ホワイトペーパー

PCI DSS 4.0: 新要件に完全に準拠しているか確認する方法

目次

コンプライアンスは、あらゆる規模の組織にとって継続的な要件です。組織に対する義務には、国内法および国際法、政府の規制、枠組み、および特定の業界または政府機関によって設定された運用要件が含まれる場合があります。サイバーセキュリティに関するコンプライアンスは主要な推進要因であり、その中でも最も顕著な要件の 1 つはペイメント カード業界のデータ セキュリティ基準 (PCI DSS) です。

その業界の PCI 評議会は、世界的な決済システムのセキュリティを確保するために PCI DSS を作成しました。PCI DSS は、ペイメント カード所有者データ (Card Holder Data) または機密認証データ (Sensitive Authentication Data) を保存、処理、送信する、またはカード所有者データ環境 (Cardholder Data Enviornment) のセキュリティに影響を与える可能性のあるすべてのエンティティにグローバルに適用されます。具体的には、これには支払いアカウントの処理に関与するすべてのエンティティが含まれます。あなたの会社が販売者、加工業者、取得者、発行者、またはその他の関連サービスプロバイダーである場合、たとえクレジット カード プロバイダーがトークン化を使用している場合でさえも、PCI DSS に準拠する必要があり、そうしないと厳しい罰則が課される可能性があります。ポリシーは、American Express、Discover Financial Services、JCB International、Mastercard、UnionPay、VISA, Inc. を含む実行委員会によって設定されます。

このホワイトペーパーでは、支払いデータのセキュリティに対する PCI DSS の意味、リスクが存在する場所、コンプライアンスに何が必要か、および Qualys Cloud Platform がどのようにして機密性の高いデータのリスクを軽減しながらコンプライアンスの重要な要素を自動的に満たすかについて説明します。

今日PCI DSS が重要な理由

PCI DSS は、2004 年の創設以来、決済データのセキュリティを確立および維持するための包括的かつ体系的なアプローチにより、決済業界以外でも採用されているサイバーセキュリティ モデルです。さまざまなコンプライアンス体制について、単なるチェックボックスにチェックを入れているだけだと冗談を言う人もいるかもしれません。しかし、PCI DSS を使用すると、組織が標準に準拠していれば、その見返りとして、機密データに対する真のセキュリティを

確保できる可能性が最も高くなります。

言い換えれば、コンプライアンスは単なる負担ではなく、強力なセキュリティを実現するための最良の友となり得るのです。逆に、遵守しなかった場合、クレジット カード会社は「プラグを抜き」、クレジット カードでの支払いを受け入れる能力を制限または消去される可能性があります。クレジット カード プロバイダーはトークン化を使用すると便利ですが、それでも PCI DSS 要件に準拠する必要がある可能性があります。これは、顧客に関するマーケティング データを収集する場合に特に当てはまります。PCI DSS 準拠の失敗によるブランドの損害と収益のリスクは非常に高くなります。大企業の場合は月額 100,000 ドルまでの罰金が課せられますが、小規模な組織の場合は月額 5,000 ドルから課せられる場合があります。

さらに懸念されるのは、現在、米国のほとんどの州にはカリフォルニア州消費者プライバシー法 (CCPA) などの厳格な民法があり、クレジット カード データに関連するものなど、個人を特定できる情報 (PII) を公開した場合、企業に罰則や罰金が科せられることです。ほとんどの州では、こうした暴露に対して弁護士が民間人に代わって訴訟を起こせる「私的訴訟原因」も認めている。法的証拠開示と裁判費用は簡単に数百万ドルに跳ね上がり、その後にブランドを傷つける見出しが報道されることもあります。

専門家らは、PCI DSS がサイバーセキュリティのゴールドスタンダードを設定していると述べています。最新バージョン 4.0 の範囲は膨大です。6 つの戦術目標、12 の主要要件、および数百のサブ要件とテスト手順があり、合計 356 ページあります。バージョン 4.0 では、コンプライアンスに対する 2 つのアプローチも導入されています。1 つは従来の「定義済み」アプローチで、技術要件、プロセス要件、およびテスト手順に厳密に従います。もう 1 つは、カスタマイズされたプロセス、または定義されたプロセスとカスタム プロセスの混合を可能にするリスクベースのアプローチです。

セキュリティとコンプライアンスの専門家にとって、PCI DSS コンプライアンスを追求する上でおそらく最もストレスを感じるのは、単一のベンダーが必要なすべてのツールとサービスを提供していないことです。したがって、中小企業から大企業に至るまで、PCI DSS コンプライアンス プロセスの確立と維持は複雑になる可能性があります。その理由を理解するために、潜在的な脆弱性がどこに存在するのか、そして PCI DSS 4.0 が新しい要件を通じてこれらにどのように対処するのかを考えてみましょう。

PCI DSS の脆弱性リスクが存在する所

PCI DSS 要件は、決済処理エコシステムのあらゆる所で潜在的に発生する脆弱性を対象としています。
あなたの会社がこのような物理的または仮想的なデバイス、システム、またはサービスを使用している場合は、注意を払う必要があります。

- クラウドベースのシステム
- エンドポイント デバイス (モバイル、ラップトップ、PC)
- 紙ベースの保管システム
- POS デバイス
- リモート アクセス接続
- Windows および Linux サーバー
- カード会員データのサービスプロバイダーへの送信
- サービスプロバイダーおよびアクワイアラーが運用するシステムの脆弱性

- Web ショッピング アプリケーション
- ワイヤレスホットスポット

脆弱性は他のリソースにも現れる可能性があり、その潜在的な範囲はハードウェア、ソフトウェア、ネットワーキング、アプリケーション、サプライ チェーン、パートナー、サービス プロバイダーにまで及びます。支払いのセキュリティを確保することが大きな課題であるのも不思議ではありません。
PCI DSS の範囲が非常に広い理由はここにあります。PCI DSS は、多くの分野にわたる多数の潜在的な脆弱性に対処する必要があります。

PCI DSS 4.0 の準拠に必要なもの

PCI DSS 4.0 は 2022 年 3 月に公開され、大きな新しいリリースではありますが、その内容の実質は劇的な変更というよりは、以前のバージョン 3.2.1 の改良版です。PCI 評議会はバージョン 4.0 に対して 4 つの戦略目標を設定しました。これは 2023 年 3 月 31 日に完全に発効しました。

1. 決済業界のセキュリティ ニーズに応え続けます。これには、多要素認証、パスワード、電子商取引/フィッシングに対するより強力な要件が含まれます。
2. 継続的なプロセスとしてセキュリティを推進します。これにより、セキュリティの実装と維持に関するガイダンスが明確になります (下記を参照)。
3. さまざまな方法論に柔軟性を追加します。単一のサイズがすべてに適合するわけではないのと同じ様に、一部の組織ではコンプライアンスへのアプローチに柔軟性が必要であることを認識します。
4. 検証方法を強化します。コンプライアンスに関するレポートまたは自己評価アンケート (Self-Assessment Questionnaire) とコンプライアンスの証明書をより緊密に連携させる必要があります。

コンプライアンスのための 4 段階のプロセス

PCI DSS 4.0 では、PCI 評議会は組織が支払いアカウント データを保護するために使用すべき 4 つの継続的な手順を提供します。*PCI DSS クイック リファレンス ガイド: ペイメント カード業界データの理解で説明されているとおり Security Standard バージョン 4.0 (p. 4)* の手順は次のとおりです。

1. 評価 - 支払いアカウント データのすべての箇所を特定し、支払い処理に関連するすべての IT アセットとビジネス プロセスの棚卸しを行い、支払いアカウント データが漏洩する可能性のある脆弱性を分析し、必要な制御を実装または更新し、正式な PCI DSS を受けます。
2. 修復 - セキュリティ管理のギャップを特定して対処し、特定された脆弱性を修正し、不要な支払いデータ ストレージを安全に削除し、安全なビジネス プロセスを実装します。
3. レポート – 評価と改善の詳細を文書化し、コンプライアンスを受諾する組織 (通常は買収銀行または決済ブランド) にコンプライアンス レポートを提出します。
4. 監視と維持 - 支払いアカウントのデータと環境を保護するために導入されたセキュリティ管理が、年間を通して効果的かつ適切に機能し続けることを確認します。これらの「通常業務」プロセスは、継続

的な保護を確保するために、企業全体のセキュリティ戦略の一部として実装される必要があります。

Qualys Vulnerability Management、Detection and Response (VMDR) および Qualys Cloud Platform のその他のアプリケーションを使用するためのプロセス方法論は、PCI Council の 4 段階のプロセスと完全に一致していることに注目してください。

以下では具体的な相乗効果について説明します。

PCI DSS 4.0 の目標と要件

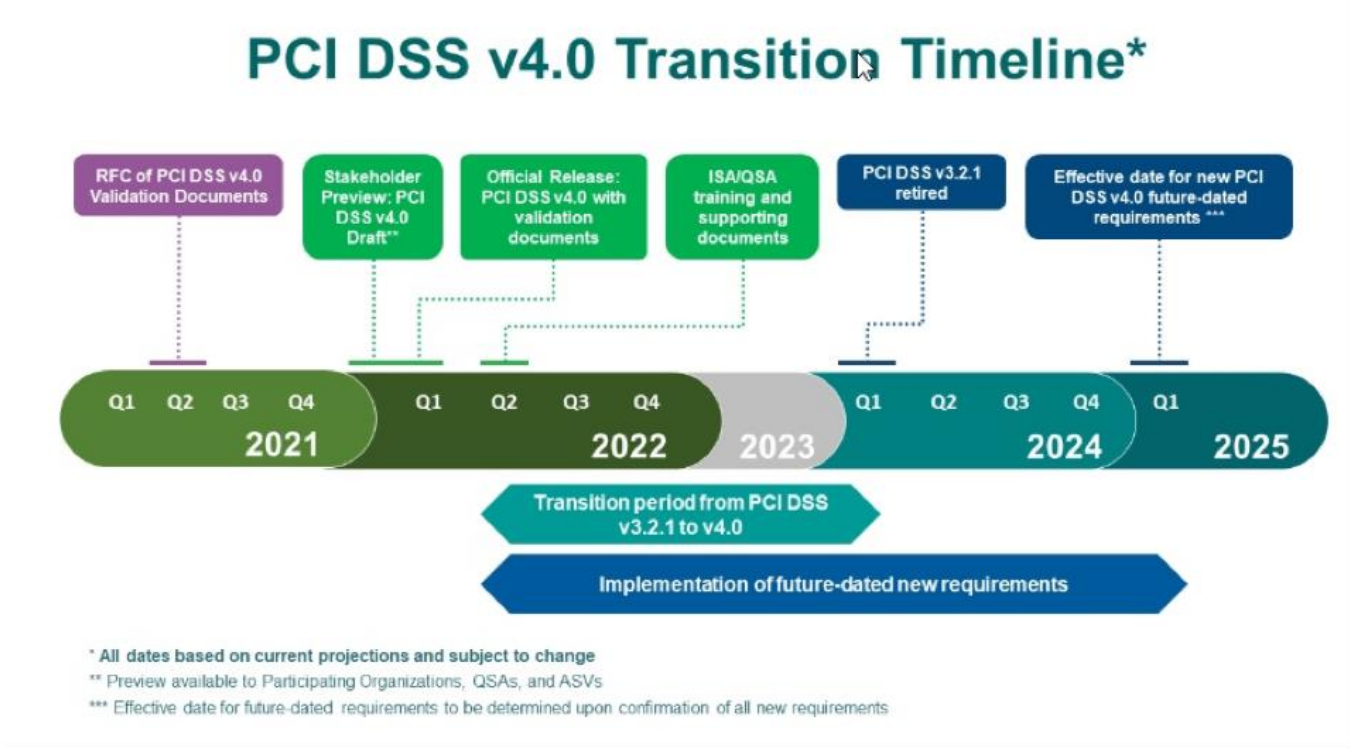
PCI DSS 4.0 の大部分は、6 つの戦術目標と 12 の要件を明確に表現したものです。下記のバージョン 4.0 の表では、いくつかの項目が調整されていますが、事実上すべては以前のバージョン 3.2.1『セキュリティとコンプライアンス』と同じです。この表は関連するすべてのコンプライアンス活動の基礎となるため、専門家はこの表に精通しているでしょう。3 番目の目標は脆弱性管理に関するものですが、すべての目標と要件はすべてのセキュリティ プログラムの基礎であり、「サイバーセキュリティのための 12 ステップ プログラム」に似ています。PCI Council もこの類似点に注目しています (『クイック リファレンス ガイド』の2 ページを参照)。
したがって、組織が PCI DSS 4.0 準拠のために行うすべてのことは、脅威から保護し、IT エコシステム全体の要素を保護することにも役立ちます。これが、Qualys Cloud Platform がコンプライアンスおよび一般的なサイバーセキュリティにとって不可欠であるもう 1 つの理由です。

目標	PCI DSS必要条件
安全なネットワークとシステムを構築および維持する	ネットワークセキュリティ制御のインストールと維持 すべてのシステムコンポーネントに安全な構成を適用する
アカウントデータを保護する	保存されているアカウント データを保護する カード所有者のデータを強力な暗号化で保護する オープンなパブリック ネットワークを介した送信
脆弱性管理プログラムを維持する	すべてのシステムとネットワークを悪意のあるソフトウェアから保護する 安全なシステムとソフトウェアを開発および維持する
強力なアクセス制御対策を実装する	システムコンポーネントのカード所有者データへのアクセスを制限する ビジネスを知る必要がある ユーザーを識別し、システムコンポーネントへのアクセスを認証する カード会員データへの物理的アクセスを制限する
ネットワークを定期的に監視およびテストする	システムコンポーネントとカード所有者データへのすべてのアクセスをログに記録し、監視する セキュリティ システムとネットワークを定期的にテストする
情報セキュリティポリシーを維持する	ポリシーとプログラムによる情報セキュリティのサポート

PCI DSS 4.0 に準拠するために制御とプロセスを適用するのは大規模な作業のように思えますが、この規格ではセグメンテーションを使用して準拠範囲を縮小できるようにすることでこれを緩和しています。セグメンテーションには、カード会員データ環境 (Cardholder data environment (CDE)) - コンプライアンスの対象となるすべてのもの -を、組織の

IT インフラストラクチャ内の他のすべてのものから分離することが含まれます。たとえば、セグメント化には物理サーバー、データ ストレージ、またはネットワーク デバイスが含まれる場合があります。また、組織のクラウド内に同じ仮想インスタンスが含まれる場合もあります。サードパーティのサービスプロバイダーの使用には、特別なセグメント化ルールが存在します(要件 12.8 および付録 A1 を参照)。セグメンテーションを使用すると、保護する必要がある範囲を大幅に縮小でき、残りの範囲内アセットの PCI DSS 検証監査プロセスが簡素化されます。

「PCI コンプライアンス」は、PCI DSS 4.0 の要件を満たすことに大まかに適用されます。しかし、これが支払いのセキュリティの唯一の基準ではありません。PCI Council は現在、15 の異なるPCI セキュリティスタンダードを管理しています。



Data courtesy of PCI Security Standards Council

Qualys がどのように PCI DSS 4.0 準拠を推進するか

Qualys Compliance Solution Set と Cloud Platform は、組織が 2 つの方法で PCI DSS 4.0 への準拠を確保するのに役立ちます。その 1 つは、コンプライアンスの自動文書化を可能にすることです。これは、基本的にPCI DSS 4.0要件の多くの管理が実施されているかどうか、およびそれらがそれぞれの役割をはたしているかどうかステータスをチェックします。
次に、VMDR、Web Application Scanning (WAS) などのさまざまな統合 Qualys セキュリティ アプリケーションを使用して、このプラットフォームは PCI DSS 4.0 要件の堅牢なサブセットに対する特定の制御も提供します。

プロセス自動化をコンプライアンスに適合させる

PCI DSS 4.0 などのコンプライアンス ルールにより、セキュリティ関係者は 2 種類のチェックを実行する必要があります。つまり、必要なコントロールが実施されていることを確認することと、コントロールが必要に応じて機能していることを確認することです。Qualys は、Qualys Cloud Platform 用の 2 つのアプリケーションを使用して、このプロセスの自動化を支援します。

PCI DSS 4.0 コントロールを検証するための Qualys ポリシー コンプライアンス

一部の中堅および大規模企業では、認定セキュリティ評価者を使用して PCI DSS 監査を実施し、コンプライアンスを検証し、結果を正式なコンプライアンス レポートとして提出する必要があります。このプロセスを実行すると、対象となるカード会員データ環境の規模と複雑さによっては、面倒で時間のかかる作業が発生します。また、このアプローチを使用している組織は、必要な年次評価が単なる時点の測定であり、1 つ以上の管理が失敗すると、数時間以内にコンプライアンスから外れてしまう可能性があるため、カード所有者と機密の認証データを潜在的な危険にさらします。PCI 評議会は関係者に対し、「コンプライアンスは常にセキュリティと同等ではない」とアドバイスしています。これは、インターネットに接続されているすべての環境に対する 24 時間 365 日の集中攻撃によって痛感されています。したがって、前述したコンプライアンスのための 4 段階の継続的なプロセスが提供されます。

Qualys の活用方法: Qualys Policy Compliance (PC) は、カード会員データ環境の継続的な評価を可能にする Compliance Solution Set に含まれるクラウド サービス アプリです。Qualys PC は、範囲内の PCI アセットの評価を自動化するセキュリティ チェックで構成される、すぐに使用できる PCI DSS 4.0 のマンデートベースのテンプレートを提供します。これらのチェックでは、技術的に安全な構成の評価要件が自動的にスキャンされます。

Qualys PC は、対象範囲内のさまざまなオペレーティング システム、データベース、Web サーバー、デバイスなどのサポートを提供します。また、適格セキュリティ評価者との連携により、コンプライアンスに関するレポートの自動生成を含む、正式な年次 PCI DSS 評価が簡素化および迅速化されます。カスタム ダッシュボードとレポートを作成できる機能により、監査人が標準以外の何かを要求した場合でも、常に監査準備完了ステータスを確保できます。

ほぼすべてのセクションの多くの要件は、「ネットワーク接続に対するすべての変更とネットワーク セキュリティ制御の構成に対する変更が承認され、要件 6.5.1 に従ってテストされる」ことを保証するなど、ポリシー コンプライアンス機能に言及しています。Qualys PC を使用すると、セキュリティ設定の評価を自動化し、PCI DSS v4.0 の技術的セキュリティ要件への準拠を迅速に特定できます。Qualys PC は、顧客が PCI DSS v4.0 Standard への準備を迅速に文書化するために実行できる、すぐに使用できるレポートも提供します。Qualys は、「範囲内の」PCI アセットの評価を自動化するセキュリティ チェックで構成される、すぐに使用できる PCI DSS v4.0 のマンデートベースのテンプレートをリリースしました。このテンプレートは、さまざまなテクノロジーにわたって検証する必要がある主要な技術的管理セットに対する PCI コンプライアンスの検証にマーチャントが取り組む必要があるプロセスを簡素化します。Qualys PC は、これらすべての PCI 制御を自動的にスキャンし、継続的なコンプライアンスを検証するための詳細なレポートを提供できるようになりました。

Qualys セキュリティ評価アンケート コンプライアンスの自己検証

中堅以下の企業では、自己評価アンケート (Self-Assessment Questionnaire(SAQ)) と呼ばれる PCI DSS 4.0 で規定された手段を使用することがよくあります。リンクで説明されているように、組織や環境のタイプに対応する 9 つの異なる SAQ があります。適格な組織は SAQ を使用して、PCI DSS への準拠を自己評価できます。検証結果は、準拠証明書と

ともに組織の取得銀行または決済ブランドに提出されます。

Qualys の活用方法:別のエージェントをマネージャに追加しなくても、組織はQualys Compliance に含まれるQualys Security Assessment Questionnaireアプリを使用して、必要な情報を収集および検証し、SAQ を完了するプロセスを自動化できます。ビジネス プロセス制御の自動化には、組織内外のすべての関係者が含まれます。簡略化されたアンケートは、ブラウザに結果を入力する適切な回答者に自動的に送信されます。事前にフォーマットされた SAQ テンプレートは、必要に応じてカスタマイズできます。特に情報の収集に人間のアクションが必要な場合、回答者は、より適切に回答できる同僚に質問を電子的に委任する場合があります。最終的な SAQ は自動的に提出用に準備され、アクワイアラまたは支払いブランドに提出できます。Qualys SAQ は、組織全体でプロセスを簡単、正確、包括的、一元化、スケーラブルで均一なものにします。

PCI DSS 4.0 要件に対する Qualys セキュリティ コントロール

現在、Quays Compliance Solution Set には、幅広い要件に対応するセキュリティとコンプライアンスのための 8 つの統合アプリケーションが含まれています。そのため、Qualys は、PCI DSS 4.0 の堅牢なセキュリティ管理要件に対処するのに最適です。

Qualys の活用方法: Qualys が対応するすべての要件とサブ要件について説明することは、このホワイトペーパーの範囲を超えています。セキュリティ チームがさらに詳細な情報を必要とする場合は、ここをクリックしてQualys に問い合わせて、Qualys アプリケーションが各 PCI DSS 4.0 要件をどのように満たしているかを示す詳細なマップを入手してください。ここでは、単一の管理コンソールとエージェントを使用するコンプライアンス ソリューション セットを使用して監査の準備を整える方法の例を示します。

Qualys 脆弱性管理(VMDR) – VMDR は Qualys Compliance には含まれていませんが、CDE サイバー リスクを管理するための推奨される基本ソリューションです **(要件 2、5、6、11)**。これは、CDE 脆弱性管理プログラムの 3 番目の目標と、CDE システムとネットワークのセキュリティを定期的にテストするという要件 11 のニーズに対応しています。VMDR は、内部および外部のリスクを検出し、脆弱性に効率的に対応することに優れています。他のスキャナとは異なり、証明書インベントリなどの認証スキャンを実行します。

Qualys Web Application Scanning (WAS) – WAS は Qualys Compliance に含まれており、CDE の内部および外部向け Web アプリケーションの脆弱性と設定ミスを継続的に検出します **(Req. 6、11)**。このアプリは、Web アプリ内のマルウェアを検出し、公開された支払いデータやその他の PII について DevOps チームに通知します。

Qualys ファイル整合性モニタリング (FIM) – FIM は、不正な変更や変更検出を含む、「低ノイズ」の CDE 整合性モニタリングの取り組みとコンプライアンス **(要件 1、10、11、12)** を提供します。これにより、誤ったアラートとポジティブなヒットを正確に分離し、ホワイトリスト登録します。

Qualys Cyber Security Asset Management (CSAM)と外部攻撃対象領域管理 (EASM) の組み合わせ – CSAM は、セキュリティ ギャップ **(要件 2)** を特定するために、すべての CDE サイバーアセットの正確でコンテキスト豊富なインベントリを提供します。また、CSAM は CDE の外部の攻撃対象領域 (要件 2、12)の完全な可視性と制御を提供します。

Qualys パッチ管理– パッチ管理により、カード所有者データ環境内のリモート デバイスであっても、オペレーティング システム、モバイル デバイス、サードパーティ アプリケーションのパッチ適用プロセス全体を自動化できます **(要件 1、6、10、11)**。

カスタム評価と修復– Custom Assessment & Remediation は Qualys Compliance に含まれており、再利用可能なカスタム検出と修復を作成すると同時に、カスタム設定の導入を可能にします。

セキュリティ評価アンケート– Qualys Compliance に含まれる SAQ を使用すると、コンプライアンスの証拠を文書化し、監査人や経営陣向けの詳細なレポートを作成できます。

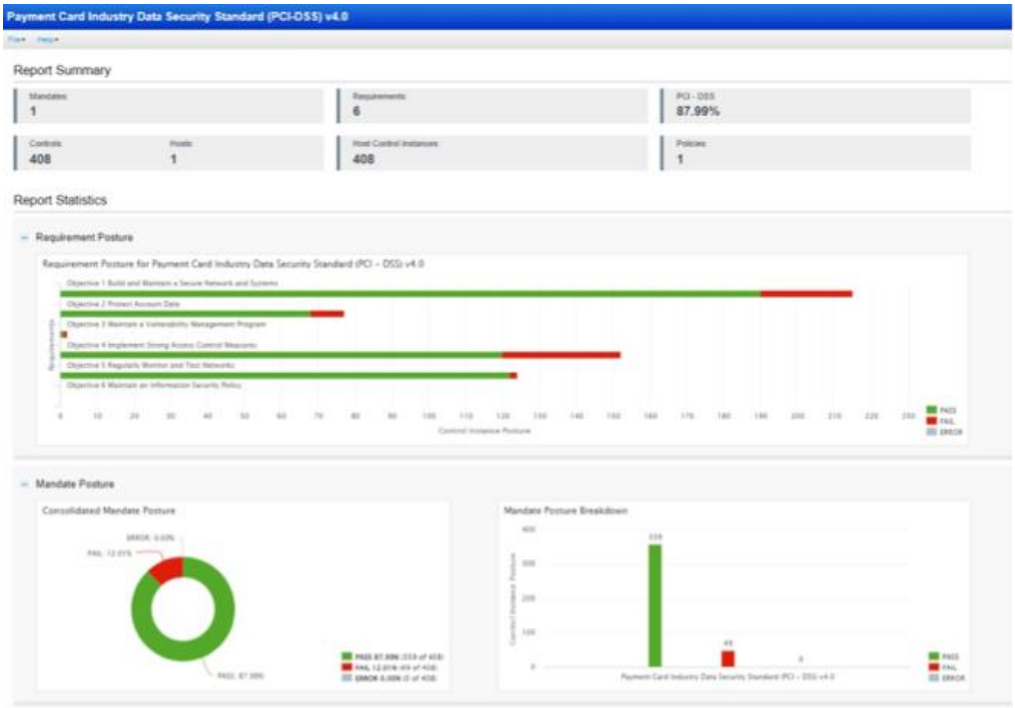
PCI ASV コンプライアンス– Qualys は、承認済みスキャン ベンダー (ASV) として、PCI DSS への準拠を示すために必要な四半期スキャンを実行する権限を PCI Security Standards Council から認可されています。これは、正確かつ効果的な PCI ASV コンプライアンス テスト、レポート、提出を保証するのに役立ちます。

Qualys Multi-Vector Endpoint Detection and Response (EDR) – EDR は Qualys Compliance には含まれていませんが、CDE の脆弱性管理とエンドポイントの脅威の検出と対応を統合するための追加として推奨されます **(Req. 5、12)**。

Qualys Context XDR – Extended Detection and Response も Qualys Compliance には含まれていませんが、MITRE ATT&CK 主導の脅威ハンティングと分析 **(Req. 10)** を使用して、CDE に対する複雑で高度な脅威の修復を加速するために追加する必要があります。

PCI DSS v4.0 のマンデートテンプレートは以下を提供します。

•組織に対する効果的な管理と、暗黙の PCI DSS v4.0 要件について迅速にレポートする機能。
•技術的に安全な構成評価要件をすべてカバー。
•さまざまな「対象範囲内」のオペレーティング システム、データベース、Web サーバー、ネットワーク デバイスなどのサポート。



結論

PCI DSS 4.0 への準拠は、世界中の何百万もの組織に当てはまる重要なトピックです。
PCI 評議会が推奨する評価、修復、報告、監視と維持の 4 段階の継続的プロセスの要件に従うことで、組織は完全なコンプライアンスに向けた実証済みの道を歩み、ブランドの損傷、罰金、訴訟のリスクを軽減できます。さらに大きな利点として、組織はエンタープライズ IT 環境全体にわたって強力なサイバーセキュリティ体制を確保できます。このプロセスのイネーブラーとして使用される場合、Qualys Compliance Solution Set は、コンプライアンス プロセスを簡素化および自動化し、カード会員データ環境を安全に保つための統合アプリケーションを提供します。PCI DSS の詳細については、PCI Council Web サイトのPCI DSS v4.0 リソース ハブにある PCI DSS 4.0 の全文およびその他のサポート文書をお読みください。また、Qualys を使用して PCI DSS 4.0 準拠を達成し、無料トライアルを開始する方法について詳しく学ぶことをお勧めします。

Contributors:
Bill Reed, Qualys Product Marketing
Dave Buerger, Qualys Product Marketing