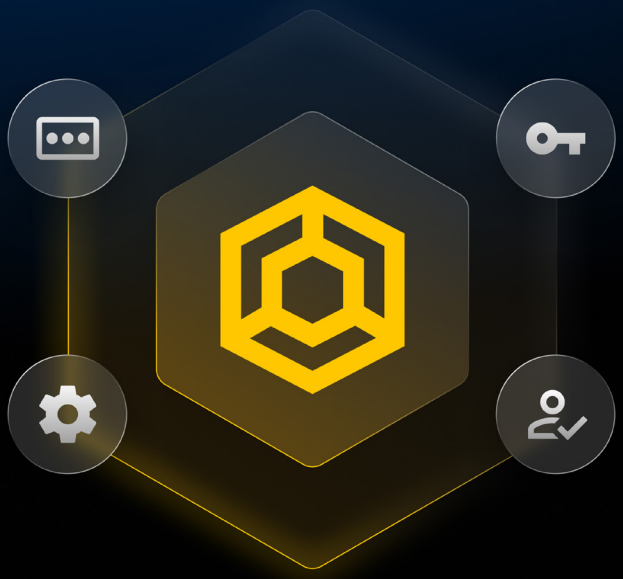
ケーススタデ

Asite、KeeperPAM®で全社規模の認証情報、シークレット、特権アクセスの保護を実現



背景

建設業界にサービスを提供するSaaS企業のAsiteは、世界中のチームや地域にまたがる組織が、3Dモデルやデジタルツインから文書管理やサプライヤーとの連携まで、複雑なプロジェクトを管理できるよう支援しています。Asiteは複数の地域で事業を展開し、9か所にデータセンターを構え、従業員数は500人を超えます。

産業
建設技術 (SaaS)

従業員数
500人以上

ソリューション
KeeperPAM

課題

重要なインフラストラクチャや防衛関連環境で事業を展開する顧客を含む大規模な建設計画をサポートするグローバルなSaaS事業に、認証情報と特権アクセスの安全な管理は不可欠です。Asiteは、組織全体のパスワード、シークレット、特権アクセス管理 (PAM) について、より一本化された強制力のあるアプローチを必要としていました。

可視性が断片的な従来型のツール - ブラウザベースのパスワードマネージャーに依存すると可視性と制御が制限され、パスワードの使い回し、脆弱な認証情報、コンプライアンスや顧客の信頼を確保するためのセキュリティ制御を実施する能力の低下により、リスクが増大します。組織の以前のシークレット管理方法やPAMプロバイダーは、コストが高く、導入が困難でした。

Asiteは、社内ユーザーの保護だけでなく、複雑な建設プロジェクトで協力体制にある外部のパートナーやサプライヤーにも同じレベルの保護を提供し、顧客の期待と契約上の義務を確実に満たす必要がありました。そのため同社は、一元化されたプラットフォーム内ですべてのサイバーセキュリティニーズに対応できる、安全で使いやすいソリューションを求めていました。

> **「KeeperPAMの (セキュリティ) アーキテクチャと柔軟性は他に類を見ません。」**
>
> **ティアゴ・ロサド氏 | 最高情報セキュリティ責任者**

Keeperのソリューション

Asiteは、組織全体の特権アクセス、認証情報、接続、シークレットを保護するための統合プラットフォームとして、KeeperPAMを選択しました。サイバーセキュリティ技術スタックをゼロトラスト、ゼロ知識を基盤とする単一のプラットフォームに統合することで、Astieは複雑さを軽減し、セキュリティとコンプライアンスを強化しました。

運用負担が軽い一元的な特権アクセス管理 - KeeperPAMは、認証情報を公開せずに、サーバーやインフラストラクチャ、機密性の高いシステムへの安全で監査可能な特権アクセスを提供します。セッションアクティビティは一元的にログに記録され、顧客環境および規制環境の全体にわたる調査、説明責任、コンプライアンスをサポートします。KeeperAIは、高リスクのセッションがあれば自動終了し、監査やインシデント対応のための正確な証拠記録を併せたアクティビティの要約を生成します。

迅速な導入と柔軟なアーキテクチャを備えたKeeperPAMにより、Asiteの従来のPAMとシークレット管理ツールは置き換えられ、特権アクセスの対象システムを追加して拡大しながらも、コストや複雑さが増えることはありませんでした。

> **「KeeperPAMの導入は非常に簡単で、私の経験上、最高のソリューションでした。他のツールも、このくらい導入が簡単であればいいのにと思います。」**
>
> **ティアゴ・ロサド氏 | 最高情報セキュリティ責任者**

KeeperPAMに組み込まれたエンタープライズ向けパスワード管理 - Asiteは、KeeperPAMプラットフォームの一部として、ブラウザベースのパスワードマネージャーに換わる全社規模のパスワード管理を全従業員対象に標準化し、認証情報セキュリティの一本化された強制力のあるアプローチを確立しました。

その結果、長さと複雑さについて管理者が制御できるパスワードポリシーが敷かれ、アプリケーション間での認証情報の使い回しが防止されました。IT部門は現在、Keeperのダークウェブモニタリングツール、BreachWatch®を使って漏洩した認証情報を特定できるようになり、組織のセキュリティ態勢をさらに強化しています。KeeperPAMと同じボルト内でパスワード管理にアクセスすることで、ユーザー体験がシンプルになるとともに、エンドユーザーと特権認証情報の両方で一貫したガバナンスが保証されます。

Keeperシークレットマネージャーによる最新のシークレット管理 -アプリケーションとインフラストラクチャのシークレットを保護するために、Asiteは、以前のシークレット管理ツールに換えて、Keeperシークレットマネージャーを KeeperPAMプラットフォームのネイティブコンポーネントとして導入しました。Keeperシークレットマネージャーは、パスワード、キー、シークレットの作成とローテーションを自動化し、長期間有効になっていたり、手動で管理されていたりする認証情報を削除します。また、わかりやすいAPIと万全なドキュメントがあるため統合が簡単で、IT部門やセキュリティチームの運用負担が最小限に抑えられます。

> **「手間や負担は最小限に抑えられています。パスワードとキーの自動化やローテーションは素晴らしい機能です。」**
>
> **ティアゴ・ロサド氏、最高情報セキュリティ責任者**

KeeperPAMでパスワードや特権アクセスとともにシークレットを管理することで、人間が使用するIDと非人間IDの両方で一貫したガバナンスが可能になりました。

高水準のセキュリティ - Keeperは、ゼロトラストおよびゼロ知識のセキュリティ設計を採用し、情報保護とデータ漏えいリスクの低減に取り組んでいます。端末レベルでの楕円曲線暗号 (ECC) に加え、ボルト、フォルダ、レコードの各階層で複数層の暗号化を適用しています。さらに、多要素認証や生体認証、FIPS 140-3に準拠したAES 256ビット暗号とPBKDF2を組み合わせることで、堅牢なセキュリティ基盤を実現しています。Keeperは、SOC 2およびISO 27001に準拠しており、業界の中でも長年にわたりこれらの認証要件への対応を継続してきました。また、FedRAMPおよびGovRAMPの認可も取得しています。

組織への影響

Asiteは、KeeperのPAMプラットフォームを完全に導入し、パスワード、シークレット、特権アクセス管理を可能にすることで、IT部門とセキュリティチームの運用上の複雑さを軽減しつつ、保護を強化する統一された拡張性の高いセキュリティフレームワークを確立しました。

目に見えて分かるセキュリティ態勢改善の成果 - 認証情報とアクセス管理を一本化することで、Asiteは総合的なセキュリティ態勢を大幅に強化することができました。パスワード管理の強化、シークレットのローテーション自動化、特権アクセスの制御により、外部の脅威と内部リスクの両方にさらされる機会が減りました。認証情報はもはや手動で作成、共有、使い回しされることはなく、組織全体でセキュリティポリシーを一貫して適用できるようになっています。

重要なのは、これらの制御が測定可能かつ監査可能である点です。異なる地域や顧客環境でも、規制および契約上の要件を満たせます。

> **「KeeperPAMプラットフォームの主なメリットは、コストの削減、システム管理の負担軽減、セキュリティ要件に対するコンプライアンスの向上、セキュリティ態勢の強化です。」**
>
> **ティアゴ・ロサド氏 | 最高情報セキュリティ責任者**

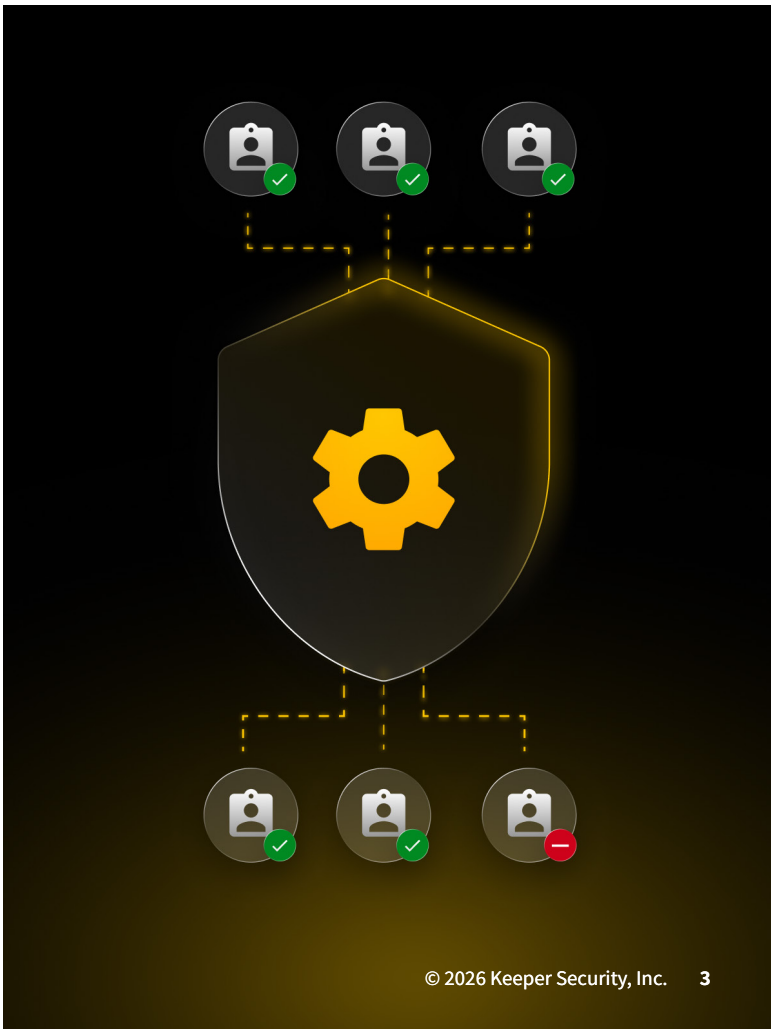
運用負担の軽減とツールの統合 - Asiteは、パスワード管理、シークレット管理、PAMを単一のプラットフォームに統合することでツールの乱立を抑え、管理を簡素化し、運用負担を軽減させました。このアプローチにより、少人数のIT部門とセキュリティチームでも、人員や運用上の負担を増やすことなく、アクセス制御をより効率的に管理できるようになり、同時に保護範囲を拡大して広範なシステムや環境を保護できるようになりました。

内部リスクの露出を抑え、説明責任を強化 - 特権アクセスを一元管理して監視することで、Asiteは高リスクのアクティビティを検出、調査、対応する能力を強化しました。セッション監視と監査証跡により、責任の所在を明確にするとともに、意図的であれ偶発的であれ、不正使用が発生する可能性を低減します。

継続的なパートナーシップと支援 – テクノロジーにとどまらず、Asiteは導入から定着までのプロセス全体において、信頼できるサポートと活用支援の重要性を強調しています。Keeperのサポートチームと支援チームは、プラットフォームを効果的に導入し、組織の運用ニーズに合致させる上で中心的な役割を果たしました。

> **「サポートの質は素晴らしく、どんなに技術的な質問でも徹底的に対応してくれました。[...] トレーニングチームも中心になって、私たちの現状に見合う研修内容をカスタマイズしてくれました。」**
>
> **ティアゴ・ロサド氏 | 最高情報セキュリティ責任者**

KeeperPAMは、Asiteのアクセスセキュリティ戦略の基盤となり、グローバルな環境で人間が使用するIDと非人間IDの一元管理を実現させました。特権アクセス、パスワード管理、シークレット管理を単一のプラットフォームに統合することで、Asiteはセキュリティを強化し、運用効率を向上させ、将来の成長を支える拡張可能な基盤を確立しました。



KeeperPAM

KeeperPAMは、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・管理する次世代の特権アクセス管理プラットフォームです。ゼロトラストおよびゼロ知識のセキュリティアーキテクチャを基盤としており、組織の規模を問わず、特権アカウントの保護、最小権限の徹底、リモートインフラの安全な運用、コンプライアンス要件への対応を支援します。高い操作性と導入のしやすさを備えている点も特長です。

Keeperは初めての方にも使いやすく、組織の規模に関係なく簡単に導入できます。KeeperPAMでは、ゼロトラストゲートウェイサービスを利用して各環境にアクセスします。ファイアウォールの更新やイングレスの変更は不要で、複雑さを排除したシームレスで安全なアクセスを実現します。リモートセッション機能では、ユーザーから認証情報やSSHキーへはアクセスできません。リソースへのアクセスは時間制限を設けることができ、アクセスが取り消されると認証情報は自動的にローテーションされるため、認証情報を公開することなくジャストインタイム (JIT) アクセスを提供します。

Keeperは、組織の規模を問わず利用できるよう設計されています。KeeperPAMでは、複数のクラウドプロバイダー、オンプレミスのワークロード、顧客環境にまたがるアクセス管理を、単一のユーザーインターフェース (UI) に集約しています。これにより、マルチクラウド環境全体を一元的に管理できます。

KeeperPAMのビジネス活用事例

- すべての特権アカウントを管理・監視
- 認証情報を開示せずにジャストインタイム (JIT) アクセスを実現
- 直感的なUIで開発ツールをひとつのプラットフォームに集約
- クラウド、ハイブリッド、マルチクラウド環境を一元的に管理
- AIによる脅威検知と自動セッション終了に対応し、複数プロトコルのセッションを記録
- パスワードローテーションを自動化
- すべてのシステムで多要素認証を強制適用
- ウェブまたはデスクトップアプリからスムーズに導入でき、SCIMによる自動プロビジョニングに対応

Keeperで組織を保護

使いやすいプラットフォームでKeeperがどのように組織を保護できるのか、詳しく知りたい方は、**営業チームまでお問い合わせ**ください。無料トライアルや、お客様に合わせたデモをご案内します。

Keeperについて

Keeper Securityは、150以上の国で幅広い企業や利用者を守る、急成長中のサイバーセキュリティソフトウェア企業です。ゼロ知識とゼロトラストを基盤とし、あらゆるIT環境に対応できるセキュリティの先駆けとして知られています。主力製品のKeeperPAM®は、AIを搭載したクラウドネイティブのプラットフォームであり、ユーザーやデバイス、インフラを包括的にサイバー攻撃から保護します。特権アクセス管理 (PAM) の分野では、ガートナー社の「Magic Quadrant (マジック・クアドラント)」において革新性が高く評価されました。Keeperではロールベースのポリシー、最小権限、ジャストインタイムアクセスを組み合わせることで、パスワードやパスキー、インフラのシークレット、リモート接続、エンドポイントを安全に管理しています。

Keeperは、世界各地の企業や利用者から高い信頼を得ています。

Gartner

KeeperPAM®を2025年版Magic Quadrant™ (PAM部門) に選出PAM

Cybersecurity Excellence Award
特権アクセス管理

Cyber Defense Magazine
エディターズチョイス - 特権アクセス管理 (PAM)

Newsweek
No.1サイバーセキュリティプラットフォーム

エンタープライズ・マネジメント・アソシエイツ KeeperPAM®、優れた製品力で高い評価を獲得