

Proteção Unificada de Aplicações da Cequence

Plataforma de Proteção de Aplicações, APIs e IA

À medida que as organizações migram cada vez mais sua infraestrutura para a nuvem, o número de aplicações e de APIs associadas cresceu de forma dramática, e os riscos de segurança aumentaram na mesma proporção. Essas aplicações estão sujeitas a ataques de bots, abuso, fraude e perda de dados — e ainda mais na era da IA baseada em agentes (agentic), em que ataques aprimorados por IA podem aprender e evoluir sozinhos. As organizações precisam de soluções que protejam suas aplicações e APIs agora e no futuro.

Desafios de segurança de API e gerenciamento de bots

As organizações atualmente enfrentam desafios únicos e multifuncionais para proteger aplicações e APIs críticas contra ciberataques. Não é apenas um problema de TI ou segurança; ataques maliciosos de bots a aplicações e APIs podem impactar o comércio eletrônico, a satisfação do cliente, o marketing, a análise de vendas e muito mais. Um programa eficaz de gerenciamento de bots e segurança de APIs é essencial para proteger a empresa e seus clientes.



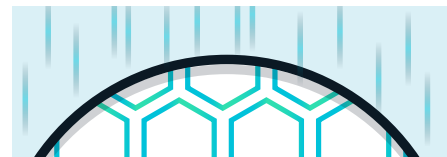
Dissipe a névoa

As APIs são rotineiramente desenvolvidas e implantadas por equipes distintas, em altíssima velocidade, em um mix de infraestrutura on-premises e em nuvem — criando uma “névoa de guerra” que encobre a visibilidade. A área de TI precisa saber quais APIs existem, onde elas estão, quem tem acesso e garantir que possuam especificações precisas.



Mantenha uma boa postura

As equipes de segurança e desenvolvimento nem sempre têm uma visão clara e consistente da postura de segurança de suas APIs em todo o portfólio de aplicações. Entender onde uma vulnerabilidade crítica, uma exposição de dados sensíveis ou uma falha de lógica de negócios pode ser explorada permite remediar com precisão as áreas de maior risco.



Proteja o núcleo

Aplicações e APIs são constantemente sondadas por atacantes em busca de qualquer oportunidade para explorar e comprometer sua organização. A capacidade de detectar e bloquear ataques em tempo real pode evitar fraudes, vazamento de dados e interrupções nos negócios.

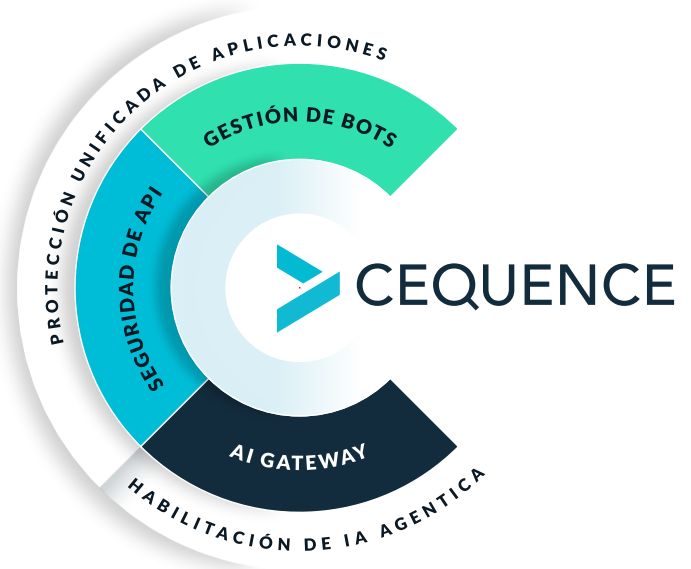
Os líderes de segurança agora estão fazendo perguntas fundamentais:

1. Quantas APIs eu tenho e onde elas estão?
2. Quais são os riscos que as minhas APIs representam?
3. Posso proteger *todas* as minhas aplicativos e APIs?
4. Meus aplicativos e APIs estão sendo atacados?

Responder a essas perguntas é fundamental para um programa de segurança robusto, uma tarefa que se torna mais difícil devido à natureza dos negócios. O lançamento de novos produtos, o crescimento orgânico e as aquisições exigem uma solução capaz de acompanhar essa mudança constante.

A Cequence Plataforma unificada de proteção de aplicações

A plataforma Cequence Unified Application Protection (UAP) une descoberta, conformidade e proteção para defender as aplicações e APIs de uma organização contra ataques, abuso de lógica de negócios e fraudes. O Cequence UAP garante a inutilidade, o fracasso e o desgaste até mesmo dos atacantes mais persistentes. Ele melhora significativamente a visibilidade e a proteção, ao mesmo tempo em que reduz custos, fraudes, perda de dados, não conformidade e interrupções nos negócios. O Cequence UAP entrega valor em minutos — e não em dias ou semanas — e oferece um modelo de implantação flexível que não exige instrumentação ou modificação dos aplicativos.



DESCOBRIR

Descoberta da superfície de ataque da API

Descubra APIs Internas e Externas | Alerta e Monitoramento de Mudanças

Descubra e inventarie toda a pegada de API da sua organização, catalogando APIs internas, externas e de terceiros. Obtenha uma visão clara da superfície de ataque acessível publicamente, permitindo que sua equipe de segurança enxergue a organização da mesma forma que um invasor. A Cequence revela continuamente novos servidores de API, endpoints e provedores de hospedagem, garantindo que as equipes de segurança e conformidade estejam sempre cientes da existência desses ativos.

CUMPRIR

Gerenciamento da postura de segurança da API

Monitorar a Postura Continuamente | Testar APIs de Pré-Produção | Corrigir Riscos

Uma solução de gerenciamento de postura de segurança de API que descobre toda a pegada de API de uma organização, garante que as APIs estejam em conformidade com as especificações, os requisitos de teste de segurança e as melhores práticas de governança, além de fornecer criação autônoma de testes de API para identificar vulnerabilidades e evitar vazamento de dados antes da produção.

PROTEGER

Gerenciamento de bots e prevenção de fraudes

Bloqueie Ataques a Aplicações e APIs | Previna Roubo, Abuso de Lógica Comercial e Fraude

Identifique e mitigue bots, prevenindo fraudes e protegendo sua organização e seus aplicativos contra toda a gama de ataques automatizados. Sem a necessidade de agentes, JavaScript ou SDKs, as impressões digitais comportamentais multidimensionais permitem a identificação até mesmo dos ataques mais sofisticados. O bloqueio nativo em tempo real garante proteção contra ataques de lógica de negócios, explorações, atividades automatizadas de bots, fraudes on-line, ataques do OWASP API Security Top 10 e muito mais.

Funciona com o Cequence AI Gateway

O Cequence AI Gateway permite o acesso de IA agente a qualquer aplicação interna, externa ou SaaS em minutos, sem necessidade de codificação. A Segurança de API pode criar automaticamente especificações de API aprimoradas que o AI Gateway utiliza para gerar servidores MCP, eliminando assim um esforço manual significativo.