事例

FORESCOUT
Active Defense for the Enterprise of Things™

South Central Power Company

Forescoutを活用して自社環境を可視化し、コンプライアンス対応とゼロトラストネットワークセグメンテーションを実施した電力会社の事例

60万ドルを超える節減効果
導入後3年間のROI

1週間
接続デバイスすべてを1週間で特定

5ヵ月以上短縮
資産インベントリ作成所要期間

業種
電力/エネルギー

事業環境
5か所の拠点で無線/有線デバイス1,400台が稼働。従業員数：250名

課題
- ネットワーク接続デバイスすべてを可視化できていない
- ネットワークの物理的セグメンテーションに起因する死角
- PCIおよび重要インフラ関連規制への準拠
- セキュリティツールの階層化および異種ベンダー製品の併用による防御策が正しく機能しているか確信がもてない
- 業務に支障を来たさずにポリシーを適用したい

概要
South Central Power Company（SCP）は会員制の電力企業で、米国オハイオ州にある24の郡で12万以上の個人世帯、法人および製造業の顧客に電力を供給しています。同社は、デバイスの常時可視化、ネットワークアクセスコントロール（NAC）およびネットワークセグメンテーションの実施にあたり、複数のベンダー製品を併用する代わりにForescoutプラットフォームを導入しました。Forescoutソリューションを導入した結果、デバイスの100%可視化・コントロールだけでなく、簡単かつ迅速にゼロトラストネットワークセグメンテーションを設計・実施でき、予想以上の効率化を図れました。金額に換算すると、3年間で60万ドル相当の節減が見込めます。

業務上の課題
「我々に必要だったのは、明確な可視性だけでなく、現行セキュリティツールの有効性を再確認してくれる兄貴分のような存在でした。セグメンテーションの面でも支援が必要でした」
South Central Power Co. アプリケーション開発・アーキテクチャ担当ディレクター Jeff Haidet氏

SCPでは多層防御や業界最高レベルのセキュリティツールを組み合わせたマルチベンダー型セキュリティスタックを展開していましたが、ネットワーク接続デバイスの数を把握しきれずにいました。個人情報（PII）や業務オペレーションを保護しつつPCI基準に準拠するには、同社のベンダー混在型ネットワークに接続するあらゆるモノを常時識別し、セグメント化してコンプライアンス対応を実施する手段が必要であり、社内セキュリティチームもその事実を認識していました。また、自社環境の各種セキュリティツールが発信する情報が正確であり、期待どおりに動作していることを検証するための手段も模索していました。担当者はさらに、社内ネットワークの物理的な設計が原因でセキュリティ対策が制限されている恐れがあると感じていましたが、確認するすべがなく、より論理的なセグメンテーションの実施方法も見いだせずにいました。

今回導入した セキュリティソリューション

- Forescout eyeSight
- Forescout eyeControl
- Forescout eyeSegment
- Forescout eyeExtend for Carbon Black

ユースケース

- ネットワークアクセス コントロール
- IoT セキュリティ
- ネットワークセグメンテーション
- 資産インベントリ
- デバイスコンプライアンス
- セキュリティ オーケストレーション

導入効果

- 価値の早期実現：わずか数週間でデバイスの完全な可視化および分類が100%完了
- ネットワーク接続するモノすべてを常時、包括的に可視化
- 手間のかかる手動管理に代わる、正確なリアルタイム資産インベントリシステム
- トラフィックフローの明確な把握およびポリシー変更シミュレーションにもとづくゼロトラストネットワークセグメンテーションの簡素化・迅速化
- ベンダー中立的な可視化により、ネットワークハードウェア切り替え時のペナルティ発生を防止
- 社内環境の監視による各種セキュリティツールの動作確認
- ゼロトラスト NAC による不正 / 準拠違反デバイスのブロック
- 可視化とコントロールにより、セキュリティオペレーションチームとネットワーク担当チームの日常業務を支援
- 優れた費用対効果：3年間で612,500ドル相当の節減見込み

Forescout を採用した理由

外部第三者による侵入テストの結果、可視性と NAC の改善が必要であることが改めてわかり、テスト担当者より Forescout の導入を強く推奨されました。SCP のアプリケーション・セキュリティマネージャー Jeff Haidet 氏は、次のように述べています「テスト開始時に Forescout プラットフォームが導入されていたら、侵入を検知・予防できていただろう」とも示唆されました。この心強い提言を受け、同社は Forescout ソリューションの検討をさらに進め、細部にわたる概念検証を実施しました。「可視化とコントロールに関するセキュリティギャップを解消する Forescout プラットフォームの威力、そして業務を妨げずにセグメンテーション不備を修復する eyeSegment の機能を目の当たりにした瞬間に、これこそ我々が求めていたものだ、とわかりました。当社では常にネットワークハードウェアを入れ替えたり更改しているため、ベンダー中立性という点も大きな魅力でした」

業務における効果

包括的な可視化で資産インベントリへの注意を喚起し、不備を修復

Forescout プラットフォームを起動してわずか数時間でネットワーク環境をきめ細かく可視化できたため、同社のセキュリティチームはさらに1週間、実行を継続しました。その結果、合計1,400のエンドポイント（社員1人あたり平均7〜8台）が特定され、経営幹部に大きな驚きをもたらしました。
さらにデバイス全体の85%が自動分類され、残りのデバイスも短時間で分類が完了しました。Forescout プラットフォームがなければ、同社の5拠点で使用されているデバイスすべての場所を特定して分類するのに最低6ヵ月はかかっていたでしょう。包括的かつリアルタイムの可視化を実現できたため、紙ベースで正確性に欠けるこれまでの資産インベントリ管理から脱却でき、機器のオンボーディング / オフボーディングプロセスも大幅に改善しました。

業務を中断せずにゼロトラストセグメンテーションを実施

セグメンテーション強化にあたり、Haidet 氏および担当チームは Forescout eyeSegment を活用しました。Haidet 氏は、次のように述べています。「eyeSegment でトラフィックフローをマッピングし、ネットワーク上で相互通信すべきデバイス、ユーザー、サービスを特定しました。セグメントを物理的ではなく論理的に定義することで、それぞれの挙動を素早く可視化できます。たとえばデバイスグループが2つあって、ゲートウェイを介さずに通信して情報を送受信している場合、送信元スイッチポートは検出されても送信先スイッチポートが検出されないケースがあります。こうした事実も eyeSegment のおかげで明らかになったため、該当箇所を可視化するためにゲートウェイを移動する措置を実施しました。また、業務を妨げない形で物理的セグメンテーションを再設計する上でも eyeSegment が役立ちました。ポリシー適用前にシミュレーションを行い、不具合を起こす恐れがないかを確認して微調整し、必要に応じてシミュレーションを繰り返すこともできます」

監視によるデバイスコンプライアンスとセキュリティツールの動作確認

SCP ではセキュリティ対策に Forescout プラットフォームを活用してエンドポイントを常時監視し、適切なマルウェア対策エージェントが稼働しているか、パッチが正しく適用されているか、重篤な脆弱性が発生していないか、Dropbox などの未承認アプリが稼働していないか、といった点を検証しています。社内ポリシーに違反しているデバイスは、Forescout プラットフォームが社内ネットワークへのアクセスをブロックする、またはゲストネットワークに回送します。Haidet 氏は、次のように述べています。「コロナ禍により大半の従業員が VPN 経由の在宅勤務となったことで、デバイスコンプライアンスの常時監視がますます重要になりました。Forescout を活用することで、社内の階層型セキュリティスタック（ファイアウォールからスイッチ、ウィルス対策に至るまで）の個別要素が想定どおりに動作しているか、ダブルチェックすることもできます」

デバイスの可視化・管理からコントロール措置の発動、ゼロトラストセグメンテーションの素早い実施に至るまでの各種機能をForescout以外で実現するとしたら、複数のツールが必要になっていたでしょう。Forescoutに一元化することでコストを大幅に節減できました」

— South Central Power Co.
アプリケーション開発・
アーキテクチャ担当ディレクター
Jeff Haidet氏

協働を通じた真のパートナーシップおよび確固たる事業価値

South Central Power Companyでは、セキュリティオペレーションチームとネットワーク担当チームの両方が日々の業務にForescoutプラットフォームを活用しています。Haidet氏は、次のように述べています。「Forescout側のチームも社内チームの一員のように貢献してくれています。ツール購入時にベンダーと信頼関係を築くのは簡単ではありませんが、Forescoutチームとはしっかりした協力体制が確立しています。まさにホームラン級と言えるでしょう。社員わずか250名の当社はForescoutにとって小規模で取るに足らない顧客かもしれませんが、真摯な姿勢で手厚いサポートを提供してくれるため、まるでFortune100レベルの大企業になったような気分です」

Haidet氏は、IDCが作成した顧客向けROIツールを用いてForescout導入による経済的効果を試算しました。費用対効果を分析した結果、3年間で612,500ドル相当の節減効果（ITスタッフの生産性改善、リスク防止、業務効率化によるメリット、およびITインフラコストの低減）が見込めることがわかりました。Haidet氏は同じ課題に悩む業界の仲間に向けて「Forescoutはベンダー中立的で、監視を一元化できるワンストップソリューションです。ネットワーク規模が大きいほど、コスト削減効果も拡大し、ビジネスケースを立証しやすくなるでしょう」と話しています。

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

詳細は Forescout.com をご覧ください