FIREEYE™

ソリューション・ブリーフ

クラウド・セキュリティのための ポリシー・ガバナンス強化

考えるべきシナリオとは

ポリシー・ガバナンスの自動化はそう難しいことではありません。しかし、真の最小権限ポリシーの規則だけを用いてポリシー・ガバナンスを自動化するのは困難です。

真の最小権限ポリシーを妥当な規模で作成するのは、特に困難です。

真の最小権限ポリシーの作成が困難な理由は、専門化したセキュリティ・コントロールに関する深い知識と、導入環境に関する深い知識、つまり、所定のコントロール群により統治されるさまざまなエンティティ（アプリケーション・サービス、システム、ユーザーなど）に予想される振る舞いとそのエンティティ間の関係に関する知識の両方が必要になるからです。

実際のネットワーク・ポリシーの作成者が、最小権限によるセキュリティと導入環境の両方に深い知識を有していることは稀です。

クラウド・プロバイダーのAPIからのデータを人工知能に与えることで、環境の振る舞いに関するコンテキスト情報が自動的にマシンに供給され、これによって、任意の規模でより優れた最小権限のセキュリティ・ポリシーが生成されます。

マシンで収集されたインテリジェンスによるポリシー・ガバナンスの強化

どのクラウド・プロバイダーも、最小権限のポリシー・ガバナンスのための、APIによるきめ細かいコントロールを提供しています。これらのセキュリティ・コントロールは、設計上はきめ細かいかもしれませんが、実際の設定では穴だらけであることがよくあります。自動化ツールを用いてプロビジョニングした場合でも、簡便さを求めてか、無知からか、あるいは不正な意図があってか、重要なセキュリティ・コントロールの設定ミスは一般的によく見られます。

クラウド・プロバイダーは、短期的な導入やハイパースケールの導入を可能にする、さまざまな機能やサービスも提供しています。成熟した導入自動化テクノロジーが広く利用され、その管理下にあるリソースと連携して、セキュリティ・コントロールの導入が自動化されています。残念ながら、このようなセキュリティ・コントロールは、最小権限アクセスのルールによるきめ細かい設定を行うという点においては、設定が不適切であったり、監査がほとんどなされていなかったりします。

組織は、Infrastructure as Code（IaC）と一時的なインフラをバージョン管理され、連携した形で導入することによる、効率的なDevOpsの導入ワークフローを維持したいと考えます。同時に、組織はSecOpsチームに対し、可視性のギャップを埋める以上のことを求める必要があります。エンタープライズ規模での優れた監視と強固なガバナンスに対するニーズは、現実のものとして差し迫っています。

組織は、より優れたきめ細かいポリシーを用いて既存の導入自動化ワークフローを強化し、コストの削減と内外の脅威の阻止を同時に実現できるような、インテリジェントな自動化を必要としています。

核心的な問題

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はるかに上回っています。この傾向は、中～大規模の企業にある共通の状況を生み出しています。複数の（分散した）DevOpsチームが成熟した導入自動化ソリューショ

ンをそれぞれ選び、その導入を独立して管理しているのです。このような導入自動化ソリューションとしては、Ansible、Chef、CloudFormation、Puppet、Salt、Terraformのほか、VM、コンテナ、プロバイダーAPIを経由した他のワークロードの連携した導入に使用されるその他のツールが挙げられます。それと同時に、中央のセキュリティ・チームは、分散したDevOpsアセットの振る舞いに対する可視性を失い、そのためガバナンスも失いました。中央のセキュリティ・チームが独自の（新しい）ツールを使用してDevOpsのガバナンスを取り戻すことは、すぐには実現しそうにありません。

SecOpsチームは、DevOps自動化ツールとの統合に苦戦しています。導入自動化テクノロジーは、あらゆる導入を作成または複製する方法を効率的に開発できますが、管理下にあるアセットの振る舞いに対する有用な可視性は提供しません。可視性のないガバナンスは、検証なしに信頼するのと同じことです。

SecOpsはこの欠陥を克服する手段を見つけなければなりません。多くの組織では、クラウド・アセットを管理するセキュリティ・ポリシーの大半を、開発者がコントロールしているからです。クラウド・テクノロジーにより実現するセルフサービスのマルチテナンシー・モデルは、導入の効率と一貫性を大幅に改善しています。しかし、組織は不確かな手段にセキュリティの判断を委ねることの危険性について知りました。多くの組織は今、長期的に利用できる、セルフサービスのマルチテナンシーのための優れたポリシー・ガードレールの必要性を認識しています。

SecOpsがこの可視性のギャップを埋める技術的方法を見出して、真の最小権限のセキュリティ・ポリシーを構築するために必要なコンテキストを得ることができたとしても、まだいくつかの課題が残ります。コンテキストの維持に多大な人的労力を必要とするなら、大規模なクラウド環境における拡張性や継続性は得られないでしょう。同時に、本番環境のアセットの管理はマシンだけに任せるわけにはいきません。自動化の形態とテクノロジー・ユーザーのグループとの間で、バランスをとる必要があります。

必要なソリューション

ガバナンス・ソリューションは、管理下にあるアセットの設定と振る舞いに対する可視性を提供するものでなければなりません。これにより、ガバナンス活動のパフォーマンスを解析し、時間をかけて改善してくことが可能になります。ガバナンスを改善する際の本当の課題は、ポリシー・ガバナンスの自動化ではありません。自動化を介して適用される最小権限のセキュリティ・ポリシーの理想的なセットを決めることです。

成熟した導入自動化テクノロジーが多くの組織で一般的に使用されるようになっている現在、ガバナンス・ソリューションはより優れたガバナンス・ポリシーの作成を自動化することに重点を置くべきであり、標準的な導入自動化パイプラインの外側で変更を導入することなしに理想的なポリシーの推奨を作成する能力を持つべきです。

ガバナンス・ソリューションの主な役割は、既存のガバナンス・コントロールを、より優れたポリシーを入力することで強化する（置き換えるのではなく）ことです。より優れたガバナンス・ポリシーを作成するには、所定のアセットのセットについての完全なコンテキストに対する深い可視性が必要となります。機械学習は、コンテキストを用いて、アセットの振る舞いを時間をかけてモデル化していくことができます。コンテキストの量が多いほど、モデルは完全なものに近づき、出力されるポリシーがより優れたものになります。したがって、インテリジェントなポリシーでガバナンスを強化するための前提条件として、ガバナンス・ソリューションは、アセットの振る舞いをモデル化して理解するために使用する多様な階層のコンテキストを収集、処理、相関分析するプロセスを自動化するものであるべきです。

理想的なソリューションとは、人工知能（AI）（機械学習）テクノロジーを用いて、クラウド・プロバイダーのAPIからアセットに関する詳細なコンテキストを取得するプロセスを自動化するものです。また、アセットに理想的な最小権限のガバナンス・ポリシーのセットを学習するための基盤として、アセットの完全なコンテキストを活用するものです。このようにしてAIにより作成されたポリシーが、既存のガバナンス・プロセスとツールを強化するために利用されます。ソリューションは、ポリシーの推奨事項をネイティブ形式にエクスポートできる必要があります。これを使用して、バージョン管理されたInfrastructure as Code（IaC）のリポジトリを更新する、あるいは既存の導入自動化ツールを用いて任意の導入に関係するセキュリティ・ポリシーを更新することができます。

Cloudvisoryの提供するソリューション

Cloudvisoryのガバナンスは、クラウド・プロバイダーのAPIとの直接的なコミュニケーションによって、ガバナンス・ポリシーのクラウドネイティブなガバナンスを提供します。Cloudvisoryは、ワークロードベースのエージェントに依存せずに、複数のクラウド・アカウントやクラウド・プロバイダーにわたるワークロードとクラウド・サービスからセキュリティ・イベントを収集、処理、初期解析する作業を、完全に自動化します。Cloudvisoryは、アセット・インベントリとセキュリティの設定に対する変更をリアルタイムで検知し、ユーザーが検知されたポリシー違反に対する対応（アラート、ロールバック、復旧など）をカスタマイズできるようにします。

Cloudvisoryは、最小権限のポリシー・ガバナンスを確立するための足掛かりの役割を果たします。これにより、組織は可視性のギャップを埋め、ガバナンスのプラクティスを改善しながら、コンプライアンスの継続的な確保を達成することができます。Cloudvisoryのガバナンスはまた、可視性とコンプライアンス機能によって提供された深いコンテキスト活用し、クラウド、履歴、セキュリティ、システムについてのアセットのコンテキストを使用して、アセットの振る舞いを自動的にモデル化します。

Cloudvisoryのガバナンスは、機械学習を利用して、管理下のアセットのニーズに基づいた最小権限のポリシーを作成する際の、困難でコストのかかるタスクを自動化します。Cloudvisoryは、ネットワークのマイクロセグメンテーションと他の最小権限のセキュリティ・ポリシーを適用するための完全なポリシー連携エンジンを提供します。また、ユーザーがガバナンスと連携に対して使用するツールを選択することもできるようになります。Cloudvisoryのガバナンスは、真の最小権限のガバナンス・ポリシーを用いて大規模なマルチクラウドの導入をサポートするための十分なパワーを備えています。また、ユーザーがより優れたガバナンス・ポリシーを用いて既存のガバナンス・プロセスを強化するための柔軟性も有しています。

Cloudvisoryを選ぶ理由
Cloudvisoryは、エンタープライズ規模の複雑なクラウド課題を効率的に解決します。

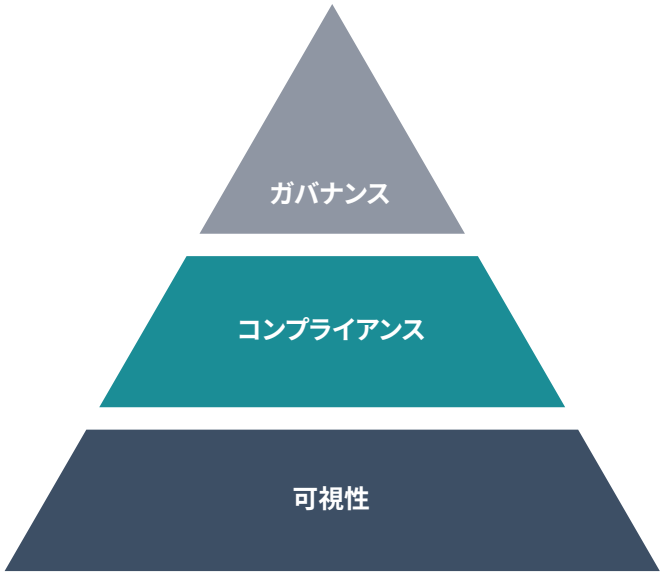
他の競合製品は高機能を謳っていても、狭い範囲の問題に対する一貫性のない結果しか生み出しません。他製品の多くは、KubernetesやOpenStackのようなパブリック・クラウド・プロバイダーのみをサポートしています。いわゆる「マルチクラウド・ソリューション」は、エージェントベースでエンドポイント頼み（オペレーティング・システム）であることが多く、クラウドネイティブと言えるものではなく、（少なくとも）クラウド・コンテキストを欠いています。

最も難しい問題は、本質的に全体的なものであり、そのような問題には包括的なソリューションが必要になります。Cloudvisoryは、クラウドネイティブでマルチクラウドのガバナンスを実現する、唯一の包括的なソリューションです。AWS、Azure、Google Cloud、Kubernetes、OpenStackなど、パブリックとプライベートのクラウド環境にわたってエージェントレスでのガバナンスのサポートを提供するのは、Cloudvisoryだけです。

包括的なテクニカル・ソリューションであっても、不十分な場合があります。テクニカル・ソリューションは、導入する人間とプロセスの間に調和がなければなりません。Cloudvisoryなら、組織やビジネス部門が、固有の要件やプラクティスに従って、ガバナンス・ポリシーを導入することが可能です。

Cloudvisoryでは、既存の自動化ツールを維持したまま、インテリジェントなマシンが組織のセキュリティ・ポリシーのガバナンスを強化します。

同時利用でより良い効果を
Cloudvisoryのガバナンスは、Cloudvisoryの可視性およびCloudvisoryのコンプライアンスを基盤として構築されています。複雑で動的なマルチクラウド環境に対して、インテリジェントでクラウドネイティブなガバナンスを提供します。Cloudvisoryの機械学習アルゴリズムは、Cloudvisoryの可視性とCloudvisoryのコンプライアンスによって提供される深いコンテキスト情報から学習し、任意の資産に関連する、クラウド、履歴、セキュリティ、システムについてのコンテキストから、できる限り多くの情報を組み入れます。コンテキストの量が多いほど、より正確なガバナンス・ポリシーが得られます。Cloudvisoryに組み込まれた人工知能により、短時間に少ない労力で、組織はより正確なガバナンス・ポリシーを生成できます。



クラウド・セキュリティのコンプライアンスを継続的に確保していくために

クラウド・セキュリティの可視化という課題

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

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™