VARMOUR DSS
分散セキュリティシステム

vARMOUR

マルチクラウド環境での可視化・解析と制御

仮想化、さらにはマルチクラウドの出現により、重要なデータへのアクセスが様々な形でできるようになっています。コンシューマデバイスが激増し、ビジネスパートナー間の連携が進むと、従来のペリメーターには多くの通信路が設けられます。明確な境界の概念はなくなり、境界の保護を目的とするセキュリティ制御はただの時代遅れなものとなってしまうのです。既存のツールは、物理ネットワーク以外の監視には適合していないため、トラフィックの可視性の欠如が問題になります。ワークロードを動的に追跡でき、シンプルかつ優れた、そして広範囲を保護するセキュリティ制御が求められています。

vArmourのソリューション

vArmour DSS分散セキュリティシステムは、こうしたセキュリティ問題を解決するvArmourの特許であるアプリケーションを認識したマイクロセグメンテーションと高度なセキュリティ分析機能を、業界初の分散セキュリティシステムで提供します。vArmour DSSは、個々のワークロードの監視と制御をインフラ全体に対して適用するように設計された、拡張性の高いソフトウェアソリューションであり、ワークロードの常駐場所を問わず、すべてのワークロードをきめ細かに保護します。

vARMOUR DSSの機能

ネットワークの可視化

すべてのワークロードがおこなう通信について、きめ細かなアプリケーション・レイヤーの可視化を同一ハイパーバイザー内であっても可能にします。従来の境界セキュリティソリューションでは実現できない機能です。

マイクロセグメンテーション

セキュリティーポリシーに従い、ネットワークレイヤーの境界とは別にワークロードとアプリケーション通信をセグメント化します。きめ細かいアクセス制御で攻撃対象になるリソースを限定し、基準情報資産や個人情報の保護、ネットワークを使ったマルウェアの二次感染などを防ぎます。

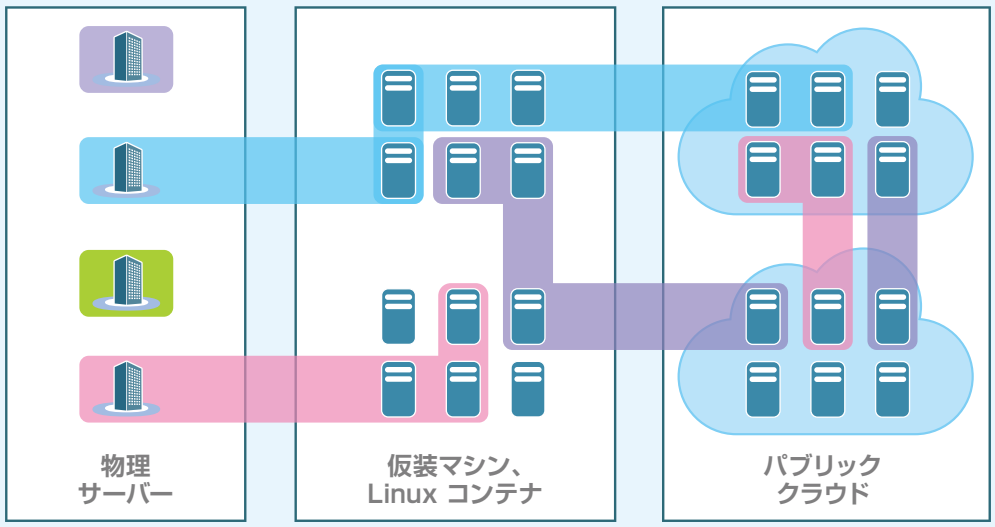
コンプライアンス保証

データアクセスをユーザーやプリケーション毎に制御し、各種の業界が定めるコンプライアンス要件に準拠します。

迅速な侵害検知とフォレンジック調査

セキュリティインテリジェンスを集め、攻撃の対象になっているマシン、システムおよびリソースを迅速に特定して異常または悪意のある活動を検知します。フォレンジック調査時間を日単位から分単位に大幅に短縮して、ワークロードを体系的に隔離することができます。

■ プラットフォームを問わず、アプリケーションレベルのセグメンテーション



VARMOUR DSS
分散セキュリティシステム

vARMOUR

特 徴

高度に拡張可能な分散アーキテクチャ

vArmour DSSは、完全なソフトウェア・ソリューションである為、サーバーの追加と共にスケール・アウトすることが可能です。ハードウェア・アプライアンスを追加する必要はありません。

きめ細かいマイクロセグメンテーションを簡単導入

vArmourアプリケーションのマイクロセグメンテーションは、複雑なネットワークオーバーレイ、サービスチェーニング、リソース集約型コンポーネントを必要とせず、3つの簡単な手順で、30分以内で導入できます。

単一システムから悪意ある挙動検知して防御

素早く移動する最新の攻撃に迅速に対抗するには、可視化と検知のソリューションだけでは一般に不十分です。vArmour DSSは、脅威を発見し、現在の脅威の拡散を防止し、セキュリティを侵害されたシステムからの新たな攻撃や感染拡大を阻止できる単一の統合システムです。

広範なプラットフォームをサポート

VMware、Nutanix、Kubernetes（Linux コンテナ）のような仮想システムや、仮想化が不可能である物理サーバーのレガシー・システムを含むオンプレミス環境のほか、Amazon Webサービス等のオフプレミス環境もサポート対象です。vArmour DSSのセキュリティポリシーは、vMotionなどのライブマイグレーションをネイティブにサポートし、アプリケーションを中断することなくワークロードを追跡します。

インフラ全体の簡単運用

vArmour DSSでは、インフラストラクチャ全体に関するポリシー管理や制御機能を一元的に行うことができます。セキュリティポリシーは、新しいアプリケーションやワークロードに対して自動的に適用されるため、新しいワークロードを追加する際に手動で作成する必要がなくなります。JSON/REST APIによる制御にも対応しており、サードパーティのオーケストレーションおよび自動化システムとシームレスに統合することができます。

偽装サーバー（Deception Technology）

従来の Honeypot（ハニーポット）技術では守備範囲が限られる事と、不正アクセスと思われるトラフィックをハニーポットに誘導することが不可能でした。vArmourのDeceptionテクノロジーでは、vArmourのファブリック内で発生した「怪しいトラフィック」を 偽装サーバーにリダイレクトし、その後の行動を監視と制御することが可能です。IDS/IPSに比較して誤検知が低く、アタッカーの攻撃が始まる前に対応をすることが出来ます。

vArmour Analytics

vArmour Fabricが収集したすべてのワークロードトラフィックを可視化するソリューションです。これらのトラフィックパターンを解析することで、疑わしい潜在的な脅威の検知とアラートの送信を行います。vArmour Analyticsを利用することで、アプリケーションまたはワークロードの予期しない挙動を把握して、適切なポリシーの変更を実施することができます。

- エンド・ツー・エンドの可視化を目的として、ネットワーク、アプリケーション、ワークロードおよびユーザー全体の継続的な監視。
- 通信の傾向を分析し、データセンター全体のセキュリティ状態を判別します。
- ネットワークトラフィックの詳細調査、迅速な対応が可能です。

vARMOURについて

カリフォルニア州、マウンテンビューに本社を置くvArmourは、高度なセキュリティ分析とアプリケーションを認識したマイクロセグメンテーションを提供するデータセンターセキュリティ業界のリーダー企業です。2011年に設立し主要なベンチャーキャピタルと豪州通信最大手のテルストラ社からの支援を受けています。vArmour分散セキュリティシステムは、世界最大級の銀行、通信サービスプロバイダー、政府機関、医療関連企業、小売業者など多数に採用され、AmazonやVMwareなどのパートナーと連携し、世界各地で多数の大規模データセンターやクラウド環境のセキュリティを保護しています。

詳細は、http://www.varmour.com/japan をご覧ください

お問い合わせは下記にご連絡ください

vARMOUR

ヴイアーマーネットワークス合同会社
〒100-0004 東京都千代田区大手町1-5-1 大手町ファーストスクエア イーストタワー4階
TEL：03-5219-1480　E-mail：info-japan@varmour.com