Case Study

マカフィー株式会社

プロファイル

世界最大のセキュリティ・テクノロジー専業のリーディング カンパニー

IT環境
60ヶ国に広がる14,000を超えるエンドポイントとネットワークデバイス

課題
重要な情報とインフラストラクチャーの保護、PCIコンプライアンス準拠、マカフィーセキュリティインフラストラクチャーでの仮想マシン活用のために、最高レベルの可視性と状況認識情報を提供する

マカフィーソリューション
- McAfee® Enterprise Security Manager
- McAfee Enterprise Log Manager
- McAfee Application Data Monitor
- McAfee® ePolicy Orchestrator® (McAfee ePO™)、McAfee Network Security Platform、McAfee Vulnerability Manager、McAfee Firewall Enterprise、McAfee Email Gateway、McAfee Web Gatewayと統合

導入効果
- セキュリティイベントの分析時間を4～6日間から10分未満に大幅に短縮
- PCIコンプライアンスレポートの作成時間を8～12時間から10分に短縮
- 管理時間と手動の保守作業を低減するとともに、不必要な活動を排除
- ディザスターリカバリーを容易にし、仮想マシンの適切な利用を実現
- 組織の総合的なセキュリティ体制を改善

NitroSecurityのSIEMソリューションにより、マカフィーの管理、分析、コンプライアンス達成までの時間の短縮とセキュリティ体制の強化が実現

マカフィーは、インテル・コーポレーション（NASDAQ:INTC）の完全子会社であり、セキュリティ・テクノロジー専業のリーディングカンパニーです。世界中で使用されているシステム、ネットワーク、モバイルデバイスの安全を実現する革新的なソリューションとサービスを提供し、ユーザーのインターネットへの安全な接続、webの閲覧およびオンライン取引の安全を確実に支えています。マカフィーは、他の追随を許さないクラウドベースのセキュリティ技術基盤Global Threat Intelligence™（グローバル スレットインテリジェンス）を活用して、革新的な製品を送り出しています。個人ユーザーをはじめ、企業、官公庁・自治体、ISPなど様々なユーザーは、コンプライアンスの確保、データの保全、破壊活動の阻止、脆弱性の把握を実現し、またセキュリティレベルを絶えず管理し、改善することができます。マカフィーは、およそ6,000名の従業員を擁し、米国とその他60ヶ国に広がる14,000のエンドポイントとネットワークデバイスで構成されるネットワークを運用しています。

セキュリティオペレーションセンターの効率性に極めて重要なセキュリティイベント管理

マカフィーは、さまざまなセキュリティソリューションから収集したデータ分析の効率化と、脅威の特定及び修復を一層強化することを目的に、数年前にセキュリティ情報/イベント管理（SIEM）ソリューションを導入しました。しかし、マカフィーのセキュリティインフラストラクチャーが成熟し、監視対象のセキュリティデバイスが大幅に増加したため、マカフィーのSIEMアプライアンスはデータ量の爆発的な急増に対処しきれなくなってしまいました。現在、マカフィーのセキュリティオペレーションセンター（SOC）は毎月平均で79億件のセキュリティイベントを記録しています。

マカフィーのSOCマネージャーであるRobert Morrisは次のように述べています。「SIEMに転送するデータ量が増加するようになると、SIEMからデータを再び取得することはほぼ不可能になりました。1つのイベントの分析に1週間かかることもありました。SIEMはSOCで重要な役割を果たすため、それほどの長時間待つことは容認できないことでした。しかも、SIEMに問い合わせを実行すると大量のフローデータが発生し、ネットワーク帯域幅が完全に飽和状態になる可能性がありました」

優れたSIEMアーキテクチャーが複数のメリットを提供

マカフィーはSIEMベンダーに課題を提示しましたが、既存のソリューションを活用してマカフィーの要求を満たすには、50万ドルの追加投資が必要でした。そこでマカフィーは別のオプションの調査に乗り出しました。4つのベンダーのテクノロジーに絞込み、各ソリューションの徹底的な検証を行った結果、マカフィーは既存のSIEMソリューションに代えてNitroSecurityを導入することを決定しました。

マカフィーのセキュリティエンジニアリング担当マネージャーのTony Gunnは次のように語っています。「NitroSecurityソリューションのアーキテクチャーは、他のベンダーと比較にならないほど優れていました。このソリューションは、毎月数十億件のイベント、1秒換算では50,000件を処理し、超高速なデータの問い合わせ、取得、分析を実現できるように一から設計されていました。このソリューションの導入と使用は、以前のソリューションよりもはるかに容易だという期待をしていましたし、実際に非常に簡単でした。また、以前のソリューションとは違い、手動での管理を必要とせずに、必要な場所で仮想マシンを使用することができました」

「NitroSecurity ソリューションの導入前は、分析用のセキュリティイベントデータの抽出に 4 ～ 6 日かかっていましたが、今では 3 分、かかっても 10 分です。つまり、データをはるかに高速に取得できるようになっただけでなく、取得したデータをより効率的に活用することが可能になったのです」

—Tony Gunn
マカフィー
セキュリティオペレーション
センターマネージャー

マカフィーは、Nitro Enterprise Security Manager（ESM）アプライアンスとNitro Enterprise Log Manager（ELM）アプライアンスを2台ずつ導入し、米国のSOCと別の大陸のディザスターリカバリーサイトに設置しました。また、8つのNitro Application Data Monitor（ADM）システムを導入し、その6つをアプライアンスとして、2つを仮想マシンとして使用しました。Nitroソリューションは、McAfee ePOソフトウェア、McAfee Network Security Platform、McAfee Vulnerability Manager、McAfee Firewall Enterprise、McAfee Web Gateway、McAfee Email Gatewayソリューション、そして複数の他社ソリューションと統合されました。

「Nitroシステムがネットワークに物理的に接続されると、必要な作業はEnterprise Security Managerと接続し、日常的に使用する複数のダッシュボードを作成し、5つのポリシールールを修正するだけでした。実装は、以前のSIEMソリューションよりもはるかに容易に行えました」とMorrisは述べています。

イベント分析の高速化と応答時間の最小化を実現

「NitroSecurityソリューションの導入前は、分析用のセキュリティイベントデータの抽出に4～6日かかっていましたが、今では3分、かかっても10分です。おかげで多大な時間が節約されています。重要な履歴分析を実行するためには、すべての関連データソースから取得したできるだけ多くのフォレンジックデータに簡単にアクセスできなければなりません。そしてセキュリティインシデントに素早く効率的に対応するには、その情報を可能な限り早く入手する必要があります。Nitroソリューションは、その両方を実現してくれました」とGunnは述べています。

マカフィーが導入したNitroシステムは、1秒間に50,000件のセキュリティイベントを処理することができます。また、受信データを自動的かつ非常に効率的に正規化します。多様なデバイスとさまざまなベンダーのソリューションからイベント情報を取得すると、「ウイルス」、「バッファオーバーフロー」、「Webエクスプロイト」、「電子メールエクスプロイト」、「潜在的脆弱性」などの正規化した区分と4つの詳細レベルを使用して分類します。したがってマカフィーのどのIT管理者でも、このソリューションのダッシュボードを通じて、発生しているイベントのタイプを即座に把握し、必要に応じてドリルダウンして詳細を理解することができます。またNitroシステムは、以前のSIEMソリューションよりも効率的にイベントに重大度レベルを割り当てます。「つまり、データをはるかに高速に取得できるようになっただけでなく、取得したデータをより効率的に活用することが可能になったのです。すべてのデータの概要を確認した後、必要に応じてダッシュボードから個別のデータに焦点を当てることができます。この情報のおかげで、リスクプロファイルとセキュリティ上の問題の評価を迅速に行えるようになったと同時に、新しい構成の発行、新しいポリシーの導入、最新のソフトウェアアップデートの導入など幅広い修正措置を分析し、開始することが可能になりました」とGunnは述べています。

管理作業を低減し、ネットワーク帯域幅を大幅に改善

「管理面で言うと、1箇所からすべてのSIEMレシーバーの管理と更新ができるようになったことで、日常の管理時間が短縮されました。1名の管理者が世界各地の8つのレシーバー全体にわずか15分で新しいパッチを適用できるため、他のセキュリティタスクに充当できる時間が増えました。かつては、1名の管理者がこの作業に丸1日を費やしていました」とMorrisは説明しています。

前述のとおり、組み込まれている正規化機能もイベント分析に役立っています。「以前は手動で多数のルールを作成し、イベントデータを掘り起こす必要があり、正しく解析できていないのではないかという懸念もありました。Nitroシステムには、非常に効率的なデータの正規化機能とその他の組み込みツールがあるので、以前手動で実施していた作業が不要になりました。たとえば、注意リストとフィルターを作成することにより、特定のネットワークから送られてくる注目すべきトラフィックのタイプをシステムに通知することができます」とMorrisは述べています。

過大な負荷がかかったネットワーク帯域幅の対処が不要であることも、時間の節約に貢献しています。「Nitroシステムを導入する前は、圧縮されていないセキュリティイベントの未加工データが単一のリポジトリーに転送されていました。そのデータの流れによってネットワークが飽和することもしばしばでした」とMorrisは述べています。問い合わせのたびに数ギガバイトの未加工データを転送する代わりに、Nitroシステムはネットワークを介してリアルタイムでインデックスを転送します。「必要に応じて特定のイベントデータを取得できますが、ネットワークが飽和状態になることはありません。さまざまなデバイスから収集された未加工のイベントデータは、毎日8つのレシーバーからMcAfee Enterprise Log Managerにバックアップされますが、トラフィックを抑制して適切なときにデータを転送することができます。データが転送されても、平均で17対1の割合で圧縮されているため、ネットワークへの影響は大幅に低減されます」とMorrisは述べています。

PCIおよびISO2007コンプライアンスまでの時間を短縮

Nitroシステムでは、コンプライアンスレポートの作成も非常に簡単です。マカフィーはレベル1のPCI加盟店であるため、PCIコンプライアンスは必須です。「Nitroシステム導入後初めてPCIギャップ分析を行った際、特定のファイアウォールで発生したセキュリティイベントを非常に簡単に把握できることに驚き、すべての重要なデバイスの監視を実施しました。監査用のレポートの作成にかかる時間は約10分ですが、以前のソリューションでは、PCIコンプライアンスの証明を提供するために8～12時間を要していました」とMorrisは述べています。

「監査役向けのレポートの作成にかかる時間は約 10 分ですが、以前のソリューションでは、PCI コンプライアンスの証明を提供するために 8 ～ 12 時間を要していました」

—Robert Morris
マカフィー
セキュリティオペレーション
センターマネージャー

Nitroシステムは、セキュリティイベントの未加工のパケットデータを保持することで、ISO 27001のコンプライアンスも促進しています。「ISOインシデント対応の一環として、特定のインシデントに関わるすべての異なるイベントを検証できなければなりません。そのために最善なのは、フォレンジックの実施に適した未加工のフォーマットでイベントを検証する方法です」とMorrisは説明しています。

統合を通じたセキュリティの向上

Nitroシステムと他のマカフィーセキュリティソリューションを統合すると、Nitroシステムの予測機能はさらに強化されます。例えば、McAfee Vulnerability Managerによって収集された脆弱性データを取得する場合、Nitroソリューションを通じて、機密性、整合性、可用性など、マカフィーのガバナンス、リスク、及びコンプライアンスポリシーで定義された要素と照らし合わせて資産の脆弱性をマッピングすることができます。マカフィーのNitroシステムは、他のマカフィーソリューションだけでなく、Microsoft Active Directory、Splunk Syslog、*nix Syslog、Cisco Syslog、Avaya Syslog、ArcSight CEF Eventsとも統合されています。

マカフィーは、コンプライアンス達成のためにディザスターリカバリーサイトにSIEM機能が必要でした。Nitroシステムによって、ディザスターリカバリーの冗長性の導入が容易になりました。「Nitroアーキテクチャーでは、レシーバーからESMとELM両方にデータを送信することができます。一方がダウンした場合、もう一方のIPアドレスを使用し、システムにそのままアクセスしてイベントを確認することができます」とMorrisは説明しています。

仮想マシンの活用

設備投資と設置面積の削減のために、マカフィーは世界各地に6つのレシーバー仮想マシンを導入しました。NitroSecurityソリューションの導入前は、各SIEMエージェントの更新は手間のかかる作業でした。どのようなタイプのMicrosoft WindowsのパッチもArcSight Connectorの更新も、ホストデバイスから導入する必要がありました。「現在の私たちの作業は、最新のパッチまたは更新をアップロードし、物理、仮想を問わず中央のコンソールから複数のデバイスに導入するだけで完了です。数分のうちに、Nitroシステムが自動的に適用してデバイスを再起動してくれます」とMorrisは述べています。

ソリューションの効率性をきっかけに買収へ

マカフィーはNitroSecurityソリューション、そしてソリューションの導入によるSOCの効率性の向上に感銘を受け、ソリューションの導入開始からわずか1年でNitroSecurity社とそのテクノロジーを買収しました。NitroSecurityはすでに3年前からMcAfee Security Innovation Allianceプログラムに参加しており、包括的なマカフィーセキュリティポートフォリオの機能を補完し、マカフィーとNitroSecurityの共同のお客様のリスク及びコンプライアンスのニーズ対応を支援していました。自社のSOCでNitroSecurityのセキュリティを使用したことが、NitroSecurityのSIEMテクノロジーを自社製品に完全に統合するという戦略的決定に大きく寄与した結果になりました。Nitroソリューションは、マカフィーのSecurity Connectedフレームワークの一部として、マカフィーのお客様にIT環境全体にわたる企業のエンドポイント資産、基盤のネットワークインフラストラクチャー、特定のセキュリティ脅威とリスク、システムの脆弱性に対する可視性を提供します。

McAfee
An Intel Company
マカフィー株式会社
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

MCACS-NTR-1209-MC