IDC MarketScape

IDC MarketScape: Avaliação Global de fornecedores de plataformas empresariais de proteção de APIs e aplicativos da Web em 2024

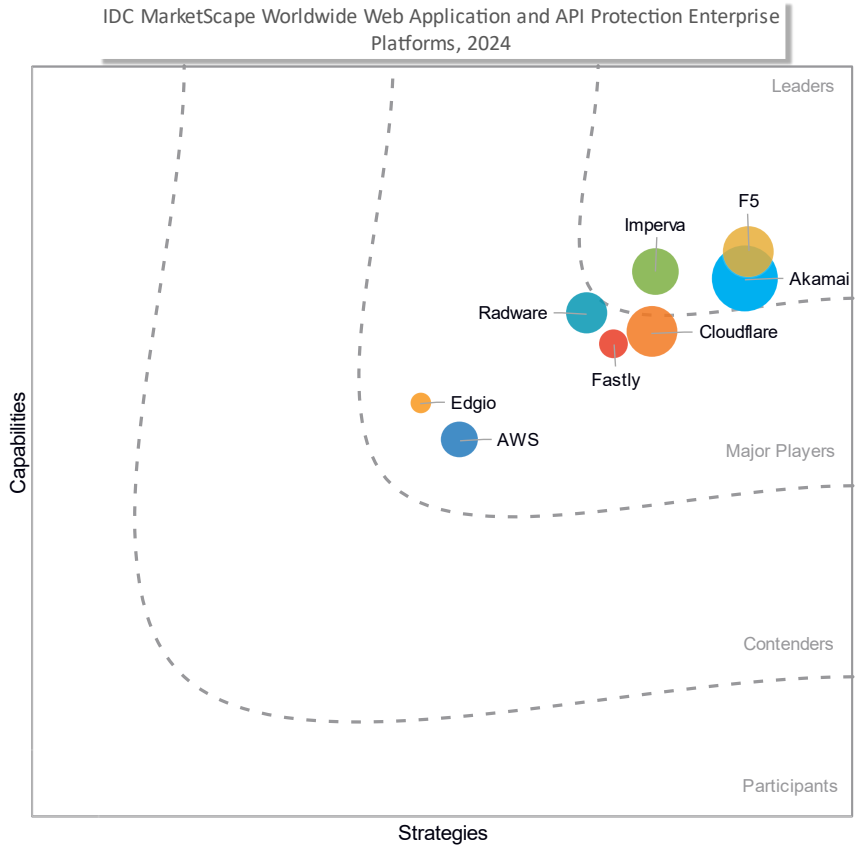
Christopher Rodriguez

ESTE TRECHO EXTRAÍDO DO IDC MARKETSCAPE APRESENTA A AKAMAI

FIGURA DO IDC MARKETSCAPE

FIGURA 1

IDC MarketScape sobre a avaliação global de fornecedores de plataformas empresariais de proteção de APIs e aplicativos da Web



Fonte: IDC, 2024

Setembro de 2024, IDC nºUS51795524e

Consulte o Apêndice para ver a metodologia detalhada, a definição de mercado e os critérios de pontuação.

NESTE TRECHO

O conteúdo deste trecho foi extraído diretamente do IDC MarketScape: Avaliação global de fornecedores de plataformas empresariais de proteção de APIs e aplicativos da Web em 2024 (Doc. nº US51795524). A totalidade ou partes das seções a seguir estão incluídas neste trecho: Opinião da IDC, Critérios de inclusão de fornecedores no IDC MarketScape, Orientação essencial, Perfil resumido do fornecedor, Apêndice e Saiba mais. As Figuras 1 e 2 também estão incluídas.

OPINIÃO DA IDC

Os aplicativos da Web são componentes fundamentais dos negócios digitais modernos, fornecendo a funcionalidade necessária para interagir com clientes reais e potenciais, parceiros e convidados, além de funcionários e prestadores de serviços. Os invasores investigam continuamente esses aplicativos e as interfaces de programação de aplicativos (APIs)relacionadas em busca de oportunidades para roubar dados, obter acesso ilícito ou defraudar empresas para obter ganhos pessoais ilícitos. Os ataques direcionados a aplicativos da Web e APIs levaram a violações de dados de alto nível, tempo de inatividade dispendioso e impactos no mundo real, inclusive roubo. Os usuários finais e os clientes geralmente são impactados por meio de perdas financeiras. Eventualmente, isso pode resultar em uma perda de confiança do cliente e em uma menor disposição de fazer negócios *on-line*.

O crime cibernético *on-line* é mais do que um mero incômodo. Ele tem o potencial de degradar e impactar os resultados de negócios. Ao longo dos anos, as empresas adotaram várias ferramentas de segurança para lidar com o fluxo constante de novas táticas de ameaças e a expansão das superfícies de ataque. O WAF (Web Application Firewall) oferece um nível básico de proteção contra explorações conhecidas e emergentes da camada de aplicativos. As empresas incorporaram várias soluções especializadas, como mitigação de DDoS, gestão de *bots* e, mais recentemente, segurança da API.

A proteção de APIs e aplicativos da Web (WAAP) combina essas tecnologias essenciais de segurança em uma plataforma integrada e coerente, para garantir um nível confiável de proteção contra as vastas ameaças *on-line*. As plataformas consolidadas e integradas ajudam a reduzir as lacunas de segurança, a complexidade do gerenciamento e a simplificar as inspeções. A pesquisa da IDC revela que 77% das empresas classificam a integração entre as soluções de segurança como sendo

"importante" ou de "importância crítica". Os aplicativos enfrentam uma série de ameaças todos os dias, e os invasores utilizam, intencionalmente, várias táticas para identificar pontos fracos nas defesas. Como resultado, as estratégias de segurança de aplicativos que se concentram em silos de segurança especializados estão destinadas, eventualmente, ao fracasso. A convergência e a consolidação da segurança são uma etapa essencial para permitir uma postura de segurança mais forte, seja por meio de uma precisão de detecção aprimorada, da diminuição de falsos positivos ou da detecção confiável de ameaças avançadas e de dia zero.

No entanto, a convergência também traz muitos benefícios aos negócios, como a redução do tempo e dos recursos necessários para a implantação e a gestão, a melhoria da experiência do usuário e o aprimoramento da análise. Além disso, a execução de todas as funcionalidades de segurança em um único serviço reduz a latência introduzida pelo roteamento do tráfego para vários pontos de inspeção de segurança.

Simultaneamente, as empresas devem adotar uma abordagem comedida, adotando toda a gama de tecnologias de proteção de aplicativos gradualmente, conforme necessário, ou conforme o tempo e os recursos permitirem. Para os clientes, é essencial uma plataforma modular e integrada para implementar facilmente a WAAP ao longo do tempo. Para os fornecedores, o desafio é identificar a combinação exata de recursos integrados nas principais áreas funcionais de segurança que devem ser incluídos em vários níveis de produtos.

Embora o WAF seja um componente fundamental, a proteção de aplicativos modernos é impossível sem uma estratégia de API coerente. As APIs agora desempenham um papel importante na era moderna dos negócios digitais, fornecendo um processo simplificado e eficiente de integração de aplicativos, a fim de oferecer uma funcionalidade poderosa e nova. No entanto, as APIs alteram a superfície de ataque de novas maneiras. As APIs são vulneráveis a configurações incorretas, exposição de dados confidenciais e ataques de negação de serviço. É importante ressaltar que, embora as APIs sejam vulneráveis a muitos dos mesmos ataques que têm como alvo as interfaces de usuário, elas também introduzem ameaças específicas a APIs, como a autorização interrompida em nível de objeto (BOLA). As APIs também fornecem um meio de comunicação entre aplicativos que pode não atravessar uma solução de proteção de perímetro, como o WAF. Isso pode resultar em um ponto cego de segurança que os invasores podem aproveitar para se moverem lateralmente, atrás das defesas baseadas em rede.

A combinação de WAF e segurança da API é fundamental para garantir a cobertura completa dos aplicativos da Web em todas as interfaces e superfícies de ataque. A proposta de valor da WAAP é complementada por tecnologias projetadas para lidar com tipos de ameaças especializadas, como ataques DDoS e atividades indesejadas de *bots*. Essas ameaças variam muito em termos de facilidade de detecção, dificuldade de

mitigação, frequência de ocorrência e gravidade do impacto. Em última análise, uma pilha completa de proteção de aplicativos requer WAF e segurança da API, mitigação de DDoS e gestão de *bots*. No entanto, os requisitos técnicos exclusivos das APIs e os requisitos especializados de ataques DDoS e atividades de *bots* significam que a evolução em direção à WAAP é uma jornada longa e sinuosa.

CRITÉRIOS DE INCLUSÃO DE FORNECEDORES DO IDC MARKETSCAPE

A WAAP é uma solução de segurança convergente para a proteção ativa de aplicativos com o WAF em seu núcleo. A IDC identificou os principais atributos discutidos nesta seção, que devem estar presentes na solução considerada para ser incluída nesta análise do IDC MarketScape para plataformas empresariais WAAP.

Os fornecedores devem oferecer uma solução WAAP convergente que combine mais dois dos seguintes itens em uma plataforma de segurança unificada:

- Segurança da API
- Gestão de *bots*
- Mitigação de DDoS
- Firewall de aplicativos da Web

Observe que o WAF é considerado fundamental e deve ser incluído para que a solução seja considerada WAAP. Além disso, as vendas pontuais de componentes WAAP como soluções autônomas não serão contabilizadas como WAAP.

Além disso, essa análise do IDC MarketScape inclui os seguintes requisitos para participação e presença no mercado:

- **Participação no mercado:** O fornecedor ofereceu funções críticas de WAAP como uma solução unificada a partir de 2023. Funcionalidades específicas essenciais ou estendidas podem ser oferecidas como parte de um pacote ou plataforma diferente, ou como soluções autônomas, desde que as funções não tenham sido oferecidas apenas como produtos autônomos ou separados. Consulte a seção “Definição de mercado” para obter uma descrição completa e detalhada da funcionalidade necessária e da opcional.
- **Representação do mercado:** O fornecedor conseguiu uma participação mínima estabelecida de receita no mercado competitivo de WAAP em 2023, conforme confirmado na ferramenta de dados Security Products Tracker da IDC.
- **Presença global:** O fornecedor tem uma distribuição mínima de receita em cada uma das principais regiões globais, incluindo América do Norte, América Latina, EMEA e Ásia/Pacífico, a partir de 2024, conforme confirmado na Security Products Tracker da IDC.

A IDC observa que alguns provedores de nuvem e segurança que oferecem componentes de uma WAAP não foram incluídos na análise devido ao foco em um produto específico em vez de uma abordagem WAAP integrada. Da mesma forma, alguns fornecedores que oferecem WAAP não conseguiram satisfazer os requisitos mínimos de representação do mercado ou de presença global.

CONSELHOS PARA COMPRADORES DE TECNOLOGIA

Principais considerações sobre os recursos do fornecedor

A análise do IDC MarketScape sobre plataformas empresariais WAAP leva em conta um nível comum de proteção exigido e esperado pelos compradores de TI, bem como a extensão da integração, a facilidade de uso, os serviços profissionais e gerenciados adjacentes e o custo total de propriedade. No nível empresarial, uma WAAP deve oferecer excelente proteção, reduzir o impacto da segurança no desempenho e acrescentar o mínimo de atrito à experiência do usuário final. A análise também enfatiza o objetivo principal da WAAP, que é combinar várias tecnologias de segurança essenciais em uma única plataforma integrada e coerente. A extensibilidade e a oferta de vários modelos de preços também são necessárias para permitir a adoção da WAAP da maneira que melhor atenda às necessidades de proteção consistente contra as vastas ameaças *on-line*, juntamente com a necessidade de valor de negócio.

As expectativas dos usuários continuam a aumentar. As empresas continuam adotando tecnologias emergentes para oferecer experiências inovadoras e agradáveis aos usuários. Os aplicativos estão se tornando cada vez mais dependentes de uma infraestrutura complexa e distribuída. As equipes de DevOps estão trabalhando de forma mais rápida e inteligente para lançar novos recursos no mercado. As empresas podem querer dar mais atenção às capacidades específicas de produtos e recursos especializados que podem ou não ser oferecidos pelos fornecedores de forma nativa, incluídos na solução por padrão ou por outros meios, como a funcionalidade complementar própria ou produtos separados, ou por meio de integrações técnicas ou OEM de terceiros. Além disso:

- **WAF no lado do cliente:** O WAF no lado do cliente, também chamado de proteção no lado do cliente, é uma tecnologia de segurança emergente projetada para lidar com um vetor de ameaça especializado, ou seja, o código do aplicativo da Web que é executado nos dispositivos do usuário final. Esse código inclui *scripts* que são executados no navegador para realizar várias funções no dispositivo, e não no servidor da Web.
- **Prevenção de fraude/abuso:** Os recursos de prevenção de fraudes e abusos *on-line* geralmente se baseiam em recursos de gestão de *bots* ajustados especificamente para abordar os padrões exclusivos indicativos de atividades

fraudulentas específicas, como a apropriação de contas ou a fraude de novas contas (também chamada de fraude de contas falsas). São necessários insights sobre a identidade do usuário, a telemetria no nível do cliente e do dispositivo, e o comportamento do usuário para detectar totalmente as fraudes e outras ações que indiquem abuso de aplicativos e APIs que funcionam adequadamente. Como resultado, existe uma variação significativa entre as soluções WAAP em sua capacidade de detectar fraudes, bem como na forma como esses recursos são empacotados e comercializados para os compradores.

- **Proxies residenciais:** As soluções WAAP variam em sua capacidade de detectar invasores que se escondem atrás de proxies residenciais ou outros métodos de ofuscação, como a rotação de IP.
- **WebSockets:** Isso envolve suporte para aplicativos que usam WebSockets, um protocolo que permite comunicações em tempo real por meio de uma conexão *full duplex.* O suporte a WebSockets é cada vez mais importante, pois os usuários *on-line* têm a expectativa de usar aplicativos interativos e em tempo real.
- **WebAssembly (WASM):** É uma linguagem de baixo nível que fornece um formato de código binário portátil. O principal benefício da WASM até o momento tem sido a compatibilidade com uma ampla gama de linguagens de desenvolvimento. A importância do suporte da WASM na WAAP aumenta junto com sua adoção.
- **Autoproteção de aplicativos em tempo de execução (RASP):** O RASP é um recurso de segurança avançado que protege o ambiente de tempo de execução do aplicativo e monitora as entradas de dados para identificar, detectar e bloquear ataques. O RASP pode ser uma opção útil para a segurança profunda de aplicativos, se as expectativas de complexidade da implantação e impacto no desempenho forem devidamente compreendidas.
- **Tokens de acesso privado (PATs):** A Apple e outras empresas de tecnologia aumentaram sua atenção à privacidade do usuário final, oferecendo métodos que atestam a autenticidade e a confiabilidade dos dispositivos que solicitam acesso, sem expor detalhes de identificação pessoal. O suporte WAAP ao Apple PAT pode ajudar a reduzir a dependência de CAPTCHAs ou outras técnicas de detecção de *bots* que introduzem atrito ou incerteza na experiência do usuário. O Apple PAT faz parte de uma iniciativa mais ampla do setor em direção a tecnologias de preservação da privacidade, que permitem o compartilhamento e o processamento de dados do usuário para pessoas ou entidades selecionadas sem a exposição de informações pessoais confidenciais.
- **Automação:** A implementação automática de atualizações melhora a facilidade de uso e agrega valor de negócio.

- **Teste de simulação:** Permite o teste de atualizações de regras antes da implementação na produção. O teste de simulação é mais eficaz quando pode ser realizado em um tráfego real.
- **eBPF:** O eBPF é um recurso do Linux que permite que programas em *sandbox* sejam executados no *kernel* do sistema operacional, o que tem grandes implicações para melhorar a observabilidade da segurança, especialmente em ambientes nativos da nuvem.

Considerações sobre a estratégia

Além disso, dada a natureza em rápida evolução das tecnologias de aplicativos da Web e APIs, as mudanças nas práticas de negócios e o nível constante de adaptação e inovação por parte dos agentes de ameaças, os compradores de segurança devem estar muito cientes da capacidade da solução de atender às suas necessidades nos próximos três a cinco anos. Além disso:

- **Ofuscação da detecção:** Os criminosos cibernéticos estão cada vez mais ousados em seus esforços para roubar dados e produtos, cometer fraudes e assediar ou extorquir empresas. As ferramentas sofisticadas e as táticas inteligentes são normalmente reservadas para os alvos lucrativos. Quando as empresas de segurança identificam e bloqueiam os ataques, os criminosos cibernéticos iniciam um processo de adaptação. Os provedores de WAAP devem investir significativamente na ocultação da natureza das detecções para garantir a longevidade dos seus esforços de mitigação. Além disso, as estratégias mais produtivas impedem que os invasores percebam quando foram detectados para drenar seus recursos. Foram observadas mitigações avançadas de *bots* e fraudes, inclusive o uso de tecnologias *deception*, ou "de engano", para evitar que os invasores fechem o ciclo do processo de desenvolvimento de armas cibernéticas.
- **Plataformização:** Os setores estão sendo remodelados por plataformas que reduzem a complexidade, fornecendo funcionalidade especializada por meio de uma interface de usuário simples, que abstrai a necessidade de desenvolvimento técnico original. Por exemplo, o Shopify é uma plataforma de comércio eletrônico que simplifica o processo de criação de novos negócios *on-line*. As funções como informações de clientes, inventário e processamento de pagamentos são oferecidas como um SaaS completo e pronto para o uso. A segurança, inclusive proteções básicas de WAF e DDoS, está incluída como funcionalidade incorporada na plataforma. Isso mudará as necessidades e expectativas dos compradores com relação às soluções WAAP e, para os fornecedores, serão necessárias adaptações estratégicas.
- **Estratégias de *shift left* (deslocamento para a esquerda):** A necessidade de implementar testes e práticas de segurança no início do ciclo de vida de desenvolvimento de software não é novidade. A detecção de vulnerabilidades

antes do lançamento na produção evita que os invasores tenham a oportunidade de descobrir e se aproveitar a vulnerabilidade. A detecção e a correção precoces também são mais eficientes e econômicas. No entanto, nos últimos anos, surgiu o conceito de *shift left*, que alcança esses ideais por meio da integração de ferramentas tradicionais de pós-produção em ferramentas e fluxos de trabalho dos desenvolvedores. Por exemplo, o uso de APIs para invocar testes dinâmicos de segurança de aplicativos (DAST) permite que o DevOps encontre e corrija as ameaças com rapidez e facilidade. Além disso, à medida que as equipes de DevOps trabalham mais rapidamente e usam microsserviços, código composto, infraestrutura como código (IaC) e outros meios para reduzir os ciclos de desenvolvimento, a necessidade de oferecer suporte a estratégias de *shift left* torna-se inevitável.

- **Mudança de personas:** As tendências de plataformização, as estratégias de *shift left* e um aumento geral na cultura de conscientização da segurança (todos são responsáveis pela segurança) estão provocando uma mudança nos compradores e decisores. Os desenvolvedores, as equipes de nuvem e de rede, e até mesmo os compradores de linha de negócios estão envolvidos no processo de compra da WAAP. Os fornecedores de WAAP devem investir cada vez mais em simplificação, automação, forte proteção pronta para uso e informação de mercado para dar melhor suporte a um amplo público de compradores e decisores.
- **IA Generativa:** A introdução da IA Generativa, ou GenAI, levantou preocupações sobre os possíveis novos riscos que a tecnologia pode introduzir nos ambientes de negócios. A pesquisa de compradores realizada pela IDC revelou que as empresas estão considerando a necessidade de aumentar os orçamentos de segurança de aplicativos como resultado. Os fornecedores de WAAP variam muito em termos de atenção e planejamento para possíveis riscos relacionados à GenAI em vários fatores, como:
  - Novas ameaças potenciais que aproveitem a IA Generativa para burlar as defesas de forma mais eficaz
  - Possíveis aplicativos para tecnologias emergentes (por exemplo, IA Generativa para mitigar as atividades de *bots*, bloquear, desacelerar ou sabotar operações de *bots*)
  - A possível necessidade de implantar recursos ou produtos especializados, ou a possibilidade de contar com as defesas existentes, à medida que as empresas desenvolvem recursos de LLM ou usam LLMs de terceiros em suas estratégias de aplicativos
  - Possíveis aplicações da IA Generativa para melhorar a eficiência e a produtividade das operações de segurança
  - Aplicações potenciais da IA para melhorar a detecção de segurança

De modo geral, apesar da grande amplitude de funcionalidades exigidas e implícitas na definição de WAAP, a IDC observou um alto nível de recursos nas soluções consideradas neste IDC MarketScape. É de se esperar que a definição da WAAP continue mudando, dadas as tecnologias emergentes e as ameaças em constante mudança. Ainda há espaço para melhorias em algumas áreas funcionais, e os fornecedores têm extensos roteiros delineados. Embora produtos pontuais especializados possam ser necessários em certos casos práticos ou para requisitos excepcionais, os fornecedores de WAAP fizeram grandes avanços no caminho em direção a plataformas completas e poderosas, com a funcionalidade profunda necessária para garantir proteção e desempenho sólidos dos aplicativos.

PERFIL RESUMIDO DO FORNECEDOR

Esta seção explica resumidamente as principais observações da IDC que levam à posição de um fornecedor no IDC MarketScape. Embora cada fornecedor seja avaliado com relação a cada um dos critérios descritos no Apêndice, a descrição aqui fornece um resumo dos pontos fortes e desafios do fornecedor.

Akamai

A Akamai é uma empresa líder no IDC MarketScape de 2024 para plataformas empresariais WAAP no mundo todo.

A Akamai é uma provedora mundial de rede e segurança fornecida pela Akamai Connected Cloud, uma plataforma distribuída de edge e nuvem, que coloca os aplicativos e as experiências mais próximos dos usuários e mantém as ameaças mais distantes. A Akamai se especializou no mercado empresarial com forte penetração na Fortune 500. O portfólio de segurança da Akamai inclui uma solução WAAP integrada chamada de App & API Protector (AAP), bem como soluções dedicadas nas categorias de segurança da API, mitigação de DDoS, gestão de *bots*, proteção de contas, WAF, proteção e conformidade no lado do cliente, DNS e proteção de marcas. A Akamai expandiu-se para a segurança empresarial com soluções para ZTNA, microssegmentação, firewall DNS, caça a ameaças e MFA.

Pontos fortes

Recursos

- O Adaptive Security Engine (ASE) oferece autoajuste para o uso confiável de regras prontas para o uso. O ASE oferece melhor proteção de dia zero, melhora as detecções (em um fator de 2 vezes, de acordo com a Akamai) e reduz os falsos positivos (em um fator de até 5 vezes, de acordo com a Akamai), além

de permitir atualizações automáticas para facilitar o uso contínuo. O ASE é alimentado pela inteligência de segurança da Akamai.

- O ASE fornece sinalização de falsos positivos para uma correção mais fácil/rápida de falsos positivos. A Akamai afirma que consegue mais de 50% após um dia e 75% em uma semana.
- A suíte WAAP abrangente oferece uma experiência de compra em um só lugar para uma segurança simplificada/completa. Uma única SKU WAAP está disponível, com complementos oferecidos para funcionalidades avançadas ou especializadas.
- Variados complementos e soluções especializadas fornecem alinhamento para usar requisitos específicos de cada caso, como ATO, proteção de marcas e proteção contra *scraping* da Web (evento de *hype*).
- A Akamai oferece uma infraestrutura de edge/CDN de enorme escala. O fornecimento de proteção próximo ao usuário garante o desempenho.
- O suporte aos fluxos de trabalho de DevOps apoia as estratégias de *shift left* dos clientes corporativos. O suporte à gestão e implantação por meio de APIs, CLI e Terraform melhora a postura de segurança sem deixar os desenvolvedores mais lentos.
- As integrações existentes com ferramentas de segurança relacionadas simplificam a integração com uma arquitetura de segurança mais ampla para oferecer melhores resultados de segurança. A solução inclui conectores pré-criados para Splunk, Qradar e ArcSight.
- É oferecida uma abordagem multimodo para a segurança da API. A abordagem oferece proteções imediatas para o tráfego de API conhecido e na plataforma, além de proteção completa da API posteriormente, conforme necessário.
- A amplitude dos recursos adicionais relacionados oferecidos junto com a WAAP garante que a segurança não prejudique o desempenho. O portfólio inclui soluções como SiteShield, mPulse Lite, EdgeWorkers, Image & Video Manager e API Acceleration.
- A Akamai introduziu recentemente novos recursos para a mitigação de DDoS na camada de aplicativos, inclusive detecção de rajadas curtas e limitação de taxa personalizável com base em pistas contextuais granulares. Esses recursos abordam toda a gama de ataques DDoS, inclusive as necessidades especializadas dos ataques à camada de aplicativos.
- Está incluída uma visão unificada da telemetria de segurança, que oferece ampla análise e visibilidade da segurança, com recursos de detalhamento. O Web Security Analytics está incluído em todos os produtos de segurança de aplicativos.

- O modo de avaliação oferece uma oportunidade de analisar os efeitos nas alterações de regras com base no tráfego real antes de implementar as alterações. Esse recurso permite a implementação de novas regras sem o risco de um impacto desconhecido no tráfego da produção.

Estratégia

- A Akamai falou de planos para a integração da WAAP com ferramentas de segurança adjacentes, como a microssegmentação. Isso complementará as ferramentas de segurança e fornecerá defesa profunda.
- A Akamai está desenvolvendo estratégias para proteger o aumento do uso do LLM. O uso de ferramentas existentes para novas práticas de segurança aumenta o valor para o cliente; no entanto, as proteções específicas da IA Generativa ainda podem ser mais especializadas.
- A empresa tem planos agressivos de expansão para a computação de edge. As opções para proteger as transações na edge podem ajudar a evitar que as ameaças cheguem aos servidores de origem.
- Foram observadas evidências de execução da estratégia, especialmente com relação à segurança da API. A estratégia de segurança da API está quase concluída após as aquisições da Noname Security e da Neosec.
- Há um sólido histórico de aquisições estratégicas, transformando produtos pontuais, como Cyberfend, Neosec, Noname Security e Prolexic, em uma plataforma coerente. Os investimentos são indicadores de uma dedicação à segurança dos clientes.
- A Akamai utiliza a telemetria para acompanhar o progresso estratégico, como uso/aceitação de políticas, o modo automático e o status da mitigação. Isso garante que as estratégias de desenvolvimento estejam alinhadas às realidades dos clientes.
- A futura WAAP de origem aborda as limitações de segurança de CDN e protege o tráfego leste-oeste, o tráfego não CDN e os ambientes multinuvem. Esse recurso estará disponível em breve, e os sinais de progresso estão sendo observados.
- São oferecidas várias rotas para o engajamento do cliente, como por conferências de clientes, reuniões regulares do conselho consultivo e processos ad hoc.

Desafios

Recursos

- Os mecanismos de IA e aprendizado de máquina não permitem um ajuste fácil pelos clientes (ou seja, não é possível alterar a ordem das regras). Isso pode gerar atrasos na resposta a falsos positivos e exigir a colaboração da Akamai

para resolver o problema. As exceções temporárias e soluções alternativas são uma opção possível para navegar pelas complexidades da ordem das regras.

- Os fatores de forma limitados, como contêineres e sem servidor, limitam o suporte a clientes que querem controlar a infraestrutura de segurança. Atualmente, a Akamai se concentra em dar suporte ao Terraform e aos controles baseados em API para implantação e automação.
- A WAAP da Akamai tem o preço de um produto premium, o que pode ser proibitivo para os decisores de negócios. No entanto, as opções de preços da Akamai incluem a proteção ZOFF (Zero Overhead Fixed Fee), preços baseados em solicitações e a Taxa de Proteção contra DDoS, que inclui zero de excedente para picos de tráfego devido a atividades de DDoS.
- Não há suporte para gRPC, que pode ser preferido em casos práticos especializados ou em setores específicos.

Estratégia

- Os recursos especializados, opcionais e os complementos podem apresentar custos adicionais, o que pode aumentar o custo total de propriedade (TCO) e impedir implantações completas. O tráfego que está fora da CDN (por exemplo, tráfego de *gateway* de API) é um custo adicional.
- A estratégia de desenvolvimento de produtos para WAAP atualmente inclui a polinização cruzada nominal com a solução Zero Trust (confiança zero) do Akamai Enterprise Application Access (EAA). Os aplicativos da Web oferecem um meio de permitir a transformação do local de trabalho, e uma maior integração entre as linhas de produtos é fundamental para dar suporte a toda a gama de casos práticos de acesso seguro.
- Várias soluções (por exemplo, Account Protector, Brand Protector e Content Protector) resultam em uma estratégia de fraudes fragmentada, o que pode aumentar a complexidade das mensagens.

Considere a Akamai quando

A Akamai oferece um conjunto robusto de recursos de entrega, desempenho e segurança, integrados para serem implementados como um serviço coerente. A Akamai licencia recursos avançados e especializados como complementos opcionais. A estratégia permite que as empresas invistam na solução personalizada que melhor atenda às suas necessidades de segurança e fornecimento. Em geral, a solução WAAP da Akamai satisfaz uma ampla gama de requisitos de segurança, disponibilidade, integridade e conformidade para empresas digitais modernas e de grande escala.

APÊNDICE

Leitura de um gráfico do IDC MarketScape

Para fins desta análise, a IDC dividiu as possíveis medidas-chave para o sucesso em duas categorias principais: recursos e estratégias.

O posicionamento no eixo y reflete os recursos e o menu de serviços atuais do fornecedor e o grau de alinhamento do fornecedor com as necessidades do cliente. A categoria de recursos concentra-se nos recursos da empresa e do produto hoje, aqui e agora. Nessa categoria, os analistas da IDC analisarão o grau em que o fornecedor está desenvolvendo/entregando recursos que lhe permitem executar a estratégia escolhida no mercado.

O posicionamento no eixo x, ou eixo das estratégias, indica o grau de alinhamento da estratégia futura do fornecedor com o que os clientes exigirão dentro de três a cinco anos. A categoria de estratégias concentra-se em decisões de alto nível e suposições subjacentes sobre ofertas, segmentos de clientes, bem como planos de negócios e de entrada no mercado para os próximos três a cinco anos.

O tamanho dos marcadores de fornecedores individuais no IDC MarketScape representa a participação de mercado de cada fornecedor individual no segmento de mercado específico que está sendo avaliado.

Para cada critério específico, os fornecedores foram avaliados em uma escala de 1 a 5, sendo 3 considerado a linha de base que indica uma avaliação média, 5 representando a melhor e mais rara avaliação e 1 sendo a mais baixa e também igualmente rara. Os critérios foram então ponderados com base na perspectiva do analista e na compreensão das tendências gerais do mercado, para melhor informar a tomada de decisão do comprador de TI. As avaliações de cada critério também foram ponderadas entre uma avaliação "quantitativa" e uma avaliação "qualitativa", conforme mais apropriado e relevante para o critério específico.

A Figura 1 fornece uma representação visual de vários fatores que são traduzidos em um posicionamento ao longo de cada eixo. Os recursos e a funcionalidade específicos do produto existente são um componente importante do eixo "recursos", mas muitos outros fatores também são considerados. Da mesma forma, o eixo "estratégias" leva muito em consideração os planos do fornecedor para futuros desenvolvimentos de produtos. No entanto, vários fatores também são considerados, inclusive a força dos negócios em geral e dos planos de entrada no mercado. Esses fatores podem ter um impacto de longo prazo na solução, e a IDC ajustou os pesos desses critérios de acordo. De modo geral, vários fatores entram na avaliação de cada fornecedor, e os

leitores são aconselhados a considerar a Figura 1 no contexto fornecido nos perfis dos fornecedores.

Metodologia do IDC MarketScape

A seleção de critérios, as ponderações e as pontuações dos fornecedores no IDC MarketScape representam o julgamento bem pesquisado da IDC sobre o mercado e fornecedores específicos. Os analistas da IDC adaptam a gama de características padrão pelas quais os fornecedores são avaliados por meio de discussões estruturadas, pesquisas e entrevistas com líderes de mercado, participantes e usuários finais. As ponderações de mercado baseiam-se em entrevistas com usuários, pesquisas com compradores e na opinião de especialistas da IDC em cada mercado. Os analistas da IDC baseiam as pontuações individuais dos fornecedores e, em última análise, as posições dos fornecedores no IDC MarketScape, em pesquisas e entrevistas detalhadas com os fornecedores, informações disponíveis publicamente e experiências de usuários finais, em um esforço para fornecer uma avaliação precisa e consistente das características, do comportamento e da capacidade de cada fornecedor.

Definição de mercado

A WAAP é uma solução de segurança convergente para a proteção ativa de aplicativos com o WAF em seu núcleo. As soluções WAAP combinam várias funções em uma plataforma de segurança unificada, que inclui WAF, gestão de *bots*, segurança de APIs, mitigação de DDoS e outras tecnologias de segurança. No entanto, o WAF é considerado fundamental e deve ser um componente integral para que a solução seja considerada uma WAAP. Além disso, as vendas pontuais de componentes WAAP como soluções autônomas não serão contabilizadas como WAAP.

Componentes essenciais da WAAP

Firewall de aplicativo da Web

Os produtos WAF monitoram, filtram ou bloqueiam as comunicações em trânsito de e para um aplicativo da Web. Um WAF pode ser baseado na rede ou na nuvem e geralmente é implantado por meio de um proxy na frente de um ou mais aplicativos da Web. O WAF é o componente principal de uma solução WAAP.

Segurança da API

As soluções de segurança da API são projetadas especificamente para proteger as comunicações de API contra uso indevido, abuso e explorações. Essas soluções fornecem recursos essenciais, em parte ou no todo, como ingestão, validação e aplicação de esquemas de API; monitoramento de tráfego dinâmico e adaptável e

análise de padrões; e detecção/prevenção de ameaças, como malware, explorações, injeção de código, *bots*, ataques DDoS, fraude e abuso.

Alguns recursos de proteção de API podem ser incluídos em uma oferta WAAP por padrão, como as inspeções de tráfego de API que podem ser concluídas no mesmo ponto de inspeção que um WAF. No entanto, uma implementação completa de segurança da API pode exigir sensores e componentes adicionais para garantir a visibilidade e o inventário de todos os endpoints de API e, por fim, a proteção de todas as comunicações de API.

Gestão de *bots*

A gestão de *bots* é a prática de garantir a integridade das comunicações *on-line*, ao limitar o acesso apenas a usuários humanos autênticos e a atividades de *bots* desejáveis sob condições controladas e aprovadas. As soluções de gestão de *bots* aproveitam vários sinais e insights sobre o cliente, o dispositivo, o navegador, a identidade do usuário e o comportamento, combinados com análises avançadas para detectar os *bots* mais sofisticados e evasivos. Essas soluções também fornecem uma categorização granular e um controle sobre todo o ecossistema de *bots*, com base em perfis de risco, tipos de *bots* ou para *bots* específicos.

O mercado mais amplo de gestão de *bots* inclui soluções criadas especificamente para atender aos requisitos de segurança exclusivos impostos por *bots* indesejados. Existem vários níveis de integração entre as soluções WAAP. Normalmente, um nível mínimo de detecção e controle de *bots* é oferecido como parte de uma solução WAAP, com recursos avançados oferecidos como complemento ou assinatura de *upgrade*.

Mitigação de DDoS

O mercado de mitigação de DDoS inclui soluções que detectam e filtram ataques distribuídos de negação de serviço. Embora os recursos de defesa contra DDoS possam existir em *firewalls*, IPS e outros produtos de segurança, as soluções criadas especificamente para mitigação de DDoS são projetadas para lidar com os maiores, mais complexos e os novos ataques. Esses produtos podem estar no local ou na nuvem, ou em um híbrido dos dois.

Dependendo da natureza da solução ou da implantação WAAP, vários níveis de proteção podem ser incluídos livremente na solução. Há também a opção de proteções ampliadas na forma de capacidade adicional ou cobertura de tipos de ataques especializados, como uma assinatura complementar ou de *upgrade*.

Componentes estendidos, avançados e opcionais da WAAP

WAF no lado do cliente

O CSWAF (WAF no lado do cliente) estende a visibilidade e o controle da segurança do aplicativo para os *scripts* executados nos navegadores dos usuários finais. As soluções CSWAF variam drasticamente em termos da extensão de seus recursos. Os principais recursos normalmente incluem visibilidade, avaliação e inventário de *scripts* e comunicações. O mercado é mais fragmentado em termos das funções avançadas de segurança oferecidas, como detecção de vulnerabilidades, criptografia, ofuscação de código, detecção de anomalias e ameaças, e aplicação de políticas.

Prevenção de fraudes *on-line*

A prevenção de fraudes abrange uma ampla gama de soluções que funcionam de forma independente ou em conjunto para proteger os sistemas digitais contra atividades fraudulentas ou indesejadas. A prevenção de fraudes *on-line* pode envolver o uso de gerenciamento de identidade, autenticação forte, soluções de comprovação de identidade, proteção contra fraudes em pagamentos, detecção de fraudes em transações, prevenção de fraudes empresariais e soluções dedicadas de prevenção de fraudes *on-line*.

No que se refere ao WAAP, os recursos de prevenção de fraudes e abusos *on-line* geralmente se baseiam em recursos de gestão de *bots* ajustados especificamente para abordar os padrões exclusivos indicativos de atividades fraudulentas específicas, como a apropriação de contas ou a fraude de nova conta (também chamada de fraude de conta falsa). São necessários insights sobre a identidade do usuário, a telemetria no nível do cliente e do dispositivo, e o comportamento do usuário para detectar totalmente as fraudes e outras ações que indiquem abuso de aplicativos e APIs que funcionam adequadamente. Como resultado, existe uma variação significativa entre as soluções WAAP em sua capacidade de detectar fraudes, bem como na forma como esses recursos são empacotados e comercializados para os compradores.

SAIBA MAIS

Pesquisas relacionadas

- *Web Application and API Security Survey Presentation, 2024* (IDC no. US52509324, agosto de 2024)
- *Identifying and Measuring the Costs of Cyberattacks Targeting Web Applications and APIs* (IDC no. US52025924, abril de 2024)
- *Market Analysis Perspective: Worldwide Active Application Security Market, 2023* (IDC no. US51332023, novembro de 2023)

- *Resumo técnico da IDC: Client-Side WAF* (IDC no. US51199423, setembro de 2023)
- *Worldwide Application Protection and Availability Forecast, 2023-2027: Threat Escalation and New Frontiers* (IDC no. US51178423, setembro de 2023)
- *Worldwide Application Protection and Availability Market Shares, 2022: Platforms Compete with Emerging Technologies* (IDC no. US51204923, setembro de 2023)
- *Tales of the Tape: WAF and API Protection Emerge as Security Essentials* (IDC no. US51187923, setembro de 2023)

Sinopse

Este estudo da IDC oferece uma visão geral das soluções WAAP disponíveis por mérito próprio, levando também em conta as vantagens do portfólio mais amplo do fornecedor, bem como parcerias estratégicas e técnicas, propriedade intelectual, aquisições, custo total de propriedade, satisfação do cliente e diferenciais competitivos. A WAAP é uma abordagem integrada para permitir o acesso seguro e de alto desempenho a importantes aplicativos da Web e APIs relacionadas. O mercado está evoluindo rapidamente, ultrapassando a capacidade dos produtos pontuais de mitigar suficientemente os riscos. Dessa forma, ainda há uma ampla gama de recursos e abordagens a serem considerados pelos compradores de segurança.

"O mercado de WAAP se encontra em um momento crítico, pois os fornecedores correm para se proteger contra a próxima geração de ameaças *on-line* e, ao mesmo tempo, se defender contra os ataques implacáveis dos dias de hoje", disse Christopher Rodriguez, diretor de pesquisa da equipe de Segurança e Confiança da IDC. "Ao mesmo tempo, os compradores empresariais estão abordando o planejamento da WAAP no contexto de tecnologias que mudam rapidamente."

SOBRE A IDC

A International Data Corporation (IDC) é a principal empresa global especializada em inteligência de mercado, serviços de consultoria e eventos para os mercados de tecnologia da informação, telecomunicações e tecnologia de consumo. Com mais de 1.300 analistas no mundo todo, a IDC oferece expertise global, regional e local sobre tecnologia, oportunidades e tendências do setor em mais de 110 países. As análises e os insights da IDC ajudam os profissionais de TI, os executivos e a comunidade investidora a tomar decisões de tecnologia bem-fundamentadas e a atingir os principais objetivos de negócios. Fundada em 1964, a IDC é uma subsidiária integral do International Data Group (IDG, Inc.).

Sede Global

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