AKAMAI 製品概要

Akamai Guardicore Segmentation

きめ細かな可視性とマイクロセグメンテーションコントロールにより、ラテラルムーブメント（横方向の移動）を阻止

エンタープライズの IT インフラは、プラットフォームとアプリケーションの導入モデルが混在しており、従来型のオンプレミスデータセンターからクラウドやハイブリッドクラウドのアーキテクチャに進化している途上にあります。このデジタルトランスフォーメーションは、ビジネスのアジリティ向上、インフラコストの削減、テレワークの実現という点で多くの企業の役に立っていますが、境界が明確に定義されず、アタックサーフェスが拡大して複雑になる原因でもあります。個別のサーバー、仮想マシン、クラウドインスタンス、エンドポイントはそれぞれデータ漏洩のポイントとなる可能性があります。ランサムウェアやゼロデイ脆弱性などの脅威が広がる現状では、攻撃者が侵入手段を見つけることは必然で、横方向に移動して価値の高いターゲットを目指しやすくなります。

Akamai Guardicore Segmentation は、ネットワーク内でゼロトラストの原則を適用するための非常にシンプルで高速、かつ直感的な方法を提供します。IT 環境内のアクティビティを可視化し、正確なマイクロセグメンテーションポリシーを実装し、潜在的なセキュリティ侵害を迅速に検知することで、ラテラルムーブメントを阻止します。

ソリューションの主な機能

AI を活用したきめ細かなセグメンテーション

AI の推奨事項、ランサムウェアなどの一般的なユースケースを修復するためのテンプレートや、プロセス、ユーザー、ドメイン名などの正確なワークロード属性を使用して、数回クリックするだけでポリシーを実装可能

リアルタイムと履歴での可視性

アプリケーションの依存関係をユーザーレベルとプロセスレベルまで、リアルタイムまたは履歴ベースでマッピング

幅広いプラットフォームのサポート

ベアメタルサーバー、仮想マシン、コンテナ、IoT、クラウドインスタンスにわたる最新および従来のオペレーティングシステムに対応

柔軟な方法による資産のラベル付け

可視性と適用のためにラベル付けの階層をカスタマイズでき、また自動ラベリングのためにオーケストレーションツールや設定管理データベースと統合でき、豊富なコンテキストを追加

多様な保護方法

脅威インテリジェンス、防御、セキュリティ侵害検知の機能と連携して、インシデント対応時間を短縮

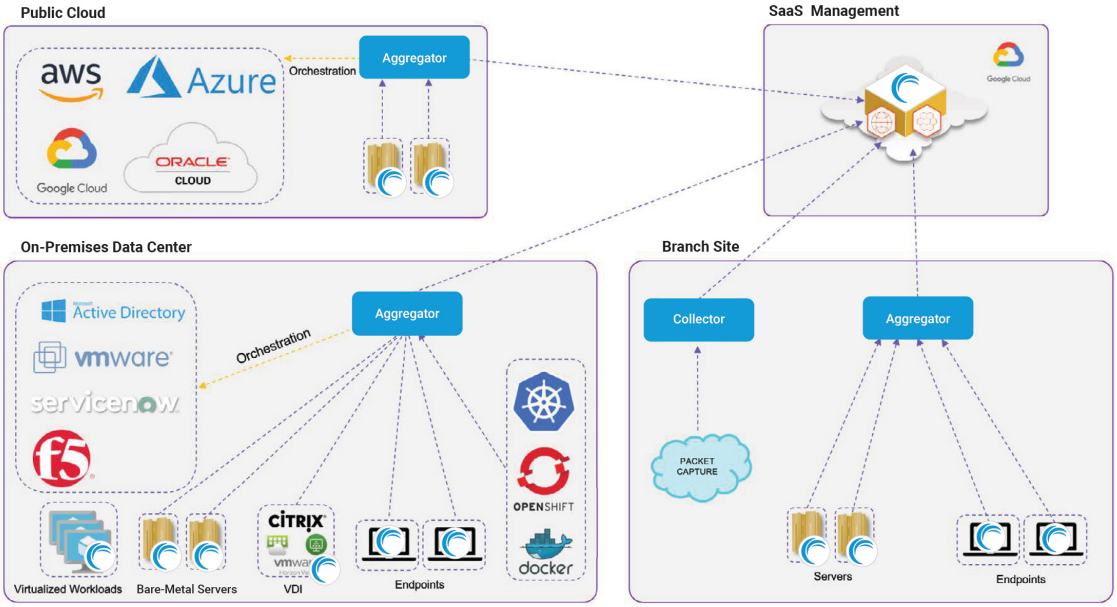
ビジネス上のメリット

- ランサムウェアの阻止
- ゼロトラストの実現
- コンプライアンスの促進
- 重要なアプリケーションをリングフェンシング
- セキュアなクラウド移行
- テレワーカーの保護
- エンドポイントの保護
- 内部ファイアウォールを超えて移動

仕組み

Akamai Guardicore Segmentation は、エージェントベースのセンサー、ネットワークベースのデータコレクター、クラウドプロバイダーからの仮想プライベートクラウドのフローログ、エージェントレス機能を有効にする統合を組み合わせて、企業の IT インフラに関する詳細な情報を収集します。高度に自動化された柔軟なラベル付けプロセスを通じて（オーケストレーションシステムや設定管理データベースなど、既存のデータソースとの統合を含む）、関連するコンテキストを情報に追加します。

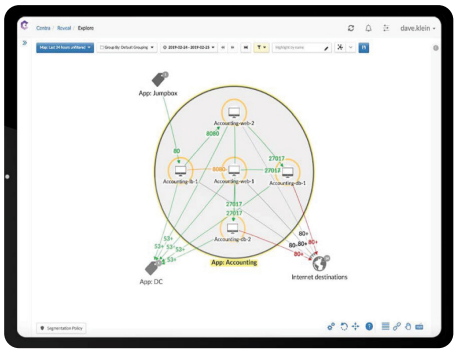
インフラのトポロジー



ほとんどのお客様は SaaS 管理を利用されていますが、
オンプレミスの管理オプションもご利用いただけます。

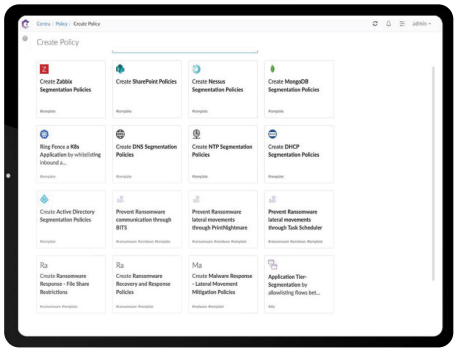
ネットワークマップ

IT インフラ全体の動的なマップを出力したものです。セキュリティチームは、これを使用して、ユーザーレベルとプロセスレベルの粒度でアクティビティをリアルタイムまたは履歴で表示できます。これらの詳細な知見と AI ベースのポリシーワークフローを組み合わせることで、セグメンテーションポリシーを実際のワークロードコンテキストに基づいて、迅速かつ直感的に作成できます。



テンプレート

事前に構築されている最も一般的なユースケース用のテンプレートを使用して、ポリシーを簡単に作成できます。ポリシーの適用は基盤となるインフラから完全に分離されるため、複雑なネットワークの変更やダウンタイムの影響を受けることなく、セキュリティポリシーの作成や変更ができます。さらに、ポリシーは、オンプレミスのデータセンターやパブリッククラウド環境といったワークロードの場所に関係なく適用されます。Akamai のセグメンテーション機能は、高度な脅威防御機能とセキュリティ侵害検知機能、および Akamai Hunt が提供するマネージド型脅威ハンティングサービスによって補完されます。



大規模で包括的な保護

あらゆる環境

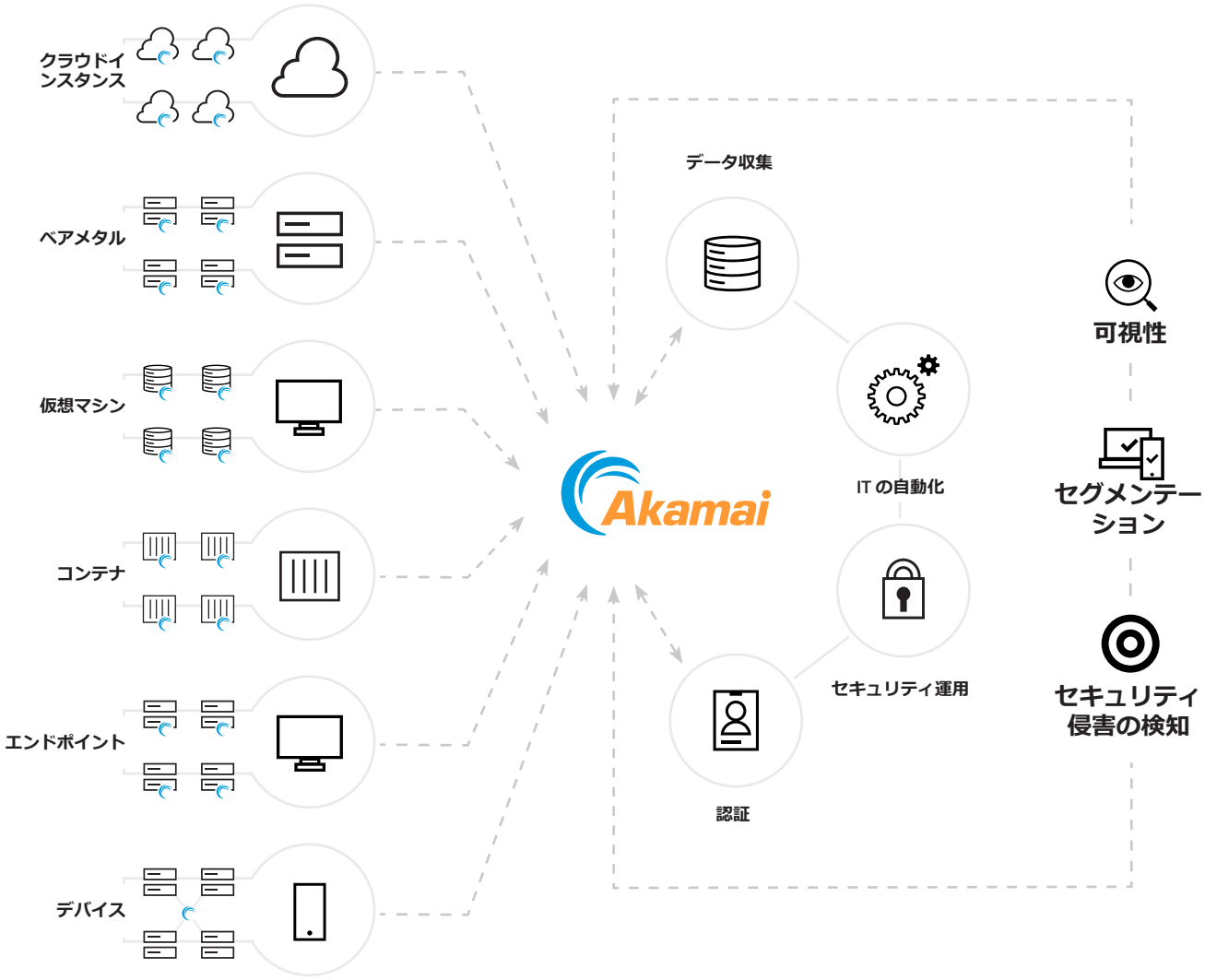
オンプレミスのワークロード、仮想マシン、レガシーシステム、コンテナとオーケストレーション、パブリック／プライベートクラウドのインスタンス、IoT ／ OT が混在した複雑な IT 環境を保護

セキュリティのシンプル化

単一のプラットフォームでネットワークの可視性、セグメンテーション、脅威防御、セキュリティ侵害検知の機能、ガイドに従ったポリシー適用を提供し、セキュリティ管理をシンプル化してゼロトラスト・イニシアチブを実現

エンタープライズのスケーラビリティとパフォーマンス

最初は最重要デジタル資産を集中的に保護し、続いて複雑さ、インフラの変更、パフォーマンスのボトルネックの影響を受けることなく、スケールアップしてエンタープライズ全体を保護



サポートされるプラットフォームとテクノロジー

- Akamai Guardicore Segmentation は、お客様の既存インフラと統合できるように設計されています。
- お客様のニーズに応じて OS のサポートを継続的に拡張しています。
- 当社の統合の一覧については、テクノロジーパートナーのページをご覧ください。

オペレーティングシステム

Linux

Apple

Microsoft

Unix

パブリック・クラウド・プロバイダー

ハイパーバイザー

ハイパービジョンオーケストレーション

セキュリティゲートウェイ

コンテナオーケストレーションとエンジン

Web コンソール用のブラウザー

メモリとシステムの最小要件

Management Server
32 GB RAM, 8 vCPUs, 530 GB

Aggregator
4 GB RAM, 4 vCPUs, 30 GB

Deception Server
32 GB RAM, 8 vCPUs, 100 GB

ESC Collector
2 GB RAM, 2 vCPUs, 30 GB

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API

Akamai Guardicore Segmentation の詳細、またはパーソナライズされた製品デモのご依頼については、akamai.com/guardicore をご覧ください。

 | サポート | | 公開日：2023 年 7 月