導入事例

ペンシルベニア州の学区がフォーティネットのセキュリティ ファブリックによりネットワークの可視化と制御を向上

イースト・ストロウドバーグの学区は、ペンシルベニア州北東部のポコノス地域に位置する216平方マイル（約559km²）の公立学校区です。この学区には、6つの小学校、2つの中学校、2つの高校、1つのサイバーアカデミーがあります。また、イースト・ストロウドバーグの敷地内には、バス車両のメンテナンスガレージなど、教育以外の施設も4つあります。この地区には6,500人の生徒がおり、1,200人の職員が勤務しています。

イースト・ストロウドバーグの学区の技術部長であるBrian Borosh氏は、「私たちも、他の学校と同様、ネットワークとITインフラに対するあらゆる脅威に直面しています。2015年当時の私たちの主な課題は、学校ではよくあることですが、不正デバイスのネットワークへの接続を阻止すること、そしてネットワークの可視性を向上することでした。その対応策として、初めてフォーティネットを導入しました」と語ります。

イースト・ストロウドバーグの学区は、フォーティネットとのパートナーシップの第一段階として、FortiNACネットワーク アクセス コントロール ソリューションを導入し、ネットワークの可視性を高めました。これにより、ITチームはネットワークから不正デバイスを即座に排除できるようになりました。次に、FortiNACとシームレスに統合されたFortiGate次世代ファイアウォール（NGFW）を追加し、エッジセキュリティとネットワークの可視性をさらに強化しました。FortiGate次世代ファイアウォールは、FortiAnalyzerの連携強化により、加えてネットワーク情報と動向を得ることができます。

進化する脅威に対応するために

2015年以降、脅威を取り巻く状況は日々進化し、地区のセキュリティニーズも変化しています。Borosh氏は、「私たちの主な目標は、あらゆる手段を講じて、攻撃者によるネットワークへの侵入を阻止することです。最近多発しているランサムウェア攻撃を最も警戒していますが、中には授業を受けたくないと思う生徒が仕掛けてくるサービス妨害（DoS）攻撃にも対応しなければなりません。最大のセキュリティ脅威が内部からもたらされるという点は、教育部門に固有の問題だと思います」と語ります。

イースト・ストロウドバーグの学区のネットワークアナリストであるDavid Cooper氏は、こう付け加えます。「ゼロデイ脅威は、新しい攻撃手法のBITB（Browser in The Browser）フィッシング詐欺のように、対応が特に大変です。サイバー犯罪者の手法はかつてないほど巧妙化しています。ですから、未知のシグネチャやプロファイルであっても、いかなる脅威を阻止できるセキュリティシステムが必要なのです」

EAST STROUDSBURG AREA SCHOOL DISTRICT

「セキュリティのアラートは常に発生しますが、必要な情報が手元になければ、対応すらできません。フォーティネットのソリューションで、まさにその情報を得られるのです」

– イースト・ストロウドバーグ学区
ネットワークアナリスト
David Cooper氏

詳細

顧客：ペンシルベニア州
イースト・ストロウドバーグ学区

業種：教育

所在地：米国

エンドポイント数：1,500

ビジネスへの効果

- 可視性と脅威への対応力を強化し、攻撃者が損害を与える前に阻止
- データ集計と詳細分析により、不審なネットワーク動作を検知し修復

フォーティネット セキュリティ ファブリックの構築

2015年以降も優れた製品とサポートを提供し続けるフォーティネットとの経験を踏まえ、イースト・ストロウドバーグの学区は、2020年と2021年に新製品のFortiEDRとFortiSIEMの導入、およびFortiGate次世代ファイアウォールのアップグレードを行い、フォーティネット セキュリティ ファブリック ソリューションを拡張しました。FortiEDRはエンドポイントの検出・対応を実行し、FortiSIEMはセキュリティ情報とイベント管理を実行する製品で、この2つを新しく導入しました。FortiGate次世代ファイアウォールのアップグレードは、同学区が冗長性の確保のためにデバイスを2倍に増やしたため、最新版への移行にいたりました。

同学区では、FortiEDRを使用して、教員用デバイスと学生用ワークステーションのリアルタイムの可視化、分析、脅威保護、修復を行い、進化する脅威の状況に対応しています。また、FortiSIEMを使用して、ネットワークとデバイス全体のデータを分析し、不審な動作やデータ流出をより的確に察知しています。FortiSIEMは、フォーティネットのプロフェッショナル サービス チームのサポートのもと導入されたため、同地区のITチームは最適なパフォーマンスを発揮するシステム統合と設定を実現しました。

高い対応性で脅威を減災

Cooper氏は「FortiEDRを1,500台の職員用エンドポイントとラボ用コンピュータを導入して以来、イースト・ストロウドバーグ学区のITチームは、システムの速度と対応性に感心するばかりです。私は、ネットワークに侵入してくる攻撃者を常に警戒しなくてはいけないので、FortiEDRは非常に頼もしい存在です」と言います。

「先日、私たちのデバイスの内1つが攻撃を受けましたが、FortiEDRはそれを直ちに検知し、侵害を発生源で自動的に停止させました。生徒や職員が不正なリンクをクリックしたり、危険なものをダウンロードしたりすると、FortiEDRはすぐにそれを検知し、自動修復してくれるため、私たちのネットワークは危険にさらされることはありません」FortiEDRは、DoS攻撃を仕掛けようとする学生をすばやく検知し、ネットワークから排除する上で、非常に役立っています。

さらにCooper氏は、同学区は、特にデータ流出の特定と阻止において、FortiSIEMは有益な効果をもたらしているとも語ります。「FortiSIEMによって、AD（Active Directory）サーバ、FortiGate次世代ファイアウォール、コアスイッチから収集したトラフィック履歴の詳細な調査・分析によって、データの流れを正確に把握でき、不審な動作を特定することができます。近々、FortiNACのデータも統合して、ネットワーク全体のすべての情報を完全に把握できるようにする予定です。フォーティネットは新たなレベルの可視化と理解を可能にしてくれます。おかげで私たちはセキュリティ態勢を大幅に強化することができました」

同学区のITチームは、ネットワークトラフィック履歴をさかのぼって確認できることがFortiSIEMの強みであると言います。このソリューションは、複数のソース間のデータを自動的に統合するため、潜在的なセキュリティ問題の解決にかかる時間を短縮することができます。FortiSIEMの導入前は、ITチームの構成員は16人と比較的小規模であったこともあり、データセットの手動での統合など時間のかかる作業はほとんど実施できていなかったとのことです。「セキュリティのアラートは常に発生しますが、必要な情報が手元になければ、対応すらできません。フォーティネットのソリューションで、まさにその情報を得られるのです」とCooper氏は言います。

ビジネスへの効果（続き）

- 手作業によるセキュリティプロセスを削減し、同学区の小規模ITチームの時間を節約
- シームレスなセキュリティシステムの相互運用性により、自動化を強化し、インフラ管理を容易に

ソリューション

- FortiGate Next-Generation Firewalls
- FortiAnalyzer
- FortiToken
- FortiNAC
- FortiSIEM
- FortiEDR

「フォーティネットは、私たちが目指すべき方向性の選択肢を広げてくれます。フォーティネットの製品カタログは、セキュリティ、ネットワーキング、テレフォニーなど他の追随を許さないほど充実しています。私たちは次に何を目指すのか、その方向性はまだ定まっていませんが、フォーティネットが私たちの長期的なパートナーであることに変わりはありません」

– イースト・ストロウドバーグ学区
技術部長
Brian Borosh氏

シームレスなインフラ管理を実現する完全な相互運用性

イースト・ストロウドバーグの学区に導入された新システムは、単体でも大きな利点をもたらしますが、これらを連携させることにより、さらなる効果を得ることができます。同区では、6つのフォーティネット製品（ワンタイムパスワードアクセス認証に使用するFortiTokenを含む）を導入し、全システムに1つのユーザーインターフェイスを通じて相互運用可能なセキュリティ ファブリックを活用し、単一の管理ポイントで管理を行っています。

Borosh氏は、「ファイアウォール、エンドポイント検知・対応ツール、SIEMのソリューションが、それぞれ異なるベンダーから提供されている場合、管理が煩雑になってしまいます。しかし、フォーティネットは、私たちのネットワーク セキュリティシステムを一元化してくれるので、非常にシンプルに管理することができます。一元管理できるので、新製品や問題解決の問い合わせは、たった1つの窓口に連絡するだけでいいのです。セキュリティ ファブリックの相互運用性は非常に優れていますので、今後、さらにフォーティネットの製品を私たちのネットワークに導入していく予定です」と語ります。

また、同地区は、セキュリティ ファブリックが可能にする自動化のレベルも高く評価しています。Borosh氏は、「相互運用性は、より優れたセキュリティを実現します。例えば、攻撃者がネットワーク上にいる場合、FortiEDRはFortiGate次世代ファイアウォールを介してFortiNACに自動的に警告を発し、FortiNACは我々が調査している間に攻撃者をネットワークから排除してくれます。セキュリティ ファブリックのおかげで、以前よりはるかに優れた可視性と応答性を実現することができました」と語ります。

未来に向けた強力なパートナーシップ

フォーティネットとの長年の良好な経験から、Borosh氏とそのチームは、フォーティネットを単なる技術ベンダーではなく、真のパートナーとして認識するようになりました。イースト・ストロウドバーグの学区は、サービスサポートだけでなく、フォーティネット プロフェッショナル サービスを活用して、システムの最適化を図っています。Borosh氏は、「フォーティネットの自社製品に対する知識の深さは随所に見て取れます。私たちはその知識を享受したいと考えています。フォーティネットの専門家チームは、私たちの機能面への投資効果を最大限に引き出してくれる非常に頼もしい存在です」と言います。

今後、同学区は、フォーティネット製品の利用を拡大する計画です。計画の発端となったのがFortiGate次世代ファイアウォールのVPN（仮想プライベートネットワーク）機能です。新型コロナウイルスの大流行によりリモート学習や教育を大規模にサポートする必要があったため、この機能を試験的に導入しました。今後、Eメールのセキュリティとユーザー ID認証にフォーティネットの製品を導入することも検討しています。

Borosh氏は、「フォーティネットは、私たちが目指すべき方向性の選択肢を広げてくれます。フォーティネットの製品カタログは、セキュリティ、ネットワーキング、テレフォニーなど他の追随を許さないほど充実しています。私たちは次に何を目指すのか、その方向性はまだ定まっていませんが、フォーティネットが私たちの長期的なパートナーであることに変わりはありません」と結論付けました。

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