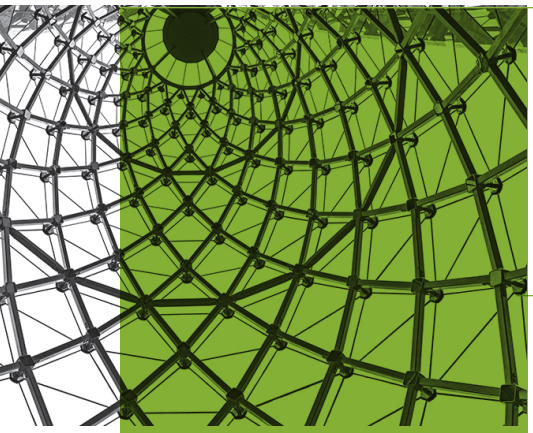

JUNIPER CLOUD WORKLOAD PROTECTION

製品概要

Juniper Networks® Cloud Workload Protectionは、アプリケーションの脆弱性を悪用する攻撃、たとえばOWASP Top 10攻撃やメモリベースの攻撃が発生したときに、クラウド環境またはオンプレミス環境におけるアプリケーションワークロードを自動的に保護します。アプリケーションの実行を制御し、アプリケーションの動作とコンテキストを監視して、リアルタイムで発生している事象に対してアプリケーションが何を実行すべきかを判断します。ランタイム保護によって、ターゲットとなっている脆弱性が悪用されることがないように自動的に保護を行い、管理者が関与する必要がありません。Juniper Cloud Workload Protectionを導入すると、本番用アプリケーションは脆弱性を狙う不正プログラムに対するセーフティネットで常に守られ、ビジネスクリティカルなサービスを継続的に接続および保護できます。

製品説明

アプリケーションセキュリティは、「エクスペリエンスファーストネットワーキング」というジュニパーの理念の中核となっています。Web閲覧からチャット、モバイルゲーム、仕事をこなすためのサービスまで、ネットワーク上で行うほぼすべてのことにアプリケーションが関わっています。アプリケーションがデータを保存、処理、交換することで、私たちは互いにつながり、デジタルライフがより快適なものとなります。アプリケーションを利用する際は、アプリケーションにすぐにアクセスできなければなりません。また、アプリケーションが安全であると信頼した上で利用しています。

アプリケーションをコーディングする際に、攻撃者の利用できるコーディングエラーが含まれることがあります。このようなエラーがあると、データベースやレジストリなどのアプリケーションが機能するうえで基盤となるリソースやプロセス（すなわちワークロード）が脆弱なものとなります。安全なコーディングを心掛けていても、アプリケーションに何らかの脆弱性があることに気付くのは、手遅れになった後という場合もあるかもしれません。ゼロデイ攻撃などの脆弱性を狙った攻撃からアプリケーションのワークロードを守るセーフティネットが必要です。

Juniper Cloud Workload Protectionは、ますます高度化している脆弱性を狙った攻撃を非常に効果的に検知します。多くの場合、アプリケーションをターゲットとする攻撃は、ネットワークとエンドポイントのセキュリティソリューションによる検知をかいくぐります。Juniper Cloud Workload Protectionは、導入が簡単な非侵襲エージェントで、数分でインストールできます。また、OCFI（制御フローインテグリティの最適化）という決定論的技術を利用して、実行時に各アプリケーションのDNAマップを自動作成します。このマップを使用することで、アプリケーションが正常に実行されているかを判別し、攻撃を非常に正確に検知し、誤検知はほとんどありません。

Juniper Cloud Workload Protectionは、パブリッククラウド、オンプレミス、ハイブリッドの各環境に導入可能で、Webアプリケーション、コンテナワークロード、Kubernetesを保護します。アプリケーションの稼働後でも稼働前であっても、Juniper Cloud Workload Protectionが効果的に防護するため、開発者は責任を問われる前に脆弱性を修復でき、企業はコンプライアンスを維持できます。

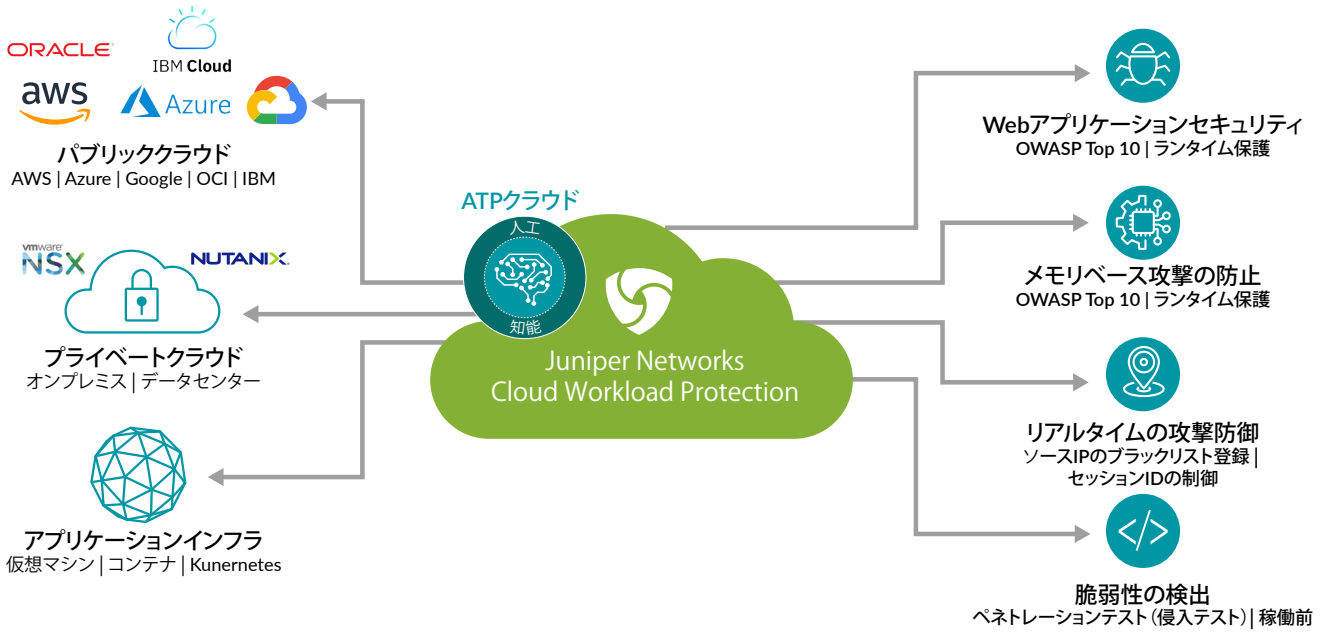

図1：Juniper Cloud Workload Protectionのアーキテクチャ。

アーキテクチャと主要コンポーネント

Juniper Cloud Workload Protectionは軽量のエージェントで、アプリケーション内だけでなく、Docker、Kubernetes、AWS Fargateのワークロードにも導入できます。サポートされているアプリケーション言語は、Java、Node.JS、PHP、Rubyです。Juniper Cloud Workload Protectionの機能は以下のとおりです。

- ゼロデイ攻撃：決定論的手法を適用して、未知の脆弱性またはパッチ未適用の脆弱性を狙ったゼロデイ攻撃を検知します。
- 脆弱性を管理：アプリケーションやコンテナに含まれる脆弱性を継続的に評価します。
- コンテナを監視：コンテナの動作を監視してレポートするとともに、脆弱性をスキャンします。
- 最小限の誤検知：独自のDNAマップを使用することで、誤検知の数が大幅に少なくなります。このDNAマップは、動作やシグニチャを参照しなくても、アプリケーションの実行を検証できます。
- 安全なメッシュ/セグメント化：セキュリティサービスメッシュとセグメント化により、ワークロードのセキュリティを向上させるとともに、攻撃が水平方向に拡散することを防止します。
- 包括的なテレメトリ：アプリケーション接続やトポロジーなど、豊富なアプリケーションレベルのセキュリティイベントを生成し、レポートを出力します。

特長とメリット

Juniper Cloud Workload Protectionは、軽量のソフトウェアエージェントです。アプリケーションの実行を制御し、アプリケーションの動作とコンテキストを監視して、リアルタイムに発生している事象に対してアプリケーションが実行すべきことを判断します。脆弱性は自動的に修復されるため、管理者が対応する必要はありません。Juniper Cloud Workload Protectionを導入すると、本番用アプリケーションは脆弱性を狙う不正プログラムに対するセーフティネットに常に守られ、ビジネスクリティカルなサービスを継続的に接続および保護できます。このジュニパーの新製品は、次のような重要な機能を備えています。

アプリケーション実行時の保護

シグネチャレスかつサーバーレスのアプリケーション実行時における自己防御機能により、攻撃からリアルタイムで保護します。エンドポイント検知やWebアプリケーションファイアウォールなどのソリューションでは対応できない高度な攻撃を検知し、人手を介さず、データの悪用や盗難などの悪意のある攻撃からアプリケーションを保護します。

OWASP Top 10攻撃およびメモリベース攻撃の防止

Juniper Cloud Workload Protectionは、OWASP Top 10攻撃やメモリベース攻撃など、重大なセキュリティリスクに対する防御をリアルタイムで行います。メモリベース攻撃としては、ファイルレス攻撃、リターン指向プログラミング攻撃、バッファーオーバーフロー攻撃などがあります。

包括的なテレメトリ

DevSecOpsチームは、アプリケーション接続、トポロジー、試みられた攻撃に関する詳細な情報など、アプリケーションレベルの各種セキュリティイベントの生成およびレポート出力により、脅威を把握できます。

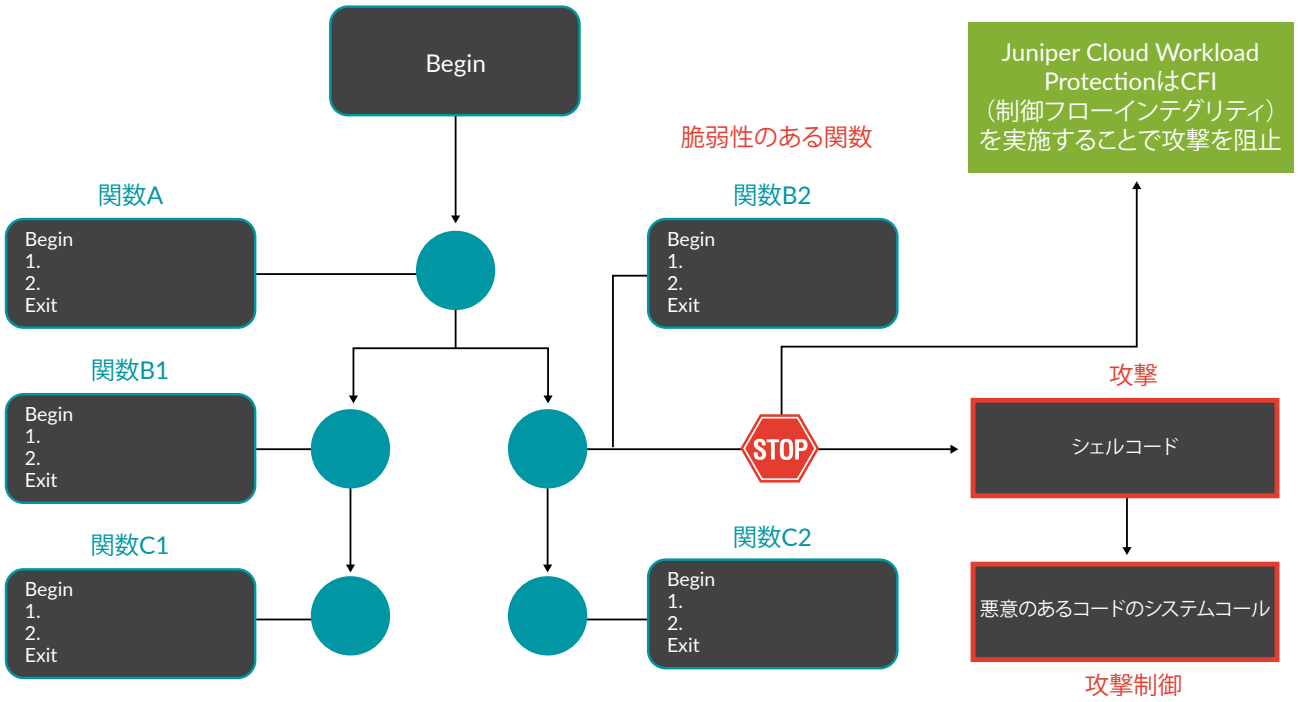

図2：制御フローを統合して脅威と攻撃を防止。

最小限の誤検知

OCFI（制御フローインテグリティの最適化）テクノロジーが、アプリケーションの実行を検証し、攻撃を検知することで、誤検知の数を最小限に抑えます。動作やシグネチャは参照しません。

Webアプリケーションセキュリティ

Webアプリケーションに対する高度な攻撃は、EDR（End-point Detection and Response）製品やWebアプリケーションのファイアウォールなどの、シグニチャやパターンマッチングを用いたソリューションの検知を回避します。Juniper Cloud Workload Protectionは、アプリケーションの実行を継続的に検証し、誤検知を最小限に抑えながら、攻撃をリアルタイムで検知します。未知の脆弱性があった場合や、すぐにはパッチを用意できない脅威があった場合でも、Juniper Cloud Workload Protectionが、ビジネスサービスとアプリケーションの脆弱性を狙った攻撃から保護します。Juniper Cloud Workload Protectionの特長は以下のとおりです。

- アプリケーションのセキュリティが大幅に向上
- Webアプリケーションに影響を与えることなく、高性能アーキテクチャを維持
- よく利用される開発言語とクラウドサービスをサポート

脆弱性の検出

セキュリティ担当チームは、短時間でアプリケーション、コンテナ、カスタムコード内に隠れた脆弱性を見つけることができます。継続的導入モデルは、テスト期間の短縮に役立ちますが、脆弱性のあるコンポーネントが本番環境に紛れ込む可能性が非常に高いという問題があります。Juniper Cloud Workload Protectionを、侵入テストツールおよびスキャンツールとともに導入や、QA環境に導入することで、脆弱性を自動的に検知する統合ソリューションとなります。Juniper Cloud Workload Protectionは以下を提供します。

- 1つのソリューションで、アプリケーション、コンテナ、ユーザーコード内の脆弱性を検知
- コード内のどこに脆弱性があるかを正確に検出し、攻撃される可能性が高い証拠を特定することで、現状を把握して迅速に修復
- 継続的な統合プロセス、継続的な開発ワークフロー、セキュリティテスト方法にエージェントを統合し、他に影響を与えることなく自動化が向上

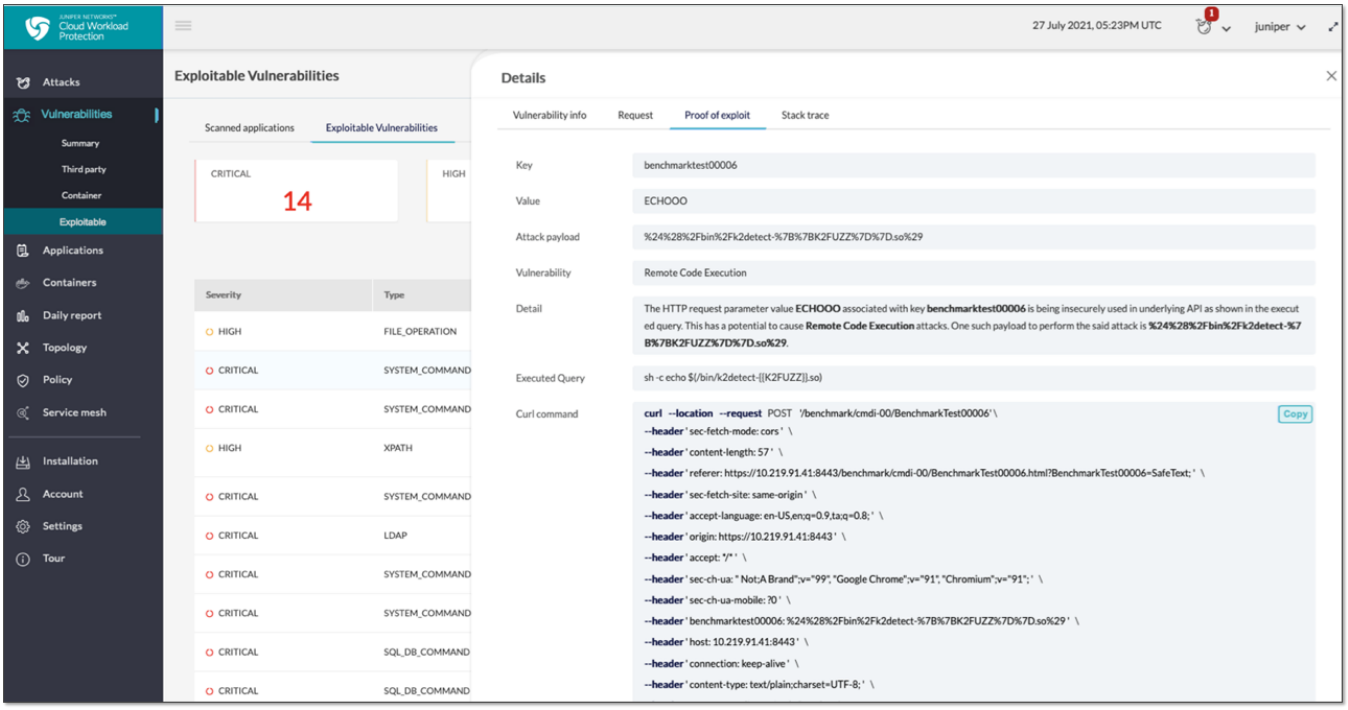

図3：悪用される可能性のある脆弱性のダッシュボード。

コンテナおよびワークロードのセキュリティ

コンテナを稼働させるクラウドネイティブアプリケーションは、コンテナに脆弱性やバックドアがあれば、侵害される可能性があります。Juniper Cloud Workload Protectionが、アプリケーションの保護に加え、コンテナの動作を監視して、脆弱性がないかスキャンすることで、セキュリティが向上します。セグメント化およびセキュアメッシュにより、セキュリティがさらに向上し、攻撃の影響範囲を狭めます。Juniper Cloud Workload Protectionは以下を提供します。

- コンテナおよびアプリケーションワークロードの脆弱性をスキャン
- すべてのコンテナの動作とAPIの利用状況を監視し、バックドアを検知
- コンテナおよびKubernetesに導入されたクラウドネイティブアプリケーションを保護

ゼロトラストのマイクロセグメンテーション

Juniper Cloud Workload Protectionは、マイクロセグメンテーションと、Juniper Networks® vSRX仮想ファイアウォールとの統合により、アプリケーションリソースを水平方向の脅威拡散から保護し、ワークロード環境や仮想環境が変化した場合も含め、リスクレベルに基づいてアクセスを制限します。セキュリティチームは、内蔵されているリアルタイムテレメトリによる脅威への自動対応により、脅威を検知すると、直ちにネットワーク全体でブロックすることができます。

Juniper Cloud Workload Protectionは、脅威を認識するネットワークを構築するうえで重要なコンポーネントである、ジュニパーのゼロトラストデータセンターアーキテクチャの最新の構成要素です。ジュニパーの世界クラスのデータセンターネットワークソリューションとConnected Security戦略が、複数のデータセンター環境でアプリケーションインフラストラクチャを接続、オーケストレーションし、データセンターゲートウェイから、サーバー間およびアプリケーションワークロード内の相互接続まで、すべての接続ポイントで安全性を確保します。

注文情報

Juniper Cloud Workload Protectionはフレキシブルなライセンスオプションを提供し、アプリケーションごと、またはワークロードごとに購入できます。すべてのライセンスを中期的に他のアプリケーションまたはワークロードに移行することもできます。追加費用はありません。

Juniper Cloud Workload Protectionのライセンスの注文情報またはソフトウェアライセンスに関する情報については、www.juniper.net/jp/ja/how-to-buy/の「購入方法」ページをご覧ください。

ジュニパーネットワークスについて

ジュニパーネットワークスは、ネットワーク運用を大幅に簡素化し、エンドユーザーに優れたエクスペリエンスを提供することを目指しています。業界をリードするインサイト、自動化、セキュリティ、AIを提供する当社のソリューションで、真のビジネス成果をもたらします。つながりを強めれば、人々の絆がより深まり、幸福、持続可能性、平等という世界最大の課題を解決できるとジュニパーは信じています。

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号：888. JUNIPER (888.586.4737)
または +1.408.745.2000
www.juniper.net

アジアパシフィック、ヨーロッパ、中東、アフリカ
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話番号：+31.207.125.700

日本
東京本社
ジュニパーネットワークス株式会社
〒163-1445 東京都新宿区西新宿3-20-2
東京オペラシティタワー45階
電話番号：03-5333-7400
FAX：03-5333-7401
西日本事務所
〒530-0001 大阪府大阪市北区梅田2-2-2
ヒルトンプラザウエストオフィスタワー18階
www.juniper.net/jp

Driven by Experience™