Guia definitivo para proteção de tempo de execução de APIs

Índice

Introdução

Por que a segurança de APIs é tão importante

Na corrida para atender às necessidades dos clientes, as organizações enfrentam pressão para desenvolver, produzir e aprimorar rapidamente aplicativos, serviços e ferramentas de IA generativa. Essa necessidade de velocidade, infelizmente, resulta em um risco oculto: As APIs que trabalham nos bastidores para todas essas inovações são muitas vezes construídas com configurações incorretas, erros de codificação e sem controles de segurança. E quando essas APIs atingem o estágio de produção, não são apenas os usuários finais que interagem com elas; os invasores constantemente testam maneiras de comprometer as APIs e acessar os dados que são trocados.

APIs mal configuradas e comprometidas são cada vez mais um fator-chave de violações significativas de dados, e ainda assim poucas organizações conseguem acompanhar as milhares de chamadas de APIs dentro de seus ecossistemas digitais. Menos ainda estão totalmente protegidas contra ameaças de tempo de execução de APIs.

Por exemplo, em 2021, uma empresa de varejo de fitness encontrou um bug em uma API para dados de conta de usuário, que permitia que qualquer pessoa fizesse solicitações não autenticadas de dados, incluindo idade, sexo, cidade, peso e data de nascimento. Embora essa vulnerabilidade tenha sido felizmente detectada e relatada à empresa por um pesquisador de segurança, bugs como esse podem passar despercebidos e ser explorados por semanas ou meses.

Em se tratando de proteger as APIs, as ferramentas tradicionais das quais organizações geralmente dependem, como, por exemplo, gateways de API e firewalls de aplicativos da Web, podem oferecer uma base de proteção. No entanto, as equipes de segurança atuais necessitam de camadas de segurança adicionais, à medida que os ataques a APIs crescem em número e em sofisticação. A chave é aumentar os controles existentes com insights mais profundos sobre vulnerabilidades, possíveis caminhos de ataque, atividades maliciosas e comportamento das APIs.

As organizações podem alcançar esses recursos com uma solução abrangente de segurança de APIs, estruturada em quatro áreas principais:

1. Descoberta de APIs
2. Gerenciamento de postura de APIs
3. Proteção do tempo de execução de APIs
4. Teste abrangente de segurança de APIs

O que este guia aborda

A proteção de tempo de execução de APIs é o processo de proteger as APIs à medida que operam e gerenciam solicitações durante o funcionamento normal. Este guia aborda os principais requisitos para proteção de tempo de execução de APIs, incluindo monitoramento de APIs em defesa de mal configuração e exploração, e prevenção de ataques contra APIs. Ele explora os conceitos básicos de prevenção de tempo de execução e apresenta os recursos de prevenção de tempo de execução oferecidos pela Akamai API Security.

Por que proteção do tempo de execução?

A proteção de tempo de execução de APIs protege as APIs durante toda a fase de produção do ciclo de vida, quando as APIs estão operacionais e disponíveis para interação com os usuários finais pretendidos — e com os invasores. Com recursos que ajudam as organizações a identificar e tratar rapidamente solicitações de APIs maliciosas, recursos eficazes de proteção de tempo de execução podem proteger APIs contra uma variedade de ameaças pós-implantação, incluindo:

- Extração de grandes volumes de dados confidenciais de uma API por invasores
- Ataques de escalonamento de privilégios que exploram bugs de segurança
- Implantação de APIs não autorizadas fora dos processos normais

Bloquear ameaças contra APIs de tempo de execução requer uma compreensão do contexto das operações para cada API individual, incluindo acesso à API, uso e comportamento. Para começar, você precisa saber o escopo do seu estado de APIs. Nosso Guia definitivo para a descoberta de API explica a importância de um inventário de APIs. Com um inventário de APIs completo, você pode monitorar todo o tráfego de APIs e construir uma compreensão básica do comportamento "típico" para cada API que pode ser usada para reconhecer comportamentos anômalos.
A proteção de tempo de execução de APIs deve detectar:

- Vazamento de dados
- Violações de política de dados
- Ataques de segurança de APIs
- Violação de dados
- Comportamento suspeito

Além disso, a proteção de tempo de execução deve registrar o tráfego de APIs, monitorar o acesso a dados confidenciais, detectar ameaças e bloquear ou corrigir vetores de ataque.

Monitoramento do tráfego de APIs para ataques

Observar o comportamento do tráfego de APIs é essencial para identificar riscos. A implantação de uma solução de monitoramento sem uma imagem precisa do seu estado de APIs apenas fornece visibilidade limitada. Depois que sua pegada de API for inventariada, a proteção de tempo de execução de APIs deve monitorar continuamente o tráfego e o consumo de APIs e procurar vulnerabilidades e configurações incorretas.

Detecção de comportamento anômalo

Ter uma linha de base do comportamento normal das APIs torna possível identificar qualquer coisa fora do comum. A reprodução de dados históricos pode ajudar a identificar comportamentos anômalos, o que também pode revelar a intenção de um invasor.

Quaisquer anomalias potenciais devem ser examinadas mais detalhadamente no contexto de outras ações que ocorrem dentro do aplicativo ou da rede. Por exemplo, se as solicitações de dados forem geralmente de um certo tamanho e uma chamada de API solicitar dados fora do intervalo das solicitações usuais, ela deve ser sinalizada. Pode ou não ser malicioso, mas a anomalia requer uma inspeção adicional.

Detecção de exposição de dados

Algumas das APIs do seu estado provavelmente enviam e recebem dados confidenciais. Informações confidenciais expostas devido a uma vulnerabilidade de segurança permitem que um invasor escale privilégios ou outras configurações de controle de acesso inadequado. A IA e o machine learning podem ser fundamentais na análise de tráfego em tempo real e na detecção de anomalias, fornecendo insights contextuais sobre vazamento de dados, adulteração de dados, violações de políticas de dados, comportamento suspeito e ataques à segurança de APIs.

Um tipo de ataque que se tornou cada vez mais comum é o de cibercriminosos conseguirem acesso a chaves de API válidas. Uma vez que um invasor tem chaves válidas em mãos, praticamente a única maneira de se proteger contra o uso indevido da API e possível violação de dados é a capacidade de detectar e bloquear comportamentos anômalos e exposição de dados.

Auditoria de segurança das APIs

As ferramentas de auditoria de segurança de APIs devem monitorar o tráfego em tempo real e alertá-lo sobre ataques e outras intenções maliciosas. No mínimo, a auditoria de segurança de APIs deve:

- Realizar monitoramento contínuo para identificar invasores e solicitações maliciosas
- Executar uma análise passiva das APIs, interna e externamente, em busca de erros de configurações e falhas que possam permitir ou piorar uma violação ou enfraquecer as defesas
- Aplicar políticas sobre quais dados devem (e não devem) ser enviados ou recebidos pelas APIs

A proteção de tempo de execução de APIs também deve ser complementada pelo gerenciamento de postura de APIs, que identifica configurações incorretas e vulnerabilidades conhecidas. Confira nosso **Guia definitivo para gerenciamento de postura de APIs** para obter mais insights.

Recursos de proteção de tempo de execução sem os quais você não pode viver

Se sua organização estiver desenvolvendo e implantando APIs ativamente, a proteção robusta de tempo de execução precisa fazer parte do seu programa de segurança de APIs. Veja aqui alguns dos principais recursos que suas ferramentas de proteção de tempo de execução devem incluir.

Monitoramento fora de banda em tempo real

O monitoramento de segurança de APIs não deve impactar, retardar ou adicionar latência ao tráfego das APIs. Ele deve ser executado completamente fora de banda, sem a necessidade de alterações na rede nem agentes complicados e difíceis de instalar. As ferramentas de proteção de tempo de execução devem espelhar o tráfego de fontes de dados identificadas e realizar análises sobre os dados desse tráfego em segundo plano, com alertas em tempo real de quaisquer problemas descobertos.

A Akamai opera fora de banda e sem agentes por padrão, mas oferecemos opções de detecção baseada em agentes e bloqueio em linha, se necessário.

Detecção de anomalia e exploração de APIs

A coleta passiva de dados não é suficiente, especialmente porque o número de APIs e o volume total de tráfego de APIs continuam a crescer. A atividade de APIs deve ser analisada continuamente para detectar eventos anômalos e alertar equipes de segurança e operações. As ferramentas de plataforma de última geração incorporam recursos de IA e de machine learning para analisar o tráfego em tempo real e aproveitar insights contextuais sobre vazamento de dados, adulteração de dados, violações de políticas de dados, comportamento suspeito e ataques à segurança de APIs.

Prevenção de ataques a APIs e remediação de riscos

Uma vez que uma anomalia ou outro problema foi identificado e um alerta gerado, o tempo é essencial. O movimento não autorizado de dados confidenciais por APIs ou outro uso indevido suspeito de APIs deve ser detectado e remediado. A proteção do tempo de execução não deve apenas impedir o uso indevido das APIs pela integração com seus firewalls e gateways de APIs existentes, mas também deve fornecer opções de remediação, automatizadas quando possível. Procure por recursos que incluam pontuações de confiança do invasor que ajudam sua equipe a determinar se sinais de abuso, ataques ou violações são legítimos e precisam de escalonamento.

Integrações para resposta a incidentes

Como regra geral, as ferramentas de proteção de tempo de execução devem se integrar facilmente com as outras ferramentas de segurança, monitoramento e gerenciamento que sua organização usa. Por exemplo, quando um incidente ocorre, as ferramentas de proteção de tempo de execução devem incluir as integrações necessárias para garantir que as tarefas de correção sejam atribuídas às equipes apropriadas. Se forem detectados erros de configurações, violações de políticas de dados ou comportamentos suspeitos, eles devem ser reportados ao gateway da API, sistema SIEM e outros mecanismos de segurança da informação para garantir o nível certo de conscientização. Ter um recurso de pontuação de confiança do invasor pode permitir que as equipes filtrem o ruído e concentrem sua atenção nas verdadeiras prioridades de segurança de APIs.

Rapyd

A Rapyd, uma empresa global de processamento de pagamentos e fintech, opera sistemas de pagamento em mais de 100 países. Sem visibilidade granular sobre o uso e o comportamento das APIs, a empresa precisava de uma maneira melhor de proteger as APIs voltadas para o público — e centenas de APIs internas — em um sistema global altamente complexo que opera a partir da nuvem AWS. A Rapyd precisava de um inventário granular de todas as suas APIs, visibilidade de configurações incorretas e vulnerabilidades e priorizou alertas de forma inteligente para uma abordagem de correção mais lógica.

O Akamai API Security atendeu às necessidades da Rapyd com visibilidade abrangente e proteção de tempo de execução que usa machine learning para criar uma linha de base do tráfego para cada API, com detecção e correção de anomalias automatizadas.

Leia toda a história do cliente

> Agora podemos avaliar os riscos da maneira mais cientificamente verdadeira possível e controlar nosso futuro.
>
> – Nir Rothenberg
> CISO, Rapyd

Proteção do tempo de execução do Akamai API Security

A capacidade de identificar e de impedir ataques a APIs à medida que estão acontecendo deve ser parte integrante do seu programa de avaliação de conformidade e risco. Você pode pensar nisso como sua última linha de defesa se outros controles de segurança não forem suficientes.

O módulo de proteção de tempo de execução do Akamai API Security inclui todos os recursos descritos na seção anterior. Sua principal função é detectar e bloquear ataques às APIs em tempo real. O monitoramento automatizado baseado em machine learning é usado para realizar análises do tráfego e fornecer informações contextuais sobre vazamento de dados, adulteração de dados, violações de políticas de dados, comportamento suspeito e ataques à segurança de APIs. A proteção de tempo de execução detecta anomalias e possíveis ameaças no tráfego de APIs e facilita a correção com base nas políticas de resposta a incidentes pré-selecionadas.

A proteção de tempo de execução se integra com WAFs, gateways de APIs, ITSMS, SIEMs e outras ferramentas de fluxo de trabalho para oferecer uma defesa holística contra ataques. Você pode optar por automatizar totalmente a correção de ameaças ou exigir diferentes níveis de intervenção manual para obter maior visibilidade e controle. A solução Akamai API Security também possui integração nativa com a plataforma Akamai que nos permite bloquear IPs de invasores diretamente na edge.

Geração de problemas

Usando machine learning, a Akamai cria um modelo para cada API. Essa linha de base do comportamento normal é então usada para detectar ataques à lógica de negócios da API, como BOLA (Broken Object Level Authorization, autorização em nível de objeto corrompida), na qual um indivíduo ganha acesso a dados aos quais não deve ter acesso. A Akamai gerará um problema em tempo real sempre que o tráfego da API se desviar do comportamento normal. Um problema é muito parecido com

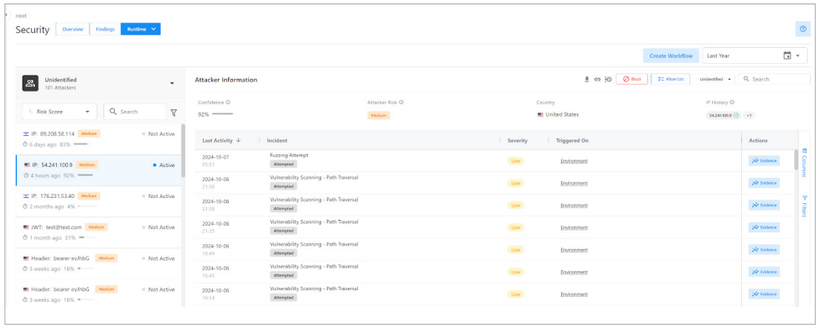
um alerta e é gerado sempre que o comportamento anômalo da API é detectado ou quando uma configuração incorreta é encontrada. À medida que os problemas são gerados, os alertas podem ser enviados automaticamente para um SIEM, como Splunk ou QRadar. Os alertas também podem ser enviados automaticamente para um sistema de tíquetes, como ServiceNow ou Jira.

Emissão de detalhes

Cada problema gerado pelo módulo de proteção de tempo de execução do Akamai API Security inclui gravidade, status, um mapeamento para o OWASP API Security Top 10 — e informações do invasor, quando aplicável.

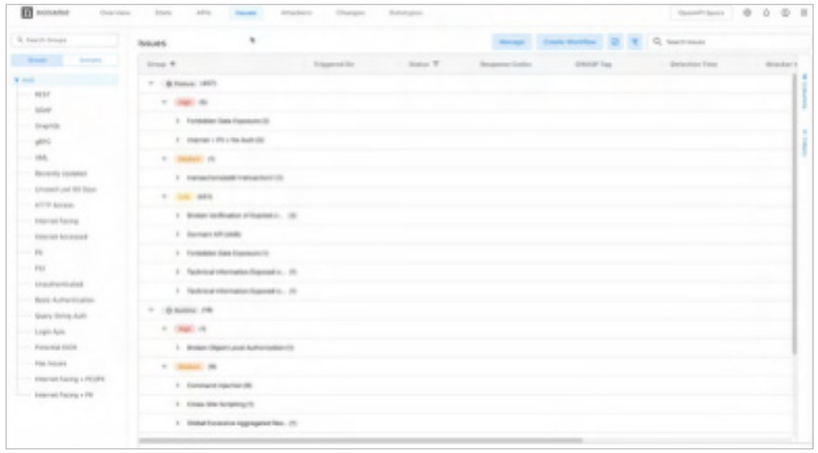
As páginas de detalhes do problema incluem uma descrição do problema e seu potencial impacto para a organização e fornecem recomendações de remediação. O Akamai API Security também permite que as organizações vejam que tipos de ações os invasores tomaram durante um período específico, com um registro histórico de cada ataque e a capacidade de agir contra agentes maliciosos.

Exemplo: Visibilidade das ações dos invasores

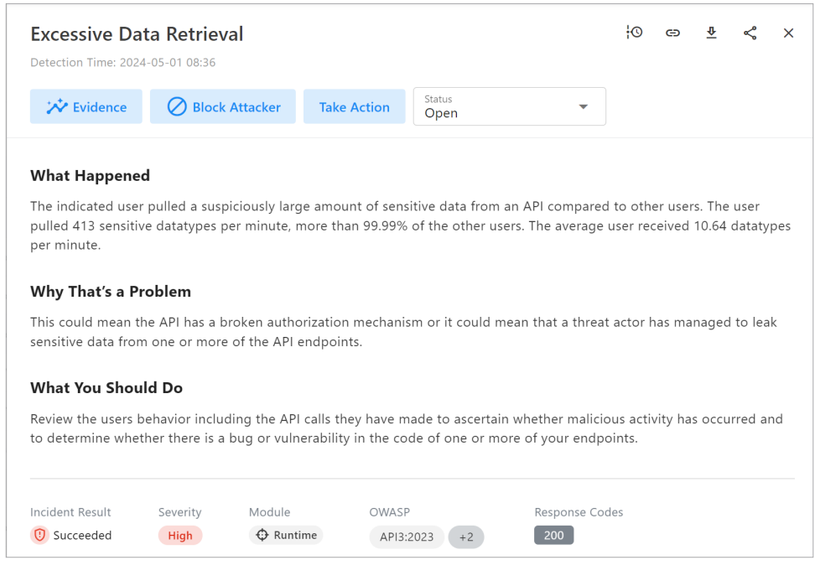


Cada problema inclui evidências. Evidências são os detalhes da sessão do invasor que levaram ao problema gerado, e uma cópia da solicitação e resposta da API, tanto os cabeçalhos quanto o corpo, para ajudar na triagem e na correção do problema rapidamente. Com painéis intuitivos, funções de filtragem, alertas e recursos de relatórios, o módulo de proteção de tempo de execução da solução do Akamai API Security pode ajudar as organizações a determinar o que aconteceu, por que isso aconteceu e o que exatamente precisa ser feito.

Exemplo: Relatórios sobre problemas de APIs com evidências



Exemplo: Insights sobre recuperação excessiva de dados



Ações de política

O Akamai API Security fornece a capacidade de tomar uma ação de política semiautomatizada para cada problema gerado. As ações podem incluir a abertura de um tíquete, o envio de informações para um SIEM ou o envio de um webhook para um sistema de terceiros. Elas também podem incluir o bloqueio de um invasor. Os tipos de ações disponíveis são determinados pelos tipos de integrações configurados na plataforma Akamai.

A solução inclui várias políticas predefinidas prontas para uso para detectar ataques a APIs e configurações incorretas de APIs. O Akamai API Security também inclui mais de 20 tipos de dados pré-configurados para ajudar você a criar as políticas de dados necessárias para detectar e tomar medidas quando tipos de dados confidenciais estão atravessando suas APIs.

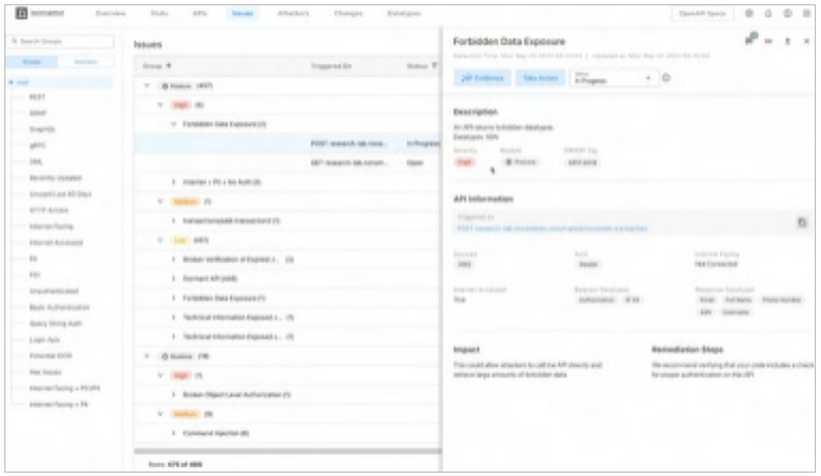
Em resumo, o módulo de proteção de tempo de execução da solução do Akamai API Security inclui detecção e prevenção em tempo real de ataques a APIs com a detecção constante de configurações incorretas de APIs, além de muitas integrações populares de fluxo de trabalho que simplificam as operações e a correção.

Anatomia de um incidente de segurança de API

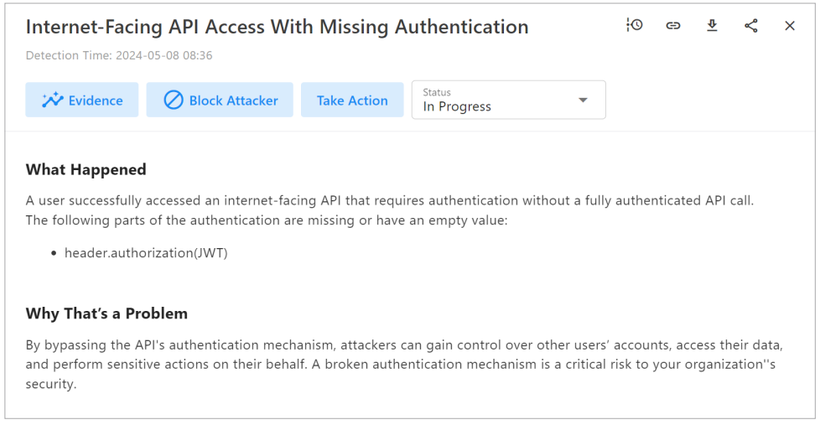
Vamos olhar mais de perto para um exemplo de exposição proibida de dados. Este exemplo ilustra um problema de postura interno a uma API. A plataforma Akamai está contextualmente ciente dos tipos de dados e valores associados a cada API.

Na figura abaixo, os dados proibidos estão sendo expostos por uma API. A plataforma Akamai detectou o tipo de dados que estão sendo transmitidos, neste caso um CPF, e entendeu que o tipo de dados CPF tinha sido previamente marcado como proibido. A Akamai também pode detectar configurações incorretas externas à API, como APIs acessíveis à Internet, mas não registradas em um gateway de API.

Exemplo: Insights sobre exposição proibida de dados



Exemplo: Identificar APIs com autenticação ausente



Próximas etapas para alcançar uma proteção eficaz de tempo de execução de APIs

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). A implementação dos principais recursos de proteção de tempo de execução de APIs, por exemplo, o monitoramento de APIs para se defender contra a configuração incorreta e a exploração, e a prevenção de ataques a APIs, pode ajudar você a proteger sua organização contra um vetor de ataque de rápido crescimento.

Saiba como avaliar os fornecedores de segurança de APIs para garantir que eles ofereçam recursos críticos de proteção de tempo de execução.

Saiba como podemos ajudar 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 **akamai.com** e **akamai.com/blog**, ou siga a Akamai Technologies no **X**, antigo Twitter, e **LinkedIn**. Publicado em 12/24.

Akamai