SUNY オールド ウェストバリー校は、シスコのクラウド E メールセキュリティにより、Office 365 セキュリティを強化しています

ニューヨーク州立大学 (SUNY) の 64 のキャンパスの 1 つであるオールド ウェストバリー校は、教員、スタッフ、学生団体の多様性と功績、および学術の革新、アクセス、社会正義への長期的なコミットメントを誇りとしています。マンハッタンの中心部から 20 マイルほど離れたロング アイランドで 50 年以上前に設立されたこの大学は、米国の『ニューズ & ワールド レポート』誌で、アメリカの最も多様性のある教養大学に常にランクインしています。

大学は今後 50 年間、最高品質を保ち、学生のニーズや要望に対応し、受講者やコミュニティにとって先進的な教育への継続的なアクセスを提供することに専念します。SUNY オールド ウェストバリー校の情報技術サービス ディレクターおよび最高情報セキュリティ責任者 (ISO) である Milind Samant の場合、テクノロジーはこれらの目標を実現する共通のテーマですが、拡張するユーザ ベースと歩調を合わせるにはセキュリティと拡張性を備えている必要があります。

概要

お客様の名前：
ニューヨーク州立大学 (SUNY) オールド ウェストバリー校

サイズ：
約 4,400 人の学生と 300 人以上のフルタイムおよびパートタイムの教員

業界：
高等教育

ロケーション：
ニューヨーク州ロング アイランド、オールド ウェストバリー

「Cisco クラウド E メール セキュリティと AMP を使用したおかげで、毎晩よく眠れるようになりました。CES がすべて管理してくれるので、CEO や VP からの「このメールは正当なものか?」や「この添付ファイルを開くべきか?」といった問い合わせに夜まで対応する必要がなくなりました」

Milind Samant
SUNY オールド ウェストバリー校の
情報技術サービス ディレクターおよび
最高情報セキュリティ責任者 (ISO)

クラウド ベースの電子メールへの依存の増大

学生および教職員の増加に伴い、Samant 氏と彼のチームは、セキュアなコラボレーション、新しい Go Green イニシアチブ、および時間や場所を問わず情報にすぐにアクセスできるという学生の期待をサポートする革新的な方法を探していました。「これらの課題にそれぞれ対応するために電子メール システムに依存することがますます多くなり、システムが過負荷になっていました」と ISO の Samant 氏は述べています。

Go Green に取り組む前は、コミュニケーションの選択肢と言えば、個人的な電子メールと、電子メールの量を抑える通常の郵便でした。「現在、大学と学生、教職員との公式の通信は、Microsoft Office 365 に基づく公式の SUNY メール システムを使用して行われています。このシステムは、学資援助の通知、講義のスケジュール、成績まであらゆるものを処理します」と Samant 氏は述べています。「Go Green に取り組むと、電子メールの量が 2 倍以上になり、すべてのアラートと通知は電子メールで通信されるようになりました。それは高速で信頼性の高いものでなければなりません。たとえば、預金に残高があり、モバイル デバイスやラップトップでその情報にアクセスしたい場合は、学生はすぐに電子メールで通知を受け取ることを望んでいます」

電子メールの量の増加に伴い、攻撃ベクトルとして電子メールを使用するスパムやその他の脅威が増えるようになりました。「Office 365 の電子メール セキュリティにもかかわらず、特に通信する必要がある情報の量と種類、しかもその大部分には個人識別情報 (PII) が含まれることを考慮すると、システムは期待したほど安全ではありませんでした」と Samant 氏は説明します。「多くの不正なメッセージが届くようになり、サービス デスクは悪意のある URL、ゼロデイ攻撃、およびランサムウェア感染の事例を含む連絡を受けていました」

管理者の特定の上級職員を対象としたスプーフィング メールが確認されるようになると、ISO は組織が重大な危機に直面しており、電子メール セキュリティを強化する必要があることを理解しました。「Office 365 は優れた電子メール プラットフォームを提供しますが、クラウド ベースの電子メール ソリューションには、より堅牢なセキュリティ機能が必要でした」と Samant 氏は説明します。「私たちは Cisco クラウド E メール セキュリティを選択しました。なぜなら、これは絶えず増加するリスクに対して電子メール保護を強化するだけでなく、Office 365 とシームレスに統合するからです。2 つが組み合わさることで、増大した電子メールの負荷を適切に処理するために必要な電子メール プラットフォームと、そのプラットフォームを保護するために必要な堅牢なセキュリティを手に入れました」

強化されたセキュリティのソリューション

SUNY オールド ウェストバリー校は、組織的なプロセスに従って Office 365 のセキュリティを強化するためのオプションを評価しました。Gartner や Forrester の調査を検討し、電子メール セキュリティ分野での上位 5 社を調べ、機能を比較して、大学の固有のニーズに適していると考えられる 3 つのソリューションに絞り込みました。ライセンスと価格設定も、判断に重要な要素でした。

「学生や教員は 1 学期以上不在にする可能性があるため、メールボックス ベースのライセンス モデルはふさわしくありません」と、Samant 氏は言います。「平均で、通常の企業よりも非アクティブなメールボックスが多く、また学生は多くの場合 1 年以内に戻ってくることがわかっているため、アーカイブを行いません。したがって、メールボックス単位のライセンスは私たちには向いていません。シスコのライセンス モデルは、高等教育向けの最適なソリューションです。支払う料金は、通過しているトラフィックの量、つまりユーザの数ではなく実際の使用量に基づいています」

SUNY OW の ITS ディレクターは、クラウド ベースの電子メール プラットフォームと適切に連携する、完全にクラウド ベースのソリューションを求めていました。「電子メール システムがクラウド化されているため、使用する電子メール セキュリティ ソリューションもクラウド化されていることを確かめようと思いました。電子メール トラフィックを、オンプレミスのデータセンターに到達するようにルーティングしてから、クラウドにルーティングし直すことはしたくなかったため、オンプレミス ネットワークとの連携は求めていませんでした」と Samant 氏は説明します。

初期の評価に基づいて、Samant 氏と彼のチームはシスコをさらに詳細に調査し、価値の検証 (POV) を設定することにしました。

「POV の期間中、シスコの皆さんは初期のセットアップの時点から申し分ありませんでした。セールス エンジニアの Rose とアカウント マネージャの Cindy は非常に知識が豊富で、評価全体を通してサポートしてくれました。その経験に感動しました」と Samant 氏は言います。「Cisco クラウド E メール セキュリティは、迅速に導入することができ、ビジネス メールの侵害からの防御やスプーフィングによるリスクの排除など、必要な保護を提供することがわかりました。このソリューションには、正当なメッセージを通過させるための抑制と均衡が備わっており、偽造の疑いがある電子メールについて注意を喚起して、ユーザに潜在的なリスクを警告することができます。また、このソリューションは、独自のライセンシング方法によって、コスト削減が可能になるため、次年度に向けて優先的に考慮することができました」

高度な脅威からの保護

Milind Samant 氏と彼のチームは、Cisco クラウド E メール セキュリティの使用を迅速に開始し、ソリューションを環境に適合させることができました。「セットアップの容易さや毎日の管理とオーバーヘッドはごくわずかで、GUI では実際に学習曲線が減少しています」と、Samant 氏は言及しています。「数時間で、ほとんど準備が整い、コントロールやカスタマイズはすでに必要なだけ行われています。Office 365 を使用すると、エンドユーザのメールボックスに到着する電子メールに対するコントロールは制限された基本レベルのものです。Office 365 を CES で補完すると、ポリシーとルールを使用して電子メールを管理する高度な機能を利用できます。

適切な電子メールを SUNY OW の人々に届けることができます。それと同時に、疑わしい電子メールを 3 分または 3 時間隔離して適切に検出、修復、削除することができます。そのオプションは素晴らしいとしか言い様がありません」

「Cisco クラウド E メール セキュリティにより、事後対応ではなく、先を見越して対応することが可能になりました。代えがたい製品です」

Evan Kobolakis、
SUNY オールド ウェストバリー校、
情報テクノロジー サービスの
CIO および AVP

チームの独自のカスタム シグニチャに加えて、Cisco クラウド E メール セキュリティは、Cisco Talos が提供する組み込みの脅威インテリジェンスで継続的に更新されます。「Talos からのインテリジェンスは、電子メールを到着前でさえサニタイズするという素晴らしい仕事を行います。今まで酷使されていた SMTP ゲートウェイの負荷が減っています」と Samant 氏は述べています。Cisco クラウド E メール セキュリティ ソリューションには Cisco AMP（高度なマルウェア制御）が組み込まれているため、スペア フィッシング、ランサムウェア、暗号化ワームのような電子メール ベースの攻撃や、その他の高度な攻撃はもはや問題ではありません。「クラウド E メール セキュリティと AMP を使用したおかげで、毎晩よく眠れるようになりました。CEO や VP からの「このメールは正当なものか?」や「この添付ファイルを開くべきか?」といった問い合わせに夜まで対応する必要がなくなりました。CES が私たちの代わりにすべてを管理しています」

ITS ディレクターおよび ISO はさらに説明しています。「AMP は、電子メール内のヘッダーとメッセージを使用して金融詐欺をユーザに通知し、このメールは詐欺メールの可能性があることを警告します。メッセージは自動的にプロキシ サーバに送信され、そこでチェックされて、アクセスが阻止されるか、安全な場合はアクセスが許可されます」

スパムはあらゆる組織で増加する問題となっており、SUNY オールド ウェストバリー校も例外ではありません。「毎日平均で 412,000 通のメールを受信します。これには、シスコの Cisco E メール セキュリティ ソリューションが自動的にブロックしていて、私たちが気付いていないものは含まれていません」と Samant 氏は述べています。「これらの 412,000 通の電子メールのうち、266,000 通はスパムとして分類され、ブロックされます。さらに多くの電子メールが商用として分類され、ブロックされます。つまり、受信メールの 75 % が不正な電子メールということになります」

さらに、AMP はゼロデイ攻撃に対抗するのにも役立ちます。「私たちは、今でも Office 365 に組み込まれているセキュリティを最初の防衛層として使用していますが、あるときゼロデイが通過するとします」と、ISO の Samant 氏は説明します。「AMP を使用すると、レトロスペクティブ アラートを受信し、電子メールを迅速に検疫して詳細な調査を実施します。そして、Talos のグローバル脅威インテリジェンスの情報に基づき、電子メールを解放またはブロックすることができます」

このレベルのインテリジェンスと自動化は Samant 氏と彼の小さなチームにとって重要です。「Cisco クラウド E メール セキュリティは、管理に必要な時間 / 工数を大幅に削減しました」と、SUNY オールド ウェストバリー校のシステム エンジニアおよび Office365 管理者である Damian Obara 氏は述べています。

「私のチームには、レポート、ログ、および IP ブラックリストの確認に毎日時間を費やせるセキュリティ専門の担当者がいません。機能を比較しているときに、グローバル レベルで生じている事柄に基づいて適応できるソリューションが必要だと考えました。世界のどこかで何か悪いことが起こった場合、私たちの側で多くの時間をかけなくても、Cisco Talos が電子メール セキュリティを更新します」と ISO の Samant 氏は付け加えています。

Cisco クラウド E メール セキュリティと AMP により、Samant 氏とチームは多くの必要な可視性と制御を得ています。「今では、何が起きているかを理解できるため、コントロールすることができます」と Samant 氏は言います。

「Cisco クラウド E メール セキュリティと AMP により、事後対応ではなく先を見越して対応することが可能になりました。代えがたい製品です」と、SUNY オールド ウェストバリー校の情報テクノロジー サービスの CIO および AVP の Evan Kobolakis 氏は付け加えています。

クラウド ベースの未来

SUNY オールド ウェストバリー校は将来に向け、ネットワークや PII を含む電子メール トラフィックの量を考慮して、秘密情報が悪用されるリスクをさらに軽減するために、Cisco Data Loss Prevention を検討しています。また、悪意のある接続が確立される前にブロックするため、不正なドメイン、URL、IP、およびファイルに対する防御の第一線を提供するセキュアなインターネット ゲートウェイである Cisco Umbrella も評価しています。「電子メール セキュリティを強化したので、ネットワーク攻撃に対するより優れた防御も検討する必要があります。Cisco Umbrella は次のステップとして当然です」と Samant 氏は述べています。

クラウドへの移行は骨の折れる作業になるかもしれませんが、Samant 氏は励ましの言葉を述べています。「誰もが必ず尋ねる質問は、「クラウド ベースのソリューションの安全性をどのように確保するのか?」というものです。私も同じ懸念を抱いていましたが、シスコを調べると、導入、調整、監視以外に、多くの作業は必要ないように見えました。シスコは、ベスト プラクティスを適用したソリューションを構築しています。それは「ターンキー（すぐに使える）」ソリューションであるため、必要な保護を得ることができ、毎日の管理と管理オーバーヘッドについて心配する必要はありません」

製品およびサービス

- Cisco クラウド E メール セキュリティ
- Cisco AMP（高度なマルウェア制御）

C36-739233-00　06/17