導入事例

自動車ディーラーがフォーティネットのSD-WANとSDブランチでセキュリティとネットワーキングを統合

自動車ディーラーは、通常、サイバー攻撃のリスクが最も高い業種の上位にランキングされることはありません。しかし、オハイオ州、ワイオミング州およびサウスダコタ州に18の拠点を持つWhite Family Dealerships社のITディレクターであるShane Williams氏は、実際は見過ごされているだけだと言います。

「カーディーラーは顧客情報の宝庫ですから、銀行と同等のセキュリティプロトコルを順守しなければなりません。もし、当社が十分な情報漏洩対策を講じておらず、情報漏洩を起こしてしまった場合、FCC（連邦通信委員会）から多額の罰金を科せられ、ブランドにも傷がついてしまいます」

ホワイトファミリーディーラー社は、顧客情報の保護、規制機関や販売する自動車メーカーの要件の順守を徹底しています。同社は、ランドローバー、ポルシェ、シボレー、ダッジ、フォードなど多岐にわたる自動車を販売しています。Williams氏は、「自動車メーカーごとにサイバーセキュリティに対する考え方は異なります。ですから、当社に求められるサイバーセキュリティも多種多様です。当社は、各自動車メーカーに、Eメールや関連するセキュリティ、アンチウイルス、物理的セキュリティなどの情報を定期的に提供しなければなりません。あるメーカーは、突然販売店を訪問して、私たちがそれらを実際に行っているのかを調査する場合もあるのです」と言います。

低コスト、使いやすさを求めて市場を調査

Williams氏の課題は、2人の従業員とともに3つの州においてIT、ネットワーク、セキュリティインフラを管理することでした。Williams氏は、以前契約していた第三者サービスプロバイダーによるネットワークセキュリティとディーラ管理システム（DMS）のサービスは理想には程遠いものだったと言います。

「変更や確認したいことがあっても、とにかく時間がかかったのです。電話をかけても、ずっと待たされるだけでした。ようやくサポート担当者とつながっても、私の説明を理解できない、ということもありました」

また、Williams氏は、かなりの時間を移動に費やしていました。「週に2～3回は、トラブルシューティング、アップデートやパッチのインストール、機器の追加などのために、ディーラーに出向いていました。このような状況だったので、実に多くの時間を無駄にしました」

同社は、ある自動車メーカーの提案を機に、IT環境を見直しました。自動車メーカーがディーラー各社に対し、特定のマネージド セキュリティ サービス プロバイダー（MSSP）と契約して、FortiGate次世代ファイアウォール（NGFW）の導入・運用を推奨したのです。当時の第三者サービスプロバイダーが提供するネットワークセキュリティの可視化に限界を感じていたWilliam氏は、FortiGate次世代ファイアウォール（NGFW）は単一の管理ポイントで管理できるという点に大変興味を持ちました。また、コストと管理の観点からも、ネットワークとセキュリティインフラを自社ですべて管理すべきだと考えたのです。

Williams氏は、「目標は、セキュリティの強化とビジネスの継続性の向上でした。ネットワークサービスを提供できない時間は、損失そのものです。特に新型コロナウイルス感

White Family Dealerships

「最近、ネットワークに侵入しようとする人が後を絶ちません」「数年前までは、自動車ディーラーは攻撃者の眼中にはありませんでしたが、今では、サイバーセキュリティのリスクは大きな脅威となっています。しかし、フォーティネットのセキュアSDブランチソリューションのおかげで、夜もぐっすり眠れるようになりました」

– Dealerships社
ITディレクター
Shane Williams氏

詳細

顧客：ホワイトファミリーディーラー社

業種：小売

所在地：オハイオ州デイトン

ビジネスへの効果

- 自動車メーカーの要件を満たすセキュリティ態勢によりITチームに安心感をもたらす

染症が流行し始めてから、インターネットでショッピングやビジネスをする人が増えました。ですから、当社のネットワークインフラの稼働率を最大化することが何よりも重要でした」と語ります。また、各ディーラーと本社間をつなぐMPLS（Multiprotocol Label Switching）をSD-WAN（Software-Defined Wide Area Networking）に置き換えることで、接続コストも削減できるとも考えたと言います。

Williams氏は、フォーティネットのソリューションは優れた選択肢であるとすぐに実感しました。フォーティネットのセキュリティ ドリブン ネットワーキングのアプローチによって、ネットワーキングとセキュリティを融合させ、ネットワークファイアウォール、SD-WAN、SDブランチの各ソリューションを単一の管理ポイントで管理できるようになったためです。フォーティネットのセキュアSDブランチは、ネットワークエッジにおける業界をリードするセキュリティでWANを保護し、ユーザーエクスペリエンスの向上と全体のコスト削減を実現します。また、SD-WANの利点を企業の拠点全域に展開し、ローカルエリアネットワーク（LAN）、エンドユーザーシステム、ワイヤレス、インターネットへの直接接続、企業が使用するあらゆるIoT（Internet-of-Things）デバイスのセキュリティを強化し、管理を簡素化します。

ホワイトファミリーディーラー社は、SD-WANネットワークの価格や、フォーティネットのセキュアSDブランチのすべてのコンポーネント内にセキュリティが搭載されていることに非常に満足しています。これに加え、Williams氏は、「使いやすさも大きな決定要因でした。私は、他のセキュリティベンダーやネットワーキングベンダーにも精通していますし、他のベンダーのソリューション認定も取得しています。フォーティネットのインタフェースはシンプルなため、同じ作業を素早く簡単に行えることに、とても感心しました」と言います。また、NGFW、スイッチ、アクセスポイント間の完全な統合も決定要因だったと言います。「フォーティネットのプラットフォームで最も気に入っている点の1つは、異なるコンポーネントが完全に統合されていることです」

フォーティネット セキュリティ ファブリックがもたらす優れた可視化

ホワイトファミリーディーラー社では、FortiGate NGFW、FortiSwitchスイッチ、FortiAPアクセスポイントを導入し、各ディーラーと本社をワイヤレスで接続しています。導入初期の段階では、レガシーMPLS接続でIPsec（Internet Protocol Security）仮想プライベートネットワーク（VPN）トンネルを介してNGFWをネットワークに接続していましたが、1年も経たないうちに、各ディーラーのFortiGateにフォーティネットのセキュアSD-WANを導入し、同社のすべてのネットワークエッジにおいてセキュリティ ドリブン ネットワーキングを確立しました。

Williams氏は、「導入したおかげで、WANに対するアプローチがよりシンプルになりました。以前使用していたIPsecメッシュには拡張性がなかったため、時間の経過とともに管理が複雑になっていました。例えば、18番目の拠点を追加する場合、既存の17の拠点それぞれにVPN接続を追加し、新設した拠点にも18番目の接続を追加して、完全なメッシュを構築する必要がありました。しかし今は、各拠点は1つのVPNトンネルだけを管理すればいいのです」と言います。

さらに同社は、エンドポイントを保護、検知、対応を実行するFortiEDRを導入し、同社全体のマシンを保護しています。いくつかの軽妙なインシデントの発生を機に、Williams氏は優れたエンドポイントソリューションの必要性を再認識したと語ります。「私は、人的要因が最大のセキュリティリスクであると考えています。あらゆるファイアウォールを導入しても、人はフィッシングメールに騙されてクリックしてしまう可能性があります。しかし、FortiEDRプラットフォームのOSカーネル上での機能のおかげで安心感を得られました」

ビジネスへの効果（続き）

- MPLS接続をSD-WANに置き換えることで、年間12万ドルのコストを削減
- MPLSからSD-WANへの移行でROIを3年で達成する見込み
- 新規ディーラーの受け入れが容易になり、成長を合理化
- セキュリティの一元管理により従業員の業務効率が大幅に向上

ソリューション

- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiManager
- FortiAnalyzer
- FortiSIEM
- FortiEDR
- FortiMail
- FortiAuthenticator
- FortiToken
- FortiExtender

「MPLSはコストがかかります。MPLSのインフラをSD-WANに置き換えることで、年間約12万ドルのコストを削減できます」

– Dealerships社
ITディレクター
Shane Williams氏

Williams氏の小規模なチームは、FortiManagerとFortiAnalyzerの仮想マシン（VM）を使用して、ネットワーク全体の脅威の検出と対応を監視しています。「FortiManagerは、フォーティネット セキュリティ ファブリックの強力な一部です。当社のネットワークインフラストラクチャの管理において、私のお気に入りのツールの1つです。ファイアウォールの設定を変更する際、FortiManagerは潜在的なエラーをチェッ

クし、接続性の損失リスクを排除してくれるため、問題を解決するためにディーラーに出向く必要がなくなりました。また、FortiManagerは、ファイアウォールをリブートすることなく、大量の設定変更を一括で実装できるため、エンドユーザに対し透明性を確保することができます。さらに、FortiManagerは、各デバイスを一台ずつ更新するのではなく、デバイスをグループで一括更新できるため、100台以上のスイッチと100台以上のアクセスポイントのファームウェアを更新する場合、以前と比べると丸1日分の時間を節約することができるのです」

さらに、同社は、アイデンティティ管理とシングルサインオン（SSO）機能を提供するFortiAuthenticator、FortiToken ワンタイムパスワード（OTP）トークン、およびEメール通信を保護するFortiMailゲートウェイを導入しました。これらのソリューションはフォーティネット セキュリティ ファブリックに統合されており、同社全体の脅威の検知と対応の可視化を強化します。

また、他のフォーティネットのソリューションからもFortiSIEMセキュリティ情報およびイベント管理システムに自動的に情報が送信されるため、Williams氏の一日の業務は、FortiSIEMにログインしてインシデントログを確認し、セキュリティアラートには至らなかった異常動作を探すことから始まります。Williams氏は、「FortiSIEMは、まるでスイスアーミーナイフのような（切れ味の良い）セキュリティツールです。FortiSIEMは、インシデントとセキュリティ管理のための包括的なソリューションなのです」

「FortiSIEMは、何千ものログを収集し、読みやすい形式に分類し、特定のイベントに対して設定した基準に基づいてアラートを送信するという優れた機能を有しています。以前は、ネットワーク全体で何が起きているのかを一目で把握できる手段がありませんでした。サードパーティサービスプロバイダーに情報を求めても、すぐに得ることはできませんでした。今では、推測ではなく、実際にあらゆる脅威を可視化することができます。さらに、FortiSIEMに搭載された統合監視により、経営陣と管理者向けに、発生しそうなネットワークの問題をリアルタイムで自動的にウェブページ上に表示できるようになりました」

時間とコストを節約するより優れたセキュリティ

MPLSからSD-WANへの移行により、ホワイトファミリーディーラー社の運営経費は大幅に削減されました。「MPLSはコストがかかります」とWilliams氏は言います。「MPLSのインフラをSD-WANに置き換えることで、年間約12万ドルのコストを削減できます。約3年で投資回収（ROI）できると予測しています」また、Williams氏は、主に拠点から拠点への移動にかかる時間を大幅に削減することができたといいます。例えば、ディーラーにFortiSwitchを追加する場合、その拠点に発送するだけで済むと説明します。

「ほとんどのディーラーには、配線接続できる従業員がいます。そのため、FortiSwitchを出荷する前に、FortiManagerでそのプロビジョニングを行い、現地の担当者が接続すると、FortiSwitchが適切な設定のダウンロードを開始するようにしています。FortiManagerを早い段階から導入したため、SDブランチの導入にともなう膨大なネットワーキングやセキュリティ変更を、実際にディーラーに赴いて個々のデバイスにログインすることなく、1つの統括拠点から実行することができました」

同社は成長過程にあるため、デバイスのリモート展開は特に有益です。Williams氏は、「当社の役員は、常に新規ディーラーをポートフォリオに加える機会を求めています。当社は、ディーラーのインフラを標準化し、フォーティネットのセキュアSD-WAN、FortiSwitche、FortiAPを含むオンボーディングキットを作成しました。こうしておけば、ITリソースにほとんど負担をかけることなく、迅速に買収先と企業ネットワークをつなげることができます」

現在、ホワイトファミリーディーラー社では、可用性強化のために各拠点に2台目のFortiGate NGFWと、SD-WAN接続の障害時にインターネット接続を確保するFortiExtenderの設置を進めています。この事業の継続性を提供するソリューションは、売上高が最も高い（つまり、システムのダウンタイムによる潜在的な収益への影響が最も大きい）ディーラーですでに導入されています。

SDブランチのソリューションは、ホワイトファミリーディーラー社が求めるセキュリティレベルを満たすと同時に、取引先の自動車メーカーが求めるサイバーセキュリティの要件をもクリアしています。Williams氏は、「最近、ネットワークに侵入しようとする人が後を絶ちません。数年前までは、自動車ディーラーは攻撃者の眼中にはありませんでしたが、今では、サイバーセキュリティのリスクは大きな脅威となっています。しかし、フォーティネットのセキュアSDブランチソリューションのおかげで、夜もぐっすり眠れるようになりました」

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ