワード管理プラットフォームのすべての機能にアクセスすることができます。

- あらゆるOSを搭載したあらゆるデバイスからアクセス可能な、安全なデジタル保管庫
- パスワードジェネレータ
- あらゆるウェブサイトやアプリで利用できるログイン認証情報の自動入力機能
- 機密ファイル、ドキュメント、写真、ビデオを保存できる安全なストレージ(デバイス無制限)

情シスは、従業員のパスワードの使用状況を完全に可視化し、コントロールすることができます。これにより、強力でユニークなパスワード、多要素認証(2FA)、およびその他のパスワードの使用とセキュリティのポリシーを強制することができます。

- 独自の特許取得済みゼロナレッジセキュリティモデル
- 初期の機器や導入コストなしで、すべてのデバイスへの迅速な導入が可能
- パーソナライズされたオンボーディングと、専任のサポートスペシャリストによる24時間対応のサポートとトレーニング
- RBAC、2要素認証、監査、イベントレポート、HIPAA、DPA、FINRA、GDPRなどの複数のコンプライアンス規格に対応
- 安全な共有フォルダ、サブフォルダ、パスワードをチームに提供
- SSOまたはマスターパスワード認証のいずれかをユーザーに提供
- SSOが利用できない場合に、オフラインで保管庫にアクセス可能
- SCIMを利用して保管庫を動的にプロビジョニング
- 高可用性(HA)の設定

シングルクラウド、マルチクラウド、ハイブリッド導入の選択肢

Keeper SSO Connectは、完全に管理されたSaaSソリューションであり、Windows、Mac OS、またはLinux環境、クラウドまたはオンプレミスに展開することができます。

ゼロナレッジアーキテクチャ

ユーザーの暗号化キーはKeeper SSO Connectによって動的に生成され、すべての暗号化と復号はユーザーのデバイス上で行われます。ユーザーのマスターパスワードから鍵を生成するために、10万ラウンドのPBKDF2が使用されます。各レコードは、クライアント側でランダムに生成された異なる固有の鍵で、AES-256を用いて暗号化されます。ユーザーやチーム間での安全な記録の共有には、RSA暗号が使用されます。Keeperのインフラストラクチャはデバイス間で暗号文を同期します。鍵の固定化は、クライアントとサーバーの間で実施されます。転送中および静止中のすべてのデータは常に暗号化されており、Keeper Security の従業員や外部の第三者が見ることはできません。

Keeper Security, Inc.について

Keeper Security, Inc. (Keeper) は、パスワード関連のデータ漏洩やサイバー脅威を防ぐための、市場をリードするトップクラスのサイバーセキュリティプラットフォームです。Keeperのゼロナレッジセキュリティおよび暗号化ソフトウェアは、サイバー窃盗のリスクを軽減し、従業員の生産性を向上させ、コンプライアンス基準を満たすサービスとして、世界中の何百万人もの人々と何千もの企業から評価を受けています。Keeper は PC Magazine のベストパスワードマネージャオブザイヤー&エディターズチョイス、PCWorld のエディターズチョイスに選ばれ、4つの G2 ベストソフトウェア賞を受賞しています。また、KeeperはSOC-2およびISO 27001認証を取得しておりSAM(System for Award Management)を通じて米国連邦政府の使用リストにも加えられています。詳細は **https://keepersecurity.com** でご確認ください。