

APPLICATION SECURITY

API Security

Proteja suas APIs contra abusos, fraudes e vazamento de dados.

As APIs se tornaram a base da operação digital moderna: conectam aplicações, parceiros, fornecedores e clientes — e são essenciais para negócios digitais. Mas cada API também amplia a superfície de ataque da organização. Ataques a APIs estão evoluindo rapidamente e, diferente de ameaças tradicionais, muitas vezes exploram lógica de negócio, comportamento e falhas de design — não apenas vulnerabilidades técnicas. Muitas organizações não têm visibilidade completa sobre suas APIs, criando pontos cegos que aumentam o risco de vazamento de dados sensíveis, fraudes, abuso de lógica de negócio, shadow APIs e vulnerabilidades não detectadas em produção.

• PROBLEMA

Falta de visibilidade sobre APIs, crescimento descontrolado do ambiente e incapacidade de detectar ataques sofisticados baseados em comportamento e lógica de negócio.

• SOLUÇÃO

Proteger APIs ao longo de todo o ciclo de vida — da descoberta ao monitoramento em produção — combinando análise de comportamento, testes automatizados e resposta em tempo real.

• IMPACTO

Redução de risco, mais controle sobre APIs expostas e maior capacidade de detectar e bloquear ataques antes que impactem o negócio.

OS 4 PILARES DA SEGURANÇA DE APIS COM A CG ONE + AKAMAI

1

DISCOVERY

Visibilidade completa do ambiente

- Descobrir todas as APIs — REST, GraphQL, SOAP, gRPC e outras
- Identificar APIs desconhecidas ou esquecidas (shadow APIs)
- Detectar APIs antigas, inativas ou expostas indevidamente
- Mapear domínios e endpoints ocultos

Resultado: eliminação de pontos cegos e maior controle sobre a superfície de ataque.

2

TESTING

Segurança desde o desenvolvimento

- Testes automatizados incluindo OWASP API Top 10
- Simulação de ataques reais contra APIs
- Validação de especificações contra políticas de segurança
- Integração ao pipeline CI/CD

Resultado: falhas corrigidas antes de virarem incidentes em produção.

3

DETECTION

Entendimento real do risco

- Identificar comportamentos anômalos e abuso de APIs
- Detectar falhas de configuração e riscos ocultos
- Entender quem acessa dados sensíveis e como
- Priorizar riscos com base em severidade

Resultado: mais contexto para decisões rápidas e assertivas.

4

RESPONSE

Bloqueio em tempo real

- Detectar e bloquear ataques em tempo real
- Prevenir vazamento e manipulação de dados
- Automatizar respostas e integrações com SOC/SIEM
- Reduzir impacto financeiro e operacional

Resultado: menos exposição e maior resiliência do negócio.



Proteção para workflows de IA e GenAI

À medida que aplicações baseadas em IA se tornam parte do dia a dia das empresas, as APIs deixam de ser apenas integrações técnicas e passam a ser o canal principal de interação com LLMs, agentes e automações inteligentes — criando uma nova superfície de ataque, mais dinâmica, menos previsível e muitas vezes invisível para controles tradicionais.

BENEFÍCIOS PARA A ORGANIZAÇÃO



Visibilidade Total das APIs

Saiba exatamente quais APIs existem, como são usadas e onde estão os riscos — sem pontos cegos.



Redução da Superfície de Ataque

Elimine APIs desconhecidas e vulnerabilidades antes que sejam exploradas por agentes maliciosos.



Segurança desde o Desenvolvimento

Integre segurança ao ciclo de vida das aplicações e evite que falhas cheguem à produção.



Proteção em Tempo Real

Detecte e bloqueie ataques em tempo real, antes que impactem o negócio ou comprometam dados.



Compliance e Governança

Atenda requisitos regulatórios e políticas internas com mais facilidade e rastreabilidade.



Menor Impacto Financeiro

Reduza custos com incidentes, downtime e retrabalho ao detectar e conter ameaças precocemente.

Diferencial: proteção contra abuso de lógica de negócio

Diferente de soluções tradicionais, API Security moderno vai além de assinaturas e regras estáticas — identificando padrões de uso suspeitos, detectando abuso de fluxos legítimos e analisando o comportamento de usuários e aplicações com IA/ML para ameaças desconhecidas.

Behavioral Analysis

Business Logic Abuse

IA/ML Threat Detection

Unknown Threat Identification

CG//One

+



CG One + Akamai: segurança de APIs com visão de negócio

A CG One apoia empresas na construção de uma estratégia de API Security que vai além da tecnologia, conectando segurança, desenvolvimento e operação. Em parceria com a Akamai, ajudamos a estruturar a proteção de APIs ao longo de todo o ciclo de vida — da descoberta à resposta em tempo real — garantindo visibilidade, controle e redução de risco.

CG One — Cybersecurity that Works.

Somos a CG One, a evolução da marca Compugraf. Com mais de 43 anos de história no mercado de tecnologia, entregamos soluções de cibersegurança que saem do discurso e entram em operação. Conheça nossos pilares:

AI Security

Infrastructure Security

Identity & User Security

AppSec & DevOps

Managed Security Services (MSS)

Entre em contato e saiba mais.

cg-one.com

Entre em contato →