

CASE STUDY

FortiSASE を利用して、 リモート従業員のデータと、 ロングビーチ地区の恵まれない 住民を保護

「FortiSASE Secures Remote Employee's Data and Long Beach's Most Vulnerable Residents」事例の抄訳です。

1940年代のカリフォルニア州ロングビーチでは、メンタルヘルスの支援を受けることが困難でした。さまざまな問題を抱える家庭で、子どもたちはしばしば問題の渦中に巻き込まれ、一部の学生は、不安や恐怖、さらに暴力を受けながら地域の学校に通っていました。一方で、所得が低い住民の場合、通常、こうした問題に対する支援が行き届いていませんでした。

The Guidance Center は、このような状況を受けて、公立学校の教師とカウンセラーの先見的なグループによって設立されました。70年以上たった現在、この非営利団体は、地域コミュニティの恵まれない子どもたちに対してエビデンスに基づくメンタルヘルスサービスを提供しています。このプログラムのサービスは長年、地域の子どものメンタルヘルスの改善を支援し、大きな成功を収めてきました。

この舞台裏では、3人からなるITチームが「ヒポクラテスの誓い（医師の倫理）」に相当する誓いを守っています。ITディレクターのIan Adduru氏は次のように述べています。「データが侵害された場合、クライアントや私たちの評判に大きな影響を与えます。収集したデータを保護するために取るべきことは何でも行う必要があります。子どもたちは助けを求めて私たちのところに来ており、彼らを保護するのは私たちの責務です。」

リスクを招くリモートワーカーの新しい環境

新型コロナウイルスのパンデミックが到来した際、The Guidance Centerの殆どのスタッフは在宅勤務を開始しました。すでに組織では、クラウド通信やファイルストレージとして、Microsoft 365のようなクラウドベースの医療アプリケーションを利用していました。Adduru氏は、「データを保管するローカルサーバーはすでに存在しません。私たちは、クラウドへのデータの移行を進めてきました。理由は、そこに未来があるからです」とコメントしています。一方で、当時の従業員は、オフィスのファイアウォールの内側の安全な場所にいました。その後、Adduru氏の精鋭チームは突然、200人のリモートワーカー、および彼らが仕事に必要なデータやネットワークトラフィックを保護する責務を負うことになりました。

Adduru氏は次のように続けます。「リモートワークの主な課題は、ユーザーの接続を保護することが困難なことです。」当初は、スタッフが喫茶店などの場所で公共のWi-Fiを利用して仕事をすると、心配していました。彼のチームは、公共のWi-Fiを介して暗号化されていないデータが共有されることを恐れ、組織のすべてのクライアントマシンのWi-Fiをオフにしました。「私たちは、CEOを含むすべての従業員に対して、イーサネットのルールで接続するよう求めました。Wi-Fiは皆が望んでいましたが、安全ではない接続による作業を許可するリスクは取れませんでした。」

解決策の模索を通して得られた教訓

The Guidance Centerが求めていたのは、ノートPCとクラウド間のデータを暗号化し、データの転送時に適切なセキュリティを確実に適用できるソリューションでした。実際、これは単に使用が便利という理由だけでなく、カリフォルニア州ヘルスケアサービス部門



「私たちの環境は安全だと考えています。私は、エンドユーザーに公共の場所で接続しないよう、契約書に署名してもらいました。一方で、仮に接続した場合でも、FortiSASEを利用することで、公共のWi-Fi経由でもリモートユーザーのインターネットアクセスは安全だと確信しています。」

– The Guidance Center,
ITディレクター、Ian Adduru氏

詳細

顧客: The Guidance Center

業種: 医療

所在地: カリフォルニア州、
ロングビーチ

エンドポイント数: 200

導入の効果

- クラウドとリモートユーザー間で、エンタープライズグレードのセキュリティを提供しつつ、高いパフォーマンスとユーザーエクスペリエンスを実現
- 転送されるデータの暗号化は、カリフォルニア州ヘルスケアサービス部門のコンプライアンス要件に準拠

のメンタルヘルスサービス局では、ローカルシステムと転送中の両方に、患者データの暗号化を求めています。Adduru 氏は、「スタッフが Wi-Fi を利用する際は、常にデータが暗号化されていることを確認する必要があります。Wi-Fi は公開されているため、ハッキングされます。ただし、データを常に暗号化していると、攻撃者は PII（個人識別情報）にアクセスできません」と説明しています。

The Guidance Center は、本社により大型のファイアウォールを設置するのはどうかというマネージドサービスプロバイダー（MSP）からの提案を検討しました。Adduru 氏は、「しかしながら、リモートユーザーのクラウド接続が本社環境に依存するのでは意味がありませんでした。これは、単一障害点となる可能性があります。たとえば、建物が停電した場合、すべてのアクセスが遮断されてしまいます」と語っています。

当組織では、代わりに、SASE（セキュアアクセスサービスエッジ）ソリューションの展開を決定しました。Adduru 氏は、彼らの要件に対応できるとする 2 つの異なるベンダーと話をしました。「両社とも私たちのデータを暗号化すると主張していましたが、ある 1 社の IPsec 接続を見てみると、暗号化ではなく、単に DNS を変更しているだけでした。別の 1 社は、デフォルトで暗号化されていましたが、ユーザーが暗号化を回避するためのバックドアを備えていました。このベンダーはそれを否定しましたが、私たちは検証中にバックドアの存在に気付きました。各プロジェクトでは、一定のコストと展開に 1 か月以上の時間を費やしましたが、検証では彼らが主張するようには機能しないことが判明しました」と説明しています。

Adduru 氏が、フォーティネットの迅速で簡単なリモートセキュリティのアプローチである FortiSASE を見つけたのはこのタイミングでした。FortiSASE は、フォーティネットが運用する FWaaS（Firewall-as-a-Service：サービスとしてのファイアウォール）で、お客様は、Web セキュリティやアプリケーション制御のように、ポリシーを導入して維持するだけで済みます。Adduru 氏のチームは、FortiSASE を徹底的にテストし、その結果に満足しました。

FortiClient：信頼性の高い暗号化

Adduru 氏のチームは、臨床医とスタッフメンバーの各ノート PC に、FortiClient のエンドポイント保護を導入しました。ユーザーがクラウドアプリケーションに接続すると、ユーザーのシステムで、FortiSASE への暗号化されたトンネルが確立され、その後、SaaS ソリューションへの HTTPS 接続が確立されます。

Adduru 氏は、「フォーティネットはデータを真に暗号化しており、ユーザーは迂回して危険な Wi-Fi 接続を確立することはできません。FortiClient により、ユーザーのデバイスと FortiSASE ネットワーク間の VPN 接続が確立されることで、インターネットを通過する際のセキュリティを維持および適用することができます。テストの結果、FortiSASE を利用することで、メンタルヘルス局から、転送中にデータが暗号化されているか尋ねられた場合、自信を持って「はい」と回答できることが明らかになりました」とコメントしています。

FortiSASE：高性能なクラウドベースの FWaaS（Firewall-as-a-Service）

Adduru 氏は次のように話します。「パフォーマンスは、展開する前の主な懸念点でした。私は、FortiSASE を介して SaaS アプリに接続してもらおうと、ユーザーの接続に影響が出るのではないかと考えていました。しかし、現在のところ「YouTube をブロックしないでほしい」などのコメント以外に、フィードバックは受け取っていません。エンドユーザーは、セキュリティソリューションの存在に気付いていないようで、これは完璧に機能していることを意味します。」

また、本ソリューションの「as-a-Service」としての部分も、Adduru 氏と同チームにとって非常にうまく適合しました。Adduru 氏は、「FortiSASE はクラウド上にあるため、オンプレミスのファイアウォールと比較して管理やパッチの適用が容易です。機器へのパッチの適用はフォーティネットが行います。各個人のオフィスに、セキュリティデバイスを物理的に追加する必要がある場合、それらのデバイスの管理には膨大な時間がかかります。デバイスが古くなったとベンダーが判断した場合、私たちは新しい更新やデバイスを展開する必要があります」と指摘しています。

最後に、ユーザーセグメンテーションが容易なため、IT チームは、セキュリティを強化し、より効率的なネットワークを構築できます。Adduru 氏は次のように述べています。「あるとき、私たちが YouTube をブロックすると、皆から IT 部門にクレームが来ました。私たちは、

導入の効果（続き）

- IT チームと経営陣は、コミュニティの恵まれない子供たちのデータを効率的に保護していると確信

ソリューション

- FortiSASE
- FortiClient

「パフォーマンスは、展開する前の主な懸念点でしたが、フィードバックは受け取っていません。エンドユーザーは、セキュリティソリューションの存在に気付いていないようで、これは完璧に機能していることを意味します。」

- The Guidance Center、ITディレクター、Ian Adduru氏

The Guidance Center のノート PC を利用するユーザーに、エンターテインメントや個人的な目的で使用をしてほしくありません。一部のユーザーは、特定のサイトにアクセスする正当な必要性があります。たとえば、HR 部門やマーケティング部門は、ソーシャルメディアにアクセスする必要がある場合があります。FortiSASE を利用することにより、これらを別のグループに簡単に配置し、他のグループに対する制限を適切に管理できます。」

最終的に、FortiSASE の総保有コスト (TCO) は、The Guidance Center が検討した他のソリューションの半分以下だと Adduru 氏は推定しています。ユーザーがアクセスすべきでないサイトをブロックする場合を除き、組織のエンドユーザーが存在を意識することはありません。

最も重要な点として、Adduru 氏は、「私たちの環境は安全だと考えています。私は、エンドユーザーに、喫茶店や空港などの公共の場所で接続しないよう、契約書に署名してもらいました。一方で、仮に接続した場合でも、FortiSASE を利用することで、公共の Wi-Fi 経由でもリモートユーザーのインターネットアクセスは安全だと確信しています」と締めくくっています。コミュニティの恵まれない人々を保護する責任を負っている組織にとって、このような確信は不可欠です。



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