

Akamai API Security para gerenciamento de ativos de APIs

As APIs estão crescendo em escopo, escala e valor à medida que as organizações se tornam cada vez mais digitais e centradas na nuvem. Elas também correm riscos cada vez maiores.

APIs expostas ou mal configuradas são predominantes e fáceis de sabotar. Elas não apenas estão desprotegidas, como também muitas vezes deixam de ser detectadas e gerenciadas, o que inclui as "APIs sombra" altamente vulneráveis. Além disso, sua proliferação dificulta a localização e o inventário de todas as APIs da empresa.

Para ajudar as organizações a obter a visibilidade de que precisam, o Akamai API Security fornece classificação e inventário automatizados de APIs para usuários internos e externos.

Para a criação de um inventário abrangente, a solução Akamai API Security usa várias fontes, como gateways de APIs, WAFs (firewalls de aplicativos da Web), serviços de nuvem pública, tráfego de redes, documentação de APIs etc. Isso garante que as alterações em APIs sejam monitoradas e que a versão mais recente seja refletida na biblioteca de APIs.

A solução Akamai API Security

O Akamai API Security consiste em quatro módulos integrados, fornecendo gerenciamento de ativos de APIs e segurança de ponta a ponta.

Descoberta

Localize e faça o inventário de suas APIs e riscos relacionados, tanto de dentro para fora quanto de fora para dentro

Postura

Descubra vulnerabilidades e configurações incorretas para acelerar a remediação e garantir a conformidade

Tempo de execução

Detecte e bloqueie ataques a APIs com análise de tráfego em tempo real alimentada por aprendizado de máquina

Testes

Encontre e corrija vulnerabilidades durante o ciclo de vida de desenvolvimento

Benefícios



Catálogo de APIs

Identifique sistemas, serviços e aplicativos que estejam expondo suas APIs com uma taxonomia detalhada



Catálogo de consultas

Explore e gerencie seu inventário de APIs de modo alinhado a casos de uso ou estruturas regulatórias



Padrões de APIs

Carregue, visualize e analise seus arquivos OpenAPI Spec e de regras de linting



Reutilização de APIs

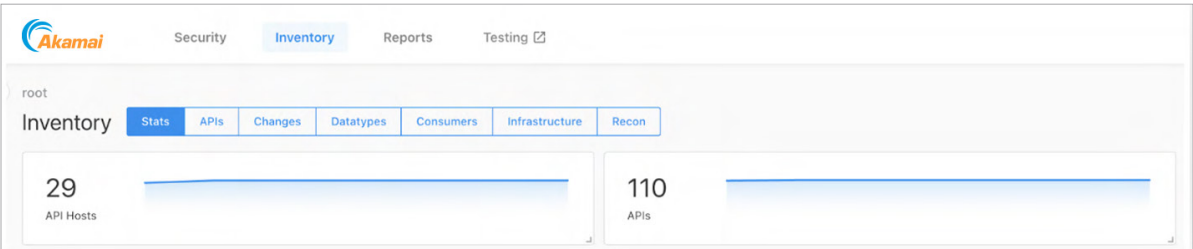
Localize APIs existentes que executem as tarefas necessárias em vez de codificar novas



Para o gerenciamento de ativos, o ponto de partida é o módulo de descoberta. Ao analisar fontes de tráfego em seu ambiente, a solução determina quantas APIs você tem e as classifica automaticamente com base em várias estruturas.

Catálogo de APIs

O Akamai API Security apresenta um catálogo abrangente de suas APIs existentes. Esse catálogo identifica os sistemas, serviços e aplicativos que expõem essas APIs e fornece uma taxonomia detalhada de cada API individual.

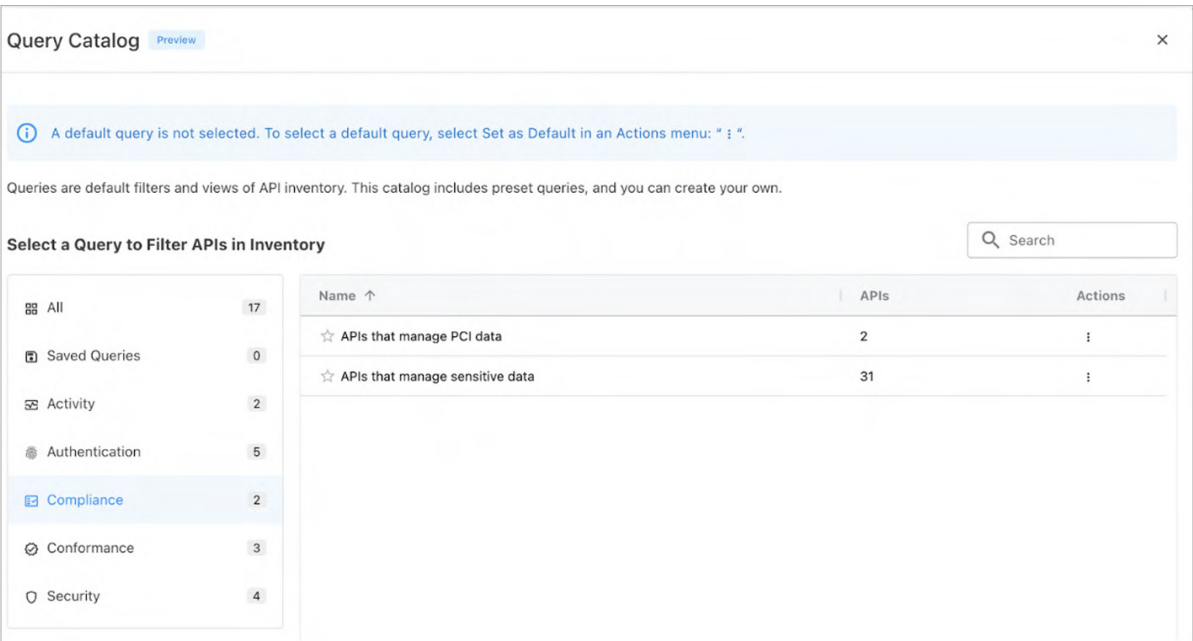


O Akamai API Security rastreia todas as alterações feitas nas APIs, permitindo que os usuários exportem documentações atualizadas como um arquivo OpenAPI Spec com base nessas alterações. Além disso, o sistema pode notificar os usuários quando novas APIs são adicionadas ao ambiente.

Você também pode usar a API de gerenciamento integrada ao Akamai API Security para extrair informações da biblioteca de APIs e criar um CMDB (banco de dados de gerenciamento de configurações) centralizado de APIs.

Catálogo de consultas

O Akamai API Security oferece um catálogo de consultas integrado, que permite explorar e gerenciar facilmente seu inventário de acordo com casos de uso específicos ou estruturas regulatórias.



Para cada API, o sistema fornecerá:

- Proprietário, tipo e fluxos de chamada da API
- Tipos de dados processados
- Métodos de autenticação compatíveis
- Origem e localização da API
- Validação se a API detectada corresponde à especificação/documentação da API
- Infraestrutura por trás da API
- Gráfico de rede completo mostrando as dependências da API

Aproveitamento de padrões de APIs

A solução também permite que você carregue, visualize e analise seus próprios arquivos OpenAPI Spec e/ou arquivos de regras de linting. Linting é o processo usado para garantir que as APIs estejam tecnicamente corretas e cumpram um conjunto de restrições adicionais que muitas vezes são documentadas na forma de diretrizes de APIs. A Akamai inclui um conjunto padrão de regras de linting para o Spectral, uma ferramenta de código aberto que permite aos desenvolvedores criar, documentar e manter APIs. Além disso, você pode carregar três formatos de arquivos de especificação:

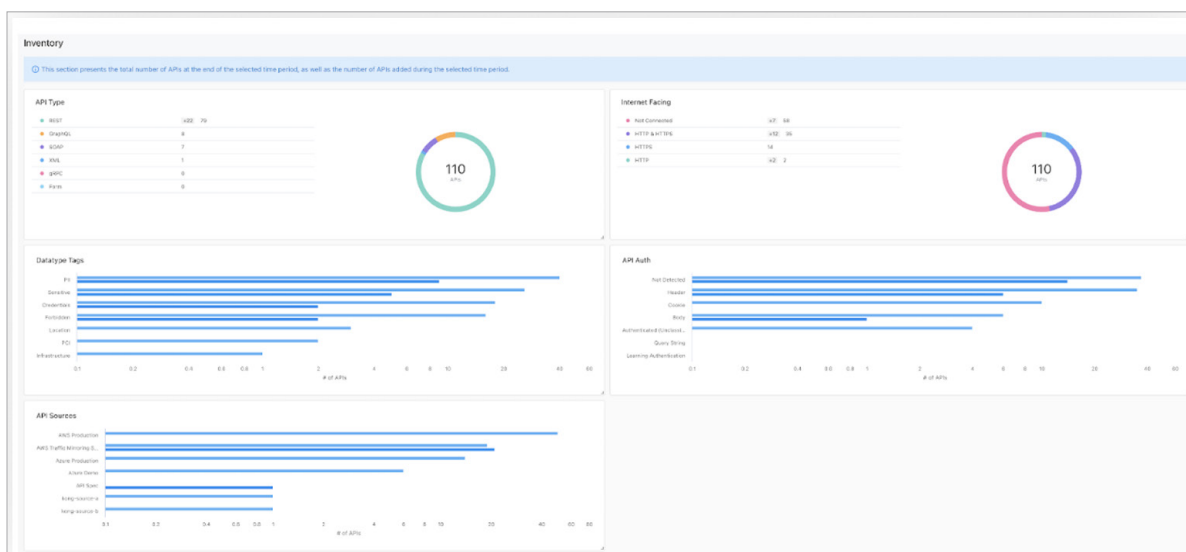
- RESTful API Modeling Language (Linguagem de modelagem de APIs RESTful)
- Web Services Description Language (Linguagem de descrição de serviços da Web)
- Web Application Description Language (Linguagem de descrição de aplicativos da Web)

Isso permite que você aproveite os padrões de APIs existentes ou defina seus próprios e os aplique no ambiente. Esses padrões podem ser específicos do setor, por exemplo, APIs de Open banking padrão para o setor de serviços financeiros com base na Banking Industry Architecture Network.

Além disso, nossa solução API Security também detectará desvios do padrão e permitirá que você defina políticas de remediação para lidar com esses tipos de detecções. O sistema também detectará e importará APIs de seus arquivos Spec e as comparará com o tráfego de rede real. Usando o recurso de reconhecimento ("recon") do Akamai API Security, também podemos detectar e importar APIs externas com base em informações simples de nomes de domínio.

Aumento da reutilização de APIs

Com uma biblioteca de APIs abrangente e fácil de pesquisar e navegar, os desenvolvedores poderão localizar APIs existentes que executam a tarefa necessária em vez de codificar novas do zero. Ao usar nosso inventário e catálogo de APIs, você pode facilmente gerar melhor reutilização de suas APIs, pois limitará quaisquer lacunas de visibilidade em seu ambiente para desenvolvedores e profissionais de segurança.



Saiba mais

As APIs são um componente-chave para que as organizações atendam aos clientes, gerem receita e operem com eficiência. No entanto, seu crescimento contínuo, a proximidade com dados confidenciais e a falta de controles de segurança tornam as APIs um alvo atraente para os invasores modernos. As organizações podem reduzir o risco e se proteger contra ataques a APIs com uma solução abrangente de segurança de APIs que forneça recursos de descoberta, gerenciamento de postura, proteção de tempo de execução e testes de segurança.

Entenda melhor como o [Akamai API Security](#) pode ajudar sua organização.