

Cequence Web Application and API Protection (WAAP)

Gerenciamento de Bots Integrado, Segurança de API, WAF e Proteção contra DDoS


As aplicações e suas APIs associadas continuam a se proliferar, e a dificuldade de protegê-las contra ataques cada vez mais sofisticados está aumentando. As organizações estão adotando arquiteturas modernas, mas as soluções existentes não conseguiram acompanhar essa evolução. Com o advento da inteligência artificial (IA), a segurança corporativa exige uma abordagem abrangente que proteja tanto contra ataques “tradicionais” quanto contra ataques aprimorados por IA — seja raspagem não autorizada de conteúdo, exfiltração de dados sensíveis, abuso da lógica de negócios ou ataques de alto volume projetados para causar interrupções.


Cequence WAAP – Visão Geral


Clientes frequentemente nos pedem para adicionar capacidades de Web Application Firewall (WAF) e Distributed Denial of Service (DDoS) às nossas ofertas existentes de Segurança de API e Gerenciamento de Bots, a fim de oferecer uma solução WAAP verdadeiramente best-of-breed. Consolidação de fornecedores, redução de custos e desempenho geral estão entre as razões mais comuns. Por isso, incorporamos um WAF poderoso e uma proteção DDoS altamente escalável para entregar um WAAP em nuvem de nível corporativo, capaz de escalar para as maiores empresas. Cequence WAAP protege todas as suas aplicações web e APIs contra ameaças sofisticadas e ataques de bots, convencionais e aprimorados por IA, tudo em um único tenant em nuvem. Esta solução SaaS integrada oferece diversos benefícios:

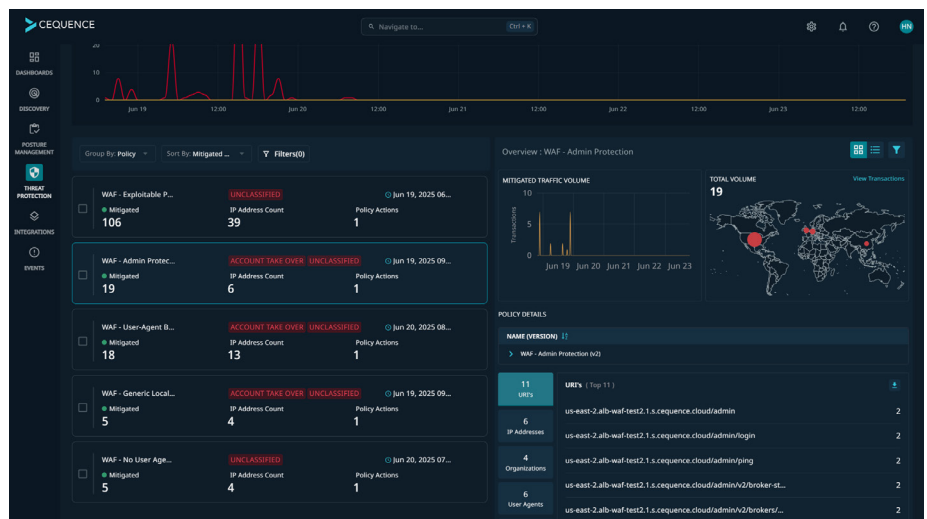
WAAP em Resumo

-  **Gerenciamento Avançado de Bots** detecta e bloqueia bots maliciosos
-  **Segurança Abrangente de API** oferece gestão de postura e testes
-  **WAF Poderoso** fornece proteção específica para aplicações web
-  **Proteção DDoS Escalável** intercepta ataques volumétricos

 **Eficiência Operacional**
Portal único de proteção de aplicações para WAF, gerenciamento de bots e segurança de API, minimizando a complexidade e a sobrecarga administrativa

 **Menor Latência**
Única implantação em nuvem elimina múltiplos saltos na nuvem

 **Menor Risco**
Componentes integrados em um único tenant eliminam lacunas de cobertura causadas por roteamento de tráfego inconsistente

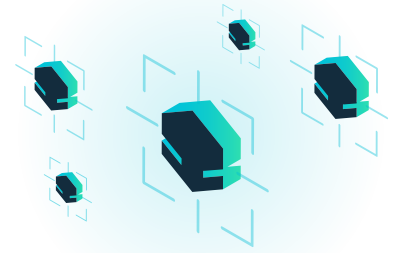


As regras do WAF acionadas são visíveis no painel do Cequence.

Capacidades do Cequence WAAP

Gerenciamento de Bots

O Cequence Bot Management protege aplicações web, móveis e APIs de uma organização contra ataques de bots volumétricos e altamente sofisticados. Sua abordagem baseada em rede não exige modificações nas aplicações, resultando em tempo de valor medido em horas em vez de semanas. O fingerprinting comportamental da Cequence fornece detecção líder de mercado de bots (bons e maus) e mitiga ataques em tempo real, diretamente para aplicações e APIs, prevenindo perda de dados, roubo e fraude que causam indisponibilidade, danos à marca, análises de vendas distorcidas e aumento nos custos de infraestrutura.

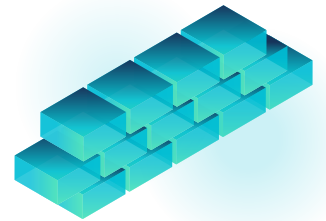


Segurança de API

O Cequence API Security descobre, monitora e testa suas APIs, avaliando uma ampla gama de riscos que podem levar a problemas de conformidade e governança, perda de dados e interrupções nos negócios. APIs internas, externas e de terceiros são descobertas, e especificações de API podem ser geradas automaticamente quando necessário. O Cequence também detecta e mascara automaticamente dados sensíveis, prevenindo exposições não intencionais. Testes de segurança de API encontram falhas tanto em desenvolvimento quanto em tempo de execução, permitindo que as organizações “se movam para a esquerda” enquanto se protegem “à direita”.

Web Application Firewall

O WAF é uma solução poderosa e altamente escalável, com um conjunto abrangente de regras e políticas, que oferece proteção contra o OWASP Top 10 para aplicações web, padrões de entrada maliciosos e ataques de injeção de SQL. Os ataques de bots detectados pelo WAF são identificados e encaminhados ao Cequence Bot Management, que oferece diversas opções de mitigação, incluindo bloqueio, rate limiting, injeção de cabeçalhos e respostas enganosas. Essa integração melhora o desempenho do WAF ao descarregar mitigações complexas para a Cequence e fornece um console único para gerenciar a atividade do WAF e o gerenciamento de bots.



Proteção contra DDoS

A proteção DDoS altamente escalável garante que aplicações e APIs estejam protegidas contra até os maiores ataques DDoS, que de outra forma sobrecarregariam a infraestrutura e interromperiam as operações. Protege recursos contra ataques volumétricos como ataques de reflexão (camada 3), ataques de protocolo de rede como SYN floods e UDP floods (camada 4), bem como ataques na camada de aplicação e API (camada 7). A solução é altamente resiliente e oferece 99,99% de disponibilidade contra ataques comuns à infraestrutura.

Implantação

O Cequence WAAP pode ser implantado em um tenant da Cequence Cloud ou no tenant de AWS do cliente. A Cequence também oferece um WAAP Gerenciado com todos os componentes totalmente administrados e monitorados pela própria Cequence. Aproveitando a presença global da AWS, garante-se proximidade geográfica dos tenants em nuvem, independentemente da localização do cliente.



WAAP e IA

A IA está mudando o jogo quando se trata de segurança corporativa, mas utiliza canais de comunicação já existentes. O Cequence WAAP já protege suas aplicações e APIs, então você pode ter certeza de que, mesmo com a evolução da IA, sua segurança permanece garantida. A Cequence também oferece um AI Gateway, a maneira mais rápida e simples de conectar agentes às aplicações corporativas e SaaS.