Case Study | 導入事例

TTUHSC、セキュリティとコンプライアンスの連携にマカフィーを選択

TEXAS TECH UNIVERSITY

テキサス工科大学健康科学センター

顧客プロファイル:
米国テキサス州(ラボック)
州立工科大学

産業:
ヘルスケア

IT環境:
6つのキャンパスにまたがる7つの学部、研究所施設、医療クリニック内
サーバー400台
クライアント:100,000ノード

課　題

- HIPAAとTAC202(テキサス州の高等教育及び州の機関向けセキュリティ基準)コンプライアンス遵守
- セキュリティ管理と脅威に対する状況認識の改善
- レガシーシステムやパフォーマンスの低いサードパーティのネットワーク、Web、Emailシステムの入替

テキサス工科大学健康科学センター(TTUHSC)は医療、看護、薬学、生体臨床医学、健康科学のプログラムを提供しています。TTUHSCは1969年から1万人以上のヘルスケア専門家を育成しています。教育と患者管理をリードする同大学の研究分野には老化、がん、再生、遺伝病、農村の健康が含まれます。

ビジネス上の要因:コンプライアンスと生産性

研究、教育、医療クリニックを通して、同大学はウエストテキサスを中心とした100以上の郡の患者の治療に貢献しています。同大学のセキュリティチームはHIPAAの規定とTexas Administrative Code(一般的にTAC 202と呼ばれる)のコンプライアンスを維持し、電子的な医療記録と健康に関する情報を保護する必要があります。

マカフィーのソリューションを導入する前、TTUHSCでは異なるベンダーの複数のデバイスを統合しないまま使用していました。情報セキュリティを担当するAndrew Howard氏は次のように述べています。「調査や監査には膨大な時間がかかります。また、当時使用していたSIEM製品は管理があまりにも複雑でした」。

ソリューションの焦点:一元管理と高度な相関分析

セキュリティチームはログ管理だけでなく、環境のイベントを相互に関連付けるため、より適切なセキュリティ情報/イベント管理(SIEM)ソリューションを必要としていました。そのため、エンドポイント、データ、電子メール、Web環境の保護にMcAfee Security Connectedフレームワークの製品を、状況認識、一元管理、高度な相関分析にマカフィーのSIEMソリューションを選択しました。

McAfee Enterprise Security Managerには事前定義のダッシュボード、完全な監査証跡、インテリジェントなログ管理など、コンプライアンス管理のための機能があります。「相関分析はすばらしい機能です。データを簡単に利用でき、インフラストラクチャ全体を確認できます。」と、Howard氏は述べます。

段階的なアプローチによるTTUHSCのセキュリティ変革

Howard氏がTTUHSCに採用された当時、その環境には約1万のエンドポイントがありましたが、基本的な仮想スキャンとマルウェア対策の保護しか適用されていませんでした。Howard氏は次のように述べています。「このような構成の標準は限られています。エンドポイントのアクセスは部署と役割によって異なります」。

中断を最小化するため、セキュリティチームは段階的なアプローチによって新しいセキュリティソリューションを導入しました。各製品はまず、部署ごとにテストされ、本番導入する前に各キャンパスでテストされました。ユーザーへの影響が少ないと判断されたら、大規模なキャンパスでMcAfee Complete Endpoint Protection—Enterpriseなどの使用を開始することになっていました。製品の使用開始後、ユーザーに大きな影響があった場合、数百のエンドポイントしかない小規模なキャンパスで導入を開始する予定でした。

intel Security

導入製品

- McAfee Enterprise Security Manager
- McAfee Advanced Correlation Engine
- McAfee Complete Endpoint Protection—Enterprise
- McAfee Network Security Platform
- McAfee DLP Endpoint
- McAfee Network Data Loss Prevention
- McAfee Email Gateway
- McAfee Web Gateway
- McAfee Host Intrusion Protection
- McAfee ePolicy Orchestrator® (McAfee ePO™) software
- McAfee Global Threat Intelligence

効　果

- レポーティング機能強化
- 数千回単位の攻撃をブロック
- セキュリティ監査の時間を大幅に短縮
- 脅威の可視化と管理の効率化

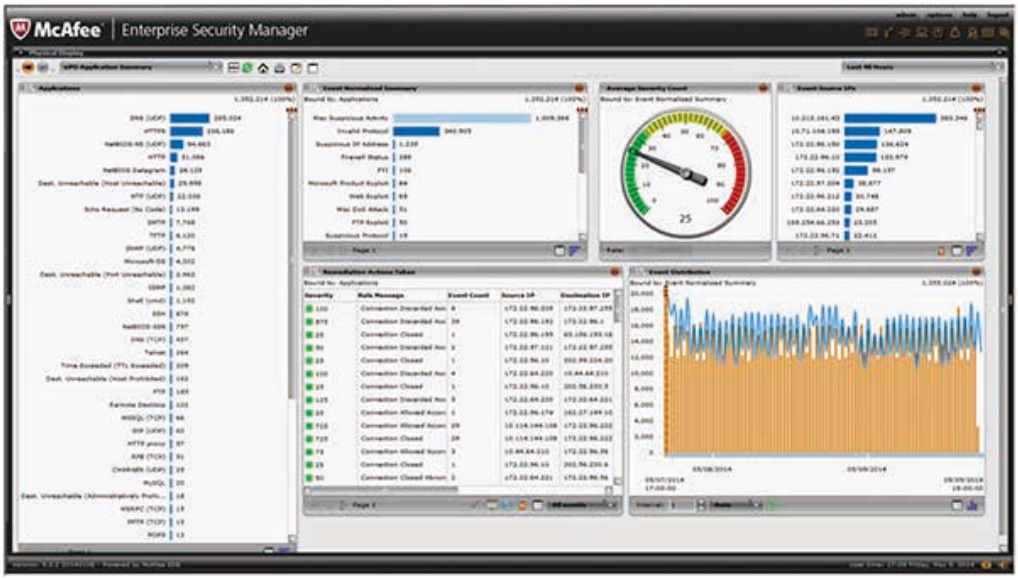

図 1. McAfee Enterprise Security Managerのダッシュボード

「いまではすべてが接続され、生産性が大幅に向上し、短期間で価値が実現しています。」

情報セキュリティ担当者　Andrew Howard 氏

McAfee Complete Endpoint Protection — Enterpriseの導入後、Howard氏率いるチームはセキュリティ戦略を展開し、耐用年数を経た既存の侵入防止システム（IPS）をMcAfee Network Security Platformに移行してスマートブロッキングを有効にしました。「McAfee Network Security Platformのデモは印象的でした。エッジ保護を効果的に導入でき、McAfee Global Threat Intelligence（McAfee GTI）を送受信のトラフィックに活用できます。」と、Howard氏は述べています。TTUHSCではMcAfee Advanced Correlation Engineをリスクベースの相関分析と設定のルールに使用して、送信元IPと送信先IPをMcAfee GTIの不正のデータベースと比較しています。

同大学では、McAfee Vulnerability Managerをそのセキュリティポートフォリオに統合することも計画しています。「すべての施設に十分なライセンスを購入しました。これまで、サーバー環境だけをスキャンしていましたが、McAfee Vulnerability Managerを導入したら、統合されたスキャンを活用します。」と、Howard氏は述べます。

ネットワークベースの脅威とポリシー違反のブロック

TTUHSCではIPSの稼働直後、McAfee Web Gatewayも本格導入しました。州の機関のため、HIPAA、PCI、バンキングなどの規制以外にプライバシーの権利はありません。学生、学部、管理者アカウントおよびすべてのトラフィックの監視は同大学が責任を負います。

「プロキシ環境がなかったため、マルウェアのウイルスと悪意のコードをエンドポイントで修正するのは大変でした。いまでは、エンドポイントに到達する前に悪意のコードを検出できます。McAfee Web Gateway導入後、8か月間で数千のウイルス、悪意のコード、Webサイトをブロックしました。」と、Howard氏は述べています。TTUHSCではMcAfee Email Gatewayを使用して、送受信の電子メールをフィルタリングしています。

一元管理によるハイパフォーマンスとハイスピード

McAfee Web and Email Gatewayに続き、TTUHSCではMcAfee ePolicy Orchestrator®（McAfee ePO™）ソフトウェアを一元化ソリューションとして導入し、エンドポイントの管理、ポリシーの策定と導入、レポート作成に利用しています。また、McAfee ePOソフトウェアをMcAfee Risk Advisorに統合し、システム脆弱性を分析しています。McAfee ePOソフトウェアは別のダッシュボードでWeb環境の監視にも使用しています。「たとえば、学生の動画再生や動画の著作権の問題を監視できます。また、McAfee ePOは月次の州のレポートにも使用しています。当校にとって、このソフトウェアが管理の中心であることは間違いありません。」と、Howard氏は述べています。

ビジネスの成果：CIOのビジョンの実現

TTUHSCにとってマカフィーの最大のメリットは、セキュリティを統合し、セキュリティソリューションの管理を一元化できることにあります。「セキュリティソリューションを検討している組織には、統合に焦点を当てることをお勧めします。当校ではマカフィー製品を使用していますが、McAfee ePOソフトウェアで大量のデータを取得したり、マカフィーのSIEMソフトウェアで問題の根本原因を迅速かつ効果的に特定できるようになりました。導入してすぐに価値を実現できるので、期待を超えるメリットがあります。」と、Howard氏は述べます。

Howard氏はマカフィーを導入した結果、生産性が向上したことにも満足しています。これまでのSIEMソリューションでは、セキュリティチームが調査のために過去6か月分や1年分のデータを必要とする場合、データを取得するまでに数日かかっていました。その後、手作業でCSVファイルを確認し、データを関連付けていました。これらの作業は自動化されていませんでした。現在では、McAfee Enterprise Security Managerで管理を一元化しているため、ログ、Webトラフィック、受信トラフィック、電子メールの見直しにかかる時間が短縮され、作業も軽減されています。

マカフィーを選択した理由

「これまで、全体的なレビューには数週間かかっていました。マカフィー製品導入後は一元化された管理を活用して、基準を指定してからわずか数分で必要なデータを収集しています。導入当初、CIOと私は完全な一元管理と迅速なレポート作成を目標にしていました。マカフィーのおかげで、セキュリティとコンプライアンスの戦略の最終目標を達成できました。」と、Howard氏は総括しています。

最新導入事例はこちらをご覧ください　http://www.mcafee.com/jp/case-studies.aspx

intel Security

マカフィー株式会社　www.mcafee.com/jp

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）

● 製品、サービスに関するお問い合わせは下記へ

MCACS-TEXAS-1504-GRP