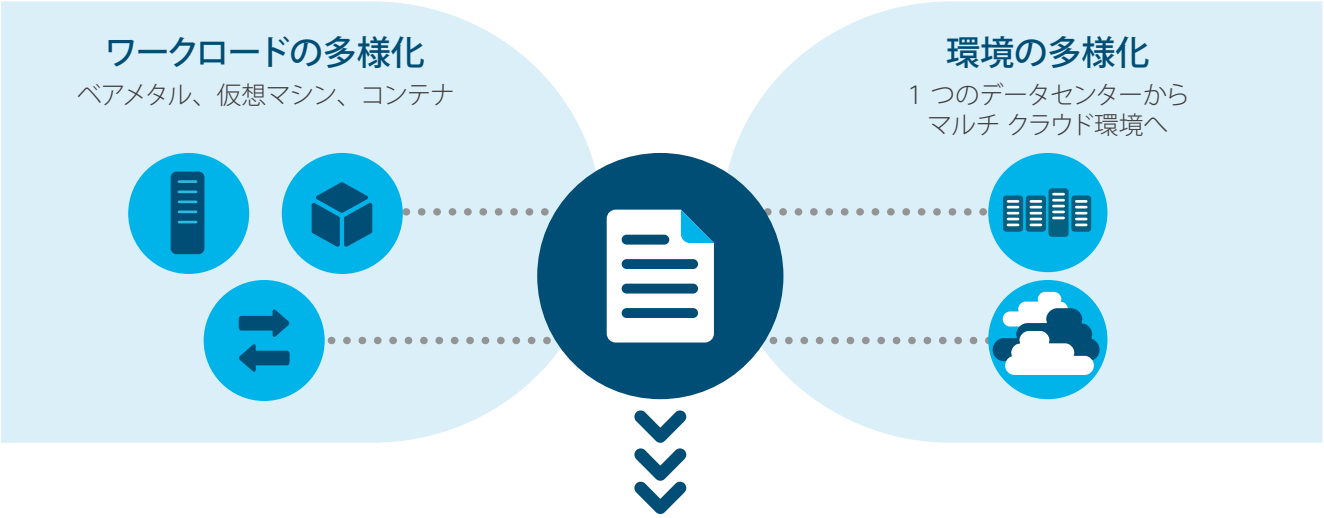
Cisco Secure Workload
(旧 Cisco Tetration)

データセンターのワークロードを保護する
新しいアプローチのセキュリティを実現

ハイブリッド クラウドのワークロードを俊敏性を損なわずに保護するには

アプリケーションの分散によって攻撃対象領域は拡大している

現在、デジタル ビジネスの根幹をなすアプリケーションの多くはモジュラ型の構成となり、複数のクラウド プラットフォームやオンプレミス環境を組み合わせたハイブリッド クラウド、マルチ クラウド環境で利用されています。その運用と管理を担う IT 部門の担当者にとって、デジタル ビジネスならではの俊敏性を維持しながら、ハイブリッド クラウド環境全体でアプリケーションを確実に保護することは大きな課題です。



主要な課題

アプリケーションの状況をもれなく把握する

すべてのアプリケーションを正常な状態に保ち、保護するには、分散して実行されているすべてのアプリケーションのマップが必要です。実行中のサービスとその相互依存の関係を、あらかじめ把握しておくことが求められます。

攻撃の対象となる領域をできるだけ少なくする

アプリケーションが複数の環境（インフラストラクチャ）上で稼働し、その構成やワークロードがダイナミックに変化するということは、攻撃の対象となる領域の拡大を意味します。従来の静的なセキュリティ ポリシーでは、十分な保護は実現できません。そこで、既知の必要な通信のみを許可し、それ以外をすべてブロックするセグメンテーションを基本とした対策の重要性が増しています。

脆弱性や異常なふるまいを早期に特定する

攻撃を受けたセキュリティ脆弱性の大半は、既知のソフトウェア脆弱性であるとされています。そうした脆弱性の特定と修復を速やかに行うことは不可欠です。また、ワークロードの異常や疑わしいふるまいを早期に特定できるようにするには、正常な状態を把握し、ベースライン化しておくことが重要となります。

今すぐ達成すべき 3 つの重要なセキュリティ戦略

自動化によって異常や脆弱性を迅速に検出

可視性

ユーザ、デバイス、ネットワーク、アプリケーション、ワークロード、プロセスを完全に可視化

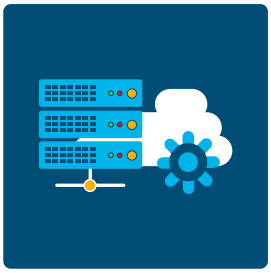
セグメンテーション

マイクロ セグメンテーションとアプリケーションのホワイトリスト化により、攻撃者のサーバ間移動を防止

脅威からの保護

マルチレイヤ脅威センサーで侵害をすばやく特定し、すばやく検出、ブロックして、データの盗難やサービスの中断を回避

その実現に必要なこと



アプリケーション通信の制御

ハイブリッド クラウド全体で効率的なセグメンテーションを実現

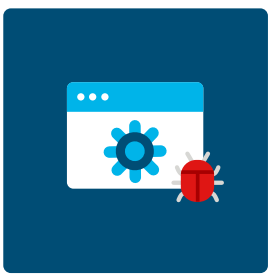
- 一貫性のあるポリシーに基づきセグメンテーション適用
- アプリケーションの振る舞いに基づいて、ホワイトリスト ポリシーを最新の状態に保つ
- ポリシーの遵守を自動的に追跡
- アプリケーションの振る舞いに異常がある場合、速やかに通知

アプリケーションの振る舞いの検出

プロセスの振る舞いの偏差（逸脱）を把握し、異常や不正行為を迅速に特定

【参照する項目の例】

- プロセス ハッシュ、系列、属性
- 特権昇格
- サイド チャネル攻撃
- ファイル アクセス
- シェル コードの実行
- Raw ソケット　など



脆弱性の検出

共通脆弱性識別子（CVE、Common Vulnerabilities and Exposures）を認識したら、直ちに攻撃対象領域を削減

- インストールされているソフトウェア パッケージとバージョンの情報をベースライン化
- インストールされているソフトウェア パッケージに関連する CVE を追跡
- 脆弱性の重大性を特定
- アクセスの制限やワークロードの検疫など各種措置を実施

Cisco Secure Workload による ハイブリッド クラウドのワークロード保護

ワークロードの種類や場所を問わない ライフサイクル全体のセキュリティ対策

Cisco Secure Workload ソリューションは、振る舞いのベースライン化と分析、ホワイトリスト ベースのアプリケーション セグメンテーションなどによって、ハイブリッド クラウド/マルチ クラウドにおける一貫性のあるワークロード保護を実現します。通常とは異なるプロセスの振る舞いの迅速な特定、脆弱性の検出と修復、そして攻撃者のサーバ間（水平方向の）移動を阻止することで攻撃対象領域を縮小します。また、ネットワークのパフォーマンス情報や、データセンター規模のテレメトリ情報をリアルタイムに取得、保持して、より的確で速やかな対応を持続的に支援します。

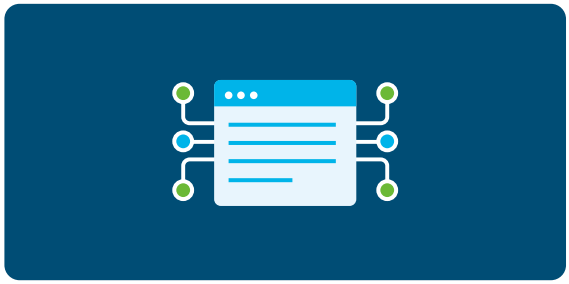
Cisco Secure Workload で実現できること

異常の検出

実行中のプロセスの振る舞いを基準としてベースライン化し、その偏差（逸脱）を使用することでアプリケーションの異常を数分で識別、特定します。

攻撃対象領域の削減

既知の脆弱性を検出して修復作業を定義します。事前対策として影響を受けるサーバを検疫し、脆弱性を排除することで、攻撃の対象となる領域を最大 85% 縮小します。



自動化されたゼロトラスト セキュリティ

自動化によってマニュアル作業を 70% 削減し、ゼロトラスト モデルの構築を支援します。効率的なセグメンテーションを使用して、脆弱性のあるアプリケーションのサーバ間（水平方向）の移動を最小化します。

一貫性のある保護

オンプレミス、プライベート クラウド、およびパブリック クラウドに存在するデータセンター全体で一貫性のあるワークロード保護を実現します。ベア メタル、仮想、およびコンテナ化されたワークロードのすべてに対応します。

Cisco Secure Workload のアーキテクチャ

データ収集	データ保存と解析	洞察から行動へ
すべての通信パケット サーバ プロセス情報、振る舞い	ビッグデータ基盤 機械学習	

サーバ用ソフトウェア センサー
Windows/Linux/コンテナ
IBM z Systems/VDI　など

その他センサー
ERSPAN センサー/Netflow センサー
Cisco AnyConnect　など

Cisco Secure Workload

アプリケーション可視化

- アプリケーション依存関係の可視化
- ネットワークの保護
- DC/ネットワーク移行の迅速化

ワークロード保護

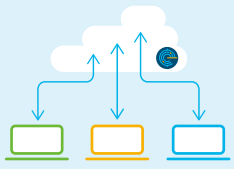
- 通信のホワイトリスト保護
- サーバ ソフトウェアの脆弱性管理
- プロセスの異常な振る舞い検知

展開モデル（導入オプション）

すべてのモデルは、オンプレミス、パブリック/プライベート クラウド上のワークロード可視化を実現

Cisco Secure Workload アプライアンス
（Cisco Secure Workload、Cisco Secure Workload-M）

- 物理アプライアンス型
- 数ヵ月から数年単位でのデータ保持
- Cisco Secure Workload では、ワークロード数 25,000 まで拡張可能（VM/ベアメタル）
- Cisco Secure Workload-M では、ワークロード数 5,000 まで拡張可能（VM/ベアメタル）



Cisco Secure Workload-SaaS

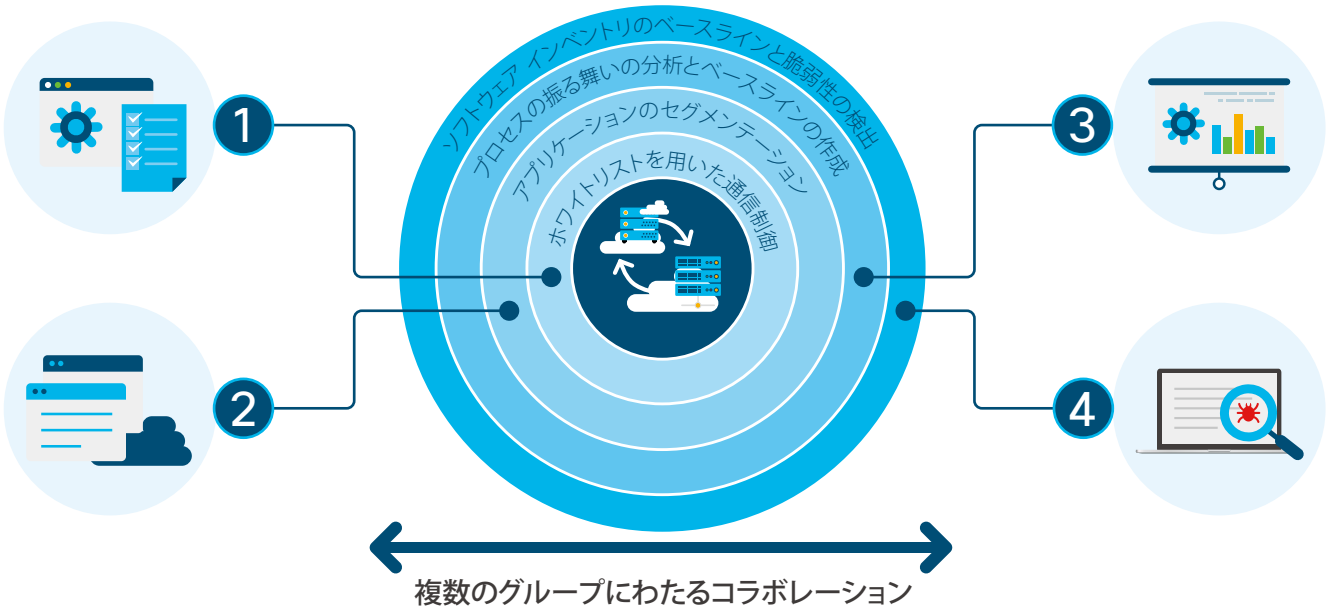
- Software as a Service 型
- オンプレミスのハードウェア管理を必要としないワークロード保護機能を実現
- 迅速なオンボーディングにより、メリットを短期間で獲得やスモールスタート可能
- 最大 25,000 ワークロードまで拡張可能
- データ保持：月単位

※データ保持期間は可視化対象数、実際の通信量により異なります

インフラストラクチャに依存しない 4 層のセキュリティ

クラウド間のワークロード全体を保護

アプリケーションは異なる環境（インフラストラクチャ）にダイナミックに分散して運用され、その複雑さはますます進んでいます。Cisco Secure Workload はインフラストラクチャに依存しない 4 層のセキュリティで、ハイブリッド クラウドやマルチ クラウド上のワークロード全体を保護することができます。これにより、アプリケーションという資産を守り、また日々の安全な利用を支えます。



1 ホワイトリストを用いた通信制御

Cisco Secure Workload は、きめ細かなホワイトリスト ポリシーを自動的に生成し、アプリケーションの状況に合わせてポリシーを最新の状態に保ちます。IT 部門は、ホワイトリスト ポリシーを使用してアプリケーションの通信を制御できます。

2 アプリケーションのセグメンテーション

Cisco Secure Workload は、単一のホワイトリスト ポリシーで通信のセキュリティ管理を一元化することができます。そうしたポリシーのきめ細かな適用によって、インフラストラクチャの種類に関係なく一貫性のあるアプリケーション セグメンテーションを実現します。ベア メタル、仮想化、コンテナ環境であるかどうかや、ワークロードの実行がオンプレミス、パブリック クラウド、プライベート クラウドのどこであるかは問いません。

3 プロセスの振る舞いの分析とベースラインの作成

Cisco Secure Workload は、稼働するプロセスの状態をベースライン化し（プロセスのハッシュ化を含みます）、振る舞い分析などの統計モデルを適用して振る舞いの偏差（逸脱）を特定します。このアプローチでは、問題を早期に特定して必要な是正措置を支援します。

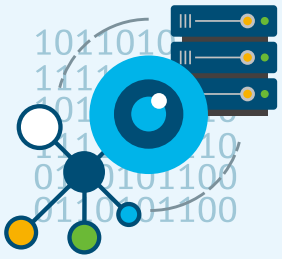
4 ソフトウェア インベントリのベースラインと脆弱性の検出

Cisco Secure Workload は、サーバにインストールされているソフトウェア パッケージとバージョンの正確なインベントリを作成し、関連する高リスクの脆弱性を特定します。それを基に、脆弱なワークロードに関するポリシーを定義します。

シスコの差別化要因

Cisco Secure Workload は、ネットワークとワークロードの両方をモニタリング、分析し、柔軟な属性情報を主体としたセキュリティ ポリシー管理を提供する唯一のプラットフォームです。

- ワークロードに対するすべての通信（パケット、フロー）をリアルタイムで分析し、アプリケーション セグメンテーションを自動化します。
- ハイブリッド クラウド、マルチ クラウドで利用される多数のアプリケーションに対して、きめ細かなホワイトリスト ポリシーを適用することができます。
- ネットワークおよびワークロードの情報を長期間保持し、詳細な調査に利用できます。
- Cisco Secure Workload は、シスコのセキュリティ ポートフォリオと連動でき、包括的で全社規模のセキュリティを実現します。



導入事例

Automatic Data Processing（ADP）

業　種 人事、給与、福利厚生システムの アウトソーシング サービス

本部所在地 米国 ニュージャージー州ローズランド

課題

- アプリケーション動作を把握し、全体にセキュリティ統制を利かすことが困難
- 従来のファイアウォールによる集中制御は非現実的
- ハイブリッド クラウド全体を統制可能なセキュリティ管理モデルの実現

ソリューション

- アプリケーションの可視化により、ホワイトリスト ルールの作成を自動化
- サーバでのホワイトリスト強制によるネットワーク保護

結果

- 14 のデータセンターとパブリック クラウドに存在する数万台のサーバの、通信の可視化とマイクロ セグメンテーションを実現
- サーバの保護ポリシーの一元管理と、サーバでのホワイトリスト強制によるゼロトラスト モデルの実践
- マルチ クラウド環境の管理を一元化

First National Bank（FNB）

規　模 従業員数 44,000 名

業　種 金融サービス

本部所在地 南アフリカ ヨハネスブルグ

課題

- データセンターの可視性の向上
- 問題の特定とトラブルシューティングの改善
- 永続的で多面的なサイバー攻撃に対する防御

ソリューション

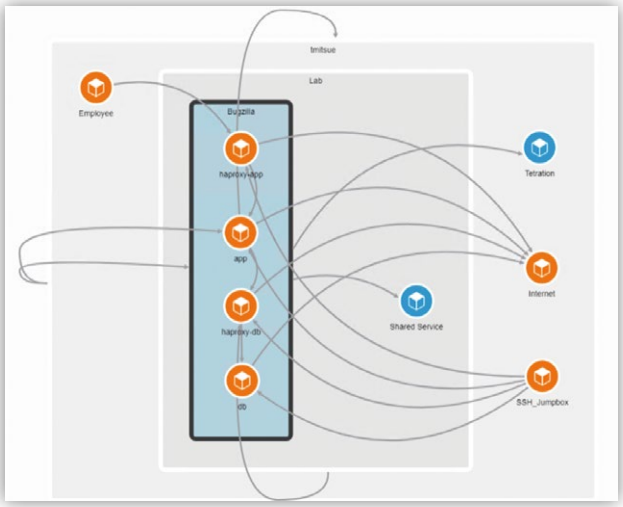
- アプリケーションの接続性と依存関係のマッピング
- コアからエッジまで、統合された多層セキュリティ
- アプリケーション中心の software-defined ネットワーク

結果

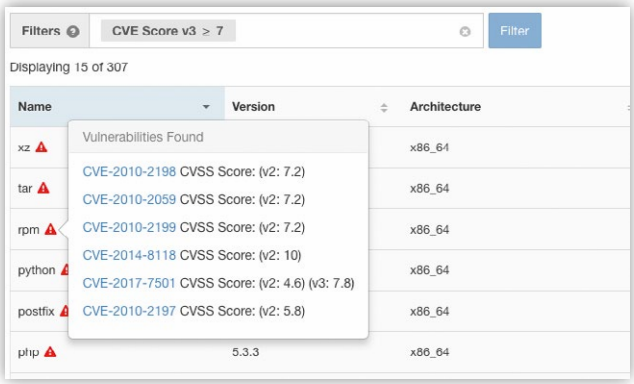
- アプリケーションの接続性、依存関係、およびデータフローの詳細な可視化を達成
- 問題の解決を数十時間から数分に短縮
- マルウェア感染率を 9% から 0.1% に減少

Cisco Secure Workload 運用イメージ

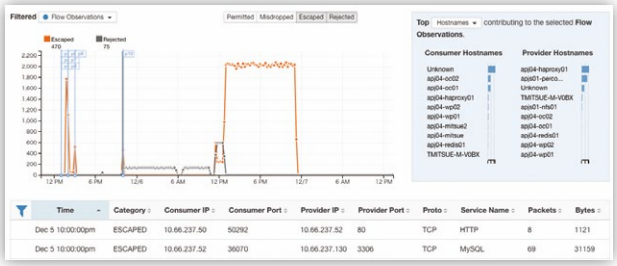
アプリケーションの依存関係を可視化



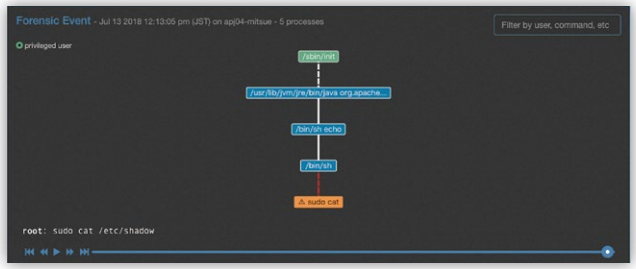
サーバの脆弱性を把握



ポリシー違反通信の検知



疑わしいプロセス証跡を記録



最新情報はこちら www.cisco.com/jp/go/cisco-secure-workload

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

お問い合せ先

2037-2110-000-F