

Segurança de APIs para o setor de saúde

Descubra como o Akamai API Security ajuda os provedores de serviços de saúde a identificar e defender-se contra ameaças de API.

As APIs permitem que os provedores de serviços de saúde aprimorem e otimizem o atendimento ao paciente, facilitando uma troca perfeita de dados entre sistemas, dispositivos e pessoas. No entanto, esses dados, como prontuários médicos e apólices de seguro, geralmente são confidenciais, tornando as APIs um alvo de alto valor para os invasores.

Suas APIs estão em risco? Considere os seguintes resultados do [estudo sobre o impacto da segurança de APIs de 2024](#):

- Quase 85% das organizações de saúde sofreram incidentes de segurança de API em 2024, em comparação com 79% em 2023.
- Apenas 24% com inventários completos de APIs sabem quais APIs trocam dados confidenciais, em comparação com 40% em 2023.

Enquanto isso, os líderes de TI e segurança de vários setores relatam gastos superiores a US\$ 943.000 em média para resolver e se recuperar de incidentes de segurança de API.

As APIs permitem uma troca de dados perfeita, oferecendo às instituições de saúde os benefícios de maior interoperabilidade e eficiência. No entanto, as APIs também expandem a superfície de ataque: à medida que se proliferam entre aplicações, ambientes em nuvem e modelos de IA, as APIs também aumentam em risco. As instituições de saúde estão implantando por descuido APIs que são mal configuradas, mal testadas e criadas sem controles de acesso, o que facilita que os invasores roubem dados e interrompam operações.

O Akamai API Security ajuda os provedores a descobrir quantas APIs eles têm e os tipos de dados que atravessam essas APIs, além de oferecer aos provedores os meios de proteger esses dados a qualquer momento. Infelizmente, muitos profissionais de saúde consideram as APIs como parte da segurança de aplicações tradicional. Mas a equipe de AppSec e DevOps precisa pensar separadamente sobre as considerações de segurança exclusivas que as APIs representam para ambos. Como a tecnologia fundamental que possibilita os cuidados modernos com a saúde, as APIs apresentam novos riscos que as ferramentas legadas não conseguem resolver.

Para estabelecer um programa robusto de governança e segurança de API, as organizações devem fazer parceria com o fornecedor de segurança de API certo. Na área de saúde, os fluxos de dados não monitorados representam riscos significativos, mas muitas organizações ainda não têm um inventário abrangente de suas APIs. O Akamai API Security ajuda as instituições a obter visibilidade total do cenário de suas APIs, identificando todas as APIs ativas e analisando os tipos de dados com que elas lidam. A partir daí, nossa solução permite a proteção contínua por meio do gerenciamento de ativos, análise de dados confidenciais, detecção de anomalias, testes de segurança de API, integração de CI/CD e a correção manual e automatizada, integrando-se perfeitamente a fluxos de trabalho de terceiros.

Desafios



As APIs expandem a superfície de ataque



Quase 85% das organizações de saúde sofreram incidentes de segurança de API em 2024



Como o Akamai API Security lida com ameaças de API

A solução da Akamai foi criada especificamente para ajudar as instituições de saúde a proteger seu patrimônio de APIs.

Descoberta abrangente de API

Identifique e faça o inventário das APIs em seu ambiente, incluindo RESTful, GraphQL, SOAP, XML-RPC e gRPC. Detecte APIs desatualizadas ou não gerenciadas que não estão protegidas pelo seu gateway de API e tenha visibilidade sobre seus atributos e metadados.

Entender o comportamento da API e detectar ameaças

Utilize a análise com tecnologia de IA para identificar automaticamente os riscos de segurança, como vazamentos de dados, acesso não autorizado, erros de configuração e atividade suspeita. Mantenha-se à frente de possíveis ameaças com monitoramento contínuo e detecção de anomalias.

Proteger APIs e corrigir lacunas de segurança

Bloqueie ataques em tempo real, corrija erros de configuração de segurança e atualize automaticamente regras de firewall para impedir tráfego mal-intencionado. Integre-se perfeitamente aos ecossistemas de segurança existentes, como WAFs, sistemas de tíquetes e plataformas SIEM, para aprimorar seus recursos de resposta.

Testar proativamente as APIs antes da implantação

Certifique-se de que as APIs sejam totalmente testadas como parte do ciclo de vida de desenvolvimento, ajudando a descobrir falhas de lógica de negócios, erros de configuração e outras vulnerabilidades antes que elas cheguem à produção. Ao integrar os testes de segurança logo no início, as organizações podem lidar proativamente com os riscos e fortalecer as defesas de suas APIs.

Akamai API Security

Da detecção de API e análise de risco aos testes e conformidade de API



Para saber mais, acesse [nossa página do API Security](#) ou entre em contato com a [equipe de vendas da Akamai](#).