

仮想パッチによる重要資産の保護と 運用性の向上

予測的に脅威を防御し脆弱性が放置される期間を短縮

目次

リスクの増加とダウンタイムにつながる脆弱性	3
臨時パッチ処理	3
変更管理アプローチ	4
事後的な変更管理	4
予防的な変更管理	4
仮想パッチ処理	4
マカフィーの仮想パッチソリューション: 多層型セキュリティリスク管理	5
McAfee Network Security Platform	5
McAfee Vulnerability Manager	5
McAfee Risk Advisor	6
導入オプション	7
仮想パッチ処理(手順ガイド)	8
マカフィーを信頼できる理由	11

昨今のIT組織にとって、予算、スタッフ、セキュリティ知識すべてが不足している状況は当たり前となつてしまいました。残念なことに、こうしたIT組織には、パッチ処理していない脆弱なインフラストラクチャーと最適化されていないセキュリティ体制も当たり前になってしまっているため、企業は大きなリスクにさらされ、高額なコストがかかっています。

予測的な脅威への対応、自動的な脆弱性スキャン、リスク視覚化を使用する仮想パッチ処理は、拡張性あるコスト効率の高い重要資産保護手法です。この手法を導入することにより、セキュリティ管理コストを大幅に削減しながら、パッチ/変更管理プロセスを強化することが可能になります。

リスクの増加とダウンタイムにつながる脆弱性

ソフトウェアには脆弱性がつきものです。IT組織は、毎年多数のサーバーと多数のクライアントの数千にのぼるCVE(Common Vulnerabilities and Exposures)に直面します。Microsoftだけでも、2009年に183のCVEを発表しており、そのうち100以上が「重大」と分類されています。脆弱性があるところには、必ずマルウェアとサイバー犯罪が発生します。

サイバー犯罪には、驚異的な速度で新しいスパイウェア、ウイルス、トロイの木馬、ワーム、その他のマルウェアが次々に投入されています。2009年だけでも、McAfee Labs™は220万以上のマルウェアを検出しました。この数は、2008年の160万件からほぼ40%増加しています。脆弱性、マルウェアとも増加しているにも関わらず、IT予算はますます削減されており、大半のIT組織は限られたスタッフでサイバー犯罪に対抗することを余儀なくされています。

パッチ処理は、マルウェアとサイバー犯罪との戦いで重要な役割を果たします。しかし、パッチ処理を行うには時間とコストがかかり、時期も予測できないため、大半の組織でパッチ処理に遅れが生じています。250名のITプロフェッショナルを対象に実施された最近の調査によると、61%が平均のパッチ処理間隔を2週間以上と回答しています。臨時公開されたパッチを定期的なパッチサイクル外で即座に適用するとして回答者は33%に過ぎません。脆弱性の発見からパッチ処理までにこうした時間的ギャップがあると、組織が大きなリスクにさらされてしまいます。

どのような変更管理/パッチ処理を行っていても、ほぼすべての企業の重要な資産が現在も危険な状態にあります。たとえば、2010年9月、米国土安全保障省の機関で他の政府機関をコンピューター侵入者から保護する(およびFAA/ホワイトハウスにセキュリティ警告を発行する)役割を担っている国家サイバーセキュリティ部門(NCSD)は、システム内に数百もの高リスクの脆弱性を発見しました。その原因は、NCSDがシステムへの最新のソフトウェアパッチ処理を怠っていたことにあります。リスクが高い脆弱性の大半には、アプリケーション、オペレーティングシステム、セキュリティソフトウェアの未適用のパッチが関連していました。結局US-CERTによって、202の高リスクセキュリティホールに加え、106の中リスク脆弱性、36の低リスク脆弱性も発見されました。¹

臨時パッチ処理

企業は、重大な脆弱性に対処するために頻繁に臨時パッチの適用を余儀なくされています。パッチおよびリスクにさらされているシステムの性質によりますが、こうした混乱を招くパッチ処理方法は予期しないダウンタイムなどのリスクをはらんでおり、サービスの停止、生産性の低下、IT部門の時間外勤務、さらにはテスト不足によるシステムのクラッシュなどに発展する可能性があります。その結果、発生する運用コストと利益の損失は、組織の最終収益に大きな打撃を与えかねません。たとえばZDNetによると、Confickerだけで91億ドルの経済的被害をもたらしています(出典:<http://www.zdnet.com/blog/security/confickers-estimated-economic-cost-91-billion/3207>)。

パッチ未処理システムのリスクに直面している組織にも、頻繁なパッチ処理で高額なコストがかかっている組織にも、脆弱なシステムがIT環境に常にもたらしている負担を軽減する効率的な手段が必要です。

Microsoftを上回る脆弱性

2010年第二四半期、世界の2大ソフトウェアベンダーであるMicrosoftとAdobeは、大量のセキュリティアップデートを発表しました。AdobeはCVEデータベースにリストされていた87の脆弱性を、MicrosoftはCVEの別の61の脆弱性を修復しました。わずか3ヶ月間に、たった2社のソフトウェアベンダーのおよそ150の脆弱性にパッチを適用する必要性が生じたのです。マカフィーの調査によると、Adobeの脆弱性は今後も増加し、脆弱性数でMicrosoftを凌ぐことになりそうです。

1. Wired Magazine, 2010年9月: www.wired.com/threatlevel/2010/09/us-cert/

変更管理アプローチ

脆弱なシステムに対して企業が選択する変更管理方法は、主に事後的、予防的、仮想パッチ処理の3つに分類されます。次のセクションでは、各方法を検証および比較し、ネットワークセキュリティおよび脆弱性管理を使用して従来の予防的なパッチ処理方法と仮想パッチ処理方法を併用するメリットについて説明します。

リスクにさらされている重要なインフラストラクチャー

先頃マカフィーでは、世界中の重要インフラ運用企業の600名のIT/セキュリティエグゼクティブを対象に調査を実施しました。この調査で、脆弱性とセキュリティに関する興味深い結果が判明しました。

- 定期的なスケジュールに従ってソフトウェアのパッチ処理/アップデートを実施していると回答したエグゼクティブはわずか57%
- 54%は、「組織犯罪、テロ、国家など、高度な敵対者からの大規模なDoS(サービス拒否)攻撃」を経験したことがあると回答
- 54%は、自社のネットワークが同様に高度な敵対者の「不正侵入」の影響を受けたことがあると回答
- これらの組織が経験した大規模なDDoS(分散型DoS)攻撃の約3分の2は、組織の業務に影響を及ぼした(公開しているWebサイトがアクセス不能になった、電子メール接続に影響が出た、インターネットベースの電話システムやその他の業務中核機能が中断したなど)

事後的な変更管理

事後的な変更管理とは、特定の変更管理計画を持たない組織にとっての唯一の選択肢です。「その場しのぎのパッチ処理方法」とも呼ばれています。

この方法でパッチ処理に対応している企業は、相当の時間、労力、資金を無駄にしていますが、組織は攻撃にさらされたままの状態です。こうした企業は、定期的なサイクルに従ってパッチを適用していないため、臨時パッチ処理という概念がありません。また、パッチに優先順位を付ける包括的な手段がないので、ほぼOSおよびアプリケーションベンダーのパッチリリースだけに頼ってパッチ処理スケジュールを決定しています。IT部門は自社の脆弱性や自社ネットワークを標的にしている脅威に対する可視性をほとんど、あるいはまったく持っていないため、重大なCVEが優先的に処理されています。

予防的な変更管理

事後的でその場しのぎのパッチ処理方法とは対照的に、予防的な変更管理では事前に処理を計画し、ベンダーの通常のパッチリリーススケジュールに基づいた予測可能なパッチ処理サイクルを実行します。通常このカテゴリーの組織は、ビジネスにとって最も都合がよいとき(営業時間外や週末など重要なシステムの使用率やネットワークトラフィック量が低いとき)にパッチ処理を計画します。クライアントシステムの多くは毎週または2週間に1回、アプリケーションサーバーは毎月、重要なデータベースサーバーは四半期ベースでパッチが適用されています。予防的な変更管理を実施している組織でも、ほとんどはシステム脆弱性の数や重大度が把握できる統合的なビューを導入していません。そのため、ネットワーク脆弱性と差し迫った脅威の関連性を把握するには、手作業で相関付けを行う必要があります。予防的な変更管理プロセスを導入している組織は、現在もリスクと臨時パッチ処理という業務上の危険にさらされていますが、計画されているパッチ処理回数を増やす手段がありません。

仮想パッチ処理

変更管理の3つ目の方法は、予防的な変更管理を補完する仮想パッチ処理です。仮想パッチ処理とは、組織が営業時間外に実施する通常の変更管理プロセスで実際にパッチを適用するまで、テクノロジーを活用して脆弱性を狙った新しい脅威から保護する方法です。この方法を採用することで、「その場しのぎ」のパッチ管理の概念をなくし、運用を合理化し、コストを削減することができます。仮想パッチ処理は、臨時パッチ処理や頻繁なパッチサイクルの必要性を低減する点で非常に有益です。

仮想パッチ処理では、次のようなテクノロジーが使用されます。

- 脆弱性スキャンによって、すべてのデバイス、アプリケーション、オペレーティングシステム、IPアドレス、ネットワークに関連するURLの脆弱性を検出します。
- リスクアセスメントツールと脅威/脆弱性/対策情報を組み合わせて、リスクにさらされている資産を正確に特定し、セキュリティ活動に優先順位を付けます。
- ネットワーク不正侵入防止システム(IPS)を利用してネットワークトラフィックを監視し、悪質な活動をブロックします。
- 企業セキュリティコンソールによって上記のシステムからすべてのデータを収集し、ネットワークセキュリティのリアルタイムビューを取得します。単一の一元管理ポイントから、相互に連携するこれらのシステムに統合的に操作を実行できます。

	事後的な変更管理	予防的な変更管理	仮想パッチ処理 + 予防的な変更管理
効率性	非効率、多くの労力を浪費	より効率的	非常に効率的
定期的なパッチ処理	実施しない	実施する	実施する
臨時パッチ処理	実施できない	重大なアップデートのときは必要	不要になり、コストを削減できる
定量化されたリスク影響度	把握できない	把握できない	把握できる
リスク体制に対する効果	限定的	改善されるが、組織はなお大きなリスクに直面する	最善、リスクは大幅に低減される
重大な脆弱性にさらされる時間	無制限	数日～数週間	数時間
総合的なリスク緩和戦略	運任せ	積極的にITインフラストラクチャーの保護を推進する	多層型のセキュリティ/組織的パッチ処理により脆弱性にさらされる期間を排除

図1: 3つの変更管理手法の比較

McAfee Global Threat Intelligence™

McAfee Global Threat Intelligence は、次のリソースを基盤としています。

- 世界中で稼働している1億を超えるマカフィーノード
- ファイル、Web、メッセージ、ネットワークなどすべての脅威媒体から取得する毎月1000億を超えるクエリー
- 市場で最も包括的な脅威インテリジェンスサービス(ファイルレピュテーション、Webレピュテーション、Web分類、メッセージレピュテーション、ネットワーク接続レピュテーション)

マカフィーの仮想パッチソリューション: 多層型セキュリティリスク管理

仮想パッチ処理は単なる一時的な修復ではありません。パッチ/変更管理プロセスを強化すると同時にシステムのリスクを低減する、信頼性の高いセキュリティ確保アプローチです。

マカフィーの仮想パッチ処理ソリューションは、セキュリティリスク管理に対して多層型のアプローチを提供します。したがって、既存の変更管理プロセスに仮想パッチ処理戦略を追加することが可能になります。実績ある防御機能、セキュリティ情報、リアルタイムのグローバル脅威インテリジェンスを組み合わせることで、組織が定期的な変更管理プロセスを通じてパッチ処理を実行するまで、脆弱性にさらされる期間を排除します。

McAfee Network Security Platform、McAfee Vulnerability Manager、そしてMcAfee Risk Advisorの統合を通じて、包括的なリスクアセスメントを実施することで、迅速に対応することができます。

McAfee Network Security Platform

McAfee Network Security Platformは、業界をリードする侵入検知/防止を含む統合型ネットワークおよびシステムセキュリティを提供します。このプラットフォームの予測型セキュリティエンジンは、異常検出機能とクラウドベースの脅威インテリジェンス、従来型のシグネチャーベース防御を組み合わせ、脆弱なシステムに対する攻撃を防止します。Network Security Platformは、不審なネットワーク侵入を検出するだけでなくとどまらず、脆弱性ベースのシグネチャーとMcAfee Global Threat Intelligence™が提供するリアルタイム脅威情報を使用して、被害が及ぶ前に悪質な攻撃をブロックします。Network Security Platformでは、仮想パッチ処理の効果をさらに高めるために、疑わしいシステムや脆弱なシステムを検疫しておくこともできるので、パッチの作成後、企業の定期的なパッチサイクル中のテスト、導入が終わるまで他のネットワークリソースを保護することができます。

McAfee Vulnerability Manager

McAfee Vulnerability Managerは、すべてのネットワーク資産の脆弱性をスキャンし、リスク影響度とポリシー違反を検出します。McAfee Vulnerability Managerは、脆弱性に優先順位を付けることによってITの効率を高め、重要なパッチ処理を高速化すると同時に優れた投資効果をもたらします。

McAfee Vulnerability Managerは、脆弱性を検出した後、迅速かつ正確に最も重要なパッチ処理および修復処理を特定できるように支援します。組織では、標準ベースのスコアリングを通じて重要資産に焦点を当ててスキャンを実行し、適切な保護策を講じているかどうかを確認することができます。

McAfee Risk Advisor

McAfee Risk Advisorは、プロアクティブに脅威/脆弱性/対策情報を組み合わせて、実際にリスクにさらされている資産を正確に特定するため、推測に頼らずに、いつ何に焦点を当ててセキュリティ作業を行うべきかを判断できるようになります。McAfee Risk Advisorは、脆弱性アセスメント結果を分析した後、誤認率を最小限に抑えて最適な保護を実現するためにどのシグネチャーや対策を使用すべきかを決定します。また、リスク低減活動の効果を評価する定量的な指標となる、最新のリスクスコアも提供します。たとえば、管理者はこのスコアを使用して、「特定の期間のリスク低減活動によって、リスクがX%増加/低下した」ことを確認することができます。

包括的な保護範囲を評価すると、マカフィーは重要なMicrosoftインフラストラクチャーの保護においても優れています。

- 2009年に公開されたリモートから悪用可能な合計183のCVEに対する他のベンダーの平均検出率は49%でしたが、McAfee® Network Security Platformは88%を超える検出率を達成し、保護範囲が最も包括的であることを実証しました。
- また重要な脆弱性の保護範囲も、他のベンダーの平均が56%であったのに対し、マカフィーは98%と最も幅広い保護を達成しました。

McAfee Network Security Platformは、市場に投入されて以来、常にこの包括的な保護を提供しています。

2009年Microsoft Bulletins保護範囲

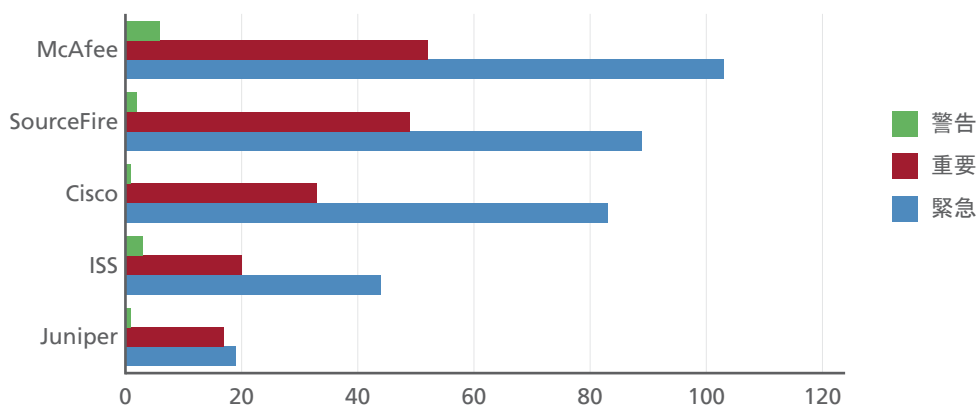


図2: 重大度レベル別のゼロデイ脆弱性保護範囲 (2009年1月~12月)

導入オプション

完全な仮想パッチ処理ソリューションを導入すると、最高レベルの可視性、価値、自動化、保護を享受することができます。マカフィーは、ベストプラクティスとして完全なソリューションの導入を推奨しています。ただし、仮想パッチソリューションの段階的な導入を選択することもできます。

Citrix Systems でのセキュリティリスク管理

Fortune 500 企業の 99% を顧客ベースに持つ Citrix Systems は、アプリケーション提供インフラストラクチャーのグローバルリーダー企業です。彼らは、マカフィーソリューションがセキュリティリスク管理で果たす重要な役割を理解しています。

マカフィーの多層型セキュリティソリューションの実装後、Citrix は次のように成果を達成しました。

- セキュリティインシデント対応時間を40%削減
- McAfee Network Security Platformを使用していなければ把握できなかった攻撃を認識してブロック
- 修復時間をおよそ70%削減し、監査修復コストを130,000ドル節約。McAfee Vulnerability Managerの導入わずか1年でROIを達成
- ePOを使用して、膨大な時間がかかっていた手動によるパッチ、アップグレード、hot fix処理を排除

- 受賞経歴のある侵入保護システムを含むMcAfee Network Security Platformが、ネットワークセグメント上の脆弱なシステムの基本的なベースライン保護を提供します。
- さらにMcAfee Vulnerability Managerを追加することにより、最もリスクが高いシステムに焦点を当ててパッチ処理やセキュリティ作業を行うことが可能になり、リスク影響度と運用効率を改善することができます。
- このソリューションを完成させるMcAfee Risk Advisorおよび統合管理コンソールMcAfee ePolicy Orchestrator® (ePO™)を導入することによって、推測に一切頼らずに、保護が必要なシステムと適切な防御メカニズムを正確に特定することができます。

McAfee® Global Threat Intelligence™ (マカフィーの優れた保護提供手段)

McAfee Network Security Platformは、シグネチャーベースの防御に加え、McAfee Global Threat Intelligence (McAfee GTI)を通じたリアルタイムのレピュテーションベースの保護を提供します。この機能によって、セキュリティが低下しているWebサイトを訪れたユーザーが予期せずにダウンロードするマルウェアからユーザーを保護することができます。McAfee Network Security Platformは、McAfee GTIのリアルタイム保護を通じて、3500万を超えるマルウェアサンプルから企業ネットワークを保護します。McAfee Network Security ManagerコンソールでMcAfee GTIをオンにするだけで、クラウドベースによるセキュリティのパワーを享受することができます。

McAfee Global Threat Intelligenceは、ファイル、Web、電子メール、ネットワークなどすべての主要脅威媒体で発生する既知および新しい脅威両方に対応する、業界で最も包括的なリアルタイム保護を実現しています。このクラウドベースの脅威インテリジェンスサービスは、インターネット全域に広がっており、数百万台のセンサーを使用して絶えず実世界の脅威情報を収集しています。

このインテリジェンスは、長期間かけてファイル、Webサイト、IPアドレス、センサーのレピュテーションを理解し、このレピュテーションベースの情報と高度な脅威保護手法を関連付け、既知および新しい電子的脅威の正確なリアルタイム情報を生成します。この優れた脅威インテリジェンスは、包括的なマカフィーセキュリティ製品スイートを通じて提供されるので、お客様がリスクにさらされる期間を数日から数秒にまで効果的に短縮するとともに、多くのケースで予測的にお客様を保護します。

- 包括的な保護によって、インシデント発生の可能性を低減し、インシデント修復にかかるコストを削減し、セキュリティ体制を改善します。
- 脅威インテリジェンスのリアルタイム収集、分析、配布を通じて、保護までにかかる期間を数日、数時間から数秒、あるいは数ミリ秒に短縮し、多くのケースで予測的な保護機能を提供します。
- マカフィー製品との統合によって、常に完全な保護範囲に対応しながら、管理のオーバーヘッドを低減します。

リアルタイムの脅威情報と優れた保護機能を提供するMcAfee GTIを活用することで、企業では仮想パッチ処理などの革新的なパッチ管理戦略を実践することができます。

仮想パッチ処理(手順ガイド)

次のプロセスは、以前のシナリオで紹介したすべての製品が導入されていることを前提としています。

ステップ1: McAfee Network Security Platformの導入

仮想パッチ処理ではMcAfee Network Security Platformの侵入防止機能を活用します。最初のステップは、関連ネットワークセグメント内の重要資産を保護するネットワークセキュリティの戦略的な導入です。ネットワーク境界から開始し、データセンターのエッジ、データセンター内のセキュリティ強化セグメント/ゾーン間に導入します。このネットワークセキュリティは、外部ソースから仕掛けられた攻撃およびネットワーク内部で発生した攻撃に対するベースライン保護を提供します。さらにMcAfee Network Security Platformは、独自のポリシーで物理/仮想両方のネットワークセグメントへ柔軟に対応する仮想化機能を含め、次世代ネットワークアーキテクチャーもサポートしています。

ステップ2: ネットワーク全体の脆弱性スキャン

卓越した拡張性を備えるVulnerability Managerは、スマートフォン、プリンター、悪質なデバイス、忘れられたVMwareホストのほか、アプリケーション、オペレーティングシステム、バージョン番号などの中間物を含む、ネットワーク内のすべての資産を入念に調査します。IPアドレスを持つ資産の場合は、IPアドレスを検出してスキャンを実行します。

たとえば、パッチが更新される火曜日には、Microsoft WindowsまたはAdobeの新しい脆弱性に影響を受ける可能性があるマシンを迅速に特定できます。Vulnerability Managerは、ネットワーク全体をスキャンし直すことなく、既存の構成データおよびリスクスコアに基づいて、新しい脅威によるリスクをはらむシステムを数分で視覚的にランク付けします。

ステップ3: 脆弱性スキャンと導入されている対策に基づいた組織のリスク体制の評価

McAfee Risk Advisorは、McAfee Global Threat Intelligenceによって提供された脅威フィードと、企業内の脆弱性/対策情報を相関付けます。組織内に存在するリスクのある資産を即座に評価し、推奨する修復策およびその後のパッチ処理手順を通知します。管理者は、脅威、脅威の重大度、脅威がもたらすリスクに関する詳細な情報を即座に取得できるので、資産の価値に応じて修復作業に優先順位を付けられます。McAfee Risk Advisorは、定量化されたリスクスコアも提供するため、時系列でリスクのレベルを把握し、グラフを作成することができます。

McAfee Risk Advisorを使用すると、脆弱性プロファイルのグラフを作成し、セキュリティ作業で何に焦点を当てるべきかを正確に把握することができます。また、McAfee Risk Advisorに表示される「At Risk(リスクあり)」および「Not At Risk(リスクなし)」サマリーをドリルダウンして、詳細情報を取得することができます。

ePolicy Orchestratorコンソールでは、企業セキュリティ管理ツールの監視だけでなく、最新の状態でないシステムに必要なDATやその他のファイルをプッシュ配信することもできます。

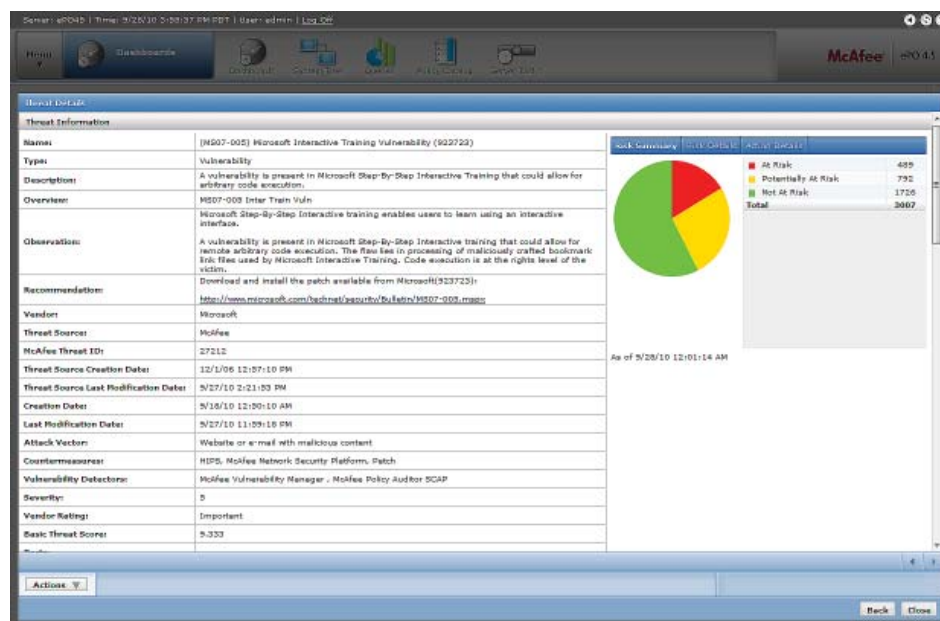


図3.:「At Risk(リスクあり)」の資産は、脆弱性があり、対策によって保護されていません。

ステップ4: McAfee Security Platformで補足的な脆弱性保護を有効化

McAfee Network Security Platformのデフォルト推奨設定は大半のベンダーの「環境に合わせてチューニングした」保護レベルよりも高度な保護を提供します。事実、NSS Labsは、2010年にMcAfee Network Security Platform自らが「推奨する」ポリシー設定を使用して、90%を超える脅威をブロックしていると報告しています。

McAfee Vulnerability ManagerとMcAfee Risk Advisorを利用することにより、組織ではシステムの脆弱性に対する保護と、推奨される適切な対策との差異を簡単にすばやく特定することができます。たとえば、特定できた適切な脆弱性ベースのシグネチャーを有効化して最新の脆弱性と脅威からシステムを保護することができ、次の定期的なパッチ処理サイクルにIT担当者がシステムに適切なパッチ処理をするまでリスクの影響を排除できます。McAfee Network Security Platformを使用することで、予測的な脅威保護とMcAfee Labsのすばやい脆弱性シグネチャーを通じて、発表後、数時間のうちにシステムを保護することができます。

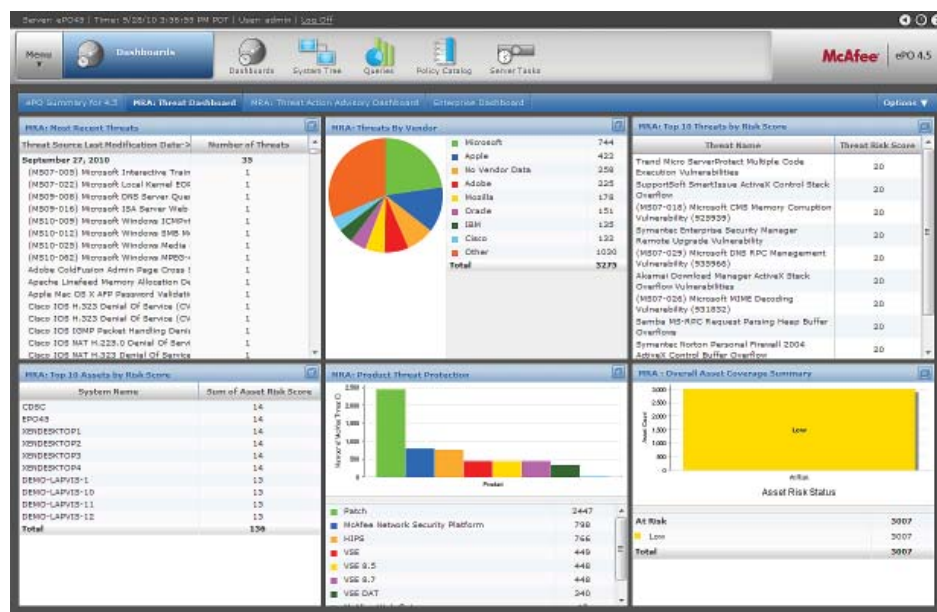


図4: McAfee ePOには、脅威と対応する脆弱性の完全なビューが表示されるため、セキュリティ管理者はセキュリティ作業に優先順位を付けることができます。

このプロセスを簡略化するために、McAfee Risk Advisorは、保護に必要なシグネチャー、および導入の有無を表示します。必要なシグネチャーを入手していない場合は、Network Security Platform コンソールからいつでもシグネチャーをダウンロードできます。

ただし、使用可能なすべてのシグネチャーを導入すると、ネットワークのパフォーマンスの低下や、誤認(正当なネットワークトラフィックのブロック)が発生する可能性がありますのでご注意ください。こうした理由から、McAfee Risk Advisorの情報を参考にしてより最適なシグネチャーを導入いただくことがベストプラクティスです。

自社のセキュリティ製品活用による運用負担の削減(マカフィー社)

	実施前	実施後
クリティカルなパッチの適用	19	9
担当運用者数	41	19
1回あたりの平均作業時間	73	68

図5: マカフィーは、仮想パッチ処理を通じて年間のパッチサイクルの負担をほぼ80%削減しました。

マカフィーのIT部門は、社内プログラムの一環として仮想パッチ処理を導入しました。その結果、パッチサイクル数と重要なITインフラ管理に必要なリソース数の削減に成功しました。McAfee Network Security Platformとともに、McAfee Vulnerability ManagerとMcAfee Risk Advisorを導入することで、時間とコストを大幅に節約するとともに、組織のリスク影響度を飛躍的に改善できました。

マカフィーを信頼できる理由

マカフィーは、コンピューターセキュリティに専念している唯一の企業です。業界で最も包括的なセキュリティ管理プラットフォームを提供し、プロアクティブなリスク管理、ビジネスオペレーションとの統合、協調的な防御を実現することができます。

マカフィーのソリューションは、お客様のITインフラに次のようなメリットを提供します。

- ・ **セキュリティ状況の把握** — リスク管理指標の監視、管理、レポート作成によって、脅威の検出および応答時間を削減し、焦点を絞ったセキュリティ作業および投資を行うことにより、コストを削減できます。
- ・ **インテリジェンスの共有** — セキュリティ階層全体にわたる協調的な防御により、エンドポイント、電子メール、Web、データ階層すべてを連携させてセキュリティ攻撃を最小化または排除できます。
- ・ **グローバルな異種混在環境の保護** — ホスティング、クラウド、SaaS、自社運用、および仮想、物理環境全体のすべてのデバイス、ネットワーク、アプリケーション、データベースのセキュリティを管理できます。
- ・ **オープンプラットフォーム** — セキュリティを既存のプロセスに統合し、システム/変更管理フレームワークを一元的なセキュリティオペレーションに組み込むことができます。



www.mcafee.com/jp

●製品、サービスに関するお問い合わせは下記へ

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