McAfee Vulnerability Manager

リアルタイムで高性能な資産監視を継続的に実施

主な差別化要因

- 非常に優れた拡張性と柔軟性を備え、非常に高い精度で診断します。
- ネットワークに接続した新しいデバイスをリアルタイムで評価します。すべてのソフトウェアとハードウェアを資産インベントリに登録し、ユーザーと資産のマッピングを行います。また、ネットワーク トポロジを自動的に作成します。
- アクティブまたはパッシブなネットワーク検出と監視を行い、仮想デバイス、モバイル デバイス、常時接続していないデバイスを特定します。
- デバイス監査でスキャンを実行し、資産データベースを更新します。
- システムのタグ付けを動的に行い、脆弱性評価を自動的に行います。
- McAfee Global Threat Intelligenceから最新の脆弱性情報と脅威情報を取得します。
- Cyber-Arkとの統合で、特権IDによるセキュリティを実行します。
- IPv4とIPv6の両方のネットワークをスキャンします。
- 柔軟なレポート機能により、スキャンした資産のレポートをいつでも作成できます。
- 自動化されたリスク管理ワークフローに、マカフィー、自社製、サードパーティのアプリケーションを組み込むことができます。

業界で最も拡張性に優れ、実績豊富な脆弱性管理でビジネスを常時保護しましょう。Intel® SecurityのMcAfee® Vulnerability ManagerはMcAfee Asset Managerの機能を使用してネットワーク上の資産を管理し、業界で最高のスケーラビリティとパフォーマンスを提供します。デバイスまたは資産にIPアドレスが設定されている場合、あるいはネットワークを使用している場合、McAfee Vulnerability Managerがネットワーク上にある資産の対応状況をリアルタイムで確認します。

McAfee Vulnerability Managerは、ビジネス要件に合わせてネットワーク/資産の構成を詳細に分析する業界最高のソリューションです。必要なときに、必要な場所をパッシブにスキャンし、資産の検出、評価、修復、報告を行います。スキャン時にネットワークに接続していないスマートフォン、タブレット、ラップトップなどのデバイスにも対応しています。スキャンされていないデバイスや未確認のデバイスは、コンプライアンスを脅かす存在になる可能性があります。McAfee Vulnerability Managerは数百ノードだけでなく、百万個以上のIPアドレスから構成される1つのスャニング ノードにも配備できます。非常に多くの組織がこのソリューションで脆弱性を迅速に特定し、対策の優先度を決めています。

簡単な実装

信頼性の高いスキャンを簡単に実装できます。McAfee Vulnerability Managerは物理または仮想ハードウェアに簡単にインストールできます。マカフィーの強固なアプライアンスを利用することもできます。インストールが完了すると数分で最初のスキャンが開始します。

資産インベントリの読み込みや維持も簡単です。新しいデバイスがオンラインになるとすぐに、McAfee Asset Managerモジュールが資産データベースを更新し、問題のあるデバイスをリアルタイムで確認できるようにします。McAfee Vulnerability ManagerはLDAP、Microsoft Active Directory、McAfee® ePolicy Orchestrator®（McAfee ePO™）などの資産管理ツールと直接統合されているので、資産データを中央のリポジトリで一元管理できます。

すべての資産を可視化

McAfee Asset Managerのオプションを使用すると、パッシブ検出と監視を常時実行し、可視性を向上させることができます。SPANポートに迅速に配備できるので、トラフィックを監視し、ネットワーク上のすべて対象（不正なデバイス、パスワードを忘れたVMwareホスト、モバイル デバイスなど）を関連付けます。デバイス、パターン、通信を再現することで、リスクを測定し、回避策を講じることができます。デバイスの詳細はMcAfee Vulnerability Managerに自動的に送信され、すぐに評価されます。McAfee Asset Managerは資産を検出するたびに、資産に関連するソフトウェア/ハードウェアの情報をインベントリに登録します。

intel Security

スキャン対象

- オペレーティング システムのスキャン: Microsoft Windows、UNIX、Cisco、Android、Linux、Apple Macintosh、Apple iOS、VMwareを含む450以上のOSに対応
- Web アプリケーションの詳細スキャン: OWASP Top 10、CWE Top 25
- 脆弱性とマルウェアの検索: Adobe、AOL、Apple、Microsoft（Office、IIS、Exchange）、Blue Coat、CA、Cisco、Citrix、Facebook、Google、HP、IBM（Lotus Notes、Websphere）、Novell、Oracle、Real Networks、RIM（BlackBerry Enterprise Server）、SAP、Oracle Java、Symantec、VMware
- データベースのスキャン: DB2、MySQL、Oracle、Microsoft SQL Server、Sybase

規格と認定

- テンプレート: ASCI 33、BASEL II、BILL 198（CSOX）、BSI IT（GR）、COBIT、FDCC、FISMA、GLBA、HIPAA、ISO 27002、JSOX、MITS、PCI、SOX、NIST SP 800-68、SANS Top 20、SCAP、OVALなど
- 対応規格: CIS認定監査、COBIT、CPE、CVE、CVSS、DISA STIG、FDCC/SCAP、ISO17799/ISO 27002/FINRA、ITIL、NIST-SP800、NSA、OVAL、SANS Top 20
- Common Criteria認証
- FIPS-140-2認定

要件に合わせてスキャンをカスタマイズ

McAfee Vulnerability Managerのオプションを使用すると、ベンチマーク テストを実施し、法規制への対応状況を報告することができます。ポリシーを迅速に定義するには、代表的なシステムをスキャンしてベースラインを設定し、付属のコンプライアンス テンプレートを利用するか、SCAP（Security content automation protocol）を利用してポリシーを読み込みます。

McAfee Vulnerability Managerは、ネットワークに接続しているすべての資産をスキャンします。エアギャップ環境や重要インフラにある資産もスキャンします。外部接続のないネットワークの場合、ラップトップ ベースのスキャナーまたは仮想スキャナーを配備すると、資産を簡単に検出できます。制限のある環境で結果を保持することも、一元管理システムに転送することもできます。

大半のオペレーティング システムでは、資産の認証情報を入力しない限り重要な構成情報にアクセスできません。セキュリティ チームが何らかの理由でこの認証情報にアクセスできない場合もあります。Cyber-Arkの特権ID管理スイートとの統合により、パフォーマンスを低下させずに、認証情報による検出とスキャンを簡単かつ安全に実行できます。

リスクを数分で特定

McAfee Asset Managerがネットワーク上で新しいシステムを認識すると、そのシステムに関する詳細情報をMcAfee Vulnerability Managerに送信し、対象のスキャンを実行します。数分でシステムの状態と環境を取り巻くリスクを確認できます。

資産のタグ付けによる生産性の向上

タグ付けポリシーを使用すると、デバイスのプロファイルとリスクに応じて新しいデバイスがスキャン グループに自動的に配置されます。適切なスキャンをすぐに実行できます。定義したポリシーによっては、次のスキャンが実行されるまで待つ必要があります。

脆弱性とマルウェアの両方を検出

他のソリューションは単にオープン ポートや設定を確認するだけですが、McAfee Vulnerability Managerはそれ以上の機能を実行します。データベース バナー、ポリシー設定、レジストリ キー、ファイル/ドライブのアクセス権、実行中のサービスなどをシステムまたはアプリケーションごとに評価します。この製品は450以上のオペレーティング システムをテストし、様々な脆弱性を検出します。また、トロイの木馬やウイルスなどの不正なコンテンツも検出します。

事前定義の検査と更新でゼロデイの脅威を検出します。カスタム スクリプトを作成して専用プログラムや古いプログラムを検査することもできます。McAfee Vulnerability Managerは、XCCDF、OVAL、SCAPなどの規格に準拠するサードパーティ コンテンツも評価します。

Webアプリケーションに対する対応

McAfee Vulnerability Managerを使用すると、従来のネットワーク資産と同様にWebアプリケーションを管理できます。Webアプリケーションの資産はグループに分類できます。これらの資産には固有の重大性、所有者、特徴があります。McAfee Vulnerability Managerは、完全な自動化機能により、Web アプリケーションに詳細なスキャンを実行し、Webの脆弱性を特定します。

常に最新の状態を維持

世界各地に配備された数百万台のセンサーとMcAfee Labsの数百人の研究者から最新の脅威情報が提供されます。McAfee Global Threat IntelligenceがMcAfee Vulnerability Managerにリスク評価と脅威アドバイザリをリアルタイムに送信するので、新たに発生する脅威も未然に防ぐことができます。

必要に応じた管理、拡張、統合

組織の要件に合わせてスキャンを柔軟に設定できます。必要に応じてレポートを作成し、管理作業を実行できます。ローカル ネットワークの資産を監視するだけでなく、リモートにある大量のスキャン エンジンの状況を1つのコンソールで確認することもできます。多層アーキテクチャを採用しているので、組織の要件に合わせて機能を拡張できます。

McAfee Vulnerability Managerは、オープンAPI（アプリケーション プログラミング インターフェース）により、大半のアプリケーションと統合することができます。

リスクの重大度に合わせた対応

脆弱性の存在を一目で確認できるので、パッチの回数や監査コストを削減できます。たとえば、毎月のセキュリティ更新の公開日に、Microsoft WindowsやAdobeの新しい脆弱性の影響を受けるコンピューターをすぐに特定できます。McAfee Vulnerability Managerはネットワーク全体の再スキャンを行わず、既存の構成データとリスク スコアから潜在的なリスクの優先度を判断し、ランク付けを行います。

この情報からリスクの重大性を判断し、要検査の資産を右クリックしてスキャンを実行できます。

簡単なコンプライアンス対応

予期したスキャン結果と実際のスキャン結果、スキャンしていないシステム、失敗したスキャンなど、確実な証拠を生成します。監査要件が厳しい状況でも、特定のシステムが脆弱でないことを証明できます。McAfee Vulnerability Managerは、アクティブ/パッシブな監視、侵入テスト、認証スキャン、認証情報を使用しないスキャンを組み合わせることで、脆弱性とポリシー違反をピンポイントで検出するので、包括的な脆弱性管理を簡単に行うことができます。

McAfee. Part of Intel Security.

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　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F
TEL 052-551-6233（代） FAX 052-551-6236

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）

www.intelsecurity.com