SOLUTION BRIEF

FortiCNPが実用的なインサイトを通じてクラウドネイティブのリスクを管理する

FortiCNP のリスク管理機能

- クラウドネイティブセキュリティツールの価値を最大化
- ハイリスクのリソースを優先的に修復
- リスク管理と封じ込めのプロセスを合理化

概要

ほぼすべての企業や組織が、業務のモダナイゼーション、迅速なイノベーション、成長の加速を目指してクラウドを導入しており、その勢いが衰える兆しはありません。Gartnerの予測によれば、2025年までに新たなデジタルワークロードの95%以上がクラウドネイティブなプラットフォームに展開されると見られています。[1]

しかしクラウドに重要なワークロードを移行する企業が増えることで新たなリスクも発生しています。従来のセキュリティソリューションには、このリスクに対応できるだけの十分な機能がありません。そして新しいポイント製品（ポイントプロダクト）のセキュリティソリューションをインフラストラクチャ全体に追加することで、セキュリティアーキテクチャが断片化されてしまうことがよくあります。その結果、あらゆる管理が難しくなり、リスクが増大することになります。

クラウドワークロードにはクラウドネイティブなセキュリティソリューションが必要

最新のデジタルビジネスアプリケーションは複数のワークロードから構成されています。これらのワークロードは非常に複雑でハイブリッドおよびマルチクラウド環境全体に展開されている場合があります。こうしたワークロードを進化する脅威環境から保護するために、クラウドセキュリティにはクラウド内の変化に対応しながら、あらゆる環境とテクノロジースタック内の複数の脅威ベクトルに柔軟に対処できることが求められています。

FortiCNPはフォーティネットのクラウドネイティブアプリケーション保護プラットフォーム（CNAPP）です。クラウドネイティブアプリケーションの保護を目的として、クラウドセキュリティポスチャ管理（CSPM）、クラウドワークロード保護プラットフォーム（CWPP）、そしてその他のセキュリティソリューションのセキュリティ機能を統合し、クラウドのリソースと環境全体でリスクをスムーズに管理できる摩擦のないアプローチを提供します。

FortiCNPはクラウドセキュリティを簡略化して企業がリスク管理のための防御策をすぐに実行できるようにします。フォーティネットの画期的なアプローチによってセキュリティソリューションに伴うありがちな課題やクラウド導入への障壁を解消することができます。

断片化したセキュリティソリューションがセキュリティポスチャを弱体化させる可能性

今日のように急激に進化しているIT環境では、企業は新たなリスクに対抗するため、新しく画期的なセキュリティソリューションに常に投資していくことになるでしょう。しかしこうしたポイントソリューションの多くは統合されていないため、新たなソリューションが追加されるたびに企業のセキュリティインフラストラクチャがさらに複雑になり、断片化されてしまいます。最近の調査では大手企業の59%が50以上の異なるセキュリティツールを導入していることがわかりました。セキュリティチームは通常、その多くを使ってセキュリティインシデントの調査と対応を行っています。[2]

セキュリティツールが多すぎるのは逆効果で、企業や組織はより多くのリスクに見舞われます。その結果、管理や更新のコストが増えるだけでなく、異なる機能を備えたソリューション、管理ツール、インタフェースによって可視性が断片化されてしまいます。また脆弱性、機密情報、設定ミス、高度な攻撃、分散化された環境でのリソースリスクなどから優先度の高いリスクを特定することがますます難しくなり、最終的にはセキュリティの対応範囲が不十分になってしまいます。

アラート対応への疲弊で妨げられるプロアクティブなリスク管理

プロアクティブにソリューションを強化し、セキュリティの対応範囲を拡大して防御を強化しようとする企業は、各セキュリティソリューションが生成するセキュリティアラートの量を少なく見積もってしまいがちです。場合によってはセキュリティソリューションが毎日数千件のアラートを出力することがあるため、優先順位の決定や管理を行う体制が整っていない企業も少なくありません。

またアラートの多くは、影響を低減するための作業の優先順位付けに必要なコンテキストを欠いているため、セキュリティチームが手作業で各アラートの分析や調査を行わざるをえない状況となっています。こうした手作業ではリスク管理やセキュリティニーズへの迅速な対応がますます困難になります。そのためセキュリティアナリストの80%以上がアラート疲れに悩まされています。[3] さらに、最近の調査ではセキュリティアナリストの3分の1以上が、アラートのキューがいっぱいになるとセキュリティアラートを無視してしまうことが判明しています。[4]

プロアクティブなリスク管理はCISO（最高情報セキュリティ責任者）の最も重要な責務の1つです。これは効果的なクラウドネイティブのセキュリティソリューションを実装し、リスクを管理し、低減することで達成できます。しかし調査が必要なデータ量が多すぎてセキュリティチームに負荷がかかりすぎたり、もしくは調査すべきデータをすっかり放置してしまったりした場合、企業のセキュリティが危険にさらされる可能性があります。たった1つのアラートを見逃すかどうかで、重大なリスクから企業を守ることができるか、それとも広範なセキュリティ侵害を引き起こし、お客様に影響を与え、組織やブランドを傷つけ、多額の罰金を科せられるかの、いわば分かれ目になる可能性があるのです。

Resource Risk Insights（RRI）によるクラウドリスクの管理

FortiCNPは、複数のリソースにわたって存在する大量のセキュリティアラートと調査結果を統合し、重要なリソースの優先処理を行うためのアクションに結び付くインサイトを備えたリソース中心（リソースセントリック）のビューを提供することで、セキュリティチームがクラウドリスクをプロアクティブに管理できるように支援します。

FortiCNP Resource Risk Insights（RRI）テクノロジーは、統合されたセキュリティサービスやFortinet Cloud Securityソリューションから発せられるセキュリティアラートと調査結果をクラウド環境全体で関連付けてコンテキスト化し、集約したリスクスコアを生成します。このスコアは、コンプライアンス、脆弱性、データ属性、ユーザーアクセスと挙動などのさまざまな側面だけでなく、企業のカスタムポリシーなどのローカルな属性も考慮されています。RRIはリソースに優先度を付けることで重大なリスクに重点を置きやすくし、アクションに結び付くインサイトも提供することで、セキュリティチームがすぐに対策を講じられるようにします。

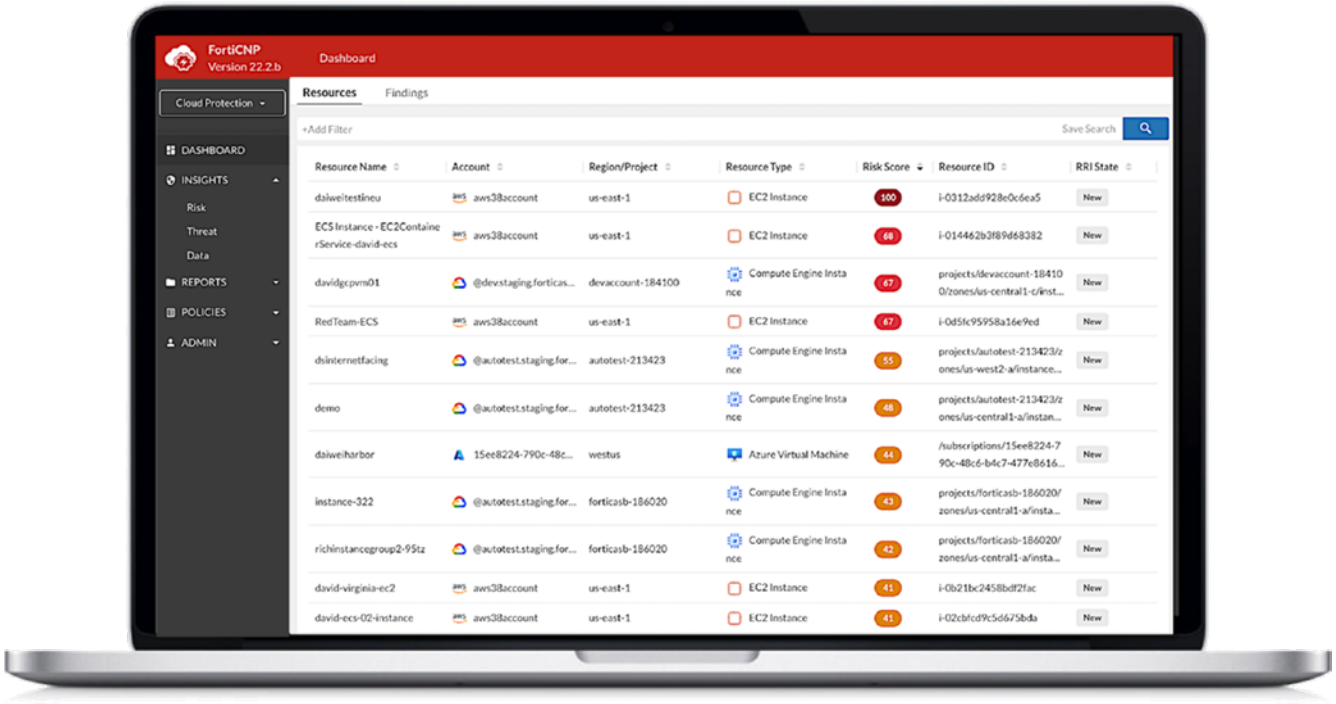

図 1：FortiCNP は膨大な量のセキュリティアラートから豊富なコンテキストを含むセキュリティインサイトを生成

クラウドネイティブなセキュリティサービスの価値を補完

クラウドサービスプロバイダー(CSP)はクラウドリソースのセキュリティを確保するためのテクノロジーに継続的に投資しています。そして多くのCSPセキュリティサービスがコンピュート、ストレージ、データベースリソースのリスク、脆弱性、脅威に関する有益な情報を提供できるようになりました。企業の57%が複雑化する脅威を管理するためのクラウドセキュリティ専門家を確保しづらいと回答している状況を考えると、これは朗報です。[5]

CSPのクラウドネイティブなセキュリティサービスを活用することで、顧客に多くのメリットを提供することができます。特定のクラウド環境のサービスやインフラストラクチャ全体に簡単に導入し、きめ細かく統合することができるので、これにより断片化されたセキュリティアーキテクチャで多くの企業が抱えている統合の問題を低減することができます。さらにこれらのサービスは、より広範囲にわたって、クラウドのワークロードの効果的な管理と保護に役立ちます。

FortiCNPはCSPのネイティブなセキュリティサービスとフォーティネットセキュリティファブリック製品を補完し、クラウドのリスクを管理する多層的なアプローチを提供します。そして、RRIはクラウドリソースに関してコンテキストリッチでアクションに結び付くインサイトを提供します。また、アクションに結び付くアラートによって企業は調査結果の重大度に基づいてアクションの優先度を決め、コンピュートインスタンス、コンテナ、データベースサービス、データストレージサービスなどさまざまなパブリッククラウドリソースの利用を保護することができます。

FortiCNPは各プラットフォームのAPIを使用してクラウドのワークロードの可視性を確保し、クラウド環境全体でのリソースのリスクを分析して優先度を決定します。セキュリティチームが最も重大なリスクを優先的に処理できるように、RRIはリスクを計算し、そのリスクスコアに基づき最もリスクの高いリソースの優先順位の判定を行います。これによりセキュリティチームはしばしば発生する大量のセキュリティデータに忙殺されることがなくなり、お客様はセキュリティツールの価値を最大化することができます。

FortiGuard Labsとの統合によって悪意のあるIPアドレス、ドメイン、URL、ボットネットに関するリアルタイムトラフィックとデバイスセキュリティ情報を基にFortiCNPのインサイトを強化することができます。

FortiCNPはCISOにとってもメリットがあります。開発者による実装が簡単で、実装済みのフォーティネットセキュリティソリューションも認識しやすくなるので、クラウドネイティブなセキュリティ制御の価値の実現をスピードアップすることができます。FortiCNPのダッシュボードを通じて、CISOは企業のセキュリティポスチャの経時的な改善状況を可視化することもできます。

FortiCNPでは標準ベース及びベストプラクティスに基づいて設定ミスのリスクを管理するために使用する事前定義されたポリシーのほかに、高度なスクリプト機能を使用してクラウドの設定を評価するカスタムポリシーを作成することもできます。

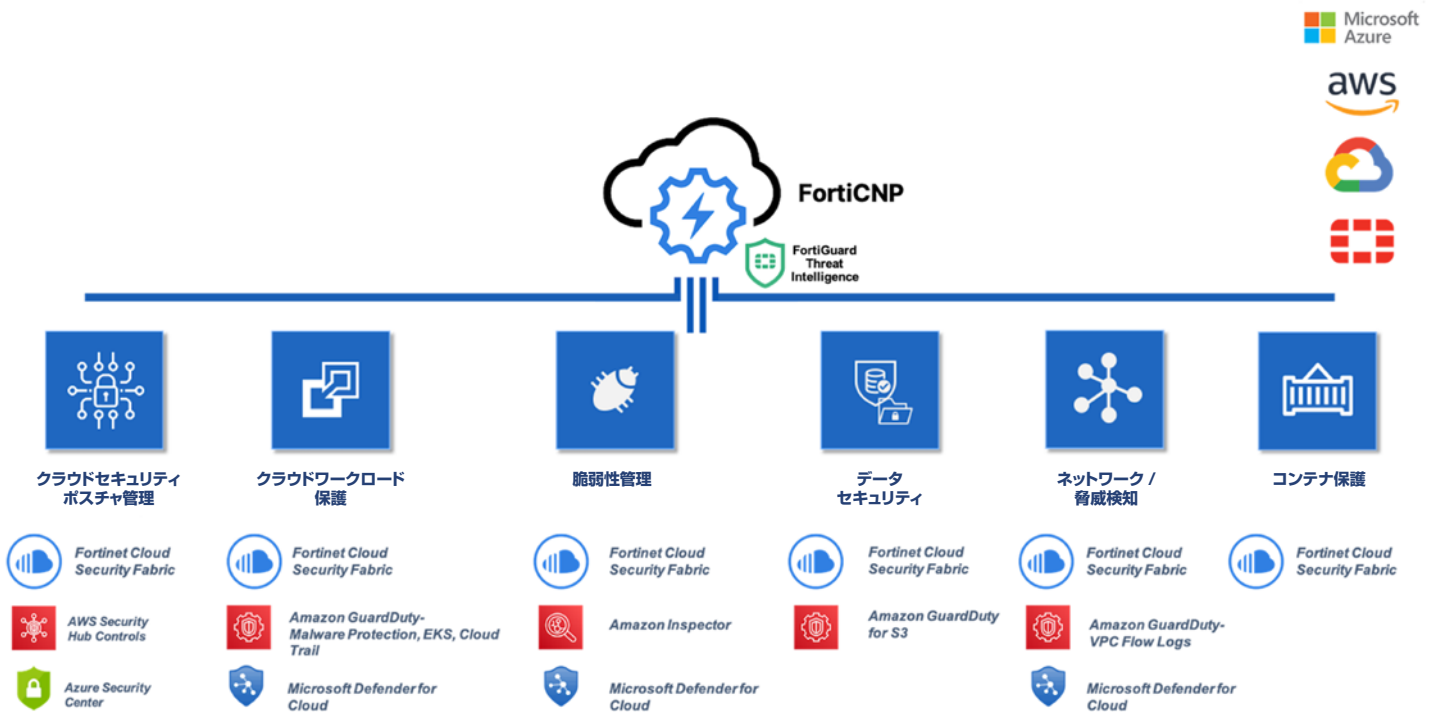

図 2 : FortiCNP によるクラウドネイティブなセキュリティサービスの統合

FortiCNP によるセキュリティ運用の効率化

FortiCNPは、優先度の高いリスクに関するインサイトを得るためにJIRAやServiceNowなどのデジタルワークフローソリューションとの統合し、リソースの所有者が重要な修復ステップを実施するプロセスを自動化し、管理することで、緩和·低減および修復プロセスの合理化を支援します。

複数のクラウドで一貫したワークフローを設けることで、セキュリティチームはセキュリティの対応範囲におけるギャップを最小化して生産性を高めることができます。

プロアクティブなリスク管理

企業はクラウドリスクをプロアクティブに管理するための戦略を進化させる必要があります。それにはまず、コンピュート、ストレージ、データベースリソースのリスク、脆弱性、脅威に対し、幅広く効果的なセキュリティ対応を実現するクラウドネイティブなセキュリティサービスを活用することから始めることになります。こうしたサービスは実装が非常に簡単で、多くの企業が経験する統合の課題も軽減します。これらのサービスとフォーティネットのクラウドセキュリティ製品が発するアラートをFortiCNPの包括的で豊富なコンテキストを含むRRIテクノロジーと組み合わせることで、企業は投資効果を最大化しつつリスクの高い項目に集中してプロアクティブなリスク管理を行うことができます。

[1] "Gartner Says Cloud Will be the Centerpiece of New Digital Experiences," Gartner, November 2021.

[2] "Cyber Resillient Organization Study 2021," IBM, 2021.

[3] "2020 State of SecOps and Automation Report," Sumo Logic, 2021.

[4] "The Voice of the Analysts," IDC, 2021.

[5] "2022 Cybersecurity Skills Gap," Fortinet, 2022.

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木7-7-7 Tri-Seven Roppongi 9階
www.fortinet.com/jp/contact

お問い合わせ

SB-k-FortiCNP-Manages-Risk-Through-Actionable-Insights-2211-R1