RESUMO DO PRODUTO DA AKAMAI

Segurança de API

O API Security da Akamai é a maneira inteligente de proteger suas APIs contra abuso de lógica de negócios e roubo de dados

As ameaças a APIs estão evoluindo

As APIs impulsionam seus negócios todos os dias, conectando os negócios a parceiros, fornecedores e clientes. Mas cada API também expande sua superfície de ataque, e os agentes de ameaça sabem disso. Os ataques a APIs estão crescendo e evoluindo rapidamente, muitas vezes, de maneiras que sua proteção de aplicativos Web e de APIs pode não detectar. E sem um inventário abrangente das suas APIs, sua equipe terá um ponto cego e as APIs de suas organizações estarão desprotegidas.

Por que o API Security da Akamai?

Nossa plataforma protege as APIs durante todo o ciclo de vida, desde o desenvolvimento até a produção. Criado para organizações que expõem APIs a parceiros, fornecedores e usuários, o API Security encontra suas APIs, entende a respectiva postura de risco, analisa o comportamento e bloqueia ameaças à espreita.

Recursos essenciais do API Security

Descoberta

É comum ter APIs que ninguém conhece. No entanto, sem um inventário preciso, sua empresa está exposta a uma série de riscos de segurança. Pare de suposições e deixe-nos ajudá-lo a:

- Localizar e fazer o inventário de todas as suas APIs, independentemente da configuração ou do tipo, incluindo RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC
- Detectar APIs inativas, legadas e zumbis
- Identificar domínios esquecidos, negligenciados ou de sombra desconhecidos
- Eliminar pontos cegos e revelar possíveis caminhos de ataque

Testes

Os aplicativos estão sendo desenvolvidos no ritmo mais rápido que já vimos. Isso significa que é mais fácil que uma vulnerabilidade de segurança ou falha de projeto não seja detectada. Aproveite nossa suíte de testes do API Security para:

- Executar automaticamente mais de 150 testes que simulam tráfego malicioso, incluindo as 10 principais ameaças de segurança a APIs do OWASP
- Descobrir vulnerabilidades antes que as APIs entrem em produção para reduzir o risco de um ataque bem-sucedido
- Inspecionar suas especificações de API em relação às políticas e regras de governança estabelecidas
- Executar testes de segurança com foco em API sob demanda ou como parte de um pipeline de CI/CD

BENEFÍCIOS PARA A SUA EMPRESA

Descubra
Como entender sua superfície de ataque de APIs. Como reduzir os custos de inventários de API e atualizações de documentação. Como melhorar a conformidade com requisitos regulatórios e políticas internas.

Teste
A redução dos custos de correção ao encontrar problemas mais cedo. A melhoria da qualidade do código sem sacrificar a velocidade. O aumento da receita ao acelerar o tempo de introdução no mercado.

Detecte
Obtenha contexto essencial aos negócios sabendo exatamente o que aconteceu. Deduza por que é um problema e descubra seu impacto potencial. Determine como você deve corrigir.

Responda
Reduza os riscos ao interromper os ataques imediatamente. Reduza os custos ao corrigir vulnerabilidades antes da exploração. Reduza a perda de receita devido ao tempo de inatividade.

Akamai

Detecção

Configurações incorretas de APIs simples podem deixar você sem defesa contra cibercriminosos. Uma vez lá dentro, os hackers podem acessar e exfiltrar rapidamente seus dados confidenciais. Use nossa plataforma para:

- Verificar automaticamente a infraestrutura para descobrir configurações incorretas e riscos ocultos
- Criar fluxos de trabalho personalizados para notificar as principais partes interessadas sobre vulnerabilidades
- Identificar quais APIs e usuários internos podem acessar dados confidenciais
- Atribuir classificações de gravidade aos problemas detectados para priorizar a correção

Resposta

Não se trata mais de se, mas de quando a sua organização será atacada, o que significa que ela precisa ser capaz de detectar e bloquear ataques em tempo real. Use nossa detecção de anomalias baseada em inteligência artificial/machine learning para:

- Monitorar a violação e o vazamento de dados, violações de políticas, comportamento suspeito e ataques a APIs
- Analisar o tráfego de APIs sem alterações de rede adicionais ou agentes de difícil instalação
- Integrar-se a fluxos de trabalho existentes (emissão de tíquetes, gerenciamento de informações de segurança e eventos [SIEM] etc.) para alertar as equipes de segurança/operações
- Evitar ataques e uso indevido em tempo real com correção parcial ou totalmente automatizada

O diferencial da Akamai: bloquear na edge

O Akamai App & API Protector descobre e mitiga ameaças a APIs para aplicativos e APIs em execução por meio da Akamai Connected Cloud, e pode bloquear qualquer tráfego que contenha possíveis ameaças não descobertas pelo API Security. Quando implantadas juntas, as proteções de APIs da Akamai oferecem visibilidade abrangente e contínua das APIs e permitem descobrir, auditar, detectar e responder a preocupações do API Security em todo o aplicativo.

Quer ver como o API Security funciona? Acesse akamai.com/apisecurity e agende um horário com a nossa equipe.