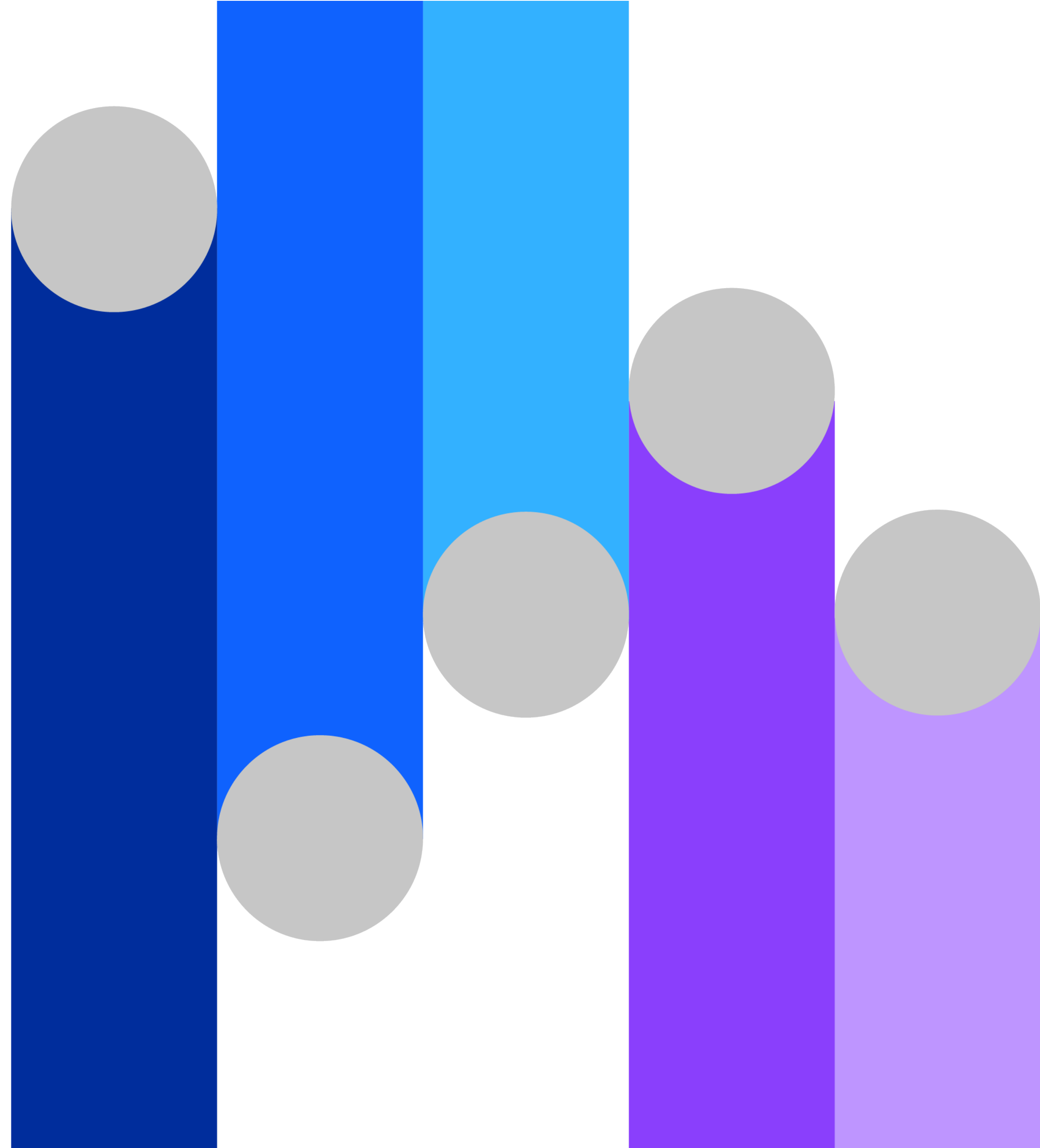


# 避けるべき5つの 一般的なデータ・ セキュリティの 落とし穴

データ・セキュリティとコンプライア  
ンス体制を改善する方法を学ぶ



# 目次

[00 →](#)

概要

[01 →](#)

落とし穴1:  
コンプライアンスを超えて  
動くことができない

[02 →](#)

落とし穴2: 一元化の必要性  
を認識していないデータ・セ  
キュリティー

[03 →](#)

落とし穴 3:  
データの責任者を定義していな  
い

[04 →](#)

落とし穴 4: 既知の脆弱性に対  
処できない

[05 →](#)

落とし穴 5: 最新のデータ・アク  
ティビティー監視の優先順位付  
けと使用の失敗

[06 →](#)

未来のために、

[07 →](#)

なぜIBM Securityか?

## 概要

データ・セキュリティーは企業にとって最優先事項であるべきであり、それには正当な理由があります

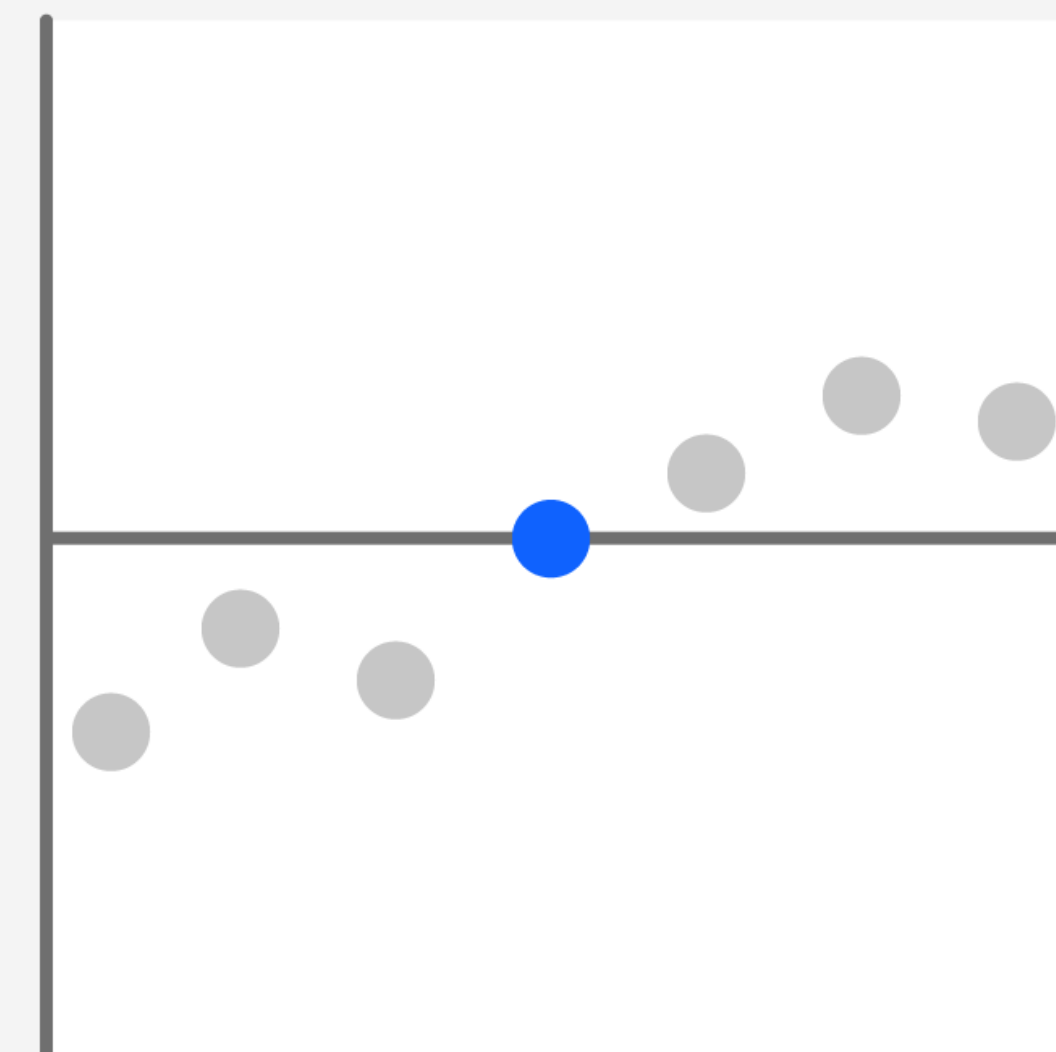
ITランドスケープがますます分散化され複雑になっている場合でも、多くのデータ侵害は防止可能であることを理解することが重要です。個々のサイバーセキュリティーの課題や目標は企業によって異なるかもしれませんが、多くの場合、組織はデータ・セキュリティーに取り組み始めるときに同じ広範な間違いを犯します。さらに、多くのエンタープライズリーダーは、これらのエラーを通常のビジネス慣行として受け入れることがよくあります。

サイバー攻撃の成功につながる可能性のあるいくつかの内部および外部要因があります。

- ネットワーク境界の侵食
- より複雑なIT環境によって提供される攻撃対象領域の増加
- クラウド・サービスがサイバーセキュリティーの実践に課す需要の高まり
- ますます巧妙化するサイバー犯罪の性質
- 根強いサイバーセキュリティースキル不足
- データ・セキュリティーリスクに対する社員の意識不足

# 445万米ドル

データ侵害の世界平均コストは2023年に上昇し、3年間で15%増加しました。<sup>1</sup>



落とし穴1:コンプライアンス  
を超えて動くことができない

落とし穴1:コンプライアンスを超えて動くことができない

コンプライアンスは必ずしもデータ・セキュリティと同じではありません。限られたデータ・セキュリティ 参考情報を監査や認証への準拠に集中させる組織は、自己満足になる可能性があります。多くの大規模なデータ侵害は、紙の上で完全に準拠している組織で発生しています。次の例は、コンプライアンスのみに焦点を当てると、効果的なセキュリティが低下する可能性があることを示しています。

#### 不完全なカバレッジ

企業は、年次監査の前に、データベースの構成ミスや古いアクセスポリシーに取り組むためにスクランブルをかけることがよくあります。脆弱性とリスクのアセスメントは継続的な活動であるべきです。

#### 最小限の労力

多くの企業は、法的要件やビジネス・パートナー要件を満たすためだけにデータ・セキュリティ・ソリューションを採用しています。「最低限の基準を導入して業務に戻ろう」という考え方は、優れたサイバーセキュリティの実践に反する可能性があります。効果的なデータ・セキュリティはマラソンであり、短距離走ではありません。

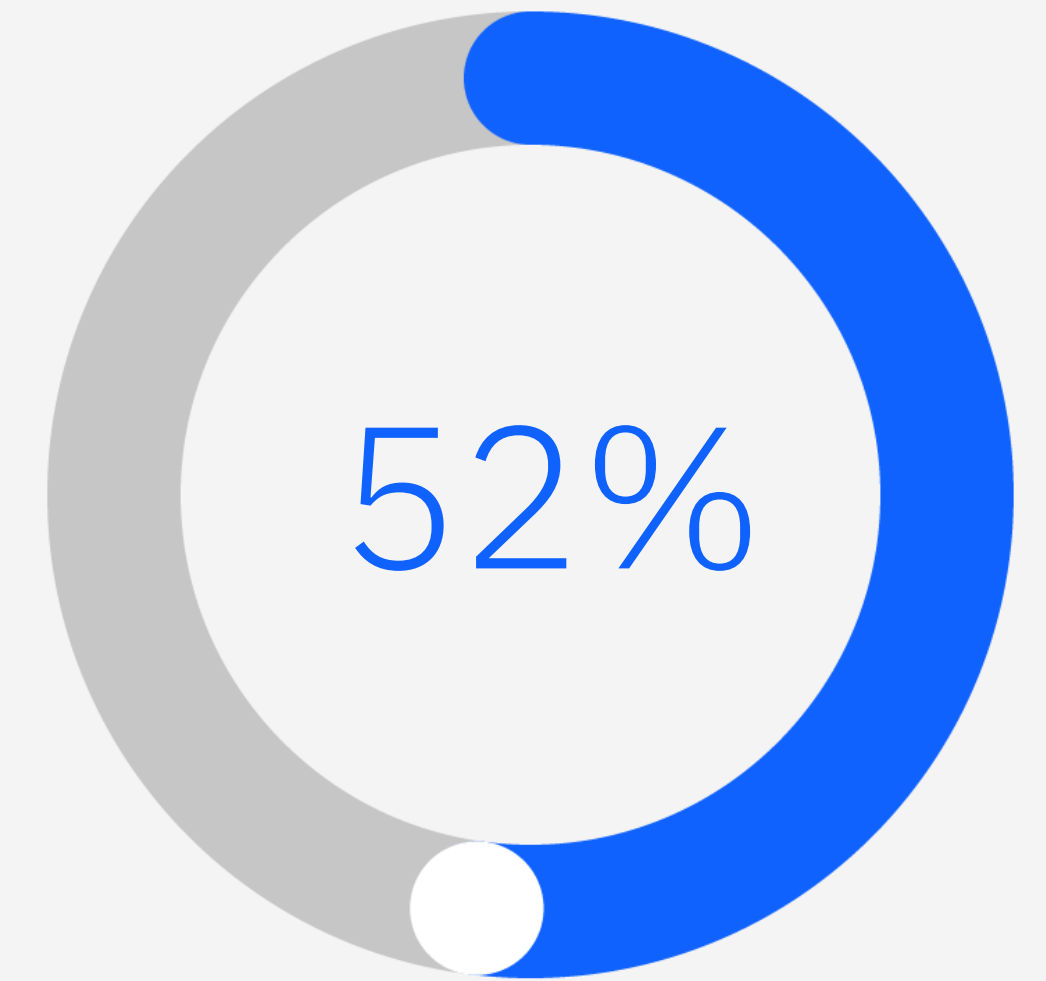
#### 緊急性の低下

企業は、サーベンス・オクスリー法 (SOX)、一般データ保護規則 (GDPR)、ペイメントカード業種・業務データ・セキュリティ標準 (PCI DSS)、カリフォルニア州プライバシー権法 (CPRA) (以前はCCPAとして知られていまし

た) などの規制が成熟すると、統制の管理に満足する可能性があります。時間が経つにつれて、リーダーは規制対象データのプライバシー、セキュリティ、保護についてあまり配慮しなくなる可能性があります。コンプライアンス違反に関連するリスクとコストは残ります。

#### 規制されていないデータの省略

知的財産などの資産は、紛失したり、権限のない担当者と共有したりすると、組織を危険にさらす可能性があります。コンプライアンスのみに焦点を当てることは、貴重なデータを見落とし、保護しているデータ・セキュリティ組織で成果を上げることができません。



組織の52%は、ワークロードをパブリッククラウドに移行することによってもたらされる複雑さにより、コンプライアンス義務の遵守もより困難になっていると述べています。<sup>2</sup>

コンプライアンスを、ビジネスをサポートするためのセキュリティ標準を革新および向上させる機会と見なします。

## ■ 解決策: コンプライアンスが出発点であることを認識し、受け入れる

データ・セキュリティ 組織は、単にコンプライアンス要件に対応するのではなく、ビジネスのクリティカルデータを一貫して保護する戦略的プログラムを確立する必要があります。

データ・セキュリティおよびコンプライアンス・プログラムには、次のコアプラクティスを含める必要があります。

- オンプレミス、クラウドデータ、保管する、店舗、サービスとしてのソフトウェア (SaaS) アプリケーション全体で機密データを検出して分類します。
- コンテキストインサイトとアナリティクス、分析でリスクを評価します。

- 暗号化と柔軟なアクセスポリシーで機密データを保護します。
- データ・アクセスと使用パターンを監視して、疑わしいアクティビティをすばやく発見します。
- 脅威にリアルタイムで対応します。
- コンプライアンスとそのレポート作成を簡素化します。

最後の要素には、規制コンプライアンスに関連する法的責任、企業が被る可能性のある損失、およびコンプライアンス違反の罰金を超えたそれらの損失の潜在的なコストが含まれます。

最終的には、保護しようとしているデータのリスクと価値について総合的に考察する必要があります。

落とし穴2: 一元化の必要性  
を認識していないデータ・セ  
キュリティー

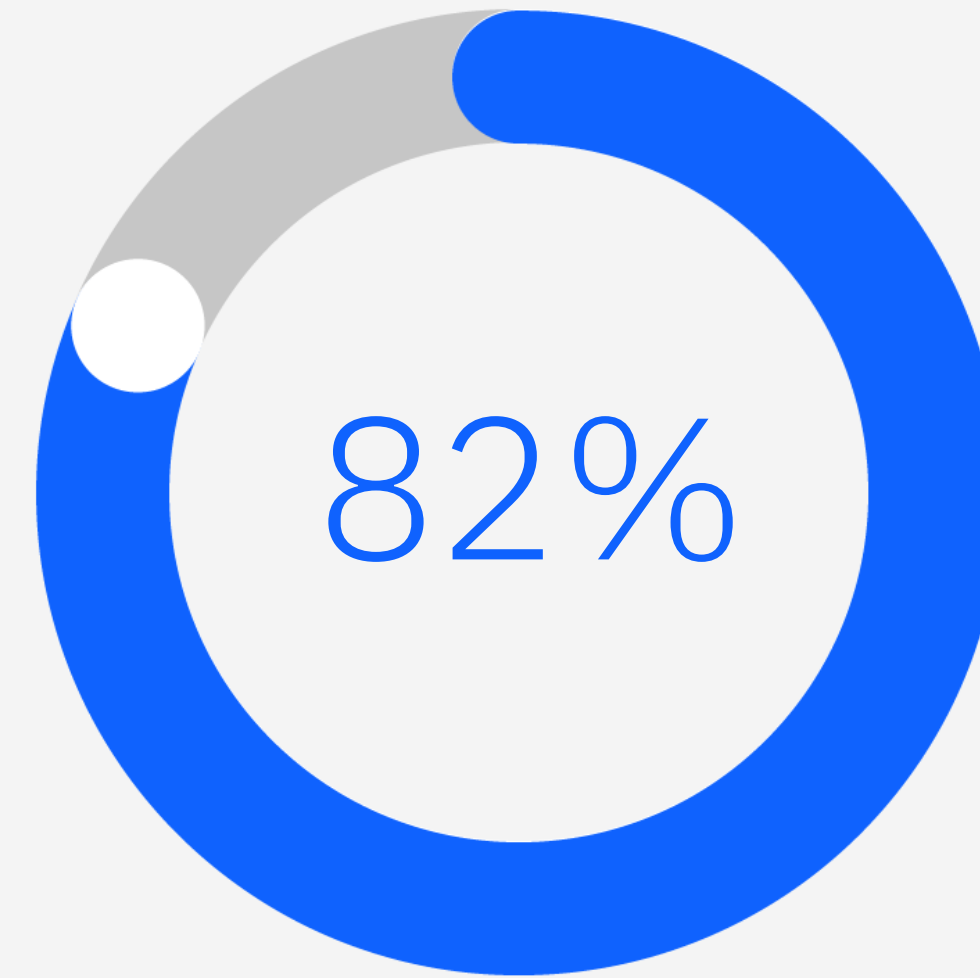
データ・プライバシーとセキュリティを対象とする広範なコンプライアンス要件がなければ、組織のリーダーは、一貫性のある企業全体のデータ・セキュリティーの必要性を見失う可能性があります。

ハイブリッド・マルチクラウド環境が絶えず変化し、成長している企業の場合、新しいタイプのデータソースが毎週または毎日表示され、機密データが大幅に分散する可能性があります。

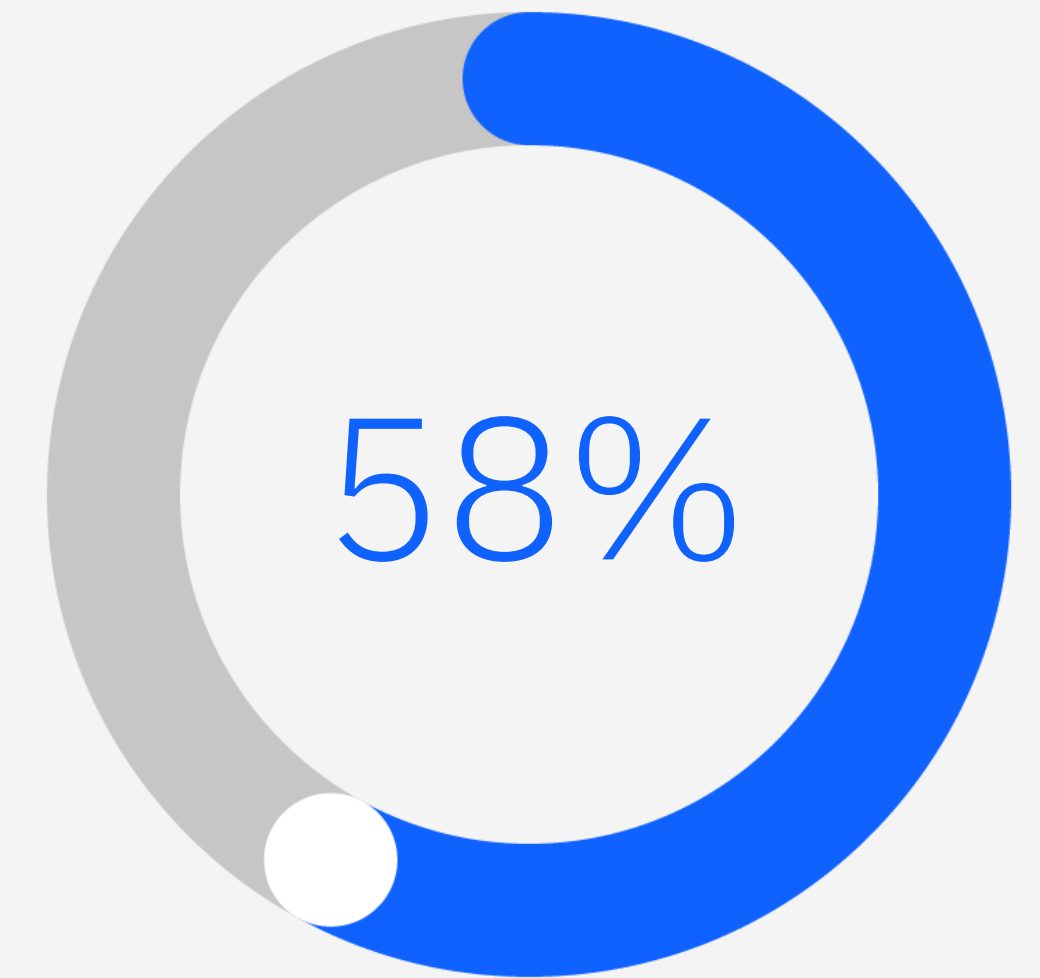
ITインフラストラクチャを成長および拡張している企業のリーダーは、攻撃対象領域の変化がもたらすリスクを認識できない可能性があります。彼らは、ますます複雑で異種のもので構成されるIT環境の周りに機密データが移動するにつれて、適切な可視性と制御を欠く

可能性があります。特に複雑な環境内で、エンドツーエンドのデータ・プライバシー、セキュリティ、保護の制御を採用できないと、非常にコストのかかる監視になる可能性があります。

サイバーセキュリティー・ソリューションをサイロで運用すると、追加の問題が発生する可能性があります。たとえば、セキュリティー・オペレーション・センター (SOC) とセキュリティー情報イベント管理 (SIEM) ソリューションを使用している組織は、データ・セキュリティー・ソリューションから収集したインサイトをこれらのシステムに提供することを怠ることができます。同様に、セキュリティーチーム、プロセス、ツール間の相互運用性の欠如は、サイバーセキュリティープログラムの成功を妨げる可能性があります。



侵害の82%は、クラウドに保管されていたデータに関係していました。<sup>1</sup>



組織の58%は、クラウドに常駐する機密データの約21%から50%が十分に保護されていないと述べています。<sup>2</sup>

機密データのセキュリティ保護は、より広範なサイバーセキュリティの取り組みと併せて行う必要があります。

## ■ ソリューション: オンプレミス、クラウドでホストされるリポジトリ、SaaS アプリなど、機密データの保管場所を把握する

機密データのセキュリティ保護は、より広範なサイバーセキュリティの取り組みと併せて行う必要があります。機密データがどこに保管されているかを理解することに加えて、この情報が急速に変化する場合でも、いつ、どのようにアクセスされているかを知る必要があります。さらに、データ・セキュリティと保護についてのインサイトとポリシーを全体的なサイバーセキュリティ・プログラムと統合して、テクノロジー間の緊密な通信を可能にする必要があります。異種のもの(で構成される)環境とプラットフォームで動作するデータ・セキュリティソリューションは、このプロセスに役立ちます。

より包括的なサイバーセキュリティプラクティスの一環として、データ・セキュリティを他のサイバーセキュリティコントロールと統合する適切な時期はいつですか?ここでは、組織がこの次のステップに進む準備ができている可能性があることを示唆するいくつかの兆候を示します。

### 貴重なデータを失うリスク

組織の個人データ、機密データ、および専有データの価値は非常に大きいため、その損失はビジネスの実行可能性に重大な損害を与えます。

**規制への影響**

お客様の組織は、クレジットカード番号、その他の支払い情報、個人データなど、法的要件を持つデータを収集し保管します。

**サイバーセキュリティーの監視の欠如**

組織は、クラウドインスタンスを含むすべてのネットワークエンドポイントを追跡して保護することが困難になるまで成長しました。たとえば、データがどこで、いつ、どのように保管されているか、店舗、オンプレミス全体で共有およびアクセスされている、クラウドデータ保管する、店舗とSaaSアプリについて明確なアイデアがありますか？

**不適切なアセスメント**

あなたの組織は、すべてのサイバーセキュリティー活動で何が費やされているかを明確に理解していない断片化されたアプローチを採用しています。たとえば、データ・セキュリティーのリスクを軽減するために、参考情報に関して投資収益率(ROI)を正確に測定するプロセスはありますか？

これらの状況のいずれかが組織に当てはまる場合は、データ・セキュリティーをより広範な既存のセキュリティプラクティスに統合するために必要なサイバーセキュリティーのスキルとソリューションの習得を検討する必要があります。



# 落とし穴 3: データの責任 者を定義していない

### 落とし穴 3: データの責任者を定義していない

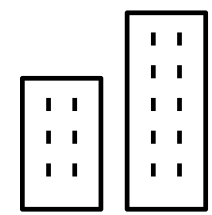
データ・セキュリティの必要性を認識していても、多くの企業には機密データの保護に特に責任を持つ人がいません。この状況は、組織が責任者を見つけるように圧力をかけられているデータ・セキュリティまたは監査インシデント中に明らかになることがよくあります。

経営幹部は、最高情報責任者 (CIO) に「私たちの仕事は主要なシステムを稼働させ続けることです。私のITスタッフの誰かに相談してください。」これらのIT従業員は、機密データが存在するが、サイバーセキュリティの予算が不足している複数のデータベースを担当している可能性があります。

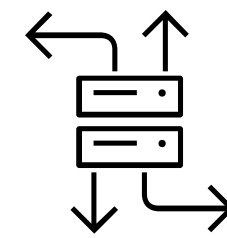
通常、最高情報セキュリティ責任者 (CISO) 組織のメンバーは、ビジネス全体を通過するデータに対して直接責任を負うことはありません。企業内のさまざまな基幹業務 (LOB) マネージャーにアドバイスを提供する場合がありますが、多くの企業では、データ自体に対して明示的に責任を負う人は誰もいません。組織にとって、データは最も価値のある資産の1つです。しかし、所有権の責任がなければ、機密データを適切に保護することは困難になります。



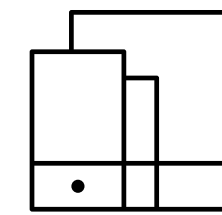
複雑な IT 環境では、次の場所にあるデータを考慮することが重要です。



事業単位間で共有



ハイブリッド・マルチクラウドのインフラストラクチャに配置



モバイル・デバイスに保管

## ■ 解決策: 機密データや重要データ資産の安全とセキュリティに専念する CDO または DPO を雇う

最高データ責任者 (CDO) またはデータ保護責任者 (DPO) がこれらの職務を処理できます。実際、ヨーロッパに拠点を置く企業や欧州連合のデータ主体と取引を行う企業は、DPO を必要とする GDPR の義務に直面しています。この前提条件では、機密データ (この場合は個人情報) には、そのデータを使用する LOB を超える価値があることが認識されています。さらに、この要件では、企業がデータ資産を担当するように特別に設計された職務を持っていることを強調しています。

CDO または DPO を選定する際には、次の目的と責任を考慮してください。

### 技術知識とビジネスセンス

リスクを評価し、適切なデータ・セキュリティ投資に関して、技術者以外のビジネスリーダーが理解できる実践的なビジネスケースを作成します。

### 戦略的实施

検知、応答、およびデータ・セキュリティ制御を適用して保護を提供する技術レベルで計画を指示します。

### コンプライアンスのリーダーシップ

コンプライアンス要件を理解し、それらの要件をデータ・セキュリティコントロールにマッピングして、ビジネスがコンプライアンスを遵守できるようにする方法を理解します。

### モニタリングとアセスメント

脅威の状況を監視し、データ・セキュリティプログラムの有効性を測定します。

### 柔軟性とスケーリング

より高度なツールを統合して、新しい環境間でデータ・アクセスおよび使用ポリシーを拡張するなど、データ・セキュリティー ストラテジーを調整するタイミングと方法を理解します。

### 分業

サービス・レベル・アグリーメント (SLA) と、データ・セキュリティーのリスクと修復に関連する責任に関して、クラウド・サービス・プロバイダーでの期待事項を設定します。

### データ侵害対応計画

最後に、戦略的な侵害の軽減と対応計画を策定する上で重要な役割を果たす準備をしてくださいます。

最終的には、企業データを効果的に保護するために全員が協力する必要があるため、CDO または DPO がチーム間および企業全体のデータ・セキュリティー コラボレーションの促進を主導する必要があります。このコラボレーションは、CDO または DPO が、組織が機密データを保護するために必要なプログラムと保護を監視するのに役立ちます。



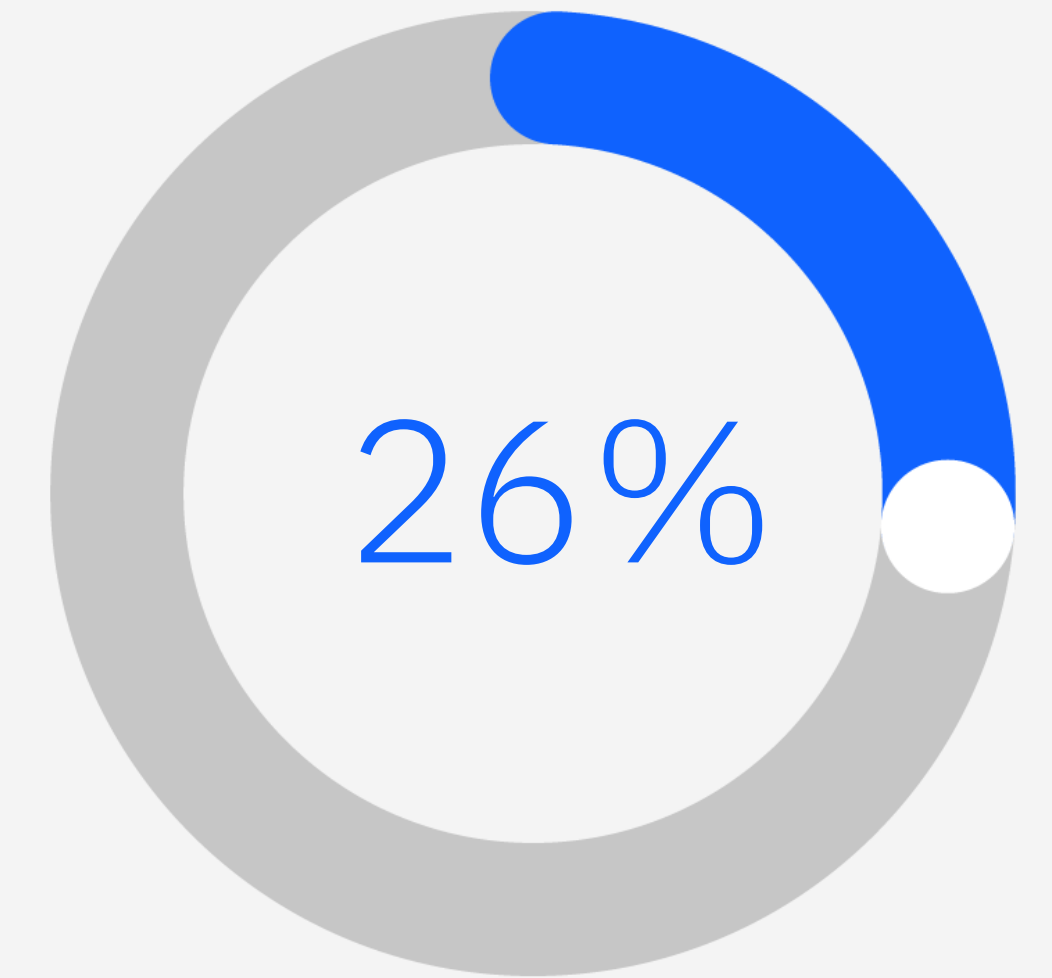
# 落とし穴 4: 既知の脆弱性 に対処できない

企業で注目を集める侵害は、パッチのリリース後もパッチが適用されていない既知の脆弱性に起因することがよくあります。既知の脆弱性に迅速にパッチを適用しないと、サイバー犯罪者がこれらの簡単なエントリポイントを積極的に探しているため、組織のデータが危険にさらされます。

ただし、多くの企業は、IT、セキュリティ、および運用グループ間の調整レベルが必要なため、パッチを迅速に実装するのが難しいと感じています。さらに、パッチは、プロセスを壊した

り、新しい脆弱性を導入したりしないかどうかを確認するためのテストを必要とすることがよくあります。

クラウド環境では、契約したサービスまたはアプリケーション・コンポーネントにパッチを適用する必要があるかどうかを判断するのが難しい場合があります。サービスに脆弱性が見つかった場合でも、そのユーザーは多くの場合、サービスプロバイダーの修復プロセスを制御できません。



新しい脆弱性の 26% は既知の悪用でした。<sup>3</sup>

データ保管庫の脆弱性アセスメントを行うことで積極的な姿勢を取り、リスクの軽減に役立てます。

## ■ 解決策: 成長をサポートする適切なテクノロジーを使用して、効果的な脆弱性管理プログラムを確立します

脆弱性管理には、通常、次のレベルのアクティビティの一部が含まれます。

- データ資産の正確なインベントリとベースライン状態を維持します。
- クラウド資産を含むインフラストラクチャ全体にわたって脆弱性スキャンとアセスメントを頻繁に実施します。
- 脆弱性が悪用される可能性と、そのイベントがビジネスに与える影響を考慮した脆弱性修復に優先順位を付けます。
- 脆弱性管理と応答性を、サードパーティのサービスプロバイダーとのSLAの一部として含めます。

- 可能な限り、機密データや個人データを難読化します。暗号化、トークン化、編集は、この目的を達成するための3つのオプションです。
- 適切な暗号化キー管理を採用し、暗号化キーが安全に保管されかつ適切に循環して、暗号化されたデータを安全に保つようにします。

成熟した脆弱性管理プログラム内であっても、システムを完全に保護することはできません。最も保護された環境でも侵入が発生する可能性があるかと仮定すると、データには別のレベルの保護が必要です。適切なデータ暗号化技術と機能のセットは、新たな脅威からデータを保護するのに役立ちます。

# 落とし穴 5: 最新のデータ・アクティビティ監視の優先順位付けと使用の失敗

データ・アクセスと使用を監視することは、データ・セキュリティ戦略の重要な部分です。組織のリーダーは、誰が、どのように、いつデータにアクセスしているかを知る必要があります。この監視には、これらのユーザーがアクセス権を持つ必要があるかどうか、そのアクセス・レベルが正しいかどうか、および企業にとって高いリスクを表しているかどうかを含める必要があります。

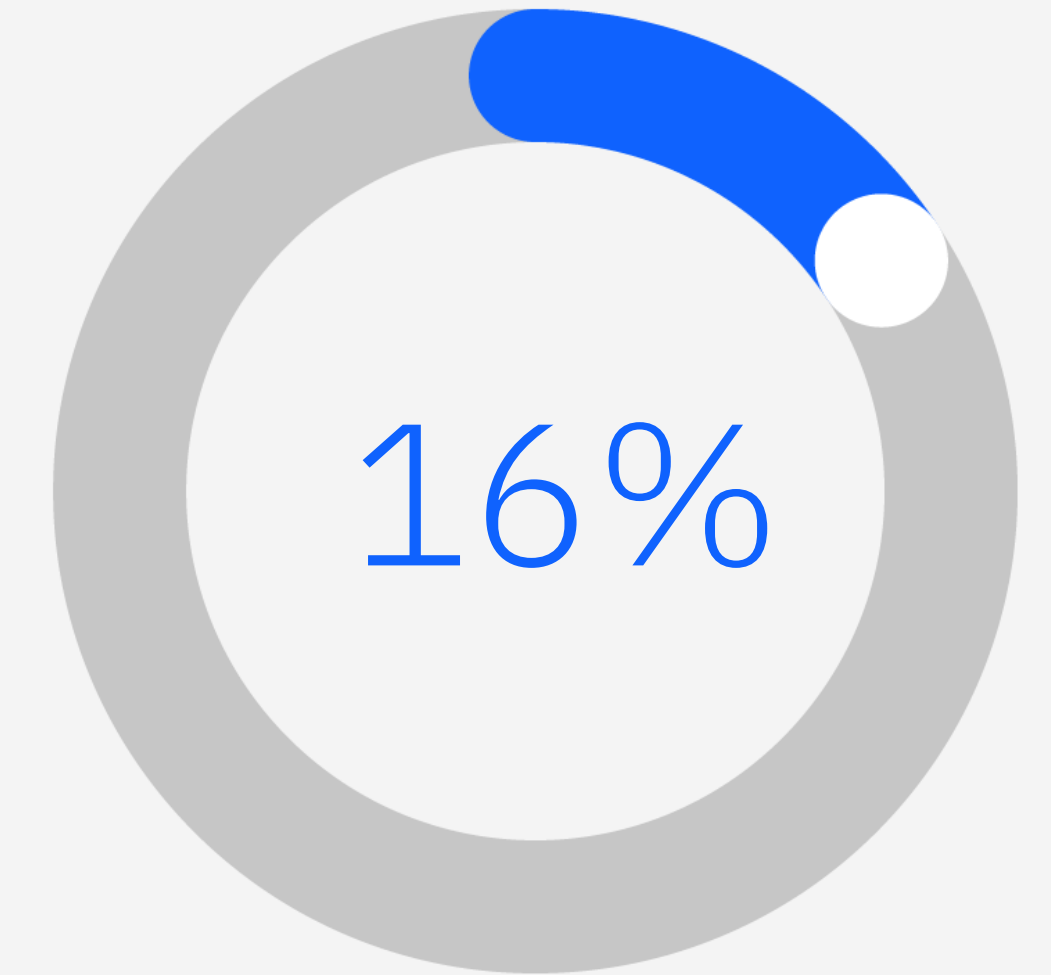
特権ユーザーは、内部脅威の一般的な犯罪者です。データ保護計画には、疑わしいアクティビティや不正なアクティビティに使用されている特権ユーザーアカウントを検知するためのリアルタイム監視を含める必要があります。

悪意のあるアクティビティの可能性を防ぐには、ソリューションで次のタスクを実行する必要があります。

- ポリシー違反に基づいて疑わしいアクティビティをブロックおよび検疫します。
- 異常な動作に基づいてセッションを中断またはシャットダウンします。
- データ環境全体で事前定義された規制固有のワークフローを使用します。
- 実用的なアラートをITセキュリティおよび運用システムに送信します。

データ・セキュリティやコンプライアンス関連の情報を把握し、潜在的な脅威にいつどのように対応すればよいかを把握することは困

難な場合があります。許可されたユーザーがデータベース、ファイルシステム、メインフレーム環境、クラウド環境、SaaSアプリなど、複数のデータソースにアクセスすると、これらすべてのやり取りからデータを保管するのは圧倒的に思えるかもしれません。課題は、膨大な量のデータアクティビティを効果的に監視、キャプチャ、フィルタリング、処理、および対応することにあります。適切な計画が整っていないと、組織は合理的に処理できるよりも多くのアクティビティ情報を保持し、データアクティビティ監視の価値を低下させる可能性があります。



観察されたインシデントの16%は、攻撃者がアクセスを取得する手段として既存のアカウントの資格情報を取得および悪用した有効なアカウントの悪用でした。<sup>3</sup>

データアクティビティ監視ソリューションを使用すると、データ・セキュリティアナリストは貴重な時間を節約できます。

## ■ ソリューション: 包括的なデータ・ セキュリティとコンプライアンス を開発するストラテジー

そのためには、データ・セキュリティへの取り組みを開始する際には、要件とリスクに適切に対処するために、監視作業のサイズと範囲を決定する必要があります。このアクティビティでは、多くの場合、企業全体で最良実施例の作成と調整を可能にする段階的なアプローチを採用する必要があります。さらに、プロセスの早い段階で主要なビジネスおよびIT利害関係者と会話して、短期的および長期的なビジネス目標を理解することが重要です。

これらの会話では、主要なイニシアチブをサポートするために必要なテクノロジーもキャプチャする必要があります。たとえば、オンプレミス、クラウドでホストされるデータ・リポジトリ、SaaS アプリを組み合わせ使用して、新しい地域にオフィスを設置することを計画している場合、データ・セキュリティ・ストラテジーでは、その計画が組織のデータ・セキュリティとコンプライアンス体制にどのように影響

するかを評価する必要があります。この場合、会社所有データは、GDPR、CPRA、ブラジルのレイジエラルデプロテソンデダドス(LGPD)などの新しいデータ・セキュリティおよびコンプライアンス要件の対象となります。

また、最も機密性の高いデータがある可能性が高い 1 つまたは 2 つのソースに優先順位を付けて焦点を当てる必要があります。これらのプラクティスをインフラストラクチャの残りの部分に拡張する前に、データ・セキュリティポリシーがこれらのソースに対して明確かつ詳細であることを確認してください。

特権ユーザーによる主要なリスクと異常な動作に焦点を当てることができる、豊富なアナリティクス、分析を備えた自動化されたデータまたはファイルアクティビティ監視ソリューションを探す必要があります。

データまたはファイルアクティビティ監視ソリューションが異常な動作を検知したときに自動アラートを受信することは不可欠ですが、データ・アクセスポリシーからの異常や逸脱が検出されたときに迅速なアクションを実行することも必要です。保護アクションには、動的データのマスクまたはブロックを含める必要があります。

データ・アクティビティの監視と保護の計画を作成するときは、多くの場合、次の質問を検討すると便利です。

- 最も機密性の高い上位 2 つのデータ・ソースは何ですか？
- 機密データの量に基づいて、次に優先順位を付ける必要がある 5～10 個のデータソースはどれですか？

- 特定のエンドポイントまたはクラウド資産は、リスクの高いデータに関連付けられていますか？
- 機密データは、オンプレミス、ハイブリッド、クラウド環境との間で自由に移動していますか？
- どのユーザーにどのような条件でデータ・ソースへのアクセス権を付与するか。
- どのリスクの高いユーザーまたは特権アカウントをオフにする必要があるか、またはより詳細な調査が必要ですか？
- データ・セキュリティー・ソリューションは、リアルタイムのアクティビティ監視と自動データ保護機能をサポートしていますか？
- SQL (NoSQL) プラットフォームだけでなく、Structured Query Language (構造化照会言語) (SQL) Database、Hadoop デイストリビューションなどのデータ保管庫に存在するファイル内のデータを追跡するリ

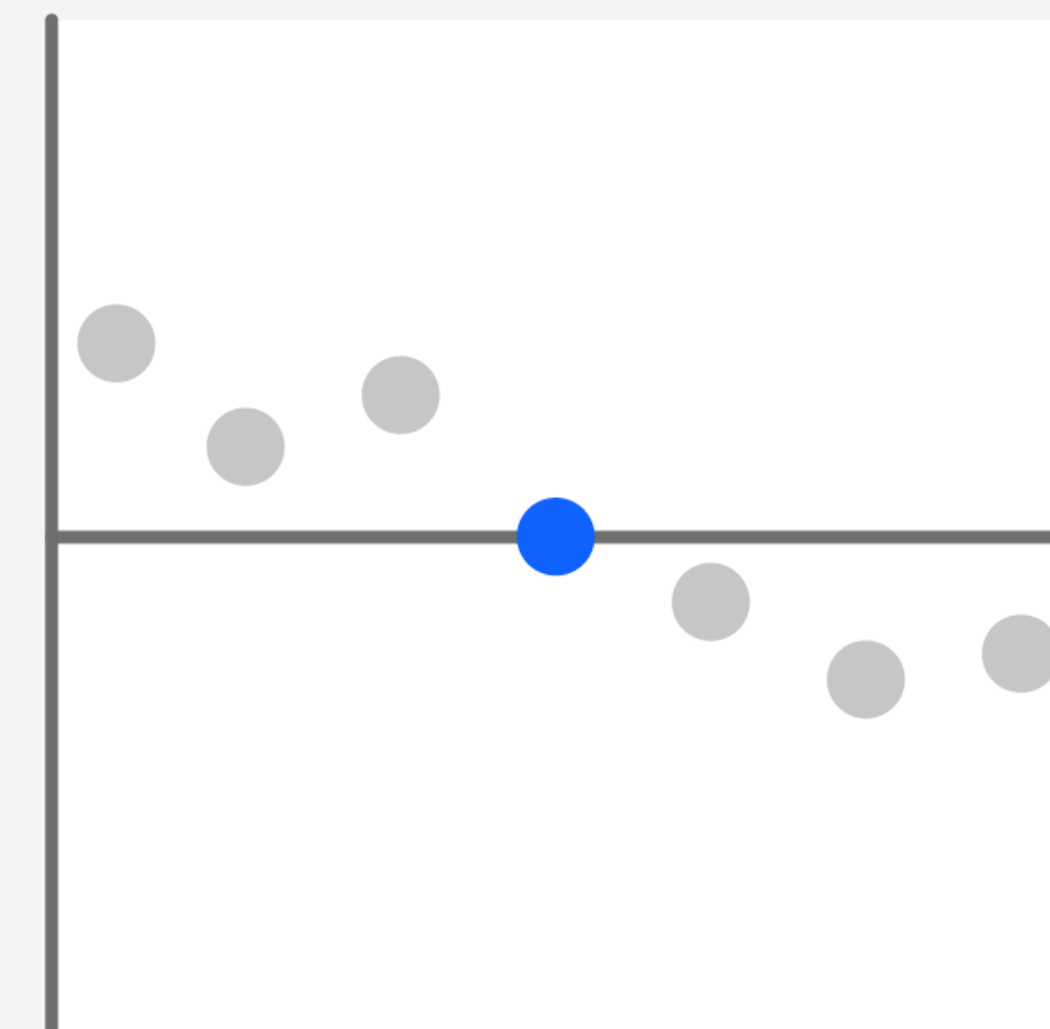
アルタイム監視は実施されていますか？

- 監視ソリューションは、ハイブリッド・マルチクラウド環境にまたがるデータ保管庫を考慮し、適切な人に適切なタイミングで送信されるカスタマイズされたレポートを生成できますか？
- リスク、脆弱性、修復作業に効果的に優先順位を付けるために必要なリスク分析、分析、およびフィルタリングされた監視機能はありますか？

監視の優先順位と保護要件についてより具体的にしなければなるほど、ソリューションは利用可能な検知・応答リソースを適用するのにより効果的になります。

# 176万米ドル

セキュリティ AI とオートメーション、自動化を広範囲に使用している組織の平均節約額は、使用していない組織と比較して 176 万米ドルです。<sup>1</sup>



## 次は何ですか？

これらの一般的なデータ・セキュリティの落とし穴、特にハイブリッド・マルチクラウド環境を追求する企業が増えている中で、どうすれば回避できるでしょうか。まず、問題を認識し、データがどこにあるかに関係なく、データを保護するためのプロアクティブで包括的なアプローチを取るよう組織を準備します。

ビジネスに複雑でハイブリッドなIT環境がある場合、データ・セキュリティへのサイロ化されたアプローチを行う余裕はありません。データ・セキュリティとコンプライアンス・ストラテジーを追加して、データインフラストラクチャ全体にまたがり、すべてのデータタイプをサポートする必要があります。

組織の貴重なデータを保護するために実行できる即時の次のステップは次のとおりです。

- 組織の短期的および長期的なビジネスおよびテクノロジー目標をサポートするデータ・セキュリティおよびコンプライアンス計画の構築
- 適切な人材、プロセス、ツールでその計画を実装する
- 参考情報を計画して、組織が最新のテクノロジーを採用するにつれて、データ・セキュリティおよびコンプライアンスプログラムを効果的に拡張できるようにします

IBM® Security Guardium® プラットフォームは、クリティカル・データおよび機密データがどこにあっても、組織がよりスマートで適応性のあるアプローチをとれるように設計されたデータ・セキュリティおよびコンプライアンス・ソリューションです。それがあなたの組織に適している理由をご覧ください。

[詳細はこちら](#) →

[お問い合わせください](#) →



406%

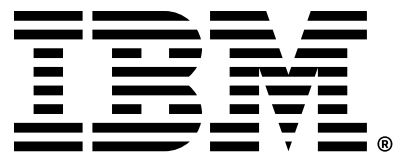
Guardium ソリューションに関する調査では、406% の ROI を達成し、3 年間で 586 万米ドルのメリットがあることがわかりました。<sup>4</sup>

## なぜ IBM Security か？

IBM Security®は、動的なセキュリティーAI機能やオートメーション機能を組み込んだセキュリティー製品とサービスを統合したポートフォリオにより、世界の大手組織や官公庁・自治体のセキュリティー強化を支援しています。世界的に有名な IBM® X-Force® の調査に裏付けられたこのポートフォリオを使うことにより、組織は脅威を予測し、データ移動時にこれを保護し、ビジネスイノベーションを妨げることなく迅速かつ正確に対応することが可能になっています。IBMは、セキュリティー・トランスフォーメーションの評価、戦略立案、実装、管理を実行するパートナーとして、何千もの組織から信頼されています。

IBMは、世界で最も広範なセキュリティー研究、開発、および配信組織の1つを運営しています。130以上の国または地域で毎日1500億以上のセキュリティーイベントを監視しています。世界中で10,000を超えるセキュリティー特許を取得しています。





1. データ侵害コストレポート 2023, IBM, July 2023.
2. 今日のクラウド時代におけるデータコンプライアンスの必要性、エンタープライズ・ストラテジー・グループ、TechTarget、2023年4月。
3. X-Force Threat Intelligence Index 2023、IBM Security、2023年2月。
4. IBM Security Guardium Data ProtectionのTotal Economic Impact™ (TEI) 、IBMが委託したフォレスター・コンサルティングの調査、2023年6月。

© Copyright IBM Corporation 2023.

日本アイ・ビー・エム株式会社  
〒103-8510 東京都中央区  
日本橋箱崎町19番21号

Produced in the United States of America  
2023年9月

IBM、IBM ロゴ、Guardium、IBM® Security、および X-Force は、International Business Machines Corporation の米国および/またはその他の国または地域における商標または登録商標です。その他の製品名およびサービス名は、IBM またはその他の企業の商標である場合があります。IBM の商標の最新リストは、[ibm.com/jp-ja/legal/copyright-trademark](https://www.ibm.com/jp-ja/legal/copyright-trademark) で入手できます。

本書は最初の発行日時点における最新情報を記載しており、IBMにより予告なしに変更される場合があります。IBMが事業を展開しているすべての国で、すべての製品が利用できるわけではありません。

本書の情報は「現状のまま」で提供されるものとし、明示または暗示を問わず、商品性、特定目的への適合性、および非侵害の保証または条件を含むいかなる保証もしないものとし、IBM製品は、IBM所定の契約書の条項に基づき保証されます。

適切なセキュリティ慣行に関する声明: どのようなITシステムや製品も完全に安全とみなすべきではなく、不適切な使用やアクセスを、完全に実効性のある形で防止できる単一の製品、サービス、セキュリティ対策もありません。いずれかの当事者による不正行為または違法行為の影響がシステム、製品またはサービスに及ばないという保証、またはこうした影響がお客様企業に及ばないようにするという保証をIBMが提供することはありません。

お客様は適用法・規則の遵守を徹底する責任を負うものとし、IBMは法律上の助言を提供せず、IBMのサービスまたは製品を使用することでお客様による法律または規則の遵守が確約されると表明することも保証することはありません。