CYBERARK®
The Identity Security Company™

電子ブック

PAM（特権アクセス管理）プログラムの再構築

インテリジェントに特権を制御し、PAMの効率性、導入効果、適用範囲を改善

目次

はじめに

現在のIT環境が複雑化しており、標的型のサイバー攻撃、クラウドやIoTの導入、生成AIなどのトレンドにより、効果的なPAM（特権アクセス管理）ソリューションに対するニーズが高まっています。脅威が進化を続け、新たな攻撃手法が次々と登場しているため、最も標的になりやすい認証情報やアイデンティティを確実に保護し、脅威の進化に後れを取らないようにする必要があります。

さらに、現在のPAMプログラムは、イノベーションによって大きく変動し、新しいアイデンティティと新しい環境によって大きく形を変える、広大で動的な脅威環境に直面しています。Okta、LastPass、Microsoft、Uberなどの大企業が最近侵害され大きな注目を集めましたが、これらのインシデントでは通常特権ユーザーではないサポート エンジニアやソフトウェア エンジニアのアイデンティティが侵害されています。例えば、SolarWindsのサプライ チェーン攻撃は、9か月も発見されず、世界中の18,000以上の組織が影響を受けました。データが侵害されると、企業の評判が著しく低下し、ビジネスが中断し収益が低下し、機密データが失われたり、法規制違反に伴う罰金が科せられたりする恐れもあります。このような現在のデジタル環境を前提にして、セキュリティ システムやプラクティスを再構築することが求められています。

「IBM X-Force脅威インテリジェンス・インデックス2024」では、重要な業界に対する攻撃の85%以上が、パッチの適用、多要素認証、最小特権の原則によって軽減できたと指摘されています。

特権アクセスが進化し、標的となり続けている現状で、多層防御戦略を採用し、PAMプログラムでは保護されてこなかった、サードパーティー ベンダー、開発者、クラウド運用チームなどの高リスクのアイデンティティを保護する必要があります。同様に、テクノロジーの継続的な進化により、PAMは、オンプレミス、ハイブリッド、クラウド環境の基盤となり、あらゆるサイバーセキュリティ戦略の重要なコンポーネントにもなっています。

本書では、次のような重要なトピックについて説明します。

1. クラウドやSaaS環境におけるPAMの重要性
2. 新しいクラウドファーストのユースケースとPAMプログラムのベストプラクティスの関係
3. CyberArkのPAMソリューションで高リスクのアクセスを保護する方法

71%

窃取や漏洩で手に入れた認証情報を使用するサイバー攻撃が前年比で増加した割合

出典：IBM X-Force 脅威インテリジェンス・インデックス 2024

クラウドやSaaSなどの動的な環境を前提にPAMを再構築する必要性

今日、ほぼすべての組織がクラウドでアプリケーションを開発して展開しています。業務運用でクラウドへの依存が高まっており、ハイブリッド クラウドやマルチクラウドIT環境において管理者レベルのアクセス権限を保護することがさらに複雑になっています。

ITの進化に伴い、システムアクセスと運用アクセスの両方を包括的に保護する必要があります。「CyberArk 2023アイデンティティセキュリティ脅威の現状レポート」によると、 **77%** の回答者が、あまりに多くの特権が開発者に付与されているため、開発者のアイデンティティが格好の標的になっていると回答しています。サードパーティー ベンダーに高リスクのアクセス権限が付与されていることも課題です。一貫性のある方法でこれらのアクセス権限を可視化して制御できなければ、外部の特権アクセスにより、セキュリティ侵害、監査の不備、サイバー保険料の加算などの新たなリスクを組織が受けることになります。多くの企業は、それぞれのIT環境に異なるソリューションを導入して管理しているため、管理負荷が増大し、効率性が低下し、システムの可視性が制限されています。

同時に、適切なアイデンティティ セキュリティを実装しなければ、監査の不備やコンプライアンス違反が発生します。これらの問題が発生すると、罰金、ビジネスの遅延、 利害関係者の信頼の低下を招く恐れがあります。2023年には、コンプライアンス違反によってデータが侵害された1件のインシデントの平均コストは**218,915** 米ドルに上昇し、年間の合計では**4.67万米ドル**に達しています。

[1]IBM、2023年「データ侵害のコストに関する調査」

あらゆる環境におけるインフラへの管理者アクセスを保護

- WindowsやLinuxのサーバー、データベース
- SaaSアプリケーション
- Elastic VM、データベース、Kubernetesのワークロード
- クラウドネイティブのサービス

シークレット管理

- サービス アカウントが使用する認証情報の保護、ローテーション、配布
- スクリプトや自動化ツールでハードコーディングされているパスワードの排除

サードパーティー ベンダーの制御

- VPN、パスワード、エージェント、会社のデバイスを使用することなく、外部アクセスをJIT（ジャストインタイム）でプロビジョニング
- エアギャップ環境の認証情報へのオフライン アクセスを安全に提供
- セッションの分離、監視、記録の一元的な制御を維持

PAM制御の提供

- IT組織が使用するマシン アカウントの保護
- メンテナンス スクリプトや自動化ツールでハードコーディングされているパスワードの排除

OT/IoTを保護するためのPAMプログラムの再構築

OT（オペレーショナル テクノロジー）のセキュリティには、不安定な旧式のテクノロジー、サポートが終了したオペレーティング システムやソフトウェア、脆弱性が存在する可能性の高いシステムが長期間利用されているなどの多くの課題が存在します。企業組織は、PAMプログラムを再構築して、高リスクのアクセスで利用される可能性がある一連のアイデンティティを保護しなければなりません。

1. デバイスの検出とファームウェアの更新

PAM（特権アクセス管理）プログラムは、ネットワークに追加された新しいデバイスやアカウントを継続的に検出してオンボーディングすることで、管理と監視を強化できなければなりません。アクセスを分離して、セッションを監視し、記録することで、有用なレポートを作成でき、コンプライアンス要件を常に満たすことができます。

一部のOTデバイスは複雑であり、環境全体が適切に可視化されていないため、それらのデバイスの特権認証情報を管理することが困難な場合もあります。

2. ゲートウェイやリモート アクセスの脆弱性

エンドポイントの特権を管理し、（可能であればデスクトップMFAを使用して）ワークステーションを保護することで、ランサムウェアやマルウェアのOTへの拡散を阻止します。EPM（エンドポイント特権管理）を導入してシステムを堅牢化し、エンドポイントの特権を厳格に保護し、最小特権の原則を強制することで、重要なシステムが不正に変更されるリスクを低減します。

PAMソリューションのリモート アクセス機能は、VPN（仮想プライベート ネットワーク）、パスワード、またはエージェントを使用することなく、認証情報が保管されるVaultへ安全にアクセスできるようにし、認証情報へのオフライン アクセスを提供します。

3. 物理的なリセット ボタン、一方向ゲートウェイ、デバイス監視に対応する多層防御

攻撃者は、新たな手法を次々と採用し、認証情報やデータを窃取しています。また、ピン先で押して初期化するなどの原始的な方法でデバイスのパスワードをデフォルトにリセットし、乗っ取ることもあります。OT環境におけるデータのフローを保護して強化することは不可欠です。

一方向ゲートウェイやデータ ダイオードをCyberArkのOTやICS（産業用制御システム）のパートナーと統合することで、PAMを回避しようとする試みを監視して検出し、不正アクセスや高リスクのアカウントの使用を防止できます。

さらに、PAMプログラムを再構築し、検証するアイデンティティや保護する環境の範囲を広げることで、特権アクセス管理のセキュリティと拡張性が向上します。PAMソリューションは、オンプレミスあるいはクラウドの両方で、永続的な認証情報とシークレットを保護し、JIT（ジャストインタイム）で特権アクセスを提供しなければなりません。

効果的なPAMプログラムの機能

PAMプログラムは、上記の課題の一部を解決し、セキュリティ環境を改善し、監査やコンプライアンスの要件を満足し、ランサムウェアを防御し、ゼロトラスト セキュリティ モデルを実装する基盤となります。ゼロトラストのアプローチを採用して、すべてのユーザーとアプリケーションを暗黙的に信頼することなく、場所やネットワークに関係なく認証と承認を求めることで、内部と外部の両方の攻撃者に対する防御が可能になります。

PAMプログラムの効果を高めるプロセス

1. 特権アクセスの制御と可視性を強化してリスクを低減する。
2. 特権制御に対するITセキュリティ監査に対応する。
3. 特権制御に対するサイバー保険の要件を満たす。
4. ベンダーやサードパーティーのアクセスを保護する。
5. PAMを全社に拡大する。

セキュリティの目標

認証情報の窃取の防止

- 認証情報の検出、安全な保管、ローテーション
- ゼロスタンディング特権によるJITアクセス
- 窃取/不正使用の検出と対応

特権の昇格の防止

- 最小特権の原則の実装
- 高リスクのコマンドの検出と対応

水平移動の停止

- セッションの分離と保護
- ローカル管理者権限の削除

インサイダーの脅威の防止

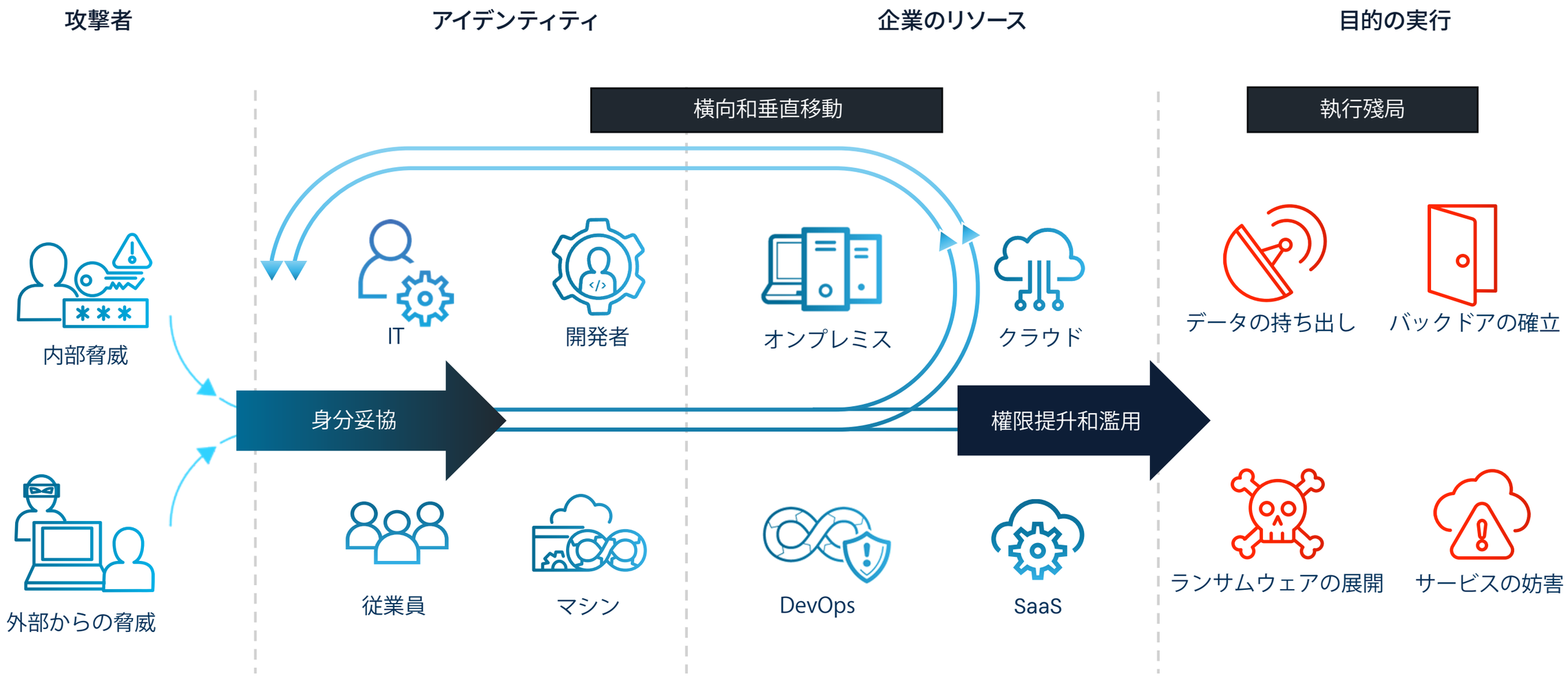
- セッションの監視と記録
- 完全な監査証跡

新たなユースケースに合わせたPAMプログラムの再構築

従来のオンプレミス サーバーからクラウドネイティブのアプリケーションなどITインフラのすべてのレイヤーにそれぞれに固有の役割があり、同時に固有のセキュリティの課題が存在します。

攻撃チェーンを理解する

侵害されたアイデンティティや認証情報は、サイバー攻撃の標的であり続けています。



1 長期間使用されるシステムにおける高レベルのアクセス権限のPAMによる制御

多くの企業が、LinuxやWindowsサーバー、データベース、社内で開発したアプリケーションなどの多くインフラを今もオンプレミスで直接管理しています。厳格な法規制が適用される業種や、金融、エネルギー、製造業などの低レイテンシーのコンピューティング環境が不可欠である業種では、特にその傾向が顕著です。これらのすでに確立されているシステムをクラウドに移行する場合、多くの組織が「リフトアンドシフト」のアプローチを採用します。これらのシステムは今も問題なく動作するため、オンプレミスのサーバーからクラウドでホスティングするVM（仮想マシン）に移行すれば、再設計は不要となります。

長期間使用されるシステムがオンプレミスあるいはクラウドのいずれかに存在する場合、これらのワークロードへの高リスクのアクセスが許可される特権認証情報やSSHキーの保護が不可欠となります。Linuxサーバーのルートアカウントなどのサーバーやに組み込まれたアカウントでは、これは特に重要です。

認証情報の自動ローテーションや最小特権の原則などの基本的なPAMのベストプラクティスにより、認証情報が窃取されるリスクが軽減されます。セッションを分離することで、エンドユーザーがターゲット リソースに直接接続できないようにすることでリスクをさらに低減し、マルウェアの拡散を抑止できるようになります。また、セッションを記録することで、特権セッションで実行されたコマンドやキャプチャされたキーストロークを証拠として監査で利用できるようになります。ITセキュリティのコンプライアンス要件を満たし、サイバー保険の支払いを受け取るためには、このような制御が必要になることもあります。

重要な戦略

優れたアイデンティティ セキュリティ プログラムには、多くのレイヤーが必要です。認証情報の保護に加えて、特権セッションの監視や分離などのPAMのベストプラクティスを追加して適用する必要があり、これは、ランサムウェアやその他のマルウェアがVMに到達するのを防止するのと同時に、内部脅威を阻止するのにも役立ちます。

2 VMで動作するワークロードへの運用アクセスのPAMによる制御

多くのVMは短時間利用されます。これは、クラウド コンピューティングの重要な利点にもなっています。クラウド コンピューティングを利用することで、インフラのメンテナンスに時間やコストを費やすことなく、レンタルしたVMでワークロードを実行できます。特定のVMでは、高リスクの管理者権限が必要となる場合もありますが、通常企業は、これらの使用期間が短いマシンへのアクセスに使用するシステムレベルの専用アカウントを作成することはなく、関連するリスクも発生しません。

PAMプログラムは、使用期間が短いワークロードへのアクセスを保護するときに重要な役割を果たします。特定のセルフマネージド システムへのアクセスが必要な場合、JIT（ジャストインタイム）でアクセス権限を昇格することで、認証情報が窃取されるリスクを低減し、永続的に利用される特権を減らすことができます。アイデンティティ セキュリティチームと開発者は、CSP（クラウド サービス プロバイダー）のタグ付け機能を利用して、特定のプロジェクトのワークロードにタグ付けすることで、特定の属性がタグ付けされたリソースのみへのネイティブ接続をエンドユーザーに許可できます。ITチームや開発チームは、ABAC（属性ベースのアクセス制御）を使用して、SSH（セキュア シェル）キーやパスワードレスアクセスをネイティブに昇格させることができます。また、ユーザーには、永続的な権限があるパスワードが付与されないため、認証情報が窃取されるリスクも大幅に低下します。

重要な戦略

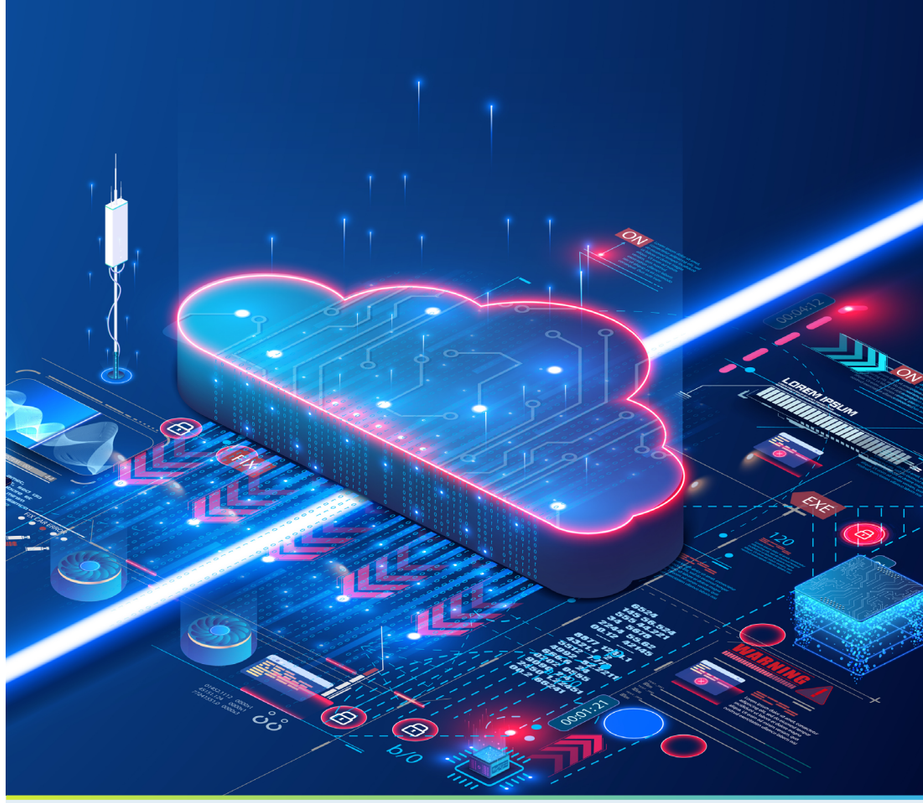
認証情報がなければ、信頼できないわけではありません。ゼロトラストの概念をクラウドでのアクセスに導入すると、「決して信頼せず、常に検証する」という考え方を取り入れることになります。最小特権の原則を適用し、セッションの分離などのPAMのベストプラクティスを取り入れることで、曖昧な信頼を制限できるようになります。同時に、適応型多要素認証（MFA）を実装してアイデンティティの検証を強化する方法も効果的であることが実証されています。

3 クラウド サービス プロバイダーによるサービスへのアクセスを保護

クラウドにおける最も強力なアクセス権限を保護することは不可欠です。これらの権限には、アプリケーションが利用するサービスを起動、構成、保守する目的でエンジニアが使用するアクセス権限も含まれます。エンジニアがWebコンソールあるいはCLI（コマンドライン インターフェイス）でこのクラウド管理レイヤーにアクセスする場合も、そのアクセスを保護する必要があります。

JITでアクセス権限を昇格すれば、このような状況で認証情報が窃取されるリスクを軽減できます。多くの組織が、ゼロスタンディング特権（ZSP）という新しいセキュリティの概念を採用して、業務の効率性を低下させることなく開発チームを保護しています。このモデルでは、エンジニアは、実行する作業に必要な権限が付与されたロールに限定して、JITでアクセスを昇格できます。これは、最小特権の原則が適用されていることを意味します。

ZSPを導入することで、多層防御によるリスク軽減が可能になります。第一に、開発者に常時アクセスが可能な認証情報が付与されないため、認証情報が窃取されるリスクは大幅に低下します。第二に、開発者が悪意のあるインサイダーになったり、開発者のアクセス権限が侵害されたりした場合も、開発者の権限は制限されるため、攻撃による活動範囲が小さくなります。



重要な戦略

ZSPは、開発者の作業を遅延させるのではなく、加速させます。重要な機能が停止したり深刻なシステム障害が発生したりするときに、エンジニアは、権限の昇格を要求し、緊急の問題を解決するために、使い慣れたツールを使用する必要があります。このようなケースに対応し、PAMの採用を意味あるものにするには、開発ツールとの統合が不可欠です。セッションを監視して内部脅威を阻止し、コンプライアンスを遵守するために監査証跡を維持する場合にも同じことが言えます。

4 SaaSアプリケーションへの高リスクなアクセスを保護

リスクは、インフラ、ネットワーキング デバイス、サーバー、OTの環境だけにとどまりません。ソフトウェア エンジニアから人事や財務の管理者までのあらゆる従業員が使用する、クラウドでホスティングされるWebアプリケーションにもリスクは存在します。このようなアクセス権限が重大なセキュリティ リスクとなるのは、これらの権限が使用されると攻撃者も機密データにアクセスできるようになるためです。

Webブラウザ セッションを保護して監視することで、クラウドにおけるこの高リスクのアクセス権限が使用される最後のレイヤーを保護できます。セッション保護は、セッションの乗っ取りやクッキー窃取攻撃からの防御を可能にします。インフラやコンソールへのアクセスと同様、高リスクのセッションを監視することで、ユーザーアクティビティの完全な監査証跡が提供され、コンプライアンス要件を満たし、インサイダー攻撃を抑止できます。12

重要な戦略

必要なレベルのクラウド セキュリティを実現するには、SaaSアプリケーションのデータのリスクレベルに応じて制御を調整します。例えば、知的財産や電子カルテのデータを含むアプリケーションへのアクセスが侵害される場合、トレーニング アプリケーションがアクセスされるよりもリスクは高くなります。高リスクのインフラへのアクセスをPAMで保護するのと同じように、最も機密性の高いデータを扱うWebアプリケーションでステップアップ認証を必須にすることは、リスクを大幅かつ簡単に低減できるベストプラクティスです。

5 アクセスとシークレット管理による PAMプログラムの進化

マルチクラウド環境で特権アクセスが必要になるアイデンティティはユーザーだけではありません。サーバーレス関数、アプリケーション アカウント、RPA（ロボティック プロセス オートメーション）ボットなどのマシンのアイデンティティも、認証情報を使用して、自動のプロセスを認証します。PAMツールのすべての機能、特に、DevOpsのユースケースでシークレット管理やIaaSを可視化するクラウドインフラ権限管理（CIEM）を広く利用することで、PAMプログラムを適用できる範囲とその効果が拡大します。セキュリティ チームが堅牢な特権アクセス管理の基盤を確立した後に注力する必要があるのは、特権アクセスが使用されるあらゆる領域にアイデンティティ セキュリティ プログラムを広く適用することです。そのためには、開発チームの作業を遅延させたり、オートメーションを遅らせたりすることなく、重要な資産にアクセスするサイクル全体で人とマシンのアイデンティティを保護しなければなりません。

PAMプログラムを再構築してIT管理者のアクセスを保護する

CyberArkのアイデンティティ セキュリティ プラットフォームのPAMの機能は、社内のIT管理者やサードパーティー ベンダーに対して包括的なセキュリティを提供し、オンプレミスやクラウドにあるシステムの保守、移行、拡張で使用される高リスクのアクセス権限を保護します。

CyberArk 是唯一擁有身分安全平台的供應商，該平台可以為客戶提供靈活性，根據身分類型和需要訪問的特定目標提供常設訪問、即時訪問或零常設權限訪問

JITのアクセス権限制御は、システム、アプリケーション、その他の高リスクの領域で使用されるアクセス権限を一時的に昇格するときにパスワードを不要にして、認証情報の窃取を防止します。ゼロスタンディング特権（ZSP）によって、セキュリティ チームはJITの概念を利用して、PAMプログラム全体を新たなレベルに引き上げることができます。ZSPであれば、JIT（ジャストインタイム）で、実行するタスクに必要な資格だけがユーザーに付与されます。

セキュリティ チームがZSPを実装する利点

- 常時アクセスを防止することで、認証情報が窃取されるリスクを低減します。
- クラウドで必要な場合に必要な権限だけをユーザーに付与することで、最小特権の原則をリアルタイムで適用します。
- アカウントの乗っ取りによる影響を軽減します。管理者レベルのアクセス権限がなければ、攻撃者が実行できる操作は極めて限定されます。
- 開発者が使い慣れているワークフローをそのまま使用できるように統合することで、ユーザーに合理的なアクセス環境を提供できます。これにより、エンドユーザーへの導入が大幅に促進されます。
- 定義可反映與雲端使用者工作相關的廣泛用例的可自訂策略。

PAMプログラムを再構築し、優れた成果を達成する

1. 目に見える形でサイバーリスクの削減を実現

高リスクのアカウントを特定してオンボーディングし、安全に管理することで、認証情報の窃取や個人情報の漏洩を防止します。インテリジェントな特権制御と最小特権の原則を実装することで、オンプレミスおよびクラウドの両方のインフラで、ラテラルムーブメントを削減し、ユーザーの脅威となるすべての行為を防止します。

2. 運用の効率化

認証情報の管理やゼロスタンディング特権によるアクセスなど、PAMを統合してサポートすることで、システムアクセスと運用アクセスの両方を保護できます。数百のインテグレーションとネイティブUXを利用することで、IT、サードパーティー ベンダー、開発者、クラウド運用ユーザーへのPAMの導入を加速することができます。

3. 監査とコンプライアンスへの対応

業界のベストプラクティスを遵守していることを証明し、コンプライアンス要件を継続的に満たすことができます。特権認証情報を安全に管理し、ローテーションします。最小特権の原則を実装し、ユーザー セッションを監視することで、SWIFT、SOC、ISO 27001などのグローバルの法規制にも対応できます。

4. デジタル トランスフォーメーションの保護

ITや開発者によるクラウド環境のあらゆるレイヤーへのネイティブ アクセスを保護します。リフトアンドシフトシステムから柔軟性に優れるワークロードとクラウドネイティブ サービスへ移行できるように支援し、特権制御をサードパーティー ベンダーにまで拡大します。シークレット管理を統合し、クラウドネイティブのアプリケーションが動作するマシンのアイデンティティを保護します。

ハイブリッド/マルチクラウド環境でのPAMのベストプラクティス

現在のPAMプログラムでは、組織全体の標準的なアクセス管理プロセスを一元的に定義して実装できます。これにより、ビジネス部門が異なるために発生していた運用の分断や非効率性が軽減されます。クラウドにおける特権アクセス保護のベストプラクティスを以下に紹介します。

基本的な要件への対応

- ゼロスタンディング特権を実装することで、常時アクセスを、ロール、ワークロード属性、責任、アクセスニーズに基づいて構成したポリシーに置き換えます。
- 開発者が使用しているワークフローをそのままサポートし、既存のツールと統合することで、シームレスでネイティブなアクセスを開発者に提供します。
- クラウド サービス プロバイダー (CSP) のルート アカウントと登録アカウントの利用を禁止し、利用されるすべてのアカウントについて、認証情報の厳格な保管、ローテーション、MFA、セッション分離を導入します。
- シークレット管理と統制を単一のハブに一元化して、開発者がツールを自由に使用できるようにし、企業は業界や社内の標準的なプロセスを適用できるようにします。
- 最初は、業界の規制を遵守するために標準的なプロセスに対応することに重点を置きます。

監査とレポートの標準化

- 監査担当者から証拠、成果物、レポートを要求されることを前提にして、プロアクティブな戦略を策定します。中核的な取り組みとして、すべてのアイデンティティのアクセスを継続的に可視化します。
- 危機的な状況 (CritSit) が発生したときのアクセスを許可するモデルを定義しておき、派遣されるクラウド エンジニアリング チームが承認を待つことなく迅速に問題を解決できるようにします。
- クラウド ワークロードやサービスに対する高リスクのアクセスを監視し、監査証跡をWebアプリケーションやオンプレミスのセッション ログと同じ場所に保存して、プロセスを合理化します。

継続的な改善

- すべての新しいクラウド環境に安全なアクセスを実現するポリシーが展開され、ロールとアイデンティティが正しく構成されており、プロビジョニング後に問題を修正する必要がないことを確認します。
- 自動化を利用して、人やサービス間のアクセスに業界や社内の標準を適用します。
- コンプライアンスと監査レポートのプロセスを自動化し、手動の作業を軽減して効率化します。

インテリジェントな特権制御をあらゆるアイデンティティと環境に提供

インテリジェントな特権制御は、あらゆるアイデンティティの保護に役立ちます。あらゆるアイデンティティを継続的に監視して分析することで、異常な行動の検知とレスポンスが可能になります。以下の5つの重要なインテリジェントな特権制御を提供します。

ZSP（ゼロスタンディング特権）とJIT（ジャストインタイム）のアクセス

常時利用できる特権を削減することは、アイデンティティの侵害とラテラルムーブメントを防止するために不可欠です。ZSPを導入することで、組織はリアルタイムで、必要な場合のみアクセス権限を昇格してユーザーに付与し、タスクが完了したらアクセス権限を失効させることができます。

これにより、認証情報が窃取されるリスクやアカウント乗っ取りの影響が軽減されます。ZSPを使用することで、JITの概念を次のレベルに引き上げ、攻撃者が実行できる操作を大幅に制限して、認証情報窃取のリスクとアカウント乗っ取りの影響を軽減することができます。特に、クラウド サービスへのアクセスのTEA（時間、資格、承認）設定を制御することで、攻撃対象領域を大幅に軽減できます。

セッションの分離と監視

セキュアで分離されたリモート特権セッションを確立し、そのセッションのすべてのアクティビティを監視して記録します。エンドユーザーがターゲット システムに直接接続しないため、マルウェアが拡散するリスクが軽減されます。セッションを記録して、安全かつ一元的に保存することで、コンプライアンス要件を常に満たすことができます。

PAM（特権アクセス管理）への安全なリモート アクセス

完全なセッション分離、監視、監査の機能により、社内の重要なインフラやリソースへの安全なアクセス権限をサードパーティーが利用できるようにして、デジタル ビジネスを推進できるようになります。JITのプロビジョニングによってゼロトラストの特権アクセスをサードパーティーに提供することで、安全で分離されたセッションを実現できます。

エンドポイントの最小特権の原則

継続的に最小特権の原則を適用し、アプリケーションのコンテキスト、パラメータ、属性などの変数を考慮して、特定のスクリプト、アプリケーション、または操作を許可またはブロックするようにして、エンドポイントを管理および保護できます。これにより、組織の攻撃対象領域を大幅に削減し、さまざまな規制要件に対応できます。

認証情報とシークレット管理

認証情報の管理には、パスワードやキーのローテーション、パスワード ポリシーの適用、アクセスを要求元の一貫性ある認証などが含まれます。シークレット管理により、マシンなどの人以外のアイデンティティにも同様のセキュリティ ポリシーを適用できるようになります

コンプライアンス要件への対応の改善

効果的なPAMプログラムは、組織がセキュリティ関連の法規制要件に対応する際にも役立ちます。具体的には、効果的なPAMプログラムを採用することで、例えば次のような法規制の要件への対応が可能になります。

全業種に適用されるセキュリティ関連の法規制

- SOC 3
- NIST SP 800-207ゼロトラスト アーキテクチャ
- ISO/IEC 27001
- PCI DSS（ペイメントカード業界データセキュリティ基準）
- SOX（サーベンス オクスリー法）財務不正管理
- CMMC（サイバーセキュリティ成熟度モデル認証）
- EU GDPR（一般データ保護規則）

金融機関に適用される法規制

- SWIFT Customer Security Controls Framework
- DORA（デジタル オペレーショナル レジリエンス法）
- MAS TRM（テクノロジー リスク管理ガイドライン）
- GLBA（グラムリーチ ブライリー法）
- SEC提出期限と自動化の役割
- IRS（Internal Revenue Service）1075

医療機関に適用されるセキュリティ関連の法規制

- HIPAA（医療保険の相互運用性と責任に関する法律）
- HITECH（経済的および臨床的健全性のための医療情報技術に関する法律）
- イツ連邦データ保護法、PDSG（Patientendaten-Schutz-Gesetz）

重要インフラのセキュリティに関する法規制

- EU NIS2（Network and Information Systems）指令
- ドイツの重要インフラに関する法規制
- フランスの軍事プログラミング法
- オーストラリアの重要インフラ安全保障法
- シンガポールのサイバーセキュリティ法

CyberArk Blueprint

CyberArk Blueprintは、効果的なPAMプログラムの計画と実装を支援するベストプラクティス フレームワークです。価値とリスクの高いターゲットを特定して、PAMの取り組みと範囲の優先度を決定することで、潜在的なリスクの削減によって得られる効果を考慮して投資できるようになります。

CyberArk Blueprintは、「侵入されることを想定した」アプローチをPAMに採用することで、システムに侵入してネットワーク内を移動し、システムを混乱させる目的で攻撃者が利用することの多い戦術から組織を守ります。CyberArk Blueprintの以下の3つの指針が、顧客の環境の保護と脅威の封じ込めに役立ちます。

- **認証情報の窃取の防止：** 管理者アカウントのパスワードでも、あるいはアプリケーションのトラフィックの保護に使用するSSHキーでも、認証情報の保護は、顧客の環境を保護する最初のステップになります。
- **水平方向と垂直方向の移動の防止：** 認証情報でアクセスできる領域の境界を明確に設定し、認証情報のランダム生成を適切な方法で実施することで、攻撃者が、ワークステーションなどの価値の低いターゲット
- **特権の昇格や悪用の制限：**最小特権の原則を実装して、攻撃を封じ込め、暗黙的に信頼されるゾーンを削減し、攻撃者が活動できる範囲を最小化します。

まとめ

多くの組織では、ワークロードやアプリケーションをクラウドへ移行する計画が進行していますが、クラウド コンピューティングの拡張性や柔軟性を利用する際には新たな課題にも直面しています。クラウド環境は極めてエラスティックであり、セキュリティの責任を共有するモデルが適用されることから、変化に柔軟に適用できる動的な保護と管理機能が必要です。PAMプログラムの効率を向上させることで、認証情報の管理、セッションの分離と監視、短期間しか利用されない動的なクラウド ワークロードへの対応が可能になり、共有アカウントや特権アカウントを保護できます。新たなステップへと踏み出し、PAMプログラムを最新化することで、PAMを導入する価値を最大化し、サイバー脅威に対するレジリエントな組織を実現してください。

CyberArk Blueprint によって効果的なPAMプログラムを再構築する方法の詳細についてご覧ください。

貴社の具体的なニーズをぜひお聞かせください

デモのリクエスト

CyberArkは、アイデンティティ セキュリティのグローバル リーダーです。CyberArkは、インテリジェントな特権制御を中心に、ビジネス アプリケーションから分散型のワークフォース、ハイブリッド クラウド ワークロード、DevOpsライフサイクル全体までの人またはマシンのあらゆるアイデンティティに対する最も包括的なセキュリティを提供しています。世界中の業界をリードする企業が、CyberArkを採用して、自社の最も重要な資産を保護していますCyberArkの詳細については、www.cyberark.com/ja/をご覧いただくか、CyberArkのブログをお読みいただくか、Twitter（@CyberArk）、LinkedIn、またはFacebookをフォローしてください。

CYBERARK®
The Identity Security Company™