ハイブリッド クラウド・セキュリティ を強化する

クラウドネイティブのセキュリティに関する重要な考慮事項でビジネスを保護

/選択肢をオープンに保つ

Red Hat

Red Hat セキュリティグローバル戦略およびエバンジェリズム担当ディレクター
Lucy Huh Kerner (ルーシー・ハー・カーナー)

目次

第1章

セキュリティを重視した ハイブリッドクラウド のデプロイ

クラウド導入の普及が進み、注目度は上昇し続けています。現在では、65% の企業がクラウドのヘビーユーザーであり、72% の企業がハイブリッドクラウド戦略を実施していると回答しています。[1]

ハイブリッドクラウドとは、ベアメタル、仮想化、プライベートクラウド、パブリッククラウドなどの独立した 2 つ以上の相互に接続された環境にわたるワークロードの可搬性、オーケストレーション、および管理がある程度組み込まれている IT アーキテクチャです。ハイブリッドクラウド・アーキテクチャを使用すると、接続された任意の環境でワークロードを実行し、それらを環境間で移動し、その環境のリソースを相互に互換的に使用できます。

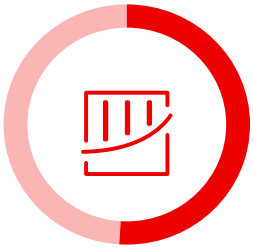
組織がハイブリッドクラウド環境を導入する目的は、次のとおりです。

- 異なるベンダーから提供されるインフラストラクチャ、プラットフォーム、アプリケーション、ツールを接続する
- 効率とスケーラビリティを向上させる
- コストを削減する
- アジリティを向上させる
- データの配置を最適化する

[1] Flexera、「Flexera 2023 State of the Cloud Report」、2023 年 3 月。

ハイブリッドクラウド導入のどの段階であっても、セキュリティは主要な懸念事項です。企業の 79% がクラウドのセキュリティを課題として挙げています。[1] ハイブリッドクラウドのセキュリティ脆弱性は、通常、認可されていないパブリッククラウドの使用、リソースの可視性の欠如、不十分な変更管理、不適切な構成管理、効果的ではないアクセス制御、人的ミスなど、リソースの監視や制御が全体に行き届かないことから生じます。このような隙があると、権限のないユーザーがそれを利用して機密データや内部リソースにアクセスする可能性があり、大きな損害に繋がりかねません。

データ漏洩の世界平均コストは 2023 年に **445 万米ドル**と過去最高を記録し、このコストの **29.2%** はビジネス上の損失が占めています。[2]



51%

情報漏洩の結果、セキュリティ投資を増やす予定であると回答した企業の割合。[2]

[1] Flexera、「Flexera 2023 State of the Cloud Report」、2023 年 3 月。
[2] IBM Security、「2023 年 情報漏えい時に発生するコストに関する調査」、2023 年。

2023 年には、データ漏洩に関わる 1 件あたりの平均コストと漏洩を阻止するために必要な時間の両方が増加しました。[2] オンプレミスとクラウドのアーキテクチャの違いを考慮した方法に適応することで、セキュリティを重視したハイブリッドクラウドをデプロイし、これらの深刻な課題を克服することが可能です。この e ブックでは、ハイブリッドクラウドのセキュリティに関する新たなアプローチと考慮事項について説明します。

277 日

2023 年のデータ漏洩の特定と阻止にかかった平均時間[2]

米ドル 102 万

漏洩を 200 日以内に特定し阻止することで節約できるコスト[2]

[2] IBM Security、「2023 年 情報漏えい時に発生するコストに関する調査」、2023 年。

第 2 章

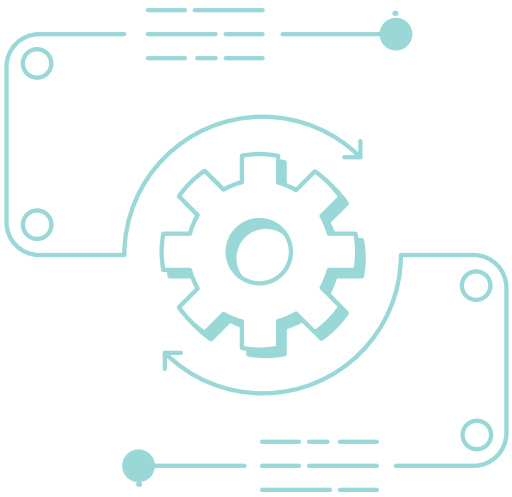
セキュリティはプロセスであり、製品ではない

効果的なセキュリティには、人、プロセス、テクノロジーを組み込んだ包括的なアプローチが求められます。セキュリティを重視した製品やツールをデプロイするだけでは、インフラストラクチャ、クラウド、またはビジネスを保護する上で十分ではありません。また、製品の能力を最大限に引き出し、リスクを軽減するためのセキュリティ戦略とプロセスについても検討する必要があります。

これらの戦略とプロセスは、テクノロジー、脅威、およびニーズの進化に合わせて適応させていくことができます。ハイブリッドクラウド環境では、セキュリティアプローチを変化させていく必要があります。ハイブリッドクラウド環境には明確な境界がないため、従来のセキュリティアプローチは効果的ではありません。

クラウドを中心とするセキュリティアプローチでは、ID 管理の一元化とアクセス制御が鍵となります。最小権限の原則を使用して、必要なアクセスだけをユーザーに付与します。このアプローチでは、各ユーザーの現在のアクセス権を監査してから、各ユーザーを再評価し、適切なアクセスレベルを決定する必要があります。

ハイブリッドクラウドのセキュリティには、環境内のオペレーティングシステム、コンテナプラットフォーム、自動化ツールといった各層の機能を使用する、階層化された多層防御のセキュリティ戦略も必要です。



オペレーティングシステム

セキュリティ・コンプライアンス要件の確保、物理的セキュリティの実装、ネットワークセキュリティの向上、ユーザーアクセスの制御、プロセスの分離、およびデータセキュリティの強化に役立つ組み込みツールを検討します。例としては、OpenSCAP、USBGuard、Security-Enhanced Linux® (SELinux)、ID 管理、NBDE (Network Bound Disk Encryption) などがあります。

コンテナ・プラットフォーム

プラットフォームと Kubernetes に組み込まれている機能を使用して、コンテナのセキュリティを強化します。例としては、Pod セキュリティポリシー、ネットワークトラフィック制御、クラスタの Ingress および Egress 制御、ロールベースのアクセス制御 (RBAC)、統合された証明書管理、ネットワークのマイクロセグメンテーションなどがあります。

自動化ツール

組織全体のすべての人 (開発、IT 運用、セキュリティ、コンプライアンスの各チームを含む) が簡単に習得して使用できる自動化言語とプラットフォームを選択します。アクセス制御機能、ロギング機能、監査機能を備えているものを探しましょう。

既存のセキュリティプロセスやツールを見直すことも重要です。使用できる機能をすべて使用していることを確認し、設定の修正や再設定によって保護を強化できないか、または新しいプロセスやツールが必要かどうかを判断します。

1. 現在の IT アセットとツールのインベントリーを作成します。
2. 既存のセキュリティおよびネットワークアーキテクチャ、サイバーセキュリティ・ポリシー、作業プロセス、スキルと人材のギャップを文書化します。
3. 脅威モデルを確立し、サイバーセキュリティ侵害に対するリスク許容度と緩和策を決定します。
4. アーキテクチャ、ポリシー、およびプロセスを評価して、変更が必要な領域を特定します。
5. 現在のツールとアセットを評価して、更新された戦略とプロセスをサポートできるかどうかを判別します。セキュリティ上のギャップに対処するための方法の文書化と計画を行います。

次のセクションでは、ハイブリッドクラウド・セキュリティに関する重要な考慮事項と、保護を強化するためのヒントについて説明します。

第 3 章

セキュリティに関する考慮事項 1

強固な基盤から開始する

なぜ重要か

ワークロードが複数の環境に分散している場合や、精査されていないオープンソース・テクノロジーが環境で使用されている場合、脆弱性がどこにあるのかを特定するのは困難です。また、強固なセキュリティ基盤がなければ、多層型のセキュリティによるリスクの低減は難しくなります。アップストリーム・コミュニティから直接提供されるオープンソース・ソフトウェアを使用すると、セキュリティリスクやサプライチェーン攻撃にさらされる場合があります。これにより、サードパーティのサービスやソフトウェアの弱点が悪用されて最終的な標的が危険にさらされます。このような攻撃は、ソフトウェア更新を乗っ取ったり、正規のソフトウェアに悪意のあるコードを挿入したりするなど、さまざまな形を取ります。ソフトウェア・サプライチェーンに対する攻撃は、過去 3 年間で年平均 742% も増加しています。[3] このような理由から、統一された安定したセキュリティ重視の基盤を構築することが、ビジネスを保護する上で非常に重要となります。

推奨事項とベストプラクティス

ソフトウェアのライフサイクル全体を通じてエンタープライズサポートを提供する、Red Hat のような信頼できるエンタープライズ・オープンソース・ベンダーのオープンソースソフトウェアを使用することで、ソフトウェア・サプライチェーンのセキュリティ・リスクを低減できます。エンタープライズ・オープンソース・ベンダーは、堅牢なソフトウェア・サプライチェーンのセキュリティプロセスを用いてソフトウェアを開発しています。このプロセスには、お客様に代わってオープンソースソフトウェアを厳選することも含まれます。これによりお客様は、信頼性と回復力が高く、安全なオープンソースソフトウェアを使用することができます。

また、重要なアプリケーションは、セキュリティ機能が組み込まれたプラットフォーム上で実行することが重要です。これにより、重要なアプリケーションを確実に実行できる基盤となるセキュリティが提供されます。また、リスクを低減するための多層型のセキュリティ機能が組み込まれ、セキュリティとコンプライアンスの自動化が実装されます。

Red Hat® Enterprise Linux® のような安定性とセキュリティが強化された、回復力のある信頼できるオペレーティングシステムを採用し、アプリケーションとプロセスのセキュリティを重視した基盤を優先しましょう。この安定した基盤により、ベアメタル、仮想、コンテナ、およびあらゆる種類のクラウド環境にわたって重要なアプリケーションを確実に拡張し、セキュリティ・コンプライアンスを維持し、新しいテクノロジーを一貫して展開できます。

[3] Sonatype、「9th Annual State of the Software Supply Chain」、2023 年。

Red Hat Enterprise Linux は、Red Hat ポートフォリオの多くの基盤であり、セキュリティ機能が組み込まれていることから、多数の企業で信頼されているオペレーティングシステムです。

Red Hat Enterprise Linux を使用すると、次のことが可能になります。

ライブカーネルパッチなどの組み込みのセキュリティ機能により、データやシステムが危険にさらされるリスクを軽減します。これにより、セキュリティパッチ適用時に再起動したりランタイムを停止したりする必要がありません。また、その他の組み込みセキュリティ機能として、アプリケーションの許可リストがあります。これは、特定のユーザーがシステム上で実行することを許可された、承認済みアプリケーションまたは実行可能ファイルのインデックスを指定するものです。また、ファイル、プロセス、ユーザー、アプリなどに対してきめ細かいレベルの制御を適用する SELinux も含まれます。

暗号化キーを管理することなく暗号化システムのロック解除を自動化できる Network Bound Disk Encryption などの組み込みのセキュリティ機能により、データ保護を大規模に自動化し、長期にわたって維持することができます。また、システム全体の暗号化ポリシーを使用することで、システム全体で一貫した暗号化設定やサイト固有のポリシー要件に対応するカスタマイズ可能な暗号化設定などを活用できるため、データの安全性を維持することに集中し、コンプライアンスに対処できます。

コンプライアンス要件を満たし、監査を最適化できます。Red Hat Enterprise Linux には、OpenSCAP によるコンプライアンススキャンと修復機能が組み込まれており、ローカルシステム上で設定と脆弱性のスキャンを実行して、さまざまな業界のセキュリティ標準への準拠を検証できます。

Red Hat Enterprise Linux が提供する基盤となるセキュリティアプローチにより、その上で実行される **Red Hat OpenShift** などの階層化された製品は、コンテナと Kubernetes に多層防御を提供します。Red Hat はスタック上のセキュリティ機能を Kubernetes のコンポーネントにまで拡張します。 同様に、**Red Hat Ansible Automation Platform** にはセキュリティ機能が組み込まれているため、セキュリティとコンプライアンスの自動化を大規模に実装することができます。

戦術的な手順

ハイブリッドクラウド・セキュリティを始める際に取るべき行動

市販のバージョンに切り替える

使用するオープンソースソフトウェアを、アップストリームのオープンソース・プロジェクトが提供するものから、信頼できる市販のバージョンに移行します。これらのバージョンはテスト済みかつ検証済みであるため、バグやセキュリティの脆弱性のリスクを軽減できます。また、セキュリティパッチを迅速に提供し、ソフトウェアをセキュリティ用に設定するためのガイダンスを提供するエンタープライズサポートが含まれる場合もあります。信頼できるエンタープライズ・オープンソース・ベンダーのオープンソースソフトウェアを使用することで、堅牢なソフトウェア・サプライチェーンのセキュリティプロセスによって開発され、ライフサイクル全体を通じてエンタープライズサポートが提供されます。こういったことにより、セキュリティリスクを最小限に抑えながらオープンソースソフトウェアを利用することができます。

セキュリティ機能が組み込まれたプラットフォームを選ぶ

セキュリティ機能が組み込まれたプラットフォーム (OS、コンテナ・アプリケーション・プラットフォーム、自動化プラットフォームなど) を選択することが重要です。これにより、重要なアプリケーションを確実に実行できる基盤となるセキュリティが提供されます。また、リスクを低減するための多層型のセキュリティ機能が組み込まれ、セキュリティとコンプライアンスの自動化が大規模に実装されます。

テクノロジースタック全体にセキュリティを導入する

セキュリティのベースとなる基盤を確立したら、その基盤の上で実行される階層型テクノロジーがセキュリティの利点を継承し、マルチレイヤー・セキュリティとして連動することを確認します。

第 4 章

セキュリティに関する考慮事項 2

DevSecOps で信頼できるソフトウェア・サプライチェーンを実装する

なぜ重要か

2023 年には、データ漏洩の 12% がソフトウェア・サプライチェーン攻撃から発生しています。[2] アップストリーム・コミュニティから直接提供される精査されていないオープンソースソフトウェアを使用すると、セキュリティの脆弱性やサプライチェーン攻撃にさらされる場合があります。これにより、サードパーティのサービスやソフトウェアの弱点が悪用されて最終的な標的が危険にさらされます。このような攻撃は、ソフトウェア更新を乗っ取ったり、正規のソフトウェアに悪意のあるコードを挿入したりするなど、さまざまな形を取ります。

アプリケーション開発とインフラストラクチャのデプロイメントにおいて、セキュリティは後回しにされることがあり、セキュリティアプローチが区分けされていると、セキュリティ上のギャップや重複作業が生じることがよくあります。開発のスピードとデプロイメントの柔軟性が増すにつれて、全プロセスを通じてセキュリティを考慮する重要性がますます高まっています。

推奨事項とベストプラクティス

ソフトウェア・サプライチェーンにセキュリティ重視のアプローチを導入するための最初のステップとして、DevSecOps の考え方を身につけることが挙げられます。DevSecOps の考え方では、アプリケーション開発者、IT 運用、セキュリティの各チームが連携して、ハイブリッドクラウド全体でエンタープライズ向けに強化されたオープンソース基盤の上に構築された、ソフトウェア開発ライフサイクル (SDLC) とインフラストラクチャのライフサイクル全体にわたってソフトウェア・サプライチェーン・セキュリティを実装します。

[2] IBM Security、「2023 年 情報漏えい時に発生するコストに関する調査」、2023 年。

DevSecOps は、初期設計から統合、テスト、デプロイメント、ソフトウェアデリバリーに至るまで、ソフトウェア開発ライフサイクルのあらゆる段階におけるセキュリティの統合を自動化します。

DevSecOps プロセスを導入するメリットには、以下のようなものがあります。

- IT およびセキュリティチームが、人、プロセス、テクノロジーを網羅する課題に取り組むのを支援する
- 効率性、一貫性、反復性、コラボレーションの向上を可能にする
- 人的ミスの削減によりリスクを軽減する

DevSecOps により、セキュリティは最初から最後まで統合された共有責任で取り組まれるものとなります。各チームがばらばらにセキュリティポリシーの設定を担うのではなく、セキュリティ、開発、運用の各チームのスタッフが連携して、可視性、フィードバック、学んだ教訓、知見を共有します。このアプローチにより、アプリケーション開発とインフラストラクチャのデプロイメントの開始時にセキュリティプロセスを組み込むことができるため、保護が強化されます。

組織のために新しいソフトウェア機能を構築するエンタープライズ・アプリケーション開発者は、認知負荷を軽減しながら、セキュリティポスチャを劇的に強化する必要があります。セキュリティは、SDLC の早期に問題を発見して長引くダウンタイムを減らすために統合されたアプリケーション・セキュリティ・チェックによってコード時に、セキュリティ重視の継続的インテグレーション/継続的デリバリー (CI/CD) ワークフローを使用してビルドシステムを保護することによってビルド時に、また、ゴールデンパス・テンプレート、脆弱性分析、アーティファクト署名、証明、実証、ポリシー施行ポイント、ソフトウェア部品表 (SBOM) を使ってデプロイ時と実行時に、SDLC 全体にわたって実装される必要があります。

また、チームが使用しているオープンソース・テクノロジーが信頼できるソースからのものであり、自動化された方法で継続的にパッチが適用され、セキュリティを念頭に置いて設定されていることを確認するための戦略を立てることも必要です。 さらに、ライフサイクル全体を通じてエンタープライズ向けのサポートが提供される、エンタープライズグレードのオープンソース製品の使用を奨励する必要があります。

Red Hat が提供するようなエンタープライズグレードのオープンソース製品を使用することで、Red Hat が製品のオープンソースソフトウェアのサプライチェーンを保護するために 30 年以上にわたって培ってきた経験を活用することができます。また、企業には、Kubernetes クラスタのデプロイ、管理、セキュリティを支援するソリューションおよびアプリケーションを安全かつ大規模に構築、モダナイズ、デプロイする統一された方法が必要です。

Red Hat OpenShift Platform Plus は、Red Hat OpenShift、Red Hat Advanced Cluster Security for Kubernetes、Red Hat Advanced Cluster Management for Kubernetes、Red Hat Quay、Red Hat OpenShift Data Foundation を含む統合プラットフォームです。このプラットフォームは、Kubernetes でコンテナ化されたアプリケーションを安全かつ大規模に構築、モダナイズ、デプロイするのに役立ちます。ソフトウェア・サプライチェーン全体の一貫性を保つため、マルチクラスタのセキュリティ、コンプライアンス、アプリケーション、データ管理が提供されます。

戦術的な手順

DevSecOps とソフトウェア・サプライチェーン・セキュリティの改善を実施する際、これらのアクションを試してみましょう。

小さく始めて拡大させる

まずプロジェクトを 1 つ選び、そこで実践してみます。実験と反復的かつ継続的な改善を奨励し、プロセスの調整と最適化を行います。成功を称賛し、実証された価値を組織内の他の人々に紹介します。

明確な目標とスケジュールを設定し、全員の承諾を得る

透明性が鍵となります。関係者全員がプロジェクトの目標とスケジュールを理解し、承諾していることを確認します。

スタッフのクロストレーニングを行う

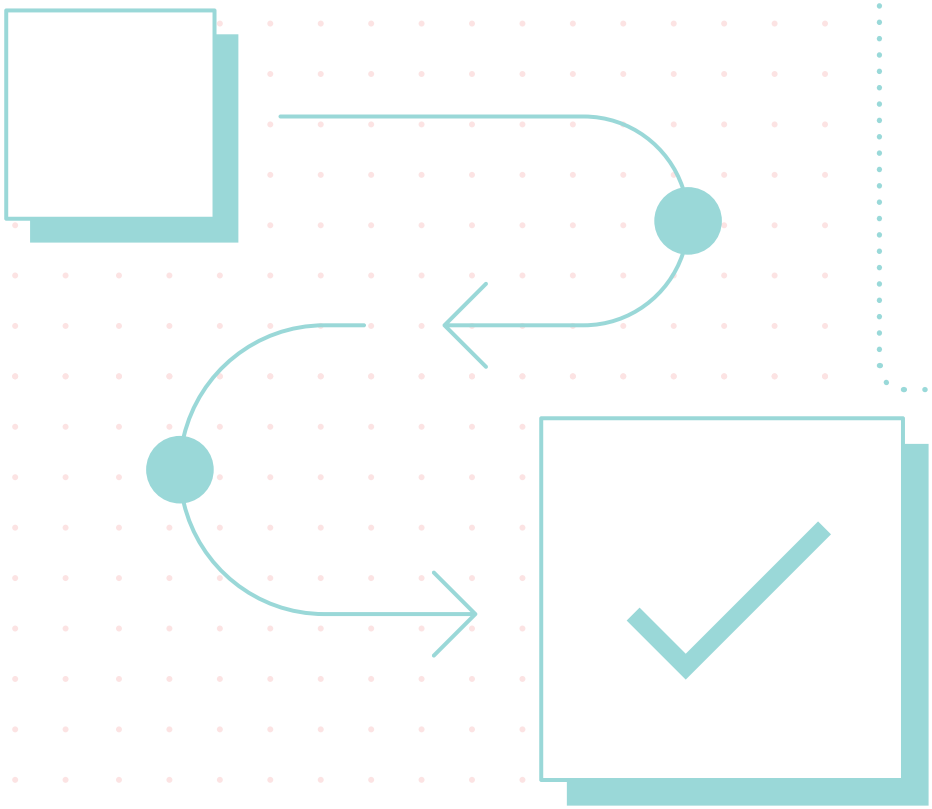
セキュリティ、インフラストラクチャ、および開発に関するラーニングパスを確立します。これは定期的に更新され、すべてのチームメンバーがすぐに利用できるようにする必要があります。

セキュリティ・ワークグループを作る

セキュリティのユースケースと戦略を定義する、分野横断的な統合チームを構築します。他者から学び、他の組織から得た知見を活用しましょう。

統合されたアプリケーション・プラットフォームにより、SDLC 全体にわたってセキュリティを実装する

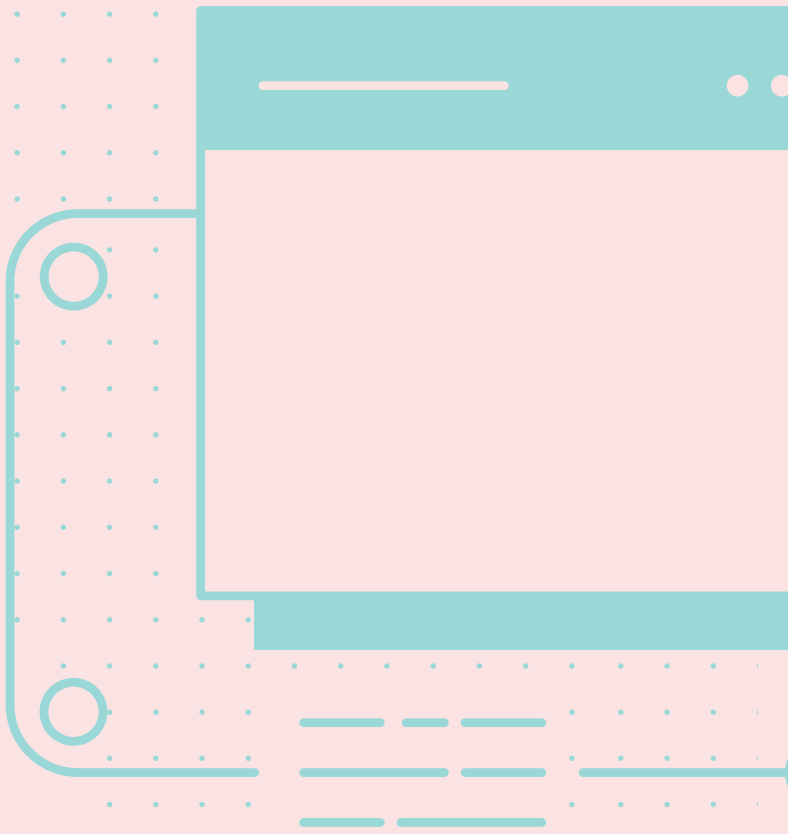
セキュリティは、SDLC の早期に問題を発見して長引くダウンタイムを減らすために統合されたアプリケーション・セキュリティ・チェックによってコード時に、セキュリティ重視の継続的インテグレーション/継続的デリバリー (CI/CD) ワークフローを使用してビルドシステムを保護することによってビルド時に、また、ゴールデンパス・テンプレート、脆弱性分析、アーティファクト署名、証明、実証、ポリシー施行ポイント、ソフトウェア部品表 (SBOM) を使ってデプロイ時と実行時に、SDLC 全体にわたって実装される必要があります。



第 5 章

セキュリティに関する考慮事項 3

自動化と管理で ハイブリッドクラウド を保護



なぜ重要か

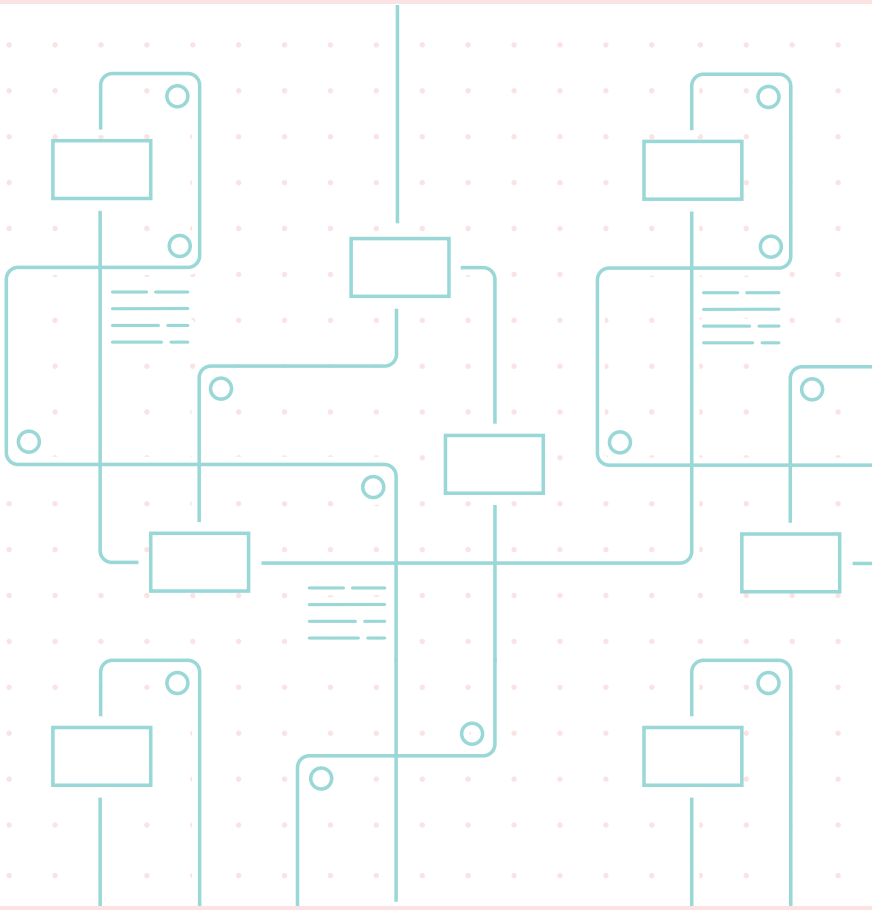
セキュリティ脅威の最大の原因は設定ミスと不適切な変更管理です。[4] 設定ミスによって、システムが攻撃に対して脆弱なままになる可能性があります。システムのライフサイクル全体で、誰が設定を変更したか、いつ、何が変更されたかがわかるようにするためには、変更管理が不可欠です。

自動化、管理、AI は、日常業務の効率化だけでなく、プロセス、アプリケーション、インフラストラクチャに最初からセキュリティを統合するのにも役立ちます。組織全体で自動化と管理戦略を持つことで、人的ミスを減らし、スピード、一貫性、反復性、検証および監査能力をもたらすことができます。また、一元化された自動化および管理戦略により、アプリケーション開発と IT 運用にセキュリティを最初からライフサイクル全体にわたって統合できるため、セキュリティとコンプライアンスが向上します。これにより DevSecOps の実装が成功します。実際、セキュリティプロセスに広範な自動化、管理、AI を組み込むことで、漏洩の平均コストを平均 39.3% 削減することができます。しかしこれを実施している組織は 28% に過ぎません。[2]

[2] IBM Security、「2023 年 情報漏えい時に発生するコストに関する調査」、2023 年。
[4] Cloud Security Alliance、「Top Threats to Cloud Computing: Pandemic 11 Deep Dive」、2023 年 10 月。

推奨事項とベストプラクティス

ダイナミックなセキュリティ、リスク、コンプライアンス要件に対応するため、全社的な自動化および管理戦略を導入します。ハイブリッドクラウドに一貫した自動化および管理戦略を導入することで、アジリティ、反復性、一貫性が向上し、監査が単純化されます。



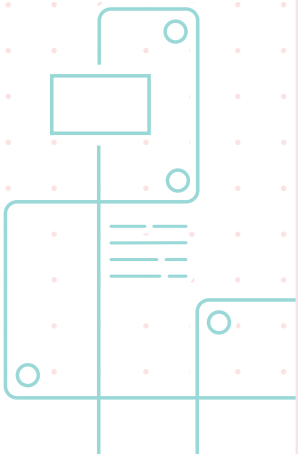
統一された自動化および管理戦略により、組織全体での設定ミスや手動エラーのリスクを軽減しましょう。 自動化および管理により、インフラストラクチャ管理、アプリケーション開発、セキュリティ運用の一貫性が最適化および強化され、保護、コンプライアンス、変更管理を強化できます。これにより、以下のことが可能になります。

事前に承認済みのポリシーに従って一貫性のある設定を行い、ライフサイクル全体で反復可能な方法でリソースをプロアクティブに維持できます。

パッチまたは再設定が必要なシステムをすばやく特定できます。

多数のシステムを対象に一貫した方法で、定義されたベースラインに従ってパッチを適用したり、システム設定を変更したりするのを効率化できます。

自動的に記録されたアクションログにより、監査とトラブルシューティングが容易になります。



企業は IT 自動化を利用して、ますます複雑化する運用環境、アプリケーション、セキュリティ運用、ハイブリッドクラウド環境におけるセキュリティを管理しています。**Red Hat Ansible Automation Platform** は、エンドツーエンドの自動化プラットフォームです。あらゆる段階でセキュリティを優先しながら、IT 自動化を大規模に構築および運用するための一貫したエンタープライズ・フレームワークを提供します。Red Hat Ansible Automation Platform は効率と生産性の向上、リスクと経費の管理に役立ち、チームが企業全体のセキュリティとコンプライアンスの一貫性を反復可能な方法で自動化できるようにして、Red Hat の 24 時間体制のエンタープライズ・サポートとともに、脅威に対応するための認定済みの自動化コンテンツを提供します。

Red Hat Ansible Automation Platform は、自動化された構成管理から自動化されたパッチ適用や修復まで、悪意のある攻撃に先んじるための自動化されたセキュリティプロセスの管理を支援します。さらに、Red Hat Ansible Automation Platform は CyberArk、IBM、Palo Alto Networks などの認定パートナーからのコンテンツを使用することでセキュリティ・ソリューションの統合ポイントとして機能できます。これらのコンテンツは幅広い外部のセキュリティ・テクノロジーの管理や統合の自動化に使用できます。

自動化プラットフォームおよびプロセスに ID 管理とアクセス制御を実装すると、許可されたスタッフのみが自動化タスクを実行できるようになります。組織内の全員が使用できる自動化プラットフォームを選択しましょう。一般的で習得しやすい自動化言語を実装するプラットフォームを使用すると、以下を改善できます。

可視性：全員が自動化された各タスクの機能を理解できます。

反復性：使いやすいプラットフォームと言語により、承認されたスタッフ全員が自動化を効果的かつ効率的に使用することができます。

コラボレーション：自動化タスクを組織全体で共有できるため、完了している作業を他のチームが活用し、作業の重複を回避できます。

監査：複数のスタッフが自動化タスクを検証し、監査用のログを表示できます。

戦術的な手順

セキュリティの自動化を開始するには、次のアクションを試してください。

単一のプロジェクトから始める
すべてを一度で自動化できると考えないようにしましょう。開始にあたっては、限定したタスクを選択しましょう。

繰り返しの多いタスクを選択する
設定管理、ソフトウェアパッケージとパッチの管理、セキュリティ脆弱性の特定と修正、ポリシーの適用など、繰り返し実行されるタスクを自動化します。

測定、調整、反復を実行する。
自動化のデプロイ、結果の測定、それに応じた調整という一連の流れを繰り返します。

エンドツーエンドのエンタープライズ自動化プラットフォームを使用して拡張を計画する
組織内の他の人々がメリットを活用できるように、すべての自動化が検証可能、監査可能、および共有可能であり、エンドツーエンドのエンタープライズ自動化プラットフォームを使用して拡張できることを確認します。

第6章

今すぐ始めましょう

ハイブリッドクラウド・セキュリティは、どの組織にとっても組織全体で共有されるべき責任です。お客様がハイブリッドクラウド導入のどの段階におられるかに関わらず、Red Hat はセキュリティを重視したハイブリッドクラウドのデプロイメントを支援します。

Red Hat のプロダクショングレードのオープンソースソフトウェアのポートフォリオは、統合された組み込みのセキュリティ機能を備えており、現在だけでなく将来にわたってセキュリティとコンプライアンスの課題を克服するためのツールとプラットフォームを提供します。また、Red Hat は、エンタープライズ向けのサポート、実践的なトレーニング、エキスパートによるサービスを提供し、お客様がハイブリッドクラウド環境をより効率的かつ安全に構築し、運用できるように支援します。

Red Hat のアプローチ：ハイブリッドクラウド・セキュリティを読む

ハイブリッドクラウド全体のセキュリティとコンプライアンスに対する Red Hat のアプローチの詳細は、以下のリソースをご覧ください。

- ハイブリッドクラウド・セキュリティの概要
- ハイブリッドクラウド・セキュリティの評価
- ハイブリッドクラウド環境向けのセキュリティ・アプローチ
- ハイブリッドクラウド・セキュリティを強化する

Red Hat セキュリティグローバル戦略およびエバンジェリズム担当ディレクター Lucy Huh Kerner (ルーシー・ハー・カーナー) について
Lucy Huh Kerner は、Red Hat および Red Hat の全ポートフォリオにおいて、セキュリティのソートリーダーシップと、セキュリティの技術戦略および市場投入戦略をグローバルにリードしています。さらに、セキュリティ関連の技術コンテンツの作成と、現場、顧客、パートナー、アナリスト、報道機関への配信を支援し、セキュリティ・カンファレンスなど数多くのイベントで講演を行ってきました。同氏は、ソフトウェアとハードウェアの開発エンジニア、ソリューションアーキテクト、およびグローバルセキュリティストラテジストとして 20 年以上の専門的な経験があり、セキュリティのさまざまな側面に取り組んできました。

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

jp.redhat.com