

Setor de seguros

Os incidentes de API estão aumentando. Descubra como o setor de serviços seguradores está enfrentando essa grande preocupação com a segurança e o que sua organização pode fazer para se proteger.

Quando ocorrem desastres — de acidentes de carro a equipamentos comerciais danificados — os segurados dependem de serviços digitais para enviar reivindicações e receber assistência de seus provedores de seguros. Por trás desses serviços, as APIs das empresas de seguros lidam com informações confidenciais que representam a história de vida de um segurado contada em formato de dados.

Em um setor em que a confiança dos clientes é primordial, as seguradoras enfrentam um desafio crescente à segurança: vulnerabilidades de APIs.

De acordo com a pesquisa abrangente da Akamai, 76,7% dos profissionais de seguros relataram incidentes de segurança de API nos últimos 12 meses — e o impacto financeiro é substancial, com as seguradoras gastando uma média de US\$ 625.634,00 para lidar com esses incidentes apenas nos Estados Unidos.

Mas talvez mais preocupante sejam os impactos comerciais: "A perda da boa vontade dos clientes e a rotatividade de contas" (28%) são as principais preocupações das seguradoras após incidentes com APIs. Em um mercado competitivo em que os clientes podem facilmente mudar de fornecedor, esse dano reputacional pode ter efeitos duradouros além dos custos imediatos.

Continue lendo para obter insights do setor a partir do [Estudo sobre o impacto da segurança de APIs de 2024](#).

Enquanto os ataques aumentam, a visibilidade permanece um desafio importante

O custo financeiro dos ataques a APIs é substancial para as seguradoras, com custos nos Estados Unidos (US\$ 625.634,00) excedendo a média entre setores (US\$ 591.404,00). O que está impulsionando esses incidentes?

De acordo com as equipes de segurança do setor de seguros, as principais causas incluem:

1. APIs não gerenciadas, como as APIs inativas ou "zumbi" (22%)
2. APIs com exposição não intencional à internet (21,3%)
3. Ferramentas tradicionais usadas para proteger APIs que não conseguem detectar ameaças (20%)
4. Vulnerabilidades de autorização (19,3%)
5. Configuração incorreta de APIs (18,7%)

Muitas organizações estão cientes das causas dos ataques às suas APIs, mas não têm visibilidade de um indicador crucial de risco: a capacidade de uma API de retornar dados confidenciais quando chamada. Enquanto 56,7% das seguradoras relatam ter um inventário completo de suas APIs (abaixo da média de 69,7% entre setores), apenas 20,7% sabem quais APIs retornam dados confidenciais.

Essa lacuna de visibilidade representa implicações significativas de conformidade e segurança em um setor que processa dados pessoais e financeiros altamente regulamentados.

76,7% das seguradoras enfrentaram incidentes com APIs nos últimos 12 meses

Apenas 20,7% das seguradoras com inventários completos de API sabem quais APIs retornam dados confidenciais

US\$ 625.634,00 = impacto financeiro de incidentes com a segurança de APIs para seguradoras norte-americanas nos últimos 12 meses

Os três principais impactos

1. **Perda da fidelidade dos clientes e rotatividade de contas (28%)**
2. **Danos à reputação dos departamentos frente à liderança (25,3%)**
3. **Custos incorridos para corrigir problemas (24,7%)**

Fonte:

Akamai, [Estudo sobre o impacto da segurança de APIs](#), 2024

Notamos **várias tendências** que dificultam a proteção de APIs:

- **Proliferação contínua de APIs:** com cada iniciativa digital, as APIs se multiplicam e evoluem constantemente, dificultando a manutenção de um inventário preciso.
- **Padrões inconsistentes:** muitas seguradoras têm várias equipes de desenvolvimento operando em silos entre unidades de negócios sem usar um manual central para projetos seguros.
- **Riscos invisíveis:** as APIs transmitem dados confidenciais de segurados, mas a maioria das organizações não consegue identificar quais APIs específicas retornam informações confidenciais.

Considere o que pode acontecer com uma API implantada por um departamento sem a supervisão adequada de uma equipe de segurança. Essa API pode ter sido criada para compartilhar registros sem controles adequados ou deixada ativa após atualizações do sistema, criando pontos de exposição potenciais para dados confidenciais do cliente.

Como os incidentes com APIs afetam a conformidade, a confiança dos clientes e o estresse das equipes

Está claro que as seguradoras têm plena consciência das consequências financeiras das ameaças às APIs. Em nossa pesquisa, pedimos aos entrevistados que compartilhassem os custos estimados dos incidentes com a segurança de APIs vivenciados nos últimos 12 meses:

	Setor de seguros	Média de todos os setores
 Estados Unidos	US\$ 625.633,70	US\$ 591.404,01
 Reino Unido	£ 493.000,50	£ 420.103,18
 Alemanha	€ 373.918,72	€ 403.453,26

Embora os impactos financeiros sejam significativos, ficou muito claro na pesquisa que os custos refletem uma mistura de preocupações com receita e reputação. Quando perguntados sobre o principal impacto do incidente enfrentado com a segurança de APIs:

- 28% citaram "perda de boa vontade dos clientes e a rotatividade de contas"
- 25,3% citaram "danos à reputação da equipe entre líderes e membros executivos"
- 24,7% listaram "custos incorridos para resolver problemas"

Reduza o risco e o estresse com a segurança de APIs proativa

Os ataques a APIs de seguradoras estão crescendo em escopo, escala, sofisticação e custo. Isso inclui ataques de bots alimentados por IA generativa que se adaptam rapidamente para contornar as ferramentas tradicionais de segurança de APIs e outras defesas de perímetro. Muitas equipes de segurança do seu setor estão vivenciando essas ameaças em primeira mão e sentindo os impactos, tanto financeiros quanto humanos. Porém, mesmo quando as organizações entendem a importância das ameaças a APIs, elas ficam com a dúvida: o que podemos fazer a respeito disso?

Tomar medidas agora para proteger melhor suas APIs (e os dados que elas trocam) pode capacitar sua organização a proteger sua receita e aliviar o fardo das equipes de segurança, tudo isso preservando a confiança arduamente conquistada de conselhos de administração e clientes. Essas etapas incluem o desenvolvimento do conhecimento da equipe sobre ameaças avançadas de APIs e os recursos necessários para se defender contra elas.



Para ler o relatório completo e saber mais sobre as práticas recomendadas de visibilidade e proteção de APIs, faça o download do [Estudo sobre o impacto da segurança de APIs de 2024](#).

Pronto para conversar sobre seus desafios e como a Akamai pode ajudar?

[Solicite uma demonstração personalizada do Akamai API Security](#)

A Akamai oferece soluções desenvolvidas para ajudar as organizações a mitigar os riscos associados às ameaças discutidas nesta seção:

- **Akamai API Security:** identifica APIs, avalia sua postura de risco, analisa seu comportamento e impede que ameaças se ocultem dentro delas
- **Akamai Account Protector:** ajuda a prevenir ataques de abertura de contas ao monitorar o comportamento dos usuários em tempo real e se adaptar às mudanças nos perfis de risco



As soluções de segurança da Akamai protegem as aplicações essenciais para o sucesso da empresa em cada ponto de interação, garantindo proteção 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](#) e [LinkedIn](#). Publicado em 05/25.