Akamai

WHITE PAPER

13 perguntas a serem feitas ao seu fornecedor de segurança de API

Introdução

A rede de APIs business-to-business está crescendo exponencialmente. E um universo cada vez maior de dispositivos da Internet das Coisas está oferecendo novas oportunidades para os desenvolvedores trazerem dados do mundo real para as aplicações por meio de APIs.

Mas embora as APIs abram muitas oportunidades de inovação e crescimento, elas também introduzem um novo conjunto de desafios de segurança, incluindo:

- Roubo de credenciais de API
- Reconhecimento de API não detectado
- Autenticação e autorização mal configuradas
- APIs shadow e zumbi desprotegidas
- Execução remota de código, injeção, inclusão de arquivo local e outras técnicas de ataque
- Vazamento ou exfiltração de dados
- Scraping de API
- Abuso de lógica de negócios

Os fornecedores de segurança oferecem muitas opções para detectar e atenuar essas e outras ameaças de API, mas essas opções não são igualmente eficazes ou fáceis de usar.

As 13 perguntas a seguir ajudarão você a estruturar suas discussões com fornecedores de segurança de API e avaliar com que eficácia seus produtos atenderão às necessidades de segurança de API da sua organização.

1 Seu produto de segurança de API é capaz de realizar a descoberta de API em toda a empresa?

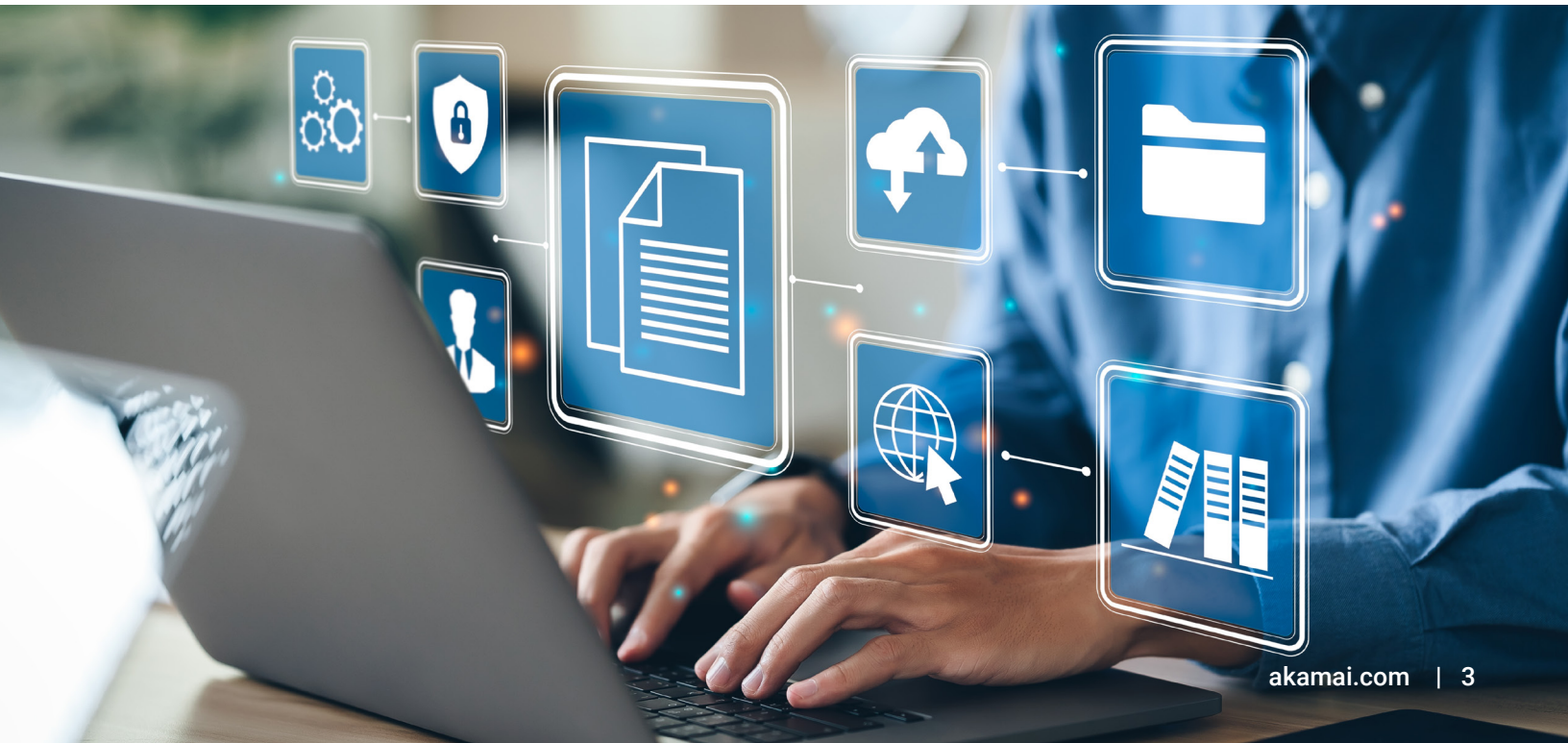
Um dos maiores problemas enfrentados pelas equipes de segurança é que elas não têm um inventário completo e preciso de todas as APIs que sua organização expõe. Muitas das APIs shadow não documentadas que as equipes de segurança perdem não fazem parte da estrutura formal de gerenciamento e segurança de APIs. Também é comum que as APIs zumbis, aquelas que a organização pensou terem sido desativadas, ainda estejam acessíveis. E mesmo entre APIs sancionadas e documentadas, pode haver parâmetros de API não documentados que podem ser explorados. A descoberta de todas as APIs norte-sul, leste-oeste e outbound é essencial. A única maneira de garantir a visibilidade completa da API em toda a empresa é examinando os dados de atividade da API existentes a partir de uma ampla variedade de tecnologias e plataformas em nuvem.

2 Seu produto descobre APIs continuamente e, em caso afirmativo, trata-se de um processo muito manual?

As APIs aparecem e desaparecem regularmente devido à rápida evolução dos processos de DevOps. Portanto, os inventários pontuais de APIs são insuficientes. Seu produto de segurança de API deve realizar a descoberta contínua, o que garante que as novas APIs documentadas sejam inventariadas, analisadas e protegidas. Ele também deve detectar quaisquer instâncias futuras de APIs shadow ou zumbi. Além disso, os produtos que sobrecarregam continuamente sua equipe para interpretar e agir sobre as descobertas não serão sustentáveis a longo prazo. Em contraste, os produtos que aplicam automação e machine learning à descoberta e à avaliação de APIs manterão sua empresa funcionando sem problemas, em vez de adicionar mais tarefas manuais à lista de tarefas diárias da sua equipe.

3 Como seu produto ajuda minhas ferramentas e processos de documentação de API?

Integrar sua abordagem de documentação à sua plataforma de segurança de API tem muitos benefícios, portanto, você deve verificar se seu fornecedor tem esse recurso. Por exemplo, o upload automático da documentação existente do Swagger para sua plataforma de segurança de API como parte do processo de integração contínua/entrega contínua (CI/CD) melhora a precisão da detecção de API shadow e da identificação de parâmetros shadow (se o fornecedor tiver a capacidade de comparar parâmetros de API descobertos com parâmetros já documentados). Sua plataforma de segurança também deve ser capaz de criar arquivos Swagger personalizados com o clique de um botão para quaisquer APIs que não tenham documentação, o que ajudará seus desenvolvedores a começar e melhorar seus processos de documentação.



4 Quanto tempo e esforço será necessário para implantar seu produto em meu ambiente?

A maneira mais rápida e eficaz de começar é usando um produto de segurança de API baseado em segurança como serviço (SaaS) que pode ingerir e analisar dados de atividade de API de seus sistemas existentes de forma não intrusiva. Uma arquitetura SaaS bem projetada para segurança de API pode ser integrada ao seu ambiente em minutos, o que pode acelerar seu tempo de valorização por ordens de magnitude e eliminar os custos e riscos contínuos associados às atualizações do sistema. Para ser ainda mais ágil, encontre um fornecedor que ofereça proteção de aplicações da Web e APIs (WAAP) e detecção e resposta de API para que os dados de tráfego de API fluam perfeitamente entre a solução que está protegendo seu tráfego de entrada e a solução que está protegendo todo o tráfego de API dentro de sua organização.

5 Como seu produto ajudará a identificar e priorizar as APIs descobertas que são arriscadas?

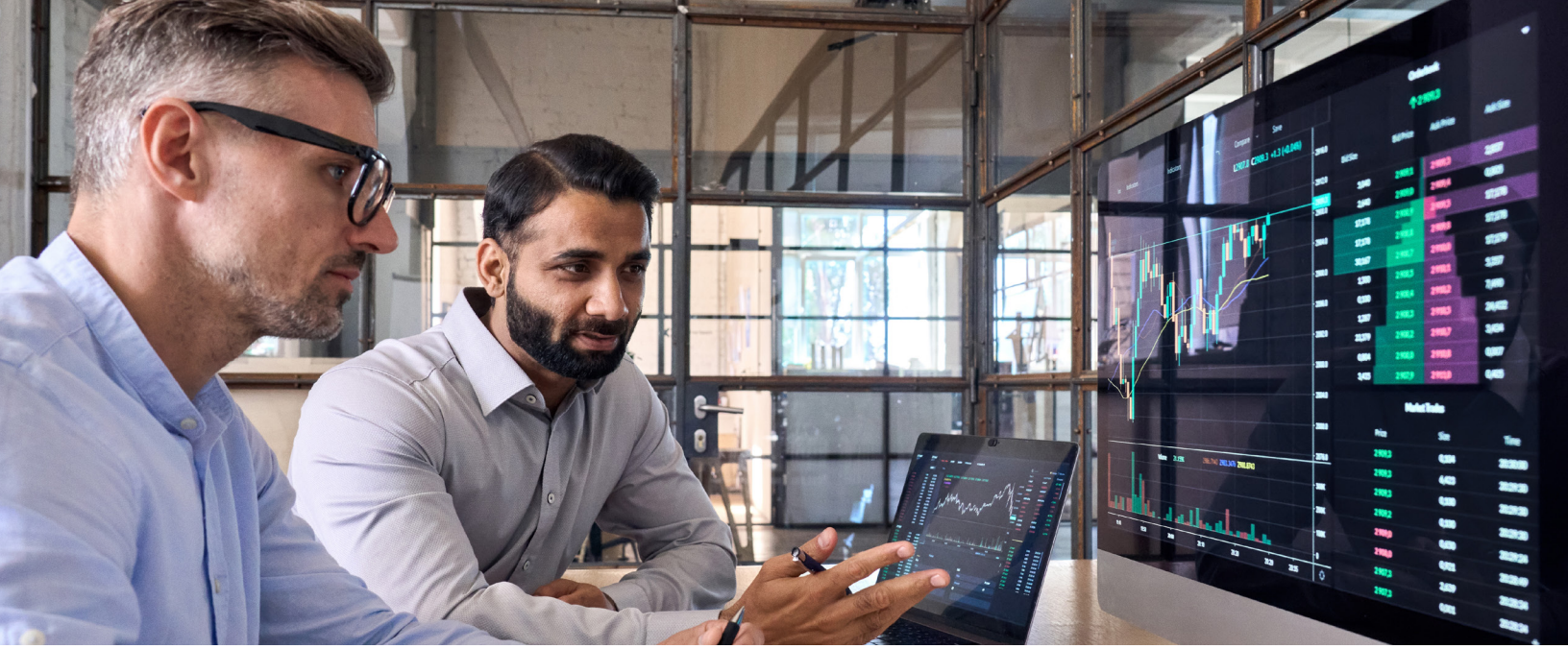
Ver um inventário de API abrangente pela primeira vez pode ser tanto empoderador quanto esmagador. Muitas equipes de segurança sofrem com a sobrecarga de informações e têm dificuldades para identificar as áreas nas quais devem ser direcionados os esforços de segurança da API. A melhor maneira de evitar isso é selecionando um produto de segurança de API que faz boa parte desse trabalho para você, incluindo:

- Destacar a presença de APIs que tornam os dados confidenciais acessíveis
- Rotular automaticamente dados confidenciais por tipo (por exemplo, informações de identificação pessoal, endereços de e-mail, dados de cartão de crédito etc.)

Sua plataforma de segurança de API também deve permitir que você crie categorias de rotulagem personalizadas para que suas equipes de API e de segurança falem uma linguagem comum que se alinhe aos seus objetivos de negócios e preocupações de segurança.

6 Seu produto usa análise comportamental para determinar uma linha de base do comportamento esperado e encontrar anomalias?

Muitos tipos de ataques podem ser detectados usando assinaturas de ataque para bloquear no nível WAAP. No entanto, muitos tipos de ataque encontrados na lista Top 10 de Segurança de API do Open Web Application Security Project (OWASP) 2023, como autorização em nível de objeto corrompida, não podem ser descobertos dessa maneira. Esses tipos de ataques são mais passivos e focados no abuso dos negócios, por isso são mais difíceis de detectar. A única maneira de se defender efetivamente contra todos os vetores de ameaças de API é usando análise comportamental e machine learning. A verdadeira análise comportamental requer grandes conjuntos de dados, algoritmos de machine learning que aprendem as especificidades de seu ambiente e a flexibilidade e a agilidade para atualizar e adaptar-se automaticamente com base em informações globais. Um modelo SaaS é a única maneira prática de realizar essas atividades em escala.



7 Você consegue capturar e analisar conjuntos de dados que são significativos o suficiente para determinar efetivamente uma linha de base de comportamento normal e detectar anomalias?

Muitos produtos de segurança de API se concentram no monitoramento de chamadas de API individuais ou, na melhor das hipóteses, na atividade de sessão de curto prazo. Isso é insuficiente, pois muitos processos comerciais legítimos, e muitos ataques, ocorrem em um período muito mais longo. O uso da API deve ser analisado em uma janela de tempo variável (no mínimo 30 dias). Isso fornece uma linha de base mais completa e precisa do comportamento esperado, incluindo todos os processos de negócios que ocorrem apenas uma vez por mês (por exemplo, faturamento). Também torna possível detectar ataques executados lentamente, ao longo de vários dias ou semanas e em inúmeras sessões de API.

8 Seu produto pode identificar cada entidade, relacionamento e atividade dentro de dados de API brutos para fornecer contexto de negócios?

A melhor maneira de tornar os dados de atividade da API acionáveis é enriquecê-los com contexto sobre as implicações comerciais do uso da API. Os seguintes recursos de identificação e rotulagem são essenciais para que sua plataforma de segurança de API avalie e defina o perfil das relações entre as diferentes entidades:

- Representações de usuários de API (entidades de usuário), como endereços IP, chaves de API, tokens de acesso, ID de usuário, PartnerId, ID do estabelecimento, ID do fornecedor etc.
- Representações de processos de negócios (entidades de processo de negócios), como reservas, pagamentos, faturamento, saldo da conta etc.

A análise granular nesse nível é a única maneira de transformar a grande quantidade de dados gerados pelas APIs em uma linha de base significativa e compreensível do comportamento esperado.

9 Seu produto pode plotar cada atividade por cada entidade em suas APIs em um cronograma para mostrar as mudanças de comportamento ao longo do tempo?

Embora a compreensão e o monitoramento da atividade e das ameaças da API em um nível macro sejam críticos, a capacidade de restringir o foco da análise a entidades específicas é igualmente importante. Por exemplo, se um comportamento anômalo for identificado para um parceiro de negócios específico, a capacidade de visualizar toda a atividade dessa entidade em um cronograma é inestimável. O mesmo se aplica às entidades de processos de negócios. Ver o histórico completo do que aconteceu e quando, em um cronograma para cada entidade dentro de suas APIs, é eficaz e torna óbvio o histórico de uso normal e abuso de negócios. A capacidade de rebobinar a atividade para ver o que aconteceu antes e depois de um alerta é uma ferramenta poderosa para ajudar você a entender o abuso da lógica de negócios.

10 Como posso integrar seu produto a ferramentas, processos e fluxos de trabalho existentes?

Enviar alertas para seu produto de gerenciamento de informações e eventos de segurança (SIEM) é útil, mas é apenas um ponto de partida. Cada vez mais, as equipes de segurança estão usando ferramentas mais sofisticadas de orquestração de segurança, automação e resposta (SOAR) para iniciar fluxos de trabalho predefinidos quando ameaças e incidentes de segurança são detectados. E como muitos problemas de segurança de API exigem ação de desenvolvedores fora da equipe de segurança, sua plataforma de segurança de API também precisa se integrar às ferramentas de gerenciamento de fluxo de trabalho e monitoramento de problemas da equipe de desenvolvimento. Se a sua ferramenta de segurança estiver analisando o tráfego de API, faz sentido que ela também deva usar APIs para ajudar a orquestrar respostas em sua CDN, firewall de aplicações da Web ou gateway de API e permitir que você crie seus próprios manuais.

11 Posso consultar a API e os dados de atividade do seu produto para obter uma busca proativa de ameaças e redução de riscos?

As integrações com ferramentas de segurança e desenvolvimento não podem ser apenas caixas pretas que enviam alertas unidirecionais para suas ferramentas. Suas equipes de segurança e API precisam ter a capacidade de acessar os dados de origem por trás de um alerta ou problema. Procure plataformas de segurança de API que permitam aos usuários consultar detalhes de API diretamente por meio de uma interface da Web integrada ou por meio de APIs que permitam a integração da plataforma de segurança de API com outras ferramentas e interfaces preferenciais. Isso capacitará sua equipe de segurança a realizar uma busca proativa de ameaças de forma eficiente e eficaz. Isso também ajudará seus desenvolvedores e outras partes interessadas não relacionadas à segurança a entender como as APIs são visadas por invasores enquanto são usadas legitimamente.

12 Que medidas você toma para garantir que os dados confidenciais coletados sobre minha empresa sejam protegidos?

A análise comportamental avançada necessária para proteger APIs contra o cenário atual de ameaças só é possível com a escala da nuvem. Considerando o tamanho e a sensibilidade do conjunto de dados da API, é importante desafiar o fornecedor de segurança a garantir que os dados serão protegidos. Verificar as práticas que seu fornecedor usa para proteger a infraestrutura de nuvem é importante, mas é apenas o ponto de partida. Exija que seu fornecedor de segurança de API use técnicas como a geração de tokens; ou seja, substitua dados confidenciais por tokens anônimos antes de serem transmitidos para a nuvem. Isso garante a privacidade dos dados, mesmo que o fornecedor, ou seu provedor de nuvem upstream, enfrente um incidente de segurança.

13 A solução fornece acesso granular aos dados de atividades da API?

Os dados são um elemento estratégico crucial para tudo, desde a conformidade até o contexto para a prevenção de ataques. Muitos fornecedores oferecem sua própria versão de armazenamento para dados de API ao longo do tempo, mas certifique-se de se aprofundar para entender o que realmente está sendo oferecido. As soluções que se limitam a alertas perdem a história completa, pois a atividade comprometida da API pode ocorrer lentamente ao longo do tempo, e não apenas quando ocorre um alerta. Como alternativa, um fornecedor abrangente removerá pontos cegos registrando toda a atividade de API e fornecerá as ferramentas para revisar essa atividade em detalhes, em vez de perdê-la em um modelo de machine learning vago. É importante ter esse acesso granular aos seus dados, pois você pode monitorar proativamente as ameaças, em vez de reagir retroativamente depois que houver um alerta de ataque.

13 perguntas a serem feitas ao seu fornecedor de segurança de API

1. Seu produto de segurança de API é capaz de realizar a descoberta de API em toda a empresa?
2. Seu produto descobre APIs continuamente e, em caso afirmativo, trata-se de um processo muito manual?
3. Como seu produto ajuda minhas ferramentas e processos de documentação de API?
4. Quanto tempo e esforço será necessário para implantar seu produto em meu ambiente?
5. Como seu produto ajudará a identificar e priorizar as APIs descobertas que são arriscadas?
6. Seu produto usa análise comportamental para determinar uma linha de base do comportamento esperado e encontrar anomalias?
7. Você consegue capturar e analisar conjuntos de dados que são significativos o suficiente para determinar efetivamente uma linha de base de comportamento normal e detectar anomalias?
8. Seu produto pode identificar cada entidade, relacionamento e atividade dentro de dados de API brutos para fornecer contexto de negócios?
9. Seu produto pode plotar cada atividade por cada entidade em suas APIs em um cronograma para mostrar as mudanças de comportamento ao longo do tempo?
10. Como posso integrar seu produto a ferramentas, processos e fluxos de trabalho existentes?
11. Posso consultar a API e os dados de atividade do seu produto para obter uma busca proativa de ameaças e redução de riscos?
12. Que medidas você toma para garantir que os dados confidenciais coletados sobre minha empresa sejam protegidos?
13. A solução fornece acesso granular aos dados de atividades da API?

Como você já deve ter adivinhado, o API Security da Akamai pode oferecer com eficiência as proteções recomendadas por esta lista. Explore nossas soluções.