ホワイトペーパー

マイクロセグメンテーションの主なユースケースについて

著者：John Grady（Enterprise Strategy Group シニアアナリスト）

2023 年 1 月

Enterprise Strategy Group ホワイトペーパーは、Akamai からの委託を受けて作成されたものであり、TechTarget, Inc. の許可を得て配布されます。

目次

概要

サイバーセキュリティ業界全体でゼロトラストが普及しています。しかし、この取り組みの幅広さと、戦略における最重要点に関する意見の対立により、何から着手すればよいのか、そしてどのツールがフレームワークのサポートに最適かについて混乱が生じています。ゼロトラスト実現への道は一つではありませんが、最終的に、リソースやエンティティがポリシーで明示的に許可されている場合にのみ、相互に通信できるようにすることが重要です。これは、マイクロセグメンテーションの重要性を示しています。

マイクロセグメンテーションツールの使用は、現時点では若干限られていますが、ゼロトラストへのマイクロセグメンテーションの重要性と、さまざまなユースケースへの適用性が認識されるにつれ、大幅に増加すると予想されています。組織でゼロトラストを検討する理由が、脅威を防止するためでも、ビジネス全体の効率性を向上させるためでも、または全体的なセキュリティアプローチを最新化するためであっても、いずれにしてもマイクロセグメンテーションが役立ちます。特に、Akamai のソフトウェアベースおよび人工知能がサポートするマイクロセグメンテーションアプローチは、精度の高い可視性を提供し、ラテラルムーブメントを防止し、ランサムウェア攻撃を阻止し、環境全体で一貫してゼロトラスト原則を適用できるように組織を支援します。

組織でゼロトラストを検討する理由が、脅威を防止するためでも、ビジネス全体の効率性を向上させるためでも、または全体的なセキュリティアプローチを最新化するためであっても、いずれにしてもマイクロセグメンテーションが役立ちます。

ゼロトラストは勢いを増していますが、明確な優先順位を確立することが重要です

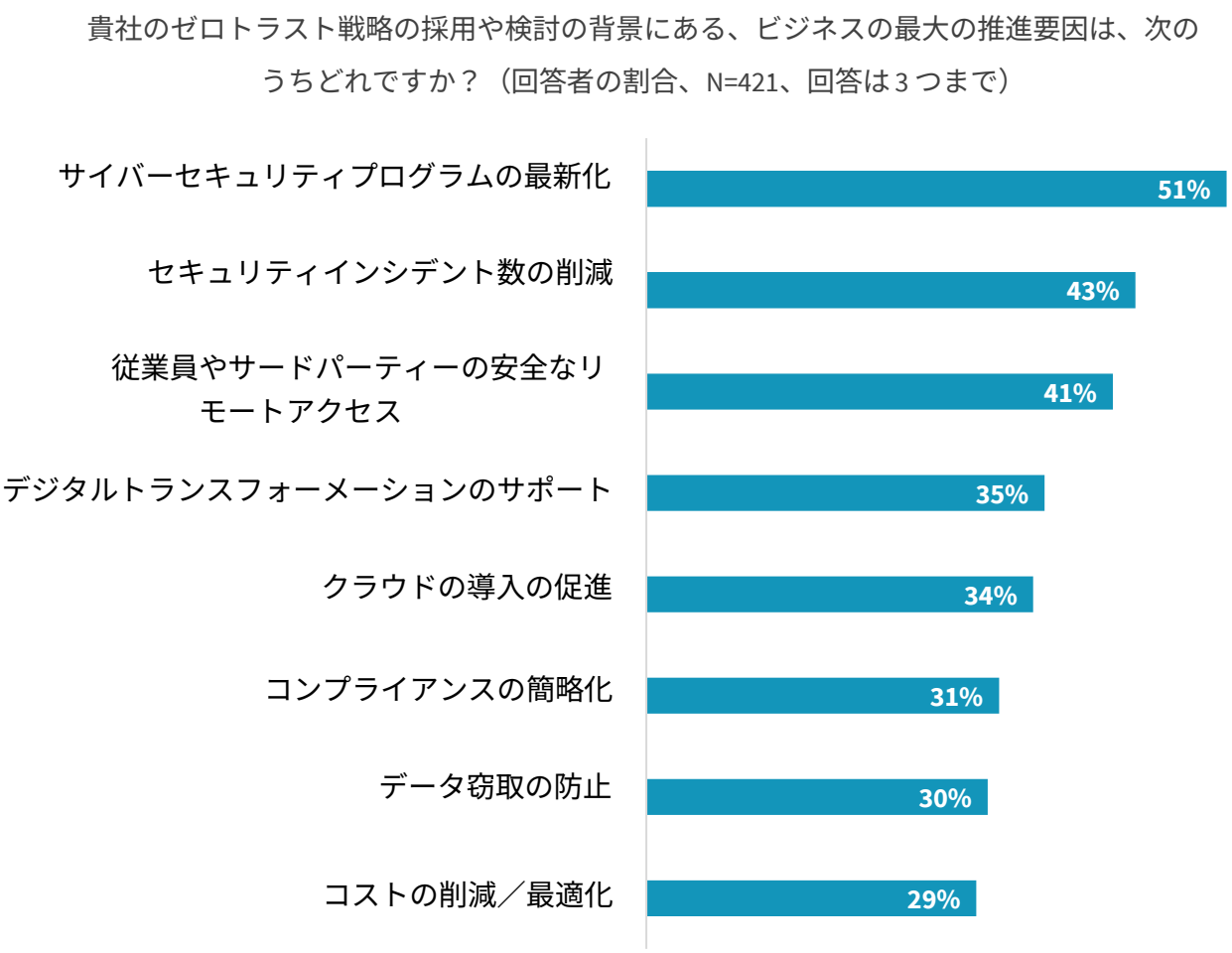
リソースがクラウドへと移行し、デジタルビジネスモデルが定着し、ユーザーの分散が進むにつれ、企業環境は複雑化し続けています。これらの変化は、サイバーセキュリティチームの仕事を本質的に困難にしています。攻撃者は、防御のギャップを探してそこから侵入し、ランサムウェア攻撃を開始したり、顧客情報を盗んだり、機密性の高い知的財産を盗もうとしています。しかし残念ながら、許容度が高い、従来の境界型制御に依存したセキュリティアプローチでは、これらの現実に対処できなくなり、セキュリティチームは戦略を再評価せざるを得ない状況にあります。さらに、攻撃の数と巧妙さは高まっており、セキュリティチームが潜在的なあらゆる脅威を把握し、対処し、パッチを適用することは不可能です。

これらの問題により、多くの企業がゼロトラストの概念に到達しました。これは新しい戦略ではありませんが、ゼロトラスト戦略は、サイバーセキュリティに対するよりダイナミックで、権限が最小で、リスクベースのアプローチへの道として、組織から大きな関心を集めています。ゼロトラストアプローチは、環境から暗黙的な信頼を排除し、すべてのデジタルインタラクションを継続的に検証します。その結果、ゼロトラストアプローチを採用することで、セキュリティチームはリソース、ユーザー、デバイスが安全で利用可能であるという信頼を高めることができます。しかし、ゼロトラストは広範に適用でき、それがどのようなものであるかについて矛盾する意見や定義があるため、混乱が生じ、どこから着手したら良いか組織で判断が困難なことがあります。

組織の優先順位と望ましい結果を評価することで、焦点を絞り、ゼロトラストの取り組みをどこから始めたらよいかを判断するために役立ちます。さまざまなビジネス要因が、組織をゼロトラストへと推進しています（図 1 を参照）。[1]最も一般的な目標はサイバーセキュリティの最新化で、回答者の 51% が挙げています。この考え方は、バイデン政権によって発令されたサイバーセキュリティに関する大統領令によって強調されており、その近代化要件の中でゼロトラスト・アーキテクチャが取り上げられています。これらの命令は民間部門を直接対象としたものではありませんが、連邦政府以外のセキュリティチームに方向性を与えてくれます。ゼロトラストのその他の戦略的目標には、デジタルトランスフォーメーションのサポート（35%）とクラウド導入の加速（34%）が含まれます。これらの要因は、多くの組織において、セキュリティチームは単に資産を保護するのではなく、ビジネスを実現する支援をすべきだという期待を強調しています。セキュリティインシデント数の削減（43%）、安全なリモートアクセスの実現（41%）、コンプライアンスの簡略化（31%）、データ窃取の防止（30%）などの、より実務的な目標も一般的です。

ゼロトラストでは、ポリシーによって明示的に許可されている場合にのみ、リソースとエンティティが相互に通信できるようにすることが重要です。

図 1．ゼロトラストの要因



出典：Enterprise Strategy Group, a division of TechTarget, Inc.

[1]出典：Enterprise Strategy Group の調査結果、『*The State of Zero Trust Security Strategies*』、2021 年 5 月。

ゼロトラスト・プロジェクトの初期の焦点を絞ることは、場合により、セキュリティチームが戦略をサポートするために必要なツールを特定するのに役立ちます。たとえば、従業員やサードパーティーの安全なリモートアクセスを改善することを目標としている場合、多くの企業はゼロトラストネットワークアクセス（ZTNA）を選択します。多要素認証（MFA）などの本人確認ツールも、このシナリオで使用される場合があります。ただし、一部の要因では、テクノロジー要件の解釈に余地があることがあり、多くの組織は焦点を絞り込んだ後でも、複数の目標に焦点を当てることがあります。このような状況では、さまざまなユースケースや成果をサポートできるツールや慣行を組織が特定することが重要です。

マイクロセグメンテーションは現在、ゼロトラストモデルのサポートでは十分に活用されていません

ゼロトラスト実現への道は一つではありませんが、最終的に、リソースやエンティティがポリシーで明示的に許可されている場合にのみ相互に通信できるようにすることが重要です。つまり、攻撃の影響を制限するため、組織のゼロトラスト哲学の重要な要素は、資産を適切に区分する能力です。これは、サイバーセキュリティの最新化などの幅広い目標や、データ窃取の防止などのより焦点を絞った目標に適用できます。

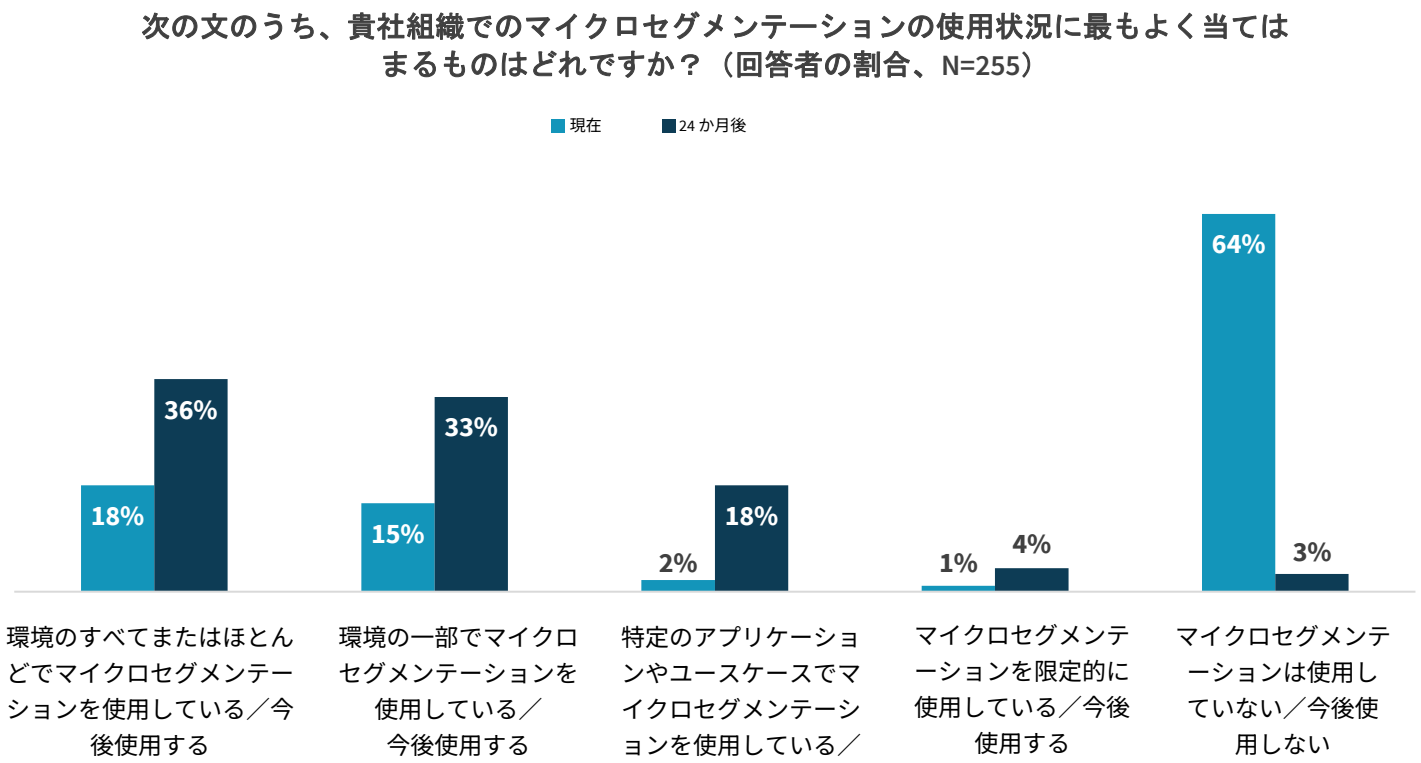
しかし、現在の環境では、精度の低いセグメンテーションだけでは一般に不十分であり、企業資産を適切に保護するためには、より詳細なマイクロセグメンテーションが必要です。最新のアプリケーションアーキテクチャは、多くの場合、複数のサーバーインスタンスに分散された、または一部のケースでは複数のクラウド環境に分散されたワークロードに依存しています。場所に基づいてリソースをセグメント化する方法は時代遅れになっており、セキュリティチームが現在直面している課題には対応していません。

これまで、組織はマイクロセグメンテーションツールの導入に躊躇してきました。TechTarget の Enterprise Strategy Group（ESG）の調査によると、組織の 28% がマイクロセグメンテーションは複雑すぎると考えています。しかし、これはおそらく、セキュリティチームがマイクロセグメンテーションに対して誤ったツールを使用していることが大きな要因である可能性があります。特に ESG の調査によると、組織の 55% が、マイクロセグメンテーションにファイアウォールなどのインフラベースのツールを使用しており、ホストベースのツールを使用しているのは 8% に過ぎません。[2]ファイアウォールでは、マイクロセグメンテーションを成功させるために必要なきめ細かなポリシーを適用できません。さらに、これらのツールではアプリケーションワークロード全体の可視性が限られており、オンプレミスとクラウドの両方の場所で環境のすべての側面に一貫して対応することが困難です。

このため、マイクロセグメンテーションは十分に活用されませんでした。ESG の調査によると、ゼロトラストにとって非常に重要であるにもかかわらず、現在マイクロセグメンテーションを使用している組織はわずか 36% です（図 2 を参照）。幸いなことに、多くの組織はこれが防御の大きなギャップであることを認識しています。その結果、91% が今後 24 か月以内にマイクロセグメンテーションを使用するだろうと予測しています。[3]マイクロセグメンテーションは最終的に、外部および内部の脅威に対して物理、仮想、クラウドネットワークを強化してゼロトラストの主なメリットを支援し、あらゆるゼロトラスト戦略の中核となるべきものです。

[2]出典：Enterprise Strategy Group の全調査結果、『*Network Security Trends in Hybrid Cloud Environments*、』、2021 年 12 月
[3]Ibid.

図 2．マイクロセグメンテーションの採用



出典：Enterprise Strategy Group, a division of TechTarget, Inc.

マイクロセグメンテーションの主なユースケース

マイクロセグメンテーションは、さまざまなゼロトラストのユースケースに幅広く適用できます。これは、マイクロセグメンテーションがこれまでになく重視されている大きな理由です。しかし何よりもまず、マイクロセグメンテーションは、組織の最も重要な資産のセキュリティを確保できるため、ゼロトラスト・ジャーニーの開始点となります。これは、使用するソリューションが、ワークロードとエンティティの関係を詳細に可視化できる場合に特に該当します。トラフィックフローと依存関係のベースラインを確立することは、ビジネスを中断することなく暗黙的な信頼を排除するための第一歩として、ゼロトラストの取り組みの基礎となります。このアプローチにより、セキュリティチームは最も重要な資産を迅速に保護し、ゼロトラストの実装の進行中に侵害が発生した場合の影響を制限することができます。その保証を確保した上で、セキュリティチームは、マイクロセグメンテーションがサポートするその他のユースケースに注意を向けることができます。

脅威の防止

ゼロトラストはセキュリティフレームワークであり、セキュリティの目標はサイバー脅威から組織を保護することです。よってゼロトラストは、脅威を防ぎ、企業のリソースへの脅威の影響を制限することに焦点を当てた、以下のような一部の主要なマイクロセグメンテーションのユースケースに従っています。

- **重要な資産をリングフェンス（分離）する。**セキュリティチームは、保護の優先順位を決定する際に、リスクを比較検討する必要があります。規制された顧客情報、知的財産、その他の機密情報を含む価値の高いアプリケーションは、システムが侵害された場合の影響を考慮して、より焦点を当て、セキュリティ管理を強化する必要があります。マイクロセグメンテーションを使用することにより、セキュリティチームは、これらのアプリケーションとそのアプリケーションを構成するワークロードをインフラの他の部分から完全に分離できます。

- **ラテラルムーブメントを制限する。**ゼロトラストの過小評価されている原則の一つは、敵対者が企業ネットワークへのアクセスを持っていると仮定した、「侵害を前提とする」考え方で行動することです。従来のエンドポイント、サーバー、クラウドリソース、さらにはスマートデバイスの無秩序な普及により、侵入は避けられないものとなっています。その結果、マイクロセグメンテーションによって潜在的な攻撃半径を制限することで、攻撃者のネットワーク内でのラテラルムーブメントを防ぐことができます。

- **脅威の検出と対応。**攻撃が発生した場合、時間が最も重要です。マイクロセグメンテーションツールを使用すると、セキュリティチームは迅速かつ効果的に対応できます。チームは、アプリケーションの関係に基づいて攻撃経路になりうる箇所を迅速に把握し、攻撃中に攻撃者が使用するポートをブロックし、影響を受けたシステムをネットワークの他の部分から迅速に隔離できます。さらに、攻撃をその初期の侵入点に制限します。

ランサムウェアからの保護

ランサムウェアの継続的な蔓延と攻撃の影響により、これらの問題は経営幹部、または役員レベルまでに達しています。ランサムウェアへの対策には強力なセキュリティだけでなく、優れたデータ保護機能とインシデント対応機能も必要ですが、マイクロセグメンテーションは、攻撃に対抗するためのしっかりとした基盤を維持するために役立ちます。攻撃者は多くの場合、環境に侵入して偵察に時間をかけた後にのみ、攻撃の過程で機密情報やシステムを標的にします。マイクロセグメンテーションを使用して重要な資産をリングフェンス（分離）し、ラテラルムーブメントを制限すると、攻撃者は環境全体を自由に移動できなくなります。さらに、ランサムウェア攻撃が検出されると、マイクロセグメンテーションを使用する組織は、攻撃者が使用する通信経路を迅速にシャットダウンし、感染したサーバーを孤立させ、攻撃がさらに広がるのを防ぐことができます。

ビジネス全体の効率性を促進

セキュリティチームの最初の目標は環境を保護することですが、今日では、ビジネスの効率に影響を与えずに保護することも義務付けられています。さらに、セキュリティチームが実際に同僚をサポートできれば、それはビジネスにとって有益です。これにはさまざまな意味合いがありますが、最も一般的なものには次のようなものがあります。

- **クラウドの導入をサポートする。**クラウドへの移行は新しいことではありませんが、多くの組織にとって、セキュリティ上の懸念は一番に挙げられます。理由の一部として、IaaS（Infrastructure-as-a-Service）プラットフォームのネイティブセキュリティ制御に精通していないためであり、またその他の理由にはハイ

ブリッドクラウド環境で発生する可能性のあるセキュリティの不統一が挙げられます。マイクロセグメンテーションは、環境のあらゆる側面でコントロールを使用し、ハイブリッドクラウドのシナリオでセキュリティの一貫性を向上できるため、組織に大きな安心をもたらします。

- **アプリケーションの最新化を実現する。**クラウドへの移行に加え、コンテナなどの最新のアプリケーションアーキテクチャの採用も加速し続けています。これらのモデルにより、アプリケーションチームはアプリケーションの設計、構築、展開をこれまで以上に迅速に行うことができます。開発者のスピードを制限することなく、これらのリソースを確実に保護し、ビジネスにプラスの影響をもたらすツールです。コンテナ環境でトラフィックフローを可視化し、コンテナがオンラインになったときや移動したときにセグメント化ポリシーを自動的に適用するマイクロセグメンテーションツールは、開発チームがアプリケーションのセキュリティを確保するために役立ちます。

- **コンプライアンスの合理化。**組織は、規制上の問題にますます多くの時間、予算、意識を注いでいます。セキュリティリスクを可能な限り分離して、データプライバシーの侵害や個人を特定できる情報の損失などの問題の可能性を制限することで、プロセスの負担を大幅に軽減できます。マイクロセグメンテーションにより、コンプライアンス要件の対象となるシステムを環境の他の部分から分離し、セキュリティチームの負担を軽減できます。

ゼロトラスト・セグメンテーション

マイクロセグメンテーションの最も魅力的な側面の 1 つは、ターゲットを細かく設定したユースケースに焦点を当てた場合、組織に即座に価値を提供できることです。あまり手間を必要とせずに簡単に価値をもたらすことのできる、拒否リスト、重要なアプリケーションのリングフェンシング、環境のセグメント化、その他のあまり複雑でないポリシーから開始できる機能は、多くの企業にとって魅力的です。企業全体に完全なマイクロセグメンテーション戦略を一度に展開する企業はほとんどありません。しかし、ゼロトラストの取り組み範囲で、環境全体にマイクロセグメンテーションがより幅広く導入されるに伴い、多くの組織はゼロトラスト・セグメンテーションへのアプローチを開始します。組織はトラフィックフローの精度の高い包括的な可視性を維持し、最も機密性の高い資産を保護し、ラテラルムーブメントを防止し、脅威に迅速に対応しながら、ビジネスをより効果的にサポートすることができるため、これまでに説明したユースケースと肯定的な結果が組み合わされます。多くのマイクロセグメンテーションプロジェクトにとっての開始点ではありませんが、これは時間をかけて最終的に達成する目標として捉えてください。

マイクロセグメンテーションに対する Akamai のアプローチ

マイクロセグメンテーションはゼロトラストの重要な側面ですが、その他にも、脅威の検知と対応、アイデンティティ、データセキュリティなどをサポートするテクノロジーを必要とする、その他の主要コンポーネントもあることを覚えておくことが重要です。テクノロジーベンダーの評価、選択、および連携は、細部に注意を払うべき体系的なプロセスであり、このプロセスによって、組

Akamai Guardicore Segmentation ソリューションは、マイクロセグメンテーションに対するソフトウェアベースのアプローチであり、デジタル環境内での攻撃者のラテラルムーブメントを阻止するように設計されています。

織のサイバーセキュリティ目標が達成できることも、ただのコスト、時間、労力の消耗となることもあります。よって、広範な統合機能と信号共有機能を備えたマイクロセグメンテーションツールを検討することで、マイクロセグメンテーションを超えるゼロトラスト戦略を推進し、運用の複雑さを軽減することができます。

Akamai は、ネットワークインフラ業界において長年の実績を持つ企業であり、マイクロセグメンテーションとゼロトラストをソリューションポートフォリオの中核としてきました。Akamai のオンプレミス環境とクラウド環境の両方に対するエンタープライズインフラ要件の知識には、潜在的なサイバーセキュリティの課題を発見して対処する経験も含まれます。

Akamai Guardicore Segmentation は、マイクロセグメンテーションに対するソフトウェアベースのアプローチであり、デジタル環境内での攻撃者のラテラルムーブメントを阻止するように設計されています。このソリューションは、精度の高い可視性を使用して、ネットワークレベルでゼロトラスト原則を適用し、組織が物理環境と仮想環境内でアクティビティと移動を可視化できるように支援します。その人工知能ベースのセグメンテーションフレームワークでは、統合テンプレートを使用し、ランサムウェア、エンドポイントベースの攻撃、リモートワークフォースを標的とした攻撃などの侵入を検出して阻止します。ベアメタルサーバー、仮想マシン、コンテナ、IoT デバイス、クラウドインスタンスなど、さまざまなプラットフォームで使用できます。

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収集、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促進する統合など、基盤となるインフラに関する広範なデータを複数の方法で収集します。動的マッピングを使用すると、管理者は精度の低いアクティビティについて、エンドツーエンドの可視化を得られます。Akamai のエンタープライズネットワーキング環境における経験を活用し、Akamai Guardicore Segmentation は、企業のトラフィックのボトルネックの原因を特定してそれを回避し、一貫したパフォーマンスとスケーラビリティを実現するように設計されています。

マイクロセグメンテーションの真実

マイクロセグメンテーションは新しいテクノロジーではありません。実際、時代を先取りしていたかもしれません。しかし、最新のハイブリッド、マルチクラウド環境を保護するためのマイクロセグメンテーションの重要性、特にゼロトラスト戦略の運用におけるその重要性は、どれだけ強調しても強調しすぎることはありません。マイクロセグメンテーションは、ミッションクリティカルおよびビジネスクリティカルな多くのユースケースでゼロトラストを実現するために必要な柔軟性、機敏性、効率性を提供し、重要なインフラや知的財産からアイデンティティや資格情報まで、あらゆるものを保護します。ネットワークインフラ、セグメンテーション、マイクロセグメンテーションにおける豊かな経験を持つ Akamai は、マイクロセグメンテーションのツールとマインドセットに基づいた安全なインフラを計画、構築、展開、さらには管理するための有力な候補です。

Enterprise Strategy Group は、市場インテリジェンス、実用的なインサイト、Go-to-Market コンテンツサービスをグローバル IT コミュニティに提供する、統合されたテクノロジー分析、調査、戦略企業です。

www.esg-global.com　contact@esg-global.com　508.482.0188