Technology Blueprint

McAfee
An Intel Company

データベースの保護

今日の攻撃と損失媒体に対して、セキュリティを強化する

SECURITY CONNECTED REFERENCE ARCHITECTURE

LEVEL 1 2 **3** 4 5

Security Connected

マカフィーのSecurity Connectedフレームワークは、複数の製品、サービス、パートナーの統合を可能にすることで、効率的かつ効果的に一元的なリスク軽減を実現します。20年以上の実績を持つセキュリティプラクティスを基盤に構築されたSecurity Connectedアプローチを通じて、規模やセグメントを問わず、すべての地域の組織がセキュリティ体制を改善し、セキュリティを最適化することでコスト効率を高め、戦略的にセキュリティとビジネスイニシアチブを整合させることが可能になります。Security Connectedリファレンスアーキテクチャーは、構想から実装までの具体的な手法を提供します。このアーキテクチャーを利用することにより、Security Connectedの概念をお客様独自のリスク、インフラストラクチャー、ビジネス目標に適合させることができます。マカフィーは、常にお客様を保護する新しい方法を見出すことに専心しています。

今日の攻撃と損失媒体に対して、セキュリティを強化する

現状

2010 年には、データ侵害の数がこれまでにない高い値を記録し、攻撃の 47% では、わずか数分、数時間でエントリーポイントからセキュリティ侵害にまで進んでいました。また、Verizon/U.S. Secret Service の『2011 Data Breach Investigations Report』（2011 年データ侵害調査報告）によると、攻撃の 44% が数日で侵害に成功しています。このように、攻撃はすばやく行われています。また、検出には時間がかかっています。セキュリティ侵害から検出までの時間は、数週間（38%）や数ヶ月（36%）となっています[1]。犯罪者が目的のものを入手して跡形もなく消えるのに、十分な時間です。

攻撃は数分や数日のタイムラインで行われ、検出は数週から数ヶ月のタイムラインで行われています。攻撃をこれほど素早く行えるのは、なぜでしょうか。新しい戦術を使用しているためです。ハッキング（50%）とマルウェア（49%）が、使用されている主な戦術でした。また、このレポートでは、攻撃者は数百万のレコードがある「大規模」なサーバーではなく、システムが十分に保護されていない小規模な組織を「格好の標的」として狙っていると結論付けています。

多くの場合、攻撃者は従業員から意図的ではない支援を得ています。ソーシャルエンジニアリングと資格情報を盗み出すことで、攻撃者は正当なアクセス権を使って容易に「内部関係者」のように見せることができます。データベース資産は重要であり、経済が低迷しているため、賄賂も有効です。上述のレポートによると、勧誘と賄賂は、人的側面で昨年用いられた最も一般的な戦術でした。そのため、データベースの保護ではネットワークの境界線上での保護は信頼できません。また、すべての従業員が正しいことをするとは限りません。

課題

データベースは、重要な情報を保存しているだけでなく、不可欠なビジネスサービスを提供する複数のシステムに接続されていることが多いです。データベースシステムへの妨害、意図しない情報開示、そしてデータ損失により、企業の業務全体が中断されて評判が低下してしまう可能性があります。また、データベースには規制の対象となる機密データが保存されるため、データベースの侵害は通常、コンプライアンスの侵害となり、莫大なクリーンアップコストが発生し、消費者の信頼が失われるとともに、時価総額が大幅に下がる可能性があります。

外部の脅威と内部の脅威の両方から機密データを保護するためには、データベースのアクティビティをリアルタイムで把握する必要があります。大部分の組織では、今日、データベースに付属しているロギングと監査ツールを利用してこの保護を行っていますが、これらのツールでは、最新のハッキングとソーシャルエンジニアリングの戦術に対処するにはまったく不十分です。データベースを悪質なコードとデータ損失から適切に保護するためには、次の問題に対処する必要があります。

- **アクティビティと変更の監視**：すべてのデータベースが、コマンドに対して応答します。コマンドは、データを要求するユーザーに適切である限り成功します。攻撃とツールがさらに高度になっているため、攻撃者は、一般的な検出手法をすり抜けて特権を昇格させることが可能です。アクセス制御が不十分だと、攻撃者の作業が容易になります。通常、特権ユーザーに付与されるアクセスのレベルは、一般ユーザーがシステムや自身の役割に必要なアクセス権を上回っています。古いアカウントをそのままにしていたり、新しいアカウントの作成時に制御が不十分であると、攻撃者が侵入できる経路が増えてしまいます。攻撃者は、まず、デフォルトのパスワードと弱いパスワードを攻撃し、次に、特権を昇格させます。ローカルアクセスの手法を使ってネットワークベースの監視システムをバイパスできるため、ネットワークベースのアクティビティ監視ではこの問題には不十分であることが判明しています。

- **監査ツール**：データベースのネイティブのロギング機能と監査機能は、状況を適切に把握するにはかなり不十分です。ほとんどの機能では、行われた変更、使用された特権、関与した管理者、またはシステムレベルの変更を把握できません。また、データベース内に組み込まれているロギング機能と監査機能を使用すると、データベースのパフォーマンスが低下する可能性があります。管理者が、セキュリティではなく監視のために設計されたこれらの機能をオフにして、ネイティブのツールで提供されている機能を無効にする可能性もあります。
- **パッチ適用で生じるダウンタイムの回避**：システムの可用性は、セキュリティよりも優先されます。パッチ適用サイクルが 12 ケ月をはるかに越える組織もあります。毎年、数百もの新たな脅威が発生していますが、データベースは重要であるため、ダウンタイムは許されません。組織では、データベースにパッチを適用せずに常に保護されることを望んでいます。
- **クラウド対応**：組織がクラウドの採用を開始するに従って、ローカルネットワーク経由だけでなく、クラウドサービスを使ってアクセスと監視を行えるようデータベースを適合させる必要があります。
- **業界標準、政府標準、内部標準への準拠の実証**：データベースの役割に応じて、PCI DSS、SOX、HIPAA、SAS 70、GLBA、FERPA などのさまざまな規制に関して準拠を確保し、レポートを行い、ポリシーを維持することが必要になる可能性があります。また、他国と取引を行っている場合は、通常、その国にも同様なプライバシー統制要件や財務統制要件が存在します。さらに、組織では独自のベストプラクティスや運用標準を作成している場合があり、幹部はガバナンス標準との比較で状態を示すダッシュボードを期待しています。

ソリューション選定の要素

アーキテクチャーには、次のような要素が影響します。

- 組織では、どの規制要件に対応する必要があるのか
- データベースの規制遵守をどのように測定およびレポートしているのか
- 64ビットOSで実行されているデータベースがあるかどうか。どのデータベースか
- データベースのセキュリティレベルを把握しているかどうか
- どの程度の頻度でデータベースにパッチを適用しているか

解決策

すべての組織が業務にデータベースを利用しています。OS の保護を OS ベンダーに委ねていない場合と同様に、データベース資産を保護するために、ベンダー提供のツールで妥協する必要はありません。データベースには固有の課題があるため、セキュリティポリシーとセキュリティ標準の実装は、通常、データベース管理者の手に委ねられています。数多くのデータベース侵害が報道されているため、悪質なコードと本来は信頼できるはずの内部関係者からデータベースの整合性を確実に保護することが可能な新しいアプローチを検討する必要があります。

これらの懸念に対処するため、ソリューションは次の要件を満たしている必要があります。

- **アクティビティと変更の監視**：データベース外部からデータベースのすべての動作とアクティビティを監視できる必要があります。この監視がデータベース内でのみ実行されている場合、データベース管理者が機能を無効にする（意図してまたは意図せずに）可能性があります。また、ポリシーに違反するセッションを終了して、一元管理のコンソールにアラートを生成し、悪意のあるユーザーや非準拠のユーザーを検疫できる必要があります。更に、Evasion 攻撃を検出して防止できる必要があります。
- **監査ツール**：同様に、監査ツールも管理者が無効にできる場合は効果がありません。確実にレコードを取得して分析に利用するためには、データベース外部に保護された監査機能とロギング機能を提供できる必要があります。インシデント後のフォレンジック分析の際に、この監査証跡を使用すると、損失したデータ量を確認し、悪意のあるアクティビティを詳しく把握できます。SOX、PCI、その他のコンプライアンス監査要件に対応する監査証跡とレポートを提供できる必要があります。
- **パッチ適用で生じるダウンタイムの回避**：既知の脆弱性と一般的な脅威経路を悪用するよう試みる攻撃を検出できる必要があります。アラートを発行するか、リアルタイムでセッションを終了させるように、ソリューションを構成する必要があります。データベースベンダーがパッチを提供するのを待ったり、生産性の低下を避けるためにパッチの適用を省略すると、数多くの脅威経路に対してデータベースが脆弱な状態のままになります。仮想パッチの概念は、ゼロデイの脆弱性や新たに検出された脆弱性から保護するのに役立ちます。この概念は、データベースのダウンタイムを発生させずに実装でき、パッチが適用できるようになるまでの期間、機密データを保護できます。

- **クラウド対応**：データセンターの仮想化環境やクラウドコンピューティング環境では、ダイナミックな分散環境を採用しているために、ネットワーク環境も動的であり、ネットワークトラフィックの分析を頼りにポリシーの違反を特定するソリューションには向きません。新しいデータベースが自動的にプロビジョニングをされる度に、ホストしているデータに基づいてセキュリティポリシーを要求し、管理サーバーにアラートの送信を開始するよう、ソリューションを構成する必要があります。また、ネットワーク接続が中断されている場合でも、ローカルで施行されているポリシーによってデータが引き続き保護される必要があります。
- **業界標準、政府標準、内部標準への準拠**：標準や規制が変更されると、保持する必要があるレポートも変更になります。そのため、最新の制御と違反ガイダンスに更新できるよう、コンプライアンスと規制に対応する最新のテンプレートを提供する必要があります。そして、発生時に脅威を特定し、リスクと法的責任を軽減するよう、防止についてレポートできる必要があります。あらかじめ作成されたテンプレートには PCI-DSS、SOX、HIPAA、および SAS-70 が含まれており、一元管理のプラットフォームからすべてのテンプレートを参照できる必要があります。

マカフィーのソリューションで使用されているテクノロジー

マカフィーは、特にデータベースセキュリティを実現するために設計された 2 つの製品、McAfee® Vulnerability Manager for Databases と McAfee Database Activity Monitoring を提供しています。McAfee ePolicy Orchestrator®（McAfee ePO™）による一元管理でこの 2 つの製品を連携させて、インフラストラクチャー全体で統合型のセキュリティとコンプライアンス管理プラットフォームを実現しています。

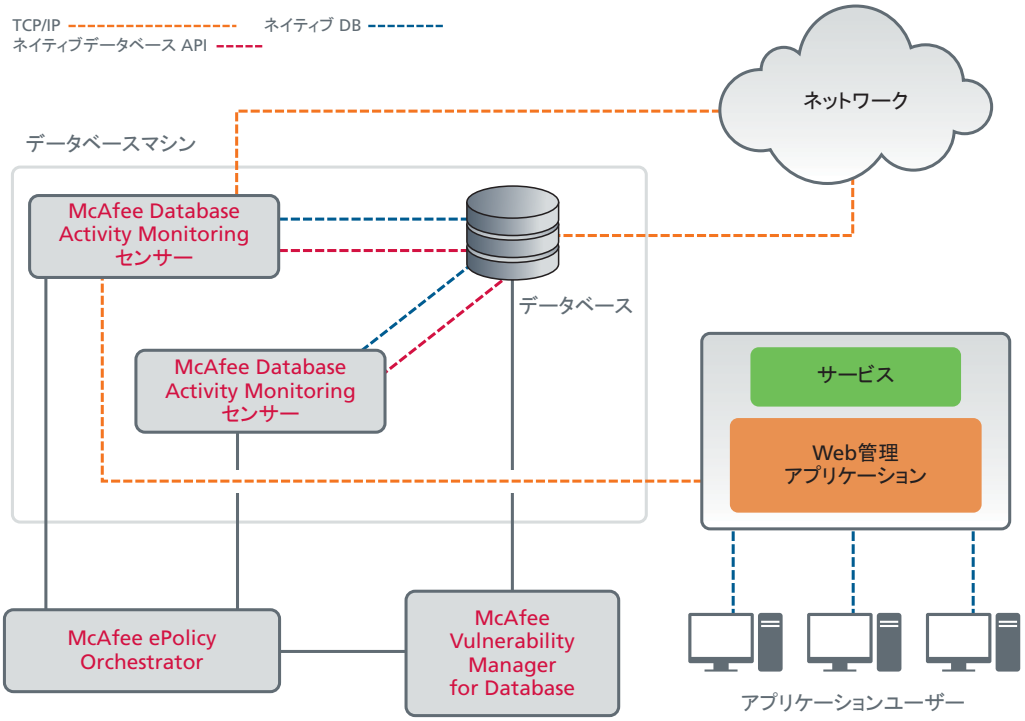
McAfee Vulnerability Manager for Databases は、SQL Server、DB2、MySQL などの主要なデータベースシステムで 3,000 以上の脆弱性チェックを実行します。データベースの脆弱性の把握を強化し、その修正について専門家のアドバイスを提供することで、損害を招く侵害が生じる可能性を低減し、監査と規制準拠の準備を適切に行えるようにすることで、監査に関する運用コストを削減します。Vulnerability Manager for Databases では、弱いパスワード、共有パスワード、デフォルトのアカウントなどのハッカーや攻撃が探している一般的な弱点を特定できるため、攻撃対象領域を低減できます。疑わしいイベントを追跡して対処できるよう、Vulnerability Manager for Databases は、バージョン/パッチのレベル、変更されたオブジェクト、変更された特権、および一般的なハッカーツールの痕跡についてレポートを提供します。

イベントが実行された後で何があったのかを通知する基本的な監査やログ分析とは異なり、McAfee Database Activity Monitoring は、損害が引き起こされる前に侵害を阻止することが可能な、リアルタイムの可視性と侵入防止機能を提供します。380 以上の事前に定義されたルールが、データベースベンダーによってパッチが適用された特定の問題と一般的な攻撃プロファイルに対処します。あらかじめ作成されたポリシーテンプレートを、適切かつ準拠したデータベースアクセスとプロセスのルールをサポートするようにカスタマイズできます。

修復を行えるよう、アラートがポリシー違反に関する詳細情報とともに監視のダッシュボードに直接送信されます。高リスクの違反については、疑わしいセッションを自動的に終了させて悪意のあるユーザーを検疫するよう構成できるため、セキュリティチームは侵入を調査する時間を確保できます。

データベース内に保存されている重要なデータをターゲットとする攻撃は、ネットワーク経由や、サーバー自体にログインしたローカルのユーザーを介して発生する可能性があり、ストアドプロシージャーやトリガーを使ってデータベース内で発生する可能性もあります。

McAfee Database Activity Monitoring は、メモリーベースのセンサーを使用して、ユーザーに負担をかけない単一のソリューションによってアクティビティを監視し、3 種類のすべての脅威を検出します。仮想パッチ処理の更新は、新たに検出された脆弱性に対応するよう、定期的に行われます。データベースのダウンタイムを発生させずに実装できるため、データベースベンダーによってパッチがリリースされて適用できるようになるまでの期間、機密データを保護できます。アクティビティ情報とイベント情報を使用して、監査のためにコンプライアンスを実証したり、セキュリティ全体を強化できます。



専用の保護により、マカフィー製品では、データベースの脆弱性を評価して、悪意のある処理やリスクのある処理を監視することが可能

McAfee Vulnerability Manager for Databases

初回のスキャンを迅速化するよう設計され、ほとんどのコンプライアンス要件に対応する、すぐに使えるレポート機能を備えた McAfee Vulnerability Manager では、単一コンソールから複数のデータベースで検出とスキャンを実行できます。McAfee Vulnerability Manager は、機密情報が含まれたテーブルを検出および特定し、ポートスキャンをすばやく実行することで、データベースのバージョンやパッチ適用状況に関する情報を収集します。基本的なパスワード強度の検出（簡易パスワード、デフォルトパスワード、共有パスワード）に加えて、SHA-1、MD5、DES などの保存されているハッシュされたパスワードもスキャンできます。SQL インジェクション、バッファオーバーフロー、悪質な PL/SQL コードや安全でない PL/SQL コードなど、データベース固有のリスクに対する脆弱性もテストできます。一般的なコンプライアンス標準に対応した、あらかじめ用意されたレポート・テンプレートにより結果が表示されます。

McAfee Database Activity Monitoring

McAfee Database Activity Monitoring は低フットプリントなセンサーであり、データベースホストサーバー自体にインストールし、すべてのアクティビティを監視するソフトウェアエージェントです。この C++ 言語で記述されたセンサーは、スタンドアロンなプロセスとしてデータベースホストマシンで実行されます。標準のプラットフォームツール（RPM、PKG、DEPOT、BFF、または EXE）を使用して、システム上の別の OS ユーザーアカウントによりインストールされます。マシン上のすべてのデータベースインスタンスを自動的に識別し、異なるデータベースタイプを含め、同じホスト上にある複数のインスタンスを監視できます。

実行時に、センサーは、読み取り専用のメカニズムとアプリケーションプログラミングインターフェイス（API）を使用して SQL キャッシュのインスタンスメモリー領域に接続し、メモリーサンプリングのポーリングループで監視を開始します。すべてのサンプルサイクルで、センサーは、現在実行されているステートメントと以前のステートメントでデータベースインスタンス内の各セッションを分析し、サーバーから受け取った事前定義のポリシーを使用して、アラートを発行したりブロックする必要があるステートメントを特定します。ポリシーに違反しているステートメントは、アラートとしてリアルタイムで管理コンソールに送信されます。センサーは、特定の違反が発生したらセッションを終了させたり、ユーザーを検疫するように構成することもできます。ユーザーに負担をかけずに、わずかな CPU リソース（マルチ CPU マシンの場合でも、単一の CPU コアの 5% 未満）しか使用しません。センサーの防止機能は、データの整合性を低下させずにデータベースセッションを終了させることが可能な、ネイティブデータベース API を使用して実装されます。

McAfee ePolicy Orchestrator（McAfee ePO）

McAfee ePO は、一元化された自動ソフトウェア配布とポリシー管理を実現します。McAfee Vulnerability Manager for Databases を McAfee ePO ダッシュボードと統合すると、すべてのデータベースについてレポーティングと概要情報を一元化できます。また、McAfee ePO を McAfee Database Activity Monitoring に接続すると、1 つの画面で表示してレポーティングを簡素化できます。

導入効果

データベースの攻撃とデータ損失媒体に対処する専用の保護を導入すると、外部の攻撃に対して検出と回避を強化するとともに、ネットワーク内でセキュリティ侵害や業務の中断が発生する可能性を低減できます。

マカフィーは、疑わしいイベントを監視してアラートを発行することで、攻撃のすべてのソースをリアルタイムで把握し、保護できるようにします。脅威がネットワーク経由、サーバー自体にログインしたローカルのユーザーを介して、またはデータベース内のいずれで発生するかに関係なく、マカフィーは、損害が引き起こされる前に攻撃を阻止することで、リスクと法的責任を最小限に抑えます。新たに検出されたデータベース脆弱性について仮想パッチ処理を行うことで、即座の保護を提供し、データベースのダウンタイムはまったく発生しません。

あらかじめ作成されたテンプレートとルール、アップデートされる自動チェック、およびウィザードベースのインターフェイスにより、導入を迅速化し、データベースセキュリティアーキテクチャーを効率的かつ容易に監査できるようになります。

追加情報

www.mcafee.com/dbsecurity（英語）
www.mcafee.com/vmfordatabases（英語）
www.mcafee.com/dbactivitymonitoring（英語）
www.mcafee.com/japan/products/epolicy_orchestrator.asp

＊本書は2012年10月時点での情報です。仕様等の変更が生じる場合や、一部、日本未発売の製品も含まれています。詳細はお問い合わせください。

著者について

Uy Huynh は、マカフィーのセールスエンジニアリング部門のシニアディレクターです。お客様がセキュリティ体制を強化し、最も重要なデジタル資産を保護するのを支援するため、Uy は、セールスエンジニアリングチームが適切なセキュリティソリューション、設計、およびベストプラクティスを確実に提供するよう取り組んでいます。Uy は、お客様の複雑な要件に対応する適切なセキュリティ製品を選択するよう、セキュリティ専門家として HP、Oracle、ATT、McKesson などの Fortune 100 の大企業のお客様などと連携して仕事をしてきました。

マカフィーの前には、Foundstone で SE 部門を創設し、その指揮をとっていました。その間、大規模なネットワークとシステム向けに、脆弱性管理とリスク管理のベストプラクティスを開発しました。Foundstone の前には、ISS のシニアコンサルタントとして、大規模な組織でさまざまなセキュリティソリューション、セキュリティポリシー、セキュリティテクノロジーの導入を行っていました。

1 http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

McAfee An Intel Company
マカフィー株式会社
www.mcafee.com/jp

東京本社　〒150-0043 東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F　TEL:03-5428-1100(代) FAX:03-5428-1480
西日本支店　〒530-0003 大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F　TEL:06-6344-1511(代) FAX:06-6344-1517
名古屋営業所　〒460-0002 愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F　TEL:052-954-9551(代) FAX:052-954-9552
福岡営業所　〒810-0801 福岡県福岡市博多区中洲5-3-8 アクア博多5F　TEL:092-287-9674(代) FAX:092-287-9675

MCABP-PYDB-1210-MC