データシート

McAfee Enterprise Log Manager

ログの収集、保存、管理を自動化してコンプライアンス コストを削減

ログを適切に収集して保存すると、アクティビティに関して疑いの余地がない明確な監査証跡を残し、コンプライアンス コストを削減できます。McAfee® Enterprise Log Managerを使用すると、ログ ファイルを効率よく収集して圧縮し、保存することができます。McAfee Enterprise Security Managerとの統合により、高度な検索、分析、相関、アラート、レポート機能を使用できます。イベントやアラートを1回クリックするだけで元のログ レコードにアクセスできるので、フォレンジックを効率よく実行できます。

主な特長

- ログ収集と保存機能でコンプライアンス要件を遵守
- ログ ソースごとにストレージと保存期間を柔軟に設定
- 証拠保管の連続性とフォレンジックをサポート
- ログの分析と検索
- ローカルまたはSANへのログの保存
- McAfee Enterprise Security Managerと完全に統合
- 物理アプライアンスと仮想アプライアンスに対応した柔軟でハイブリッドな配備オプション

McAfee Enterprise Log Managerは、ログ ファイルを収集し、署名して保存します。Microsoft Windows イベント ログ、データベース ログ、アプリケーション ログ、Syslogなど、様々なログの管理と分析を自動的に行います。正当性と整合性を維持するため、ログに署名を行い、検証します。これはコンプライアンス対応で必要な機能です。すぐに使えるコンプライアンス ルールとレポートが用意されているので、コンプライアンス対応やポリシー施行を簡単に行うことができます。

この統合されたログ収集/管理/分析環境では、セキュリティを強化するだけでなく、PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA、SOXなどの法規制へのコンプライアンスを改善できます。

インテリジェントなログ管理

McAfee Enterprise Log Manager はログを自動的に収集し、コンプライアンス対応に使用するログを保存します。また、セキュリティを強化するため、ログの解析と分析を行います。コンプライアンスで特別な理由がある場合には、ログを元の形式で保管することもできます。元のログ ファイルは変更されないので、証拠保管の連続性が維持されます。

情報の保存期間はログ ソースやコンプライアンス要件によって異なります。McAfee Enterprise Log Managerでは、適切な量のログが正確に記録されるように、ストレージ プールをカスタマイズできます。アプライアンスのハードディスクに最適なストレージ オプションを選択できます。また、光チャネル ケーブルで高速のSANストレージに接続することも可能です。

ログ ファイルだけで必要な情報が得られるわけではありません。ログには重要なエビデンスの断片が記録されているので証拠保管の連続性には不可欠ですが、セキュリティ管理の点では問題があります。たとえば、アクセス ログにはユーザー情報が記録されていますが、ユーザーの役割や権限に関する情報はありません。アクセスされたシステムは確認できますが、そのシステムで使用された情報の種類や、アクセスした人物は特定できない場合があります。

intel Security

McAfee Enterprise Security Managerとの統合

McAfee Enterprise Log Managerは、McAfee Enterprise Security Managerのオプション コンポーネントです。McAfee Enterprise Security Managerは、McAfee Enterprise Log Managerが収集したログの解析と正規化を行い、セキュリティ調査やインシデント対応で使用できるように結果をリアルタイムで提供します。

セキュリティ イベントが生成されると、解析されるイベント ファイルが元のログ ファイルや特定のログ レコードと関連付けられます。イベント管理やフォレンジック プロセスの実行中にワンクリックでアクセスできます。複雑な手順はありません。別のアプリケーションを起動する必要もありません。ログを手動で検索する必要がないので、余分な時間もかかりません。

豊富なコンテキスト情報を使用した分析

McAfee Enterprise Security ManagerとMcAfee Enterprise Log Managerは、ログに関するコンテキスト情報を提供します。ログ レコードから貴重な情報を得ることができます。次の情報を利用できます。

- 送信元または送信先のIPアドレス
- IDのコンテキスト
- 使用されたホスト名またはサービス
- 脆弱性評価スキャナーから取得した脆弱性情報
- ネットワーク トポロジ情報
- ポリシーとプライバシー情報

柔軟なストレージ プール

McAfee Enterprise Log Managerのストレージ プールでは、ログの保存方法と保存期間を柔軟に選択できます。ストレージ プールは使用可能なストレージの仮想グループです。要件に合わせて様々な物理ストレージ デバイス（ローカル ストレージ、NFS、SAN、CIFなど）にログを分散し、管理できます。

図 1. ログの保存期間を設定できる柔軟なストレージ プール

ストレージ プールを複数のデバイスから構成し、ソース デバイスに基づいて特定のプールにデータを割り当てることができます。セキュリティ、コンプライアンス、機密性などの要件を考慮して、ログの保管場所を決めることができます。たとえば、コンプライアンスに重要なログを複数のネットワーク ストレージ デバイスから構成されたプールに保存します。重要度の低いログは、冗長性の低いシステムに保管し、フォレンジックに役立つログはローカルに保存してすぐに分析できるようにします。

迅速な配備

McAfee Enterprise Log ManagerとMcAfee Enterprise Security Managerは単一のアプライアンスに配備できます。また、大規模な企業ネットワークで使用する場合には、これらの機能を分散させることもできます。柔軟でハイブリッドな配備オプションにより、物理アプライアンスや仮想アプライアンスに配備できます。

インフラへの統合

大半のログ管理ソリューションは単独で実行されていますが、McAfee Enterprise Log Managerは他の情報セキュリティ システムと一緒に使用できます。McAfee Enterprise Security Managerを介して残りのセキュリティ インフラと統合されるので、セキュリティ管理作業が簡素化され、全体の効率が向上し、コストを削減できます。インテリジェントなログ管理を強力な分析、ネットワーク調査、データベース イベント モニタリングなどの機能と統合できます。

詳細については、**mcafee.com/siem**をご覧ください。

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 13 階 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