O guia definitivo para o gerenciamento da postura de segurança de APIs

Índice

Por que a segurança de APIs se tornou indispensável

As APIs permitem que os desenvolvedores de uma organização trabalhem com eficiência, em uma profissão em que a velocidade não é negociável. No entanto, embora as APIs sejam fáceis de usar pelo desenvolvedor, e fundamentais para a interoperabilidade de ativos de software e dados, a segurança de APIs não acompanhou a velocidade da inovação.

Oitenta e quatro por cento das organizações sofreram um incidente de segurança de APIs nos últimos 12 meses, contra 78% em 2023.[1] Em parte, isso se deve ao fato de as APIs também oferecerem eficiência aos invasores. Muitas APIs são desenvolvidas com configurações incorretas, erros de codificação e sem controles de autenticação. Como resultado, um ataque à API pode ser bastante simples de conduzir e uma maneira direta de roubar dados.

E, quando se trata de dados, apenas 27% das empresas com inventários completos de APIs sabem quais APIs retornam dados confidenciais, desde dados de clientes até propriedade intelectual, em comparação com 40% em 2023.[2] Com o aumento dos ataques e a diminuição da visibilidade, as empresas precisam de uma maneira de avaliar e melhorar sua postura de segurança de APIs.

1, 2. Akamai, Estudo sobre o impacto na segurança de APIs em 2024

Como é a segurança completa de APIs

À medida que o uso de APIs pela sua empresa se expande, sua superfície de ataque também se expande, criando novos desafios de segurança.

Em se tratando de proteger as APIs, as ferramentas que as organizações usam tradicionalmente, como gateways de API e firewalls de aplicativos da Web, podem oferecer uma certa proteção. Porém, à medida que seu patrimônio de APIs se torna mais complexo, por exemplo, envolvendo uma grande quantidade de APIs não gerenciadas que são difíceis de ver e proteger, algo precisa mudar.

As APIs merecem uma presença substancial no plano de jogo de segurança da empresa. E uma solução de segurança de APIs dedicada, projetada para enfrentar os riscos e os métodos de ataque atuais das APIs, pode fornecer a visibilidade e os recursos para a execução desse plano. Não é muito diferente do conceito de defesa em profundidade, em que as ferramentas se complementam para cobrir todas as etapas do caminho do ataque.

Uma plataforma completa de segurança de APIs, desenvolvida para fornecer descoberta de APIs, gerenciamento de postura, proteção de tempo de execução e testes de segurança, pode ajudar você a ver os riscos ocultos das APIs, identificar os caminhos de ataque às APIs e mitigar as ameaças descobertas em tempo real.

Em nosso e-book relacionado, O guia definitivo para a descoberta de APIs, explicamos o primeiro elemento crítico da segurança de APIs: localizar suas APIs. Depois de descobrir e inventariar todas as APIs em uso na sua organização, a próxima etapa é aprimorar a postura geral de segurança de APIs.

O gerenciamento da postura pode ser especialmente importante para empresas que compram aplicativos de provedores terceirizados e os utilizam, atribuem sua marca e vendem como se fossem seus. Por exemplo, quase todos os carros novos dos últimos cinco anos compartilham funcionalidades telemáticas praticamente idênticas. Se um invasor encontrar vulnerabilidades nos pontos de extremidade da API de um fabricante, ele terá um ponto de entrada fácil para ataques remotos de controle de contas e violações de dados.

O que este guia aborda

O gerenciamento da postura da API fornece as ferramentas para gerenciar, monitorar e manter a segurança de suas APIs durante todo o ciclo de vida da API. Este guia definitivo concentra-se nos principais requisitos para o gerenciamento da postura de segurança de APIs, incluindo a detecção de vulnerabilidades e a proteção de dados confidenciais. Ele explora e apresenta os métodos e recursos de gerenciamento da solução Akamai API Security.

Por que gerenciar a postura?

O gerenciamento de postura da API garante que você faça o melhor possível no que diz respeito à segurança de APIs. Ele ajuda você a entender o risco das APIs descobertas, identificando os tipos de dados que estão fluindo por elas, se há alguma vulnerabilidade ou configuração incorreta, se as APIs estão devidamente autenticadas, entre outras coisas. A capacidade de identificar as vulnerabilidades da API e corrigi-las rapidamente permite que você tome medidas corretivas antes que ocorra uma invasão.

O gerenciamento completo da postura oferece visibilidade de todas as atividades relacionadas às APIs para que você possa aplicar políticas de segurança, garantir a conformidade com as normas e auditar as alterações no ecossistema de APIs. Ele protege suas APIs contra ataques mal-intencionados usuários

Apenas 27% das empresas com inventários completos de APIs sabem quais APIs retornam dados confidenciais, em comparação com 40% em 2023.[3]

3. Akamai, Estudo sobre o impacto na segurança de APIs em 2024

não autorizados e violações de dados, sendo que qualquer um deles pode levar a danos significativos à reputação, perda de negócios e penalidades regulamentares.

A implementação das práticas recomendadas para o gerenciamento da postura minimiza a superfície de ataque à API e reduz grande parte do risco. Criar inventários completos das APIs e dos armazenamentos de dados confidenciais da sua organização é essencial para um bom gerenciamento de postura. Na próxima página, discutiremos outros elementos do gerenciamento da postura da API: detecção de vulnerabilidades, monitoramento da API e correção de problemas.

- ## Detecção de vulnerabilidades

  Análise: inspecione o código-fonte em busca de pontos fracos comuns, entenda como uma API interage com sistemas externos e avalie seus recursos de autorização e autenticação.

  Observação: inspecione o tráfego de e para uma API para identificar configurações incorretas, detectar vulnerabilidades e desenvolver um entendimento do comportamento da API de linha de base.

O gerenciamento da postura é apenas uma parte de um programa completo de segurança de APIs. Também é fundamental usar testes completos de pré-produção para impedir que as vulnerabilidades cheguem à produção.

- ## Monitoramento de API

  Identifique e monitore as chamadas de API na produção, rastreie as solicitações de API, detecte desvios do uso da linha de base e crie alertas quando o uso da API exceder os limites predefinidos.

- ## Remediação

  Corrija os pontos fracos ou as vulnerabilidades identificadas para tornar uma API mais segura e compatível por meio de alterações no código, ajuste fino das configurações de segurança ou correção de falhas na API. O bom gerenciamento da postura permite que a correção ocorra antes que uma vulnerabilidade possa ser explorada.

Recursos de gerenciamento da postura sem os quais você não pode viver

Talvez você já saiba, ou suspeite bastante, que a postura de segurança de suas APIs não é tão forte quanto poderia ser. Aqui estão alguns dos principais recursos que suas ferramentas de gerenciamento da postura devem incluir.

- **Classificação de dados confidenciais**
  Uma API que fornece dados meteorológicos de fontes públicas é muito menos preocupante do que uma que transmite informações de cartão de crédito. As ferramentas de gerenciamento da postura da API devem conseguir identificar rapidamente quantas APIs conseguem acessar dados de cartão de crédito, números de telefone, números de previdência social (SSNs) e outros dados confidenciais, bem como o número de usuários que acessaram dados confidenciais por meio das suas APIs.
- **Avaliação da configuração**
  Muitos ataques cibernéticos conseguem penetrar como resultado de uma simples configuração incorreta das redes, gateways de API ou firewalls que intermediam e protegem o tráfego de API. O gerenciamento de postura sólido exige a capacidade de verificar regularmente as configurações de infraestrutura e software, incluindo arquivos de registro e arquivos de configuração. A verificação regular ajuda a descobrir configurações incorretas e vulnerabilidades e identifica os riscos criados pelo desvio de configuração.
- **Pontuação de confiança do invasor**
  Procure um mecanismo de pontuação de confiança do invasor que use algoritmos avançados de machine learning treinados para avaliar sinais externos e internos, inclusive comportamento de API, padrões de tráfego de rede, dados de

geolocalização, feeds de inteligência contra ameaças e outros fatores contextuais. Isso pode ajudar você a determinar o nível de confiança de que um incidente no tempo de execução detectado é resultado de atividade mal-intencionada. Esse recurso exclusivo permite que os clientes se concentrem rapidamente nas ameaças críticas e criem fluxos automáticos de correção e notificação para ataques de alta probabilidade.

- **Fluxos de trabalho personalizados**
  Além da gravidade personalizável, você precisa conseguir criar fluxos de trabalho para agir imediatamente quando as vulnerabilidades forem identificadas. Os fluxos de trabalho personalizados podem variar desde a criação de tíquetes de problemas até a notificação das principais partes interessadas e a atualização das configurações de rede.

- **Documentação gerada automaticamente**
  A documentação da API informa aos consumidores de uma API o que ela faz e como usá-la. As APIs seguras devem ser avaliadas quanto à conformidade com as especificações e documentadas com precisão. Documentação incompleta ou inexistente torna os testes de segurança mais difíceis, aumentando o risco de uma API entrar em produção com uma vulnerabilidade não detectada.

Muitas vezes, esse problema acaba ganhando uma proporção maior devido à terceirização do desenvolvimento de APIs. Independentemente da origem do problema, as documentações desatualizadas, incompletas e ausentes são inaceitáveis se você quiser que seu programa de segurança de APIs seja bem-sucedido.

A especificação OpenAPI (anteriormente chamada de Swagger) define descrições de interface padrão. As ferramentas de gerenciamento da postura devem conseguir gerar automaticamente a documentação completa da OpenAPI com base no estado atual e futuro da API para garantir que todas as APIs sejam documentadas corretamente e que a documentação esteja atualizada.

Líder em seguros aprimora a postura de segurança de APIs com a Akamai

À medida que os consumidores se afastam do físico em favor do digital, as empresas de serviços financeiros precisam inovar em um ritmo acelerado. Como muitos de seus pares, a Aflac, principal fornecedora de seguro saúde suplementar nos Estados Unidos, enfrentou desafios crescentes de segurança de APIs.

A Aflac recorreu à plataforma Noname API Security (agora parte da Akamai API Security) para atender às suas necessidades. O módulo de gerenciamento de postura ajuda a equipe a identificar os tipos de dados que atravessam as APIs da empresa, fornecendo visibilidade sobre quais APIs acessam dados confidenciais e identificando quaisquer anomalias no acesso aos dados.

Leia o estudo de caso completo da Aflac para saber mais.

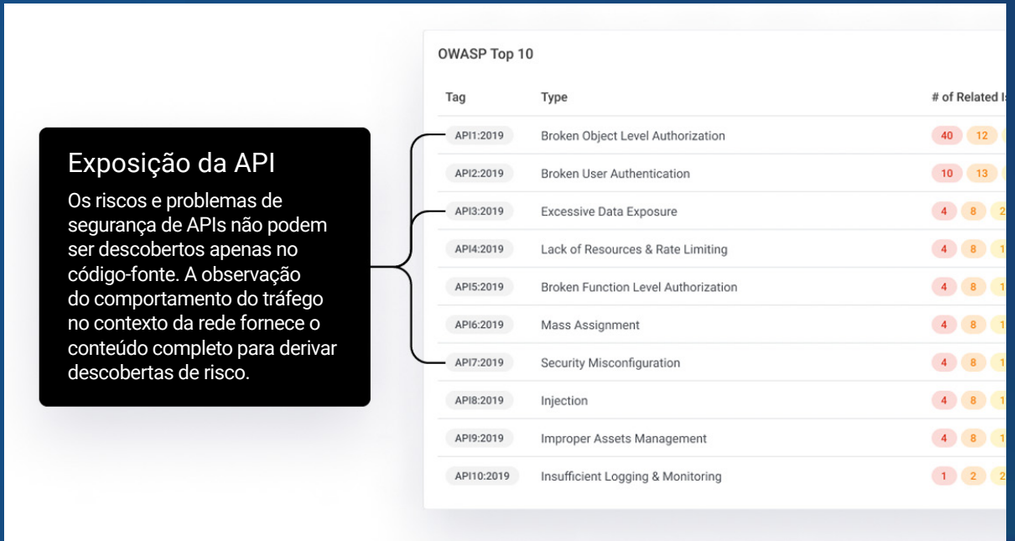
"Estávamos cientes de que nossa pegada de API era grande e queríamos ter certeza absoluta de que cada API era contabilizada, que tínhamos visibilidade total de suas operações e que elas estavam sendo continuamente testadas quanto a riscos de segurança.

- DJ Goldsworthy, vice-presidente de operações de segurança e gerenciamento de ameaças, Aflac

A abordagem da Akamai para o gerenciamento da postura

O módulo de gerenciamento da postura da solução Akamai API Security oferece uma visão completa do tráfego, do código e das configurações para avaliar a postura de segurança de APIs da organização. A Akamai determina qual é a sua verdadeira superfície de ataque em APIs e aplicações Web e descobre todas as formas de dados confidenciais que passam por suas APIs, ajudando na proteção de dados confidenciais.

Configurações incorretas de APIs simples podem deixar você sem defesa contra cibercriminosos. Uma vez dentro, os hackers podem acessar e exfiltrar rapidamente seus dados confidenciais. O módulo de gerenciamento da postura da solução Akamai API Security fornece esses principais recursos:



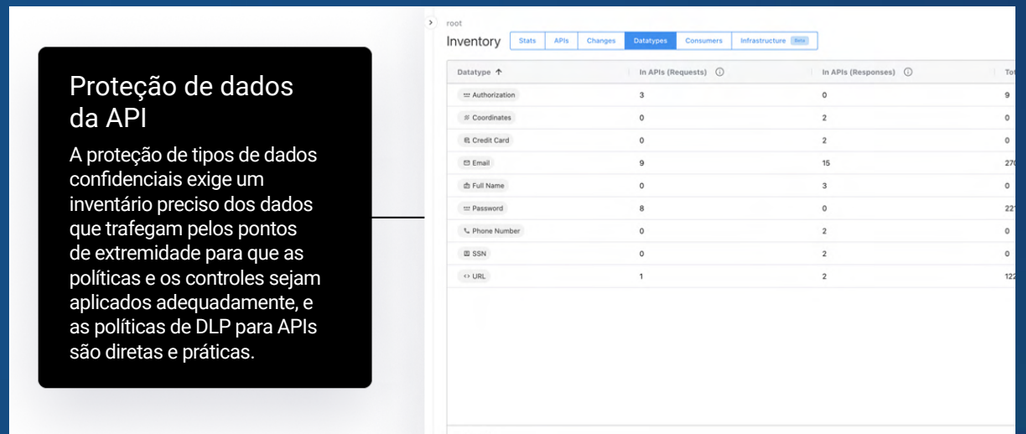
- integração fora de banda para descoberta constante de APIs no local, e em nuvens híbridas e públicas;
- um inventário de API simples e buscável que inclui detalhes de esquema, posicionamento de rede e tipos de dados;
- geração automatizada de documentação de APIs (OAS/Swagger);
- análise com reconhecimento de contexto de vulnerabilidades e configurações incorretas das APIs com priorização
- detecção de todas as vulnerabilidades do OWASP Top 10 em segurança de APIs;
- descoberta e classificação automatizadas de dados confidenciais e alterações de APIs.

Exposição da API

Além de descobrir riscos no código de uma API, também é importante observar o tráfego das APIs com atenção ao comportamento, típico ou atípico, e no contexto da rede.

O gerenciamento da postura da solução Akamai API Security analisa o conjunto mais amplo possível das fontes para detectar vulnerabilidades, incluindo arquivos de registro, reproduções de tráfego histórico, arquivos de configuração e muito mais. A solução detecta todas as vulnerabilidades do OWASP Top 10 de segurança de APIs e protege as APIs contra vazamento de dados, problemas de autorização, abuso, uso indevido e corrupção de dados.

A Akamai identifica e prioriza de forma inteligente as possíveis vulnerabilidades. As vulnerabilidades podem ser corrigidas manualmente, de forma semiautomática ou totalmente automática por meio de integrações com WAFs, gateways de API, ferramentas SIEM e ITSM, ferramentas de fluxo de trabalho e outros serviços.



Proteção de dados de API

A proteção de tipos de dados confidenciais exige um inventário preciso dos dados que trafegam pelos pontos de extremidade para que as políticas e os controles sejam aplicados adequadamente, e as políticas de DLP ou APIs são diretas e práticas.

A conformidade está assumindo uma dimensão totalmente nova com o crescimento do uso de APIs. Uma onda de regulamentações surgiu em resposta à crescente ameaça de ataques. Os setores regulamentados agora devem considerar as APIs em seus planos de conformidade.

O módulo de gerenciamento da postura da solução Akamai API Security identifica todas as formas de dados confidenciais que circulam por suas APIs, incluindo todas as informações de identificação pessoal (PII), como cartões de crédito, SSNs, endereços, informações sobre seguros e muito mais. Ao reduzir o acesso a esses tipos de dados e implementar uma estrutura de gerenciamento de dados, ajudamos você a garantir que os dados confidenciais estejam onde precisam estar e protegidos contra ameaças mal-intencionadas.

Como o gerencia-mento da postura para APIs pode ajudar você

Toda vez que um cliente, parceiro ou fornecedor interage digitalmente com sua organização, há uma API nos bastidores que facilita a troca rápida de dados (geralmente confidenciais). Obter visibilidade de todas as APIs da sua organização e avaliar seus atributos de risco, como, por exemplo, quais APIs retornam dados confidenciais, pode ajudar você a proteger sua organização contra um vetor de ataque que cresce rapidamente. O gerenciamento da postura de segurança de APIs também pode ajudar você a garantir a conformidade com as normas globais que visam evitar violações de dados.

Saiba mais sobre as normas de proteção de dados que exigem a visualização e a proteção de todas as APIs.

Saiba como podemos ajudar você agendando uma demonstração personalizada do Akamai API Security.

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em **www.akamai.com** e **www.akamai.com/blog**, ou siga a Akamai Technologies no **X**, antigo Twitter, e **LinkedIn**. Publicado em 12/24.

Akamai