ソリューションの概要・エンタープライズ IAM

ca technologies

どうすれば組織内部の脅威に対抗できるか

エンタープライズ IAM が提供する効果的な対策をご紹介します。

CA Technologies が提供する多層防御エンタープライズ・アイデンティティ / アクセス管理ソリューションを活用したゼロトラスト・モデルを採用すれば、進化し続ける脅威に対して、それが内部の脅威でも外部の脅威でも、包括的な戦略を確立できます。

概要

課題

データは組織にとって不可欠であり、意思決定に使用されるだけでなく、何が起きているかを知らせてくれます。どの業界でもアプリケーションによるデジタル・トランスフォーメーションが進んでいますが、これらのアプリケーションは、ユーザとデータとをつなぐ新しいインタフェースに過ぎません。データには価値があります。それを所有する組織にとっても、このデジタルの宝物を盗もうとする現代の海賊にとっても。企業は、データを外部の攻撃から守るために熱心に取り組んでいますが、脅威はますます組織内部からやって来るようになっています。 金銭的利益のために機密データを悪用しようとする内部関係者や、うっかりフィッシング・メールをクリックして自分のクレデンシャルを盗まれてしまう不注意な内部関係者に対して、どのような防御策を講じればいいでしょうか。

ビジネス・チャンス

CA Technologies は、多層防御エンタープライズ・アイデンティティ / アクセス管理（EIAM）アプローチを提供しています。CA の特権 ID アクセス管理（PAM）ソリューションは、不正アクセスや特権アカウントの不正使用を防いで、内部の脅威や標的型の侵害と戦います。CA Single Sign-On は、すべてのオンライン・アプリケーションについて類似のアクセス制御を実施します。CA Threat Analytics for PAM は、機械学習とリスク分析を組み込んで、異常な動作を特定するための基準となる動作を確立します。CA Advanced Authentication は、機密情報へのアクセスを許可する前にユーザのアイデンティティを適切に検証することで、ログイン・プロセスを強化し、不注意な内部関係者の脅威を軽減します。最後に、CA Identity Suite は、最小限の特権という原則を適用すると同時に要求者と承認者の両方にとって機能性が高く使いやすいエクスペリエンスを提供できるガバナンスを実現するユニークなアプローチを提供します。

メリット

最近の EIAM ソリューションは、企業データのセキュリティとユーザ・アクセスの簡便性との適正なバランスをとります。そして、それが内部の脅威であっても外部の脅威であっても、進化し続ける脅威に対する包括的な戦略を提供します。従来のアイデンティティ / アクセス管理（IA）技術がユーザ動作分析によって強化されて、摩擦がさらに軽減し、リスクが高まったときの緩和プロセスが自動化されました。つまり、CA Technologies の EIAM ソリューション・スイートは、企業の IT アプリケーション、データ、インフラストラクチャへのアクセスを管理・制御してリスクを最小化し遵守性を改善するための、最高の基盤を提供します。

背景

標的型の大規模な攻撃が成功してデータが漏えいすると大ニュースになりますが、組織に対する脅威は外部の攻撃者だけではありません。企業は、金銭的利益のために機密データを悪用しようとする内部関係者や、うっかりフィッシング・メールをクリックして自分のクレデンシャルを盗まれてしまう不注意な内部関係者からデータを守ることについても、しっかりと取り組む必要があります。

Cybersecurity Insiders による最近の調査で、回答者の 90% が内部の脅威に対して脆弱だと感じていることがわかりました。この調査では、内部の脅威がほとんどの人が考えるよりも広がっており、さらに増大しつつあることもわかりました。実際、回答者の 53% は過去 12 か月間に内部関係者による自社への攻撃を経験したと報告しており、20% は 12 か月の間に 6 回以上の攻撃があったと報告しています。また、27% の回答者はこの期間中にもっと頻繁に攻撃があったと報告しています。[1]

さらに、Verizon の「2017 Data Breach Investigations Report（データ侵害調査レポート）」には次のように記されています。「悪意のある内部関係者は、データの山をつかみ取ってきれいに包装して WikiLeaks にプレゼントする人ばかりではありません。このようなデータ流出は、大ニュースになって脚光を浴び、おそらく最後には攻撃者が刑務所に入れられます。もっと一般的なのは、データをいつか現金化したいと考えて持ち逃げする平均的なエンドユーザです（60%）。社員はときどき好奇心に負けて、無許可ののぞき見をすることがあります（17%）。」[2]

これらすべてを踏まえて、企業はどうすれば内部の脅威に対抗して組織を守れるでしょうか。良いニュースは、調査によると回答者の 73% が、内部関係者の攻撃を検出して防止するための適切な制御が確立されていると感じていることです。悪いニュースは、その制御が非常に有効だと感じている人が 33% しかいないことです。企業は自ら講じた制御の有効性をどの程度確信できているのでしょうか。 既存の制御を改善するために何ができるでしょうか。

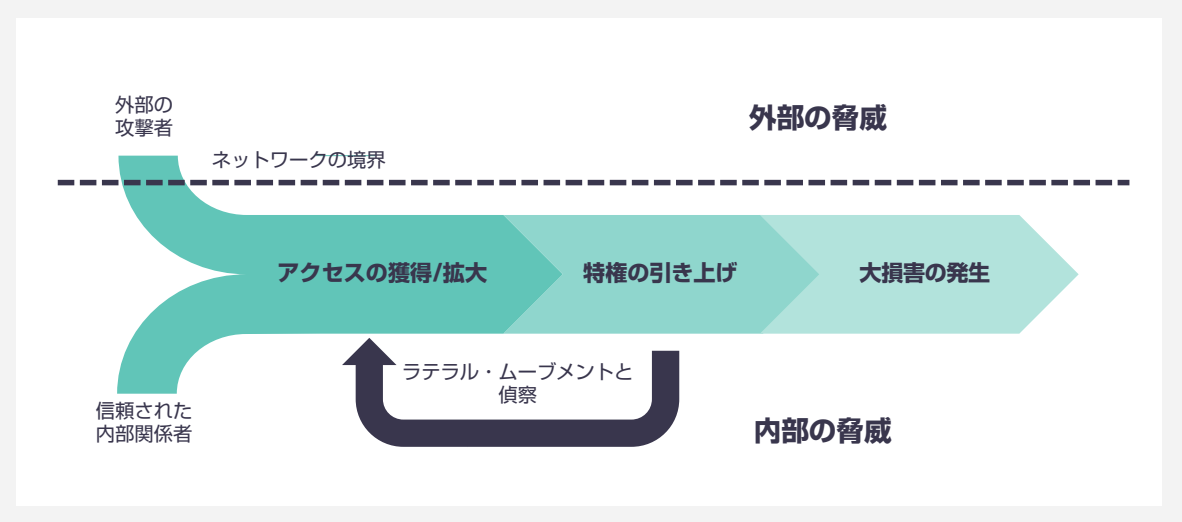
このソリューションの概要では、内部の脅威の性質とインパクトについて説明し、特権 ID アクセス管理に対する CA Technologies の包括的なアプローチを使って潜在的な攻撃を緩和する方法を見ていきます。

キル・チェーンと内部の脅威のジレンマ

Lockheed Martin 社のサイバーセキュリティ・チームはまず、一般的なデータ漏えいを狙った攻撃ベクターを特定し、それを「キル・チェーン」と名付けました。その攻撃経路のどこかを断ち切れば攻撃を阻止（つまり「キル」）できるからです。キル・チェーンは、攻撃者が首尾よく目的を果たすために達成しなければならない一貫した予測可能な一連の手順で構成されます。一部のキル・チェーンは複雑すぎて説明が難しいものもありますが、一般的なデータ漏えいキル・チェーンに伴う鍵となるステップについて簡単に示します。

次の図に示すように、その手順は驚くほど単純です。攻撃者は、すでに持っているクレデンシャルとアクセス権を悪用して（信頼された内部関係者の場合）、または侵害によってそのようなクレデンシャルを入手して（外部の攻撃者の場合）、アクセスを獲得します。アクセスを獲得した攻撃者は通常、次のステップとして他の特権クレデンシャルを侵害することによって自分の特権を引き上げます。攻撃者が非常に幸運でない限り、最初に侵害したシステムが最終ターゲットであることはまずありません。したがって次

図 1.
データ侵害のキル・チェーン・プロセス



のステップでは、ネットワークを偵察して、最終目標に向かってシステム間およびサーバ間を移動していきます（ラテラル・ムーブメント）。このプロセスは、攻撃者が目標に到達して目的のデータを盗んで大損害を引き起こすまで繰り返されます。

Cybersecurity Insiders の調査により、最も攻撃されやすいのは企業の機密情報（財務データと顧客データ）であることがわかりましたが（57%）、2 番目に攻撃されやすいのは特権アカウント情報（パスワード、クレデンシャルなど）でした（52%）。残念ながら、この 2 つは相互に関連していて、2 番目を盗めば 1 番目も盗めます。

アイデンティティは最も頻繁に侵害される攻撃ベクターです。Verizon の 2017 年の侵害レポートでは、侵害の 81% が、紛失したか盗まれたか脆弱なクレデンシャルが使われていたことが明らかになりました。したがって、キル・チェーンを断ち切るための最も一般的なアプローチは、アクセスを監視して、盗まれたログイン・クレデンシャルに対する防御を固めることです。しかし、このアプローチを内部の脅威に対して適用するのは外部に対するよりはるかに困難です。自分のアクセス権を使用する内部ユーザの目的が正当かそうでないかをどうすれば判別できるでしょうか。

しかし、特定より重要なのは阻止です。残念ながら、攻撃を数分で検出できたと述べた回答者はわずか 22% です。攻撃を数分で検出して阻止できたと感じた回答者はさらに少なく、わずか 17% です。これは、大多数の組織が攻撃の発生から数時間経過してしまうまでその攻撃の検出も阻止もできないことを意味します。そしてその時間に、すでに大きな損害が生じている可能性があります。その主な理由の 1 つは、内部の脅威に対抗する従来の技術の多くが、静的なルールに基づいており、現在の攻撃に対して効果がない可能性があります。企業は、特権アカウントの安全を確保する必要があるだけでなく、侵害されたアカウントや悪意のある内部関係者の検出を自動化し、それらの攻撃が損害を与える前にリアルタイムで阻止する必要があります。

これらの課題に対する戦略的な解決策は、機械学習とリスク分析を組み込んだ最新の特権 ID アクセス管理技術であり、大規模なエンタープライズ・アイデンティティ / アクセス管理フレームワークと統合してフル機能の特権アイデンティティ・ライフサイクル管理とガバナンスを提供します。

内部の脅威および標的型の侵害との戦い

企業は内部関係者による侵害を防御するために、すべての物理、仮想、そしてクラウドベースのアプリケーションおよびシステムについて、特権アカウントへのアクセスを管理・制御する必要があります。多層防御 EIAM アプローチを活用したゼロトラスト・モデルを採用すれば、進化し続ける脅威に対して、それが内部の脅威でも外部の脅威でも、包括的な戦略を確立できます。

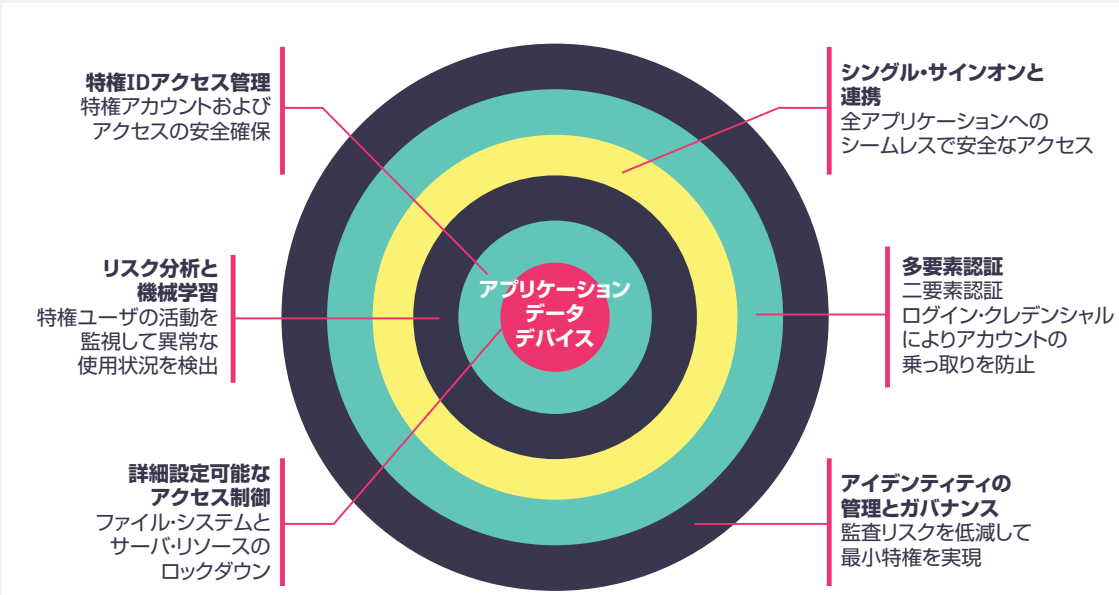
図 2 に示すように、最近の EIAM ソリューションは複数の防御層で構成されています。それぞれについて見てみましょう。

特権 ID アクセス管理

ほとんどの組織にとって、開始点は特権 ID アクセス管理（PAM）です。Cybersecurity Insiders によれば、特権アカウント情報は 2 番目に最も標的とされるデータですが、内部関係者やハッカーが特権アカウントを使って機密データにアクセスすることが多いため、それは驚くに値しません。

特権アカウントには、システム管理やネットワーク管理の直接的かつ実際的な責任を負う社員だけでなく、ベンダ、請負業者、ビジネス・パートナー、および組織内のシステムへの特権アクセスを付与された人たちも含まれます。多くの場合、特権アカウントは人ですらなく、ハードコーディングされた管理クレデンシャルによって権限を与えられたアプリケーションや構成ファイルであることもあります。PAM ソリューションは、特権アカウントへの不正アクセスを防止し、特権のエスカレーション、偵察、およびラテラル・ムーブメントを制限し、特権ユーザの活動を監視、記録、および監査することにより、キル・チェーンを断ち切って攻撃者を阻止し侵害を防ぐための複数の手段を提供します。

図 2.
包括的なエンタープライズ・アイデンティティ / アクセス管理



CA Technologies は、相互に補完的な 2 つの特権 ID アクセス管理ソリューションを提供しています。

- **CA Privileged Access Manager（CA PAM）**では、特権ユーザと、特権ユーザがデジタル・インフラストラクチャへのアクセスや管理に使用するクレデンシャルを防御し、管理できます。CA PAM は、特権ユーザ・アクセスに対してセキュリティ・ポリシーと役割ベースの制限をプロアクティブに適用し、仮想、クラウド、そして物理環境における特権ユーザの活動を監視し記録します。CA PAM はパスワード・ボールトです。つまり、特権アカウントのパスワードを発行、管理するプロキシベースのゲートウェイです。このソリューションは、侵害されたクレデンシャルへの対応に役立ちます。特権アカウントのパスワードを、エンド・ユーザの手に渡らないように、保管し管理します。さらに、どのユーザがそれらのアカウントをチェックアウトして使用できるかも制御できます。
- **CA Privileged Access Manager Server Control** は、物理サーバー上のオペレーティング・システム・レベルのアクセスとアプリケーション・レベルのアクセスに対して、ローカライズされた詳細設定可能なアクセス制御と保護を提供します。CA Privileged Access Manager Server Control は、最も重要なインフラストラクチャにセキュリティの層をもう 1 つ付け加えるエージェントベースのソリューションです。

詳細については、最近公開された「Gartner Market Guide for Privileged Access Management (ID: G00315141)」を参照してください。サイバーセキュリティ市場のトレンドと、適切なソリューションを選択するためのアドバイスが記載されています [3]。

シングル・サインオン

前述したように、Cybersecurity Insiders の調査で、一般社員も特権を持つ IT ユーザーも両方とも、組織に対する最大の内部関係者によるセキュリティ・リスクを生じさせていることが明らかになりました。しかし、一般ユーザと特権ユーザの違いは何でしょうか。その違いは、ユーザに付与された特権か、特定の時点で使用されるアクセス権と活動に基づいています。実際には、組織はビジネス・ユーザが使用できる機能を増やし続けており、一般ユーザのアクセス権が引き上げられて、ほぼ「特権アクセス」と言えるものになっています。したがって、シングル・サインオン・ソリューションも、内部の脅威になり得るプログラムの一部と見なす必要があります。

企業がオンライン・サービスを社員、請負業者、パートナーに提供する方法を急速に拡大するにつれて、いつでもどこでも、どのデバイスからでも便利にアクセスできることを新たな標準にする必要が生じました。Web アクセス管理（WAM）において、従来のシングル・サインオン（SSO）の使用は、PAM ソリューションへのアクセスも含めて、リソースへのアクセスを制御するために不可欠でした。SSO はシームレスで安全なエクスペリエンスをユーザに提供し、Web ベースのアプリケーション間をユーザが簡単に移動できるようにしたり、パートナーのドメインとの連携を可能にします。この種のソリューションは、すべての Web ベースのアプリケーションにアクセス制御を適用するための手段も提供していました。

CA Technologies は、市場をリードする 2 つのアクセス管理ソリューションを提供しています。

- **CA API Management** は、API 層のセキュリティを一元管理し、ほとんどの厳しい規制および遵守性の基準を満たします。アプリケーション、モバイル、および IoT に対するアクセス管理を拡張し、CA Advanced Authentication と CA Single Sign-On と統合されて、すべてのアクセス・チャネルで便利で一貫したユーザ・エクスペリエンスを提供します。
- **CA Single Sign-On（CA SSO）** は、モバイル、Web、および SaaS アプリケーションに対して、それがホストされている場所やアクセス方法に関係なく、安全で柔軟なアクセス管理を提供します。拡張性に優れ、何百ものサイトのミッションクリティカルなデプロイで有用性が実証されている CA SSO は、IT 部門とアプリケーション開発者が共有できる標準に基づいたフレームワークを使用して、ユーザの身元とユーザが何をしようとしているかを特定して適切なアクセス・ポリシーを適用することで、セキュリティを向上させます。

リスク分析と機械学習

CA PAM や CA SSO などのアクセス管理技術は、保護対象の IT リソースへのアクセスを管理・制御することに長けており、セキュリティ・ポリシーに基づいてアクセスを許可 / 拒否したり、特定のアクションを阻止することができます。

しかし、現在のセキュリティ侵害の多くは、アカウント（特に特権アカウント）の悪用から始まっています。特権アイデンティティに関連したセキュリティ侵害は、インパクトもきわめて大きくなります。攻撃者が正規のユーザ・アイデンティティを使ってアクセスした場合、そのアイデンティティでアクセス可能なすべてのデータとシステムにアクセスできることになります。こうした攻撃は数週間あるいは数か月にわたって発見されないことも多く、攻撃者はその間にシステム内を縦横に移動してしまいます。従来のアクセス管理ソリューションは、この新たな現実に適応する必要があります。

組織は、この脅威に対処するために自動化されたメカニズムを採用する必要があります。そのメカニズムはユーザ動作分析（UBA）と呼ばれ、アイデンティティを監視して、異常な活動を特定するための基準となる動作を確立します。高度なアルゴリズムが特権アイデンティティの動作を継続的に分析し、過去の所見や他のアイデンティティの動作と比較します。アルゴリズムは次にリスクを評価し、悪意ある活動を迅速に検出します。

正規のユーザ動作は変化しますが、その変化は緩やかです。機械学習アルゴリズムは、変化と新しいパターンを学習することでそれに適応します。これは、誤検出を削減するためにも使用されます。このように UBA ツールは自動分析を使用し、アイデンティティを継続的に監視して、攻撃や高リスクの活動、違反を迅速に検出します。

CA Technologies は次の 2 つの UBA ソリューションを提供しています。

- **CA Threat Analytics for PAM** では、リスクを継続的に分析して、特権ユーザの不正な活動をすばやく検出できます。これは CA PAM の付加価値コンポーネントで、ユーザ動作のモデル化と分析を提供します。特権ユーザの通常の動作をモデル化して、動作パターンが変化したときを検出します。このコンポーネントは、新たな方法で内部の脅威に対処します。内部ユーザは、悪事に走る前には通常の使用パターンで活動しますが、悪事を働くときにはそのための方法を探すので、パターンが変化します。ユーザ動作分析エンジンは、このような変化を検出して対処します。同様に、正規のユーザ・アカウントが侵害された場合も、外部のハッカーは正規のユーザとは異なる使用パターンを見せるので、それも検出されます。

- **CA Risk Authentication** は、CA Advanced Authentication の中核的コンポーネントであり、多様な要素（ユーザの動作、デバイスの特性、位置情報、速度データなどを含む）の集合を分析することで、エンド・ユーザによる直接入力を必要とせずに、高リスクのログイン試行や他の警戒すべきアクセスを検出して防御します。そして、リスクが高すぎると判断した場合は、自動的にそのユーザに対して、身元を証明する追加のクレデンシャルまたは情報をさらに入力するように要求することができます。

多要素認証

悪意のある内部関係者はフォースの暗黒面に誘い込まれた元は善良だったユーザですが、不注意な内部関係者は通常は外部のハッカーによって侵害されたアカウントの持ち主です。このようなアカウントはどのように侵害されるのでしょうか。主な要素は、Cybersecurity Insiders によれば、フィッシング詐欺にだまされること（67%）、脆弱な / 再使用されたパスワード（56%）、および共有パスワード（44%）です。このリスクを軽減するために、多くのセキュリティ専門家はユーザ名とパスワードの単純な組み合わせをより強力な本人認証で置き換えるか強化することを推奨しており、いくつかの法規では多要素認証が推奨または要求されています。要素としては、たとえば次のものがあります。

- 本人が知っていること（パスワードや PIN など）
- 本人が持っているもの（スマートカード、デジタル ID、ワンタイム・パスワード（OTP）ジェネレータ、モバイル・デバイスなど）
- 本人の特徴（指紋、声紋、ユーザ動作などの生体識別要素）

ログイン・プロセスを強化し、機密情報へのアクセスを許可する前にユーザのアイデンティティを適切に検証することで、不注意な内部関係者の脅威を軽減できます。

CA Technologies は包括的な本人認証ソリューションを提供しています。

- **CA Advanced Authentication** は、クラウドベースのサービス、特権アカウント、リモート・アクセス、仮想デスクトップ、Web リソースなどを含む企業の数多い機密リソースを保護するために、ユーザにとって便利で費用対効果の高い安全な方法を提供します。ソフトウェアベースの多様な多要素認証クレデンシャルを提供するだけでなく、ユーザの動作、デバイスの特性、および位置情報に基づくリアルタイムのリスクを評価できます。これらの機能が連携して、ユーザ・アイデンティティと企業のデータを保護するためのインテリジェントな階層化されたセキュリティ・アプローチを実現します。

アイデンティティの管理とガバナンス

特権ユーザの管理は継続的で重要なプロセスです。まず、管理者アカウントの所在を突き止め、不適切な特権と孤立アカウントを除去する必要があります。次に、それらのユーザに対して最小特権ポリシーを適用し、共有アカウントを除去する必要があります。これを、特権アクセス管理（PAM）と呼びます。最後に、権限のクリープを防ぎ、各ユーザが自分が持つ過剰な権限を今でも必要としていることを確認するために、特権アクセスを管理する必要があります。これらの不可欠な機能の 1 つでも弱かったり欠けていたりすると、侵害や内部の脅威の全体的リスクが大幅に高まります。

しかし、そもそも特権ユーザとはどのようなユーザでしょうか。単に管理者アカウントへのアクセス権を持っているユーザのことでしょうか。最近の Ponemon の調査によると、回答者の 71% が自分がアクセスするべきでないデータへのアクセス権を持っていると述べており、IT 専門家の 80% が自分の組織では「最小特権」ポリシーが適用されていないと述べています [4]。ここで疑問がわきます。一般ユーザはどの時点で特権ユーザになるのでしょうか。1 つの定義として、「特権ユーザ」は、誤用されたり侵害されると組織にとって許容できない損害または損失を引き起こす可能性があるアクセス権または権限を与えられた人だと言うことができます。これは警戒すべきことです。私たちが考えていたよりはるかに大きな「特権ユーザ」のプールがあるかもしれないからです。

したがって、アイデンティティ管理ソリューションは内部の脅威と標的型の侵害に対する防御の最後の層と見なす必要があります。

CA Technologies は、市場をリードするアイデンティティ管理ソリューションを提供しています。

- **CA Identity Suite** は、最小特権の原則を適用すると同時に要求者と承認者の両方にとって機能性が高く使いやすいエクスペリエンスを提供できるガバナンスを実現するユニークなアプローチを提供します。通常および特権アカウントへのアクセス権の自動プロビジョニング / プロビジョニング解除と、全ユーザの役割およびグループの管理も可能になります。

CA Technologies のメリット

侵害が当たり前のように発生し、情報が氾濫し、パーソナライズされたエクスペリエンスがデジタル・トランスフォーメーションを推進する現在の世界では、アイデンティティが鍵となります。アイデンティティは、ゼロトラストのオンラインの世界における信頼の基礎です。CA Technologies では、企業データのセキュリティとユーザ・アクセスの利便性との間で適切なバランスを維持することがどれほど重要であるかをよく理解しています。したがって、CA はその IAM ソリューションを差別化するために 3 つの戦略的イニシアチブを採用しました。

- **ハイブリッド・クラウド：**アプリケーション環境がハイブリッド・モデルへと移行しているので、CA は現在の EIAM ソリューションもそうするべきだと考えています。EIAM インフラストラクチャはミッションクリティカルです。ラテラル・ムーブメントを防いで重要なインフラストラクチャと機密データを守るためには、仮想、クラウド、および物理環境ですべてのアクセスを保護、監視、監査することが重要です。
- **動作分析：**ユーザとそのアカウントの行動を可視化することは、2 つの理由で重要です。第 1 に、悪意のある内部関係者の異常な活動を検出したり、乗っ取られたアカウントを特定することができます。第 2 に、積極的に正規のユーザを識別して不正なユーザと区別することで、ユーザ・エクスペリエンスを簡略化して手間を削減することができます。CA の戦略は、高度な分析を CA のセキュリティ製品に適用して PAM および IAM プロセスの効果を高めるというものです。
- **導入、維持・管理にかかる総コスト（TCO）：**EIAM ソリューションは、攻撃対象を低減し、驚くべき早さで価値を実現できます。それこそが、組織が侵害の危機に瀕したときに真を問われる問題です。包括的なソリューションは、必要な機能をすべて提供し、財務、ビジネス、および生産性の面で長期的に価値を発揮します。

次のステップ

悪意のある内部関係者と不注意な内部関係者からの攻撃の増大には警戒が必要です。組織はオプションをよく検討して、内部の脅威および標的型の侵害と戦うために、多層防御アプローチを提供するベンダを選ぶ必要があります。CA Technologies の EIAM ソリューションは、常に進化し続ける脅威に対して、それがどこから来るものであろうと、包括的な戦略を提供します。このソリューションの概要で論じた内部の脅威とソリューションの詳細については、https://www.ca.com/jp/products/insider-threat.html をご覧ください。

詳細については、**ca.com/jp/pam** をご覧ください。

CA Technologies にアクセスしてください

CA Technologies（NASDAQ：CA）は、企業の変革を推進するソフトウェアを開発し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスを獲得できるよう支援しています。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。計画から開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。詳細については **ca.com/jp** をご覧ください。

1 Cybersecurity Insiders、Crowd Research Partners、「Insider Threat – 2018 Report」、2017 年 12 月、https://www.ca.com/jp/collateral/ebook/insider-threat-report.html

2 Verizon、「2017 Data Breach Investigations Report」、2017 年 7 月、www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

3 Felix Gaehtgens、Anmal Singh、および Dale Gardner、Gartner、「Market Guide for Privileged Access Management」、2017 年 8 月、www.gartner.com/doc/3789663/market-guide-privileged-access-management

4 Ponemon Institute、「Privileged User Abuse & The Insider Threat」、2014 年 5 月、www.raytheon.com/capabilities/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf

technologies

CS200-343242_2018