

IBM Security MaaS360 with Watson

エンタープライズ・グレードの脅威管理でエンドポイントを保護



ハイライト

Watsonを駆使したAIとセキュリティ分析を利用

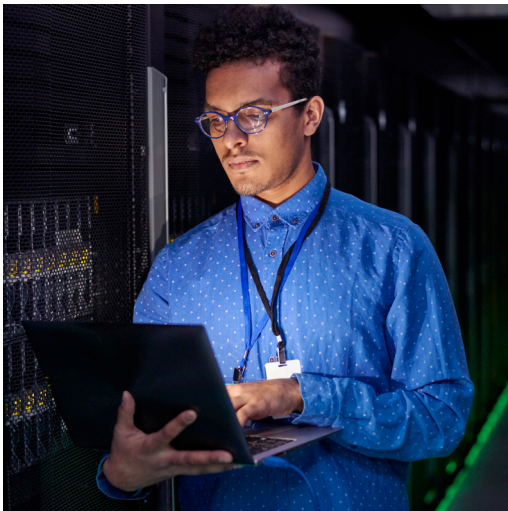
堅牢なセキュリティ・ポリシーでエンタープライズ・データを保護

高度な脅威検知と修復を実現

SIEM、SOAR、およびIAMのサポートを統合

現在の「どこにいても仕事ができる」世界において、組織が追求しているのは、エンドポイントとセキュリティを一元的に管理すること、エンドユーザーに快適なエクスペリエンスを提供すること、サイバー脅威を軽減すること、および所有コストを低く抑えることです。企業は、複数のエンドポイント・セキュリティ・ツールやダッシュボードを使用しなければならない、という課題に直面しています。複数のツールやダッシュボードが存在することで、セキュリティ・アナリストやIT管理者による脅威の軽減と対処への効果的な取り組みが制限される可能性があります。例えば、米調査会社ポネモン・インスティテュートの調査を取り入れたIBMの年次の「Cost of a Data Breach」レポートでは、調査対象組織のデータ漏洩のグローバル平均総コストは、2021年の424万ドルから2022年の435万ドルに2.6%増加したと報告されています。この金額はこのレポートの過去最高値であり、調査対象組織の83%が複数のデータ侵害を経験しています。¹

IBM Security® MaaS360® with Watson®は統合エンドポイント管理(UEM)ソリューションです。その標準装備の脅威管理機能は、これまでの小規模な検出から進化を遂げ、メール・フィッシングやSMSフィッシングなどの脅威や、内部関係者による脅威に対処するための新しい一元化されたポリシーと、広範な一連の検出および対応が組み込まれるようになりました。このソリューションの目的は、モバイル・デバイス、ラップトップ、デスクトップ、ウェアラブル、高耐久性デバイスなどのエンドポイントを管理することで、また拡張された脅威管理機能を使用してそれらのエンドポイントを保護することで、組織が効率と効果の両方を実現できるように支援することです。これらの脅威管理機能はあらかじめ製品に組み込まれており、企業が目標とする総所有コスト水準を達成できるように支援します。



進化した脅威の検出と修復

IDC社の「U.S. Enterprise Workspace Management and Security Survey for 2021」によると、米国のIT管理者やセキュリティ管理者が最も頻りに経験するモバイル・セキュリティ脅威のトップ2として、モバイル・メール・フィッシングとSMSフィッシングが挙げられています²。

IBM Security MaaS360 with Watsonでは、一連の検出と対応によってその脅威管理機能が拡張され、流動的な内部関係者による脅威のユースケース、より重要な地位の内部関係者による脅威、およびゼロトラストの検出が組み込まれるようになりました。MaaS360 with Watsonでは、ポリシーと対応の定義が一元化されたポリシーに統合されます。またリスク・ダッシュボードがフル機能のセキュリティ分析ダッシュボードに拡張されており、APIに基づいた統合の機会が提供されます。これらすべてがリスクベースの条件付きアクセスと組み合わせられ、脅威への対応が自動化されます。

MaaS360 with Watsonは、マルウェア、ジェイルブレイク・デバイス、root化デバイス、および安全でないWiFiに対する保護を行い、さらにSMSフィッシング、メール・フィッシング、Androidデバイスの過剰なアプリケーション権限、WindowsとMacOSのユーザーの権限管理、およびAndroidデバイスのデバイス構成ベースの脅威を検出します。お客様の組織がすでに高度な脅威管理ソフトウェアを使用している場合でも、MaaS360 with Watsonは、既存のほとんどのサード・パーティー・ベンダーと統合できます。

堅牢なセキュリティ・ポリシーを設定して、またはあらかじめ定義されたポリシーを選択して企業データを保護する

IBM Security MaaS360 with Watsonでは、更新された一元管理のエンドポイント・セキュリティ・ポリシーを使用でき、さまざまな種類の脅威の検出と対応を制御できます。MaaS360 with Watsonには、ジェイルブレイク・デバイスやroot化デバイスのシグニチャー・ベースの検出、IBM X-Force® Exchangeのフィッシング検出（メールおよびSMS）、過剰なアプリケーション権限の検出、マルウェアや安全でないWiFiの検出、WindowsおよびMacOSのユーザーとプロセスの権限検出などのユースケースに対応するポリシーが組み込まれています。

IT管理者には、一般的なサイバー脅威の他に、企業のデバイスの返却の管理やデバイスを紛失した従業員の支援など、対処すべき優先事項があります。このようなケースでは、管理者はオンデマンドで場所を確定できます。これにより、紛失したデバイスや盗難にあったデバイスを取り戻すことができ、侵害された可能性のあるユーザー・デバイスが地理的に異常な場所にあることを検出できます。管理者は暗号化のサポートも利用でき、問題が解決されるまで、自動化されたアクション（基本的なアラートから企業リソースの選択的なワイプまで）を有効にできます。

Watsonを駆使したAIとセキュリティー分析を利用

セキュリティー分析とダッシュボードは、最新のUEMソリューションの重要な要素です。IBM Security MaaS360 with Watsonは、洞察と自動化されたアクションの推奨事項を提案するために、構造化データと非構造化データの両方に加えて応用行動分析を使用し、AIを活用して分析と洞察を行います。

ポリシー推奨エンジンは、顧客分析を使用して、組織により適合する可能性のあるポリシーへの個々の変更を提案します。進化した脅威管理機能に適合するように、セキュリティー・ダッシュボードが強化されています。検出結果は、セキュリティー・ダッシュボードの「セキュリティー・インシデント」セクションに表示されます。これらのセキュリティー・インシデントは、セキュリティーAPIを介して使用することもでき、リスク・ルールに基づいてリスク・スコアを計算するために使用されます。デバイス・アクティビティー、アプリケーション、インストール済みソフトウェアでのデータの使用状況などが記載された詳細なレポートも提供されます。

MaaS360 with Watsonでは自動化も適用されるため、IT管理者は、特定のパラメーターに関するレポートを毎日、毎週、または毎月送信するようにメール配信をスケジュールでき、組織の重要な最新の統計を常に把握できます。

SIEM、SOAR、およびIAMのサポートを統合

セキュリティー情報イベント管理(SIEM)およびSecurity Operations, Automation and Response (SOAR)テクノロジーは、世界中の組織で堅牢なセキュリティー体制の一部になっています。MaaS360 with Watsonでは、これらのテクノロジーとの統合が強化され、MaaS360により生成されたインシデント・イベントやデータをサード・パーティー・システムに提供する新しいAPIが作成されています。MaaS360は、エンドツーエンドのセキュリティー・エクスペリエンスを提供するIBM® QRadar®とシームレスに統合されます。これにより、検出されたすべてのインシデントを構成が容易な事前パッケージ済みのログ・ソースを介して参照できます。

企業が、企業標準や業界標準に準拠しつつ、適切なリソースへのきめ細かなアクセス権を付与することで企業情報を保護したいと考えている場合、ID管理とアクセス管理(IAM)が非常に役立ちます。

MaaS360には、エンタープライズSSO用の統合ランディング・ページがあり、IDランチパッドや統合アプリケーション・カタログで使用する企業アプリケーションをプロビジョニングできます。また、危険なユーザーやデバイスが機密データとその他の企業リソースに接触することがないように、リスクベースの条件付きアクセス・ポリシーを構成できます。MaaS360は、従業員IDとクライアントIDの両方の機能を提供するIBM Security Verifyとも統合され、さらに条件付きアクセス機能をサポートする既存の標準IDプロバイダーとも統合されます。MaaS360 with Watsonには、特定のSaaSアプリケーションに適用できる多要素認証が組み込まれており、複数の第2要素がサポートされています。

結論

MaaS360 with Watsonは、自動化、最新のエンドポイント管理、標準装備の脅威管理機能を提供し、フィッシング、中間者攻撃、その他の一般的な脆弱性などのサイバー脅威からの保護に役立ちます。組織は高価なアドオンを購入する必要がなく、MaaS360を既存のセキュリティー・アプリケーションと統合して、目標とする総所有コスト水準を保つことができます。

なぜIBMなのか

IBM Security MaaS360 with Watsonは、エンドポイント、アプリケーション、およびコンテンツのための高度なセキュリティー機能を備えており、主要なすべてのオペレーティング・システムとデバイスの種類に基本的に対応します。MaaS360は、AIとセキュリティー分析、データ損失防止、モバイル脅威管理、ID管理とアクセス管理を提供し、ポリシーとコンプライアンス・ルールを使用できるようにすると同時に、企業がセキュリティー・フレームワークに対してゼロトラスト・アプローチを確立できるように支援します。

詳細情報

IBM Security MaaS360 with Watsonについての詳細は、IBM担当員またはIBMビジネス・パートナーにお問い合わせいただくか、ibm.com/jp-ja/products/maas360をご覧ください。

注

1. The Cost of a Data Breach Report 2022、IBM、2022年7月
2. U.S. Enterprise Workspace Management and Security Survey, 2021: Endpoint Device Management Highlights and Trends、IDC、2021年8月

© Copyright IBM Corporation 2022

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

Produced in the
United States of America
October 2022

IBM、IBMのロゴ、MaaS360、QRadar、IBM Security、IBM Watson、with Watson、およびX-Forceは、米国およびその他の国、またはそのいずれかにおけるInternational Business Machines Corporationの商標または登録商標です。他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。現時点でのIBMの商標リストについては、ibm.com/trademarkをご覧ください。

Windowsは、米国、その他の国、またはその両方におけるMicrosoft Corporationの商標です。

本書は最初の発行日時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「現状有姿」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ます。

IBM製品は、IBM所定の契約書の条項に基づき保証されます。

