ケーススタディ

オーストラリア国立大学、ゼロトラストでより安全なキャンパスを構築

Gigamonを導入したことで、場当たり的、または手当たり次第に脆弱性を追跡するのではなく、戦略的なアプローチでサイバーセキュリティに取り組めるようになりました。Gigamonは、ネットワークレジリエンスを構築し、攻撃の対象領域を減らし、攻撃しにくいIT環境を構築するために必要なデータを提供してくれます。

SUTHAGAR SEEVARATNAM氏
オーストラリア国立大学CISO

課題

- ゼロトラスト・ネットワーク・アーキテクチャのための正しい基盤を確立する
- ハイブリッドクラウド環境のセキュリティ確保
- 学生、職員、大学のデータを保護するためのサイバーセキュリティ態勢の整備

ソリューション

- GigaVUE® Cloud Suite
- GigaVUE HCシリーズ
- GigaVUE-FM
- GigaSMART®

顧客のメリット

- 60サイトにわたるデバイス、ネットワーク、トラフィックの詳細な可視化を実現
- ゼロトラスト環境のための強固な基盤を確立
- 導入の容易さと会社全体の可視化

お客様について

オーストラリア国立大学（ANU）は世界で最も優れた大学のひとつです。オーストラリアの首都キャンベラに位置するANUは、4,500人の学術・専門スタッフを擁し、約10,000人の学部生と約11,000人の大学院生にサービスを提供しています。2018年の時点で、7つのアカデミック・カレッジと18億ドルの基金があります。Suthagar Seevaratnam氏は同大学のCISOであり、就任してから3年になります。

経営課題

同大学は2018年にデータ漏洩に見舞われ、Seevaratnam氏とそのチームは、原因はフィッシングメールの可能性が高いことを突き止めました。この攻撃は、大学のセキュリティ体制を改善するための警鐘となりました。日本のITサービス企業であるNTTデータが発表した2020年のグローバル・インテリジェンス脅威レポートによると、教育機関は最も攻撃を受けている分野のひとつです。同レポートによると、2019年に教育部門が受けた攻撃は全体の38%で、政府部門に次いで2番目の多さでした。Seevaratnam氏は、サイバー攻撃が増加していることを認め、大学のセキュリティ戦略を強化するために積極的な措置を講じました。

Seevaratnam氏は、ランサムウェアとデータ流出の両方を組み合わせた攻撃を特に懸念していました。一方で彼は、1種類の攻撃に注目するだけでは不十分であることも知っていました。サイバー攻撃が高度化し、大学のITインフラが複雑化する中、Seevaratnam氏はゼロトラスト・アプローチが最善の道だと判断しました。

解決

様々なベンダーを検討した結果、Seevaratnam氏は、大学のネットワーク・アーキテクチャをゼロトラストの戦略的方向に導く中核プラットフォームの1つとしてGigamonを選択しました。多くの大学の典型的なハイブリッド環境では、これが理にかなっていました。ゼロトラストの基本的な信条は、「決して信用せず、常に検証する」ことであり、これはネットワークだけでなく、ユーザーやデバイスにも当てはまります。

Gigamonは、組織がデバイス、ネットワーク、トラフィックにおける可視性のギャップを埋め、隠れた脅威や新たな脅威をよりよく検出することを可能にします。ANUのネットワーク上で、構内やクラウド上で動いているすべてのデータを深く観察できるため、大学は耐障害性を強化し、攻撃を寄せ付けないようにすることができます。

ANUでは、2か所のデータセンターと60以上の拠点に350台以上のGigamonデバイスを配備し、ANUアクトン・キャンパスをはじめ、オーストラリア全土の多数の拠点をカバーしています。また、仮想ネットワーク・ターミナル・アクセス・ポイント（TAP）を導入し、26台以上のVMware ESXiホストに可視化機能を提供しています。GigaSMARTは、アプリケーション・トラフィックの可視化を向上させるため、より深いインテリジェンスによってこれらの機能を拡張します。GigaSMARTに組み込まれたセンサーはNetFlowとアプリケーション・メタデータを脅威ハンティング・ソリューションに供給し、学校がアプリケーションをどのように使用しているかについての更なるインサイトを提供します。

Gigamonのおかげで、ANUは可視化のギャップを埋め、East-Westトラフィックを含むあらゆるデバイス、ネットワーク、トラフィックタイプのアクティビティを追跡できるようになりました。GigaSMARTからの詳細なデータは、資産の発見およびサイバーセキュリティの自動化ツールに供給され、ネットワーク上のすべての接続されたデバイスを識別し、セグメント化し、コンプライアンスを実施します。このソリューションを組み合わせることで、潜在的に脆弱なデバイスが大量に発見されました。モノのインターネット（IoT）機器、医療用IoT機器、保守終了（EOL）オペレーティングシステムを搭載した機器などです。大学の環境は常に変化し、成長しているため、ANUはGigamonと提携して、GigamonがANUに提供する可視化ソリューションを最適化し、拡大するために、エンジニアを常駐させています。

Gigamonは、主要なネットワーク分析ソリューションであるExtraHopとも統合されています。これは、セキュリティチームが継続的なデジタルトランスフォーメーションを可能な限り成功させるために、パフォーマンス評価指標のベースラインを確立するのに役立っています。

メリット

「Gigamonを導入したことで、場当たり的、または手当たり次第に脆弱性を追跡するのではなく、戦略的なアプローチでサイバーセキュリティに取り組めるようになりました。これにより、ネットワークレジリエンスを構築し、攻撃の対象領域を減らし、攻撃しにくいIT環境を構築するために必要なデータを提供してくれます」とSeevaratnam氏は語りました。

Gigamonは、サイバーセキュリティ体制を強化するために必要な詳細な可視化と忠実度の高い脅威検知を大学に提供します。この統合ソリューションは、ANUがゼロトラスト・アプローチを導入するための強固な基盤を提供するもので、ネットワーク・アーキテクチャの観点からはまさにパラダイム・シフトとなります。この最新のセキュリティ・スタックによって実現されたネットワーク監視技術により、ANUは将来のインシデントを防止し、インフラを保護するために必要なツールを手に入れました。

Gigamon について

Gigamon のディープオブザーバビリティパイプラインは、ネットワークレベルの実用的なインテリジェンスを活用し、お客様のオブザーバビリティツールを強化します。この強力なコンビネーションを活用すれば、IT 組織は、セキュリティとコンプライアンスのガバナンスを維持しながら、パフォーマンスのボトルネックの根本原因をすばやく分析し、ハイブリッドおよびマルチクラウドの IT インフラストラクチャ管理に伴う運用コストを削減できます。その結果、先進的な企業はクラウドへの完全な転換を実現できます。Gigamon は世界中で 4,000 社以上の顧客にサービスを提供しています。これには Fortune 100 企業の 80% 以上、10 大モバイルネットワークプロバイダーのうち 9 社、世界中の何百もの政府および教育機関が含まれます。詳しくは、gigamon.com をご覧ください。

Gigamon®

本社
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

06.23_02