セールスツール

効果の大きいセグメンテーションのためのサービス

Akamai でセキュリティの複雑さとリスクを軽減

はじめに

オンプレミスのデータセンターとパブリッククラウド環境全体にわたって重要な資産を保護することがこれまで以上に重要になっています。そのためには、脅威の状況が急速に変化する中で、新しいアプリケーション展開モデルに遅れをとることなく対応できる専門知識がますます必要になります。当社のサービスエキスパートは、Akamai のセキュリティポートフォリオへの投資を具体的なビジネス主導の成果につなげることに重点を置いています。

Akamai のマイクロセグメンテーション・サービス・チームは、民間企業と軍関係の情報機関両方での豊富なトレーニングや実体験を有するセキュリティエキスパートで構成されています。Akamai の柔軟なサービス提供により、この専門知識を社内の IT チームやセキュリティチームの延長として利用し、データセンターからクラウドまで、最高レベルのセキュリティを実装することができます。

カスタマージャーニー

通常、カスタマージャーニーは、Akamai の Professional Services Delivery による展開と設定から始まります。Akamai がお客様の環境の設定を行い、資産やラベルを定義し、最初のいくつかのユースケースについてポリシーを実装します。

その後、そのソリューションを使用するチームメンバーの一部に管理およびエンジニアリングのトレーニングを提供します。

さらに、Day-2 Operation Services を利用して、展開の継続と強化（より多くの資産やラベルの定義、追加のユースケースに対するポリシーの実装）や、セキュリティインシデントの処理とセキュリティ対策の改善、監査に必要な制御とレポートの提供、お客様のインフラとの統合を改善するためのカスタム開発の提供を行うことができます。

ソリューションのライフサイクルを通じて、発生する可能性のあるあらゆる問題の解決を広範なサポートサービスで支援し、お客様が Akamai 製品の価値を最大限に引き出せるように、当社のカスタマー・サクセス・チームがお手伝いします。

Akamai マイクロセグメンテーションサービスによるカスタマージャーニー

カスタマーサクセス
お客様が Akamai 製品の価値を最大限に引き出せるよう支援

Professional Services Delivery
製品の展開、最初のユースケースの実装

トレーニング
綿密なトレーニングおよび認定プログラム

Day-2 Operation Services
資産／ラベル／ポリシーの継続的な維持と拡大

セキュリティ体制の見直しと IR、監査準備、カスタムの開発および統合

Technical Account Manager ／ Resident Engineer

カスタマー・サポート・サービス
テクニカル・サポート・サービス：24 時間体制のサポート、指定エンジニア

Professional Services Delivery

セキュリティアーキテクト、プロジェクトマネージャー、開発者で構成される総合チームが、お客様のチームと協力して Akamai Guardicore Segmentation プラットフォームを実装します。お客様のニーズに応じて、Akamai はパッケージ化された成果物のセット、または期限付きの Implementation Engineer を提供します。どのパッケージをお選びいただいても、Akamai はお客様の重要な資産を確実に保護するオーダーメイドのサービスを提供します。

Jumpstart

Jumpstart は、Akamai Guardicore Segmentation の展開を迅速に行う必要があるものの、その後のポリシーの実装や管理は当社エキスパートに相談しながら自社で行うことを希望するお客様向けに設計されています。ネットワーク環境のセグメント化、アプリケーションのリングフェンス、サーバーへのアクセス制限など、お客様の目的に応じて、Akamai のエンジニアがお客様の最初のポリシーの設計と実装を行い、同時にお客様が後でポリシーを自社で実装できるように、指導とガイダンスを提供します。

また、Akamai のチームがお客様と協力してセキュリティアーキテクチャの計画を行い、アプリケーション設計の考慮事項を把握します。これには、ラベリング戦略の定義と文書化、プラットフォーム内での資産のラベリング、ユースケースをサポートするポリシーの正式な作成と微調整が含まれます。

Akamai が最初のポリシー実装を完了した後、当社のエンジニアが継続的にその後のあらゆるポリシー実装に際してお客様のチームを直接支援し、お客様の展開目標が達成されるまで、お客様の拡張チームの一員であり続けます。

Extended Jumpstart

達成するセグメンテーション目標が複数あるエンタープライズ組織には、Extended Jumpstart が最適です。Akamai のエキスパートがお客様のチームと協力して複数のセグメンテーションポリシーを実装し、重要な資産や高額な資産の保護を強化します。

Akamai のチームがお客様と協力してセキュリティアーキテクチャの計画を行い、アプリケーション設計の考慮事項を把握します。これには、ラベリング戦略の定義と文書化、プラットフォーム内での資産のラベリング、複数のセキュリティ戦略をサポートするポリシーの正式な作成と微調整が含まれます。

実装する一般的なポリシー目標

ネットワーク環境のセグメント化、アプリケーションのリングフェンス、サーバーへのアクセス制限など、お客様の目的に応じて、お客様の資産を確実に保護するために、当社のエンジニアがすべてのステップでお客様と協力します。

このサービスの一環として、お客様は複数のポリシー目標を選択することも、特定の優先度の高い目標に重点を置くこともできます。お客様の資産が事前に特定した目標どおりに保護されるまで、ポリシーを形成する必要なラベルとルールを当社のエンジニアが実装します。

以下に例を示します。

- **環境のセグメンテーション** — 異なる環境のサーバーは、明示的に許可された通信以外、通信することができない。
- **アプリケーションのリングフェンシング** — 基幹アプリケーションは、明示的に許可された相手とのみ通信する。内部アプリケーションの通信は許可される。
- **アプリケーションのマイクロセグメンテーション** — 基幹アプリケーションの内部および外部トラフィックは、明示的に承認された場合のみ許可される（ゼロトラスト）。
- **「企業ネットワーク外」のエンドポイントのセグメンテーション** — 企業ネットワークの保護外にあるエンドポイントのアタックサーフェスは制限される。Akamai Guardicore Segmentation は、企業ネットワークの内外で異なるルールセットの設定が可能。
- **サーバーへの権限アクセス** — サーバーアクセス制御ポリシーを実装し、たとえば、管理ポートをジャンプボックスのみに制限したり、ソースのユーザーアイデンティティに基づいて特定のサーバーへのアクセスを阻止したりすることができる。
- **セキュリティ・ベスト・プラクティスの適用** — ブロック・リスト・ルールを導入し、ネットワークセキュリティのベストプラクティスを適用する。

Implementation Engineer

エンタープライズ組織が必要とするポリシー目標の数が多い場合、Akamai のエンジニアがお客様のために作成できるポリシーの数に制限を設けることなく、一定期間、担当のエンジニアが協力することが実装の成功に望ましいケースがよくあります。ネットワークに完全なエンドツーエンドのセグメンテーションが必要なときに、Akamai がお客様の目標達成に必要な実装サポートを提供できることが理想的です。

	Jumpstart	Extended Jumpstart	Implementation Engineer
インストール	✔	✔	✔
ラベリングスキーマの導入	✔ 制限あり	✔ ✔ ✔	一定期間、包括的な実装リソースを提供し、ユースケースの制限なく、お客様の成功目標が達成できるよう支援
全体的なセキュリティ対策に関するガイダンス	✔ 制限あり	✔ ✔ ✔	
ポリシー作成に関するガイダンス	✔ 制限あり	✔ ✔ ✔	
ポリシーユースケースの実装	**単一のポリシー**	**複数のポリシー**	
エンドユーザーのトレーニング	✔	✔	✔
一般的な期間	**6 か月**	**12 か月**	**6 ～ 18 か月**
オプションの選択場面	お客様またはパートナーのほとんどが自社で実装することを望むため、Akamai は最初のユースケースのみを実装	Akamai が複数のユースケース、複数のポリシーを実装し、広範なガイダンスを提供	お客様またはパートナーが完全な実装（複数のユースケース）を希望し、その期間中、正確に何をどのようにするかを探り、定義することを望んでいる場合

Akamai トレーニング

マイクロセグメンテーションのための Akamai 認定トレーニングを受けると、管理者（GCSA）や運用エンジニア（GCSE）は、関連の保守作業や管理作業を成功させるために必要なスキルと情報を身に付けることができます。

お客様やパートナー様のニーズに合わせて、基本的なオンライントレーニングから、インストラクターによる認定トレーニング、さらには個人向けの専門トレーニング（オンラインまたは対面式）まで、多様なトレーニング方法が用意されています。

Guardicore Certified Segmentation Administrator（GCSA）

この 5 日間の半日プログラムを通じて、Akamai Guardicore Segmentation プラットフォームユーザーは、このプラットフォームのあらゆる要素を適切に運用するために必要な専門知識を習得することができます。GCSA 修了者は、組織のセキュリティニーズを実装・維持するために自分自身でプラットフォームを使用できるようになります。

このコースでは、Akamai Guardicore Segmentation の中核的な機能である可視化、ラベリング、マイクロセグメンテーション、侵害検知について学びます。このコースは主に機能のふるまいと使い方に重点を置きながら、Akamai Guardicore Segmentation の初期設定から日常の一般的な運用まで、受講者をガイドします。

Guardicore Certified Segmentation Engineer（GCSE）

この 3 日間の半日プログラムを受講すると、システムの運用担当者は、プラットフォーム関連の管理および保守業務を遂行するために必要なスキルと知識を習得することができます。

GCSE 修了者は、Akamai Guardicore Segmentation 環境の運用全般を管理できるようになります。このコースでは、プラットフォームとコンポーネントの設定、サードパーティーツールとの連携、プラットフォームの健全性チェック、トラブルシューティング、一般的な保守業務について学びます。

両コースとも、コース期間中すべての受講生が利用可能なオンラインの実践演習が付属しています。各コースの終わりに認定試験が行われます。

Enterprise Support と Customer Success

当社の Enterprise Support プログラムは、お客様の組織における Akamai Guardicore Micro-segmentation の使用に際して生じ得るあらゆる結果をサポートするよう設計されています。Akamai のサポート組織が 24 時間体制でお客様のあらゆるサポートケースに対応し、アップグレードや修正を支援します。

当社の Customer Success プログラムは、お客様の組織の短期的および長期的なセキュリティ目標の達成を支援すると同時に、お客様による当社プラットフォームへの投資の価値を最大限に引き出します。

Elite Support

Akamai の Elite Support は、お客様の組織に指定された、経験豊富なトップクラスのエスカレーションエキスパートへの優先的なアクセスを提供します。お客様のデータセンターや社内プロセスを熟知したスキルの高いスペシャリストがお客様の連絡窓口となり、お客様のあらゆる問題への対応と解決を迅速化し、ソフトウェアベースのセグメンテーションに対する投資を最大限に活用できるよう支援します。

	Premium	Elite
サポートの可用性	**24 時間**	**24 時間**
無制限のサポートケース	✔	✔
アップグレードと修正	✔	✔
電話、メール、Slack、ポータル	✔	✔
根本原因分析（要求に応じて）	**重大度 1**	**重大度 1 & 重大度 2**
指定された経験豊富なエンジニアによる優先的なケース処理		✔ 指定エンジニアは営業時間内にサポートを提供
プロアクティブで継続的なシステム健全性の監視		✔
パーソナライズされた最適化		✔ 四半期ごとの最適化セッション
定期的な課題評価とサポートレポート		✔ 週次課題評価、月次サポートレポート
コンサルテーション日数		✔ 規模（SKU）に応じて年 2 日／4 日／6 日
オプションの選択場面	展開規模が小さい、主にサポートが必要	展開規模が大きい、継続的な課題に対してより高度な制御が必要

Day-2 Operation Services

最初にいくつかのユースケースを展開した後、お客様は Akamai Guardicore Segmentation 製品から価値を得ることができます。しかし、この製品から得られる価値を最大限に引き出すためには、継続的な保守とアップデートが必要です。

- 展開（資産、ラベル、ポリシー）をアップデートして、組織で発生した変更を反映する
- 初期の展開段階で処理できなかったユースケース（製品を使用し始めてから新たに特定したユースケース、処理が必要な追加のサービスやアプリケーションなど）を追加で実装
- クラウドベースのネットワークやアプリケーションなど、組織の他の部門での Akamai Guardicore Segmentation を追加で実装（新規または第 2 段階として残されていたもの）
- 追加のエンドポイント、モノのインターネット（IoT）デバイス、仮想デスクトップインフラ環境などへの展開
- Akamai Guardicore Segmentation を使用したセキュリティイベントの特定と緩和（ネットワーク内のラテラルムーブメント（横方向の移動）の阻止など）。お客様の環境を Akamai Security Operations Command Center に接続し、24 時間体制の監視とリアルタイムの警告および緩和を獲得
- Akamai Hunt、Akamai Edge DNS（セキュリティを確保した DNS および分散型サービス妨害攻撃からの防御）、Akamai Enterprise Application Access（アクセスとアイデンティティ管理）を通じたプロアクティブで強化されたセキュリティの獲得
- Akamai Guardicore Segmentation を使用した認定監査の支援

これらのサービスは、GcSP 認定パートナーにより提供されます

Technical Account Manager および Resident Engineer

Akamai Technical Account Manager および Resident Engineer は、広範で潜在的に複雑なセグメンテーションのニーズを有するエンタープライズ組織向けの経験豊富な技術アドバイザーです。Akamai のエンジニアはお客様の組織に組み込まれると、すぐにお客様の環境のエキスパートとなり、お客様が Akamai Guardicore Segmentation で素晴らしい成功を達成できるように支援します。

お客様のアカウントを担当する Resident Engineer* はお客様のチームに組み込まれ、お客様が Akamai Guardicore Segmentation から常に最大限の価値を引き出せるようにお客様のあらゆる業務をプロアクティブにサポートします。

Resident Engineer は、ポリシー決定のガイダンス、Akamai 製品に導入予定の最新機能についての情報提供、アップグレードの計画（および実行の支援）、エグゼクティブ・ビジネス・レビューの実施により、お客様が確実に成功できるよう支援します。

担当の Technical Account Manager または Resident Engineer は、お客様の Day-2 Operation Services の監督と実行も可能です。

Resident Engineer* **はリモートの場合もあります

Akamai Hunt：マネージド型脅威ハンティングサービス

Akamai Guardicore Segmentation の拡張機能である Akamai Hunt は、Akamai のマネージド型脅威ハンティングサービスであり、極めて巧妙に検知を逃れようとする脅威に先手を打ち、組織をより適切に保護します。

Akamai Hunt チームは、最先端のセキュリティソリューションさえも常に回避する異常な攻撃のふるまいや巧妙な脅威を常時探索しています。Hunt を導入すれば、ネットワークで検知された重大なインシデントがただちに通知されます。さらに Akamai のエキスパートがお客様のチームと緊密に連携し、侵害を受けた資産を修復して迅速に解決します。

ランサムウェアの検知と防止、巧妙な持続的脅威の撃退、ゼロデイ脆弱性に対する保護、あるいは一般的な IT セキュリティ対策の改善など、お客様が何に重点を置いているかに関わらず、追加のソフトウェアやエージェントの導入、アップグレードの必要なく、Akamai Hunt は Akamai Guardicore Segmentation の展開から最大のセキュリティ価値を引き出すことを可能にします。

Akamai Hunt は次を提供しています。

24 時間体制のエキスパートによる人的分析 — 当社のサイバーセキュリティのプロフェッショナルは、セキュリティリサーチ、攻撃的なセキュリティ、軍事インテリジェンス、レッドチーム、インシデント対応、データサイエンスなど、幅広い分野から招集されています。

真の脅威に対するアラート — アラート疲れを防ぐため、Hunt チームは、お客様に送信するアラートを真の脅威のみに限定することでフォールス・ポジティブ（誤検知）を確実に回避します。

独自のハンティングツール — Akamai Hunt のエキスパートは、ユーザーおよびネットワークアクティビティの異常なふるまい、実行可能な分析、ログ分析など、高度な脅威ハンティングアルゴリズムを定期的に開発し、迅速な検知と対応を実現する強力なツールセットを構築します。エンドポイントとサーバーにリアルタイムでクエリーを送信するパワフルな OS クエリーベースツールの Akamai Guardicore Insight が、追加コストなしでサービスに含まれています。

コンテキストに富んだ脅威インテリジェンス — Akamai の Hunters チームが、Akamai Guardicore Segmentation と Akamai の大規模なグローバル脅威インテリジェンスを活用し、IP やドメインからプロセス、ユーザー、サービスに至るまで、さまざまな侵害の指標を収集しています。

ネットワーク、クラウド、エンドポイントの可視化 — Akamai Guardicore Segmentation の導入で生成されたデータと Akamai のグローバルセンサー（Akamai DNS クラウドに対して発信される毎日 7 兆件以上の DNS リクエストを含む）を組み合わせることで、Akamai のチームはお客様の環境を非常に包括的に可視化します。

迅速な通知とプロアクティブな知見 —

- 脅威を検知すると、直ちにメール通知が送信される
- エグゼクティブレベルの定期脅威レポートには、分析、統計、指標が含まれており、エグゼクティブや経営陣は大規模な攻撃キャンペーンを把握できる
- Akamai Guardicore Segmentation コンソールとの統合により、インシデント管理が容易

Akamai Guardicore Segmentation の詳細については、akamai.com をご覧ください