Trend Micro
Deep Security

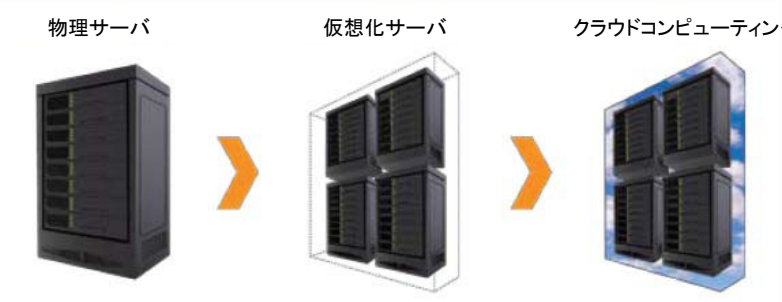
サーバのセキュリティ

動的なデータセンターの保護

トレンドマイクロ ホワイトペーパー | 2009 年 8 月

I. 動的なデータセンターのセキュリティ

IT セキュリティの目的はビジネスを可能にすることで、妨げることではありませんが、IT セキュリティについて直面する課題と複雑さは日々に増大するばかりです。コンプライアンス要件は、サーバ上のデータとアプリケーションにセキュリティ基準を課します。コストの削減、グリーン化、スケーラビリティの向上のため、物理サーバは仮想マシンに置き替えられています。クラウドコンピューティングは従来型の IT インフラストラクチャを発展させて、柔軟性、キャパシティ、選択の自由度を拡大しながら、さらにコスト削減ができるようにします。サーバは、もはや境界での防御線では保護できず、ノート PC と同様に、セキュリティ境界の外側で最前線の防衛を必要としています。徹底的な防衛のためのセキュリティ戦略には、サーバとアプリケーションの保護システムを配備して、包括的なセキュリティ管理を実現しながら、現在と将来の IT 環境をサポートしていくことが必要不可欠です。トレンドマイクロは、Deep Security ソリューションなどの製品で、これらの課題に対処します。



サーバへの圧力

Verizon Business Risk Team の「2008 Data Breach Investigations Report」によると、最近起こったデータ侵害の 59%は、ハッキングと侵入の結果として発生しています。小売大手の TJX 社と Hannaford 社で起きたデータ侵害は、どの業界でもシステムによって企業の評判と業務運用に悪影響を受ける危険性があることをあらためて示しました。組織では、リソースの保護の必要性と、リソースへのアクセスをより多くのビジネスパートナおよび顧客に開放する必要性との間でバランスをとる努力を続けています。

現在のクレジットカード業界データセキュリティ基準（Payment Card Industry Data Security Standards、PCI DSS）は、従来型の境界の防御ではもはや最新の脅威からデータを保護できず、アプライアンスベースのファイアウォールや侵入検知および防止システム（IDS/IPS）を超える、複数層での保護が必要であるとしています。無線ネットワーク、暗号化された攻撃、モバイルリソース、脆弱性のある Web アプリケーションはいずれも、企業のサーバを侵入と漏えいの危険にさらす弱点になります。

過去 5 年間に、主に物理サーバをベースとしてきたデータセンターのコンピューティングプラットフォームは、大きなテクノロジの変化を遂げました。サーバの統合整理によって、従来型データセンターの設置領域は小さくなり、コスト削減と「グリーンな」IT を実現できるようになっています。ほとんどの組織は、データセンターでの作業量の一部またはすべてを仮想化し、これまでシングルテナントつまり単一目的で使用されていた物理サーバを、マルチテナントで使用できるようにしています。Gartner Group は、これから 2011 年までに仮想マシンのインストールベースは 10 倍以上に拡大し、2012 年までに x86 サーバでの処理の大半は仮想マシン内で実行されるようになると予測しています。

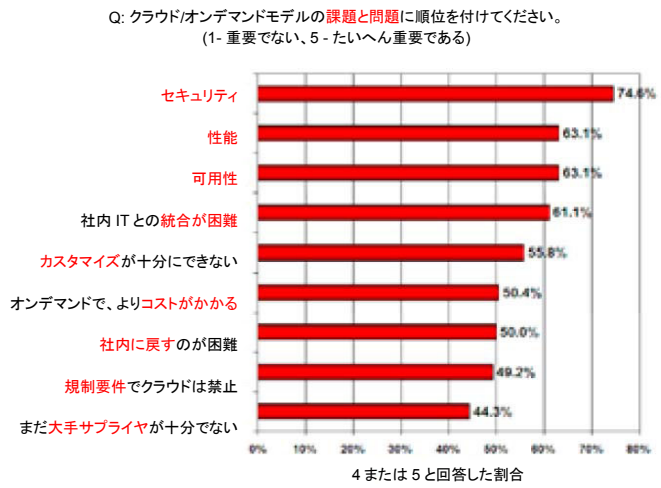
サーバの急速な増加と進展

IT 仮想化の大きなメリットは、組織が幅広い選択肢を得ることです。仮想化によって、社内の要求に合わせてキャパシティと対応力を向上し、ハードウェアおよびソフトウェアライセンスをより効率的に利用してサーバ負荷の統合整理を継続できます。仮想化環境では、ネットワークデバイスとサーバとの間の厳密な区別が小さくなって、仮想化プラットフォーム内で 1 つに結合されます。ただし、ネットワークセキュリティアプライアンスでは仮想マシン間で送信されるトラフィックは認識できないため、機密度の異なる複数の処理をホストすると攻撃を受ける可能性が広がります。モーションツールは、計画的なダウンタイムの管理、仮想化リソースの有効利用、アプリケーションの可用性に不可欠ですが、その結果サーバ上で共有する作業負荷が増え、コンプライアンスの履歴管理と仮想セキュリティアプライアンスに影響を及ぼします。避けられない仮想マシンの「スプロール（増殖）」によって、最新のパッチを適用していないコンピュータが悪意のあるトラフィックに露出される可能性も高まります。IT 担当技術者は、企業サーバの仮想インスタンスを保護する方法について詳しく調査する必要があります。

クラウド内でオープンになるサーバ

クラウドコンピューティングは、日常業務での処理要求に応じる企業の能力を拡張します。ますます多くの組織がクラウドコンピューティングのメリットを活用し、サービスプロバイダがパブリッククラウドを構築するようになると、仮想化された作業負荷を効率的にホストするため、セキュリティモデルにはさらに課題がのしかかります。ビジネスの作業負荷をパブリッククラウドに移すことを組織がためらう最大の理由はセキュリティです。IDC は最近、IT 部門および基幹業務（Line-Of-Business、LOB）部門の担当重役/CIO の 244 人を対象に、IT クラウドサービスの利用についての意見と認識を調査しましたが、クラウドコンピューティングの最大の課題として挙げられたのはセキュリティでした。

サーバをパブリッククラウドリソースに移すと、仮想化されたサーバにインターネットを介して直接管理アクセスするようになるため、データセンターの境界では保護できません。これに伴って、パッチの管理、コンプライアンスレポートなど、データセンターがすでに直面している問題はさらに複雑になります。クラウド内で唯一の意味のある保護は、ベンダーがその境界で実現できる保護、または組織が自身の仮想マシンに装備できる保護の、共通する一部の機能のみになります。これは、その組織の作業負荷が他の組織の作業負荷とともにサーバ上でホストされるためです。



出典: IDC Enterprise Panel、2008 年 8 月 n=244

"クラウドサービスの最大の懸念事項は、間違いなくセキュリティです。ビジネス情報と重要な IT リソースをファイアウォールの外に出すことになるので、顧客は脆弱性を攻撃されることを心配しています。"

—IDC 上級副社長兼チーフアナリスト Frank Gens

II. Trend Micro Deep Securityの概要

Trend Micro Deep Security ソリューションは、サーバとアプリケーションを保護するソフトウェアで、仮想化環境、クラウドコンピューティング環境、従来型のデータセンター環境のすべてに統一したセキュリティを提供します。組織がデータ侵害と業務の混乱を防ぎ、PCI などの重要な規制および標準規格へのコンプライアンスを実現し、現在の厳しい経済状況で運用コストを低減するために役立ちます。Deep Security ソリューションは、システムの自己防衛を可能にして、機密データの保護を支援しアプリケーションの可用性を維持するために最適化されています。Deep Security ソリューションは、次の機能を含む包括的な保護を提供します。

- ディープパケットインスペクションによる侵入検知および防止（IDS/IPS）、Web アプリケーションの保護、アプリケーションの制御
- ステートフルファイアウォール
- ファイルおよびシステムの整合性の監視
- ログの検査

III. 包括的で管理可能なセキュリティ

Deep Security ソリューションは、次のモジュールを使用して、重要なサーバおよびアプリケーション保護の要件にこたえます。

	Deep Security のモジュール					
データセンターの要件	ディープパケットインスペクション			ファイアウォール	整合性の監視	ログの検査
	IDS/IPS	Web アプリケーションの保護	アプリケーション制御			
サーバの保護 – 既知の攻撃およびゼロデイ攻撃からの保護 – パッチが適用できるまで脆弱性に対処	●			●	●	○
Web アプリケーションの保護 – SQL インジェクション、クロスサイトスクリプティング、総当たり攻撃など、インターネットを利用した攻撃からの保護 – PCI DSS 要件 6.5 への対応 ― Web アプリケーションファイアウォール	●	●			○	●
仮想化のセキュリティ – 既知の攻撃およびゼロデイ攻撃からの保護 – パッチが適用できるまで脆弱性に対処 – VMware vCenter 統合による可視性と管理の強化	●	○		●	●	○
疑わしい挙動の検出 – 偵察スキャンからの保護 – 不適切なポートを介する許可されたプロトコルの検出 – 攻撃の可能性のある OS およびアプリケーションエラーの警告 – OS およびアプリケーションの重大な変更の警告	○		●	●	●	●
クラウドコンピューティングのセキュリティ – ファイアウォールポリシーを使用した仮想マシンの分離 – 既知の攻撃およびゼロデイ攻撃からの保護 – パッチが適用できるまで脆弱性に対処	●	○		●	●	●
コンプライアンスレポート – 重要なサーバに対するすべての変更の可視性と監査証跡 – 重要なセキュリティイベントの検査および関連付けと、修復、レポート作成、アーカイブのためのログサーバへの転送 – 検出および防止された設定、アクティビティの報告	○	●	○	○	●	●

● = 必要不可欠 ○ = 重要

IV. メリット

データセンターのサーバセキュリティアーキテクチャは、仮想化と整理統合、新しいサービス配信モデル、クラウドコンピューティングを含む IT アーキテクチャの変化に対応できなくてはなりません。これらすべてのデータセンターモデルで、Deep Security ソリューションは次のように役立ちます。

- データ侵害と業務の混乱を次のように防止
  - サーバ自体で防御線を装備 ― 物理、仮想、クラウドのすべてに対応
  - Web アプリケーションおよび企業アプリケーションとオペレーティングシステムの、既知および未知の脆弱性に対処し、これらのシステムへの攻撃をブロック
  - 疑わしい挙動を識別し、先んじて予防する手段を提供
- コンプライアンスを次のように実現
  - 6 つの主要な PCI コンプライアンス要件（Web アプリケーションセキュリティ、ファイルの整合性の監視、サーバのログ収集を含む）と、その他の幅広いコンプライアンス要件に対応
  - 詳細で監査可能なレポートを作成して、防止した攻撃とポリシーコンプライアンス状態を文書化し、監査を支援するための準備時間を短縮
- 次の方法で運用コストを削減
  - 脆弱性の保護を提供して、安全なコーディングを優先し、費用対効果がより高い方法で予定外のパッチを実装できる
  - 組織に必要なセキュリティを提供して、仮想化またはクラウドコンピューティングを十分に活用し、これらのアプローチによってコスト低減を実現
  - 単一の一元管理されたソフトウェアエージェントで包括的な保護を提供し、複数ソフトウェアクライアントの配備の必要性とこれに伴うコストを削減

V. モジュールおよび機能

Deep Security ソリューションでは、1 つ以上の保護モジュールを配備することで、変化するビジネス要件に合わせて適切な保護のみを導入できます。包括的な保護の配備によって自己防衛型のサーバおよび仮想マシンを作成することも、または疑わしい挙動を検出する整合性監視モジュールの使用から始めることもできます。すべてのモジュールの機能は、サーバまたは仮想マシンに単一の Deep Security Agent として配備されます。このエージェントは、Deep Security Manager ソフトウェアによって一元管理されて、物理環境、仮想化環境、クラウドコンピューティング環境のすべてに対応できるように統一されています。

ディープパケットインスペクション（DPI）エンジン

侵入検知および防止、WEB アプリケーションの保護、アプリケーション制御を実現
このソリューションの高性能ディープパケットインスペクションエンジンは、SSL トラフィックを含むすべての送受信トラフィックを検査して、プロトコルの逸脱、攻撃を示すコンテンツ、ポリシー違反を検出します。検出または防止モードで運用して、オペレーティングシステムおよび企業アプリケーションの脆弱性を保護できます。Web アプリケーションを、SQL

インジェクション、クロスサイトスクリプティングなどの、アプリケーション層の攻撃から保護します。詳細なイベントは、攻撃者、攻撃の発生日時、悪用方法などの有効な情報を提供します。インシデントが発生した場合は、管理者に自動的に警告を通知できます。DPI は、侵入検知および防止、Web アプリケーションの保護、アプリケーションの制御に使用されます。

侵入検知および防止（IDS/IPS）

既知の攻撃およびゼロデイ攻撃からタイムリーに保護し、パッチが適用できるようになるまでオペレーティングシステムおよび企業アプリケーションの脆弱性に対処

脆弱性ルールは、たとえば「Microsoft Tuesday」で公開された既知の脆弱性が、無限に悪用される可能性に対処します。Deep Security ソリューションには、データベース、Web、E-mail、FTP の各サーバなど、100 を超えるアプリケーションにすぐ使用できる脆弱性保護が組み込まれています。新たに発見された脆弱性に対処するルールは、数時間以内に自動的に配信され、数分以内に何千台ものサーバにプッシュできます。また、システムの再起動は不要です。

- スマートルールは、悪意のあるコードを含む異常なプロトコルデータを検出することで、未知の脆弱性を攻撃する未知の悪用に対するゼロデイ保護を提供します。
- 悪用ルールは、既知の攻撃および不正プログラムを防止します。これは、シグネチャを使用して既知の悪用を個々に識別しブロックする、従来のウイルス対策ソフトウェアに似ています。

Microsoft Active Protections Program（MAPP）の発足当初からのメンバとして、Deep Security ソリューションは Microsoft から、月次セキュリティ報告より先に脆弱性情報を受け取ります。そのため、出現したばかりの脅威に先んじて対処し、セキュリティ更新によって効率的かつ効果的に、よりタイムリーな保護を共通の顧客に提供できます。

WEB アプリケーションのセキュリティ

Deep Security ソリューションは、Web アプリケーションとその処理データを保護して、PCI 要件 6.6 へのコンプライアンスを可能にします。Web アプリケーションの保護ルールは、コードによって修正できるようになるまで脆弱性に対処して、SQL インジェクション攻撃、クロスサイトスクリプティング攻撃、その他の Web アプリケーションの脆弱性から保護します。このソリューションはスマートルールを使用して一般的な Web アプリケーション攻撃を識別しブロックします。Deep Security を配備した SaaS データセンターで、顧客のリクエストによって侵入テストを実施したところ、Web アプリケーションおよびサーバで発見された重大性の高い脆弱性の 99%を抑えることができました。

アプリケーションの制御

アプリケーションの制御ルールは、ネットワークにアクセスするアプリケーションの可視性を高め、制御する手段を提供します。このルールは、ネットワークにアクセスする不正ソフトウェアを識別するか、サーバの脆弱性を低減するためにも使用できます。

ファイアウォール

物理および仮想サーバの攻撃面の縮小

Deep Security ファイアウォールソフトウェアモジュールは、企業レベルの、双方向でステートフルなファイアウォールです。適正なサーバ運用に必要なポートおよびプロトコルを介した通信を可能にし、それ以外のポートおよびプロトコルはすべてブロックすることで、サーバへの不正アクセスのリスクを低減します。主な機能は次のとおりです。

- 仮想マシンの分離: クラウドコンピューティングつまりマルチテナントの仮想化環境で仮想マシンを分離できるようにして、仮想スイッチ構成を変更することなく仮想セグメント化を実現します。
- 粒度の高いフィルタリング: IP アドレス、MAC アドレス、ポート、その他に基づいてファイアウォールルールを設定し、トラフィックをフィルタリングします。ネットワークインタフェースごとに異なるポリシーを設定できます。
- IP ベースのプロトコルへの対応: フルパケットキャプチャをサポートして、トラブルシューティングを簡単にし、発生した TCP、UDP、ICMP などのファイアウォールイベントを理解するために役立つ詳細情報を提供します。
- 偵察の検出: ポートのスキャンなどのアクティビティを検出します。ARP トラフィックなど、IP 以外のトラフィックを制限することもできます。
- 柔軟な制御: ステートフルファイアウォールは柔軟で、必要な場合は、規定に従って検査をバイパスすることもできます。通常の状況でまたは攻撃の一部として、任意のネットワーク上で見つかることのある、あいまいなトラフィック特性に対処します。
- 事前定義されたファイアウォールプロファイル: Web、LDAP、DHCP、FTP、データベースなど、共通の企業サーバタイプをグループ化して、大規模で複雑なネットワークでもファイアウォールポリシーの迅速で、容易な、一貫性のある配備を確実に実現します。
- 操作可能なレポート: 詳細なログ、警告、ダッシュボード、柔軟なレポート作成機能を備えた Deep Security ファイアウォールソフトウェアモジュールは、誰がどのようにポリシーを変更したかなどを示す設定変更を取得し追跡して、詳細な監査証跡を提供します。

整合性の監視

不正な、予期しない、または疑わしい変更の監視

Deep Security の整合性の開始ソフトウェアモジュールは、ディレクトリ、レジストリキーおよび値など、オペレーティングシステムとアプリケーションの重要なファイルを監視して、疑わしい挙動を検出します。主な機能は次のとおりです。

- オンデマンドのまたはスケジュールを設定した検出: 整合性の検索は、スケジュールを設定するか、必要に応じて実行できます。
- 広範なファイルプロパティのチェック: 事前設定済みの整合性ルールを使用して、ファイルとディレクトリの内容、属性（所有者、アクセス権、サイズなど）、日付と時刻のタイムスタンプの変更を監視できます。Windows レジストリキーおよび値、アクセス制御リスト、ログファイルの追加、変更、削除も監視して警告できます。この機能は PCI DSS の 10.5.5 要件に適用できます。

- 監査可能なレポート: 整合性の監視モジュールは、Deep Security Manager のダッシュボードに整合性イベントを表示し、警告を生成し、監査可能なレポートを作成できます。Syslog を使用して、イベントをセキュリティ情報およびイベント管理(SIEM)システムに転送することもできます。
- セキュリティプロファイルのグループ化: 整合性の監視ルールは、グループまたは個々のサーバに対して設定できるため、監視ルールセットの配備と管理が簡単になります。
- 基準の設定: 基準となるセキュリティプロファイルを確立して、変更の比較、警告の発信、適切な処置の決定に使用できます。
- 柔軟で現実的な監視: 整合性の監視モジュールは、ユーザ固有の環境に合わせて監視アクティビティを最適化できる柔軟性と制御を提供します。これには、検索パラメータでのファイルの包含/除外の指定、ファイル名のワイルドカード指定、サブディレクトリの包含/除外の指定などがあります。また、独自の要件に合わせてカスタムルールを作成できる柔軟性もあります。

ログ検査

ログファイルに埋もれた重要なセキュリティイベントの検出と分析

Deep Security のログ検査ソフトウェアモジュールは、オペレーティングシステムおよびアプリケーションのログからセキュリティイベントを収集して分析する機能を提供します。ログ検査ルールは、複数のログエントリに埋もれた重要なセキュリティイベントの識別を最適化します。これらのイベントは SIEM システムまたは一元化されたログサーバに転送して、関連付け、レポートを作成して、アーカイブできます。Deep Security Agent も、イベント情報を Deep Security Manager に転送します。ログ検査モジュールには次のようなメリットがあります。

- 疑わしい挙動の検出: 使用するサーバ上で発生した可能性のある疑わしい挙動を確認できます。
- 環境全体のイベントの収集: Deep Security ログ検査モジュールは、Microsoft Windows、Linux、Solaris の各プラットフォーム全体のイベントと、Web サーバ、メールサーバ、SSHD、Samba、Microsoft FTP などからのアプリケーションイベント、またカスタムアプリケーションログイベントを収集して関連付けることができます。
- 異なるイベントの関連付け: 様々な警告、エラー、情報イベントを収集して関連付けます。これには、システムメッセージ(ディスク空き容量なし、通信エラー、サービスイベント、シャットダウン、システム更新など)、アプリケーションイベント(アカウントのログイン/ログアウト/失敗/ロックアウト、アプリケーションエラー、通信エラーなど)、管理操作(管理者のログイン/ログアウト/失敗/ロックアウト、ポリシー変更、アカウント変更など)が含まれます。
- コンプライアンスのための監査可能なレポート: すべてのセキュリティイベントの監査証跡を生成して、PCI 10.6 などのコンプライアンス要件への準拠を支援します。

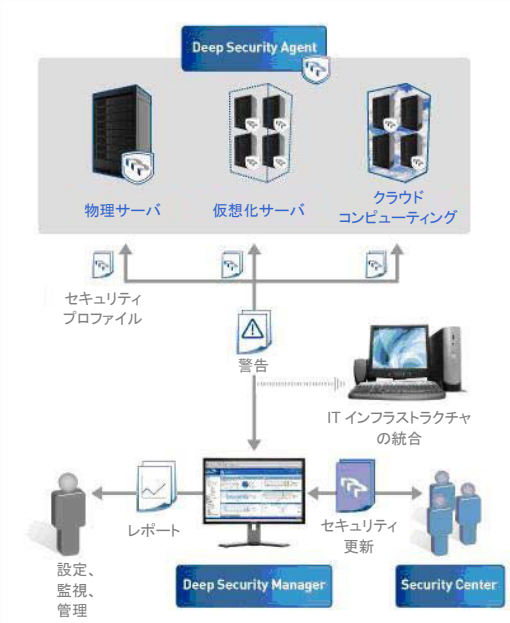
VI. Deep Securityソリューションのアーキテクチャ

Deep Security ソリューションアーキテクチャは、次の 3 つのコンポーネントで構成されます。

- Deep Security Agent は、保護対象のサーバまたは仮想マシン上に配備されます。
- Deep Security Manager は、ポリシー管理の一元化、セキュリティ更新の配信、警告およびレポートによる監視を実行します。
- Security Center は、専門の脆弱性調査チームが出現した脅威に対応するルールの更新を開発するホステッドポータルです。更新は、Deep Security Manager によって定期的にプルされます。

処理の流れ

Deep Security Agent は、Deep Security Manager からセキュリティ設定を受信します。これは、通常はセキュリティプロファイルです。このセキュリティ設定には、サーバ上で実施される、ディープパケットインスペクション、ファイアウォール、整合性の監視、ログ検査の各ルールが含まれています。サーバに割り当てるルールは、推奨検索を実行することで容易に決定できます。推奨検索とは、サーバにインストールされたソフトウェアを検索して、そのサーバの保護に必要なルールを推奨する機能です。すべてのルール監視アクティビティについてイベントが作成され、これらのイベントは Deep Security Manager と、指定によって SIEM システムに送信されます。Deep Security Agent と Deep Security Manager との間のすべての通信は、SSL の相互認証によって保護されます。



Deep Security Manager は Security Center へのポーリングを実行して、新しいセキュリティ更新を使用できるかどうかを確認します。新しい更新を使用できる場合、Deep Security Manager は更新を取得し、そのアップデートによる保護の追加を必要とするサーバに手動または自動で適用できます。Deep Security Manager と Security Center との間の通信も、SSL の相互認証によって保護されます。Deep Security Manager は、管理を容易にするために、IT インフラストラクチャの他の要素にも接続します。Deep Security Manager は、VMware vCenter と、Microsoft Active Directory などのディレクトリに接続して、サーバ設定とグループ化情報を取得できます。Deep Security Manager には Web サービス API もあります。この API は、プログラムによってアクセスするために使用できます。

Security Center は、ユーザが使用するオペレーティングシステムとアプリケーションを保護するため、パブリックとプライベートの両方の脆弱性情報元を監視します。

Deep Security Manager

Deep Security ソリューションは、困難なセキュリティ問題に対処する、現実的で実証された制御を提供します。操作とアクションが可能なセキュリティ機能で、単なる情報ではなく、セキュリティイベントについての知識を組織に提供します。多くの場合、これは「誰が、何を、いつ、どこで」行ったかを示すので、正しくイベントを理解して、セキュリティ制御機能自体が実行した対処以上の、その後の対処を実行できます。Deep Security Manager ソフトウェアは、次のような機能で、セキュリティ要件と運用上の要件に対処します。

- 一元化された Web ベースの管理システム: 使い慣れたエクスプローラ形式の UI でセキュリティポリシーを作成および管理し、脅威とそれに対応する防止操作を追跡できます。
- 詳細なレポート: 試みられた攻撃に関する様々な詳細レポートを、セキュリティ設定および変更の監査可能な履歴として使用できます。
- 推奨検索: サーバおよび仮想化マシン上で動作するアプリケーションを識別して、そのシステムに適用すべきフィルタを推奨して、最小限の労力で適切な保護を実現できるようにします。
- リスクのランキング: セキュリティイベントは、脆弱性情報によって分類するだけでなく、資産の価値に基づいて参照することもできます。
- ロールベースのアクセス: 複数の管理者を設定して、それぞれ異なるレベルの権限を付与し、システムの異なる側面を操作して対応する情報を受信できます。
- カスタマイズ可能なダッシュボード: 管理者は特定の情報にナビゲートしてドリルダウンし、脅威を監視して防止措置をとることができます。個々にカスタマイズしたビューを複数作成し保存できます。
- スケジュールされたタスク: レポート、更新、バックアップ、ディレクトリの同期化など、日常的な作業をスケジュール設定して自動実行できます。

Deep Security Agent

Deep Security Agent は、Deep Security ソリューションのサーバベースのソフトウェアコンポーネントで、IDS/IPS、Web アプリケーションの保護、アプリケーション制御、ファイアウォール、整合性の監視、ログ検査を可能にします。送受信トラフィックでのプロトコルの逸脱、攻撃を示すコンテンツ、ポリシー違反を監視することでサーバまたは仮想マシンを保護します。必要に応じて、Deep Security Agent は悪質なトラフィックをブロックして、脅威に介入し無効化します。

Security Center

Security Center は、Deep Security ソリューションの必要不可欠なコンポーネントです。これはセキュリティ専門家による動的なチームで、ユーザが最新の脅威に先んじることができるように、発見された様々な新しい脆弱性や脅威にタイムリーかつ迅速に対応し、カスタマポータルと連携してセキュリティ更新と情報を提供します。Security Center の専門家は、高度な自動ツールを利用して、次に示す厳密な 6 つの手順で迅速な対応プロセスを実施します。

- 監視: 100 を超える情報源のパブリックデータ、プライベートデータ、政府データを系統的かつ継続的に監視し、新種の脅威と脆弱性を識別して関連付けます。Security Center の専門家は、タイムリーで正確な保護をユーザに配信するため、他の組織との協力関係を利用して脆弱性に関する情報を早期に、時にはリリース前に入手します。情報源は、Microsoft、Oracle などのベンダーの諮問機関、SANS、CERT、Bugtraq、VulnWatch、PacketStorm、Securiteam などです。

- 優先順位付け: ユーザへのリスクの評価とサービスレベルアグリーメントに基づいて脆弱性に優先順位を付け、さらに詳細に分析できるようにします。
- 分析: 脆弱性の徹底的な分析を実施して、必要な保護を特定します。
- 開発およびテスト: 脆弱性に対処するソフトウェアフィルタと、フィルタを推奨するルールを開発し、誤検出を最小するために幅広いテストを実施して、ユーザが迅速かつスムースに配信できることを確認します。
- 配信: 新しいフィルタをセキュリティ更新としてユーザに配信します。新しいセキュリティ更新がリリースされると、ユーザは Deep Security Manager の警告によってただちに通知を受け取ります。フィルタは、自動または手動で適切なサーバに適用できます。
- 連絡: 新たに発見されたセキュリティの脆弱性について説明するセキュリティアドバイザリによって、ユーザへの連絡を継続的に維持します。

保護を強化する予防的な調査

Security Center チームではさらに、全体的な保護メカニズムを向上させるための継続的な調査を実施しています。この作業は、脆弱性と脅威に対応する中で見つかった結果や傾向によって強く影響されます。こうした結果は、新しいフィルタおよびルールの作成方法と、既存の保護メカニズムの質にも影響を与え、最終的には全体的な保護を向上させます。

幅広い脆弱性の保護

Security Center は、既製のアプリケーションとカスタマイズした Web アプリケーションの両方を保護するフィルタを開発し配信します。悪用と脆弱性のフィルタは受動的で、発見された既知の脆弱性への対応策として使用されます。これに対して、スマートフィルタは予防的な保護を提供します。整合性の監視フィルタは、様々なシステムコンポーネントとその固有のプロパティをチェックし、特定のトリガー条件に合致した場合には管理者に警告します。一部のコンポーネントでは、システムディレクトリ、ファイル、Windows レジストリ、ユーザアカウント、ポート、ネットワーク共有なども監視できます。ログ検査フィルタは、オペレーティングシステムおよびサードパーティ製アプリケーションのログを解析して、特定のイベントが発生していれば管理者に警告します。

Security Center ポータル

Security Center ポータルは、次のような製品関連情報とサポートにアクセスできる、単一で安全なポイントをユーザに提供します。

- セキュリティ更新
- セキュリティアドバイザリ
- 脆弱性の CVSS スコア情報
- Microsoft Tuesday の警告の概要
- 脆弱性の詳細検索
- Third Brigade が保護しないものも含む、脆弱性のすべての公開情報
- 各脆弱性のパッチ情報

- RSS フィード
- トラブルチケット
- ソフトウェアダウンロード
- 製品に関するドキュメント

VII. 配備と統合

Deep Security ソリューションは、企業で迅速に配備できるように設計されています。既存のインフラストラクチャと設備を利用して統合し、優れた運用効率の実現を支援し、運用コストの削減をサポートします。

- VMware の統合: VMware の vCenter および ESX Server との緊密な統合によって、vCenter および ESX のノードから Deep Security Manager に組織および運用に関する情報をインポートし、企業の VMware インフラストラクチャに詳細なセキュリティを適用します。
- SIEM の統合: 詳細なサーバレベルのセキュリティイベントが、ArcSight、Intellitactics、NetIQ、RSA Envision、Q1Labs、LogLogic などの、SIEM の複数の統合オプションによって提供されます。
- ディレクトリの統合: Microsoft Active Directory など、企業内のディレクトリと統合します。.
- 設定可能な管理通信: Deep Security Manager または Deep Security Agent から通信を開始できます。これによって、一元管理されるシステムで通常必要になるファイアウォールの変更を、最小限にするか完全になくすことができます。
- ソフトウェアの配信: エージェントソフトウェアは、Microsoft SMS、Novell Zenworks、Altiris などの標準的なソフトウェア配信メカニズムによって容易に配信できます。
- フィルタリングの最適化: インターネットプロトコルテレビ（IPTV）などのストリーミングメディアの高度な取り扱いにより性能を最大化します。

VIII. Deep Securityの他製品との違い

トレンドマイクロのサーバおよびアプリケーション保護機能は、今日の動的なデータセンターに伴うセキュリティ課題とコンプライアンスの必要性に対処します。包括的な保護、運用効率の向上、優れたプラットフォームサポート、既存システムとの緊密な統合を実現し、ユーザの要求により迅速に対応できます。Deep Security ソリューションでは、次の機能を利用できます。

- より深い保護: ステートフルファイアウォール、侵入検知および防止、アプリケーション層のファイアウォール保護、ファイルおよびシステムの整合性の監視、ログ検査を単一のソリューションにまとめています。
- 運用効率の向上: 迅速で幅広い配備と、各サーバに適用する適切な保護の推奨などの多くの主要作業の自動化によって、ソリューションをより効率的に管理して、既存の IT リソースへの影響を最小限に抑えます。
- 優れたプラットフォームサポート: より多くのプラットフォームですべての機能を利用できるようにし、プラットフォームの最新バージョンをより迅速にサポートするため、保護を犠牲にすることなく、最新の仮想化プラットフォームおよびオペレーティングシステムリリースを継続的に導入できます。

- 緊密な統合: ディレクトリ、仮想化プラットフォームなどの IT インフラストラクチャとの、また SIEM などその他のベストオブブリードのセキュリティ機能との緊密な統合により、企業での効率的な配備とベンダー選択の柔軟性を継続的に支援します。

詳細は、次の Web サイトをご覧いただくか、電話でお問い合わせください。
www.trendmicro.com/go/enterprise
+1-877-21-TREND