CYBERARK®
The Identity Security Company™

ソリューション概要

すべてのインフラストラクチャにおける IT 管理者アクセスの保護

特権アクセス管理プログラムの再定義

課題

IT　環境は進化しています。新たな攻撃手法が出現しています。しかし、サイバーセキュリティの主要なリスクである、漏洩したアイデンティティや認証情報は依然として変わっていません。そして、管理者が使用する強力なアカウントと認証情報が最大の標的となります。攻撃者は、最初のアクセス権を獲得すると、横方向に移動し、データの流出、ビジネスの妨害、ランサムウェアの展開が可能になるまで権限をエスカレートさせます。

適切なアイデンティティ　セキュリティの導入を怠ると、監査の失敗やコンプライアンス違反につながり、その結果、金銭的な罰則、ビジネスの遅延、利害関係者の信頼の低下を招きます。しかし、データ漏洩がビジネスの評判、業績、継続性にもたらす混乱に比べれば大したことではありません。

ハイブリッド IT やマルチクラウド IT における管理者アクセスの保護は、ますます複雑になっています。ITの進化に伴い、組織はシステムアクセスと運用アクセスの両方を総合的に保護する必要があります。

システムアクセスは、組み込みのシステムアカウントや管理者が共有する特権アカウントなど、専用のアカウントと認証情報の使用を説明します。例えば、Windows や Linux サーバー、ドメインコントローラー、データベースへのアクセスに使用されるアカウント、SaaS や IaaS 環境のルートアカウントや管理者アカウントなどです。運用アクセスとは、SaaS　アプリケーション、エラスティックワークロード、クラウドネイティブのサービス管理で使用されるアイデンティティおよびアクセス管理（IAM）ロールへのフェデレート　アクセスなど、継続的なIT運用のためにプロビジョニングされたアカウントとロールの使用を説明します。

99%

のセキュリティエキスパートが、今後 1 年以内にアイデンティティ関連の侵害に直面することに同意しており、クレデンシャル盗難が最大の懸念事項であることに変わりはありません。[1]

82%

クラウド環境、—　パブリック、または複数の環境にまたがって保存されたデータに関連する侵害の割合。[2]

第三者ベンダーによるハイリスクアクセスも課題です。一貫した可視化と制御がなければ、外部からの特権アクセスは、侵害、監査の不合格、サイバー保険への加入不能といった新たなリスクに組織をさらすことになります。

異なる環境に対して別々のソリューションを維持することは、オーバーヘッドや非効率を生み、システム全体の可視性が制限されます。また、ゼロトラストのフレームワークや持続的なランサムウェアの脅威に関する取締役会からの圧力が、この課題をさらに複雑にしています。

[1]CyberArk 2023 アイデンティティ セキュリティ脅威情勢レポート
[2]IBM　2023 データ漏えいのセキュリティ コストレポート

- すべての環境でインフラストラクチャへの安全な管理アクセス：
  - Windows および Linux サーバー、データベース
  - SaaSアプリ
  - Elastic VM、データベース、Kuberenetes ワークロード
  - クラウドネイティブサービス
- シークレット管理に拡張：
  - サービス　アカウントで使用される認証情報を保護し、ローテーションして配信します。
  - スクリプトや自動化ツールのハードコード化されたパスワードを排除します。
- 第三者ベンダーの管理に拡張：
  - VPN、パスワード、エージェント、企業デバイスを使用せずに、外部アクセスをジャストインタイムで提供します。
  - エアギャップ環境における認証情報へのオフラインアクセスを安全に提供します。
  - セッションの分離、監視、記録を一元管理し、維持します。
- IT組織が使用するマシン　アカウントにPAMの制御機能を提供し、メンテナンス　スクリプトや自動化ツールからハードコードされたパスワードを排除します。

CyberArkは、2023 Gartner® Magic Quadrant™において、特権アクセス管理のリーダーの１社に位置づけられています。

ソリューション

CyberArk Identity Security Platformから提供される特権アクセス管理（PAM）の機能は、あらゆる環境の IT チームの高リスクアクセスを保護します。

認証情報管理、ローテーション、セッションの分離などの基本的な PAM コントロールは、共有システムアカウントによる特権アクセスのリスクを大幅に低減します。セッションは隔離され、認証情報はユーザーやマシンにさらされることなく、対象システムで直接使用されます。

セキュリティチームは、オンプレミスまたはクラウドでシステムを維持、移行、拡張するために使用される運用アクセスに深層防衛制御を適用することもできます。このプラットフォームは、共有およびフェデレーションされたアクセスモデルにわたって、役割固有の最小特権ジャストインタイム（JIT）およびゼロスタンディング特権（ZSP）ワークフローを提供します。

ネイティブなユーザーエクスペリエンスとテクノロジーの統合により、 IT の採用が向上してリスク低減の利点を拡大し、運用効率が向上します。CyberArk は、強力な認証とエンドポイントの特権制御により、組織内で最もターゲットを絞ったユーザーの作業環境を保護します。

PAM の制御は、管理されていない認証情報の数、ローカル管理者権限を持つユーザー、永続権限を持つユーザーの数を大幅に削減するなど、測定可能なリスクを削減 し、同時に保護される IT 対象システムの数を増加させます。セッションの分離と保護は、横方向の移動を防止し、マルウェアの拡散を制限します。

CyberArk は、企業が監査やコンプライアンスに関する幅広い要件を満たすことができるよう支援します。このプラットフォームは、管理者アクセス権の使用と付与、アクセス認証、特権ライフサイクル管理の自動化に関する包括的なレポートを提供します。一方、リスクスコアリングを組み込んだセッションの監査証跡と記録を一元管理することで、貴重な時間とリソースを節約できます。

総合的なPAMプログラムを導入することで、企業はデジタル変革の安全性を確保しながら 意図したリスク削減、監査、コンプライアンスの成果を達成することができます。

IT 管理者アクセスを保護 する方法についてご覧ください。

Gartner® Magic Quadrant™ for Privileged Access Management，by Felix Gaehtgens，James Hoover，Michael Kelley，Brian Guthrie，Abhyuday Data，2023年9月5日.

CYBERARK®