ハイブリッドクラウド環境での DDoS 防御

目次

進化を続ける DDoS

分散型サービス妨害攻撃（DDoS）は最も古いタイプのサイバー脅威の 1 つですが、今でも進化を続けており、現在ではサイバー犯罪者やイデオロギー的な動機を持つハクティビストが利用する、高度なツールとなっています。実際、DDoS 攻撃は、大企業や中小企業だけでなく、ヘルスケア、エネルギー、公益事業、教育などの分野における重要な公共インフラにもセキュリティリスクをもたらします。

この変化し続ける情勢をさらに複雑にするのは、公共機関と民間機関の両方でクラウド・コンピューティング・リソースが普及している現状です。これらの組織が既存のオンプレミスリソースとクラウドを組み合わせて利用すると、その結果として、非常に複雑なハイブリッド環境が生まれます。アプリケーション、アプリケーション・プログラミング・インターフェース（API）、データ、マイクロサービス、ワークロードは、断片化された環境を通過しなければなりません。これらの環境のアーキテクチャが異なると、新たな脆弱性と細分化されたアタックサーフェスが生まれ、サイバー犯罪者はそれを悪用して、ますます巧妙で大きな被害をもたらす DDoS 攻撃を仕掛けてくるおそれがあります。

組織は、デジタルインフラを確実に保護するために、急いで対策を講じています。組織に必要なのは、短時間で急激な DDoS 攻撃からオンプレミス（プライベートクラウド）インフラを保護できる統合型ハイブリッド DDoS 防御プラットフォームです。また、大規模なボリューム型 DDoS 攻撃に対してクラウドスクラビングの規模とキャパシティを活用できることも必要です。

トレンドを見ると、より強力な DDoS 攻撃が以前より頻繁に行われることがわかります。2023 年 2 月、Akamai は、アジア太平洋地域（APAC）を拠点とする Akamai Prolexic 顧客に対して仕掛けられた最大規模の DDoS 攻撃を緩和することに成功しました。この攻撃のピークトラフィックは 900.1 ギガビット／秒、および 1 億 5,820 万パケット／秒（Mpps）でした。このわずか数か月前、ヨーロッパでは、Akamai Prolexic を導入しているある顧客に対して最大規模の DDoS 攻撃が仕掛けられました。組織の事業活動の妨害を狙ったこの大胆な攻撃により、攻撃トラフィックは 704.8 Mpps まで急上昇しました。このほかに、Akamai がこれまでに緩和した最大規模の DDoS 攻撃も発生しています。これは、1.44 テラビット／秒（Tbps）、385 Mpps のグローバル分散型攻撃で、2 時間近く続きました。Akamai は、トラフィックと攻撃パターンに関する知見をもとに、2023 年全体で DDoS 攻撃の頻度が高まり、長時間化、高度化（複数のベクトルの使用）が進み、水平方向のターゲット（同一の攻撃イベントで複数の IP 宛先を攻撃すること）に重点が置かれるようになったと判断しました。

増大する脅威

今日のほとんどの DDoS 攻撃はマルチベクトル攻撃であり、多くの場合、10 以上の攻撃ベクトルを使用して初歩的な DDoS 防御システムやプラットフォームを過負荷状態にします。実際、Akamai の社内脅威インテリジェンスによると、マルチデスティネーション攻撃または水平型 DDoS 攻撃の件数は 2022 年から 2023 年にかけて倍増しました。そして、2023 年に発生したボリューム型 DDoS 攻撃の全体的な数、規模、時間は過去最高になりました。

組織のセキュリティ計画をさらに複雑にしているのは、攻撃者が従来のボリューム型攻撃と組み合わせて使用しているさまざまな戦術が進化していることです。

DDoS 攻撃者は、次を含めたあらゆる潜在的な障害点をターゲットにします。

- Web サイト
- Web アプリケーションとその他のエンタープライズサービス
- 企業リソースにリモートアクセスするための VPN コンセントレーター
- SD-WAN コントローラー
- アプリケーション・プログラミング・インターフェース（API）
- ドメイン・ネーム・システム（DNS）とオリジンサーバー
- データセンターとネットワークインフラ

DNS インフラ

組織の DNS インフラに対する DDoS 攻撃が広がりつつあります。特に NXDOMAIN 攻撃（疑似ランダムサブドメイン攻撃、DNS 水責め攻撃、DNS リソース枯渇攻撃とも呼ばれます）が一般的な脅威になっています。2023 年に Akamai が緩和した DDoS 攻撃の 60% 以上に DNS コンポーネントがあり、NXDOMAIN 攻撃はその DNS DDoS 攻撃の約半分を占めていました。このような攻撃によって企業の DNS がダウンすると、オンラインプレゼンスも損なわれるため、企業の収益と評判に重大なリスクをもたらします。

アプリケーションレイヤー攻撃

アプリケーションレイヤー（レイヤー 7）に対する DDoS 攻撃が巧妙化しています。攻撃者が、一見無害に見えるロジックとワークフローを悪用する戦術を進化させているためです。2023 年に発見された HTTP/2 の脆弱性をついて、過去最大のレイヤー 7 DDoS 攻撃が発生しています。

サービスとしての DDoS

Anonymous Sudan や Killnet などの組織化されたサイバー犯罪者グループが、サービスとしての DDoS を提供しています。こうしたケースでは、サイバー犯罪者グループがサービス（通常はボットネット）を有料で提供し、クライアントに代わって攻撃を実行します。このような DDoS 請負サービスは、特定の動機を持つグループに大きな収益をもたらします。

ランサムウェア + DDoS = RDDoS

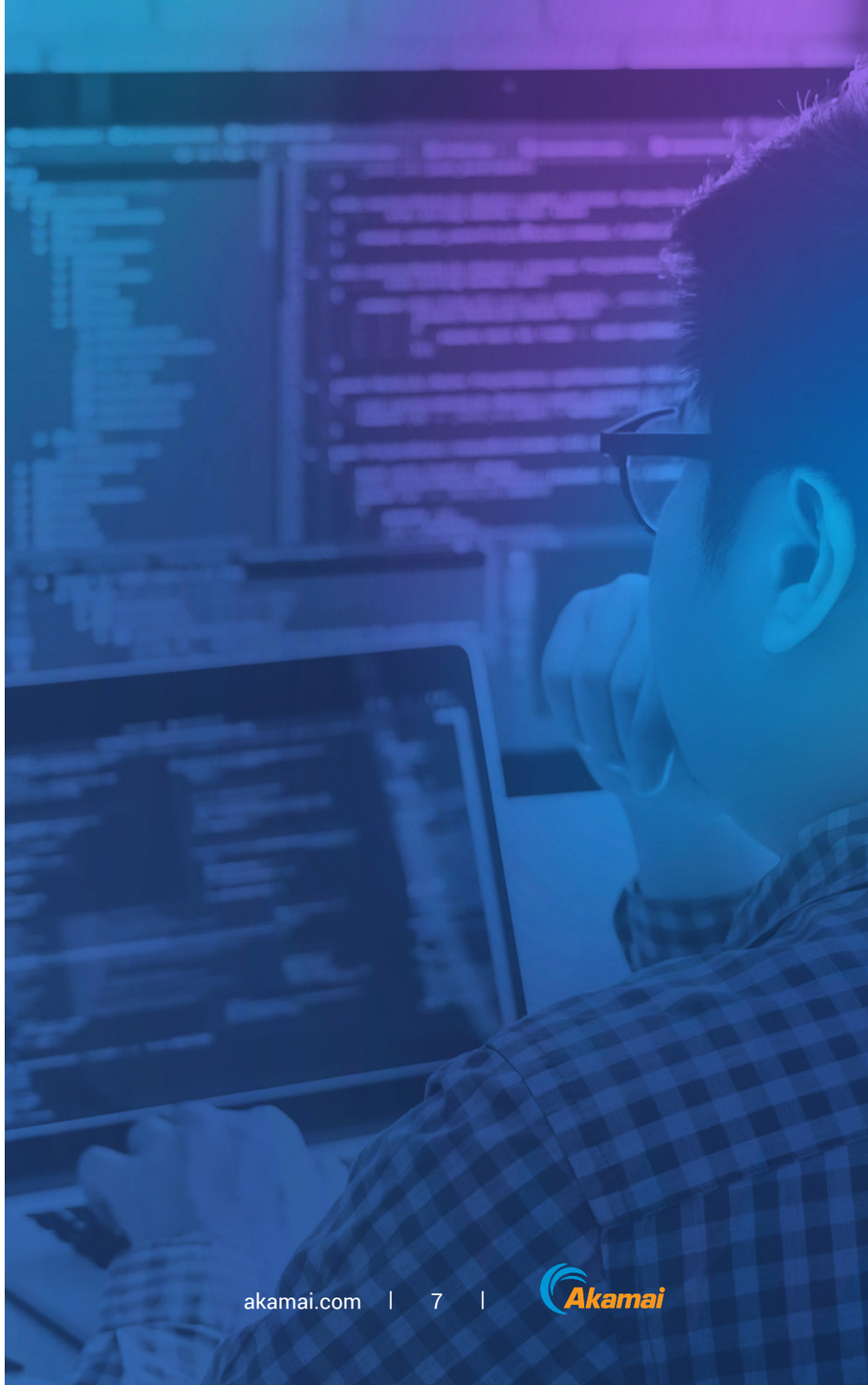
DDoS などの戦術をサービスとして利用できるため、攻撃者は DDoS 攻撃を隠れ蓑として使用し、容易にセキュリティチームを欺くことができます。そして同時に、ランサムウェア攻撃や三重脅迫型攻撃を仕掛けるのです。これらは、ランサム DDoS（RDDoS）攻撃と呼ばれます。

DDoS 攻撃による被害

ネットワーク（レイヤー 3）とトランスポート（レイヤー 4）レイヤー DDoS 攻撃の場合、大量のプロトコルベース攻撃でインターネットパイプを満杯にし、サーバーに過剰な負荷をかけ、ステートテーブルのエントリーを使い果たして、ネットワークとサービスを利用できなくします。レイヤー 7 攻撃では、Low & Slow（少しずつ時間をかけた）攻撃や HTTP フラッドなどのベクトルを通じて Web パフォーマンスとユーザー体験を妨害し、ダウンタイムを発生させ、収益に影響を与えることが狙いです。DNS への DDoS 攻撃はやや複雑です。攻撃の種類によっては、組織のネットワークのさまざまなレイヤーに影響が出る可能性があります。たとえば、DNS リフレクション攻撃と増幅 DDoS 攻撃は、企業のネットワークのレイヤー 3 と 4 でトラフィックを生成しますが、NXDOMAIN または DNS フラッドタイプの DDoS は、多くの場合、ネットワークのアプリケーションレイヤーを攻撃します。

ただし、ダウンタイムの影響は、攻撃の標的となるサービスやアプリケーションが利用できない場合のコストだけではありません。Ponemon Institute によれば、組織が被る DDoS 攻撃の平均コストは年間 170 万ドルにのぼります。その主な要因は、テクニカルサポートの増加、インシデント対応リソースの消費、社内エスカレーション、訴訟費用、業務の中断、従業員の生産性低下によるものです。さらに、金融サービス機関、ゲーム企業、メディア企業、E コマース組織などの消費者向けビジネスでは、オフラインになることで金銭的損害が発生するだけではありません。さらに重要なのは、致命的な風評被害につながる可能性があることです。

影響が甚大であることは明らかで、ハイブリッド・クラウド・インフラへの移行が増えることで、さらにその影響は大きくなります。

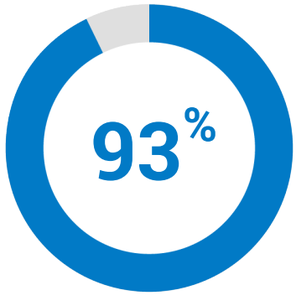


ハイブリッドとマルチクラウドはセキュリティ対策を複雑化し続けている

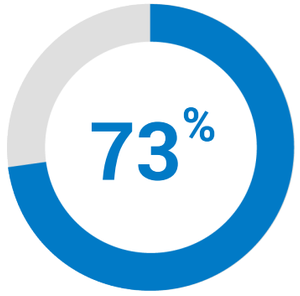
さまざまな組織が一部のワークロードをオンプレミスのデータセンターやプライベートクラウドで保持し、他のアプリケーションをパブリッククラウドのホスティング環境に移行しています。インフラに対するこのハイブリッドアプローチによって、堅牢なセキュリティを確立する作業は非常に複雑になっています。同様に、企業ではハイブリッド DNS インフラがよく使われていますが、このインフラの場合、権威 DNS ゾーンの一部がクラウドで管理され、残りのゾーンはオンプレミスのネームサーバーとグローバル・サーバー・ロード・バランサー（GSLB）によって管理されています。組織が一部のオンプレミス DNS インフラを維持し続ける理由はいくつかあります。たとえば、コンプライアンス要件を満たすために、オンプレミスインフラのセットアップに多額の資金をすでに投入している場合があります。すべての DNS をクラウドに移行する作業は複雑であり、財政的にも現実的でないことがあります。

攻撃者は、このような断片化された環境から生じる脆弱性をよく認識しています。彼らは、セキュリティポリシーや要件の一貫性のなさが原因で発生する組織のセキュリティアーキテクチャや対策の弱点につけこもうと躍起になっています。また、断片化された多様なクラウドホスティング型インフラにおけるトラブルシューティングの複雑さを巧みに利用しようとしています。

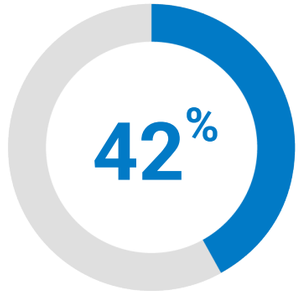
残念ながら、パブリッククラウド環境のセキュリティ対策はプロバイダーごとにまちまちです。そのため、多くの組織が誤った想定をしており、その結果、自社が危険に晒される可能性があります。たとえば、IBM が実施したアンケート調査では、エンタープライズ組織の 73% が、パブリック・クラウド・サービス・プロバイダー（CSP）が Software as a Service（SaaS）のセキュリティ確保に主な責任を負っていると回答しました。一方で、42% は、CSP が主にクラウド Infrastructure-as-a-Service（IaaS）のセキュリティ確保に責任があると回答しています。このように、セキュリティ制御の責任に対する知識不足が妥協につながる可能性があります。これはどの組織も許容すべきではないリスクです。



マルチクラウド戦略を導入している組織の割合



パブリック CSP が SaaS のセキュリティ確保に責任があると回答した組織の割合



CSP がクラウド IaaS のセキュリティ確保に責任があると回答した組織の割合

組織は、アプリケーション、API、DNS、基盤となるインフラを保護できる、拡張性と包括性に優れた統合型 DDoS 防御プラットフォームを提供する DDoS セキュリティプロバイダーに注目しています。

DDoS 緩和サービスはどれも同じとは限らない

企業がクラウドインフラへの投資を続ける中、ハイブリッド環境全体で一貫した制御を確保することがセキュリティチームにとっての課題です。そして、アプリケーションが複数のバックエンド・クラウド・インフラに展開されるのに伴い、保護することはより難しくなり、多くの組織では防御を調整するための単一の制御ポイントを求めています。

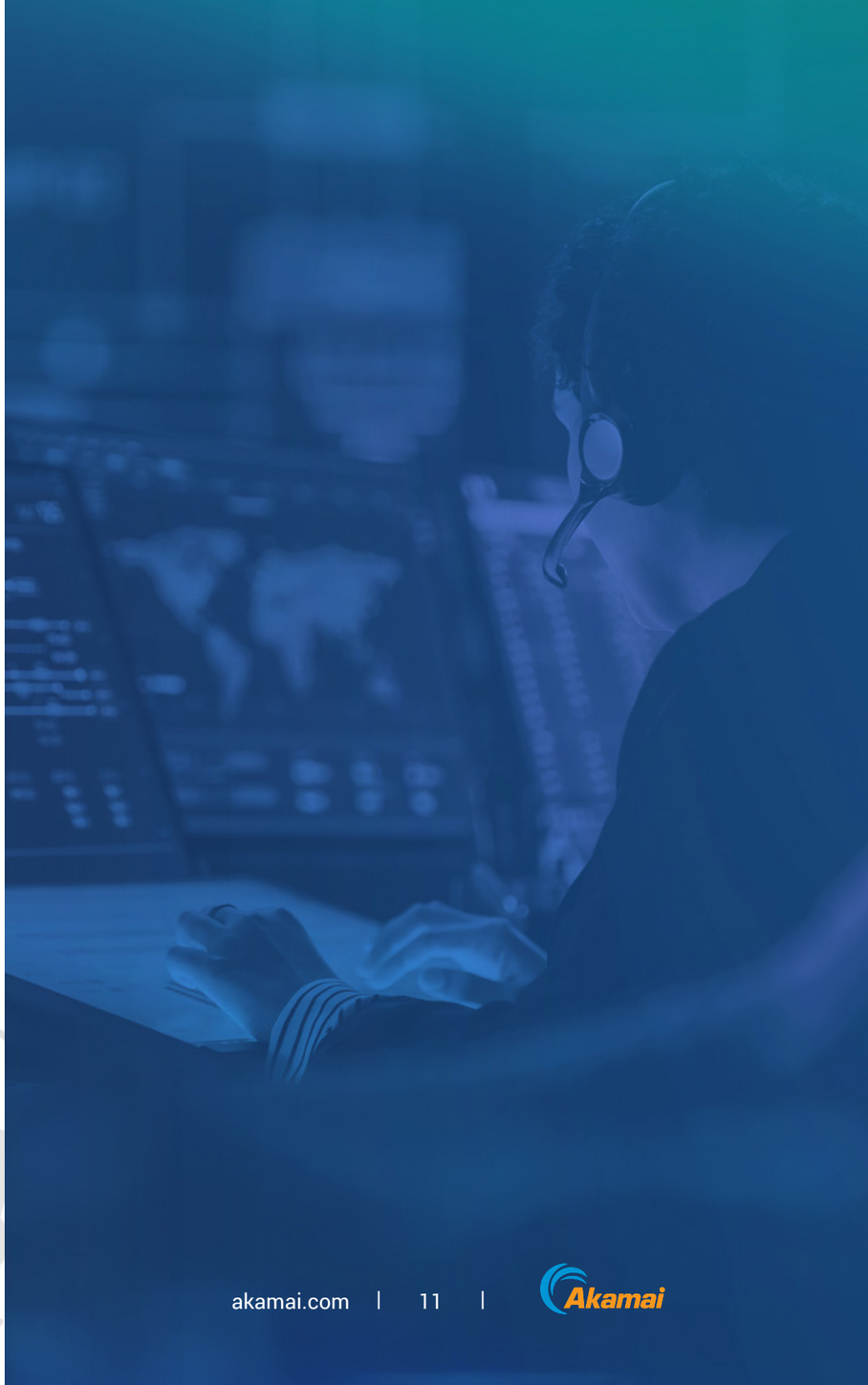
セキュリティのテクノロジースタックがより複雑化するのに伴い、環境の統合されたビューを求める声は多くなっています。それは、可視性の最適化だけでなく、API を介してイベントデータ相関システムにフィードできるレポートの作成を合理化するためでもあります。

組織は、この問題を解決するため、アプリケーション、API、DNS、基盤となるインフラを保護できる、拡張性と包括性に優れた統合型 DDoS 防御プラットフォームを提供する DDoS セキュリティプロバイダーに注目しています。組織が求めているのは、オンプレミス、クラウド、ハイブリッドなど、エンタープライズサービスの存在する環境に関係なく適用できるスケーラブルでレスポンシブな防御です。このようなソリューションが求められているのは、CSP 固有の環境で DDoS 防御を統合、展開、管理するための運用が複雑化しているためです。また、インターネットに面した資産が複数のプライベートクラウドとパブリッククラウドに数多くあるため、事態はすぐに複雑になります。

このようなプレッシャーに加え、多くの CSP の自社開発 DDoS 緩和ソリューションは、可視性、サービスレベル契約（SLA）、レポート作成という今日のエンタープライズ防御策の強化に欠かせない重要な領域の機能が十分とは言えません。

セキュリティチームにとって、インシデント対応と対策を最適化するためには、可視性と実践的な知見を得ることが非常に重要です。一部の CSP の DDoS ソリューションは、レポート作成、可視性、および攻撃後の分析に関する透明性がほとんど（またはまったく）ありません。CSP が分析とレポート作成のブラックボックスと呼ばれているのもうなずけます。一部の CSP では、組織のセキュリティチームがクライアント固有の環境に対して制御を設定し、主権を維持することを許可していますが、通常、DDoS トラフィックに対する責任をすべて拒否し、DDoS 攻撃（アプリケーションレイヤー攻撃、ネットワークレイヤー攻撃、DNS DDoS 攻撃など）に伴う膨大な量の悪性トラフィックに対して顧客に課金します。

さらに、CSP やセキュリティベンダーの中には緩和所要時間（TTM）SLA を提供せず、その代わりに影響を受けた組織にサービスクレジットを付与しているところもあります。TTM の条項に攻撃を特定する時間が含まれているかどうかを理解することが重要です。緩和プロトコルが開始する前にプラットフォームが DDoS 攻撃を識別するのに数分さらには数時間もかかる場合、被害を受けた組織は長時間オフライン状態が続く可能性があるからです。一刻を争う対応が重要な場合、組織にはプロバイダーがパフォーマンスの低下を招くことなくアップタイムと可用性の維持を約束するという確証が必要です。



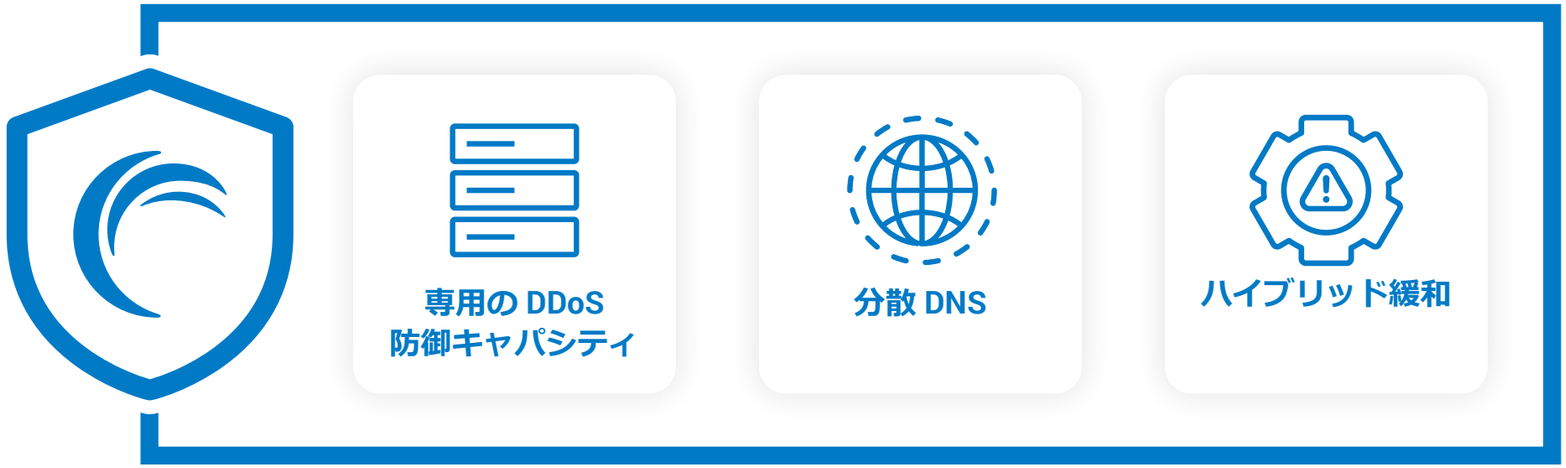
さらに、セキュリティチームやバイヤー組織にとって、DDoS セキュリティベンダーや CSP が**専用の DDoS 防御キャパシティ**を提供しているのか、それとも防御キャパシティが CDN ネットワークと共有されているのかを確認することも、同様に（あるいは、もっと）重要です。専用の DDoS 防御は、SWAT チームのようなものです。DDoS 攻撃への対処に集中し、ビジネスの他の側面（コンテンツ配信など）とリソースやインフラを共有しないため、記録的な DDoS 攻撃が発生しても影響を最小限に抑制できます。DDoS 防御を評価中の組織は、ベンダー自身が DDoS 攻撃を受ける場合があることを理解し、ベンダーがアップタイム／可用性 SLA を提供しているかどうかをしっかり確認する必要があります。

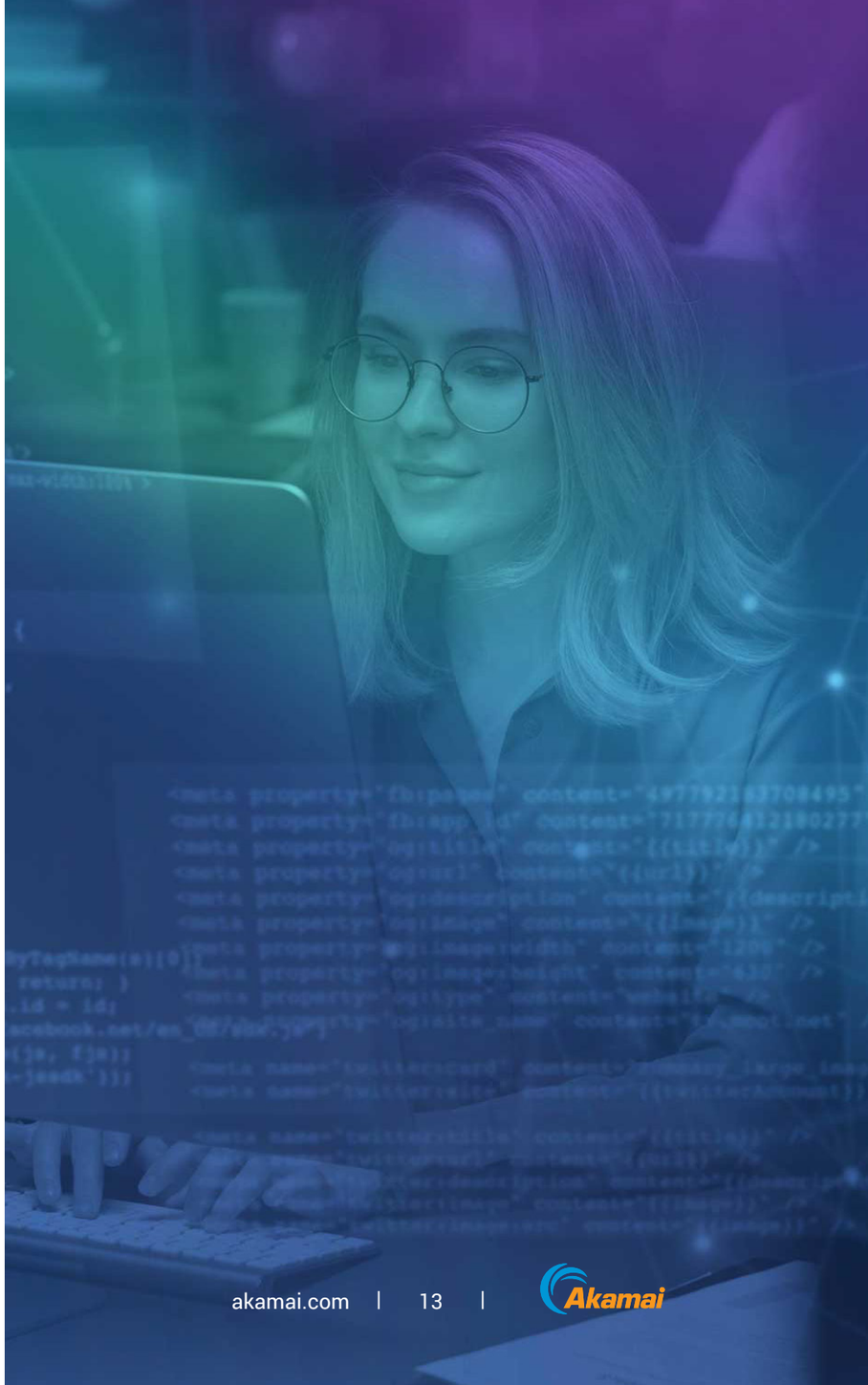
最後に、CSP やセキュリティベンダーの多くは、攻撃前、攻撃中、攻撃後の支援も、24 時間体制のグローバルなセキュリティ・オペレーション・センター（SOC）サポートをオンデマンドで利用できるサービスも提供していません。もし提供しているとしても、それはプレミアムサービスとして提供され、多くの場合、クラス最高レベルのプロバイダーが提供する専門のハイブリッド DDoS 緩和ソリューションより費用がかかります。フルマネージド型のハイブリッド DDoS 防御ソリューションの場合、サービスプロバイダーは企業や組織のインシデント対応チームの一部として機能し、DDoS イベントにすばやく対応するための専門知識を提供します。

現在の脅威環境では、先進的な企業は、ハイブリッド環境全体にわたって合理化されたセキュリティ体験を提供し、アタックサーフェスの複雑さを軽減する DDoS 緩和パートナーを選択しています。DDoS 防御パートナーを選択する際には、貴社のハイブリッド戦略、マルチクラウド戦略、ビジネス目標を妨げるのではなく、後押ししてくれるパートナーを選ぶことが重要です。

Akamai による専用の DDoS 緩和

組織は、ハイブリッド環境とマルチクラウド環境を含むエンドツーエンドのデジタルインフラ戦略を必要としています。同様に、エンドツーエンドの DDoS 防御も考慮する必要があります。Akamai は包括的なアプローチを取ることで、防御の最前線として機能し、専用のエッジ、分散 DNS、巻き添え被害や Single Points of Failure を防ぐように設計されたハイブリッド緩和戦略で防御します。他の CSP に見られる「オールインワン」ソリューションとして構築されたアーキテクチャとは異なり、Akamai の専用 DDoS ソリューションは増強された耐障害性、専用の DDoS 防御キャパシティ、そして Web アプリケーションやインターネットベースのサービスの特定の要件にもきめ細かく調整できる高品質の緩和機能を備えています。Akamai の DDoS 防御は、オンプレミス、クラウド、ハイブリッドなど、必要な場所で Always-on またはオンデマンドで利用できます。この包括的な保護を実現するのが、Akamai の 3 つの主要製品です。





Akamai Prolexic は、組織の事前対応型のポジティブセキュリティ対策に合わせて設計された世界クラスの DDoS 防御

最新のスケーラブルなアーキテクチャ

Akamai Prolexic は、エッジコンピューティング、5G/6G、ネットワーク仮想化に関するネットワークトレンドの変化に対応できる完全なソフトウェア定義アーキテクチャを使用しています。仮想化されたソフトウェア環境への移行により、Prolexic は専用ハードウェアへの依存を完全に排除しました。この展開の標準化により、Akamai はお客様の進化するニーズにより迅速に対応できるようになり、モジュラー展開を促進してキャパシティを拡張しました。また、低レイテンシーリンクで地域カバレッジを強化し、プラットフォームの冗長性を改善しました。さらに、このアーキテクチャは Prolexic の高度なふるまい学習機能を高速化して、攻撃シグネチャーから学習し、新たな脅威ベクトルに適応し、DDoS に強い体制をプロアクティブに構築します。Prolexic Cloud は、**世界 32 都市に複数のスクラビングセンターを配置しており、計 20 Tbps を超える専用防御キャパシティを備えています**。Prolexic の防御キャパシティをわかりやすく説明すると、最大規模の既知のレイヤー 3 DDoS 攻撃やレイヤー 4 DDoS 攻撃であっても、Prolexic の顧客が利用できるキャパシティの 10% にも及びません。

柔軟性と信頼性に優れた、包括的な DDoS 防御

Akamai Prolexic には、Prolexic Cloud、Prolexic On-Prem、Prolexic Hybrid があります。

Prolexic Cloud は、クラウドベースの DDoS 防御として業界でも先駆的な製品です。ゼロ秒緩和を実現し、100% のプラットフォーム可用性を保証する SLA を提供します。緩和制御により容量を動的にスケーリングすることで、IPv4 および IPv6 のトラフィックフロー全体の攻撃を阻止します。どのような緩和制御のスケールアップが必要になっても、コンピューティングリソースを動的に割り当てることができます。

Prolexic On-Prem は、物理的または論理的な、インラインのデータパス DDoS 防御を Always-on で提供します。エッジルーターとネイティブに統合されており、トラフィックバックホールを必要とせずに顧客のネットワークのエッジで 98% 以上の攻撃を自動的に阻止します。大部分の小規模で高速な攻撃や、超低レイテンシーの DDoS 防御を必要とする企業に最適です。

Prolexic Hybrid は、Prolexic On-Prem のパワー、自動化、パフォーマンスを、業界屈指の Prolexic Cloud のスケールとキャパシティにオンデマンドで統合し、最大規模の DDoS 攻撃から顧客のオリジンを守ります。

DDoS を超えるセキュリティ

Akamai Prolexic には Prolexic Network Cloud Firewall が追加されています。この完全セルフサービスかつユーザー設定可能な機能を利用することにより、独自のアクセス・コントロール・リスト（ACL）とネットワークのエッジで適用するルールを簡単に定義、展開、管理できるようになります。 これは、他のすべてのファイアウォールの前に配置されるファイアウォールです。また、Network Cloud Firewall は、Akamai の脅威インテリジェンスデータに基づいた最適な事前対応型の防御体制を実現するための ACL を推奨し、既存のルールの実用的な分析を提供します。Network Cloud Firewall は、次世代の「サービスとしてのファイアウォール」として、次のことを行えるよう支援します。

- 事前対応型の防御を定義し、悪性のトラフィックを即座にブロックする
- ルールをエッジに移動することで、ローカルインフラを軽減する
- 新しいユーザーインターフェースでネットワークの変更に迅速に適応する

Akamai Edge DNS と Akamai Shield NS53 は、重要な DNS インフラのセキュリティを確保し、強化する

Akamai Edge DNS は、オンプレミス、クラウド、ハイブリッドのいずれの環境であっても、DNS インフラに対するさまざまな DNS 攻撃から包括的に保護します。また、高レベルの DNS パフォーマンス、回復力、可用性も提供します。世界中に分散された Anycast ネットワーク上に構築されているため、Edge DNS をプライマリまたはセカンダリ DNS サービスとして実装し、必要に応じて既存の DNS インフラの代替とすることも、補助として追加することもできます。

Akamai Shield NS53 は、オンプレミスとハイブリッドの DNS インフラ（GSLB、ファイアウォール、ネームサーバーなど）を DNS リソース枯渇（NXDOMAIN）攻撃から保護する双方向 DNS リバース・プロキシ・ソリューションです。独自の動的セキュリティポリシーの自己設定、管理、適用をリアルタイムで行えます。不正な DNS クエリーと DNS 攻撃フラッドを Akamai ネットワークのエッジで阻止して、重要な DNS インフラを DNS DDoS 攻撃から保護します。

Akamai App & API Protector は、DDoS 攻撃からアプリケーションと API を保護する

市場トップクラスの Web アプリケーションおよび API 保護（WAAP）ソリューションとして認められている App & API Protector は、ネットワークレイヤーの DDoS 攻撃を（Akamai Connected Cloud でホストされているプロパティの）エッジで直ちに阻止し、アプリケーションレイヤーの DDoS 攻撃に対する徹底的な防御戦略を提供します。

Akamai を選ぶ理由

Akamai は、世界で最も信頼されているグローバル DDoS 緩和ソリューションを提供しています。保護する対象が個々のアプリケーション、データセンター全体、重要な DNS インフラのいずれであっても、最大のキャパシティ、最強の回復力、最速の緩和を念頭に置いて設計された Akamai の DDoS 緩和ソリューションで対応できます。

私たちはこれまで、世界で発生した最大規模の DDoS 攻撃のいくつかを緩和してきました。Akamai は、事前対応型の緩和制御により、文字通りのゼロ秒緩和と、業界をリードする SLA を提供しています。また、複数のクライアント向けに複数の DDoS 攻撃を同時に阻止する DDoS 防御サービスも提供しています。

DDoS 攻撃ベクトルは変化し続け、攻撃規模も大きくなり続けているため、信頼できる DDoS プラットフォームは脅威をプロアクティブに検知し、緩和戦略を調整し、影響を最小限に抑えるための機能を継続的に刷新、開発、展開する必要があります。Akamai は、攻撃が開始する前に緩和することで、脅威に先手を打つことに専念しています。

DDoS 緩和戦略は、ハイブリッドおよびマルチクラウド戦略を強化するものでなければなりません。Akamai の次世代 DDoS ソリューションは、貴社のデジタル・ネットワーク・インフラ、アプリケーション、DNS を、オンプレミス、クラウド、またはその両方において保護します。さらに、機械の知能と人間の知能、両方を組み合わせたメリットを提供します。

さらに詳しく

 | サポート | | 公開日：2024 年 10 月