CEQUENCE

FOLHA DE DADOS

Gerenciamento de Bots Cequence

Detecção de Bots, Mitigação e Prevenção de Fraudes

Bots, tanto bons quanto ruins, geram quase metade de todo o tráfego da web atualmente. Inicialmente, os bots maliciosos tinham como alvo principal sites e aplicativos, mas hoje frequentemente contornam os aplicativos e atacam diretamente as APIs. A ubiquidade das APIs, combinada com sua acessibilidade, facilidade de uso e flexibilidade, as tornou um dos principais alvos para agentes mal-intencionados. Mesmo APIs bem programadas podem ser exploradas por meio do abuso da lógica de negócios, como parte de campanhas de tomada de conta em larga escala (ATO – Account Takeover) ou uso de bots de compras. A criação massiva de contas falsas e a extração de conteúdo (scraping) são ataques comuns direcionados a aplicativos e suas APIs. As organizações precisam de uma solução que detecte e impeça ataques automatizados contra seus aplicativos e APIs, seja fácil de implementar e tenha impacto imediato.

Visão Geral do Gerenciamento de Bots Cequence

A Cequence protege as aplicações web, móveis e APIs de uma organização contra toda a gama de ataques de bots, prevenindo a perda de dados, roubo e fraude. Alimentado por um mecanismo de análise baseado em aprendizado de máquina (ML), que determina em tempo real se as transações de aplicativos e APIs são maliciosas ou legítimas, ele mitiga ataques de forma nativa e elimina impactos negativos nos negócios, como tempo de inatividade, danos à marca, distorção de análises de vendas e aumento dos custos de infraestrutura.

Recursos de Gerenciamento de Bots

Sem Modificação de Aplicação ou Fricção para o Cliente

A abordagem baseada em rede da Cequence elimina a necessidade de agentes ou qualquer modificação na aplicação, como a integração de JavaScript ou SDKs móveis. Essa estratégia remove a fricção do cliente causada por métodos tradicionais de prevenção de bots, como CAPTCHAs, garantindo proteção abrangente para todas as aplicações e APIs, não apenas aquelas que podem ser instrumentadas. A proteção baseada em rede também elimina o esforço de desenvolvimento e testes exigidos pela instrumentação de aplicativos, reduzindo tempo e custos.

Visão Geral do Gerenciamento de Bots

- **Sem necessidade de CAPTCHA —** Abordagem baseada em rede que dispensa agentes, JavaScript ou integração de SDKs.
- **Mitigação Nativa —** Identificação e bloqueio de ataques sem depender de infraestrutura terceirizada, como WAFs.
- **Opções de Mitigação Robustas —** Inclui bloqueio, registro, limitação de taxa, injeção de cabeçalhos e dissuasão.
- **Modelo de Implantação Flexível —** Suporta implementação local (on-premises), SaaS e híbrida.
- **Prevenção de Fraude em APIs —** Políticas personalizáveis e detalhadas para casos de uso específicos da organização.

As organizações podem nem perceber que têm um problema com bots, pois eles são apenas um meio de automatizar ataques em grande escala. A Cequence detecta e mitiga diversos tipos de ataques, incluindo:

Tomada de Conta

Vulnerabilidades BOLA

Vendas relâmpago, vendas de alto interesse e lançamentos de tênis

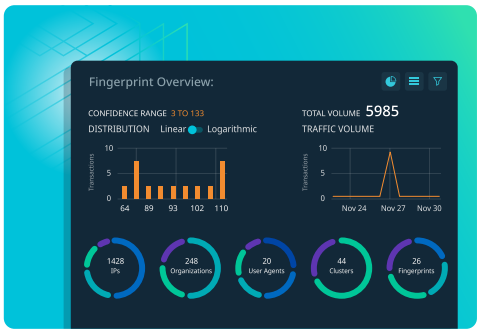
Exposição de dados sensíveis

Abuso de cartões-presente e programas de fidelidade

Criação de contas falsas

Detecção Contínua de Ameaças Baseada em Comportamento

O mecanismo de análise baseado em aprendizado de máquina (ML) da Cequence examina a intenção comportamental em tráfego web, móvel e de API, identificando tráfego legítimo e malicioso com base no comportamento, e não apenas nos endereços IP. Com essa análise, a solução cria impressões digitais comportamentais que monitoram continuamente ataques sofisticados, mesmo quando os invasores modificam suas táticas para evitar a detecção. Essa abordagem é altamente eficaz e não exige integração no lado do cliente ou modificação na aplicação, garantindo a proteção mais ampla possível para aplicações e APIs.



Defesa Contra Bots Impulsionada por IA e ML

A Cequence utiliza inteligência artificial (IA) e aprendizado de máquina (ML) em toda a plataforma UAP, desde a detecção de ataques até a mitigação. Os modelos de ML permitem uma classificação precisa de endpoints e ameaças, detecção de dados sensíveis, impressões digitais comportamentais e muito mais. Além disso, a IA fortalece a capacidade exclusiva da Cequence de identificar atividades maliciosas e criar regras e políticas de mitigação automaticamente, que podem ser aplicadas de forma autônoma ou após revisão humana. A Cequence protege o uso autorizado de IA generativa (GenAI) e IA agente nas empresas, além de defender contra extração indesejada de dados (scraping) por bots de IA e ataques sofisticados realizados por agentes mal-intencionados com IA.

Rápido Retorno sobre o Investimento

A Cequence é implantada de forma rápida e oferece proteção imediata, sem necessidade de modificações nas aplicações. A solução conta com opções de implantação flexíveis, incluindo SaaS, on-premises e híbrida, garantindo adaptação às necessidades de qualquer organização.

Prevenção de Fraudes Adaptada ao Seu Negócio

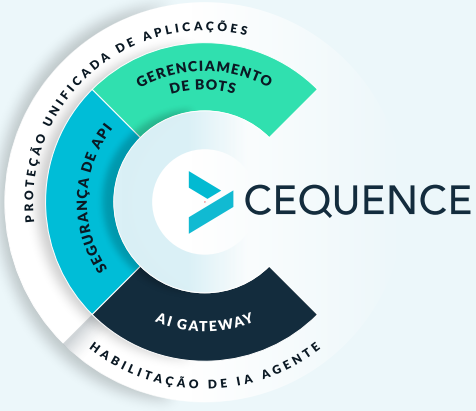
O Cequence Bot Management também inclui recursos de prevenção a fraudes que suportam políticas personalizáveis e granulares para casos de uso específicos do seu negócio e do seu setor. À medida que o tráfego flui para as APIs, atividades que correspondem a essas políticas de fraude são identificadas e bloqueadas em tempo real, e são fornecidas informações detalhadas para análise de cada campanha de fraude. Os clientes podem criar novas políticas e modificar as políticas prontas para uso, sem necessidade de código.

Funciona com o Cequence AI Gateway

O Cequence AI Gateway habilita o acesso de IA baseada em agentes (agentic) a qualquer aplicação interna, externa ou SaaS, em minutos e sem necessidade de código. O Bot Management garante que as aplicações e APIs corporativas estejam protegidas contra agentes maliciosos.

O Gerenciamento de Bots é Parte da Plataforma Cequence Unified Application Protection

A plataforma Cequence Unified Application Protection une descoberta, conformidade e proteção para defender as aplicações e APIs de uma organização contra ataques, abuso de lógica de negócios e fraudes. Demonstrando valor em minutos — e não em dias ou semanas —, a Cequence oferece um modelo de implantação flexível que não exige instrumentação ou modificação dos aplicativos. Confiada pelas maiores e mais exigentes organizações dos setores público e privado, a Cequence protege mais de 10 bilhões de interações de API por dia e 4 bilhões de contas de usuários.



CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai