ケース スタディ

クラウド セキュリティを使ってユーザ、データ、オープン カルチャーを保護する最先端の研究大学

「Cloudlock の機能は非常に素晴らしいです。DLP から UEBA まで、クラウド環境に必要な可視性を実現し、その場所までセキュリティ ポリシーを広げることができました」

Aaron Baillio
オクラホマ大学
セキュリティ オペレーションおよびアーキテクチャ、マネージング ディレクタ

The UNIVERSITY of OKLAHOMA

組織のスナップショット

組織:
オクラホマ大学（OU）

所在地:
オクラホマ州、ノーマン

ユーザ:
36,000 - Cloudlock
6,000 - Umbrella

目標:
OU がキャンパス全体を Office 365 に移行する際、クラウド内とオンプレミスで機密性が高いデータや規制が厳しいデータを保護するための新しいセキュリティ アプローチが必要でした。

解決策:
Cisco Cloudlock
Cisco Umbrella

影響:

- 感染した一連のアカウントをすばやく修復
- マルウェア感染数を大幅に削減
- ブロックされた脅威の数が 1 時間あたり数千単位まで増加
- クラウド内のユーザ、データ、アプリケーションを保護
- セキュリティの管理や修復にかかる時間を削減

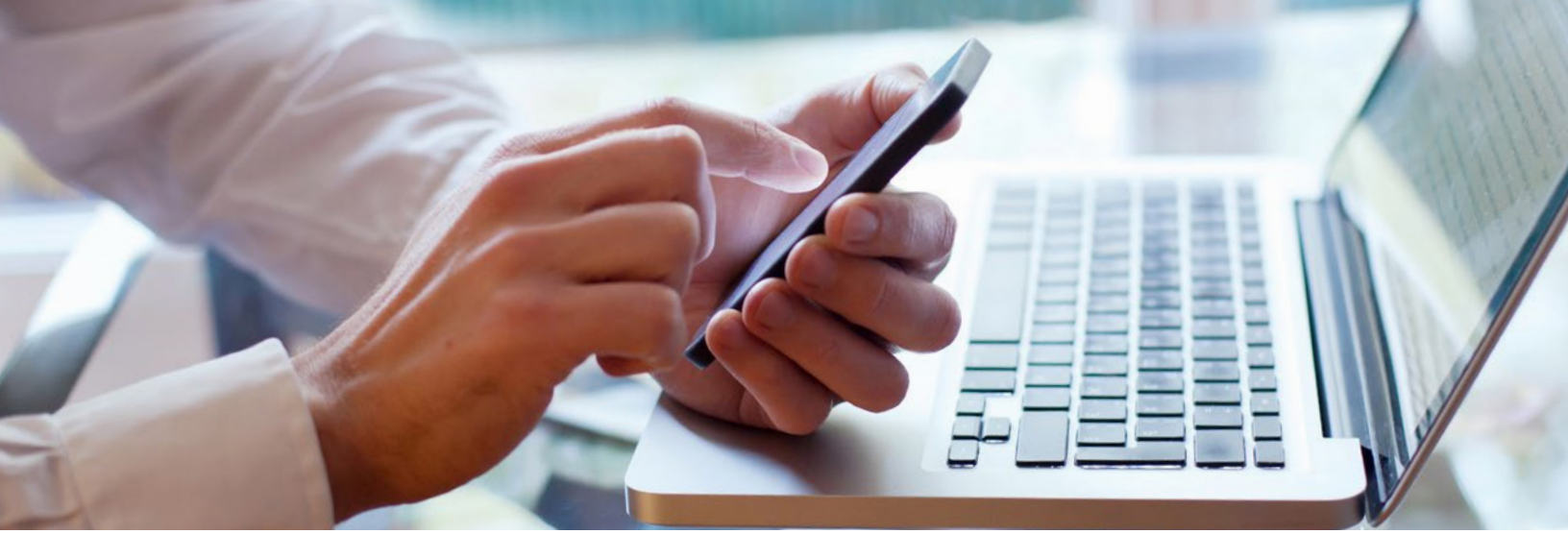
目標

マルチクラウド時代のセキュリティ

かつて数々のスポーツで全国制覇し、その名を知られていたオクラホマ大学（OU）は、グラウンド外でも世界的に有名な研究機関に成長しました。研究施設のキャンパスにおよそ 100 万平方フィート（約 9 万平方メートル）の公的機関および民間企業とのコラボレーション専用スペースを有する OU は、カーネギー教育振興財団によって研究活動分野のトップ大学に分類されました。

OU でセキュリティ オペレーションとアーキテクチャを管理している Aaron Baillio 氏は次のように述べています。「当校のミッションは、意見の交換を促進することです。これにはオープンなプロトコル、そしてクラウドとオンプレミス アクセスの適切な組み合わせが必要です。当校のユーザは、Dropbox、Amazon Web Services（AWS）、Salesforce、その他のアプリケーションを使って、クラウドを積極的に利用するようになってきています」。

大学が Office 365 に移行したときに、アカウントの感染の可能性について懸念が広がりました。OU は、センシティブな研究データに加え、HIPAA や PHI データを保護するために、クラウド環境の可視性を拡張する必要がありました。「当校の研究データは競争優位性があります。このデータを損失した場合、当校の評判に傷がつくだけでなく、大学は数千ドルのコストを負担しなければならず、契約や今後の研究機会を失う可能性があります」と Baillio 氏は述べています。



ソリューション

センシティブな研究データと生徒のアカウントを保護する

ユーザとデバイスからクラウド内のデータやアプリケーションを閲覧可能にするために、大学はクラウド アクセス セキュリティ ブローカ（CASB）ソリューションを調査しました。

Baillio 氏は次のように述べています。「当校が Cisco Cloudlock に関心を持ったのは、強力なセキュリティ、高等教育機関における幅広い経験、研究予算に適した価格設定、競合他社よりも豊富なカスタマイズ オプションに加え、ネットワーク上とネットワーク外のアクティビティに対応する API アプローチを備えていたからです。Cloudlock は、Dropbox などのクラウド アプリで法規制を確実に遵守するのに役立ち、HIPPA やその他の個人の医療情報が誤って公開されるのを防ぐことができます。Cloudlock はデータ流出回避のニーズに対応すると同時に、クラウド環境内のデータを管理する多くの規制の遵守も確実に実現します」。

マルウェアの増加に対応するため、OU は当初、複数の Web フィルタリング ソリューションを検討していましたが、それらのソリューションには、Umbrella の機能や脅威インテリジェンスが備わっていないことに気づきました。

Baillio 氏は次のように述べています。「Cisco Umbrella の良い点は、その多くをグローバルな DNS トラフィックから取得した実際のデータを利用し、シスコの Talos 脅威インテリジェンスも活用している点です。当校の生徒のアカウントは特に、マルウェアやランサムウェアにつながっている可能性のある悪意のあるリンクに脆弱ですが、今は Umbrella を使うことで、接続が確立される前にこれらの宛先をブロックできるようになりました」。

Cloudlock の実装後、OU は Umbrella をランサムウェア、マルウェア、フィッシング攻撃などのインターネット脅威を防ぐための最前線として追加しました。また、Umbrella 仮想アプライアンスを AD 統合と併せて実装し、ユーザのアクティビティに対する可視性を強化しました。

「Cisco Umbrella の良い点は、その多くをグローバルな DNS トラフィックから取得した実際のデータを利用し、シスコの Talos 脅威インテリジェンスも活用している点です」。

Aaron Baillio
オクラホマ大学、
セキュリティ オペレーション
およびアーキテクチャ、
マネージング ディレクタ

結果

クラウド アクティビティと脅威トラフィックの実用的な洞察

Baillio 氏は次のように述べています。「Cloudlock によってクラウド内のユーザとデータを把握できるようになり、感染した 200 近いアカウントをすぐにロックすることができました。このように、UEBA と IT の成果が早い段階で現れました。数日のうちに、アラート パターンによって、私達が確認していたのはいくつかの 1 回限りのインシデントではなく、繰り返される侵入アクティビティであったことが明らかになりました」。

Cloudlock で侵入の痕跡を示す異常なユーザ アクティビティをすばやく特定することで、OU はその送信元を特定し、影響を受けるアカウントを確実にブロックおよびリセットして、拡散を食い止めることができました。「Cloudlock によって迅速な調査と修復が可能になり、アクセスできなくなったり、ヘルプ デスクのサポートを必要とするユーザの数が減りました」と Baillio 氏は述べています。

Cisco Umbrella の導入によって、大学はランサムウェアを防ぐことができるようになりました。

Baillio 氏は次のように述べています。「Locky ランサムウェアの攻撃を受けた際、Palo Alto Networks のファイアウォールでは検出に 4 時間かかりましたが、アンチウイルス ソフトウェアでは 1 週間何も検出されませんでした。アウトバウンド トラフィックや攻撃に対する Umbrella の包括的な保護を導入してから、1 時間あたり 1,000 を超える脅威をブロックできるようになりました。一方、Umbrella を導入していない姉妹大学では、ネットワーク共有ファイルへの繰り返しの攻撃が続いています。OU ノーマン キャンパスでは、ランサムウェアは制度上のささいな問題となっています」。

OU で、IP 空間からの指揮および統制トラフィックが考慮される BitSight スコアが確実に改善していることは、マルウェアの数が大幅に削減していることを示しています。Umbrella 導入前のスコアは F でしたが、導入後は一気に C に上がり、さらに上昇を続けています。

Baillio 氏は次のように述べています。「全体的として、より適切なポリシー作成とアーキテクチャを伝える重要な洞察によってセキュリティの強化を図り、タイプ、重要度、および場所に基づいたデータ管理に関するポリシーの発行を開始できるようになりました。悪意のあるアクティビティのブロック、デバイスの保護、最も感染が進んでいるマシンの隔離と検疫、ライセンス契約の有無に関わらないすべてのクラウド プラットフォームでのセンシティブ データの安全な管理を実行できるようになりました」。

「Cloudlock によってクラウド内のユーザとデータを把握できるようになり、感染した 200 近いアカウントをすぐにロックすることができました。このように、UEBA と IT の成果が早い段階で現れました」。

Aaron Baillio
オクラホマ大学、
セキュリティ オペレーション
およびアーキテクチャ、
マネージング ディレクタ