

Cequence Platform

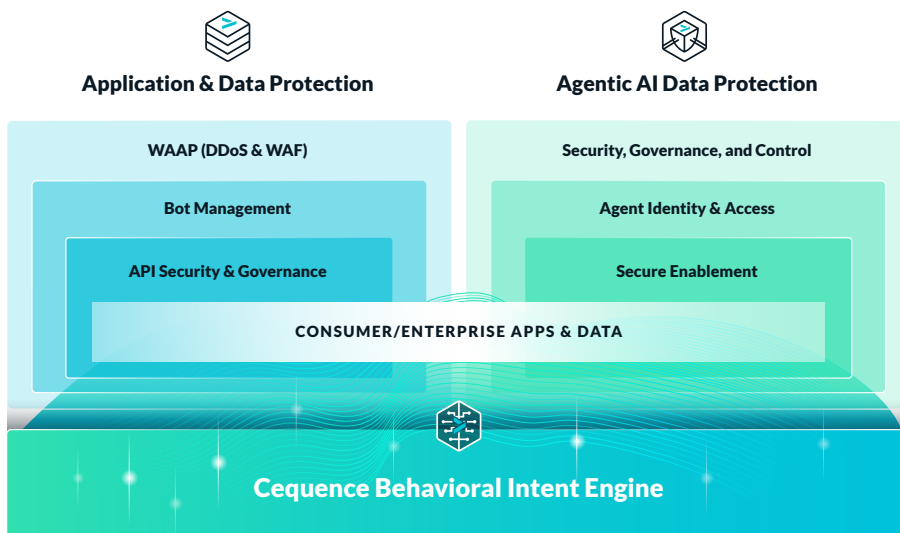
Proteção comportamental para aplicações, APIs e IA

A superfície de ataque continua crescendo

A adoção da nuvem, sistemas cada vez mais integrados, dependências de terceiros na cadeia de suprimentos e o surgimento da IA aumentaram drasticamente a superfície de ataque das empresas, colocando aplicações e dados em risco. Aplicações e APIs continuam a se multiplicar, a IA permite que agentes maliciosos descubram vulnerabilidades e ataquem em velocidade de máquina, e agentes de IA sem governança adequada ameaçam vaziar dados e ultrapassar seus privilégios de acesso. As organizações precisam de uma solução que lhes permita aproveitar a promessa de produtividade e crescimento impulsionados por IA, ao mesmo tempo em que protegem aplicações, APIs e dados contra ataques, abuso de lógica de negócios e fraudes.

A abordagem exclusiva da Cequence

Cada interação entre aplicações, APIs e IA revela sua intenção por meio de seu comportamento. A intenção comportamental é a base da plataforma Cequence. Ela cria perfis de cada usuário, bot e agente que interage com suas aplicações, APIs e dados, estabelecendo identidades digitais capazes de diferenciar automação legítima de atividades maliciosas. Essa mesma capacidade agora se estende à IA agêntica: a Cequence aplica análise comportamental ao tráfego entre agentes e aplicações para aplicar, em tempo real, controles sobre o que os agentes podem fazer, quais dados podem acessar e tomar medidas quando suas ações ultrapassam limites aceitáveis.



Produtos da Cequence



AI Gateway

Conecta e protege fluxos de trabalho de IA agêntica



Bot Management

Protege aplicações e APIs contra ataques automatizados e fraudes



API Security

Descubra, inventarie, teste e proteja seus endpoints de API



WAAP

Bot Management, API Security, WAF e proteção contra DDoS

O **Cequence AI Gateway** permite que as organizações disponibilizem suas aplicações e dados para agentes de IA de forma simples e segura. Ele oferece um ponto central para visibilidade e monitoramento, registros confiáveis de MCP, APIs, LLMs e Skills, além de um catálogo de aplicações aprovadas pela empresa. O AI Gateway conta com governança integrada e mecanismos de proteção para restringir o comportamento dos agentes por meio de recursos como acesso com privilégio mínimo, limitação de taxa (rate limiting) e proteção de dados sensíveis.

Baseado em princípios de Zero Trust, o AI Gateway fornece verificação e validação contínuas do comportamento em tempo de execução. Com esses controles e guardrails implementados, o AI Gateway permite que as organizações inovem rapidamente, respeitando requisitos de governança e avançando do protótipo para a produção sem incorrer em dívida técnica ou limitações de escalabilidade associadas a soluções básicas.

O **Cequence API Security** é uma solução AI-first que descobre, inventaria e testa APIs, fornecendo gerenciamento abrangente da postura de segurança de APIs. Ele descobre APIs internas, externas e de terceiros, bem como provedores de edge, infraestrutura, gateways e hospedagem.

A combinação de descoberta de dentro para fora (inside-out) e de fora para dentro (outside-in) fornece visibilidade e inventário tanto da superfície de ataque quanto das APIs internas. O API Security identifica de forma autônoma dados sensíveis que trafegam pelas APIs e os mascara em tempo de execução, impedindo a exfiltração indesejada.

O API Security inclui um Assistente de IA para orientar os profissionais e um servidor MCP integrado para se conectar aos seus fluxos internos de trabalho com IA agêntica.

O **Cequence Bot Management** detecta uma ampla variedade de ataques automatizados e aplica políticas de mitigação em tempo real para evitar perda de dados, roubo e fraude. O Bot Management é baseado em rede, integra-se à infraestrutura existente e não requer agentes, JavaScript ou SDKs.

Impressões digitais comportamentais e análises multidimensionais proporcionam uma compreensão profunda do contexto de negócios para identificar e bloquear ataques nativamente em tempo real. Ele mitiga uma ampla variedade de ataques cibernéticos, incluindo ataques de lógica de negócios, exploits, atividade automatizada de bots, fraudes online e ameaças listadas no OWASP API Security Top 10.

O **Cequence Web Application and API Protection (WAAP)** combina Bot Management e API Security com proteção WAF e DDoS em um único ambiente SaaS.

Componentes integrados dentro de um pipeline de tráfego compartilhado eliminam lacunas de cobertura e inconsistências de roteamento que afetam implantações com múltiplos fornecedores. Um único portal de proteção de aplicações abrange WAF, gerenciamento de bots e segurança de APIs, reduzindo a complexidade administrativa e mantendo uma defesa consistente e coordenada em cada interação com aplicações e APIs.

Casos de uso



Segurança e governança para IA agêntica

Visibilidade, monitoramento, guardrails e controle para fluxos de trabalho de IA agêntica



Sem JavaScript ou SDK

A implantação não requer modificações nas aplicações



Implantação em qualquer lugar

Ambientes on-premises, SaaS ou híbridos



Prevenção de ataques de bots

Defesa eficaz contra ataques em aplicações web, móveis e APIs



Não é uma caixa-preta

Acesso imediato ao tráfego de ataques, políticas e dados para respostas rápidas



Habilitação segura de IA agêntica

Torne aplicações corporativas e SaaS prontas para agentes com segurança



Arquitetura aberta

Importe dados para enriquecer análises e exporte informações para SIEMs e WAFs para aprimorar fluxos de trabalho



Prevenção da exploração de vulnerabilidades

Bloqueie ataques de dia zero e atenda aos requisitos do OWASP API Security Top 10 e PCI DSS



Inventário e avaliação de risco de APIs

Inventarie APIs internas, externas e de terceiros, avaliando continuamente os riscos



Prevenção de vazamento de dados sensíveis

Identifica e mascara automaticamente dados sensíveis para impedir exfiltração

Recursos da plataforma Cequence

Inteligência comportamental e identidade precisa

A Cequence analisa o comportamento de usuários e entidades para estabelecer identidades digitais ricas, permitindo que as organizações habilitem agentes produtivos sem abrir espaço para bots maliciosos. Ela distingue com precisão humanos de bots e diferencia automações legítimas de ameaças. Para um nível adicional de autenticação, o Biometric Check da Cequence pode utilizar o Secure Enclave do dispositivo do visitante, em vez de adicionar atrito desnecessário com um CAPTCHA.

Proteção em tempo de execução e resposta em tempo real

A Cequence opera em tempo de execução, detectando ataques no momento em que surgem e respondendo dinamicamente antes que causem danos. Em vez de depender de regras estáticas ou análises posteriores ao incidente, a plataforma avalia continuamente o tráfego em tempo real para identificar ameaças e acionar contramedidas imediatas e precisas, mantendo aplicações, APIs e dados protegidos sem interromper usuários legítimos.

Arquitetura modular e implantação flexível

A Cequence analisa e protege mais de 10 bilhões de interações entre aplicações e APIs todos os dias em algumas das maiores organizações globais dos setores financeiro, varejista e de telecomunicações. Comece com os produtos Cequence que você precisa hoje e expanda conforme suas necessidades evoluem. Implantações rápidas e flexíveis em ambientes SaaS, on-premises e híbridos significam que a plataforma se adapta à sua infraestrutura — e não o contrário.

Plataforma unificada e proteção integrada

A plataforma Cequence foi construída para integração desde sua fundação. Nossa integração nativa elimina pontos cegos e a sobrecarga operacional causada pela combinação de soluções isoladas, proporcionando uma defesa única e coerente para casos de uso envolvendo bots, APIs e IA.

“Não quero ter nenhuma interação com agentes de ameaça na borda da minha rede — quero empurrar esse perímetro o mais longe possível. A Cequence consegue interceptar tráfego malicioso de agentes de ameaça fora do nosso perímetro. Com essa capacidade, nossa postura de segurança melhorou significativamente.”

Maria Ng
CISO

