FIREEYE™

ソリューション・ブリーフ

クラウド・セキュリティの可視化という課題

40万人を対象とした調査では、43%が主な課題として「インフラに対するセキュリティの可視化」を挙げています。

Cloud Security Report
Cybersecurity Insiders

考えるべきシナリオ
ほぼすべての企業は何らかの攻撃を経験していると思われますが、データ侵害が発見されるケースはまれです。

検知された数少ない事例でも、検知までに6〜12か月かかっており、それも、たまたま見つけたというものや、取引先やセキュリティ企業など第三者からの指摘によって知ったというものです。

侵害は、組織内の力によって見つけ出すよりも、善意の外部者から知らされることの方が多くなっているようです。

さらに、この結果はあくまでもデータ侵害を受けた時点で「コンプライアンスを考慮している」組織に対する調査の結果であり、コンプライアンスやデータ侵害調査を気にかけないような組織についての情報は反映されていません。

同じことなら、お客様に指摘されるよりも、自社内で早期に攻撃を発見するに越したことはないでしょう。

可視化のギャップ
可視化は、クラウド・セキュリティ戦略における最重要基盤です。すべては可視化次第であるとさえ言えるでしょう。コンプライアンスの確保、脅威ハンティング、ガバナンス・ポリシー、リスクの復旧などをクラウド・セキュリティ戦略の中心に据える企業は多いでしょう。

しかし可視化は、多くの組織にとってクリアすることのできないハードルなのです。セキュリティ担当者を対象とした調査では毎年、インフラ・セキュリティの可視化が最重要課題として挙げられています。

その他の高度なセキュリティ戦略に取り組む前に、まずこの可視化とのギャップ問題に対処する必要があります。

核心的な問題
セキュリティ・チームは、企業内部で水平展開する攻撃に対する、中央集中管理可能でコンテキスト情報が豊富なセキュリティ・オペレーション（SecOps）に関わる、さまざまな課題に直面しています。

組織が成長し、それぞれの部署に所属する社員たちがさまざまなテクノロジーを利用するために多くのクラウド・プロバイダー、アカウント、地域、サービスを利用するようになると、可視化のギャップはさらに大きくなります。

セルフサービスの導入で業務の効率は上がりますが、一方で、安全なインフラを提供したり、監視することができなくなります。クラウド・テクノロジーによって、さまざまな形で、インフラ導入はより大規模、分散的、かつ動的なものになり、場合によっては導入後すぐ撤収することも可能になりました。従来型のセキュリティ・ツールは、このクラウドのスケールとスピードに追いつくことはできません。過去10年間で、導入自動化テクノロジーの進歩は、適合性、機能、成熟度といった点で、セキュリティ自動化テクノロジーの進歩を上回っています。

従来、SecOpsは、攻撃の検知よりも防御に重点を置いてきました。しかし、防御はいつか破られます。従来、防御は企業の境界線における、静的に定義された対策を中心に行われてきました。しかし、クラウドにおける境界とは静的ではなく動的であり、論理的に定義されるものであって、物理的な境界は存在しません。

分散的かつ動的なクラウド環境において、従来型のセキュリティ・ツール（物理的もしくは仮想ファイアウォールなど）による攻撃の検知やブロックは困難です。クラウドの急激な変化と企業におけるクラウド利用の分散化と多様化は、セキュリティ・ソリューションがクラウド環境全体への可視化を提供することを困難にしたのです。

求められるソリューション
ここで求められるソリューションには、現状設定やアセットに関連するセキュリティ・イベント履歴を、広範かつ詳細に監視する能力が求められます。

インフラ・セキュリティを包括的に可視化するには、以下の目的で、さまざまな可視性を同時に得る必要があります。

- **すべてのアセットのインベントリ情報を常に確保する**
  監視対象となるすべてのアセットの完全なインベントリ情報（現状および履歴）の可視化は、不完全なコンプライアンス監査やセキュリティ解析を避けるためにも必須です。
- **あらゆるアセットの現状について、コンテキスト情報を検索可能にしておく**
  コンテキストは、監視対象となるすべてのアセットの現状を可視化することで得られます。コンテキストがないと、コンプライアンスの確保や異常検知といった概念の意味も有効性も失われます。
- **各アセットに対する監視対象のセキュリティ・イベントの履歴を完全に記録する**
  ワークロードとユーザーの実際の行動に対する可視化を行わない限り、ガバナンス・ポリシーが実際に機能しているかの確認や、特定のインフラが不正なユーザーによって乗っ取られていないという確証を得ることができません。

単にログからアセットのインベントリやアセットの状態に関するデータを引き出すだけでは、不十分といえます。データギャップは、立ち上げ期間やサービス中断時、もしくはその他の不具合の結果、生じます。

発見したアセットやサービスに関連するクラウド・プロバイダーのAPIからアセットの現在の構成状態が直接的にわからない場合、アセットのインベントリは不完全であり、攻撃者が検知を容易にすり抜ける可能性があります。ログは役に立つストーリーを提供してくれますが、API経由の情報に嘘はありません。

したがって、必要となるソリューションは、大規模、短期的、サーバーレスなどの可能性のある、ハイブリッド・クラウドやマルチクラウドなどの、複合的かつ分散型の導入環境に対して包括的な可視化を提供するものとなります。求められるソリューションは、包括的な可視化機能はもちろん、各アセットに関する入手可能な、あらゆる形状のコンテキストについて、統合的で検索可能な可視性を提供できるものでなければなりません。可視化ソリューションでは、クラウドの境界を越えて実施されるセキュリティ解析やコンプライアンス監査を実施するインターフェイスにより、UIやAPI経由であらゆるアセットのコンテキストをアドホックに検索可能でなければなりません。

理想的なソリューションでは、アドホックな監査クエリを定期的なコンプライアンス・チェックとして利用することができるため、可視化ギャップがなくなるだけでなく、コンプライアンスの確保、ガバナンス・ポリシー、脅威ハンティングといった、より高度なセキュリティ対策の基盤としても、包括的な可視性を利用することができます。

CLOUDVISORYが提供する可視化

Cloudvisoryは、あらゆるインフラ・セキュリティに対する包括的な可視化を、単一のソリューションとして提供します。アセットのディスカバリーは自動実施され、監視対象となるすべてのアセットのリアルタイムなインベントリ情報が維持されます。Cloudvisoryは、監視している環境に存在したことのあるすべてのアセットについて、最新状態に関する詳細な情報を保存するため、クラウド・プロバイダーのAPIを通じて行われる自動ディスカバリーによって発見されるアセットは、深いコンテキスト情報を持つことができます。アセットの状態には、複数の層から成る詳細なコンテキストから得た情報が含まれます。各アセットに関する情報には次のようなものがあります。

- **クラウドに関するコンテキスト：**アセットに関連するクラウド・プロバイダー/アカウント/地域/グループ/役割などについての情報
- **履歴に関するコンテキスト：**アセットのライフサイクルの中で作成された、セキュリティ・イベントの履歴の記録から得た解析
- **セキュリティに関するコンテキスト：**アセットのセキュリティ・コントロールの現状の構成
- **システムに関するコンテキスト：**アセットのオペレーティング・システムから直接記録された現状の情報

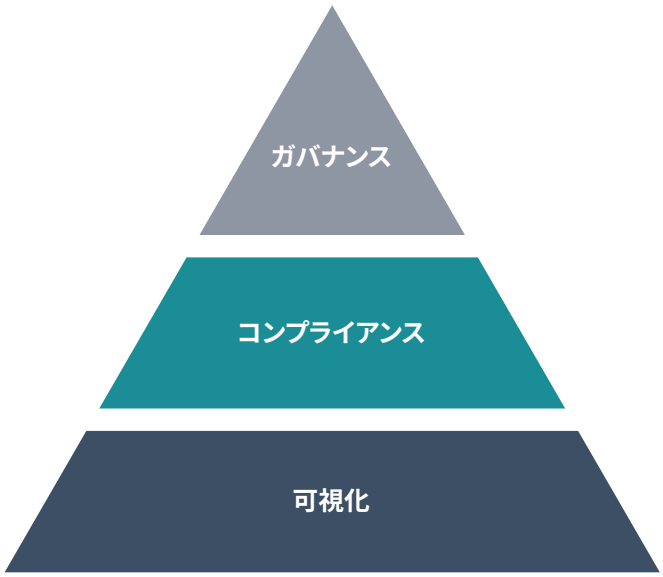
Cloudvisoryを選ぶ理由

Cloudvisoryソリューションは、マルチクラウドでマルチなオペレーティング・システムを利用するあらゆる環境に、最適な保護を提供します。Cloudvisoryは、広範かつ詳細なカバレッジを提供するほか、各コンポーネント（可視化、コンプライアンス、ガバナンス）が連携して機能するよう設計されたソリューションです。

単一クラウド・プロバイダー内の複数デプロイメントやアカウントに対するセキュリティ体制を迅速に評価する製品は数多くあります。また、多くの組織はハイブリッド・クラウドやマルチクラウド戦略を持っており、それに対するセキュリティ対策は非常に限定的です。しかし、包括的な可視化を通じた即効的な投資対効果があり、さらに今後数年間にわたって効率とセキュリティの両方に対する改善をもたらす将来性も備えた、マルチクラウド向けセキュリティ・ソリューションが一つだけ存在します。それがCloudvisoryです。

同時利用でより良い効果を

可視化はコンプライアンスの基盤になりますが、コンプライアンス・チェックを繰り返し行うことで、可視化データが生まれます。この相乗関係が付加的なセキュリティと履歴に関するコンテキストをもたらします。コンテキストをインプットとして機械学習を行うアルゴリズムが、インテリジェントな最小権限ポリシーとして生み出されるのです。



対象クラウド・サービス・プロバイダー

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

対象OS

- CentOS
- Redhat
- Ubuntu Linux

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。

Cloudvisory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-000302-01

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™