DATA SHEET

FortiCNP

提供形態：

クラウド

セキュリティリスクの優先度の設定

クラウドコンピューティングの採用の急拡大により、セキュリティチームは、増え続けるクラウドワークロードに対して十分なセキュリティを確保するため、リアクション型で作業を進めることを強いられています。このような状況では、すべてのセキュリティツールから発生する大量のアラートを処理することはできません。

クラウドネイティブの保護を提供するFortiCNPを利用することで、クラウド環境における広範囲のセキュリティシグナルに基づき、セキュリティリスクの優先度を設定することができます。FortiCNPは、CSPMとデータスキャン機能を内蔵し、脆弱性スキャン、権限の分析、脅威検知を提供する複数のクラウドネイティブのセキュリティサービスやフォーティネットのクラウドセキュリティ製品からの情報も収集します。

FortiCNPが収集したこれらの情報を利用して算出するクラウドリソースの総合リスクスコアを参考にすることで、FortiCNPから得られる実用的インテリジェンスに基づき、リスク管理作業を制御できます。

FortiCNPは、エージェントを必要とし、過剰な権限が付与され、管理不可能な量のデータが生成される従来型のCSPMやCWPPとは異なり、クラウドネイティブのセキュリティサービスや他のフォーティネット セキュリティ ファブリック製品との統合により、クラウドインフラストラクチャのセキュリティの詳細な可視性を提供し、セキュリティワークフローに優先度を設定することで、効果的なリスク管理を可能にします。

主なメリット

- クラウドリスク修復作業の特定、トリアージ、優先度の設定にかかる時間を短縮
- クラウドネイティブのセキュリティサービスの価値を最大化
- フォーティネットのクラウドセキュリティ製品の価値を最大化

主な機能と特長

- クラウドリスクの優先度の設定
- 脆弱性管理
- クラウドセキュリティポスチャ管理
- マルウェアスキャン
- クラウドネイティブセキュリティの統合
- ワークフローの統合

ハイライト

Resource Risk Insights（RRI）

Resource Risk Insights（RRI）は、大量のデータを実用的インテリジェンスに変換します。FortiCNP は、クラウドネイティブとフォーティネットの広範囲のセキュリティ製品からの情報を包括的なクラウドリスクグラフデータベースに相関付けることで、クラウド環境のリスクの相互依存性の最新かつ正確なマップを作成します。環境やワークロードに固有の属性に基づき、環境に合わせて RRI をカスタマイズすることができます。RRI のベースとなるのは、クラウドの構成、脆弱性、権限、アクセス可能なデータ、脅威、さらには、収集したデータの関連性を分析した情報です。

> *BK Bank の CTO である Caio Hyppolito 氏は、次のように述べています。「FortiCNP があれば、直感的なダッシュボードで包括的にクラウドを可視化し、リスク管理を継続的かつ容易に追跡できます。最も重要なのは、セキュリティに関して抽出された多種多様な情報の振り分けに時間をとられることなく、優先度の高いリソースの保護に集中できることです。導入済みの製品と統合すれば、さらに多くの価値がもたらされ、広範囲の可視化と容易かつプロアクティブなクラウドセキュリティ管理が可能になります。」*

マルウェアスキャン

FortiCNP のマルウェアスキャン機能は、Fortiguard Labs のマルウェアスキャンテクノロジーをクラウド環境のすべてのデータストアに活用することで、休眠状態のマルウェアの潜在的な影響からの保護を可能にします。マルウェアを事後に検知するエージェントを展開する必要があるランタイムのワークロードのスキャンとは異なり、FortiCNP は、クラウドデータストア、ディスクボリューム、ワークロードのイメージをスキャンすることで、データサプライチェーン全体のマルウェアを検知する機能を提供します [1]。

クラウドネイティブの統合

FortiCNP の RRI テクノロジーにより、クラウドプロバイダーのセキュリティサービスが提供する容易なシングルクリックによる導入の特長が失われることなく、関連する大量のアラートへの対応から解放されます。このモデルにより、エージェントの導入の面倒なプロセスが不要になり、クラウドネイティブのセキュリティサービスをシングルクリックで導入できます。FortiCNP のアクティベーションにより、これらのサービスからの情報の取得と関連付けが開始され、実用的インテリジェンスが提供されます。また、次のような統合サービスをご利用いただけます。

- 脆弱性評価サービス
- エンタイトルメント管理サービス
- 脅威検知サービス
- データスキャン / 分類サービス
- フォーティネット セキュリティ ファブリック（FortiGate、FortiWeb）

> *「複数のサードパーティツールをクラウドに導入することは、時として終わりのない面倒な作業が続きます。クラウドネイティブのツールを活用して出力の無駄をなくし、フォーティネットの他の製品から取得したセキュリティ情報と相関付けることで、時間を節約し、短時間で結果を出すことができます。」*

フォーティネット、CISO オフィスのセキュリティエンジニア、Roger Rustad

関連製品

以下のクラウドネイティブサービスは、FortiCNP のセキュリティ情報を提供することで、実用的インテリジェンスの精度を向上させます。

- Amazon GuardDuty
- Azure Security Center
- Amazon Inspector
- FortiGate-VM
- FortiWeb Cloud

詳細情報

詳細については、www.forticnp.com をご覧ください。

1. ディスクボリュームとワークロードのイメージスキャンについては、次期リリースで提供を開始する予定

技術仕様

主な機能		
	説明	**統合**
クラウドセキュリティポスチャ管理	FortiCNP は、お客様のクラウド構成をスキャンして監視することで、ベストプラクティスを評価し、構成ミスのリスクを検知します。	AWS Security Hub Azure Security Center GCP Security Health Analytics
脆弱性管理	FortiCNP は、クラウドリソースに対する脆弱性の影響を分析することで、リスクを評価します。	Amazon Inspector Microsoft Defender for Cloud
脅威検知	FortiCNP は、クラウドネイティブのセキュリティサービスやフォーティネット製品から情報を取り込み、ワークロードやネットワークの脅威検知情報を取得します。	Amazon GuardDuty、VPC Flow Logs、CloudTrail Microsoft Defender for Cloud、NSG Flow Logs、Log Analytics Google VPC Flow Logs、Cloud Logs
エンタイトルメント管理	FortiCNP は、権限情報を取得することで、異なるリソースのリスクの影響を相関付けることができます。	
データのセキュリティ	FortiCNP は、データに含まれるマルウェアをスキャンし、クラウドネイティブツールのデータ分類情報を利用して、データに対するセキュリティリスクやデータに含まれるセキュリティリスクの影響を評価します。	Amazon S3 Azure Blob GCP Cloud Storage
Kubernetes セキュリティ	FortiCNP は、Kubernetes 環境との統合により、構成をスキャンし、トラフィックフローを監視します。	Amazon EKS Azure AKS Google Kubernetes Engine Self-Managed Kubernetes
コンテナレジストリ	FortiCNP は、コンテナレジストリの脆弱性をスキャンします。DevOps チームは、ビルドパイプラインの合否をスキャン結果に基づいて判断することができます。	Amazon ECR Azure Container Registry Google Container Registry Harbor Container Registry OpenShift Container Registry Docker Hub
チケット管理と CI/CD の統合	FortiCNP を利用することで、セキュリティアナリストは、組織にとって最も自然な方法で他のチームとやり取りすることができます。	JIRA ServiceNow Jenkins
レポート	FortiCNP は FortiCNP を利用しないユーザーに対し、現在のリスクのスナップショットやコンプライアンスレポートを提供します。	

AWS のサービス	**統合内容**
Resource API	AWS Resource API を使用して、クラウドリソースに関する情報を読み取り専用で収集します。
Organizations	AWS Organizations を使用して、複数の AWS アカウントが含まれる、AWS Organizations の機能を使用して編成された環境をインポートします。
CloudTrail	FortiCNP は、CloudTrail イベントを取り込むことで、お客様の環境の変化を特定します。
VPC Flow Logs	VPC Flow Logs を使用して、お客様の環境のトラフィックパターンを確立し、正常なパターンからの逸脱を検出します。
Security Hub	AWS Security Hub を使用して、GuardDuty や Inspector などの AWS サービスからあらゆるセキュリティ情報を収集します。FortiCNP は、Security Hub の情報の正規化と集計の機能を利用します。Security Hub コントロールは、FortiCNP では使用されません。
GuardDuty	FortiCNP は、GuardDuty 脅威検知サービスを使用して、リスクを切迫した脅威に相互付け、優先度を設定します。
Inspector	Inspector Vulnerabilities を使用して、パッケージ、ライブラリ、ネットワーク構成の脆弱性リスクを確立します。

技術仕様

主な機能	
Azure のサービス	**統合内容**
REST API	Azure REST API を使用して、クラウドリソースに関する情報を読み取り専用で収集します。
Azure Log Analytics	Azure Log Analytics を使用して、Azure プラットフォームからの情報を収集し、リソース構成に対する変更を検知します。
Azure NSG Flow Logs	NSG Flow Logs を使用して、お客様の環境のトラフィックパターンを確立し、正常なパターンからの逸脱を検知します。
Azure Security Center	Azure Security Center は、Microsoft Defender からの情報を FortiCNP に提供することで、クラウドワークロードの脆弱性と脅威の検知を可能にします。
GCP	**統合内容**
Google Cloud API	GCP API を使用して、クラウドリソースに関する情報を読み取り専用で収集します。
GCP VPC Flow Logs	VPC Flow Logs を使用して、お客様の環境のトラフィックパターンを確立し、正常なパターンからの逸脱を検出します。
Google Cloud Logs	Cloud Logs を使用して、GCP から情報を収集し、リソース構成に対する変更を検知します。

オーダー情報

PRODUCT	DESCRIPTION
BRING YOUR OWN LICENSE (BYOL)	
Cloud Native Protection	FortiCNP Cloud Native protection – Risk, Threat and Data insights for 20 resources in all supported public cloud environments.
	FortiCNP Cloud Native protection – Risk, Threat and Data insights for 100 resources in all supported public cloud environments.
Data Protection	FortiCNP Data Protection Standard. License for malware and anti-virus scanning of 100GB of data. Requires FortiCNP protected resource license. Cannot be combined with FortiCNP Data Protection, Advanced.
	FortiCNP Data Protection Advanced (Standard plus DLP scanning) - License for pattern-matching (DLP), malware and anti-virus scanning of 100GB of data. Requires FortiCNP protected resource license. Cannot be combined with FortiCNP Data Protection, Standard.
	FortiCNP Data Protection Standard. License for malware and anti-virus scanning of 1TB of data. Requires FortiCNP protected resource license. Cannot be combined with FortiCNP Data Protection, Advanced.
	FortiCNP Data Protection Advanced (Standard plus DLP scanning) – License for pattern-matching (DLP), malware and anti-virus scanning of 1TB of data. Requires FortiCNP protected resource license. Cannot be combined with FortiCNP Data Protection, Standard.
Container Protection	FortiCNP Container Protection. Subscription per 4 container hosts/worker nodes.
AWS MARKETPLACE	
Monthly	Minimal subscription protecting 20 workloads and scans up-to 100GB of data for malware.
	Additional protected resources that were protected during the month using highest watermark metering. Increments of 1.
	Volume of data that has been scanned for the month beyond the first 100GB. Increments of 1.
Annual	Minimal subscription protecting 100 workloads and scans up to 1TB of data for malware.
	Allocation of additional protected resources for the year. Increments of 100.
	Volume of data scanning capacity beyond the first 1TB. Increments of 10TB.
	Any exceeded capacity for protected workloads or data scanning charged per monthly prices.

* Denotes TBA

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