IDが無秩序に増加する時代のサイバーセキュリティ対策

統一IDセキュリティを使って、重大な暴露ギャップをなくし、
Zero Trustの取り組みをサポートする方法

ONE IDENTITY by Quest

CISOであるあなたは、サイバーセキュリティに関する懸念を取締役会に報告しましたが、マクロ経済の課題、パイプラインの複雑さ、リモートアクセスを激増させるニーズによって、ほとんどかき消されてしまいました。

土曜日の朝のことです。自宅オフィスで仕事用の携帯電話の呼び出し音が鳴っています。

ITセキュリティディレクターからの電話です。同時にメールもきています。どうしたのでしょうか?

「良いニュースじゃないな」とあなたは考えます。

その通りです。

サイバー攻撃があったのです。程度は不明ですが、ITセキュリティディレクターが、チームが状況を評価中であると報告します。

疑問が頭の中を駆け巡ります。

- どうやって侵入されたのか?
- 内部ユーザが攻撃に加わっていたのか?
- アクセスされた機密情報はどのくらいあるのか?
- 取締役会にはどのように報告すればよいだろうか?
- これは、提案した来年度のサイバーセキュリティ予算に対して有利に働くのか?不利に働くのか?
- 私の履歴書を更新する必要があるだろうか?

サイバー攻撃があったのです。程度は不明ですが、ITセキュリティディレクターが、チームが状況を評価中であると報告します。

IDの無秩序な増加のリスク

組織は、組織自身のIDが無秩序に増加することの犠牲になっています。これは、より迅速かつ効果的な組織運営の支援を目的とした生産性とイノベーションの形を装って、知らない間に徐々に造られていくセキュリティリスクです。

日常業務の実行を強化するリソースを使ってビジネスをサポートするのは、正しいことのように思えました。問題は、ユーザが接続する新しいシステム、アプリ、またはデータベースごとに固有の資格情報処理プロセスと要件があることです。他ほど厳重ではないものもあれば、他より安全性が低いものもあります。他より良いものもありますが、他より悪いものの方が多いのです。多くの場合、誰がアクセス権を持ち、そのアクセス権を使って何をしているのかが可視化されていません。

こうした問題に加えて、特権リモートアクセスを管理者に提供する必要性が常にあります。また、増え続ける外部ユーザがさらに多数のデバイス、オペレーティングシステム、およびブラウザに接続するのを管理する必要もあり、アカウント、ID、およびパスワードの増大を制御しようとしています。

IDが無秩序に増加しています。

これを制御および管理して、生産性とセキュリティのバランスを取るために何をしますか。

以下は、IDの無秩序な増加における、8つのステップの概要です。このe-bookでは、従来のセキュリティ境界の消失、サイバーセキュリティ対策の実現、Zero Trustモデルについて説明します。どのように包括的なアプローチを取るのか、どのように統一IDセキュリティプラットフォームを使って組織を、そして皆様の評価を守ることができるのかについて学びます。

IDの無秩序な増加を促す傾向

前述したように、IT環境が目の前で進化しており、組織がいかに自衛してサイバーセキュリティ対策を確保しなければならないのかに重大な影響を与えています。遅れずについていくのは大変です。セキュリティ専門家は、例えば、次のような変化に迅速に対応する必要があります。

- 従来型のオフィスとインフラストラクチャが急速に姿を消している
- 組織の分散が定着 – 自宅や遠隔地での勤務がますます増加
- 価値を拡張、拡大するために請負業者と外部パートナーに依存
- リモートアクセスや、従来とは異なる作業環境に対応するために新しいプラットフォームやテクノロジーの採用を推進
- クラウド・ファースト・コンピューティングが台頭し、クラウドサービスが別々の物理的な場所に分散
- 効率、アクセス可能性、およびコスト削減のために最適化するという要望が絶えない
- GDPR、HIPAA、CCPAなどのプライバシー規制への対応や、プライバシーやセキュリティの維持に役立つデータ共有プロセスにより、ITが複雑化
- これまで手作業で時間がかかっていたプロセスを合理化するためにロボティック・プロセス・オートメーション（RPA）の使用が徐々に増加

こうした各傾向は、効率とサイバーセキュリティ対策向上の新たな機会を生み出す一方で、それぞれが新たな課題を生み出す可能性もあります。なぜでしょうか? それぞれに共通しているのが、IDの激増です。簡単に言えば、より多くの人（内部と外部）、ロボット、マシン、およびデバイスが会社の資産にアクセスする必要があるということです。その上、組織が多世代にわたるIT環境をサポートすることで、ユーザアカウントも急増しています。これらすべてが、サイバーセキュリティのおそらくこれまでで最大の課題である、IDの無秩序な増加を招いているのです。

無秩序な増加を抑えることがなぜ重要なのか

悪意のある攻撃者がサイバーセキュリティのギャップを悪用することは誰もが知っています。ギャップが存在するところなら場所を問わず、多くの場合は大規模です。これが、IDの無秩序な増加に伴ってリアルタイムで起きており、IDと資格情報を盗む攻撃が最近急増しているのは誰もが知るところとなっています。

例えば、Verizonの2021 Data Breach Investigations Report（DBIR）によれば、すべての侵害の63 %が資格情報に関わるものであり、CensusWideによれば、調査対象組織の半数近くが前年に特権資格情報の盗難に見舞われています。

こうしたID関連のギャップが引き起こす壊滅的な影響が、ニュースサイトのトップページを毎日のように賑わしています。SolarWinds製品のハッキング、サイバー攻撃を受けたColonial Pipeline、Exchange Serverの脆弱性などは、ほんの氷山の一角です。これらの侵害は、一般の人々の安全や暮らし、セキュリティに影響を与えただけでなく、結果的に組織にも悪影響を及ぼすことになりました。

さらに、いくつかの攻撃は簡単に成功を阻止できたはずでした。Cybersecurity Insidersが最近のレポートで指摘したのは、全ユーザのほぼ半数が業務で必要とする以上の権限を持っていることです。企業がIDと権限を優先させているのを目にするだけでなく、政府もその相対的重要性を訴えているのはそのためです。米国行政管理予算局（OMB）が2021年9月の草稿で2024会計年度末を期限とする一連の成果物に焦点を当てましたが、この中に、政府機関による多要素認証の導入、企業全体のID管理プロセスの設定などが含まれていました。

組織がこのサイバーセキュリティの暴露ギャップをなくすには、IDの無秩序な増加を抑える必要があります。そうしないと、罰金や訴訟、顧客の信頼、そして収益の損失に直面することになります。

新しい境界としての重要性が高まるID

ID関連の課題がより一般的になり、影響力が強くなるにつれ、IDセキュリティの重要性が高まってきているのは当然です。

従来の境界もサイバー攻撃の重要な防御手段であることには変わりませんが、いろいろな意味で、これは別の時代のために生まれたものです。インフラストラクチャ中心のこのアプローチは、長年にわたり、サイバーセキュリティ戦略の礎となってきたもので、企業内のあらゆるものを保護することが可能であるという信念に基づいています。当然、この高尚な目標を達成する唯一の方法は、最も外側の場所の防御を最適化することです。ここなら、すべての場所の侵害を防ぐことが可能かもしれないからです。

このアプローチに依存することは、セキュリティ境界が急速にITの言い伝えになりつつある現在、まったく現実的ではなく、時代遅れです。ITセキュリティの上級管理者は、今では、侵害は避けられないと認めています。そのため、より実用的な戦略は、悪意のある攻撃者を排除するだけでなく、ネットワーク内に侵入された後の悪用を防ぐための対策を講じることです。このID中心のアプローチにより、先見の明のある組織は、最も重要なものを優先し、何よりもまず、アクセス権を付与する前にあらゆるものを検証する対策を講じようとしています。例えば、このユーザは誰で、何にアクセスできるべきで、その権限が付与されたら何をするのか、そのユーザの権限はいつ変えるべきか、などです。

つまり、従来の境界は侵食されつつあり、IDが新たなエッジとして浮かび上がってきているのです。

25

一般的な大企業で
アクセス権を管理
するシステムの数。

サイバーセキュリティ対策の主な障害物

IDセキュリティは新たに出現した重要な動きですが、この取り組みで成功することは必ずしも容易ではありません。この主な要因は、ID進化の状況にあります。これまで、組織の主な関心対象は、単一の仕事をするために雇われ、オフィスに縛られ、単一の場所からリソースにアクセスする内部従業員でした。ほとんどのIDはユーザだったのです。

ところが、今日では状況が一変し、まったく異なる力学が働いています。セキュリティ専門家は、内部従業員だけでなく、請負業者、供給業者、およびパートナーのIDも考慮しなければなりません。従業員は1つの仕事をするのではなく、役割は頻繁に変わる傾向があり、オフィスに縛られず、複数の場所から必要なものにアクセスすることもしばしばです。そして、セキュリティ専門家は、ユーザだけでなく、アプリケーションやマシンについても考慮する必要があります。ユーザはさらに多くのアカウントの間で複数のIDを持つことができるようになりました。ユーザがマシンやロボットの場合もあります。人間のユーザは、異なるバージョンや世代のアプリケーションと接続する複数のデバイスを持つことができ、誰もがあちこちに移動しながら、異なる物理アクセスポイントやシステムからリソースにアクセスします。

その上、ほとんどの組織のアクセス権の管理が現在ではサイロ化しています。Third Annual Global Password Security Reportによると、平均的な大企業では25の異なるシステムでIDを管理しています。環境がこのように広範で多様なため、ITセキュリティチームは、ユーザのアクティビティを完全に可視化することができません。また、エンド・ツー・エンドの方法で分析を適用することもできません。こうした課題が最終的にギャップと不整合を引き起こします。ユーザアクセスを付与する前にあらゆるものを検証することは、現代のセキュリティアプローチの実装で欠かすことができない部分ですが、その障害になることがあります。

これらのギャップを埋めることができないと、組織は、ユーザの役割/責任の変更、ITインフラストラクチャの変更、そして新たな脅威や高まる脅威に適応できなくなる可能性があります。このギャップに適切に対処することが、組織のサイバーセキュリティ対策に役立つのです。

ONE IDENTITY by Quest

IDセキュリティの包括的なアプローチの事例

IDセキュリティは柔軟性があり、ユーザの集団とニーズによって、また、どのリソースが接続され、企業を構成しているかによって、実にさまざまな形式を取ることができます。成功の鍵は、IDセキュリティの状態を断片化された状態から統一された状態に移行することです。

多くの組織は、IDセキュリティの主な形式に対処しています。IDガバナンスと管理（IGA）、IDアクセス管理（IAM）、特権アクセス管理（PAM）、Active Directory管理およびセキュリティ（ADMS）などの形式に別々の方法で対処しています。それぞれに、検討すべきサイロが複数あることが多く、人、アプリケーション、およびデータがすべて個別に管理されています。この断片化された状態によって数多くの摩擦が生じ、自動化が妨げられ、アクセス権をいつどのように管理するかについて組織に最善の推測を強いています。

新たに出現したこのモデルははるかに包括的で、IDセキュリティの主な形式が一緒に対処されます。これは、アプリケーションが重複し、データサイロが解放され、人、アプリケーション、およびデータがすべて1つのものとして揃えられることを意味します。この統一IDセキュリティのアプローチにより、すべてのIDを相互に関連付け、より優れた統合で摩擦をなくし、攻撃対象領域を減らし、サイバーセキュリティ対策を強化できます。

ONE IDENTITY by Quest

Zero Trustの主要構成要素としての統一IDセキュリティ

今では、Zero Trustが堅牢で選択的なセキュリティを実装するための、実証済みのモデルであることが広く理解されています。脆弱な権限、不要で過剰なアクセス権を取り除き、特定の権限の委任ときめ細かいプロビジョニングを選択します。IDセキュリティを断片化された状態から統一された状態に移行することで、組織はこの約束の実現に向けて大きく前進できます。

Zero Trustを成功させるには、網を十分に広げて張ることから始めます。これは、つまり、人だけではなくマシンのIDや、多世代、ハイブリッド、およびエッジのIT環境に組織が移行する際に拡大し続けるアカウントにも注目するということです。円を小さく描きすぎると、悪意のある攻撃者のために通用口を開けっ放しにしておくことになります。IDセキュリティ戦略を統一することで、この問題を確実に回避しやすくなります。

Zero Trustの2番目の重要要素は、組織全体に一連の権限を提供することです。追加の可視性と洞察を入手できると、セキュリティ専門家は、より迅速かつ効率的に、権限の追加、削除、および調整をちょうどよいタイミングで行うことができます。そうすることで、ユーザが自分の業務に必要なものだけに適切なタイミングでのみアクセスできるように制御でき、エラーが発生しやすい手動プロセスやIT部門の多大な関与を取り除くことができます。

Zero Trustの最後の重要要素は適応性であり、これは統一IDセキュリティ戦略で実現されます。コンテキストに基づく認識と行動分析を含む包括的なアプローチを活用することで、組織は新たに出現する脅威に対処する是正措置を、より迅速かつ効率的に予測、検知して、実行できます。

IDセキュリティのアプローチを統一するための ベストプラクティス

テクノロジーによって、組織がIDセキュリティの統一に成功する可能性を劇的に高めることができますが、セキュリティ専門家は、結果を最適化するためにソリューションプロバイダーに何を求めるべきでしょうか。以下に、代替手段を検討する際に必要な5つの要素を示します。

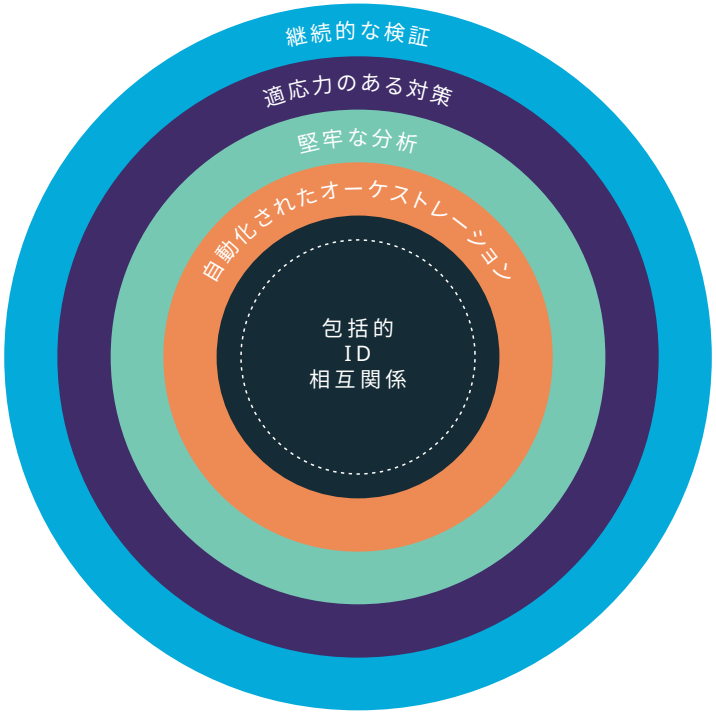
1. **包括的な相互関係:** 可視性を最適化して最適な情報を元にした意思決定を行うために、何よりもまず、組織はすべてのIDとアカウントをエンド・ツー・エンドで統一する必要があります。

2. **自動化されたオーケストレーション:** 統一IDセキュリティ戦略の2番目の主要要素は、IDと権限に対する摩擦のないガバナンスです。これにより、効率を大規模に促進できます。

3. **堅牢な分析:** IDセキュリティの幅広く、進化する性質を考慮すると、組織には、大規模に新たに出現する脅威を予測および検知して、是正措置を講じるために必要な洞察のレベルを提供するソリューションが必要です。

4. **適応力のあるサイバーセキュリティ対策:** 脅威の状況や企業がもはや固定ではないことを認識して、サイバーセキュリティ専門家は必要に応じて素早く方向転換し、投資を将来にわたって保証できる必要があります。

5. **継続的な検証:** 統一IDセキュリティが最も成功するのは、アクセスが付与される前にあらゆるものを検証できる場合です。状況認識、セッション監視、および行動分析によって強化されたテクノロジーは、セキュリティの実現に役立ちます。



ONE IDENTITY by Quest

統一IDセキュリティで解決される主な問題

ここまで、IDセキュリティに統一アプローチを追求する際の大まかな課題と利点について概説しました。
しかし、サイバーセキュリティのリーダーは、このような戦略で具体的にどのような使用例を期待できるのでしょうか。以下に、よくある結果の例を示します。

主な問題	使用例	結果
組織をセキュリティで保護する: **人、アプリケーション、およびデータを保護する**	• Zero Trust: 適応力のあるZero Trustフレームワークを構築することで、大規模に保護し、侵害リスクを減らす • 特権リモートアクセス: リモートワーカーや請負業者が、面倒なVPNを使用せずに、重要情報に安全にアクセスできるようにする • エンドポイント特権管理: AD/Azure AD、Unix/Linux、WindowsおよびmacOSデスクトップのエンドポイントセキュリティを統一する • 特権分析およびセッションの終了: 特権ユーザのリスクを検知し、組織への損害を防ぐ • ハイブリッドのAD管理とセキュリティ: IT部門のプロビジョニングタスクへの関与を減らし、手作業によるエラーを取り除く • AD/Azure ADの特権セキュリティ: 内部環境を境界と同じくらい厳重にセキュリティで保護して、重要で頻繁に狙われる資産を保護する • パスワードボールト: パスワード管理をシンプル化し、特権資格情報を保護する	• 脆弱性とリスクを取り除く • Zero Trustを実装する • 侵害を防ぐ • クラウドサービスとオンプレミス環境全体でIDを統一する • 特権アクセスをセキュリティ保護する
運用効率を向上させる: **セキュリティプロセスを一元化する**	• 特権アクセスのガバナンス: 特権アクセスと標準のユーザIDとの間のポリシーとセキュリティのギャップをなくす • Active Directoryの管理とセキュリティ: ユーザおよびグループのセキュリティ確保と管理を行い、権限委任により管理者アクセスを制御する • Active Directoryブリッジの作成: 運用システムおよびプラットフォーム全体で、ポリシーベース管理を統一する • 合併と買収: 従業員の行動やパンデミックなど、通常は手作業による大幅な介入が必要な変化にスムーズに適応する	• ID管理ポリシーとプロセスを統一する • 効率を大幅に向上させる • すべてのリソース、システム、およびプラットフォームへのアクセスを制御する • 一般的なタスクを自動化して、ITスタッフの作業の焦点を最適化する • 入社/異動/退社プロセスを容易に行える

主な問題	使用例	結果
コンプライアンスと監査の要件に対処する: **IDの無秩序な増加を管理し、ポリシー準拠を証明する**	• IDガバナンス: ポリシーが実施され、ユーザアクセスが要件に従って管理されるようにし、証拠を示せるようにする • エージェントレスセッション監査: 自動化された記録と分析により、最も重要なリソースとユーザを保護する。さらに、フォレンジック調査をサポートし、特権アクセスのコンプライアンス要件を満たす • コンプライアンスレポートの即時作成: 監査人とコンプライアンスの要件を満たすために、企業全体のすべてのユーザとリソースのコンプライアンス対策について、リアルタイムのレポート作成機能を利用できる	• 権限関連の情報に対する監査人の要求を満たす • ID中心のポリシーの違反リスクを最小化および除去する • すべての特権セッションアクティビティに対する、信頼性の高い監査証跡を作成する • セキュリティチームが特定のイベントを検索し、特権セッションを再生できるようにする • 特権アクセスを監視するためのコンプライアンスニーズを満たす
デジタルトランスフォーメーションをセキュリティ保護する: **IDを保護しながら、機能とアクセスを改善する**	• DevOpsセキュリティオーケストレーション: ID中心のセキュリティでDevOpsパイプラインをセキュリティ保護する • アプリケーションガバナンス: アプリケーションアクセスの決定を合理化し、基幹業務マネージャが情報を元にして意思決定できるようにする • RPAのセキュリティの最適化: RPA IDの無秩序な増加に関連するリスクを管理する • 複雑な環境の管理: 異種混在環境の管理オーバーヘッドを削減し、セキュリティ、スピード、および意思決定を促進する	• ハイブリッド環境をシームレスに管理する • RPAを安全に導入して実行する • DevOpsを使いやすくする • 従業員と請負業者のアカウンタビリティを向上させる • エラーの削減、セキュリティの向上、効率の最適化、および複雑さの最小化

まとめ

強い力が働き、ビジネスとITの状況が急速に進化したことで、IDが急増しています。このIDの無秩序な増加は、日々悪化しています。サイバーセキュリティ専門家が真剣に受け止めなければならない、極めて現実的な一連のリスクを生み出しています。サイバーセキュリティを断片的に管理することを止めるときがやって来たのです。

アクセス権の管理に包括的なアプローチを採用することで、CISOはサイバーセキュリティの重大な暴露ギャップをなくし、組織のサイバーセキュリティ対策を向上させ、急速に企業の義務になりつつあるZero Trustの約束を実現するための重要な一歩を踏み出すことができます。

IDは新しいエッジです。統一IDセキュリティ戦略は、現代の攻撃手法に対抗し、組織を未来に導く方法です。

これで、ITセキュリティディレクターから電話がかかってきたときに、IDセキュリティの状態とネットワーク上でどのようなアクションが行われているかを、即座に評価するための情報を持っていると確信できるようになるでしょう。

One Identityについて

One Identityは、お客様がサイバーセキュリティ全体の体制を強化し、ビジネスに欠かせない人員、アプリケーション、およびデータを保護することを支援する、統一IDセキュリティソリューションを提供します。当社の統一IDセキュリティプラットフォームは、クラス最高のIDガバナンスと管理（IGA）、IDおよびアクセス管理（IAM）、特権アクセス管理（PAM）、およびActive Directoryの管理とセキュリティ（ADMS）の機能を統合し、組織がIDセキュリティに対して、断片的なアプローチから包括的なアプローチに移行できるようにします。One Identityは世界中の5,000超の組織で2億5千万を超えるIDを管理し、全世界の実績と信頼を得ています。詳細については、www.oneidentity.com/jp-ja/をご覧ください。

本書の使用に関して不明な点がありましたら、以下までお問い合わせください。

www.quest.com/JP-JA/company/contact-us.aspx

eBook-UnifiedIdentitySecurity-KA-JA-WL-69156

ONE IDENTITY by Quest