McAfee Host Intrusion Prevention for Server

サーバーとアプリケーションを保護する高度な脆弱性対策

企業のサーバーには、事業の継続に必要な最も重要な情報資産が保存されています。これらのサーバーとアプリケーションを保護し、ビジネスの妨げになる既知の脅威と未知の攻撃を阻止することは、IT部門にとって重要な課題の一つです。

主な特長

強固なセキュリティ

- ネットワーク、アプリケーション、実行など、すべてのレベルにIPSとゼロデイ脅威対策を実施。

コストの削減

- 強力な統合コンソールでイベント、ポリシー、エージェントを管理。配備、管理、レポート、監査にかかる時間を短縮し、コストを削減。
- エンドポイントに対するパッチの適用回数を削減。緊急性の高いパッチも減少。

コンプライアンス対応の負荷を軽減

- 簡単で使いやすいビュー、ワークフロー、イベント モニタリング、レポート機能を搭載。適切な調査とフォレンジックが可能。

McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention for Serverは、Webサーバーとデータベース サーバーに特化した保護機能と業界で唯一の動的なステートフル ファイアウォールにより、高度な脅威と不正なトラフィックを阻止し、システムの稼動時間とビジネスの継続性を維持します。また、シグネチャと動作分析による侵入検知システム（IPS）も提供します。McAfee Host Intrusion Prevention for Serverでは、パッチの適用回数だけでなく緊急性の高いパッチの適用回数も少なくなるので、ビジネスの継続性と従業員の生産性を維持できます。また、データの機密性を保護し、コンプライアンスを強化できます。

攻撃や情報漏えいからサーバーとアプリケーションを保護

企業のサーバーには日々の業務に必要な大量のデータが保存されています。このようなデータを狙った攻撃が増加しています。McAfee Host Intrusion Prevention for Serverは、基幹業務で使用されているサーバーを保護し、システムの稼働時間と生産性を維持します。

- Webサーバーの保護:
  - HTTP要求をフィルタリングし、ディレクトリ トラバーサル、Unicode、サービス拒否（DoS）攻撃を阻止します。
  - 事前定義の保護ポリシーとルールにより、攻撃と情報漏えいを防ぎます。
- データベース サーバーの保護:
  - データベース クエリーを検査し、SQLインジェクションなどの攻撃を阻止します。
  - 事前定義の保護ポリシーとルールにより、異常な動作を排除し、データの改ざんを防ぎます。

動的でステートフルなシステム ファイアウォールで高度な脅威を阻止

ルールのみを使用する従来のシステム ファイアウォールと異なり、McAfee Host Intrusion Prevention for Serverは、McAfee Global Threat Intelligence（McAfee GTI）から接続のレピュテーションをリアルタイムで取得し、攻撃が発生する前に不正なトラフィックをブロックして、ボットネット、分散型サービス拒否（DDoS）などの高度な攻撃からサーバーを保護します。McAfee GTIにより、増加を続ける高度な脅威に対しても最も洗練されたセキュリティが実現されます。

OS、アプリケーションに対する緊急パッチの適用回数が減少

大半のエクスプロイトは、脆弱性が開示されてから3日以内に出現しています。しかし、多くの企業では、パッチのテストからエンドポイントへの適用が完了するまでに30日ほど費やしています。

システム要件

ハードウェア最小要件

- IntelまたはAMD x86/x64
- ディスクの空き容量（クライアント）: 15 MB。インストール時は100 MBが必要
- メモリ: 256 MB以上のRAM
- ネットワーク環境: MicrosoftまたはNovell NetWareネットワーク。NetWareネットワークの場合にはTCP/IPが必要。
- NIC: ネットワーク インターフェース カード、10Mb以上

対応OS

- Microsoft Windows Server 2003 SP2、2003 R2、2003 R2 SP2（すべてのエディション、32ビット/64ビット）
- Microsoft Windows Server 2008、2008 SP1、2008 SP2、2008 R2（すべてのエディション、32ビット/64ビット）
- SPARC Solaris 9 sun4u（32ビット/64ビット）
- SPARC Solaris 10 sun4u、sun4v（32ビット/64ビット）
- Red Hat Linux Enterprise 4（32ビット）
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4（64ビット）
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5（32ビット）
  - 2.6.18-8.el5
  - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5（64ビット）
  - 2.6.18-8.el5
- SUSE Linux Enterprise 10（32ビット）
  - 2.6.16.21-0.8-bigsmp
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp

McAfee Host Intrusion Prevention for Serverを使用すると、パッチをより簡単かつ効率的に適用し、セキュリティ ギャップを解消できます。

- MicrosoftとAdobeの両方の脆弱性に対応しています。シグネチャを自動的に更新し、脆弱性を悪用する攻撃からエンドポイントを保護します。
- シグネチャの更新は自動的に実行され、定期的にダウンロードされます。これにより、保護状態が維持されます。

スタートアップから保護

サーバーの起動直後は無防備な状態です。スタートアップ後すぐにセキュリティ ポリシーが有効になるわけではありません。ポリシーが施行されるまでは、ネットワーク ベースの攻撃を受けたり、セキュリティ サービスが無効にされる可能性があります。McAfee Host Intrusion Prevention for ServerはIPSでシステム起動時から攻撃を阻止します。

- スタートアップ時は、ファイアウォール ポリシーが完全に施行されるまで送信トラフィック以外は許可しません。
- IPSポリシーが完全に施行されるまで、弊社のセキュリティ サービスが無効にされないように保護します。

簡単な管理作業

大規模な組織では、複数のファイアウォール ポリシーと侵入検知システム（IPS）ポリシーを作成し、管理しなければなりません。しかし、これは多くの時間と労力を要する作業です。McAfee Host Intrusion Prevention for ServerのポリシーとIPSカタログを使用すると、管理作業を簡単に行うことができます。複数のファイアウォール ポリシーとIPSポリシーを作成し、必要に応じて適用できます。

McAfee® ePolicy Orchestrator®（McAfee ePO™）の集中管理コンソールにより、組織全体の保護状況をすばやく把握し、最適な保護状態を維持することができます。McAfee ePOと完全に統合されているので、管理コストを削減し、運用効率を大幅に改善できます。

詳細については、弊社営業担当までお問い合わせいただくか、以下のWebサイトをご覧ください。
www.mcafee.com/jp

対応OS（続き）

- SUSE Linux Enterprise 10（64ビット）
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11（32ビット）
  - 2.6.27.19-5-default
  - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11（64ビット）
  - 2.6.27.19-5-default

対応Webサーバー

- Microsoft Windows
  - IIS 6.0、7.0
- SPARC Solaris
  - Apache 1.3.6以降のWebサーバー
  - Apache 2.0.42以降のWebサーバー
  - Apache 2.2.3以降のWebサーバー
  - Sun Java Web Server 6.1
  - Sun Java Web Server 7.0
- Linux（RHEL、SUSE）
  - Apache 1.3.6以降のWebサーバー
  - Apache 2.0.42以降のWebサーバー
  - Apache 2.2.3以降のWebサーバー

対応データベース サーバー

- Microsoft SQL Server 2005、2008

主な仮想化プラットフォームとの互換性

多くのIT部門が仮想化を導入しています。製品を正常に動作させるには、仮想化プラットフォームとの互換性が問題になります。McAfee Host Intrusion Prevention for Server 8.0は、VMware、Citrix、Microsoft Hyper-Vの主要な仮想化プラットフォームに対応しています。対応製品は次のとおりです。

VMware	Citrix	Microsoft
VMware ESX 3.5、4.0	Citrix XenServer 5.0、5.5	Microsoft Hyper-V Server 2008/2008 R2
VMware Vsphere 4.0	Citrix XenDesktop 3.0、4.0	Microsoft VDI
VMware View 3.1、4.0	Citrix XenApp 5.0、6.0	Microsoft App-V 4.5、4.6
VMware ThinApp 4.0、4.5		Windows 7のXPモード
VMware ThinApp 4.0、2.6		
VMware Workstation 6.5、7.0		
VMware Player 2.5、3.0		

McAfee. Part of Intel Security.
マカフィー株式会社
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ェスト 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

17802ds_hips-server_1110B