IBM **Cloud**

コンテナー・プラットフォームの保護

信頼の連鎖を築く

IBM

DevOps の課題:イノベーションを安全かつ迅速に推進

競争の激しい市場でビジネス目標をサポートするには、アプリケーション開発エグゼクティブとそのチームは各種デバイス・タイプに対し、良質な顧客体験をこれまで以上に速いペースで実現する必要があります。その結果、DevOps チームは、独立系ながら相互運用できるマイクロサービスとしてクラウド・ネイティブ・アプリを作成、再現するプロセスの自動化を最大限にするために、これまで以上にコンテナーベースのクラウド・プラットフォームとアジャイル協働手法、ツールチェーンを使っています。

優れたセキュリティーを設定し維持することは、クラウドベースの DevOps シナリオに移行する際に課題を生みだしそうですが、セキュリティーは絶対に無視できません。ほとんどのクラウド・プラットフォームはたとえば、コンテナーに Docker を使用しており、コンテナーは共有 Linux カーネルで稼働し、そのセキュリティー面の課題を受け継いでいます。コミュニティー・エクスチェンジからダウンロードしたコンテナー・ソフトウェアに未検出のウイルスが潜んでいて、1 つのホストの Linux カーネルで特権昇格を取得すると、データの引き出しやウイルスの拡散を開始して、サービス妨害 (DoS) 攻撃によるダメージをもたらす可能性があります。コンテナーは、チャネル、ライブラリー、バイナリなどのリソースへのアクセスをすべて共有しているので、他のコンテナーと干渉することもあります。

Bring-Your-Own-Device (BYOD) モデルの採用が広がるにつれ、多くの企業は企業のエンドポイントへのコントロールも失い、従来の企業境界が脆弱化しています。ワークロードがデータセンターとクラウドに移動すれば、セキュリティーも一緒についていかなければなりません。

侵入、居座り、拡散、収集、引き出しといった攻撃の連鎖は同じですが、攻撃者の創造力は永遠に発揮され続けます。重大なデータ漏洩を伝える記事の見出しをよく見かけますが、このことは、セキュリティーについての全体像が変化し続けていることを反映しています。

- 攻撃者はサイバー犯罪がもうかることに気付き、高度な長期的脅威や他の急速に変異するマルウェアが発生することになります。
- 国家はサイバー戦争における能力をさらに高度なものにしました。多くの国では、攻撃者は国のリソースを使って高度なツールを開発し、本業よりも大金を稼げる夜の犯罪活動にいそしみます。

クラウド・プラットフォーム保護するという基本課題に対処するため、セキュリティー責任者は確かに夜も多忙を極めることがあるかもしれません。CISO の目標は、企業のセキュリティのフレームワークと要件を定義することで、リスクを最小化し、規制遵守を満たすことです。実装は監査可能な方法で行う必要があります。

これらの要件のため、CISO は AppDev エグゼクティブのニーズと対立する可能性があります。AppDev エグゼクティブは、できるだけ自動化を実現し、DevOps プロセスとパイプラインに柔軟に統合する (完全に透明にすることができない場合) セキュリティー・ソリューションを必要としているからです。

主要関係者の重要でも対立するニーズをクラウド・プラットフォームで効率的、効果的に満たすには

信頼の連鎖を作る

解決策は、ハードウェアに根を持つ信頼の連鎖を築いて、クラウド・プラットフォームのあらゆる関連コンポーネントの完全性を検証することです。**真の信頼の連鎖はホスト・チップ・ファームウェアで始まり、コンテナー・エンジンと編成システムを通じて育まれ、アプリケーションのライフサイクルの間、重要なデータとワークロードをすべて保護します。**その結果、高度に自動化された信頼コンテナー・システムが生まれます。

ハードウェアは、シリコンがベースになっていてハッカーによる改竄が困難なので、理想的な基盤となります。各コンポーネントが次のレベルを測定、検証、開始する測定と検証セキュリティー・モデルを使うことで、信頼の連鎖がこの基盤から築かれていきます。このプロセスはコンテナー・エンジンに及び、信頼境界を作り出します。測定値はホストの信頼プラットフォーム・モジュール (TPM) に保存されます。別のサーバー上の認証ソフトウェアが、最新の測定値と既知の正常値を比較検証します。コンテナー編成ソフトウェアは認証サーバーと通信して、ワーカー・ホストおよびそれらのホストに展開されたコンテナー・イメージの完全性を検証します。

図 1 は、新しいワーカーを Kubernetes クラスターに追加する際に関わる、ハードウェアベースの信頼の連鎖を示します。図の中の番号は、ここで説明するステップ 1 からステップ 6 に相当します。起動元ホストの測定値を検証するには、別の認証サーバーに保存された既知の正常値との比較が必要である点に留意してください。

1. ワーカー・ホストでは、TPM ハードウェアがシステム・ファームウェアを認証して、オプションの ROM など、BIOS を測定および検証します。それから、BIOS が起動します。
2. BIOS は、オペレーティング・システム (OS) を測定、検証、起動します。
3. OS は Docker コンテナー・ランタイム、Docker プラグイン、および信頼コンピューティング・ベース (TCB: Trusted Computing Base) の一部であるすべての主要コンポーネントを測定、検証、起動します。
4. Cloud Integrity Technology (CIT) プラグインにより、Kubernetes マスターは認証サーバー経由でワーカー・ホストを検証します。認証クラウドでは、適切に地理位置情報が特定されないワーカーによる使用をブロックするなど、Kubernetes クラスターの地理位置情報/境界情報もチェックされます。
5. Kubernetes マスターは、有効に認証されたホストを既存クラスターの一部として構成し、そのホストにコンテナーを割り当てたりします。
6. 暗号化された接続を通じて認証サーバーと通信する、ワーカー・ホスト上の Docker エンジンは、コンテナー・イメージの完全性を検証し、セキュリティー・ポリシーに対するチェック作業を行います。

セキュリティー・ポリシー駆動型なので、コンテナー・プラットフォーム全体が、既知の正常な状態にあるホストとコンテナーだけを自動的に実行します。

主なメリット

クラウド・プラットフォームで、セキュリティーの自動化に不可欠なポリシー管理型信頼境界がサポートされていることを確認します。

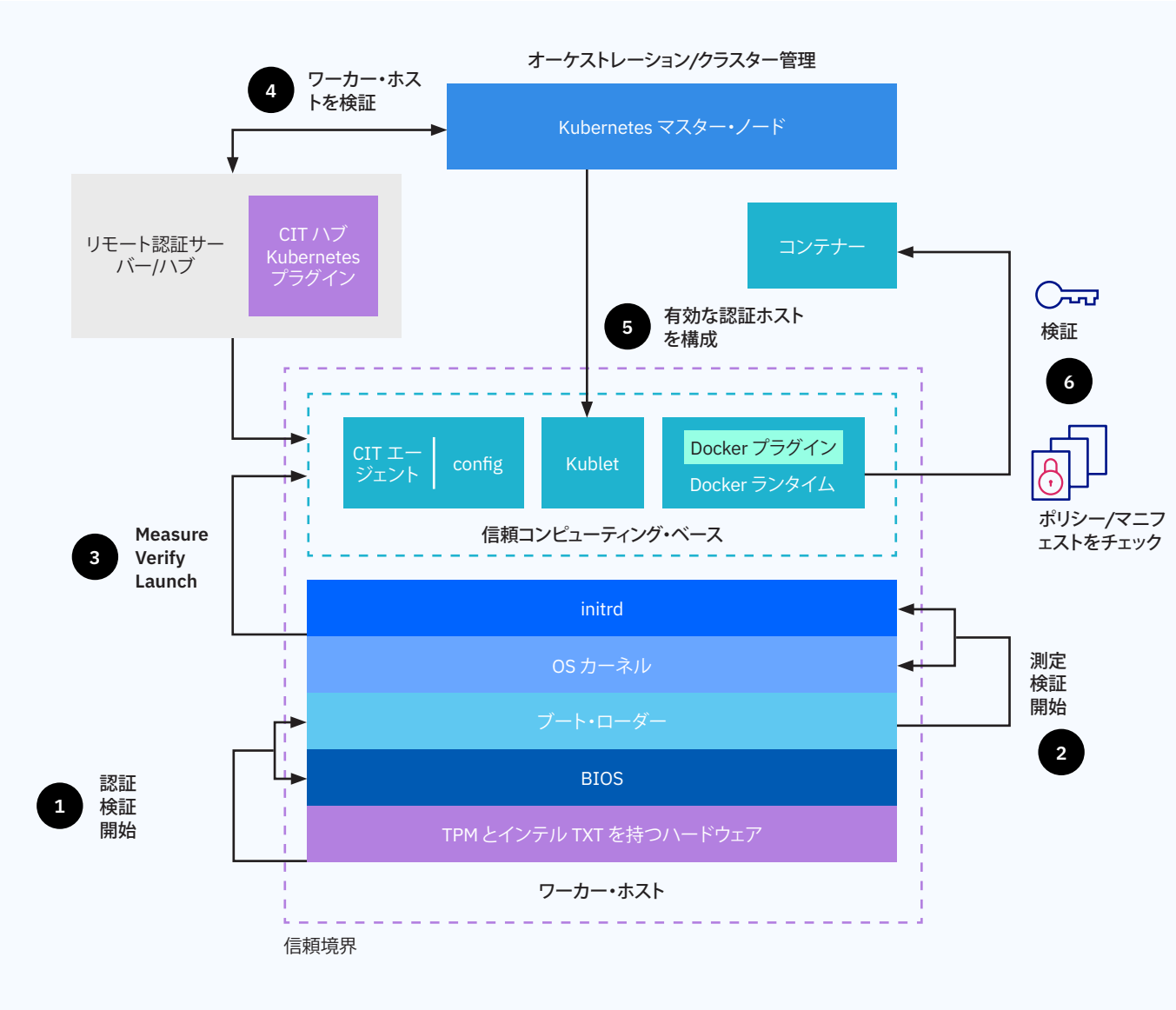


図 1. コンテナーにおいて信頼の連鎖を実現する基準アーキテクチャー。Kubernetes 編成レベルにまで拡大される測定-検証セキュリティー・モデルを基盤として採用。6 ステップの詳細については、3 ページを参照。

信頼されるコンテナーの実現

Docker のようなコンテナー・システムには、システムの個々の要素周辺にマイクロ境界を構築して要素間の通信を保護するための手法が組み込まれています。

コンテナー・アプリが十分に保護されているかどうかを評価するには、Docker 実装のこれらの側面についてクラウド・プラットフォーム・ベンダーに問い合わせてください。

ソフトウェア・イメージはプライベート・レジストリに維持されているか? Docker Registry V2 をベースにしたクラウド・プラットフォームは、イメージが保管され指定のユーザーとグループしか共有できないセキュアなプライベート・イメージ・レジストリを各企業に割り当てることができます。イメージをプライベート・レジストリに追加するプロセスでは、ローカル・イメージの作成やコピー、または Docker Hub のようなパブリック・レジストリから直接イメージをインポートするための権限をユーザーに付与します。

Docker 実装によってそのイメージを暗号化することができるのか?
暗号化は、レジストリ内のイメージを改竄から保護します。

コンピュート・ホストで稼働するDocker デーモンは、ユーザーが直接アクセスせずにセットアップされているか? 構成を行ったのはサービス・プロバイダーだけか?
答えは両方とも「はい」であるべきです。他のお客様によるホストへの直接アクセスによって、コンテナーのセキュリティーが侵害されるおそれがあります。

すべての Docker デーモン・ソケットがトランスポート層セキュリティー (TLS) 証明書で保護されているか?
TLS はパブリックキー暗号化、外部のサードパーティ検証、セッションごとの暗号化の高度な機能を組み合わせます。

特権的な Docker コンテナーが許可されているか?
特権コンテナーを禁止すると、自社データとアプリケーションが格納されている可能性のあるコンピュータ・ホスト上のハードディスクに、他のサービス・プロバイダーの顧客のコンテナーがアクセスできなくなります。

ノード信頼環境から信頼クラウドへの移行

コンピュート・ノードは、信頼の連鎖の確立における焦点となり、各ノードには自身の信頼境界があるため、Kubernetes クラスターとポッドの全メンバーは、データの計算と転送が行われる前にワークロード全体の保護を開始します。

クラウド・プロバイダーに、信頼テクノロジーの説明と実演をしてもらいましょう。たとえば、インテル・トラステッド・エグゼキューション・テクノロジー (インテル TXT)、仕様 1.2 または 2.0 に準拠した TPM、インテル CIT は、プロバイダーが信頼クラウドの構築に使うかもしれない確立されたテクノロジーです。

- **インテル TXT** は、システムや BIOS コードを破損させたりプラットフォームの構成を変更したりして機密情報を盗もうとするソフトウェアベースの攻撃から防御します。
- **TPM** はハードウェアベースのセキュリティー・デバイスで、測定-検証セキュリティー・プロセスで使われた測定値を保管します。システム制御を次のレベルのソフトウェアにリリースする前に、システムが改竄されていないことを確実に検証できるよう支援します。
- **インテル CIT** は信頼の基盤を基にポリシー駆動型の認証情報を提供することで、パブリックおよびプライベート・クラウド環境双方でコンプライアンスに準拠した検証済みのハードウェア上でワークロードが実行されるようにします。

リモート認証は信頼プロセスの重要なステップであり、その範囲はホスト信頼境界を越えてコンテナー編成レベルにまで及びます。 Kubernetes のようなオーケストレーターは、コンテナーをコンピュート・ノードに展開する前に、そのコンピュート・ノードの完全性を検証できなくてはなりません。

リモート認証を提供するため、クラウド・ベンダーは CIT テクノロジーを使って、クラウド・コンピュート・ノードがコンテナー環境に割り当てられるたびに、さらに認証ステップを追加する場合があります。たとえば、インテル CIT はインテル TXT と連携して、ノードをコンテナー・クラスターに受け入れる前に、そのノードがこれまでどおり改竄されていなくて信頼できる状態であることを確認します。インテル CIT は、アプリケーション開発者がポリシーに対処しなくても、DevOps チームがワークロードのセキュリティー・ポリシーを容易に実施できるようにするエクステンションも提供しています。

重要なポイント

ノードレベルの信頼境界を拡大するには、実証済みの暗号化ソリューションが必要です。

リソースの分離によるセキュリティー保護

Kubernetes オーケストレーターは、サービス・プロバイダーの管理対象リソースを企業のアカウントのプライベート要素から分離可能にすることで、クラスターの保護も支援します。

- Kubernetes 専用マスター・ノード、イメージ・アクセスが制御されたプライベート・イメージ・レジストリは管理対象ネットワークで実行できます。
- Kubernetes ワーカー・ノードとコンテナー・ワークロード・ポッドは、プロバイダーではなく、企業が管理する専用ネットワーク上の企業のインフラストラクチャー・アカウントに展開できます。

このアプローチを採用すると、DevOps チームは高レベルのコントロールを得て、CISO が望む分離を実現できます。マスターとワーカー・ノード間の通信 は、Kubernetes が提供する暗号化とキーで暗号化されたネットワーク接続経由で行われます。Ingress Controller は、Kubernetes ポッドにアクセスするための TLS 証明書を自動生成します。Kubernetes のロールベースのアクセス制御を使用することで、企業はクラスター内のリソースに対して粒度の細かい制限を設定することができます。

ポリシー駆動型の自動化

Kubernetes により、DevOps チームはシステムの役割を原子レベルの非常に小さい要素に分類できます。これらの各要素をベース信頼アーキテクチャーに結びつけることで、各要素がポリシーに従ってアクセスと通信を許可できるようにします。チームが複雑なマイクロサービス・アーキテクチャーを構築する一方で、ポリシー駆動型の自動化はアクセスとルーティングを制御して、個々のアプリケーションとそのコンポーネントの拡張と縮小を容易にします。

Calico と Istio は、アプリケーションとワークロードのセキュリティーを支援する、Kubernetes エコシステムの重要な 2 つのコンポーネントです。Calico は、コンピュート・ノードのワークロードに割り当てられた IP アドレスの管理を簡素化し、各コンピュート・ノードのアクセス制御リストをプログラミングしてセキュリティー・ポリシーを適用します。ラベルを介して設定し適用するポリシー定義により、Istio は、Kubernetes ポッドまたはクラスター内のマイクロサービス間の通信を証明書ベースで制御します。

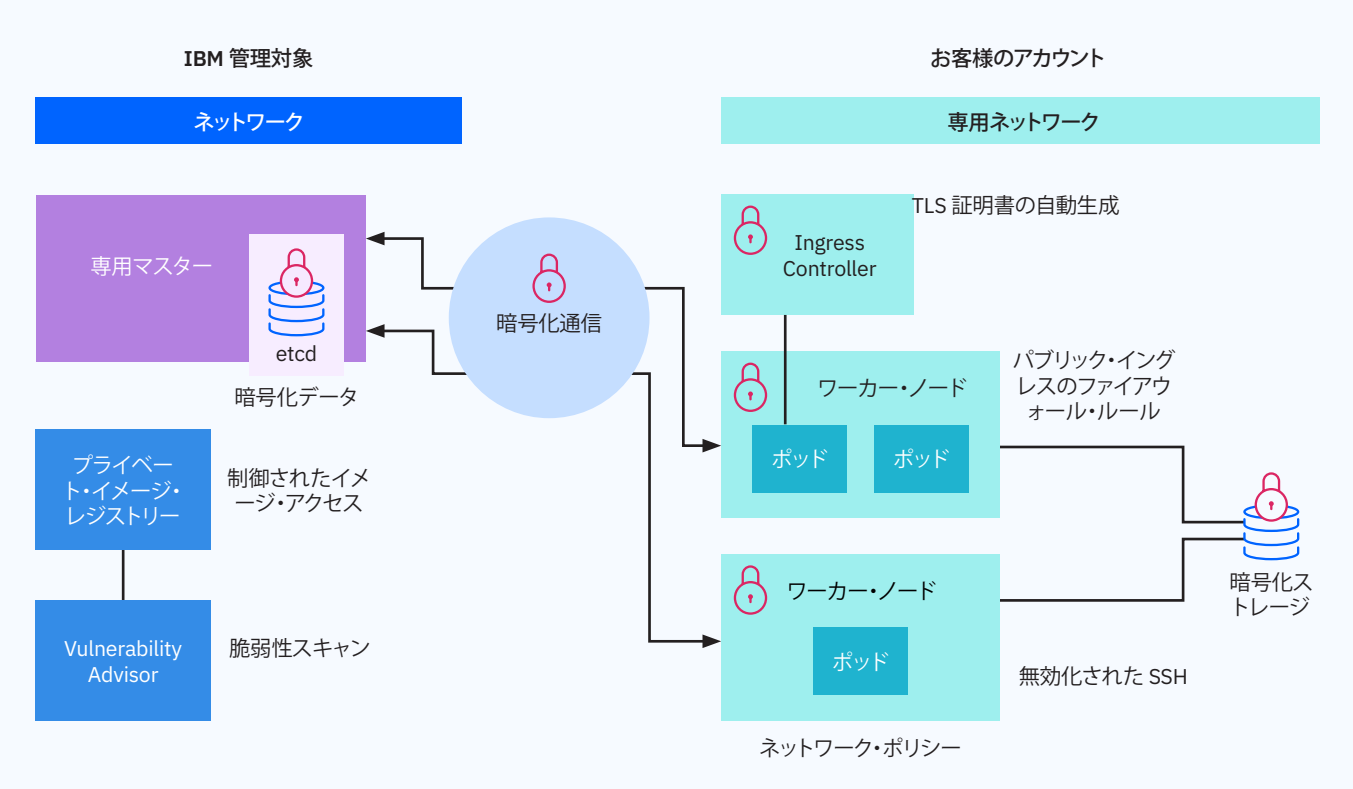


図 2. プロバイダー管理対象および顧客管理対象クラスター・エレメントの分離。

信頼の連鎖におけるメリットを拡大

フル実装された信頼の連鎖、セキュリティー・ポリシーに結び付けられたリモート認証と暗号化により、コンテナー・アプリケーション、ワークロードを管理するこれらの重要な機能が実現します。

- **透明性とスケーラビリティー:** 信頼の連鎖によって実現する自動化のおかげで、DevOps チームは足かせから自由になってスムーズに作業に取り込めます。DevOps チームは、信頼されるコンテナー・システムがその測定値を評価するセキュリティー・ポリシーのみ管理すれば済みます。適切に構成すれば、オーケストレーションによって、リアルタイムのトラフィックを基にアプリケーション・リソースがある程度自動的にスケーリングされます。
- **地域のワークロード・ポリシーの検証:** スマート・コンテナー・オーケストレーションは、承認された場所だけに移動を制限します。
- **コンテナーの確実な完全性:** コンテナーを移動する場合は、プロセスの間に改竄が行われていないことがチェックされます。移動されたコンテナーは、元の作成されたコンテナーと同じかどうかが検証されます。
- **機密データのセキュリティー:** 暗号化コンテナーは、特定の場所の承認済みサーバー上でしか復号化できません。
- **簡素なコンプライアンスの管理とレポート:** メタデータ監査証跡は、信頼できるサーバー上で重要なコンテナー・ワークロードが稼働していることを可視化し、監査可能な証拠を提供します。

重要なポイント

自社チームがクラウド・プラットフォームを評価する際、アプリケーションをホストするテクノロジーのフットプリントで信頼がどのように確立され、維持されるのかベンダーに説明を求めてください。これは、顧客エンゲージメントと重要データの保持を行う上で自社ビジネスが依存する基盤です。

典型的な例: GDPR への不安の軽減

あなたの会社では欧州に顧客がいて、EU 一般保護規則 (GDPR) が発効するに伴う大きな義務について不安を抱いているとしましょう。主権要件や他の規制のために、特定の種類のデータを作成元の国から送信できないので、あなたの会社は次のことを行う必要があります。

- ワークロードを特定の場所で実行したい場合、ほかの場所には移動できず、移動しないことを強く保証する。
- ワークロードを配置した場所以外でデータを復号化できないように、ワークロードの暗号化鍵を管理する。

ハードウェアベースの信頼の連鎖を確立したら、完全性の維持にとって重要なすべてのエレメントを結びつけて、キーを管理し、ワークロードのローカリティを保証できます。また、この信頼をポリシーを通じて推進して、アプリケーションの展開とともにセキュリティーをスケーリングできます。

固定コンテナーとライブ・コンテナーのスキャン

Docker コンテナーの導入は簡単です。開発者は Docker Hub で公開されているコンテナー・イメージをプルダウンして、たとえば、イメージ・スタックの部品準備に必要な時間を回避または大幅に短縮できます。問題は、導入前にイメージに何があるのかが確実にわからないことです。したがって、DevOps パイプラインに正式にリリースする前に、各イメージをスキャンする習慣をつけることが必要です。クラウド・プラットフォームは、この処理を効率的に実行できなくてはなりません。

IBM® Cloud Container Service はたとえば、Vulnerability Advisor (VA) システムを提供して、固定コンテナーとライブ・コンテナー両方のスキャンを実行します (図 3)。VA はクラウドのお客様のプライベート・レジストリーに格納された各イメージのすべての層を検査して、イメージの展開前に脆弱性やマルウェアを検出できるように支援します。ただし、レジストリーのイメージをただスキャンするだけでは、固定イメージから展開済みコンテナーへのドリフトなどの問題が見落とされることがあるため、VA は実行中のコンテナーの異変がないかもスキャンします。また、段階的アラートの形で推奨事項を提供します。

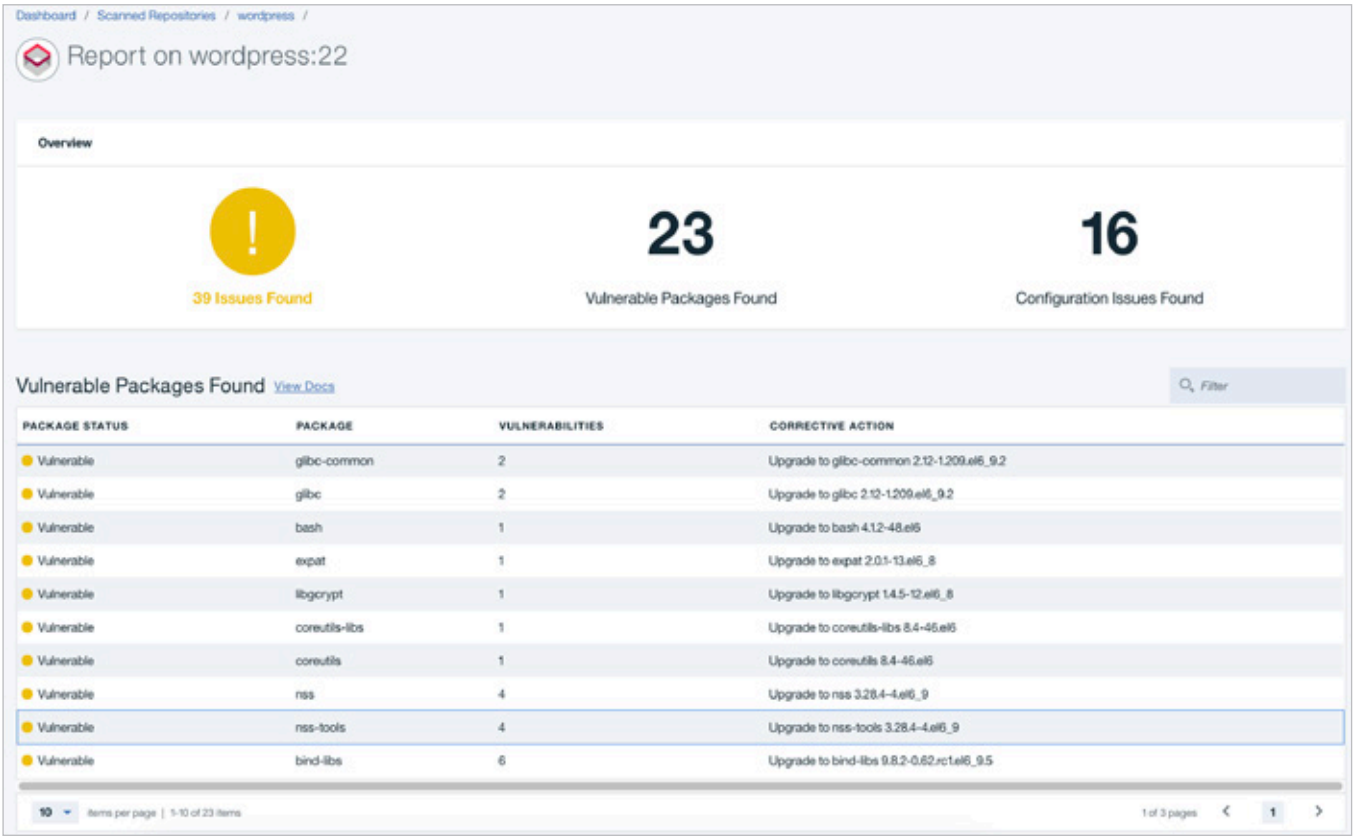


図 3. VA が X-Force と統合して、攻撃元区分、攻撃の複雑さ、既知の修正の利用可能性を基に脆弱性を評価。

クラウド分離テクノロジー

チップベースのテクノロジーからわかるように、信頼の連鎖を実装するには、VPN アクセスをサポートする専用ホストに展開する機能が必要です。すべてのコンテナーが、コンピュート・ホスト上でそれぞれ個別に分離されたプロセスとして実行されるべきであり、そのリソースへのアクセス権を制限するべきです。

クラウド・プロバイダーは、最適なコンピュート・ホスト・カーネルを使用することで、すべてのコンピュート・ホスト上で実行されているスレッドとプロセスの総数を自動的に制限できる必要があります。この最適化により、アプリケーション性能に影響を及ぼす可能性がある、ホストの過負荷を確実に避けられます。

また、サービス・プロバイダーは、継続的にコンピュート・ホストを監視して、Fork 爆弾や他のプロセスレベルの DoS 攻撃を制御し、修正する必要があります。フォルダー、ファイル、ネットワーク・ドメインへのアクセス、データの作成と変更の権限を管理するセキュリティー・コントロールは、Linux カーネル・レベルで開始する必要があります。

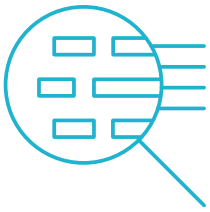
クラウド・セキュリティーの可視化

運用エンジニアはオンプレミスのリソースを精査することが習慣化しており、当然、クラウドベースのコンテナー化されたワークロードにも同じ洞察を期待します。この可視性を実現するには、クラウド・ベンダーは、企業またはベンダーかに関係なく、すべてのユーザー・アクセスと管理アクセスを自動的に記録すべきです。組み込みのクラウド・アクティビティー・トラッカーは、プラットフォームとサービスへのすべてのアクセスの証跡を作成して、お客様の企業に関連ログへのアクセス権を付与できます。

すべてのログとイベントをオンプレミスのセキュリティー・オペレーション・センター (SOC) 、およびセキュリティー情報とイベント管理 (SIEM) システムに統合する選択肢を確保してください。一部のクラウド・サービス・プロバイダーは、インシデント管理と報告機能の付いたセキュリティー・モニタリング、セキュリティー警告のリアルタイム分析、複数のハイブリッド環境の統合ビューなど、追加のサービスを提供します。

たとえば、IBM QRadar® は包括的な SIEM ソリューションで、企業のニーズに応じて拡張できるセキュリティー・インテリジェンス機能を提供します。インテリジェント・セキュリティー免疫システムを強化するやり方で脅威パターンに照準を合わせる機械学習機能が搭載されています。

Vulnerability Advisor について



IBM Vulnerability Advisor の機能は次のとおりです。

- **ポリシー違反設定:** VA を使用すると、管理者は、既知の脆弱性があるインストール済みパッケージ、リモート・ログインの有効化、パスワードを容易に推測した一部のユーザーによるリモート・ログインの有効化という 3 種類のイメージの失敗のケースを基に、イメージ展開ポリシーを設定できます。
- **ベスト・プラクティス:** VA は現在、ISO 27000 を基に 26 のルールをチェックします。チェックには、パスワードの最小期限、最小パスワード長、リモート・ログインの有効化などの設定が含まれます。
- **セキュリティーの構成の誤りの検出:** VA は、不適切な構成の問題それぞれにフラグを立ててその状態を説明し、修正するための対策を推奨します。
- **IBM X-Force® との統合:** VA は 5 つのサードパーティ・ソースからセキュリティー情報を取得して、攻撃元区分、攻撃の複雑さ、既知の修正の利用可能性などの基準を使ってそれぞれの脆弱性を評価します。評価システム (重大、高、中、低) により、管理者は脆弱性の重大度を素早く理解して、修正の優先順位を付けます。

ビジネス・サービスにおけるエンド・ツー・エンドのセキュリティーのニーズ

コンテナー・テクノロジーは、クラウド環境における共同作業の速度を効率化し、速めることでアプリケーション開発チームの役に立ちます。しかし、これらのメリットを実現するには、クラウド・プラットフォームは必要以上の摩擦を引き起こさずに、CISO セキュリティー要件を満たさなければなりません。したがって、DevOps チームはビジネス目標の達成のために、自動化セキュリティーを介して CISO ポリシーを実装する必要があります。

ハードウェア・ベースの信頼の連鎖は、この目標を達成するための効果的な基盤になります。信頼コンテナーを実現するテクノロジー、コンテナーの展開を管理するセキュリティー・ポリシーを適用するためのテクノロジーがその中に含まれている必要があります。信頼の連鎖テクノロジーは、セキュリティーおよび急速なイノベーションの両方の差し迫ったニーズを満たすようになっています。

- セキュリティー責任者は、作成または移動された各コンテナーに自動的に適用されるセキュリティー・ポリシーを定義できます。
- シーケンスの各ステップが自動化されるので、DevOps チームは、作業を中断してセキュリティー・コンポーネントを追加しなくても、アプリケーションを素早く構築し、展開できます。

このアーキテクチャーは、クラウド・プラットフォームのハードウエア・レベルからコンテナー・オーケストレーション層までのデータとアプリケーションを保護して、EU GDPR、米国連邦政府のリスク・認証管理プログラム (FedRAMP: Federal Risk and Authorization Management Program) や米国医療保険の携行性と責任に関する法律 (HIPAA: Health Insurance Portability and Accountability Act) などのコンプライアンス体制を満たせるように企業を支援します。企業は、業界に必要なポリシーを正確に定義し、確実さの要素を保証します。

IBM の観点

信頼の連鎖を革新することは、IBM とパートナー企業にとって重要な焦点です。IBM とインテルは長期的に提携して、信頼の連鎖セキュリティー・ソリューションの開発に打ち込んでおり、現在、その専門知識をコンテナーベースの製品に適用しています。その目標は、今日の革新者が求め、受けるに値する開発の柔軟性と最先端のマイクロサービス・アーキテクチャーを実現できるように、コンテナーを安全かつ敏捷に展開できるように企業を支援することです。

IBM Cloud は、展開と管理を自動化する、すぐに使用できるオープン・ソース・ツールをチームに提供します。また、お客様がワークロードを複数のクラウドに展開したいのであれば、クラウド・プラットフォームは、一貫して同じツールをマルチクラウド環境で使用できるようにしなくてはなりません。コンテナー・セキュリティーの将来は、オープンで敏捷性に富み、可能な限り自動化されており、強力かつインテリジェントな防御機能を備えたものになります。

コンテナー・セキュリティーの将来は、オープンで敏捷性に富み、可能な限り自動化されており、強力かつインテリジェントな防御機能を備えたものになります。

詳細情報

コンテナー・セキュリティーの信頼の連鎖を構築する方法については、ibm.com/cloud/container-service をご覧ください。

セキュリティーと DevOps についてもっと知りたいですか? Slack チャネル に参加して、IBM Cloud Container Service 製品チームと意見を比べてください。

IBM とつながる

IBM Cloud Container Service
IBM Cloud ブログ

フォローする

@IBMcloud
Facebook

お問い合わせ先

LinkedIn
YouTube

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722

Produced in Japan February 2018