Akamai

WHITE PAPER

11 recursos essenciais de detecção e resposta de APIs

Como desenvolver sua estratégia de segurança de APIs

Introdução

As APIs desempenham um papel fundamental em todos os aplicativos que sua organização cria para clientes, usa internamente e disponibiliza para fornecedores. A função delas: trocar informações (geralmente dados confidenciais) entre tecnologias. Onde elas estão presentes: não apenas em seus aplicativos, mas também em suas migrações na nuvem, ferramentas de IA generativa e cadeia de suprimentos digital.

O desafio é que as APIs também ganharam espaço na superfície de ataque da sua organização.

À medida que as empresas correm para inovar, as APIs são desenvolvidas de modo apressado, testadas de forma insuficiente e lançadas em produção com configurações incorretas e ausência de controles de segurança. Além disso, essas APIs se tornaram tão numerosas e dispersas que as equipes de segurança não conseguem ter uma visão completa de grande parte do seu conjunto de APIs. E sem a devida visibilidade, as organizações:

1. Não conseguem detectar APIs não gerenciadas, esquecidas e persistentes com exposição não verificada a dados confidenciais, à Internet e a invasores
2. Por sua vez, não conseguem avaliar os riscos das APIs: por exemplo, apenas 27% das empresas com inventários completos de APIs sabem quais delas retornam dados sensíveis, uma queda em relação a 40% em 2023
3. Ficam com uma superfície de ataque repleta de vulnerabilidades centradas em APIs que os invasores exploram com frequência e facilidade

Até recentemente, as organizações se sentiam confortáveis em confiar em uma lista de ferramentas usadas para gerenciar APIs e obter uma linha de base de proteção. Considerando que 84% das organizações enfrentaram um incidente de segurança de APIs nos últimos 12 meses, versus 78% em 2023, algo precisa mudar.

À medida que os ataques de API aumentam em número e sofisticação, é hora de explorar a adição de novas camadas de proteção a ferramentas como gateways de API, firewall de aplicativos da Web (WAFs) e plataformas de proteção de aplicativos da Web e de APIs (WAAP).

Essas novas camadas devem proporcionar maior visibilidade de todas as APIs em seu ambiente e seus riscos, incluindo a grande parte das APIs que não são gerenciadas, como:

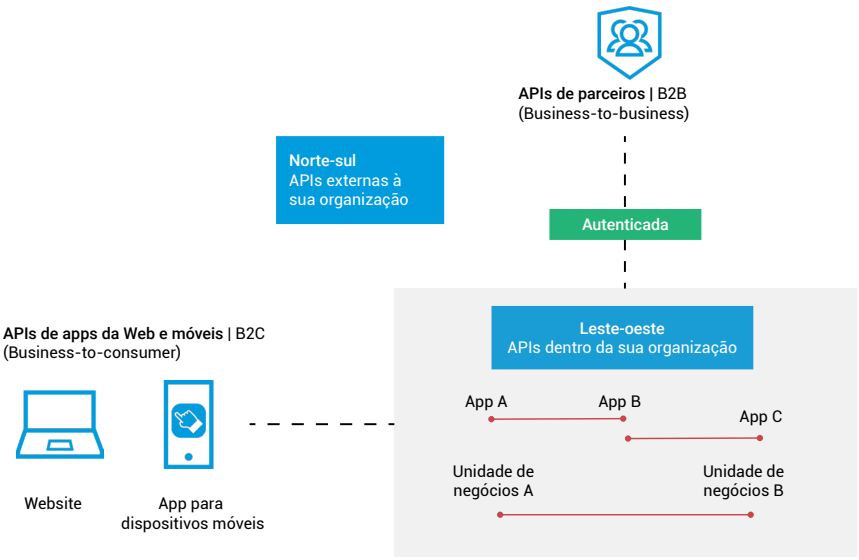
- APIs zumbis que deveriam ter sido desativadas, mas permanecem ativas
- APIs de sombra não documentadas e que devem ser eliminadas ou introduzidas em processos formais de governança

As organizações também precisam de recursos mais profundos para detectar e lidar com ataques e abusos de API, incluindo todas as ameaças detalhadas no relatório OWASP Top 10 API Security Risks. Com o objetivo de encontrar e corrigir vulnerabilidades em todo o ciclo de vida de uma API, as empresas devem adotar testes de segurança rigorosos e em tempo real para APIs, desde os primeiros estágios de desenvolvimento até a produção.

Isso significa acrescentar uma nova ferramenta para cada problema que surgir? Na verdade, é mais como garantir que uma orquestra tenha os músicos certos para cada papel, tocando as notas corretas nos momentos certos e em perfeita harmonia com os outros músicos.

Ao pensar em como adicionar novas camadas à proteção de suas APIs, considere a abordagem de defesa em profundidade que as equipes de segurança aplicam a outras ameaças, como a implantação de uma série de controles para detectar, prevenir e mitigar os efeitos de um ataque de ransomware. É exatamente assim que as organizações devem pensar sobre APIs.

Neste white paper, vamos analisar 11 recursos críticos que você pode incorporar à sua estratégia de segurança de APIs, com foco na detecção e resposta de ameaças a APIs.



O contexto é fundamental

Como a detecção e resposta a ameaças a APIs se encaixam em sua estratégia de segurança de APIs?

Como você provavelmente viu em primeira mão, as APIs mudaram a forma como as empresas operam, permitindo mais casos de uso, acelerando a mudança, transportando mais dados confidenciais e estando mais abertas a mais usuários. Não é de se surpreender que as organizações tenham criado muitos mais canais de API do que interfaces de aplicativos da Web. E o risco aumenta à medida que essas APIs em proliferação são integradas com volumes cada vez maiores de dados essenciais para o negócio e lógica de processos empresariais.

Dada a prevalência das APIs em diversas tecnologias que as equipes de segurança já estão protegendo (ou seja, aplicativos), a maioria das categorias de produtos de segurança oferece algum tipo de suporte para APIs. No entanto, APIs e aplicativos não são iguais: eles até mesmo aparecem como ativos diferentes em algumas estruturas de conformidade. Não basta adicionar recursos de proteção fragmentada contra ameaças a APIs a, por exemplo, um produto de segurança de aplicativo existente. As APIs merecem mais foco do que normalmente recebem na maioria das organizações. As equipes de segurança de hoje devem encarar as APIs como uma classe de ativos distinta, com um conjunto próprio de atributos de risco, e buscar recursos importantes para visualizar e proteger cada API em grande escala.

No passado, se uma organização tivesse um inventário de APIs e algumas ferramentas de base para gerenciamento e proteção de APIs, ela teria uma boa chance de evitar uma variedade conhecida de ataques comuns a APIs. Infelizmente, os invasores de hoje inovam da mesma forma que as empresas, com um foco semelhante em melhoria contínua.

- Agentes mal-intencionados estão evoluindo suas táticas de forma estratégica para contornar as ferramentas usadas pela maioria das organizações para defender suas APIs.
- Da mesma forma que a maioria das empresas usa IA, os atacantes estão ampliando suas capacidades humanas limitadas com o apoio contínuo de ferramentas de IA generativa.
- Cada vez mais, os invasores estão procurando elos frágeis na cadeia de suprimentos digital conectada por APIs de uma empresa, como os parceiros B2B (Business-to-business) que podem não estar priorizando a proteção das APIs.

Por exemplo, algumas formas de abuso de API têm origem em clientes e parceiros que receberam credenciais de API, mas optaram por usá-las de maneiras não autorizadas. Também existem maneiras de sequestrar credenciais de API aparentemente legítimas ou tokens de segurança. As vulnerabilidades ocultas nas implementações de clientes de API são outro vetor de ataque que os agentes de ameaças podem explorar para abusar das APIs de maneiras que as ferramentas de segurança tradicionais não conseguem detectar.

A boa notícia é que as capacidades essenciais para proteger as APIs contra métodos de ataque em rápida evolução estão disponíveis em larga escala para as organizações. Continue lendo para obter detalhes sobre os 11 principais recursos com os quais sua equipe pode começar a tomar medidas para proteger suas APIs, e os dados que elas trocam, contra ataques.

Recurso crítico n.º 1

Descoberta e gerenciamento de postura de APIs de modo contínuo

Um inventário abrangente e continuamente atualizado das APIs em uso na organização é uma base crucial para qualquer estratégia de segurança de APIs. Sem isso, uma organização não pode proteger o que ela não sabe que tem em seu ambiente. Muitos produtos de segurança de APIs alegam executar algum nível de descoberta de APIs, mas limitam-se à operação diária ou sob demanda. É importante garantir que os recursos de descoberta de API da sua plataforma incluam:

- Detecção automatizada e contínua de APIs 24 horas por dia, incluindo descoberta de APIs que são usadas apenas uma vez (a descoberta diária ou sob demanda é insuficiente)
- Descoberta de APIs em diferentes tecnologias e infraestruturas
- Descoberta de APIs recém-implantadas e comparação com APIs bem documentadas para identificar APIs de sombra
- Pontuação de risco de cada serviço de API e ponto de extremidade: isso ajuda as equipes de segurança e desenvolvimento a reduzir o ruído e priorizar APIs com o maior impacto potencial, caso sejam comprometidas
- Detecção de instâncias de vulnerabilidades conhecidas de APIs, como as descritas na lista OWASP Top 10 API Security Risks

Visibilidade aprimorada

Nunca mais perca de vista seu inventário de APIs

Recurso crítico n.º 2
Visualização do comportamento da API

A capacidade de visualizar o comportamento real das APIs (chamadas de API) é fundamental para uma plataforma de segurança de APIs. Esse recurso é necessário para permitir que as principais partes interessadas dos departamentos de segurança, desenvolvimento e operações visualizem e entendam como as APIs estão sendo usadas ou abusadas, para que possam se comunicar entre as equipes e investigar casos. Os recursos de visualização específicos a serem procurados incluem:

- **Investigação:** qualquer alerta deve incluir a capacidade de inspecionar a atividade da API original, chamada por chamada, para identificar o acionador específico do alerta.
- **Fidelidade e enriquecimento dos dados:** para cada chamada de API, deve ser possível informar quem é o usuário, qual operação ele usou, quais registros acessou ou manipulou, quais cabeçalhos e parâmetros foram usados etc.
- **Privacidade de dados:** embora a fidelidade dos dados seja importante, os dados confidenciais não podem ser armazenados em repouso. Uma solução deve analisar o tráfego e enviar apenas metadados relevantes para atualizar painéis.

Recurso crítico n.º 3

Descobrir tentativas de abuso de API por meio de contexto em entidades de usuário

As equipes de segurança precisam ter a capacidade de rastrear atividades mal-intencionadas para entidades como endereços IP e entidades de processos de negócios, como IDs de pagamento. Isso pode ser extremamente valioso quando combinado com recursos para correlacionar ataques de IPs diferentes em casos em que outros identificadores relevantes podem oferecer contexto em eventos de abuso de API.

Digamos que um usuário desconhecido esteja chamando a API de uma empresa de varejo usando /api/getpaymentID/50 como seu ID. Neste cenário, a equipe de segurança do varejista sabe que todos os outros usuários na plataforma da empresa estão vinculados a um tipo de ID de pagamento. Se um analista de segurança perceber, repentinamente, que o usuário desconhecido está fazendo chamadas repetidas, cada vez ajustando ligeiramente o número de ID (/api/getPaymentID/51 … 52 … 53 … 54), este é um indicador chave de tentativa de invasão de API.

Ter uma visão em tempo real do comportamento atípico do usuário pode ser a diferença entre uma tentativa de violação frustrada e um ataque de API bem-sucedido.

US$ 943.162

O custo médio para corrigir incidentes de segurança de APIs, de acordo com os CISOs, CIOs e CTOs dos EUA que relataram ter vivenciado esses eventos nos últimos 12 meses.

Saiba mais sobre as visões e experiências dos seus colegas no Estudo sobre o impacto da segurança de APIs de 2024.

Recurso crítico n.º 4
Análise comportamental e detecção

Embora a análise de chamadas individuais de API de entidades de usuários (ou até mesmo sessões individuais) possa ajudar as equipes de segurança, é fundamental ter uma detecção de ameaças abrangente para APIs, focada na visão geral. Busque recursos para obter uma compreensão profunda dos padrões comportamentais e anomalias em todo o estado da API. Para determinar se o comportamento de uma API é anormal, indicando que ela pode estar comprometida, o uso da API deve ser analisado por períodos mais longos e com uma base de contexto criada por um acompanhamento completo do comportamento por longos períodos. Isso fornece às equipes de segurança uma linha de base confiável, pois elas monitoram continuamente o comportamento para detectar anomalias.

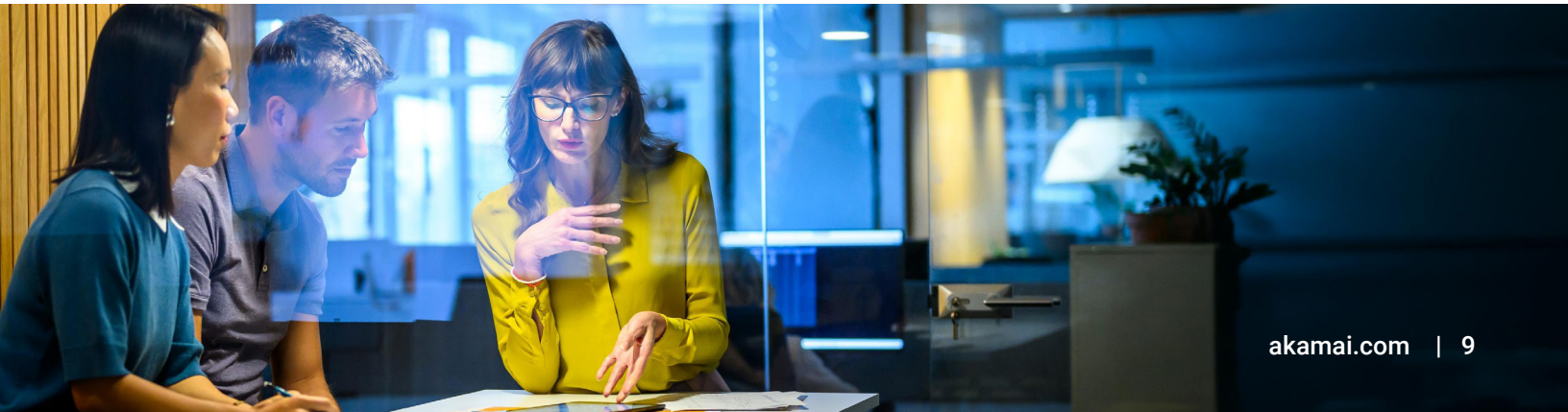
Recurso crítico n.º 5
Detecção de desvio de especificação da API

As APIs estão em constante fluxo em meio à mudança da demanda do mercado e dos requisitos de negócios. Como resultado, as organizações estão lançando continuamente novas implementações de pontos de extremidade para atender às necessidades de negócios em rápida evolução, corrigir bugs e introduzir melhorias técnicas. Atualizar a documentação da API de forma sincronizada com essas mudanças, com base nas especificações da API, é fundamental. Além disso, é importante dedicar atenção especial para garantir que o tráfego da API esteja sempre em conformidade com suas especificações.

Para tornar as APIs resilientes contra violações e ataques, as organizações devem buscar recursos para detectar desvios nas especificações da API. Para isso, elas comparam continuamente o tráfego da API em tempo real com as especificações definidas. Isso ajuda as empresas a identificar quaisquer discrepâncias ou lacunas na documentação da API.

Se a função de desvio da especificação da API identificar qualquer discrepância ou pontos de extremidade não documentados sendo acessados em produção, ela pode alertar os desenvolvedores e as equipes de segurança, permitindo que eles:

- Antecipem problemas antes que eles se tornem críticos
- Certifiquem-se de que as APIs funcionem conforme o esperado
- Reforcem a segurança dos aplicativos compatíveis com essas APIs
- Mantenham a integridade do ecossistema de APIs da empresa



Recurso crítico n.º 6
Cobertura de API B2B e leste-oeste

A área de maior crescimento no uso de APIs é a de casos de uso de B2B (Business-to-business) tanto interna quanto externamente. A segurança de APIs deve abranger APIs B2B (Business-to-business), máquina para máquina, incluindo instâncias norte-sul (voltadas para o exterior) e leste-oeste (voltadas para o interior).

Embora os aplicativos da Web B2C (Business-to-consumer) recebam proteção das plataformas WAAP e WAF, alguns dos tipos mais confidenciais de atividade de API, como APIs internas leste-oeste ou funcionalidade de aplicativos proprietários expostos a parceiros por meio de APIs B2B (Business-to-business), ainda podem ser comprometidos mesmo quando passam pela WAAP.

Muitas vezes, depois que um usuário é autenticado em uma API de parceiro B2B (Business-to-business), ele é considerado seguro e nenhum monitoramento adicional é realizado. Isso cria uma lacuna crítica na postura de segurança de APIs de muitas organizações. Para fornecer uma visão completa da atividade de API e do cenário de ameaças mais amplo, as organizações devem usar uma abordagem que forneça visibilidade, observação e monitoramento eficazes para todos os casos de uso.

Recurso crítico n.º 7
Alertas significativos com contexto

Depois que uma organização tem visibilidade de toda a atividade de API e análise comportamental em escala, os alertas sobre a atividade de API se tornam muito mais significativos. Mas como você pode ter certeza de que está direcionando a atenção e recursos para verdadeiras ameaças de API? Um mecanismo de avaliação da confiança de um atacante pode utilizar algoritmos avançados de machine learning, treinados para analisar sinais internos e externos, como comportamento da API (incluindo padrões de tráfego de rede, dados de geolocalização, fontes de inteligência de ameaças e outros fatores contextuais) para determinar o nível de confiança de que um incidente identificado de tempo de execução seja resultado de uma atividade maliciosa. Esse recurso pode ajudar uma equipe de segurança a zerar rapidamente as ameaças críticas e deve ser complementado por funções que criam correções automáticas e fluxos de notificação para ataques de alta probabilidade.

Recurso crítico n.º 8
Respostas personalizadas e automatizadas

Abordagens tradicionais de API em linha podem tomar ações automáticas para bloquear ataques de API suspeitos, com a ressalva de que as organizações precisam ser capazes de identificar os ataques. Uma vez que a análise comportamental e a identificação de anomalias em APIs são realizadas ao longo do tempo com um contexto empresarial muito mais amplo, a profundidade da detecção permite que as anomalias venham à tona. Isso permite uma ampla gama de respostas automatizadas e personalizadas, que podem ser executadas com alta precisão. Exemplos incluem:

- Bloqueio ou limitação do tráfego em gateways de API compatíveis e filtros de edge de CDN (Rede de Entrega de Conteúdo)
- Notificações por e-mail para interessados em segurança e negócios
- Criação de tíquetes para desenvolvedores
- Acionamento de webhooks

O que as organizações podem fazer para ajudar as equipes de segurança sobrecarregadas a maximizar sua equipe e energia à medida que as ameaças às APIs crescem? Buscar recursos de automação que melhorem a eficiência e a produtividade simplificando a criação e o gerenciamento de fluxos de trabalho de várias ações. Os recursos certos de automação devem oferecer uma interface de designer visual sem código que possa criar processos complexos de resposta a eventos bem como sincronizar dados relacionados a incidentes entre suas principais soluções de segurança de APIs e inúmeros serviços de terceiros, incluindo ServiceNow, Jira e Azure DevOps.

Recurso crítico n.º 9
Análise de tráfego de API

As organizações precisam de recursos sempre ativos para gravar, visualizar e analisar o tráfego de API em seus ambientes sem implantar um data lake. Ao registrar fluxos de dados de API que correspondem a critérios específicos em ambientes de aplicativos, incluindo atividades de API típicas e anômalas, as organizações podem procurar ameaças de forma mais eficaz enquanto gerenciam a exposição a riscos de usuários suspeitos e comportamentos incomuns de API. É importante ter funções de auditoria de tráfego de API que possam ser personalizadas para um caso de uso específico, permitindo que as organizações capturem e retenham o tráfego de acordo com filtros e regras predeterminados.

Recurso crítico n.º 10
Testes rigorosos de API em tempo real

Na pressa de inovar, as organizações estão lançando APIs em produção com vulnerabilidades e falhas de projeto que muitas vezes não são detectadas. As organizações podem evitar esses problemas adotando uma abordagem shift-left para o teste de API em desenvolvimento. Os principais recursos incluem:

- Realizar testes automatizados que simulem tráfego mal-intencionado, incluindo os tipos abordados no relatório OWASP Top 10 API Security Risks
- Inspecionar as especificações de API em relação às políticas e regras de governança estabelecidas
- Realizar teste de APIs sob demanda ou como parte de um pipeline de CI/CD

Recurso crítico n.º 11
Proteção independente de plataforma

Os serviços de API geralmente são implementados por diferentes grupos em uma organização, que costumam usar um conjunto diversificado de plataformas e tecnologias. Por exemplo, algumas APIs são implementadas no local, enquanto outras são executadas na nuvem pública. Muitas vezes, as organizações usam tecnologias intermediárias, como proxies reversos, gateways de API, WAFs e CDNs, que oferecem valor comercial, mas deixam a visibilidade da API mais complexa.

A capacidade de acessar dados de atividade de API de cada uma dessas diferentes tecnologias é essencial. Uma abordagem de proteção contra ameaças de API independente de plataforma garante que sua organização tenha sempre uma visão abrangente da atividade das APIs, independentemente dos detalhes de implementação ou da infraestrutura utilizada. Isso fornecerá cobertura de proteção para:

- Todos os departamentos, empresas adquiridas e ambientes
- APIs sancionadas e de sombra, quer usem o gateway de API ou não

Uma abordagem independente de plataforma também ampliará a visibilidade além das APIs norte-sul e incluirá APIs públicas, parceiras e internas leste-oeste.

Garantir que a visibilidade da plataforma de proteção contra ameaças de API seja a mais abrangente possível protegerá sua organização contra ameaças internas e abusos de APIs por organizações parceiras, além dos riscos provenientes de atores de ameaças externos.

Conclusão

As APIs são um componente essencial da capacidade das organizações de atender clientes, gerar receita e operar de forma eficiente em uma economia digital e centrada na nuvem. No entanto, seu crescimento contínuo, proximidade com dados sensíveis e a falta de controles de segurança tornam as APIs uma fonte significativa de risco.

O API Security da Akamai fornece todos os 11 recursos essenciais abordados neste white paper, ajudando as organizações a desenvolver suas abordagens existentes com funções fundamentais, como:

- Descoberta de APIs
- Avaliação de riscos (incluindo exposição a dados confidenciais)
- Detecção de invasões e ataques de API
- Testes de APIs quanto a riscos e vulnerabilidades de segurança

Saiba mais sobre como se proteger contra os riscos do OWASP Top 10 API Security Risks.

Descubra 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 akamai.com e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e LinkedIn. Publicado em 01/25.