PCI コンプライアンスの実現

業界をリードする Financial Tech 社は、中堅の金融専門業者向けにクラウドベースの買掛金および支払いの自動化ソリューションを提供し、不正行為に対する保護を保証しています。そのため、現在および将来の顧客のデータの安全性を保証するには、PCI への準拠が求められています。同社では、F5® Distributed Cloud App Infrastructure Protection（F5 Distributed Cloud AIP, 旧製品名：Threat Stack）を使用することで、コンプライアンスの目標を達成するだけでなく、インフラストラクチャにおけるセキュリティの可視性も大幅に向上させることに成功しました。

課題

顧客の自社データが安全に保護されていることを保証するために、同社のオペレーション担当ディレクターは、PCI 監査合格に向けて環境を整理し監視する必要がありました。監査に合格するために、彼が率いるチームは、クロック同期のための NTP、ホストやネットワークの侵入検出、ログ管理とアーカイブ、ファイル整合性の管理、暗号化キーの管理など、複数の新しいテクノロジをセットアップしました。

> *「[Distributed Cloud AIP] を使うことで、1 つのソリューションで複数の PCI 要件を同時に満たすことができました」*
>
> **オペレーション担当ディレクター**

ソリューション：Distributed Cloud AIP

Financial Tech 社が Distributed Cloud AIP を選択した理由は、その一連のセキュリティ機能がリスクを大幅に軽減し、クラウド環境に対するセキュリティを詳細に可視化できるためです。これらの機能には、Distributed Cloud AIP のホスト侵入検知（HIDS: Host Intrusion Detection）によるユーザとシステムアクティビティのリアルタイムモニタリング、そしてシステムを最新かつ最も脆弱性の低いパッケージに更新できる継続的脆弱性評価などが含まれます。さらに、ファイル

創業
2010 年

本社
テネシー州ナッシュビル

業種
Fintech（フィンテック）

従業員
50 人以上

整合性モニタリング（FIM: File Integrity Monitoring）は、機密ファイルがアクセスされるたびに警告を発し、機密データの安全性を確保します。

最高レベルの PCI 認定を取得するために、チームではサードパーティの認定セキュリティ評価者（QSA: Qualified Security Assessor）に自社環境の監査を依頼しました。監査は厳格に評価され、関連するすべてのポリシーと手順、技術的な詳細やエビデンスの文書化が求められました。さらに、Distributed Cloud AIP エージェントが機密データを操作または収集せず、いかなるコマンド & コントロールも実行しないことを実証する必要もありました。.

成果

Distributed Cloud AIP は、PCI コンプライアンスを達成するプロセスを大幅に簡素化しました。オペレーション担当ディレクターと彼のチームは、クラウドセキュリティ戦略を成功に導き、効率的に作業を進めています。オペレーション担当ディレクターは、その理由として、「[Distributed Cloud AIP] により、1 つのソリューションで複数の PCI 要件を同時に満たすことができるようになった。具体的には、[Distributed Cloud AIP] を使用することで、ホスト侵入検知、ネットワーク侵入検知、システムアクセスのモニタリング、システムユーザアクティビティのロギング、ファイル整合性のモニタリングを可能とし、侵害が発生しフォレンジック分析が必要となった場合には、それに関連するすべてのイベントのロギングとアーカイブが提供される。ロギングとアーカイブには、改ざんできない方法でアーカイブされたログを維持する機能も含まれる」ことを挙げています。

さらに、彼は次のようにも述べています。「[Distributed Cloud AIP] はプラットフォームへの革新と、改善を続けています。時間の経過と共に使いやすさが増し、インストール済みアプリケーションの日次レポートなど、軽減の必要があるセキュリティ問題を新たに特定する便利な機能も追加されています」

PCI 監査に合格して以来、同社はファイナンシャル機関の顧客に価値のある安全なサービスを提供しています。

PCI コンプライアンスについての簡単な説明

ペイメントカード業界データセキュリティ基準（PCI DSS: Payment Card Industry Data Security Standard）は、2004 年、Visa、MasterCard、American Express、Discover、JCB などのクレジットカード事業者が共同で策定したものです。その目的は、カード所有者のデータの取り扱う際の標準を導入し、クレジットカード詐欺を減らすことでした。

PCI 監査に合格するには、事業者は認定セキュリティ評価者（QSA: Qualified Security Assessor）に、カード所有者のデータを安全に取り扱うために使用する制御を文書化していることを示す必要があります。カード所有者のデータを処理するにも格納するにも、ネットワーク内のシステムは PCI ギャップ内にあると見なされ、これらに制御を適用する必要があります。セキュリティを向上させる方法としては、これらのシステムとネットワークを他のすべてから分離することが一般的なやり方であり、これらの関連システムにはカード所有者のデータにセキュリティを確保するツールを用意することが大事なポイントとなります。

THREAT STACK：F5 ソリューションになりました

Threat Stack は製品名称変更し、現在、F5 Distributed Cloud App Infrastructure Protection（AIP）になりました。本ソリューション、F5 のセキュリティオペレーションセンター（Distributed Cloud AIP Managed Security Services、Distributed Cloud AIP Insights を含む）、およびその他につきまして詳しくは、F5 のクラウドセキュリティとコンプライアンスの専門家までお気軽にお問い合わせください。

クラウドセキュリティのお悩みは F5 のセキュリティ専門家にぜひお任せください。詳細およびデモのご予約については、F5 のウェブサイトをご覧ください。

DC 10.2022 | JOB-CODE-CS-950855297-PCI-Compliance