McAfee Application Data Monitor

アプリケーション レイヤーに潜む脅威を検出。

McAfee® Application Data Monitorアプライアンスセキュリティおよびコンプライアンスは、あらゆる手段でアプリケーションレイヤーをモニタリングし、ログ管理の限界を超えます。アプリケーションコンテンツを詳しく調査し、最深部までネットワークの使用状況を把握できるようにします。

McAfee Application Data Monitorアプライアンスは、全体のアプリケーションのセッションをレイヤー7にデコードし、基底部のプロトコルから詳細に分析し、アプリケーション自体（電子メールや添付ファイルなどのテキスト）のコンテンツに整合性を持たせます。これにより、アプリケーションの実際の使用状況を正確に分析し、アプリケーション使用ポリシーを施行して不正なトラフィックや不審なトラフィックを検出します。

この詳細な調査は、ネットワークの機密データのすべての使用を追跡して、コンプライアンスをサポートします。McAfee Application Data Monitorアプライアンスは違反を検出すると、コンプライアンス監査要件として、インシデントの回答、フォレンジックのためにそのアプリケーションの詳細をすべて保存します。

同時に、McAfee Application Data Monitorアプライアンスは、合法的なアプリケーションとして仮の脅威に可視性を提供します。

- 高度なアプリケーション レイヤーの脅威
- 未承認の利用または機密データの盗難
- 「ブラインドスポット」上、または「ブラインドスポット」からのセキュリティ攻撃
- 危険なレガシーコードの使用
- ユーザー認証情報の盗難または不正使用
- アプリケーションを介した機密データの送信
- 壊れたビジネスプロセス

データ漏えいおよびコンプライアンス違反

McAfee Application Data Monitor アプライアンスは、電子メールの添付、インスタント メッセージ、ファイル転送、HTTP 送信、その他のアプリケーションで送信される機密情報を検出すると、ユーザーにすぐに通知し、外部への流出を防ぎます。

主な特長

- アプリケーション セッション全体をレイヤー 7 にデコードします。何百ものアプリケーションとプロトコルに対応しています
- 事前定義の検出ルールで規制対象のデータや機密データを検出して提供
- カスタマイズのためのユーザー定義辞書とルールをサポート
- コンプライアンスにアプリケーション イベントの完全な監査証跡を作成
- 受動的なアプリケーションインターフェースの回避操作
- イベントおよびその他のデータフィードをアプリケーションコンテンツとの相関のできるMcAfee Enterprise Security Managerと統合
- 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

クレジットカード情報、社会保障番号などの機密データを検出します。重要情報や機密情報について独自のディクショナリを定義すると、McAfee Application Data Monitor アプライアンスの検出機能をカスタマイズできます。McAfee Application Data Monitorアプライアンスは、機密性の高いデータを検出し、個人に適切なアラートを通知し、犯罪を記録し、監査の追跡を維持します。

文書の検出

McAfee Application Data Monitorアプライアンスは、電子メール、チャット、P2P、ファイルの共有、その他の手段でネットワークを交換する際に500種類以上の文書を検出します。McAfee Application Data Monitorアプライアンスは、文書がメールゲートウェイ、侵入検出システム（IDS）または侵入防御システム（IPS）デバイスにバイパスする偽装文書ーなどの拡張に関係なく文書を検出します。文書がアーカイブのように他の文書の内部に埋め込まれたり、圧縮されていても、エンコードされた文書は、ファイル名や作業などの実用的なメトリックスで検出されます。

アプリケーション レイヤーの脅威

最近、共通システムのビジネスアプリケーションではネットワークに侵入して重要情報を盗み出すため、脆弱性を悪用する巧妙な脅威が発生しています。従来のファイアウォールやIDS/IPSでは、このようなアプリケーション レイヤーの脅威を簡単に検出できません。McAfee Application Data Monitorアプライアンスでは、アプリケーションのすべてのコンテンツ（プロトコルを含む）を検索し、トラフィックに潜むペイロードやマルウェア、PDF内部に隠された通信チャネルも検出します。

プロトコルの異常

異常は、差し迫った脅威をプロアクティブに識別し、リスクを減らし、損失を最小限にします。従来のセキュリティソリューションは、ネットワーク分析に限定されていたので、McAfee Application Data Monitorアプライアンスは、このアプローチを次のレベルへと進めます。アプリケーションやプロトコル内の異常を検出するために、過去のネットワークの動作を調査し、さらに強力で、プロアクティブなリスクの検出方法を提供しています。

干渉のないアプリケーション

McAfee Application Data Monitorアプライアンスは、SPANポート上で操作するので、アプリケーションの性能、信頼性、待機時間などを干渉しません。

インフラへの統合

大半のネットワーク モニターソリューションは単独で実行されていますが、McAfee Application Data Monitorアプライアンス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。損失と詐欺の検出を強力な分析、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。

ユースケースの利用例

McAfee Application Data Monitorアプライアンスは、さまざまな未承認のアクティビティ、ポリシー違反、盗難や詐欺を検出できます。いくつかの例を示します。

500以上サポートされたアプリケーションとプロトコル

- **低レベルネットワークプロトコル:** TCP/IP、UDP、RTP、RPC、SOCKS、DNS およびその他
- **電子メール:** MAPI、NNTP、POP3、SMTP、Microsoft Exchange
- **Webメール:** AOL Webmail、Hotmail、Yahoo! Mail、Gmail、Facebook、およびMySpace 電子メール
- **インスタント メッセンジャー:** AOL、ICQ、Jabber、MSN、SIP およびYahoo
- **ファイル転送プロトコル:** FTP、HTTP、SMB、および SSL
- **圧縮と抽出プロトコル:** BASE64、GZIP、MIME、TAR、ZIP、その他
- **アーカイブファイル:** RAR アーカイブ、ZIP、BZIP、GZIP、Bin-hex、Uu エンコードアーカイブ
- **インストールパッケージ:** Linux パッケージ、InstallShield キャビネット、Microsoft キャビネット
- **画像ファイル:** GIF、JPEG、PNG、TIFF、AutoCAD、Photoshop、ビットマップ、Visio、Digital RAW、およびWindowsアイコン
- **オーディオ ファイル:** WAV、MIDI、RealAudio、Dolby Digital AC-3、MP3、MP4、MOD、RealAudio、SHOUTCastなど
- **ビデオ ファイル:** AVI、Flash、QuickTime、Real Media、MPEG-4、Vivo、Digital Video (DV)、Motion JPEGなど
- **その他のアプリケーションとファイル:** データベース、スプレッドシート、ファクス、web アプリケーション、フォント、実行可能ファイル、Microsoft Officeアプリケーション、ゲーム、およびソフトウェア開発ツール
- **その他のプロトコル:** ネットワークプリンター、シェルアクセス、VoIP、ピアツーピア

機密性の高い盗難情報

tyamada@company.comでログインした従業員が電子メールをnakama@gmail.comに送信しました。電子メールには、「秘密の数式」という言葉を含むshoo.docというファイルが添付されています。その電子メールは、午後12時20分にホストのデスクトップ 0232 (192.168.0.36) から送信されました。SMTPサーバ (10.0.2.13)を使用し、このサブジェクトには、「手に入れました」と書かれていました。

未承認のアプリケーションの使用

従業員は、彼がインストールしたアプリケーションを共有したピアツーピアファイルを使用し、音楽を転送したことで、ポリシーに違反しました。彼は、貴重な帯域幅を消費して勤務時間中に大きなファイルを送信しました。さらなる調査で、その従業員は、本当に犯罪者だということが明らかにされました。彼はJabber とIRCを使い、デスクトップ上の承認されていない web サーバーを走査します。

職場でのサイバースラッキング

従業員も、隠れたデイトレーダーです。勤務中に、彼女は、朝と晩に平均1時間、金融取引サイトに接続します。会社の VoIP (SIP) システムも利用して、Yahoo! Messenger で「トレーダータロウ」という名前で「トレーダージロウ」や「トレーダーハナコ」に1日に平均6回電話をして、何時間もの時間を過ごしています。

脆弱なパスワードの使用

企業のセキュリティ ポリシーでは、すべてのユーザーシステムとアプリケーションアカウントに強力なパスワードを使用するよう要求しています。Microsoft Active Directory アカウントは厳しく管理されています。しかし、数十もの脆弱なパスワードが、FTP外部サーバー、メールサーバー、および Active Directory を使用しない重要な web アプリケーションで使用されています。

詳細を見る

詳細については、**www.mcafee.com/siem**をご覧ください。

〒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（代表）
www.mcafee.com/jp