ケーススタディ

エンドポイント保護を見直してセキュリティ体制の革新と強化を実現

McAfee を利用して、革新的なグローバル ビジネス プロセス トランスフォーメーション企業が自身のセキュリティ プロセスをトランスフォーム

Sutherland Global Services

顧客情報
ビジネス プロセス トランスフォーメーションの多国籍企業

業界
テクノロジー及びビジネス サービス

IT環境
6 大陸 16 か国に約 50,000 のエンドポイントが存在

Sutherland Global Services はデータ分析やその他の技術、デザイン思考の専門知識、そして業界知識を用いて、16 か国、100 社以上の Fortune 1000 企業でビジネス プロセスのデジタル化を支援しています。Sutherland Global Services (ニューヨーク州ピッツフォード) は、自社のエンドポイント セキュリティをトランスフォームさせ、セキュリティを大幅に改善するだけでなく、コストや労力も削減しました。さらに、Open Data Exchange Layer (OpenDXL) を用いて、様々なセキュリティシステムが互いを補完しあう統合的な防御策を構築しました。

McAfee とつながる

事業の中断やデータ漏洩の防止

Sutherland Global Services でテクノロジー インフラストラクチャのグローバルヘッドをしている Prashanth M J 氏は次のように述べています。「ユーザーが必要とするときにシステムが利用できない場合、私たちは多額の費用を無駄にしていることになります。事業の中断とデータ漏洩は非常にリスクが高いので、確実に防止しなければなりません。当社は、これらのリスクを最小限に抑え、革新的なカスタム ソリューション及びサービスをお客様に提供し続けられるよう、徹底した管理を行っています。」

約 50,000 のノード (1,000 のサーバーを含む)、80 か所以上のデータセンター / デリバリー センター、そして 6 大陸 16 か国に広がるデジタル バックボーンを抱えているため、セキュリティ リスクを最小化するには多くのセキュリティ ソリューションが必要です。多数のシステムと制御を連携させ、セキュリティ インテリジェンスを共有して企業全体を保護するため、テクノロジー インフラストラクチャ チームは常に課題をかかえています。

重要な課題：革新をサポートする戦略的パートナー

Sutherland Global Services は非常に大規模な企業で多くの地域に広がっているため、McAfee のような戦略的パートナーの支援が必要になります。Prashanth 氏は次のように述べています。「私たちは常に革新的でいなければなりません。McAfee はそういった私たちの要件を満たしてくれるので、非常に信頼しています。革新こそが私たちの会社の存続と繁栄のカギなのです。」

Prashanth 氏は続けます。「私たちのサービスはビジネスとテクノロジーとの関係に革新を起こし、プロセスをトランスフォームさせ、お客様のビジョンを実現します。McAfee はそういった私たちのビジネス要件に見合ったソリューションを常に提供してくれています。例えば検出から修復までのギャップを埋め、デジタル トランスフォーメーションを推進してくれます。」

OpenDXL を活用した統合防御

Prashanth 氏はまた、McAfee の OpenDXL を高く評価しています。これはテクノロジー業界のイニシアチブで、セキュリティ上の決断が迅速かつ正確に行えるよう、情報を連携し共有する相互接続ソリューションから成る適応システムを構築します。現在 Sutherland Global Services は OpenDXL を用いて、同社で使用しているサードパーティのセキュリティ情報 / イベント管理 (SIEM) ソリューションと McAfee のエンドポイント保護を統合させようとしています。Web ゲートウェイとファイアウォールの統合も OpenDXL を用いて将来実現させる予定です。

Prashanth 氏は次のように述べています。「OpenDXL には大きな可能性があります。現在、様々なベンダーのセキュリティ製品を多数使用しており、それぞれが独立しています。サイバー攻撃への統合的防御を構築するには、それぞれのシステムのインテリジェンスを共有することが必要です。」

課題

- 全世界のユーザーにシステムを年中無休で提供
- 統合サイバー防御に向けたセキュリティ ソリューションの統合
- 規制順守の効率化 (特にヘルスケア及び金融サービス業界)

McAfee のソリューション

- McAfee® Advanced Threat Defense
- McAfee® DLP Endpoint
- McAfee® Endpoint Encryption
- McAfee® Endpoint Security
- McAfee® Endpoint Threat Defense and Response
- McAfee® ePolicy Orchestrator®
- McAfee® File Integrity Monitoring
- McAfee® プロフェッショナル サービス
- McAfee® Threat Intelligence Exchange

エンドポイント保護の統合でコストを削減し将来の収益増加へとつなげる

Sutherland Global Services は世界中のエンドポイントの保 護 に McAfee ePolicy Orchestrator (McAfee ePO ™) 集中管理コンソールを活用しています。McAfee ePO ソフトウェアでは、複数の McAfee 製品とセキュリティ機能 (ウイルス対策、ホスト データ損失防止、ホスト侵入防止、エンドポイント暗号化、ファイル整合性監視など) を一か所で管理し監視できます。

Prashanth 氏は以下のように述べています。「McAfee ePO (ソフトウェア) で、全社をシームレスに管理できるようになりました。このソフトウェアのは操作が簡単で、コストの高いレベル 2 や 3 のセキュリティ エンジニアを雇う必要はありません。」

Sutherland Global Services はエンドポイント保護策のアップグレードとトランスフォームの一環として、この 2 年のうちに、各国に散在していた 7 つの McAfee ePO ソフトウェア サーバーを 1 つに統合しました。現在、セキュリティ オペレーション センターにある McAfee ePO 集中コンソールから約 50,000 のエンドポイントを管理しています。

Prashanth 氏は次のように述べています。「他の 6 つの McAfee ePO (ソフトウェア) サーバーをディコミッションしたことにより、コストを削減できました。ハードウェアやソフトウェアのコストが減っただけでなく、データセンターの電力消費量も減り、またメンテナンスにかかる時間や諸経費も減少しました。さらに、新しい人員を追加することなく新しい機能も追加でき、またスタッフはより付加価値の高い活動に時間を費やせるようになりました。」

Prashanth 氏は次のように続けます。「エンドポイント保護を見直すことによって全社でシステムの可用性が向上し、これによって収益向上のポテンシャルが増えました。」

迅速かつ簡単なコンプライアンス レポートでコンプライアンスのレベルを 95% 以上に引き上げ

集中コンソールに統合することで、コンプライアンス維持にかかる時間を大幅に削減できます (特にヘルスケア及び金融サービス業界)。Prashanth 氏は以下のように話しています。「集中コンソールにより、コンプライアンス レポートの作成効率が格段に上がりました。さまざまな地域、クライアント、業界のセキュリティ オーナーの状況に合った、カスタマイズ ダッシュボードを迅速かつ簡単に提供できます。そのため必要なレポートの作成が容易になり、またコンプライアンス レベルを 95% 以上にまで引き上げることができました。」

効果

- 管理オーバーヘッド、ハードウェア／ソフトウェアコストの削減
- システム可用性の向上
- 収益向上のポテンシャルの増加
- 容易なエンドポイント保護で全世界の管理者の負担を軽減
- ゼロデイ攻撃を含むマルウェアに対する、マルチレイヤーの強固な防御
- 全世界におけるコンプライアンス レポートの効率化
- コンプライアンス レベルの向上 (95% 以上)
- 脅威検出及びレスポンスの迅速化

マルチレイヤーの脅威情報共有でゼロデイ攻撃への防御を強化

McAfee® VirusScan® Enterprise から McAfee Endpoint Security への移行は、エンドポイント保護の改革において極めて重要な要素でした。Prashanth 氏は次のように説明します。「保護レイヤーを追加した次世代の堅牢なマルウェア対策が必要だと考えていましたが、McAfee はまさに私たちが必要としていたものを提供してくれました。未知のファイルを隔離する Dynamic Application Containment と、臨機応変に不審なファイルを分析する Real Protect の機械学習機能は特に役立っています。」

同社は McAfee Endpoint Security に移行することで McAfee Threat Intelligence Exchange を活用できるようになりました。これは常時アップデートされるグローバル / ローカル脅威インテリジェンスを蓄積し、それを Data Exchange Layer (DXL) を通してすべての DXL 連携システムに双方向共有します。McAfee Endpoint Security は複雑な設定なく、すぐに DXL に接続できます。Prashanth 氏は以下のように説明します。「エンドポイントに悪意あるファイルが送られた場合、またはグローバ ルリサーチ センターが新しいゼロデイ攻撃を発見した場合、すべてのエンドポイントがそういった脅威をすぐに自動認識できるので、管理者によるシグネチャの提供を待つ必要はなくなります。」

Sutherland Global Services は McAfee プロフェッショナル サービスを活用して、全世界のシステムを停止させることなく、スムーズに段階的に McAfee Endpoint Security に移行しました。すべてのエンドポイントを McAfee Endpoint Security に移行することで、本ソリューションの Advanced Threat Protection モジュール (Dynamic Application Containment 及び Real Protect テクノロジー) を活用できるようになりました。同社はまた、DXL ファブリックと McAfee Threat Intelligence Exchange を社内すべてのネットワークに展開しています。

インシデント レスポンスの迅速化

Sutherland Global Services はエンドポイント保護のトランスフォーメーションの一環として、動的 / 静的サンドボックス分析ができる McAfee Advanced Threat Defense アプライアンスを導入しました。Prashanth 氏は次のように述べています。「McAfee Advanced Threat Defense には 2 つ重要な機能があります。1 つ目の機能では、エンドポイントに未知のファイルが送られそれを隔離した場合、そのファイルが McAfee アプライアンスに直接送付され詳細分析されます。分析後の結果は [McAfee Threat Intelligence Exchange] を経由して全社に共有されます。これにより多数の悪意あるファイルを発見でき、エンドポイントをプロアクティブに保護できています。」

「私たちのサービスはビジネスとテクノロジーとの関係に革新を起こし、プロセスをトランスフォームさせ、お客様のビジョンを実現します。McAfee はそういった私たちのビジネス要件に見合ったソリューションを常に提供してくれています。例えば検出から修復までのギャップを埋め、デジタル トランスフォーメーションを推進してくれます。」

—Sutherland Global Services シニア バイスプレジデント兼テクノロジー インフラストラクチャ グローバル ヘッド Prashanth M J 氏

「もう 1 つの機能は IoC 調査プロセスの迅速化です。未知の IoC については、これまでは McAfee サポートにハッシュのサンプルを送って、それが悪意あるものかどうかの診断を待たなければなりませんでした。しかし McAfee Advanced Threat Defense を導入することにより自社で IoC の分析ができるようになり、必要なアクションをより迅速に決定できるようになりました。」

さらに同社は McAfee Endpoint Threat Defense and Response の導入を進めており、これにより脅威をプロアクティブに発見する能力が増強される予定です。Prashanth 氏は以下のように話しています。「ディフェンスではなくオフェンスに回る必要があります。McAfee Endpoint Threat Defense and Response は、すでに私たちの環境内に潜んでいるかもしれない脅威に対抗するための、非常に重要なツールになると思います。レスポンスはスピードが重要です。正しいアクションでも遅すぎては無意味だからです。」

将来への備えには製品のみでは不十分

Sutherland Global Services の CIO 兼チーフ デジタル オフィサーの Doug Gilbert 氏は以下のように話しています。「McAfee とのパートナーシップは私たちにとって実り多いものでした。システムは完璧に保護され、将来に向けて準備ができていると確信できるようになりました。どの会社とパートナーを組むかを判断するには、製品だけでなくエコシステム全体を見ることが必要です。McAfee は常に私たちに寄り添ってくれています。単に製品を販売するためではなく、それらをデザインし、展開し、維持し、最適化する手助けをするためです。」

Sutherland Global Services はクラウドへさらに移行してデジタル トランスフォーメーションを推進し続けるため、McAfee は今後も同社において重要な役割を果たし続けます。Prashanth 氏は同社に必要な改革のもうひとつの例として新しい McAfee® MVISION 製品を挙げています。「脅威ランドスケープは非常に複雑なので協力が不可欠です。McAfee は私たちに [正しい] テクノロジーを提供してくれます。そして私たちはビジネスの [知識] を提供します。『Together is Power』こそが私たちの進むべき方向です。」

「McAfee とのパートナーシップは私たちにとって実り多いものでした。システムは完璧に保護されていると確信できるようになりました。どの会社とパートナーを組むかを判断するには、製品だけでなくエコシステム全体を見ることが必要です。McAfee は常に私たちに寄り添ってくれています。ただ製品を販売するためではなく、それらをデザインし、展開し、維持し、最適化する手助けをするためです。」

—Sutherland Global Services
CIO 兼チーフ デジタル オフィサー
Doug Gilbert 氏

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