IDC MarketScape

IDC MarketScape: Worldwide Web Application and API Protection Enterprise Platforms 2024 Vendor Assessment (Japanese)

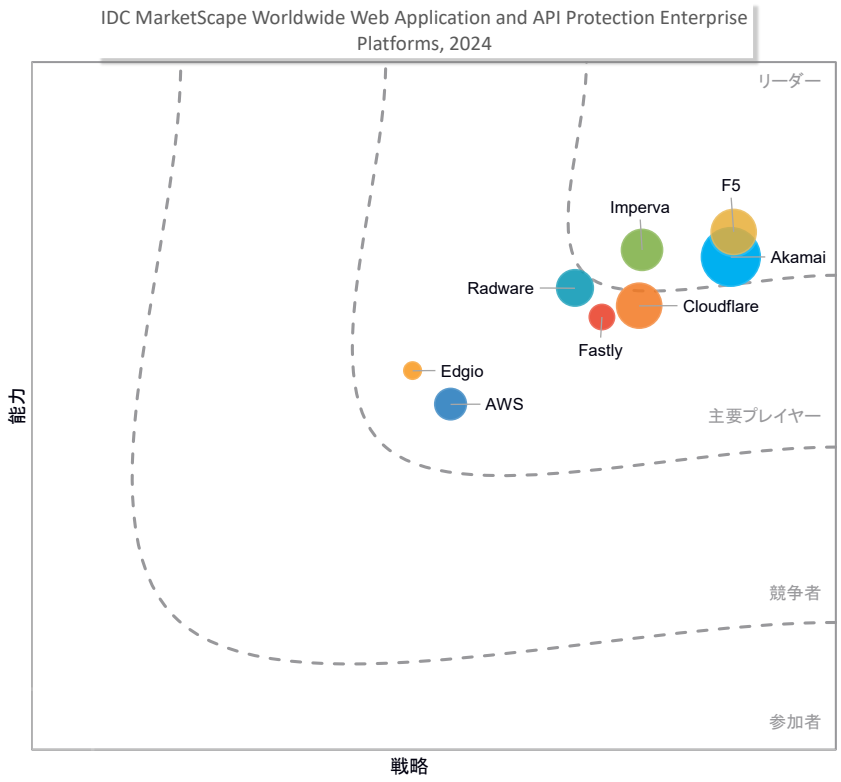
Christopher Rodriguez

THIS IDC MARKETSCAPE EXCERPT FEATURES AKAMAI

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Web Application and API Protection Enterprise Platforms Vendor Assessment



Source: IDC, 2024

September 2024, IDC #US51795524e

調査方法、市場定義、ベンダーの評価基準については、「補遺」セクションを参照のこと。

調査概要

本 IDC MarketScape Excerpt は、『IDC MarketScape: Worldwide Web Application and API Protection Enterprise Platforms 2024 Vendor Assessment（IDC #US51795524）』からの抜粋である。本調査レポートには、Figure 1 および 2 に加え、「IDC の見解」「IDC MarketScape における評価対象ベンダー選定基準」「テクノロジーバイヤーへの提言」「ベンダープロファイル（要約）」「補遺」「参考資料」のセクションの内容、またはその一部が含まれる。

IDC の見解

Web アプリケーションは、最新のデジタルビジネスの基礎的な構成要素であり、顧客や見込み客、パートナーやゲスト、従業員や請負業者とのやり取りに必要な機能を提供する。攻撃者は、これらのアプリケーションや関連する API（Application Programming Interface）を常に調査し、自己の不正な利益を得るためにデータの窃盗、不正アクセス、企業への詐欺行為の機会を狙っている。Web アプリケーションや API を標的とした攻撃は、重大なデータ漏洩や多額の損失を生じるシステム中断、および盗難など実世界への影響を招いてきた。エンドユーザーや顧客は、多くの場合、直接的に金銭的損失を被る。最終的には、顧客の信頼を失い、顧客がオンラインでの取引を控える可能性もある。

オンライン上のサイバー犯罪は、単なる迷惑行為に留まらず、ビジネス成果の低下や損失を招く可能性がある。長年に渡り、企業は次々と現れる新たな脅威の戦術や拡大する攻撃対象領域に対処するために、数多くのセキュリティツールを採用してきた。WAF（Web Application Firewall）は、既知および新しいアプリケーション層の攻撃に対し、基本レベルの保護を提供する。企業は、DDoS（Distributed Denial of Service）による影響の緩和、ボット対策、そして最近では API セキュリティなど、数多くの特定のソリューションを積み重ねてきた。

WAAP（Web Application and API Protection：Web アプリケーションと API の保護）は、これらの重要なセキュリティテクノロジーを組み合わせ、一貫性のあるプラットフォームに統合し、広範なオンライン脅威に対する信頼度の高い保護を確保する。融合かつ統合されたプラットフォームは、セキュリティギャップの縮小、管理における複雑性の低減、検査の合理化に役立つ。事実、IDC の調査では、企業の 77%がセキュリティソリューションの統合を「重要」または「極めて重要」と評価している。また、アプリケーションは、日々さまざまな脅威にさらされており、攻撃者は防御の弱点を見極めるために、複数の戦術の相乗効果を得ようとしている。その結果、特定のセキュリティサイロに焦点を合わせたアプリケーションのセキュリティ戦略では、最終的に失敗に終わる。検出精度の向上、

誤検出の減少、高度なゼロデイ攻撃の確実な検出などいずれの方法であれ、セキュリティの集約と融合は、より強固なセキュリティ体制を実現するための必須のステップである。

その一方で、集約は配備や管理に必要な時間とリソースの削減、ユーザーエクスペリエンスの向上、より良い分析など、多くのビジネス上の利点ももたらす。さらに、すべてのセキュリティ機能を一つのサービスで実行すると、複数のセキュリティ検査の実施箇所へトラフィックを回送することによる遅延も削減できる。

同時に、企業はアプリケーション保護技術の全面的な導入に当たり、必要に応じて、あるいは時間やリソースが許す範囲で段階的に進め、慎重なアプローチを取らなければならない。顧客にとって、モジュール式の統合プラットフォームは、時間をかけて容易に WAAP を導入するために不可欠である。ベンダーにとっての課題は、さまざまな製品グレードに含まれるべき、中核的なセキュリティ機能分野で統合の対象となる機能の適切な組み合せを設計することである。

WAF はセキュリティにおいて基礎的な構成要素である一方で、一貫した API 戦略がなければ最新のアプリケーション保護は不可能である。いまや API は、現代のデジタルビジネス時代において重要な役割を果たし、アプリケーションを統合するプロセスを合理化および効率化し、強力な新規機能を実現しているのである。その一方で、API はこれまでにない形で攻撃対象領域を変化させている。API は、誤設定、機密データの露出、DoS（Denial of Service）攻撃に対して脆弱である。さらに重要なことに、API はユーザーインターフェースを標的とする攻撃と同じ攻撃の多くに対して脆弱であるだけでなく、BOLA（Broken Object-Level Authorization：オブジェクトレベル認可の不備）といった API 特有の脅威をもたらす。また API は、WAF のような境界保護ソリューションを超えられないアプリケーション間の通信を可能にする手段を提供する。その結果、セキュリティの盲点が生じ、攻撃者はこれを悪用して、ネットワークベースの防御の背後で横方向に移動できるようになる。

WAF と API セキュリティを組み合わせることは、すべてのインターフェースと攻撃対象領域に渡って Web アプリケーションを完全に保護するために必須である。WAAP の提供価値は、DDoS 攻撃や迷惑ボットの活動など、特定の脅威に対処するように設計されたテクノロジーが補完し完成させているのである。これらの脅威は、検出しやすさ、緩和の難しさ、発生頻度、影響の深刻度の観点で見ると、非常に多様である。そのため、完全なアプリケーション保護スタックには最終的に、WAF と API セキュリティ、DDoS 緩和、ボット管理が必要である。しかし、API に固有の技術的要件と、DDoS 攻撃やボットの活動に特有の要件を考慮すると、WAAP への進化は長く困難な道のりとなる。

IDC MARKETSCAPE における評価対象ベンダー選定基準

WAAP は実行中のアプリケーションの保護を目的とする集約されたセキュリティソリューションであり、WAF を中核としている。IDC は、WAAP エンタープライズプラットフォームに関する本 IDC MarketScape 分析の対象となるには、ソリューションに本セクションで取り上げた重要な属性が必要であるとしている。

ベンダーは、以下のうち 2 つ以上を統一セキュリティプラットフォームに組み合わせ、集約された WAAP ソリューションを提供しなければならない。

- API セキュリティ
- ボット管理
- DDoS 緩和
- WAF

WAF は基礎をなすと考えられるため、WAAP と認められるためには WAF が含まれていなければならないことに留意していただきたい。さらに、WAAP コンポーネントをスタンドアロンソリューションとして 1 回の取引で買い切りの形で販売している場合も、WAAP とは認めない。

また、本 IDC MarketScape の分析には、市場参入とプレゼンスに関する以下の要件が含まれる。

- **市場参入：** ベンダーは 2023 年時点で、必須の WAAP 機能を統一ソリューションとして提供していた。特定の中核的な機能または拡張機能は、スタンドアロンまたは別製品としてのみ販売されるものではない限り、異なるバンドルまたはプラットフォームの一部として、あるいはスタンドアロンソリューションとして提供される場合がある。必須機能およびオプション機能の完全かつ詳細な説明については、「市場定義」のセクションを参照のこと。
- **市場の代表性：**ベンダーは、IDC の Security Products Tracker で確認できる通り、2023 年の WAAP 競合市場において、収益のシェア確立で最低要件を満たしている。
- **グローバルプレゼンス：** ベンダーは、IDC の Security Products Tracker で確認できる通り、2024 年時点で、北米、中南米、EMEA、アジア太平洋地域などの各主要グローバル地域において、収益分配で最低要件を満たしている。

WAAP のコンポーネントを提供するクラウドおよびセキュリティプロバイダーの一部が、統合された WAAP アプローチではなく、ポイント製品に焦点を合わせているため、今回の分析には含まれないことを IDC は指摘する。同様に、WAAP を提供する一部のベンダーは、市場の代表性やグローバルプレゼンスの最低要件を満たしていなかった。

ベンダーの能力に関する主要な検討事項

WAAP エンタープライズプラットフォームに関する IDC MarketScape の分析では、IT バイヤーが必要とし、期待する一般的なレベルの保護と共に、統合の程度、使いやすさ、周辺の専門的サービスおよびマネージドサービス、TCO（Total Cost of Ownership：総所有コスト）を考慮している。エンタープライズレベルでは、WAAP は優れた保護を提供し、セキュリティがパフォーマンスに与える影響を低減し、エンドユーザーのエクスペリエンスに与える摩擦を最小限にしなければならない。また、この分析では、一つに統合された一貫したプラットフォームに、複数の不可欠なセキュリティテクノロジーを組み合わせるという、WAAP の主要な目的も重視している。広範なオンライン脅威に対する一貫した保護のニーズとビジネス価値のニーズを最大限に支援する形で WAAP の導入を可能にするには、拡張性と多様な価格モデルの提供も必要である。

ユーザーの期待は高まる一方で、企業は革新的で快適なユーザーエクスペリエンスを提供するために、新しいテクノロジーを今後も採用する。アプリケーションは複雑な分散型インフラストラクチャへの依存をますます強めるばかりである。DevOps チームはより迅速かつ効率的に作業し、新しい機能をいち早く市場に投入しようとしている。企業は、特定の製品や機能に特化した能力について、ベンダーがネイティブに提供しているか、ソリューションにデフォルトで含まれているか、あるいはファーストパーティのアドオン機能や別の製品など他の手段を通じて、またはサードパーティの OEM や技術統合を通じて提供されているか否か、いっそう留意すべきである。さらに、以下の事項についても考慮すべきである。

- **Client-Side WAF（CSWAF）**：CSWAF は、Client-Side Protection とも呼ばれ、エンドユーザーのデバイス上で実行される Web アプリケーションコードという特定の脅威ベクトルに対処するために設計された新しいセキュリティテクノロジーである。このコードには、Web サーバーではなくデバイス上でさまざまな機能を実行するためにブラウザー内で実行されるスクリプト（簡易プログラム）が含まれる。
- **詐欺／不正防止**：オンライン詐欺および不正防止能力は、通常、アカウント乗っ取りや新規アカウント詐欺（偽アカウント詐欺とも呼ばれる）など、特定の詐欺行為を示す固有のパターンに対処するために特別に調整されたボットへの対処能力に根ざしている。正常に機能しているアプリケーションと API の不正利用を示す詐欺やその他の行為を完全に検出するには、ユーザーID、クライアントおよびデバイスレベルのテレメトリー（遠隔測定）、ユーザーの行動に関するインサイトが必要である。結果として、詐欺の検出能力、およびこれらの能力がどのようにパッケージ化され、バイヤーに販売されているかに関して、WAAP ソリューションの間には大きな違いがある。

- **住宅用プロキシ：** WAAP ソリューションにおける、住宅用プロキシや、IP ローテーションなどその他の偽装手法の背後に隠れている攻撃者に対する検出能力には、製品ごとの差異がある。
- **WebSocket**：全二重接続によるリアルタイム通信を可能にするプロトコルであり、WebSocket を利用するアプリケーションのサポートが含まれる。オンラインユーザーがインタラクティブでリアルタイムのアプリケーションを求めるにつれ、WebSocket のサポートはますます重要になっている。
- **WebAssembly（WASM）**：ポータブルなバイナリーコード形式を提供する低級言語である。これまで WASM の主な利点は、幅広い開発言語を容易にサポートできることであった。WASM の採用が増えるにつれ、WAAP におけるサポートの重要性が高まっている。
- **RASP（Runtime Application Self-Protection）**：アプリケーションのランタイム環境を保護し、データ入力を監視して攻撃を特定、検出、防止する高度なセキュリティ機能である。RASP は、配備の複雑性やパフォーマンスへの影響に関する想定が適切に理解されている場合、アプリケーションのセキュリティを徹底する上で有効な選択肢になり得る。
- **PAT（Private Access Token：個人用アクセストークン）**：Apple やその他のテクノロジー企業は、エンドユーザーのプライバシーに対する関心を高めており、個人を特定できる詳細情報を開示することなく、アクセス要求元のデバイスの真正性と信頼性を証明する方法を提供している。Apple PAT の WAAP のサポートは、ユーザーエクスペリエンスに摩擦や不確実性をもたらす CAPTCHA やその他のボット検出技術への依存を低減する上で役立つ可能性がある。Apple PAT は、機密性の高い PII（Personally Identifiable Information：個人識別用情報）を公開することなく、選択された関係者間でユーザーのデータの共有や処理を可能にするプライバシー保護技術を推進する業界全体の取り組みの一環である。
- **自動化：** アップデートの自動化は、使いやすさを向上し、ビジネス価値を高める。
- **シミュレーションテスト：**本番環境への導入に先立って、ルールの更新をテストできる。シミュレーションテストは、実際のトラフィックで実行できる場合に最も効果的である。
- **eBPF**：サンドボックス化されたプログラムをオペレーティングシステムのカーネル内で実行できる Linux の機能である。特にクラウドネイティブ環境におけるセキュリティのオブザーバビリティの向上に大きく影響する。

戦略の検討事項

加えて、Web アプリケーションおよび API テクノロジーの急速な進化、ビジネス慣行の変化、脅威アクターによる一定水準の適応と革新を考慮すると、セキュリティバイヤーは、今後 3〜5 年間に渡ってニーズを満たすソリューションの能力を十分に認識する必要がある。さらに、以下の事項についても考慮すべきである。

- **検出の攪乱：**サイバー犯罪者は、データや製品を盗み、詐欺を働き、企業への嫌がらせや恐喝を行おうと、ますます大胆になっている。高度なツールや巧妙な戦術は、通常、利益の高い標的に対してのみ使用される。セキュリティ企業が攻撃を特定し、防止すると、サイバー犯罪者はそれに適応するプロセスを開始する。WAAP プロバイダーは、自社の対策の長期的な有効性を確保するに当たり、検出の性質について秘匿性を高めるために多大な投資を行うべきである。さらに、最も生産的な戦略は、攻撃の検知を攻撃者自身に認識させず、リソースを消耗させることであり、攻撃者にサイバー攻撃ツールの開発プロセスを完了させないためのデセプションテクノロジーの利用など、高度なボットおよび詐欺への対策が関心を集めている。
- **プラットフォーム化：** 業界は、複雑性を軽減したプラットフォームによって再構築されつつある。このようなプラットフォームは、独自に技術開発を行う必要がないシンプルなユーザーインターフェースを通じて、専門的な機能を提供する。たとえば、Shopify は、オンラインビジネスの新規立ち上げプロセスを簡素化する e コマースプラットフォームである。顧客情報、在庫、支払い処理などの機能は、すべて揃った、ターンキーの（直ちに利用可能な）SaaS（Software as a Service）として提供される。基本的な WAF や DDoS 防御などのセキュリティは、プラットフォームの組み込み機能として実装されている。こうしたことによって WAAP ソリューションに対するバイヤーのニーズや期待は変化し、ベンダーには戦略的な適応が求められることになる。
- **「シフトレフト」戦略：** ソフトウェア開発ライフサイクルのセキュリティテストやセキュリティ対策を早期に実施する必要性があるのは、今に始まったことではない。本番環境でのリリース前に脆弱性を検出することで、攻撃者が脆弱性を発見し、悪用する機会を常に排除できる。早期の検出と修正は、より効率的で費用対効果も高い。近年、シフトレフトという概念が登場し、従来は本番環境でのリリース後に使用していたツールを開発ツールやワークフローに統合することで、これらの理想を実現した。たとえば、API を使用して DAST（Dynamic Application Security Testing：動的アプリケーションセキュリティテスト）を実行すれば、DevOps チームは脅威を迅速かつ容易に発見し、修正できる。さらに、DevOps チームがより迅速に作業を行い、マイクロサービス、組み換え可能なコード、IaC（Infrastructure as Code）などの手段を活用して開発サイクルを短縮するにつれ、「シフトレフト」戦略を支援する必要性は避けられないものになる。
- **ペルソナの変化：**プラットフォーム化のトレンド、「シフトレフト」戦略、広範なセキュリティ意識の高まり（全員がセキュリティに責任を負う）が、バイヤーや意思決定者の変化を促しており、開発者、クラウドおよびネットワークチーム、さらには事業部門のバイヤーも WAAP の購入プロセスに関与している。WAAP ベンダーは、幅広いバイヤーや意思決定者に、より優れた支援を行うために、簡素化、自動化、追加設定不要の強力な保護、市場教育にますます投資する必要がある。
- **Generative AI（生成系 AI：以下、GenAI）：** GenAI の導入によって、このテクノロジーがビジネス環境にもたらし得る新たなリスクが懸念されるようになった。IDC

のバイヤー調査では、その結果として、企業はアプリケーションのセキュリティ予算を増やす必要性を検討していることが分かった。以下のような多様な要素に渡る、GenAI に関連する潜在的なリスクに対する注意および計画は、WAAP ベンダー間で大きな違いがある。

- GenAI を活用し、防御をより効果的に回避する新たな潜在的脅威
- 新しいテクノロジーの潜在的な用途（GenAI によるボット活動の低減、ボット操作の遅延や妨害、ターピットなど）
- アプリケーション戦略において LLM（Large Language Models：大規模言語モデル）能力を構築、またはサードパーティの LLM を活用する上で、専門的な機能や製品を配備する必要性、あるいは既存の防御に依存する可能性
- セキュリティ運用の効率と生産性の向上における GenAI の潜在的な用途
- セキュリティ検出の向上における AI の潜在的な用途

全体として、WAAP の定義で必要とされる、あるいは暗示される機能の圧倒的な幅広さにもかかわらず、本 IDC MarketScape で検討されたソリューションは高度な能力を備えていることに IDC は注目した。WAAP の定義は、新しいテクノロジーや脅威の変化に伴い、今後も変化することが予測される。一部の機能領域では改善の余地が残されており、ベンダーは広範なロードマップを策定している。特定のユースケースや例外的な要件では、専門性の高いポイント型製品が必要になる場合もあるものの、WAAP ベンダーは、強力なアプリケーション保護とパフォーマンスを確保するために必要な高度な機能を備えた、完全かつ強力なプラットフォームの実現に向けて大きく前進している。

ベンダープロファイル（要約）

本セクションでは、IDC MarketScape におけるベンダーのポジションを判断する上で決め手となった IDC の所見を簡潔に記述する。各ベンダーは、「補遺」のセクションに示す基準に沿って評価されるが、ここではベンダーの強みや課題を述べる。

Akamai

Akamai は、『2024 IDC MarketScape for worldwide WAAP enterprise platforms』においてリーダー（Leader）として位置づけられている。

Akamai は、分散型エッジおよびクラウドプラットフォームである Akamai Connected Cloud から提供されるネットワーキングおよびセキュリティの世界的プロバイダーであるため、アプリケーションやその使い勝手をユーザーの希望に近づけ、脅威を遠ざける。Akamai はエンタープライズ市場に特化しており、Fortune 500 に名を連ねる企業への普及率が高い。Akamai のセキュリティポートフォリオには、App & API Protector（AAP）と呼ばれる統合型 WAAP ソリューションを始め、API セキュリティ、DDoS 緩和、ボット管理、アカウント保護、WAF、クライアント側の保護およびコンプライアンス、DNS、ブランド保護などのカテゴリーに特化したソリューションがある。Akamai は、ZTNA、マイク

ロセグメンテーション、DNS ファイアウォール、脅威ハンティング、MFA などのソリューションによって、エンタープライズセキュリティの分野にも進出している。

強み

能力

- Adaptive Security Engine（ASE）は、初期設定のルールを信頼して使用できるようにするセルフチューニングを提供する。ASE はゼロデイ攻撃に対する、より優れた保護を提供し、検出を向上させ（Akamai によると 2 倍）、誤検知を低減し（Akamai によると最大 5 分の 1）、自動更新によって継続的な使いやすさを実現する。ASE は Akamai のセキュリティインテリジェンスによって強化されている。
- より容易または迅速に誤検知を修正するために誤検知のフラグを立てる。Akamai は 1 日で 50%、1 週間で 75%の誤検知を削減すると断言している。
- 包括的な WAAP スイートは、簡素化された完全なセキュリティの購買手続きをワンストップで提供する。WAAP の SKU は 1 つであり、高度または専門的な機能が必要な場合はアドオンが提供される。
- 幅広いアドオンと専門的なソリューションによって、ATO、ブランド保護、スクレイパー（過剰なイベント）保護など、ユースケース特有の要件に対応する。
- Akamai は非常に大規模なエッジ／CDN（Contents Delivery Network）インフラストラクチャを提供している。ユーザーの近くで保護を提供することで、パフォーマンスを確保する。
- DevOps ワークフローのサポートによって、シフトレフト戦略に関してエンタープライズの顧客を支援する。API、CLI（Command Line Interface）、Terraform を通じて管理と配備を支援することで、開発者の作業を遅延させることなくセキュリティ体制を強化する。
- 関連セキュリティツールとすでに統合しているため、セキュリティ成果の向上に向けた、より広範なセキュリティアーキテクチャとの統合が容易である。そうしたソリューションには、Splunk、Qradar、ArcSight の事前構築済みのコネクターなどがある。
- API セキュリティにはマルチモードアプローチが提供される。このアプローチでは、プラットフォームにおける既知の API トラフィックの保護が初期設定されており、必要に応じて、後から API 保護を完了させる。
- WAAP と共に広範な追加の関連能力が提供されるため、セキュリティがパフォーマンスの妨げにならないことが保証される。このポートフォリオには、SiteShield、mPulse Lite、EdgeWorkers、Image & Video Manager、API Acceleration などのソリューションが含まれている。
- Akamai はアプリケーション層における DDoS 緩和のために、詳細な文脈上の手がかりに基づく「短時間バーストの検出」やカスタマイズ可能なレート制限といっ

た、新しい能力を最近発表した。これらは、アプリケーション層における攻撃に特有のニーズなど、あらゆる DDoS 攻撃に対応する。

- セキュリティテレメトリーの統一されたビューを搭載し、ドリルダウン能力を備えた広範なセキュリティ分析、可視性を提供している。Web Security Analytics は、すべてのアプリケーション向けセキュリティ製品に含まれている。
- 評価モードでは、変更を実行する前に、実際のトラフィックに基づいてルール変更の影響を確認する機会が与えられる。この機能によって、本番トラフィックに未知の影響を及ぼすリスクもなく、新しいルールを実装できる。

戦略

- Akamai は、マイクロセグメンテーションなど、隣接するセキュリティツールと WAAP を統合する計画を明らかにした。これによって、セキュリティツールが補完され、多層防御が実現するとみられる。
- Akamai は、増加する LLM の利用を保護する戦略を策定している。新しいセキュリティ対策に既存のツールを使用することで、顧客価値は向上するが、GenAI のみを対象にした保護はさらに専門化される可能性がある。
- 同社はエッジコンピューティングへの積極的な進出を計画している。エッジでトランザクションを保護するオプションは、脅威が元のサーバーに到達するのを阻止してくれる可能性がある。
- 特に API セキュリティに関して、戦略を実行した証拠が提示された。Noname Security および Neosec の買収によって、API セキュリティ戦略は完了に近づいている。
- Cyberfend、Neosec、Noname Security、Prolexic などのポイント型製品を一貫したプラットフォームへと進化させ、戦略的買収において高い実績を持つ。投資は、顧客のセキュリティへの献身を示す指標である。
- Akamai は、ポリシーの利用／承認、自動モード、緩和状況などの戦略的進捗を追跡するためにテレメトリーを活用している。これによって、開発戦略が顧客の現実に合致していることが保証される。
- 今後登場する WAAP は、CDN セキュリティの限界に対処し、東西のトラフィック、非 CDN トラフィック、マルチクラウド環境を保護する。この機能はまもなく発表される予定であり、進展の兆しに関心が集まっている。
- 顧客会議、諮問委員会の定例会議、臨時のプロセスなど、顧客が関与できる手段が多数提供される。

課題

能力

- AI/ML（Machine Learning：機械学習）エンジンは、顧客による容易な調整（つまり、ルールの順序変更）を許容しない。そのため、誤検知への対応が遅れる可能性

があり、解決には Akamai との連携が必要となる。ルールの順序の複雑性を制御するには、一時的な例外や回避策が選択肢として考えられる。

- コンテナやサーバーレスなどの、機能制限のあるフォームファクターでは、セキュリティインフラストラクチャを管理したい顧客へのサポートが制限されてしまう。現在、Terraform および API ベース管理のサポートが、Akamai の配備と自動化の焦点となっている。
- Akamai の WAAP はプレミアム製品として価格が設定されており、事業上の意思決定者が導入を決断できない可能性がある。しかし、Akamai の価格設定オプションには、ZOFF（Zero Overhead Fixed Fee：諸経費なしの固定料金）保護、リクエストベースの価格設定、および DDoS 活動によるトラフィック急増分の超過課金が控除される DDoS Protection Fee などがある。
- gRPC はサポートされていない。特定のユースケースや業界ではその方が望ましい場合があるためである。

戦略

- 専門性の高いオプション機能やアドオンには追加費用が発生し得るため、TCO が増加して全面的な配備が妨げられる可能性がある。CDN を介さないトラフィック（API ゲートウェイのトラフィックなど）には追加費用が発生する。
- 現在、WAAP の製品開発戦略では、Akamai Enterprise Application Access（EAA）のゼロトラストソリューションとの相互交流は名目上のものである。Web アプリケーションは、職場環境の変革を可能にする手段であり、製品ライン間の統合を増やすことが、セキュアアクセスのユースケースを幅広くサポートするための鍵である。
- Account Protector、Brand Protector、Content Protector などのように、ソリューションが複数あると不正対策戦略が断片化し、顧客へのメッセージが複雑になる可能性がある。

Akamai を検討すべき場合

Akamai は、配信、パフォーマンス、セキュリティ能力を一つの一貫したサービスとして実装するために統合し、強力なセットを提供している。また、高度な専門機能は追加オプションとしてライセンスを提供している。この戦略によって、企業は自社のセキュリティおよび配信のニーズにさらに適するようにカスタマイズされたソリューションに投資できるようになる。全体として、Akamai WAAP ソリューションは、大規模な最新のデジタルビジネスにおける広範なセキュリティ、可用性、完全性、およびコンプライアンスの要件に対応している。

IDC MarketScape Graph の読み方

IDC では、企業の成功の可能性を示す主要な指標として、能力と戦略の 2 つのカテゴリーに分けて分析している。

Y 軸は、サービスメニューや顧客ニーズへの貢献度のような、ベンダーの現在の能力（ケイパビリティ）を示す。このケイパビリティは、現在の組織や製品の能力に関するものである。このカテゴリーに基づき、IDC アナリストは、企業が選択した市場戦略を遂行する上で、こうした能力をどのように築き上げ、発揮しているかを分析している。

X 軸は、ベンダーが 3〜5 年後の将来に、顧客からの要求に応えられる度合いを示す戦略軸である。この戦略軸は、高度なレベルの意思決定や製品／サービス提供、顧客セグメント、事業に関する計画、3〜5 年後の顧客への製品／サービス提供計画に関するものである。

IDC MarketScape の個々のベンダーマーカーのサイズは、評価の対象となっている市場セグメントにおける各ベンダーの市場シェアを示す。

各評価基準について、ベンダーは 1 から 5 の段階で評価され、3 が平均的な評価を示すベースライン、5 が最高かつ最も稀な評価、1 が最低かつ同様に稀な評価とされる。さらに、IT バイヤーが意思決定を行う際に最適な情報を提供するために、アナリストの視点と一般的な市場動向の理解に基づいて評価基準に重み付けを行った。各基準に対する評価も、「定量的」および「定性的」評価の間で、特定の基準に最も適切で、関連するように重み付けが行われた。

Figure 1 は、各軸に沿った位置づけに変換されたいくつかの要素を、視覚的に表現している。既存の製品固有の特徴や機能は「能力」軸の重要な構成要素であるが、それ以外にも多くの要素が考慮される。同様に、「戦略」軸では、ベンダーの将来の製品開発計画が大きく考慮される。ただし、事業全体や市場投入計画の強みなど、いくつかの要因も併せて考慮される。これらの要因は、このソリューションに長期的な影響を与える可能性があるため、IDC は、これらの基準の重みを適宜調整している。全体として、各ベンダーの評価にはいくつかの要素が含まれており、読者には、ベンダープロファイルに記載された文脈に沿って Figure 1 を検討することを勧める。

IDC MarketScape 調査方法

IDC MarketScape の評価基準、重み付け、ベンダースコアは、市場やベンダーに関する十分な調査に基づいた IDC の判断によって設定されている。IDC のアナリストは、標準特性の範囲を定め、その基準に基づき、市場のリーディングベンダー、市場参入ベンダー、エンドユーザーとのインタビュー、分析、調査を通して、ベンダーの評価を行っている。市場の重み付けは、各市場に関するユーザーインタビュー、バイヤー調査、IDC の専門アナリストで構成される委員会のレビューに基づき行われている。IDC のアナリストは、詳細

な調査、ベンダーへのインタビュー、公開情報、エンドユーザーの経験に基づいて、各ベンダーの特性、行動、能力に関する正確で一貫性のある評価を行うことで、個々のベンダーのスコア、IDC MarketScape における最終的なポジショニングを提供している。

市場定義

WAAP は実行中のアプリケーションの保護を目的とする集約されたセキュリティソリューションであり、WAF を中核としている。WAAP ソリューションは、WAF、ボット管理、API セキュリティ、DDoS 対策、その他のセキュリティテクノロジーなど、多様な機能を統一的なセキュリティプラットフォームに統合している。しかし、WAF は基礎をなすと考えられるため、WAAP と認められるためには、WAF が構成要素として組み込まれていなければならない。さらに、WAAP コンポーネントをスタンドアロンソリューションとして 1 回の取引で買い切りの形で販売している場合も、WAAP とは認めない。

WAAP に不可欠なコンポーネント

WAF

WAF 製品は、Web アプリケーションとの間で転送される通信の監視、フィルタリング、またはブロックを行う。WAF はネットワークベースまたはクラウドベースのいずれかであり、1 つ以上の Web アプリケーションの前にプロキシを介して配備されることが多い。WAF は、WAAP ソリューションの中核となるコンポーネントである。

API セキュリティ

API セキュリティソリューションは、API 通信を誤用、不正、および情報窃取から保護するように特別に設計されている。こうしたソリューションは、API スキーマの取り込み、検証、実行を提供し、トラフィックの監視とパターン分析の動的な適応を実施し、マルウェア、情報窃取、コードインジェクション、ボット、DDoS 攻撃、詐欺、不正といった脅威の検出／防止を行うなど、重要な機能を一部またはすべて提供する。

API 保護能力の一部は、WAF と同じ検査ポイントで完了できる API トラフィックの検査など、WAAP サービスにデフォルトで含まれている場合がある。しかし、API セキュリティを完全に配備するには、すべての API エンドポイントの可視性と一覧表を確保し、最終的にはすべての API 通信を保護するために、追加のセンサーや構成要素が必要になる場合がある。

ボット管理

ボット管理とは、認証済みの人間のユーザーと、制御および認可された条件に基づくボットの望ましい活動のみにアクセスを制限することで、オンライン通信の完全性を確保する手法である。ボット管理ソリューションは、クライアント、デバイス、ブラウザー、ユーザーの ID および挙動に関する多数の兆候と洞察を、高度な分析と組み合わせて活用し、最も巧妙で検知しにくいボットを検出する。また、これらのソリューションは、リスクプロ

ファイル、ボットの種類に基づいて、または特定のボットのために、ボットのエコシステム全体を詳細に分類および制御できる。

より広義のボット対策市場には、迷惑ボット向けの固有のセキュリティ要件に対処するために設計された専用ソリューションも含まれる。WAAP ソリューションの統合レベルは、さまざまである。通常、WAAP ソリューションの一部として最低限のボット検出および制御機能が提供され、高度な能力は追加機能またはアップグレードの利用契約となる。

DDoS 対策

この市場には、DDoS 攻撃の検出およびフィルタリングを行うソリューションが含まれる。DDoS 防御機能はファイアウォールや IPS、その他のセキュリティ製品に搭載されているが、DDoS 対策専用ソリューションは、最大規模で最も複雑かつ新手の攻撃でも対処できるように設計されている。このような製品は、オンプレミス、クラウド、あるいはそれらのハイブリッドでも利用可能である。

WAAP ソリューションや配備の性質に応じて、ソリューションにさまざまなレベルの保護を自由に組み込める。能力追加や特殊な攻撃タイプへの対応といった保護の拡張は、追加またはアップグレードの利用契約として提供される場合がある。

WAAP の拡張的、先進的、追加的構成要素

CSWAF

CSWAF は、アプリケーションのセキュリティに関する可視性と制御をエンドユーザーのブラウザーで実行されるスクリプトにまで拡張する。CSWAF ソリューションは、その能力範囲において、製品によって非常に大きな差がある。通常、中核的な能力には、スクリプトと通信の可視性、評価、およびインベントリーが含まれる。脆弱性検出、暗号化、コード偽装、異常および脅威の検出、ポリシーの適用など、高度なセキュリティ機能に関して、市場はさらに細分化されている。

オンライン詐欺防止

詐欺防止には、詐欺行為またはその他の望ましくない活動からデジタルシステムを保護するために、単独または組み合わせて機能する幅広いソリューションが含まれる。オンライン詐欺防止には、ID 管理、強力な認証、本人確認ソリューション、支払い詐欺防止、取引詐欺検出、企業詐欺防止、およびオンライン詐欺防止専用のソリューションの利用が含まれるであろう。

WAAP に関連して、オンライン詐欺および不正防止能力は、通常、アカウント乗っ取りや新規アカウント詐欺（偽アカウント詐欺とも呼ばれる）など、特定の詐欺行為を示す固有のパターンに対処するために特別に調整されたボット管理能力に根ざしている。正常に機能しているアプリケーションと API の不正利用を示す詐欺やその他の行為を完全に検出するには、ユーザーID、クライアントおよびデバイスレベルのテレメトリー、ユーザーの行動に関する洞察が必要である。結果として、詐欺の検出能力、およびこれらの能力がどの

ようにパッケージ化され、バイヤーに販売されているかに関して、WAAP ソリューションの間には大きな違いがある。

参考資料

関連調査

- *Web Application and API Security Survey Presentation, 2024*（IDC #US52509324、2024 年 8 月発行）
- *Identifying and Measuring the Costs of Cyberattacks Targeting Web Applications and APIs*（IDC #US52025924、2024 年 4 月発行）
- *Market Analysis Perspective: Worldwide Active Application Security Market, 2023*（IDC #US51332023、2023 年 11 月発行）
- *IDC TechBrief: Client-Side WAF*（IDC #US51199423、2023 年 9 月発行）
- *Worldwide Application Protection and Availability Forecast, 2023–2027: Threat Escalation and New Frontiers*（IDC #US51178423、2023 年 9 月発行）
- *Worldwide Application Protection and Availability Market Shares, 2022: Platforms Compete with Emerging Technologies*（IDC #US51204923、2023 年 9 月発行）
- *Tales of the Tape: WAF and API Protection Emerge as Security Essentials*（IDC #US51187923、2023 年 9 月発行）

Synopsis

本 IDC MarketScape では、幅広いベンダーポートフォリオ、戦略および技術的パートナーシップ、知的財産、買収、TCO、顧客満足度、および競合他社との差別化要因の利点を考慮しながら、利用可能な WAAP ソリューションの概要を、その真価に基づいて紹介する。WAAP は、重要な Web アプリケーションおよび関連 API への安全かつ効率的なアクセスを可能にする統合的なアプローチである。市場は急速に進化しており、ポイント型製品でリスクを十分に軽減することは難しくなっている。そのため、セキュリティバイヤーが検討すべき能力やアプローチは、依然として多岐に渡っている。

「ベンダーが現代の執拗な攻撃を防御しながら、次世代のオンライン脅威から保護しようと競争しているため、WAAP 市場は、重大な岐路に立っています。同時に企業のバイヤーは、急速に変化するテクノロジーを背景に、WAAP 計画に取り組みつつあります」と、IDC Security and Trust チームのリサーチディレクターである Christopher Rodriguez は述べている。

IDC 社概要

International Data Corporation（IDC）は、IT および通信分野、消費者向けテクノロジー市場に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です。世界中に 1,300 人以上のアナリストを擁する IDC は、110 か国以上を対象として、世界規模、地域別、国別での IT ベンチマーキングとソーシング、市場動向の調査・分析および市場予測を行っています。IDC の分析と洞察は、IT 専門家、企業経営者、および機関投資家が客観的にテクノロジー導入の意思決定を行い、主要な事業目標を達成するのに役立ちます。1964 年創業の IDC は、IDG（インターナショナル・データ・グループ）の完全子会社です。

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com