データシート

Keeper リモートブラウザ分離

エンドユーザーデバイスからウェブブラウジングアクティビティを安全に隔離 – 制御されたリモート環境でブラウジングセッションをホストすることで、サイバーセキュリティの脅威を軽減します。

課題

01

すべての組織がセキュリティと効率性を確保しながら、アプリケーションやウェブサイトへのアクセスを提供する必要があります。Keeper のリモートブラウザ分離は、VPN や ZTNA を必要とせずに制御されたリモート環境でブラウジングセッションをホストし、エンドユーザーのデバイスからウェブブラウジングアクティビティを隔離することで、サイバーセキュリティの脅威を軽減します。

02

従業員はウェブサイトやツールにアクセスすることを要求しますが、VPN は設定やメンテナンスがますます難しくなってきており、特に請負業者やベンダーにとってはアクセス過多になることがよくあります。VPN には事前承認された URL のリストへのアクセスをロックダウンする能力がないことがよくあります。そのため、認証されたアクティビティのみが実行されることを保証できないのです。

03

さらに、セキュリティ、コンプライアンス、監査要件の確保が、管理者や組織全体に波及する要因となっています。多くのソリューションはツールを組み合わせることでこのようなニーズに対応しようとしますが、これではユーザーを複雑にして不満を募らせるだけで、導入が減り、セキュリティリスクが増加するのみです。

解決法

Keeper コネクションマネージャー 内のリモートブラウザ分離なら今日の分散型リモートワーク環境で頭痛を引き起こすことなく、アプリケーションやウェブサイトへのセキュリティ、使いやすさ、そして合理化されたアクセスを提供する最新のエージェントレスソリューションで、複雑さとセキュリティのジレンマを解決します。

リモートブラウザ分離は顧客データを送信しないプライベートブラウザセッションで、真のゼロ知識セキュリティを提供します。ユーザーのローカルブラウザのバージョンに関係なく、最新の Chromium ブラウザを介してサイトへの安全なアクセスが可能になりウェブブラウジングが簡素化されるため、デバイスが侵害された場合のデータ流出のリスクを防ぐことができます。すべての閲覧活動は顧客の Keeper コネクションマネージャーコンテナを介して行われるものであり、決して Keeper のサーバー経由ではありません。

ユーザーのデバイスに認証情報を送信することなく、ログイン情報とパスワードの詳細を隔離されたブラウザセッションに自動的に入力します。これにはベンダーのアクセスを制限し、記録やキーストロークのロギングでセッションを綿密に監視することが含まれます。

完全に記録されたウェブサイトのやり取りでコンプライアンスを簡素化し、適切なやり取りを確実にし、内部リスクを軽減し、監査プロセスを合理化します。

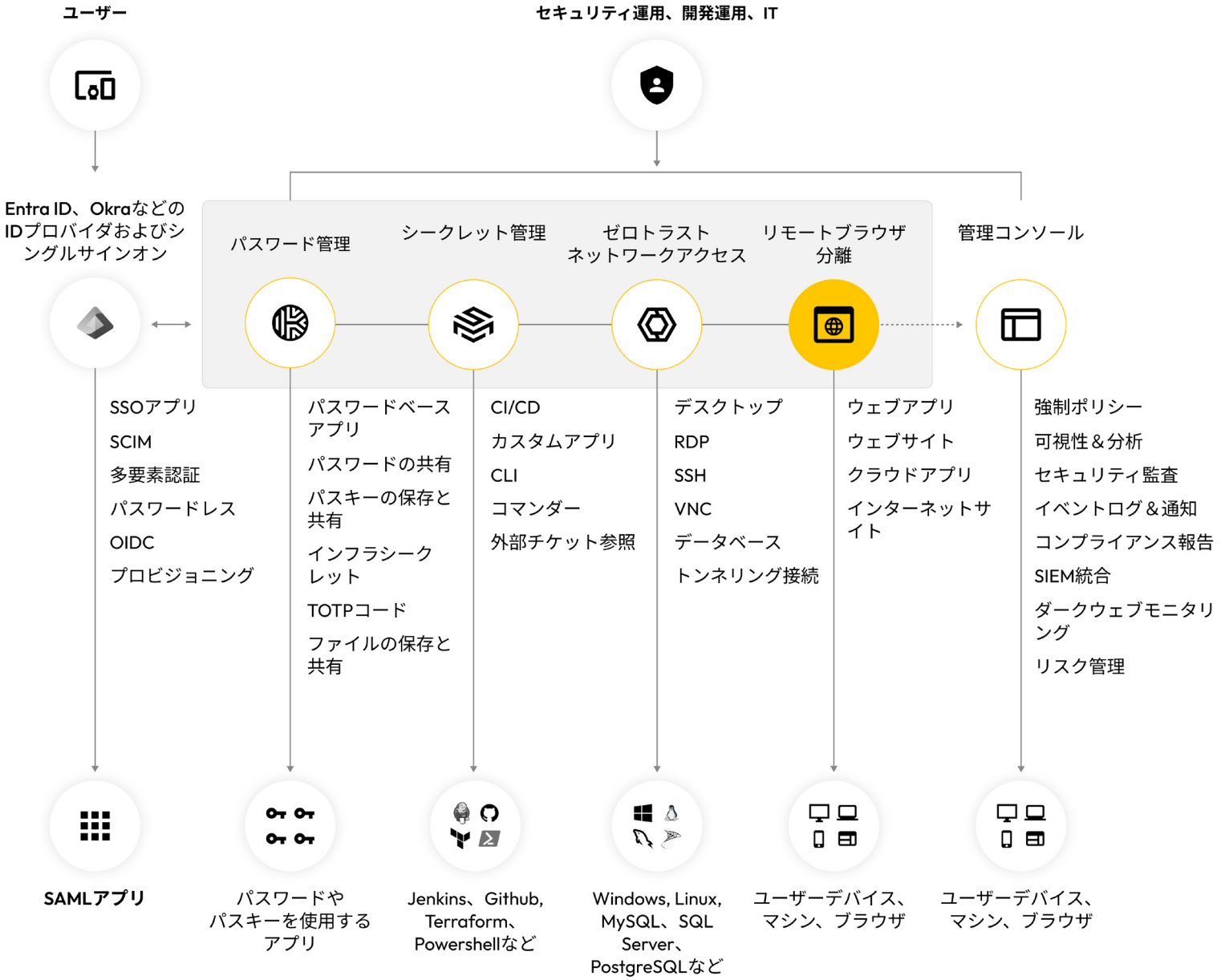
カスタマイズ可能な管理制限でアクションを制限し、クリップボードの使用やファイルのアップロード、ダウンロードなどを禁止することでデータ漏洩を防ぐブラウジングセッションを提供します。

主なメリットと機能

- エンドツーエンドの暗号化を備えたウェブベースのアクセス
- 記録されたウェブセッション
- 制御されたウェブブラウジング
- パスワードの自動入力
- VPN や ZTNA を必要としない安全なアクセス
- ゼロ知識セキュリティ
- ゼロトラストフレームワーク
- 役割ベースのアクセス制御
- 多要素認証
- 管理制御
- 共同ブラウジング
- あらゆるウェブベースのアプリケーションで SSO を有効にする
- ベンダーや BYOD ユーザーからの安全でないアクセスを防ぐ
- データ漏洩を排除する

KEEPER CONNECTION MANAGER

Keeper特権アクセス管理プラットフォーム



ビジネス価値

監査
保護されたウェブサイト上でのユーザーのアクティビティは、レビューやコンプライアンス、セキュリティの目的で記録され、適切なやり取りの確保や内部脅威や詐欺の削減に繋がるものとなる可能性があります。

テスト
ウェブサイトやアプリケーションでバグを再現するのが難しい場合があります。Keeper コネクションマネージャー 経由で環境にアクセスすることで、テストチームや品質保証チームは問題を再現するための手順を常に確実に記録できるようにします。

アクセス制御
護されたウェブサイトへのアクセスは、たとえターゲットウェブサイトが直接アクセス制御をサポートしていない場合でも、ロールベースのアクセス制御によって簡単に制限されることがあります。

共同閲覧
共同作業やトレーニング用に、他のユーザーとウェブセッションのアクティブなビューを共有します。

究極のプライバシー
自動化された認証情報はエンドユーザーが決して見られない、あるいは利用できないため、DOM 検査やクロスサイトスクリプティング攻撃から最大限の保護を提供します。

セキュリティチーム
仮想マシンを起動することなく、不審なリンクをテストします。