小売チェーン、PCI DSSへのコンプライアンスを実現

ある大手小売業者は、Quest®ソリューションを使用して年に1度のPCI DSS監査にスムーズに合格し、企業全体で強力なセキュリティを維持しています。

「PCI DSSコンプライアンスを維持するためには、ネイティブのログ記録をすべて有効にし、前年度の完全なログを監査人に提供する必要があります…。InTrustがなければ、とっくにスペースが枯渇していたでしょう。」

大手小売チェーン、エンタープライズ管理者

お客様のプロファイル

業種	小売
国	米国

ビジネスニーズ

ある大手小売チェーンでは、年に1度のPCI DSS監査へ合格してセキュリティを確保するために、コストパフォーマンスの高い長期データストレージを備えたエンタープライズクラスのログ管理と、Active Directoryの高度な監視および変更監査を必要としていました。

ソリューション

Quest®InTrust®により、同社は対象の小売IT環境で4,000のPOSエンドポイントおよびその他のシステムからデータを収集し、コンプライアンス監査とセキュリティ調査のための簡単で安全なアクセスを維持しながら、すべてのデータを高度に圧縮された形式で何年間も保管できるようになりました。一方、管理責任の安全な委任やオブジェクト保護などの機能を備えたQuest Change AuditorとActive Rolesを導入することで、ビジネスIT環境では包括的なセキュリティを得ています。

メリット

- PCI DSS監査に必要なすべてのデータの効率的な収集と、コストパフォーマンスの高い保管を実現
- Active Directoryを強力に制御できるようになり、セキュリティが向上
- 一貫性の確保、および管理タスクの安全な委任により、時間を節約
- 管理アカウントおよびその他の重要なADオブジェクトへの変更を防止することにより、攻撃をブロック

ソリューションの概要

- Microsoftプラットフォーム管理

現代の小売組織は、Payment Card Industry Data Security Standard（PCI DSS）へのコンプライアンスを維持し、年次監査でそのことを証明する必要があります。監査に不合格になると、クレジットカード払いの許可がすべて禁止され、ビジネス全体が危機に陥る可能性があります。前年度の完全なIT監査証跡の作成は、準拠するのが特に困難なPCI DSS要件でしょう。しかし、ある大手小売チェーンでは、Quest Softwareのソリューションを使用して同社の小売IT環境全体から必要なすべてのログデータを収集し、必要に応じてコストパフォーマンスの高い方法で保管し、さらにはビジネスIT環境で強力なセキュリティを維持しています。

「Active Directoryは Active Rolesのポリシーによって管理され、すべての操作の一貫性が保証されます。これにより、管理者や私の作業が簡単になります。」

大手小売チェーン、
エンタープライズ管理者

PCI DSSコンプライアンスは、現代のすべての小売組織にとって非常に重要

小売業者は、対象のIT環境全体のログデータを収集して、PCI DSSコンプライアンスを維持する必要があります。しかし、現代のITエコシステムは混み合っており、膨大な量の重要なログデータが多様なシステムによって収集されています。この大手小売チェーンのITチームは、手書きやその他の手作業による方法では監査を乗り切れないことを認識していました。代わりに、PCI DSSの要求に応じて数十の遠隔地にある約4,000のPOSエンドポイントを含む幅広いシステムから必要なすべてのデータを収集し、そのすべてのデータを少なくとも1年間、コストパフォーマンスの高い方法で保管できるエンタープライズ品質のソリューションを必要としていました。

対象のPOS環境に加えて、ITチームは、ExchangeやHRシステムなど、現代のどの組織にも設置されている通常の業務処理システムも担当しています。急速に進化する脅威状況を受けて、ITチームは、外部の攻撃、悪意のある内部関係者、および管理者によるミスや不正行為からActive Directoryをより安全に保護したいと考えていました。その厳しいセキュリティを実現するために、Active Directoryを適切に管理し、ユーザやグループを含むADオブジェクトへのすべての変更を綿密に監視する方法が必要でした。

ACTIVE DIRECTORYエキスパートによるクラス最高のソリューション

市場のオプションを慎重に評価した後、この小売業者は4つのQuestソリューションを選択しました。InTrust®は、Windows、UNIX/Linux、データベース、アプリケーション、ネットワークデバイスなどのすべてのユーザワークステーションと管理者のアクティビティを監視できる、スマートでスケーラブルなイベントログ管理ツールです。さらに、20:1のデータ圧縮により、これらのイベントログを何年間もコストパフォーマンスの高い方法で保管できます。また、自動化された処理でリアルタイムのアラートも提供し、不審なアクティビティへの迅速な対応を保証します。

Active Rolesは、ユーザとグループの管理を合理化して、セキュリティを劇的に向上させます。オンプレミス環境またはハイブリッドAD環境全体のすべてのシステムを、1ヶ所から自動的かつ一貫性のある包括的な方法で簡単に管理できます。Change Auditor for Active Directory およびChange Auditor for Windows File Serversを使用すると、主要な構成のすべての変更を追跡、監査、レポート、および警告できます。また、管理アカウントやグループなどの重要なオブジェクトが変更されないように最初から予防的に保護することもできます。

製品とサービス

ソフトウェア
Active Roles
Change Auditor for Active Directory
Change Auditor for Windows File Servers
InTrust

INTRUSTによるPCI DSSコンプライアンスの確保と証明

この会社はInTrustを短期間で導入して、対象の小売IT環境全体の複数のシステムからデータを収集するようにしました。「私たちのPOSエンドポイントはすべてInTrustを搭載しています」とエンタープライズ管理者は言います。「また、InTrustを使用して、SQL Server、ターミナルサーバ、FTP、およびIISからログを収集しています。また、1つのサーバからはカスタム・テキスト・ログを取得し、Syslogもいくつか収集しています。」

これらのデータはすべて高度に圧縮され、中央のInTrustリポジトリに格納されます。コンプライアンスとセキュリティで必要とされている期間、コストパフォーマンスの高い方法でデータを保管できます。「PCI DSSコンプライアンスを維持するためには、ネイティブのログ記録をすべて有効にし、前年度の完全なログを監査人に提供する必要があります…」と管理者は述べています。「エンドポイントとアクティビティの数がとても多いので、データの量は膨大です。約800ギガ相当のログが常に存在します。InTrustがなければ、とっくにスペースが枯渇していたでしょう。もしそうなっていたら会社にとって大打撃でした。PCIの要件を満たせなければ、最終的にはクレジットカード払いを許可できなくなってしまいます。」

しかし、InTrustが提供する高度な圧縮のおかげで、監査に必要なデータを提供できないかもしれないという心配から解放されました。「InTrustの圧縮率は非常に高いです」と同氏は報告しています。「これにより、スペースが大幅に節約されるため、PCI DSSコンプライアンスに必要なすべてのログデータを保存できます。実際、InTrustがなければ、保管はおろか、すべてのデータを収集できたかさえも定かではありません。それほど大量の未圧縮データを転送するには大量の帯域幅が必要だったでしょうから。」

簡単な検索、事前組み込み済みのレポート、および高度なアラート

さらに、InTrustによって、ITチームはセキュリティ調査を実施するために必要な特定のデータに素早くアクセスし、監査人からの質問に迅速に回答し、セキュリティを維持できます。「InTrustリポジトリの高度なインデックス作成により、検索は非常に高速で簡単です」と管理者は述べています。「そして、この組み込み済みのレポートは、私が必要とするほぼすべてをカバーしています。すでに設定されている内容で十分に間に合います。」

プロアクティブな警告もセキュリティとコンプライアンスの両方に不可欠であり、同社はInTrustのリアルタイムアラート機能に非常に満足しています。「新しいユーザの作成やマシンの追加など、Active Directoryで行われるほとんどすべてのイベントについて、InTrustのアラートを設定しています」と管理者は述べています。「監査に合格するためには、この設定が欠かせません。例えば、技術者がエンドポイントを置き換えると、そのエンドポイントが再び追加され、その処理に関するアラートが発行されます。監査人は、エンドポイントの交換が対応するヘルプデスクチケットの要求に応じて行われたことを証明するため、そのアラートを確認する必要があるでしょう。InTrustアラートを使用すると、監査人が必要とする情報を含め、必要なものをすべて入手できます。」

ACTIVE ROLESとCHANGE AUDITによるADの管理と保護の維持

Exchangeメッセージングなど、オフィスおよび倉庫業務に使用されるIT環境では、同社はActive Rolesに依存して厳しいセキュリティを維持しています。「Active Rolesを使い始めて5～6年間です」と管理者は言います。「以前は、Active Directoryはめちゃくちゃな状態で、多くの管理者がさまざまな方法であらゆる操作を行っていました。現在、約12人の管理者がActive Directoryへのアクセス権を持っており、その唯一のアクセス手段はActive Rolesです。Active DirectoryはActive Rolesのポリシーによって管理され、すべての操作の一貫性が保証されます。これにより、管理者や私の作業が簡単になります。例えば、Active Rolesではすべてのコンピュータアカウントを最初から適切なOUに作成する必要があるため、後でPowerShellを使用して移動する必要がありません。」

> 「私たちが依頼したペンテスターも、Change Auditorのオブジェクト保護を通過できなかったことにとても驚いていました。」
>
> *大手小売チェーン、*
> *エンタープライズ管理者*

「私たちはたくさんのライセンスを持っていますが、サポートを依頼することはほとんどありません。年に1回程度です。しかしサポートを依頼したときは、サポートチームはいつも、私が抱えている問題を親身になって解決してくれます。」

大手小売チェーン、
エンタープライズ管理者

また、主任管理者がアクセス許可を他の管理者にきめ細かく委任できるため、コントロールを喪失することなくワークロードを分散できます。「Active Rolesのおかげで時間を節約できます。私は多くの役割を担っており、365日24時間対応でずっと待機している状態なので、このことは重要です」と語っています。「以前は、例えばヘルプデスクのスタッフにActive Directoryの設定を変更してもらうことができなかったため、私がタスクを委任できるのはごく少数の管理者のみでした。Active Rolesを使用すると、私は各人のできることとできないことを制御できるため、より多くのタスクを委任できます。例えば、各店舗にはディレクターがいます。そのうちの1人がヘルプデスクに電話してパスワードをリセットするように依頼した場合、ヘルプデスクはそれを行うことができませんでした。ディレクターのパスワードを変更できるのは、リクエストを行った人のIDを確認できる地域のマネージャだけでした。」

2つのChange Auditorソリューションにより、環境のセキュリティがさらに強化されます。「Change Auditorのオブジェクト保護はとても役立っています」とクラークは言います。「これを導入したのは、ファイルサーバ上の特定のディレクトリのACLへの変更を防止し、すべての管理アカウントを保護するためでした。私たちが依頼したペンテスターも、Change Auditorのオブジェクト保護を通過できなかったことにとても驚いていました。」

ワールドクラスのサポート

このエンタープライズ管理者は、Questサポートについても自ら言及しました。「私たちはたくさんのライセンスを持っていますが、サポートを依頼することはほとんどありません。年に1回程度です」と彼は述べています。「しかしサポートを依頼したときは、サポートチームはいつも、私が抱えている問題を親身になって解決してくれます。Questコミュニティのサポートフォーラムも非常に便利です。それまで十分に活用していなかった機能について、良いアイデアや提案をもらっています。」

QUESTについて

Questは、急速に変化するエンタープライズITの世界にソフトウェアソリューションを提供しています。データの爆発、クラウドサービスへの拡張、ハイブリッドデータセンター、セキュリティ脅威、規制上の要件によって生じる課題のシンプル化を支援します。Questのポートフォリオは、データベース管理、データ保護、統合エンドポイントの管理、IDおよびアクセス管理、Microsoftプラットフォーム管理などのソリューションで構成されます。

その他の導入事例: Quest.com/Customer-Stories

CaseStudy-RetailerPCIDSS -US-KS-JA-WL-55478#