FIREEYE™

ソリューション・ブリーフ

クラウド・セキュリティに対する継続的なコンプライアンス保証

考えるべきシナリオとは

現時点で100%コンプライアンスに準拠している2つの承認を受けたシステム、システムAとシステムBがあるとします。しかし、長期間、システムAとシステムBのデータベースのレプリカとして機能していた未承認のシステムCに関する記録は残されていなかったとします。この場合、システムAとシステムBに対する注意義務を履行していた、つまりデュー・デリジェンスの証拠はなにもないことになります。

現時点で100%コンプライアンスに準拠している、承認を受けたシステムDがあるとします。しかし、最後の監査から現時点までの期間のコンプライアンスに関する証明がありません。この場合、システムDのデュー・デリジェンス証明は、「現時点」で証明可能な部分に限定されることになります。

多くの場合、コンプライアンス監査では、継続的、もしくは繰り返される、現在進行中のデュー・デリジェンス証明の提示が求められます。

その証明が繰り返し必要だったり大規模なものである場合、運用コスト削減のためにも、可能な限りで自動化が必要です。

コンプライアンスの継続的な保証

コンプライアンスの保証とはつまり、デュー・デリジェンス証明手段を確立することです。結果、グループや個人、組織は、法的その他の免責を得ることができます。コンプライアンスの保証に関する活動に必要となる投資は、デュー・デリジェンスを効果的に実現できる限り妥当とみなされており、それに応じたセキュリティ予算が確保されます。

しかし、コンプライアンスの保証に必要な予算がセキュリティ予算を大きく凌ぐような場合、コンプライアンスの保証は、高度な攻撃に対するあらゆるセキュリティ対策の礎でもあるべきです。コンプライアンス・チェックだけでは、すべての高度な攻撃を阻止することができないとしても、さまざまな基本的事項確認を継続的に検証し、コンプライアンス・チェックを繰り返し行うことにより、ノイズの大幅な除去が期待できます。

コンプライアンスの確認作業の自動化は、コンプライアンス活動を徹底的かつ効率的に行う最善の方法です。必要なのは、自動化による効率向上でコストを節約しながら、アセットを幅広くカバーし、さまざまなレベルでそれぞれのコンプライアンス状態を提供できるような、本当に役立つコンプライアンス保証ソリューションです。クラウド・アプリケーション（サーバーレス機能など）、ネットワーク（VPNなど）、サービスとワークロード、従来型のオペレーティング・システムの設定とパッチなどを対象に含めておくべきでしょう。

核心的な問題

パブリックおよびプライベートのクラウド環境のコンプライアンス保証を継続するにあたって、セキュリティ・チームは数多くの課題に直面するでしょう。特に大変なのは、さまざまなクラウド・アセットが、複数のクラウド・プロバイダー、アカウント、OS、リージョン、サービス、その他の論理グループに及ぶような場合です。

マルチクラウド環境のアセットの状態とコンプライアンスの履歴の両方を可視化する、包括的かつ自動化された手法がない限り、コンプライアンス監査のたびに担当者は膨大な時間を割かなければならなくなります。担当者にとって、コンプライアンス保証に関する作業は大きな業務中断を招くものです。さらに多大な運用コストがかかり、利益に直結した活動でもありません。

プロセスの自動化やツール化を行おうと苦戦する場合もあるでしょう。しかしDevOpsモデルを活用してコンプライアンスの保証の効率化を図るのは困難です。

また、コンプライアンス保証にまつわる問題解決に有効な技術ソリューションもなかなか見つかりにくいものです。その理由として、従来のコンプライアンス・ツールには、以下の重要な機能が欠けていることが挙げられます。

- API経由でクラウド・プロバイダーからアセットのインベントリ情報を自動的に収集する
- インラインで攻撃を検知、ブロックする強制力のある、コンプライアンスのガードレール的機能
- クラウドレベルおよびOSレベルでの脆弱性に対する包括的な可視性
- アラートやレポート、検知やブロックなど、コンプライアンス違反の検知と対応
- 業務ニーズに応じた、コンプライアンス規則に対する時間的例外の取り扱い
- 検出したアセットのサブセットに対する、コンプライアンス設定のグループレベルでの設定
- 特定のアセットに対する、オンデマンド（APIベース）のコンプライアンス・スキャン
- リスクの復旧対応のトリアージを可能にするリスク解析
- 一般的なコンプライアンス・レポート基準としての、標準化されたサポート

必要なソリューション

クラウド環境とは本質的に動的なものです。クラウド・ユーザーは、必要なリソースを必要な時に作成することができますが、これは同時に、リソースが勝手に作成されたり、変更されたり、あるいは破壊されうることを意味します。

クラウド・アカウントの認証情報が侵害されると、ハッカーは、従来の監視ツールの対象外となる、安全でない無許可のリソースに自由勝手にアクセスできるようになります。対象となるすべてのインフラ資産に対して継続的にデュー・デリジェンス証明を得る、すなわちコンプライアンスを継続的に保証するためには、以下の条件を満たすクラウド・セキュリティ・ソリューションが必要です。

- 対象となるアセットの、詳細で検索可能な各アセットの状態の記録を含む完全なインベントリを継続的に維持
- 各アセットに関する、ソリューションにより生成されたコンプライアンス・チェックの結果を含むセキュリティ関連のイベントの完全な履歴を記録

ひとつのソリューションで、複数の論理的および物理的インフラをまたがった、コンプライアンス保証を評価できれば理想的です。こうすることで、事前定義されたクエリとアドホックのクエリを使用して、論理的な属性別にリスク（コンプライアンス・エラー）を集約できるようになり、DevOpsやSecOpsの担当者は、脆弱な領域に対するリスクの復旧作業を優先させることができます。

コンプライアンスを保証するソリューションは、クラウド・プロバイダーのAPIから収集したコンテキストを利用して、多くのコンテキスト情報を含むデータ・セットを提供します。ユーザーはUIやAPI経由でこのデータ・セットに対してクエリやフィルタリングを行うことで、カスタマイズされた新しいコンプライアンス・チェックを作成することができます。アセットのインベントリの基本的な監査、コンプライアンス・チェックの結果、コンプライアンスの保証のレポートを使用することは、効果的かつ簡単であるべきです。ソリューションのコンプライアンス・エンジンは、組織に固有のニーズに沿って、より高度で非定型的な形式のコンプライアンス・チェックに対応する柔軟性が必要です。

継続的なコンプライアンス保証の要件

- **幅広さ**
  クラウドのアカウント、クラウド・サービス、IDオブジェクト（ユーザー、グループ、役割など）、ネットワーク、オペレーティング・システム、パッチなど、現代の各種テクノロジーにおいてさまざまなレベルで、広範なコンプライアンス・チェックを行う能力。

- **深さ**
  アセットの設定と振る舞いの両方に関して、コンテキスト情報を含む深いデータを収集する能力。多くのセキュリティ製品は、幅広さを優先して深さを犠牲にしたり、逆に深さを優先して幅広さを犠牲にしています。理想的なソリューションとは、現代の各種テクノロジーにおける複数のレイヤー（レベル）にわたって、コンプライアンスの状態に関して深い適用範囲を提供するものであるべきです。

- **統合**
  既存の運用ツールと連携する能力。コンプライアンスの不備の早期検知に対する関心が高まる中、自動コンプライアンス・チェックを既存のDevOps導入（CI/CD）パイプラインと統合することが、ますます重要になっています。ソリューションは、オンデマンドのコンプライアンス機能を機敏なテスト環境に統合するために、RESTful APIを提供すべきです。そうすれば、導入チームは、コンプラインスの不備を早期の検査環境（開発、ラボ、品質保証など）で検知し、修正することが可能になります。

Cloudvisoryの提供するソリューション

Cloudvisoryは、マルチアカウント、マルチクラウド、マルチオペレーティング・システムなどの環境に対し、継続的なコンプライアンスの保証を提供します。任意の設定が可能なチェックを既知のアセット、コントロール、イベントに対して行って、リスクを自動的に検知します。一方で、手動および自動で対応するためのオプション（アラート、レポート、復旧）も提供しています。Cloudvisoryのコンプライアンスには、1,300を超えるコンプライアンス・チェックが事前設定されています。これらのコンプライアンス・チェックをカスタマイズし、自組織用に新しいチェックを追加することができます。

ポイント&クリックのシンプルなユーザー・インターフェイスで、アドホック監査で明らかになった「気づき」を、継続的なコンプライアンス・ガードレール（繰り返しの間隔を設定可能なコンプライアンス・チェック）として簡単に実装できます。検出されたクラウド・アセットに関連するコンプライアンス・チェックの全履歴を追跡し、コンプライアンス保証に関する内外の要件に適合するよう、豊富なレポート機能を提供します。すべてのコンプライアンス・チェックと、その中のあらゆるサブセット（カスタマイズされた内部基準向けまたはコンプライアンスのレポート用）について、さまざまなフォーマット（PDF、XLS、CSVなど）でコンプライアンス・レポートを簡単に生成、エクスポートできます。また、一般的なコンプライアンス用のレポートが事前設定されています。

Cloudvisoryを選ぶ理由

真に継続的な、統合されたコンプライアンス保証を提供できるのは、Cloudvisoryだけです。他の製品は、以下の重要な機能をサポートしていない場合があります。

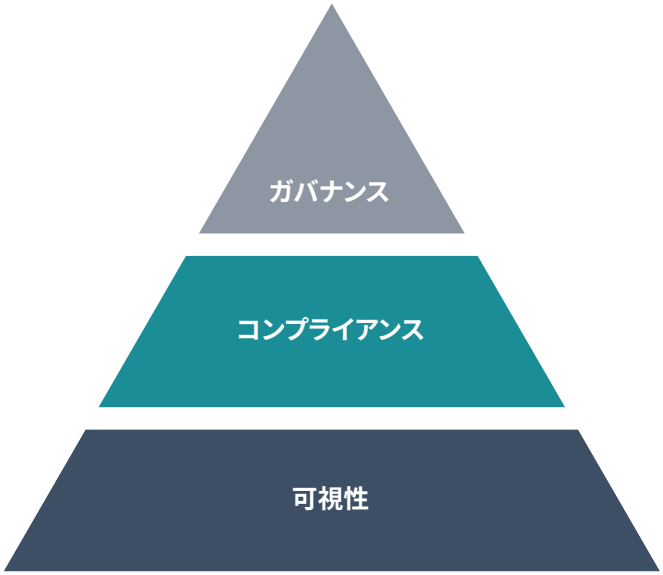
- さまざまなクラウド・プロバイダーやオペレーティング・システムを幅広くカバーすること
- クラウドやOSなど、任意のコンプライアンス対象で有用となるレベルのデュー・デリジェンスを確立するために必要な幅広いカバー範囲を持つこと
- コンプライアンスの自動化を既存の運用プロセスやツールに統合するために必要なRESTful API

Cloudvisoryのコンプライアンスは包括的な可視性による強力な基盤の上に築かれており、任意のアセットについて、コンプライアンスのさまざまなレベルと状態を評価するためのコンテキストを提供します。Cloudvisoryのコンプライアンスは基本的な組み込み機能として提供されています。たとえば、インラインの復旧、承認に基づくコンプライアンス規則の一時的例外適応、Cloudvisory APIを介した特定のアセットに対するオンデマンドでのコンプライアンス・スキャン、論理的および物理的なインフラの境界を越えたリスクに対する評価、リスク集約のドリルダウンなどが挙げられます。

他の製品は、単一クラウド・プロバイダーや単一OSのみを対象とするなどの限定的なコンプライアンス機能を提供している場合があります。また、ログファイルのみを基にするなど限定的な可視性に起因する、一貫性に欠けた価値の少ない結果しか提供できていないこともあります。Cloudvisoryは、エンタープライズ機能の中核を、市場をリードする拡張可能なコンプライアンス・フレームワークと結びつけます。Cloudvisoryなら、あらゆる環境でコンプライアンスを保証するための活動を簡単に自動化でき、組織は少ないコストでより良いセキュリティを実現できるようになります。

同時利用でより良い効果を

Cloudvisoryのコンプライアンスは、Cloudvisoryの可視性によって得られる深いコンテキストの基礎の上に構築されています。Cloudvisoryのコンプライアンスは、任意のコンプライアンスの目的に拡張可能ですが、多くのカスタマイズした基本的なコンプライアンス・チェックを、Cloudvisoryの可視性によって提供されたデータ・セットに対するアドホックのクエリから簡単に作成することができます。Cloudvisoryの可視性が提供し、Cloudvisoryのコンプライアンスで使用される主要なデータ・セットには、クラウドのリソースの設定（VMなど）、クラウドのセキュリティ・コントロールの設定（IAMポリシー、ネットワーク・セキュリティ・グループなど）、クラウドのオブジェクトのログ、ネットワーク・フローのログ、オペレーティング・システムの設定、オペレーティング・システムのログが含まれます。カスタマイズされたコンプライアンス・チェックのバッチは、Cloudvisoryで簡単に作成でき、コンプライアンスの保証に関するニーズを満たします。



対象コンプライアンス基準

クラウド・プロバイダー

- AWS CIS Benchmark
- AWS GDPR
- AWS HIPAA
- AWS NIST 800-53 Revision 4
- AWS PCI DSS 3.2
- Azure CIS Benchmark
- Azure GDPR
- Azure HIPAA
- Azure NIST 800-53 Revision 4
- Azure PCI DSS 3.2
- Kubernetes CIS Benchmark
- OpenStack Security Checklist

オペレーティング・システム

- CentOS CIS Benchmark
- Redhat CIS Benchmark
- Ubuntu 16.04 CIS Benchmark
- Ubuntu 18.04 CIS Benchmark

対象クラウド・サービス・プロバイダー

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

Gartner Cool Vendor 2018

Cloudvisoryは「Cloud Security 2018」でGartner Cool Vendorに選ばれました。

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS-2017

Cloudvisoryは、CIO Application誌におけるAmazonソリューション・プロバイダーの上位25社に位置付けられました。

AICPA SOC

Cloudvisory-SaaSは単独でSOC2認証を受けています。

FireEyeの詳細については、**www.FireEye.jp/solutions/cloudvisory**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03-4577-4401 |
Japan@fireeye.com

©2020 FireEye, Inc. All rights reserved. FireEyeはFireEye, Inc.の登録商標です。その他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。
CS-EXT-SB-JA-JP-000300-02

FireEyeについて

FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデントレスポンスといった、組織がサイバー攻撃対策をする上での課題となっていた複雑性や負担を解消します。

FIREEYE™