

BigFix Compliance

セキュリティーおよび法的ポリシーへのコ
ンプライアンスを継続するために



エンドポイント数とそれらを侵害する脅威がこれまでにない勢いで増加している中、BigFix® Compliance は複雑で高度に分散化された環境を保護するために統一化されたリアルタイムの可視性とポリシーの強制を提供します。

組織全体にわたるエンドポイントのセキュリティーを強化するため、BigFix Complianceは組織のエンドポイントを保護し且つセキュリティー・コンプライアンスの要件やポリシーに適合させます。この容易に管理でき、迅速に展開できるBigFixソリューションは、サーバーからデスクトップ、「ローミング」しているインターネットに接続されたラップトップやクラウド内のエンドポイント、さらに店頭デバイスなどの専用装置、ATMやセルフサービス・キオスクに至るまでの多数多様なエンドポイントを有する環境のセキュリティーをサポートします。

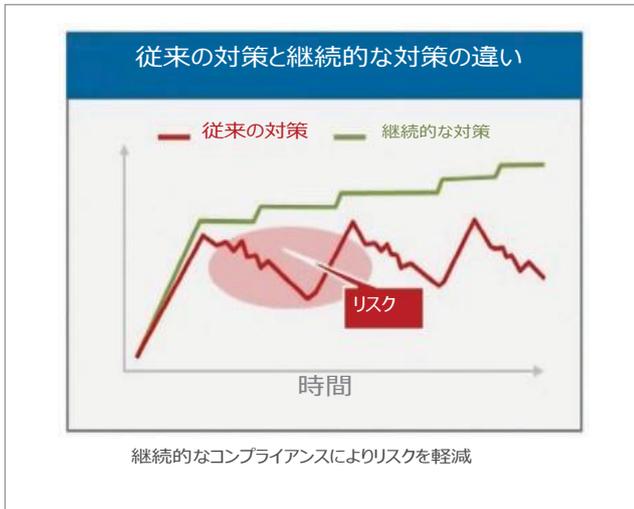
BigFix Compliance を使えばビジネス・アジリティー、修正までのスピード、正確性が向上し、IT管理のコストと複雑さが軽減されます。エンドポイントの運用に及ぶ影響は少ないので、生産性とユーザーエクスペリエンスを改善できます。エンドポイントがローミングしている場所に関わらず常にポリシーへのコンプライアンスを強制するため、リスクを減らし監査の可視性が向上します。BigFix Compliance のインテリジェント・エージェントはスピードがあり効率性が高いため、数分から数週間の単位で測定した自動監査サイクルに永続的に適合させます。

ハイライト

- CIS や DISA STIG などの業界ベストプラクティスのセキュリティー・ベンチマークをベースにしたすぐ使える数千ものセキュリティー・コントロールを使って継続的な構成の適合を保証し、逸脱した構成を効果的に修正します。
- OSの種類、場所、タイプに関わらず、すべてのエンドポイントに対するパッチを管理・配信します。BigFix Compliance には BigFix Modern Client Management が含まれるようになり、従来のエンドポイントに加えて、最新のクライアント (Windows 10 や macOS) を管理できます。
- ポリシー・コンプライアンスの状態と履歴トレンドを、セキュリティー構成、パッチ、脆弱性の3つのセキュリティー分野全体にわたって追跡・分析・レポートして、エンドポイントのセキュリティーリスクを評価し、コンプライアンスの進捗状況を提示します。
- アンチウイルスやアンチマルウェア・ツールなどの様々なサードパーティー製エンドポイントの保護ソリューションの展開状況とそのヘルス状態をモニターして管理します。
- BigFix Compliance に含まれる BigFix Insights Vulnerability Remediation の脆弱性スキャナーが検出した脆弱性に対して最適なパッチと構成設定 (修正 Fixlets) と相関付け、これを採用する組織は迅速に修正アクションを優先付けして、企業の攻撃対象領域を削減できます。

組織全体わたるセキュリティー・ニーズへの対応

BigFix Compliance はデスクトップ、サーバー、モバイル・ラップトップ、分散化された環境などに関連したセキュリティー課題に取り組んでいます。包括的なエンドポイントの管理とセキュリティーを実施することで、継続的な保護とコンプライアンスの保証をサポートします。たとえば、セキュリティー構成の監視と数分ほどの逸脱した構成の修正を行うことでセキュリティー曝露におけるギャップを劇的に削減できます。またセキュリティー戦略とポリシーを確立して実行する機能、リアルタイムでデバイスを管理する機能、セキュリティーやコンプライアンス問題に関するレポートを生成する機能など様々な機能間のギャップを効果的に埋めることもできます。



BigFix Compliance の機能

BigFix Compliance には以下を含む重要な機能が数多くあります。

- セキュリティー構成のリアルタイム且つ自動の評価、セキュリティー・ポリシーの継続的な強制、逸脱した構成の効果的な修正を行います。つまり、継続的な自己治癒によるコンプライアンス維持が可能です。
- Payment Card Industry Data Security Standard (PCI DSS)、Center for Internet Security (CIS)、Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs) など業界のベストプラクティス・セキュリティー・ベンチマークに基づいた、追加設定なしにすぐ使えるチェックリストをサポートしています。
- 60以上のOSとアプリケーションのセキュリティー構成を管理します。
- 多種多様なOSおよびソフトウェア・アプリケーションのパッチに関する管理と配信を行います。
- セキュリティー構成、パッチ、脆弱性という3つの主要セキュリティー分野全体にわたってポリシー・コンプライアンスの状態を追跡・分析・レポートします。
- アンチウイルスやアンチマルウェア・ツールなどの様々なサードパーティー製エンドポイントの展開状況とそのヘルス状態をモニターして管理します。
- IPアドレスでアクセスできるすべてのデバイスについてネットワーク全体のスキャンを行い、BigFixの管理対象となっていないエンドポイントがないかどうかを調べます。
- Query ツールおよび事前設定もしくはユーザー定義のクエリを用いてエンドポイントに問い合わせを行い、数秒で正確な応答を取得します。
- BigFix エージェントからの制御と可視性を維持しつつ BigFix エージェント自身を使ってシステムを検疫し、ネットワーク内の対象を隔離して、修正・問題解決を行います。
- 脆弱性スキャナーを統合して、修正アクションを迅速に優先付けし、企業の攻撃対象領域を減らします。

BigFix Compliance により自動化され且つ対象を絞ったプロセスを使ってコントロール、可視性を行い、変更を迅速に適用してコンプライアンスに関するレポートを挙げます。高度なゼロデイ攻撃の脅威の対応には、ほぼリアルタイムで組織全体をカバーする分析と、BigFix のようなアクション・ツールを採用することが不可欠です。BigFix を使えば、修正サイクルは短く、迅速であるため、マルウェアやセキュリティー曝露に対応できる業界トップの高速応答な機能が得られます。

幅広い強力なセキュリティー機能を提供

BigFix Compliance には以下の主要機能が含まれており、追加も必要なく、実装コストもかかりません。

デバイス・ディスカバリー

BigFix Compliance を使うと、デバイス・ディスカバリーをするのにスナップショットを数える必要はなくなります。変化し続ける状況についてダイナミックな状況認識を作成します。頻繁にネットワーク全体をスキャンできるため、可視性とコントロールが波及的に広がり、各組織はすべてのIPアドレスでアクセス可能なデバイスを迅速に識別できます。

モダン・クライアント管理

BigFix Lifecycle に含まれている BigFix Modern Client Management では MDM API アプローチを使って Windows 10 と macOS のエンドポイントの可視性とコントロールを拡張します。このアプローチにより各組織は単一の企業エンドポイント管理ソリューションを使って、従来のエンドポイントと最新のエンドポイントの両方を管理できるようになります。またエンドユーザーから開始される登録、エンドポイントの詳細なインベントリ、リモートワイプなど数多くの MDM アクションも提供されます。

パッチ管理

パッチ管理には、Windows, UNIX, Linux, macOS および、Adobe, Mozilla, Apple, Java などのサードパーティー製アプリケーション用のパッチを、分散化されたエンドポイントの場所、接続タイプまたは状態などに左右されることなく配信するための包括的な機能が含まれています。単一の管理サーバーで最大 250,000 のエンドポイントに対応可能で、低帯域幅や世界中に分散したネットワークに対してエンドポイントの機能ロスなく、パッチ適用時間を短縮できます。仮想パッチ管理機能により、オフラインのパッチ適用ができ、従来の仮想マシンのイメージは過去のものとなります。リアルタイム・レポートにより、完全なクローズド・ループのパッチ・ソリューションについては、どのパッチがいつ誰により展開されたという情報が表示され、パッチが適用されたという自動確認が行われます。

セキュリティー構成管理

BigFix Compliance には CIS, DISA STIG, USGCB, PCI DSS などが公表している権限あるセキュリティー・ベンチマークに基づいて開発された広大なチェックリストが追加設定なしにすぐ使える状態にあります。チェックリストに含まれるチェックは、各組織のセキュリティー・ポリシーに対応するよう簡単にカスタマイズできます。エンドポイントにチェックリストが適用されると、BigFix はエンドポイントのセキュリティー構成を展開したチェックリストと照合して評価し続けます。コンプライアンス状態も継続的に収集され BigFix サーバーにレポートされます。「逸脱した構成」があってもすぐに特定され、管理者が見つかった構成の問題をリモートで修正できます。IT環境全体にわたるセキュリティー構成の監視・レポート・修正という強力なアプローチを取ることで、各組織はエンドポイント・セキュリティー・ポリシーを強制し、セキュリティーリスクを最小限化し、効果的にエンドポイント管理コストを削減できます。

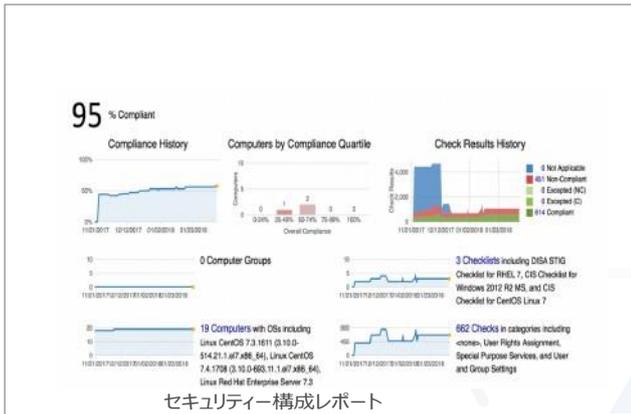
Compliance Analytics

BigFix の強力な Compliance Analytics エンジン、データベースおよび UI を使って、展開したポリシーに対する全エンドポイントのコンプライアンス状態を継続的に収集し、連結化して、レポートします。展開全体または各エンドポイントの現在の状態および履歴トレンドを示す多様なコンプライアンス・レポートには、セキュリティー、IT 運用、コンプライアンス・チームなど様々なニーズに合わせた包括的なアナリティクスがあります。Compliance Analytics を使って各組織はそのコンプライアンス努力の効果を追跡して、セキュリティー曝露やリスクを迅速に特定できます。Compliance Analytics は3つのセキュリティー分野全体にわたって一貫したレポートを提供します。

セキュリティー構成、パッチおよび脆弱性

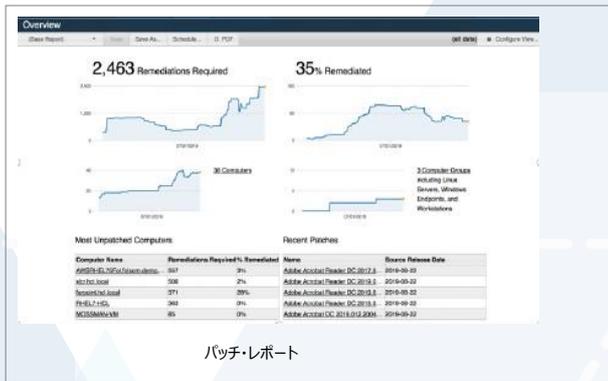
セキュリティー構成レポート

BigFix Compliance を使って環境全体にわたって展開されたセキュリティー構成チェックリストのすべてのについて、Compliance Analytics は様々なレポートを提供して、個々のエンドポイント、個々のチェックリスト、さらには個々のチェックのレベルに至るまで現在の状態と履歴の両方の傾向を表示します。また希望するセキュリティー構成ポリシーに向けた全体的な状態や進捗状況をレポートする、展開全体の統合的コンプライアンス・ポスターも提供されます。



パッチ・レポート

パッチ・レポートは BigFix Compliance のアナリティクスおよびレポート能力をセキュリティ構成からセキュリティのパッチ適用まで拡張したものです。この機能により各組織は展開全体にわたってパッチ適用作業を包括的に見て、全体的なパッチ適用の状況の評価ができます。またクリティカルで重度の高いパッチで未適用のものを特定することにより脆弱性修正の優先付けを効果的に行えます。さらに各パッチのリリースと各エンドポイントへの適用を追跡し、法令 / ポリシーへの各組織のコンプライアンスを示して、監査の合格をサポートします。



脆弱性レポート

BigFix Compliance Vulnerability Reporting は BigFix 10 に新たに導入されたもので、パッチ適用のアクションの結果としてのエンドポイントの脆弱性ポスターを追跡・レポートに重点を置いています。これにより各組織はより広範囲にリスクを特定し、コンプライアンスを示すことができます。この脆弱性レポート機能は多数のチームに重要な価値をもたらします：

- **リスク・ポスター評価：**セキュリティ・オペレーションセンターのマネージャーやセキュリティ・アナリストは各ポイントや環境全体にわたって存在した様々な重度の脆弱性詳細の現在の状態、履歴トレンド、詳細を把握できます。
- **修正タスクの優先付け：**IT オペレーション・スペシャリストはパッチ適用アクションを効果的に優先付けするための情報をより多く得られるようになり、脆弱性ポスターの変更に対する影響を最大にできます。
- **脆弱性に関するコンプライアンスの証明：**コンプライアンスのスペシャリストはパッチ適用アクションにより脆弱性をどのように修正したかを報告し、特定の法令または組織のポリシーへのコンプライアンスを証明できます。

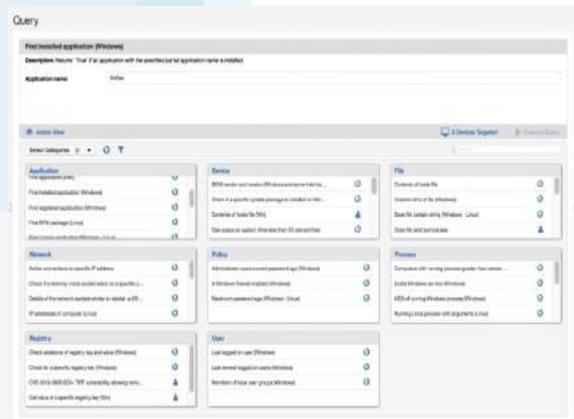


不適合システムの検疫

社内のイントラネットにエンドポイントがアクセスする方法をエンドポイントの状態や構成を事前定義したポリシーに照らし合わせて厳密な管理を望んでいる組織はたくさんあります。たとえば、最新のセキュリティ・パッチをインストールしていないエンドポイントや、アンチウイルスツールの提供される最新のウイルス定義を適用していないエンドポイントにはイントラネットへのアクセスを許可されません。BigFix Compliance には自己検疫機能があるため、エンドポイント・ポリシーのコンプライアンスに即していないエンドポイントがあることが判明した際には、そのコンプライアンスが達成されるまで当該エンドポイントはネットワーク検疫に置かれます。検疫を受けているエンドポイントには（修正を行うために）依然として BigFix との接続がありますが、他のネットワークアクセスはすべて無効化されます。

エンドポイント検査

BigFix Query により全エンドポイントの状態がリアルタイムで把握でき、ユーザーフレンドリーな Web インタフェースを使って脆弱なデバイスの正確な特定と検査が行えます。エンドポイントに直接問い合わせを行っても数秒で正確な応答が返され、どのポリシーが強制されているか、どのアプリケーションやサーバーがインストールされているかが分かります。さらにファイルやシステム構成まで調べられるため、さらなるセキュリティ脅威も識別できます。また事前定義されたクエリの使用や、ユーザー独自のカスタムクエリの作成を迅速且つ容易にできます。BigFix Query はエンドポイントの修正を検証できるため、セキュリティと IT 運用の間のギャップを埋めて、自社環境に適正なテクノロジーを選択できます。



Payment Card Industry Data Security Standard (PCI-DSS) へのコンプライアンス

BigFix Compliance Payment Card Industry (PCI) Add-on は、最新の PIC-DSS 要件を満たすために必要なポリシー強制とコンプライアンス・レポートに対応するベグデザインされたものです。特定の PCI-DSS の構成およびポリシーへのコンプライアンスチェックと専用の各ダッシュボードにより、PCIへのコンプライアンスのモニターとレポートが単純化されます。またシステム構成と通貨を継続的且つ自動的に管理する機能によりエンドポイントのセキュリティとインテグリティが改善されます。これらの機能が一緒になって、OPEX とセキュリティ管理コストを抑えつつも、悪意による、あるいは意図しない機密顧客の損失を防ぎ、財務情報を保護します。これにより、クレジットカードのデータ漏洩によって発生しがちな否定的な報道や法的・財政的な悩みから解放されます。



BigFix Family

BigFix への投資はエンドポイント管理を変え、ソフトウェアコストを削減し、360度の可視性を実現します。BigFix の顧客は自宅勤務など新しい働き方をサポートする一方で、ITツールとエンドポイントを大幅に集約させました。

BigFix Family には以下のものがあります。

- **BigFix Inventory** — ユーザーはデスクトップ、ラップトップおよびサーバーにインストールされたアプリケーションを発見・分析し、ソフトウェア・パブリッシャー、タイトル、アプリケーションなどに関する情報をバージョンレベルにまでドリルダウンができます。インベントリーには、組織が所有しているもの、インストールはしてあるが所有していないもの、ソフトウェアの使用頻度など重要なインサイトがあります。
- **BigFix Lifecycle** — 数十万件のエンドポイントを数時間・数分間のうちに迅速に発見・捕捉・管理し、Windows, UNIX, Linux, macOS を実行しているエンドポイントで、オンプレミス、ローミング中あるいはクラウド上に関わらず、98% 以上のファーストパス・パッチ成功率を誇る自動化・単純化されたパッチプロセスを提供します。BigFix Lifecycle にはまた、OS プロビジョニング、ソフトウェア展開、リモートコントロール、サーバー自動化、電力管理、Insights の高度化アナリティクス・プラットフォーム、モダン・クラウド管理、先導的な脆弱性管理システムとの統合なども含まれています。
- **BigFix Insights** — Analytics Platform — このプラットフォームを使って BigFix のデータをサードパーティーのソリューションからのデータと組み合わせ、企業のトレンドを迅速に可視化し、組織の大部分にとって重要なエンドポイントの問題を優先付けて自動的に対応させることができます。その結果、対応が迅速化しプロセスが合理化され、コンプライアンスが向上します。BigFix Insights は BigFix Lifecycle にも BigFix Compliance にも含まれています。
- **重要な連携・統合機能** — エンドポイント管理プロセスと様々な関係者が利用するエンドポイントデータの自動化により、IT およびセキュリティ組織のスタッフの生産性を向上し、ROIを増やすことができます。最新の連携・統合機能を2例挙げます。

BigFix Insights for Vulnerability Remediation Module — 脆弱性管理システムにある迅速な脆弱性修正で、スキャンしたデータを BigFix Fixlets に自動的に相関付けることによってこれを実現します。このモジュールは BigFix Lifecycle V10 または BigFix Compliance V10 のライセンスを有するユーザーが利用できます。

BigFix ServiceGraph Connector — ServiceNow® CMDB にデータが自動的に、かつほぼリアルタイムに格納され、エンドポイントデータの活用が実現できます。

利用可能なその他のインテグレーションについては担当の BigFix スペシャリストにお尋ねください。

なぜ BigFix なのか?

BigFix は判断機能をエンドポイントに分散させた独自の目付高度にスケーラブルに構築されています。このことにより、エンドポイント管理コストと複雑性を軽減する一方で、BigFix Family のソリューション全体にわたってきわめて機能的な利点とパフォーマンス面の利点を得ることができます。

BigFix の機能

- **単一のインテリジェント・エージェント** — BigFix エージェントは、継続的な自己評価、ポリシー強制などを含む数多くの機能を、システムへの影響を最小抑えつつ、実行します。アクションをインテリジェントに開始させ、上流の中央の管理サーバーにメッセージを送信して、リアルタイムにパッチ、構成、その他の情報をエンドポイントに引っ張ってきます。BigFix エージェントは Windows, Linux, UNIX, macOS の 90 以上の OS に対応されます。
- **BigFix Fixlets™** — BigFix Fixlets は日々の運用や繰り返しの作業を単純化させる自動化スクリプトです。BigFix には 500,000 件以上のすぐに使える Fixlets があり、HCL BigFix チームが月間平均 130 件の Fixlets を配信してライブラリーを更新しています。BigFix ユーザー、ビジネスパートナーおよび開発者はカスタム Fixlets を作成してカスタムポリシーやエンドポイントサービスを実装させることができます。Fixlets のコミュニティ・ライブラリーが BigFix.me にあります。
- **高いスケーラビリティに対応できるアーキテクチャー** — 単一の BigFix 管理サーバーで、プライベートまたはパブリック・ネットワークを介して最大 250,000 の物理および仮想コンピューターを管理できます。管理対象のエンドポイントにはサーバー、デスクトップ、ローミング中のラップトップ、クラウド内のエンドポイント、店頭 (POS) デバイス、現金自動預払機 (ATM)、セルフサービス・キオスクなどの専用機器などがあります。
- **マルチクラウド・サポート** — クラウド・エンドポイントは、従来型のエンドポイントと共に、簡単に発見・表示できます。何が環境に存在するかを知ることが大切です。BigFix を使うと BigFix エージェントをクラウド・エンドポイント上に展開して、完全な可視性・コントロール・セキュリティを実現することができます。これにより、Amazon Web Services, Microsoft Azure, Google Cloud Platform, VMware など複数のクラウド環境上で実行されるエンドポイントを、BigFix が管理する他のエンドポイントと共に管理できます。



さらに詳しい情報

BigFix についてもっとお知りになりたい場合には、HCL Software の代理店や HCL Business Partner にご連絡いただく www.BigFix.com をご覧ください。

HCL Software について

HCL Software は HCL Technologies の一部門であり、柔軟性の高い消費モデルを持つ企業レベルのソフトウェアベースのオファーの次世代ポートフォリオを開発・提供しています。これらオファーは従来型のオンプレミスのソフトウェア、Software-as-a-Service (SaaS) からバンドル化されたマネージドサービスまでカバーしています。弊社はお客様が価値を作り出すためのスピード、インサイト、革新 (大規模なものも小規模なものも) をもたらします。HCL Software の分野には DevOps、セキュリティ自動化、アプリケーション近代化、データおよびインテグレーション基盤、一部のビジネス・アプリケーションなどが含まれます。HCL はメインフレームからクラウドに及ぶマルチモードに至るまで、あらゆるマルチモードITにおける現実世界の複雑性に対処しつつ、お客様の成功を主眼を置き「契約を超えた関係性」を構築します。

© Copyright 2020 HCL

HCL Corporation Pvt. Ltd.

Corporate Towers,

HCL Technology Hub, Plot No 3A, Sector 126,

Noida - 201303.UP (India)

Produced in the United States of America.

製品名、商標名、登録商標名はすべてそれぞれの所有者の資産です。