Red Hat
Enterprise Linux

クラウドでのセキュリティを単純化する

Red Hat Enterprise Linux は、環境全体で一貫したセキュリティ機能を提供します

クラウド環境全体で一貫した運用が可能

Red Hat Enterprise Linux には、クラウド上で信頼性の高い、セキュリティに重点を置いたパフォーマンスを確保するためのさまざまな最適化手段が含まれています。Red Hat Enterprise Linux は、ハイブリッド環境とマルチクラウド環境に一貫した運用基盤を提供するため、アプリケーションを最適な場所で実行できます。

クラウドでの Red Hat Enterprise LInux の価値の詳細をご覧ください。

クラウドでのセキュリティは最重要事項

クラウド導入が進むにつれ、セキュリティはあらゆる規模の組織にとって主要な懸念事項となっています。実際、85% の企業がクラウドの課題としてセキュリティを挙げています。[1] 2022 年に起きた侵害の 45% はクラウドで発生しているため、この懸念も無理はありません。[2]

どのような環境においても、一貫性は、セキュリティとコンプライアンスのベストプラクティスの核となるものです。ビジネスを守るためには、データセンターで行っているのと同じレベルのセキュリティポリシーとアクセス制御がクラウドでも必要です。すべてのインフラストラクチャのフットプリントで一貫したセキュリティ制御を提供するオペレーティングシステムを標準化することで、組織全体のセキュリティとコンプライアンスを向上させることができます。Red Hat® Enterprise Linux® を環境全体で運用基盤として使用すると、クラウドにおけるセキュリティとコンプライアンスを維持するために必要な一貫性が得られます。

環境間で一貫したセキュリティとコンプライアンスの基盤を採用する

Red Hat Enterprise Linux により、オンサイト、クラウド、エッジの環境全体で、セキュリティとコンプライアンスをよりシンプルに維持することができます。セキュリティは、Red Hat Enterprise Linux のアーキテクチャとライフサイクルの鍵となる要素です。組み込み型のセキュリティ機能と業界および政府規制へのコンプライアンス遵守は、クラウドでのシステムを保護します。ベストプラクティスに基づいた初期設定により、最初からセキュリティが強化されたシステムを構成することができます。ビルド済みのクラウドイメージ向けにパッケージセットが最小化されており、サイバーセキュリティ脅威の攻撃対象領域が縮小されます。セキュリティ・アップグレードとライブパッチも、Red Hat Enterprise Linux のサブスクリプションの一部として提供されます。

Red Hat Enterprise Linux を使用することで、ハイブリッド環境およびマルチクラウド環境において、セキュリティリスクの軽減、階層的なセキュリティの実装と維持、コンプライアンスの最適化が可能になります。この概要では、ハイブリッドおよびマルチクラウド環境において一貫したセキュリティアプローチを採用するための主な特徴と機能について説明します。

Red Hat Insights で大規模に脆弱性を検出して修復する

データ漏洩の特定と封じ込めにかかった 2022 年の平均日数は 277 日でした。[2] 200 日以内に情報漏洩を発見し、阻止することで、その結果生じるコストを平均 24% 削減することができます。[2] 日常的に一貫した監視を行うことで、業務への支障や侵害につながる前に脆弱性やコンプライアンスリスクを特定することができます。

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

1 Flexera、「Flexera 2022 State of the Cloud Report」、2022 年 3 月。
2 IBM Security、「2022 年データ侵害のコストに関する調査レポート」、2022 年。

Red Hat
Enterprise Linux

セキュリティとコンプライアンスの運用を高速化

Red Hat Insights は、セキュリティとコンプライアンスの運用を加速化するのに役立ちます。

- **91%** セキュリティの脆弱性の検出にかかる時間を短縮[3]
- **69%** ポリシー違反の検出にかかる時間を削減[3]

Red Hat Enterprise Linux によるセキュリティとコンプライアンスの管理について詳しくご覧ください。

- 概要：Red Hat Insights でセキュリティリスクを管理する
- デモ：Red Hat Insights で問題を解決する
- ライブデモ：セキュリティ・コンプライアンスと脆弱性スキャンのために OpenSCAP を使用する

Red Hat Enterprise Linux に含まれる Red Hat Insights は、Hybrid Cloud Console 上のホストサービススイートです。プラットフォームやアプリケーションを継続的に分析し、ハイブリッドクラウド環境の管理および最適化を支援します。Red Hat Insights は、予測分析と深い専門知識を用いてセキュリティやコンプライアンスリスク、その他の運用リスクを特定、評価し、改善策を提案します。また、重大度、リスクの種類、変更による影響に基づいて、修正アクションに優先順位を付けます。Red Hat Insights はオンサイト環境とクラウド環境で機能し、単一のインタフェースからすべての Red Hat Enterprise Linux システムを管理できるようにします。また、Red Hat アカウントをクラウドプロバイダーのアカウントにリンクし、クラウドベースのシステムとワークロードをプロビジョニング時に Red Hat Insights や他の Red Hat サービスに自動的に接続させることもできます。

Red Hat Insights には、ハイブリッドおよびマルチクラウド環境の保護に役立つサービスが含まれています。

- **脆弱性対策サービス：**共通脆弱性識別子 (CVE) システムのスキャン、スキャン情報の収集、修復ガイダンスへのアクセスを単一のインタフェースで行うことができます。
- **マルウェアサービス：** アクティブなマルウェアのシグネチャを含むシステムを迅速に特定し、長期的な露出を防止します。

組み込みのスキャンおよび修復機能によりコンプライアンスを確保する

準拠していないことにより、セキュリティ侵害に加えて、罰金、ビジネスへの損害、認証の喪失につながる可能性があります。コンプライアンス違反が多発した組織の 2022 年のデータ漏洩の平均損害額は、557 万米ドルとなりました。[2] コンプライアンス違反の多発により、2022 年のデータ漏洩の損害額は平均 25 万 8,293 米ドル増加しています。[2]

Red Hat Enterprise Linux は、政府および業界の主要な規格に準拠しているため、高度に規制された環境でも自信を持って使用することができます。Red Hat Insights には、ハイブリッドおよびマルチクラウド環境におけるコンプライアンスの維持をより容易にするためのサービスが含まれています。

- **コンプライアンスサービス：**OpenSCAP ポリシーの遵守状況を監査し、遵守できていないシステムを修復し、法令順守やセキュリティ監査用のレポートを作成します。また、デフォルトのポリシーを組織の環境や運用に合わせて調整することで、より正確な結果を生成することができます。主要な組み込みベースラインには以下が含まれます。
  - Payment Card Industry Data Security Standard (PCI-DSS)
  - Enhanced Operating System Protection Profile (Common Criteria)
  - Australian Cyber Security Centre (ACSC) Essential Eight
  - Center for Internet Security (CIS) Benchmark
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Defense Information Systems Agency Secure Technical Implementation Guidelines (DISA STIG)
- **ポリシーサービス：**カスタム・セキュリティ・ポリシーを定義し、システムのコンプライアンスを監視し、システムがコンプライアンス違反となった場合にチームに警告します。

3 Principled Technologies (Red Hat 後援)、「Red Hat Insights をアクティベートして監視を自動化し、管理者の時間と労力を節約する」、2020 年 9 月。

Red Hat
Enterprise Linux

イメージビルダーサービスを使用してクラウド全体で一貫性のある強化されたイメージをデプロイする

現在、89% の組織がマルチクラウド戦略を導入しています。[1] マルチクラウドアプローチでは、ワークロードごとに適切なクラウドを選択できる反面、これにより複雑さが増し、不整合のリスクも高まるためセキュリティやコンプライアンスの問題にもつながります。

Red Hat Insights のイメージビルダーサービスを利用することで、ハイブリッドクラウド環境全体でより迅速かつ容易に Red Hat Enterprise Linux オペレーティングシステム・イメージを作成、管理、デプロイすることができます。カスタマイズされ、セキュリティ強化されたイメージを構築し、テンプレートとして保存して複数のクラウドプロバイダーのインベントリーにプッシュして、プロビジョニングを単純化することができます。その結果、複数のクラウドで一貫してシステムを構成できるようになります。

リモート認証で環境全体のシステムの整合性を検証する

大規模で分散化が大きく進んだ環境では、システムの整合性の確保が不可欠です。信頼できない侵害されたシステムは、悪意のある攻撃者によって危険にさらされる可能性があります。

Red Hat Enterprise Linux には、ブート時にシステムの状態を検証し、リモートシステムの整合性を継続的に監視するためのリモート認証機能があります。Keylime オープンソース・プロジェクトをベースとしたリモート認証では、組み込み型の Trusted Platform Module (TPM) ハードウェアや Linux カーネル Integrity Measurement Architecture (IMA) を使用して、大規模なシステムの監視を行います。また、監視対象システムに暗号化されたファイルを送信したり、監視対象システムが整合性テストに失敗した場合に実行される自動化されたアクションを指定したりすることもできます。

クラウド上のデータを Network Bound Disk Encryption (NBDE) で保護する

データはビジネスにとって重要な資産であり、クラウドでの保護は不可欠です。

Red Hat Enterprise Linux には、Network Bound Disk Encryption (NBDE) のサポートが含まれており、保管されているデータの保護を単純化できます。NBDE は、1 台以上のネットワークサーバーへの接続により、ストレージ・ボリュームのロックを自動的に解除します。これにより、暗号化キーを手動で管理することなくボリュームを復号化することが可能となり、セキュリティが確保されているときのみボリュームを利用できるようになります。Red Hat Enterprise Linux は、暗号化されたボリュームのロックを解除する前にシステムの整合性を確保するために、TPM を介した NBDE もサポートしています。

組み込みの ID 管理とアクセス管理機能によりゼロトラスト・アーキテクチャをより簡単に実装する

従来の境界に基づくセキュリティアプローチでは、広く分散したクラウドベースの新しい環境を効果的に保護することはできません。ゼロトラスト・アーキテクチャは、ネットワークの境界だけにセキュリティを適用するのではなく、各アセットにセキュリティを適用することで保護します。実際、ゼロトラストを導入することで、データ漏洩によるコストを平均 20.5% 削減することができます。[2] ID 管理とアクセス管理は、ゼロトラスト・アーキテクチャの中核をなすものです。

Red Hat Enterprise Linux に含まれる Red Hat Identity Management は、ID 管理の一元化、セキュリティ制御の適用、環境全体でのセキュリティ基準への準拠を支援します。ID 管理インフラストラクチャを単純化しながら、ゼロトラストのベストプラクティスを実装するために必要な機能を提供します。データセンター全体をカバーするスケーラブルな単一のインタフェースでユーザーを認証し、ポリシーベースまたはロールベースのアクセス制御 (RBAC) を実装します。Red Hat Identity Management は、標準のインタフェースを通じて Microsoft Active Directory、軽量ディレクトリ・アクセス・プロトコル (LDAP)、およびその他のサードパーティ製ソリューションと統合できます。Red Hat Identity Management は、証明書ベースの認証および認可技術もサポートしています。

Linux 環境でゼロトラストの基盤を構築する

ゼロトラスト・アーキテクチャによって、IT 環境と組織の保護を強化することができます。

- Red Hat Enterprise Linux によるゼロトラストの実装について、詳しくはこちらをご覧ください。
- Red Hat Enterprise Linux のユーザー管理に関するライブデモをご覧ください。

リリース全体のセキュリティを短時間で管理する

自動化により、手作業によるミスを減らしてシステムをより迅速に管理することができます。

Red Hat Enterprise Linux のシステムロールに関するライブデモをご覧ください。

システムロールでセキュリティ設定と管理を最適化する

インフラストラクチャの規模と複雑性が増すにつれ、手動での管理は難しくなります。クラウドの構成ミスは、データ漏洩の 15% において最初の攻撃ベクトルとなっており、2022 年には漏洩 1 件あたりの平均コストが 414 万米ドルとなりました。[2] 自動化により、より速く、より一貫性を持って、より少ない労力でシステムを構成および管理することができます。

Red Hat Ansible® Automation Platform を備えた Red Hat Enterprise Linux システムロールは、自動化を利用して、セキュリティ設定を短時間で大規模にインストールし、管理できるようにします。システムロールは、インフラストラクチャのフットプリント全体で、複数の Red Hat Enterprise Linux リリースで機能するため、単一のコマンドまたはワークフローで新しいセキュリティ設定を構成し、すべてのシステムでそれを維持することができます。

詳細はこちら

ハイブリッド環境とマルチクラウド環境におけるセキュリティとコンプライアンスへの一貫したアプローチにより、組織をより適切に保護できます。Red Hat Enterprise Linux は、データセンター、クラウド、エッジなど、あらゆるインフラストラクチャでアプリケーションを実行するための、セキュリティに重点を置いた基盤を提供します。

ハイブリッドクラウド・セキュリティに対する Red Hat のアプローチについて、詳しくはこちらをご覧ください。

Red Hat について

エンタープライズ・オープンソース・ソフトウェア・ソリューションのプロバイダーとして世界をリードする Red Hat は、コミュニティとの協業により高い信頼性と性能を備える Linux、ハイブリッドクラウド、コンテナ、および Kubernetes テクノロジーを提供しています。Red Hat は、クラウドネイティブ・アプリケーションの開発、既存および新規 IT アプリケーションの統合、複雑な環境の自動化および運用管理を支援します。受賞歴のあるサポート、トレーニング、コンサルティングサービスを提供する Red Hat は、フォーチュン 500 企業に信頼されるアドバイザーであり、オープンな技術革新によるメリットをあらゆる業界に提供します。Red Hat は企業、パートナー、およびコミュニティのグローバルネットワークの中核として、企業の成長と変革を支え、デジタル化が進む将来に備える支援を提供しています。

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
275099_0323_KVM

Copyright © 2023 Red Hat, Inc. Red Hat、Red Hat ロゴ、および Ansible は、米国およびその他の国における Red Hat, Inc. またはその子会社の商標または登録商標です。Linux® は、米国およびその他の国における Linus Torvalds 氏の登録商標です。