O guia definitivo para a descoberta de APIs

Índice

A importância da descoberta de APIs

Se você está começando com a segurança de APIs ou procurando aprimorar ainda mais sua estratégia, encontrar e inventariar cada API em toda a sua organização é um passo fundamental. Por quê? Para cada aplicativo que sua empresa cria, cada carga de trabalho que migra para a nuvem e cada ferramenta que seus funcionários usam para colaborar, há APIs nos bastidores trocando dados que, muitas vezes, são confidenciais. O desafio é que a maioria das organizações, mesmo aquelas que entendem o valor de um inventário completo, não consegue ver uma grande parte de suas APIs.

E se você não pode vê-la, você não pode protegê-la.

À medida que as organizações se tornam cada vez mais centradas na nuvem e digitais, seu patrimônio de APIs cresce em escopo, escala e complexidade. As APIs são frequentemente distribuídas em vários ambientes, desde no local até na nuvem híbrida. Além da complexidade, seu ecossistema de APIs provavelmente se estende muito além de sua própria presença de rede e nuvem. Pense na infinidade de conexões que suas APIs estabeleceram com aplicativos, serviços e sistemas pertencentes a terceiros e ecossistemas de desenvolvedores.

À medida que suas APIs aumentam em escopo, escala e complexidade, é difícil conseguir insights em tempo real sobre:

- Onde suas APIs estão localizadas em várias unidades de negócios que, em muitos casos, têm suas próprias equipes de desenvolvedores
- Como suas APIs são configuradas, onde elas são roteadas e se elas têm os controles adequados de autenticação e autorização
- Se suas APIs retornam dados confidenciais quando chamadas e quem pode ter acesso a esses dados

Tornando as coisas ainda mais desafiadoras, uma grande parte das APIs que as organizações acumulam não são gerenciadas, são invisíveis e muitas vezes estão desprotegidas. Elas incluem APIs inativas, sombra e zumbi que, em muitos casos, passam despercebidas pelas ferramentas de defesa comumente usadas, como gateways de APIs e WAFs (firewalls de aplicativos da Web). É certo que essas ferramentas oferecem benefícios e proteção de linha de base, mas o cenário atual de ameaças a APIs requer um maior grau de visibilidade, proteção em tempo real e os testes contínuos que as soluções especializadas de segurança de APIs podem fornecer.

Se você conseguir descobrir todas as suas APIs, terá a base para as próximas etapas essenciais, como avaliar os riscos de cada API, entender a postura de segurança de APIs da sua organização e usar os insights obtidos para aplicar proteção em tempo real que impede ataques. Neste white paper, compartilharemos:

- Insights sobre o que torna certos tipos de APIs tão difíceis de entender para equipes de segurança
- Detalhes sobre recursos de descoberta de APIs que podem ajudar você a ter visibilidade e impedir ataques

Por que as APIs são tão difíceis de encontrar?

Não é incomum ter APIs não gerenciadas em produção que ninguém nas equipes de operações ou segurança sabe, expondo os negócios a uma série de riscos de cibersegurança e dificuldades operacionais. APIs expostas ou mal configuradas são predominantes, desprotegidas e fáceis de serem comprometidas por agentes mal-intencionados. E os riscos são altos. Os ataques às suas APIs podem comprometer a receita, a resiliência e a conformidade regulatória de uma empresa.

Veja quatro maneiras pelas quais APIs não autorizadas podem surgir:

1. Atalhos e falhas de processo de APIs

Algumas APIs não autorizadas são resultado de não se comunicar com as pessoas certas. Por exemplo, uma equipe de linha de negócios (LOB) pode criar APIs para atender a necessidades específicas sem informar à equipe de TI, ou os desenvolvedores podem estar mais preocupados com a execução do que com o procedimento. APIs que foram “herdadas” como parte de uma aquisição também são frequentemente negligenciadas. Esses tipos de APIs não autorizadas muitas vezes são chamadas de APIs sombra.

2. Versões antigas de APIs

Em muitos casos, pode acontecer de uma versão mais antiga de uma API, possivelmente com segurança mais fraca ou uma vulnerabilidade conhecida, nunca ser removida. Uma versão antiga pode ter que coexistir com uma nova versão por um tempo enquanto o software é atualizado. Mas a pessoa responsável por desativar a API pode sair da empresa, ser realocada ou simplesmente se esquecer de desligar a versão antiga. As APIs também podem ser oficialmente desativadas, mas permanecerem em operação devido a descuidos operacionais. Qualquer um dos cenários resulta no que às vezes é referido como uma API zumbi.

3. APIs herdadas

As APIs “herdadas” como parte de fusões ou aquisições também são frequentemente ignoradas e se tornam APIs sombras. Inventários (se existirem) podem se perder no difícil e complicado trabalho de integração de sistemas. Empresas maiores que fazem inúmeras aquisições de empresas menores estão especialmente em risco, já que os patrimônios de APIs de empresas menores geralmente estão espalhados e não documentados.

4. APIs comerciais

Alguns pacotes de software comercial incluem APIs para se conectar com outros aplicativos e fontes de dados externas. Essas APIs algumas vezes são ativadas sem que ninguém perceba.

O que é a descoberta de APIs?

A descoberta de APIs é um processo e um conjunto de recursos que ajuda as organizações a identificar, catalogar, gerenciar e avaliar o risco entre suas APIs. Realizada corretamente, a descoberta de APIs pode ajudar as organizações a:

- Reduzir a proliferação de APIs (o acúmulo de APIs em rápido crescimento sem documentação ou supervisão adequada) e melhorar a postura de segurança
- Entender melhor seu cenário atual de APIs e tomar decisões embasadas sobre futuros desenvolvimentos
- Monitorar e controlar o acesso a essas APIs, garantindo que apenas usuários autorizados possam acessá-las

Principais recursos de descoberta de APIs para aumentar a visibilidade e reduzir o risco

É comum ter APIs que ninguém conhece. No entanto, sem um inventário preciso, sua empresa está exposta a uma série de riscos. Para fazer um inventário eficaz de suas APIs, você precisa ser capaz de:

Localizar
e fazer o inventário de todas as suas APIs, independentemente da configuração ou tipo

Detectar
APIs não gerenciadas, como APIs inativas e zumbis

Identificar
domínios esquecidos, negligenciados ou de sombra desconhecidos

Eliminar
lacunas de visibilidade e revelar possíveis caminhos de ataque

À medida que você avalia novas soluções para descoberta de APIs, considere os seguintes recursos: uma ferramenta de descoberta deve incorporar todos eles.

Descoberta de todos os tipos de APIs

Uma ferramenta de descoberta de APIs deve ser capaz de identificar as APIs de todas as configurações ou tipos, incluindo RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC.

Inventário granular de APIs

Uma ferramenta de descoberta de APIs também deve criar um inventário que é atualizado automaticamente para evitar que fique obsoleto, além de fornecer a capacidade de pesquisar, marcar, filtrar, atribuir e exportar APIs com base em qualquer atributo.

Detecção de APIs elusivas

As APIs não gerenciadas podem predar as iniciativas de segurança de APIs da sua organização. As origens da proliferação de suas APIs podem ter começado com uma equipe de desenvolvedores que não está mais na sua empresa. Essas APIs normalmente não possuem propriedade e funcionam sem qualquer controle de visibilidade ou segurança. É fundamental que uma ferramenta de descoberta localize essas APIs.

Descoberta de domínio de API sombra

Além das APIs sombra, você pode ter domínios sombra inteiros: nomes de domínio de API dos quais você não tem conhecimento. As ferramentas de descoberta de APIs devem identificar domínios sombra esquecidos, negligenciados ou desconhecidos que possam representar um risco de segurança.

Verificação automática de APIs

Varreduras são essenciais para eliminar pontos cegos e identificar problemas críticos, incluindo:

- Credenciais e chaves de APIs vazadas
- Exposição de esquema e código de APIs
- Configurações incorretas da infraestrutura
- Vulnerabilidades na documentação, repositórios GitHub, espaços de trabalho Postman etc.

Identificar essas e outras fontes de inteligência explorável também pode ajudar as equipes a entender possíveis caminhos de ataque que podem ser explorados por cibercriminosos.

Sem necessidade de integrações

Uma ferramenta de descoberta de APIs deve ser capaz de descobrir totalmente o seu patrimônio de APIs, encontrando APIs vulneráveis e domínios de sombra, sem precisar de integrações especiais ou instalação de software. Isso é fundamental para evitar lacunas de visibilidade que ocorrem simplesmente porque você não conseguiu instalar os agentes certos ou configurar a ferramenta corretamente.

Desenvolvimento personalizado limitado

Finalmente, uma ferramenta de descoberta de APIs deve ser projetada de forma que impeça a necessidade de desenvolvimento personalizado para fontes de tráfego. Essas ferramentas devem vir com integrações incorporadas para os principais componentes de infraestrutura. O desenvolvimento personalizado normalmente consome muito tempo e, se houver mudanças na origem da fonte, uma integração provavelmente precisaria ser reformulada, o que não é viável para equipes de segurança de TI.

Como as soluções de segurança da Akamai podem ajudar você a descobrir todas as APIs

Com recursos abrangentes e contínuos de descoberta de APIs, as organizações podem realizar os seguintes benefícios para seus negócios:

- Entender a superfície de ataque completa de APIs
- Reduzir os custos de inventários de APIs e atualizações de documentação
- Melhorar a conformidade com requisitos regulatórios e políticas internas

As ameaças atuais exigem uma solução completa de segurança de APIs, abrangendo quatro áreas críticas: descoberta de APIs, gerenciamento de postura, detecção e correção de ameaças e testes de segurança. O Akamai API Security fornece todos os quatro módulos essenciais, protegendo as APIs ao longo de todo o seu ciclo de vida, do desenvolvimento à produção. Criado para organizações que expõem APIs a parceiros, fornecedores e usuários, o API Security descobre suas APIs, entende a respectiva postura de risco, analisa seu comportamento e bloqueia ameaças à espreita.

Leia mais sobre métodos de ataque de APIs, vulnerabilidades comuns de APIs e como proteger sua organização.

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

Sobre as soluções de segurança da Akamai

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 10/24.