Akamai

WHITE PAPER

Dez recursos fundamentais de detecção e resposta de APIs

Como aprimorar sua estratégia de segurança de APIs

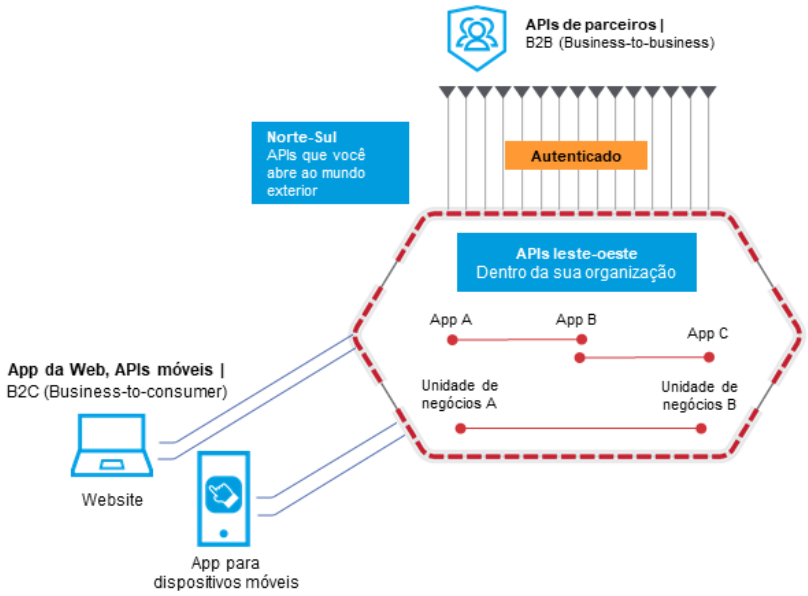
Introdução

As APIs são os principais componentes que impulsionam a inovação, e os aplicativos B2B (Business-to-business) e B2C (Business-to-consumer) estão no centro dessa transformação. Isso significa que é essencial proteger comunicações críticas, e muitas vezes confidenciais, internamente entre microsserviços e externamente entre clientes e parceiros. A maioria das organizações agora reconhece que uma estratégia sólida de segurança de aplicações é necessária para o sucesso de longo prazo dos negócios e usa tecnologias de segurança, como plataformas de proteção de aplicações Web e APIs (WAAP), recursos e produtos de segurança na nuvem e ferramentas de teste de segurança para reduzir o risco de segurança de aplicações. É importante reconhecer como os ataques evoluíram para contornar as WAAPs e as APIs de destino dentro das organizações. É hora de discutir como ajustar sua estratégia de segurança de API antecipadamente diante dessas ameaças.

Onde se encaixa a detecção e resposta de API em uma estratégia de segurança de API?

Ao longo dos últimos anos, as organizações criaram muitos mais canais de API do que interfaces de aplicativos da Web, e essas APIs incluem volumes crescentes de dados essenciais para os negócios e lógica empresarial. As APIs alteraram a forma como as empresas operam, pois possibilitam mais casos de uso, aceleram mudanças, transportam dados mais confidenciais e estão abertas a mais usuários.

Qual é o seu cenário de API?



Embora a maioria das categorias de produtos de segurança ofereça suporte a APIs de alguma forma devido à sua prevalência crescente, as APIs são uma classe de ativos diferente e até mesmo aparecem como um ativo diferente em algumas estruturas de conformidade. Adicionar capacidades de proteção contra ameaças de API a um produto de segurança legado, como uma plataforma WAAP, não aborda os novos desafios introduzidos pelos ativos de API. As organizações de segurança devem tratar as APIs como uma classe de ativos separada e reconhecer os recursos essenciais que protegem totalmente as APIs em escala.

Vamos começar com os fundamentos de como as proteções de API mudaram para atender às ameaças emergentes. No passado, se uma organização tivesse um inventário completo de suas APIs e uma WAAP robusta, as ameaças de API poderiam ser evitadas. Agora, os ataques estão visando APIs dentro das organizações e de suas organizações parceiras de maneiras projetadas para contornar a WAAP.

Por exemplo, algumas formas de violação 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 credenciais de API aparentemente legítimas ou tokens de segurança serem sequestrados. Vulnerabilidades ocultas nas implementações de clientes de API são outro vetor de ataque que atores de ameaças podem explorar para violar APIs de maneiras que não são detectáveis por ferramentas de segurança tradicionais.

A boa notícia é que os recursos essenciais necessários para proteger as APIs contra tendências emergentes, especificamente detecção e resposta, já estão disponíveis em escala para as organizações. As páginas seguintes oferecem uma consideração cuidadosa das capacidades críticas que tornam essas plataformas eficazes contra um cenário de ameaças de API em constante mudança.

Capacidade crítica nº 1
Proteção independente de plataforma

Os serviços de API são geralmente implementados por diferentes grupos em uma organização, geralmente usando uma coleção diversificada de plataformas e tecnologias. Por exemplo, algumas APIs podem ser implementadas no local, enquanto outras podem ser executadas na nuvem pública. Também pode haver tecnologias intermediárias em uso, como proxies reversos, gateways de API, WAFs (firewalls de aplicativos da Web) e CDNs (redes de entrega de conteúdo), que criam complexidade para a visibilidade da API.

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 sempre tenha uma visão completa de todas as atividades de API, independentemente dos detalhes da implementação ou da infraestrutura em uso. Isso fornecerá cobertura de proteção para:

- Todos os departamentos, empresas adquiridas e ambientes
- Tanto APIs confirmadas quanto APIs de sombra, independentemente de utilizarem o gateway de API
- Visibilidade estendida além das APIs norte-sul, incluindo APIs públicas, de parceiros 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 violações de APIs por organizações parceiras, além dos riscos provenientes de atores de ameaças externos.

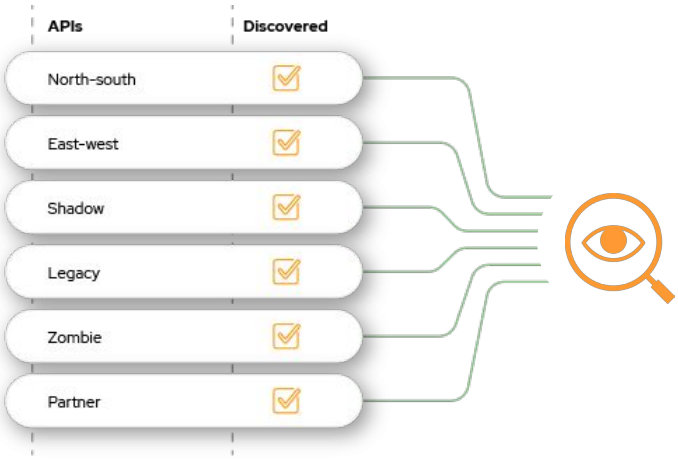
Capacidade crítica nº 2
Descoberta contínua de API e gerenciamento de postura

Um inventário abrangente e continuamente atualizado de todas as APIs em uso em toda a organização é uma base crucial para qualquer estratégia de segurança de API. Sem isso, uma organização não pode proteger o que ela não sabe que tem em seu ambiente. Muitos produtos de segurança de API alegam executar algum nível de descoberta de API, 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 todas as 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
- Detecção de instâncias de vulnerabilidades conhecidas de API, como as descritas no OWASP API Top 10

Visibilidade aprimorada

Nunca mais perca de vista seu inventário de API

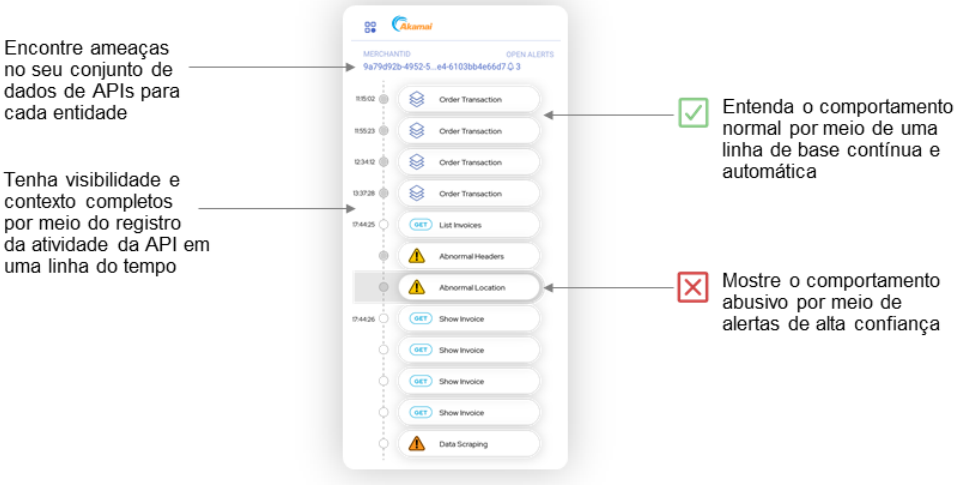


Capacidade crítica nº 3
Visualização do comportamento da API

A capacidade de mostrar e visualizar o comportamento real da API (chamadas de API) é um recurso fundamental de uma plataforma de segurança de API. 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 violadas, 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.
- **Busca por ameaças:** os dados históricos devem se estender a pelo menos uma exibição contínua de 30 dias, incluindo a capacidade de ver todas as atividades de API e consultar intervalos de tempo e chamadas além de alertas específicos. Este recurso também ajuda na conformidade.
- **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. A geração de tokens é necessária para preservar a riqueza dos dados sem armazenar dados confidenciais.
- **Visualização da linha do tempo:** os usuários devem ter uma visualização que facilite avançar e retroceder através de sequências de atividades.

Detecte ameaças usando análise comportamental



Capacidade crítica nº 4
Rastreamento de várias entidades de usuário

Entender a entidade e ser capaz de ver a atividade de API relacionada oferece contexto para qualquer uso ou violação, por isso, é fundamental que sua plataforma de proteção de API tenha a sofisticação de rastrear cada uma dessas entidades individualmente. Isso fornece um contexto essencial, uma vez que a atividade normal para uma categoria de usuários pode ser um sinal de aviso de violação para outro usuário. A capacidade de visualizar a atividade de cada entidade em uma linha do tempo fornece visibilidade vital e compreensão contextual. Por exemplo:

Atividade de API	Participantes	Entidades	Entidades de processos de negócios
Exemplos	usuários internos, parceiros B2B, usuários externos	endereço IP, token de API, ID do estabelecimento, ID da sessão, ID do locatário	ID do pagamento, ID da fatura

Capacidade crítica nº 5
B2B e cobertura de API leste-oeste

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

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, ainda podem ser comprometidos mesmo quando passam pela WAAP.

Muitas vezes, depois que um usuário é autenticado em uma API de parceiro B2B, ele é considerado seguro e nenhum monitoramento adicional é realizado. Isso cria uma lacuna crítica na postura de segurança de API 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.

Capacidade crítica nº 6
Análise comportamental e detecção

A detecção de ameaças sofisticadas de API não é possível analisando chamadas individuais de API, ou mesmo sessões individuais. A detecção e a resposta de APIs exigem um profundo entendimento e aprendizagem de contextos comportamentais. Para saber se o comportamento de uma API é anormal, o que indica que ela pode estar comprometida, é necessário analisar o uso da API por períodos mais longos. A técnica de análise comportamental determina um comportamento normal de linha de base do usuário e monitora continuamente esse comportamento para detectar anomalias.

Os recursos de armazenamento e computação necessários para executar esse nível de análise para uma atividade de API típica de uma empresa tornam impraticável a entrega usando ferramentas de segurança de API no local com restrições de escala. As soluções EDR e XDR lideraram o caminho mostrando que há a necessidade de uma arquitetura baseada em software como serviço (SaaS) para realizar análises comportamentais significativas. O poder e a escala da nuvem permitem o armazenamento de dados ao longo do tempo, e isso possibilita a análise que determina o comportamento normal do usuário ao longo do tempo, a fim de detectar a agulha no palheiro revelando violações. Uma abordagem SaaS tem outros benefícios, como implementação mais rápida e simples, e escalabilidade e elasticidade aprimoradas à medida que o uso de API cresce.

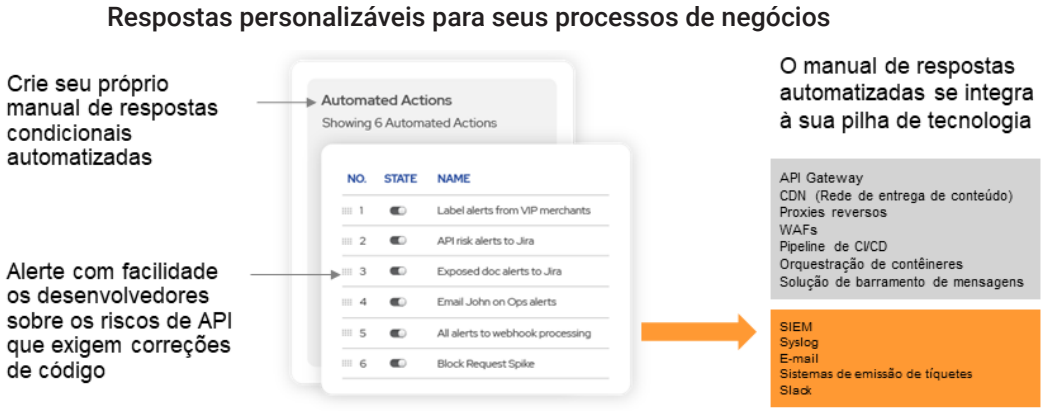
Capacidade crítica nº 7
Alertas significativos com contexto

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. As organizações eliminaram a necessidade de antecipar todos os métodos de ataque possíveis tornando a abordagem de monitoramento de segurança mais abstrata. A definição da base do comportamento normal e a detecção de anomalias também possibilitam a identificação de violação de API, que geralmente não pode ser percebido por nenhum padrão ou assinatura. Além disso, a capacidade de retroceder o ataque e ver o que aconteceu antes de um alerta fornece insights valiosos sobre o uso e a violação de um conjunto de APIs.

Capacidade crítica nº 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:

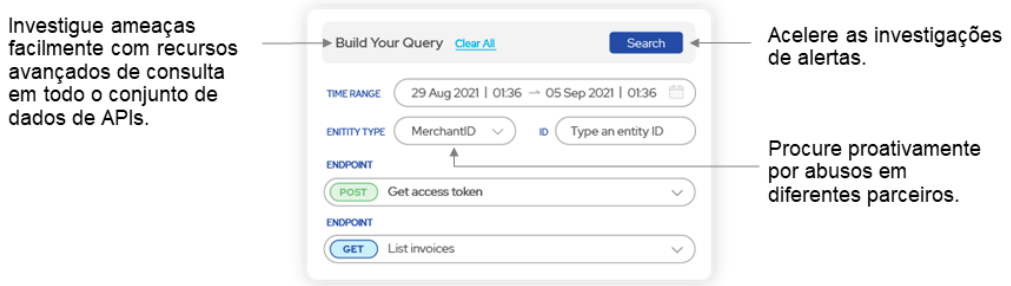
- Bloqueio ou limitação do tráfego nos gateways de API suportados e nos filtros de edge de CDN (rede de entrega de conteúdo)
- Notificações por e-mail para interessados em segurança e negócios
- Criação de tíquetes para desenvolvedores
- Acionamento de webhooks



Capacidade crítica nº 9
Investigação proativa e busca de ameaças

Muitas organizações não têm o luxo de esperar que um incidente de segurança ativo ocorra antes de agir. Uma abordagem mais eficaz é identificar situações indesejadas e procurar ativamente por elas. Por exemplo, um alerta que detectou uma violação em uma API pode ser identificado executando o mesmo comportamento em outra API por meio da caça proativa a ameaças. Portanto, uma plataforma de proteção contra ameaças de API deve incluir a capacidade de pesquisar tipos específicos de comportamento além dos alertas gerados em resposta a incidentes ativos. Os recursos de busca de ameaças exigem acesso a dados históricos para encontrar a violação oculta nos dados de atividade da API. Soluções de solicitação única que não enriquecem os dados para fornecer contexto não são capazes de unir uma história coerente. A busca e as investigações de ameaças são baseadas nos fundamentos dos dados históricos.

O poder de investigar e de procurar ameaças ao seu alcance



Capacidade crítica nº 10
Data lake observável

Em todos os recursos para uma estratégia de segurança de API robusta, o contexto é fundamental para proteger qualquer API durante um longo período. A melhor maneira de manter contexto suficiente para observar ameaças, identificar potenciais vulnerabilidades e solucionar problemas em caso de um ataque é registrar todo o comportamento da API e manter um histórico dessa atividade. Isso pode ser feito com um data lake associado à solução de segurança de API. Procure um data lake que forneça a maior quantidade de detalhes históricos para informar sua estratégia. Embora a alimentação de dados básicos de solicitações para modelos de machine learning possa ser útil, ter detalhes como os parâmetros de solicitação permite que as organizações realmente atuem em seus dados históricos de formas que os protejam de ameaças e ataques futuros.

Nº 1 Proteção independente de plataforma	Garantir que a visibilidade da plataforma de proteção contra ameaças de API seja a mais abrangente possível protegerá sua organização contra ameaças e violações.
Nº 2 Descoberta contínua de API e gerenciamento de postura	Um inventário abrangente e continuamente atualizado de todas as APIs em uso em toda a organização é crucial, pois as organizações não podem proteger o que não sabem que têm em seu ambiente.
Nº 3 Visualização do comportamento da API	A visibilidade é necessária para que as principais partes interessadas da segurança, do desenvolvimento e das operações possam ver e entender como as APIs estão sendo usadas ou violadas e podem se comunicar entre as equipes e investigar casos.
Nº 4 Rastreamento de várias entidades de usuário	Entender a entidade e ser capaz de ver a atividade de API relacionada oferece contexto para qualquer uso ou violação, por isso é fundamental que sua plataforma de proteção de API tenha a sofisticação de rastrear cada entidade individualmente.
Nº 5 Cobertura de API B2B e leste-oeste	Para fornecer uma visão completa da atividade da 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.
N º 6 Análise comportamental e detecção	Para saber se o comportamento de uma API é anormal, o que indica que ela pode estar comprometida, é necessário analisar o uso da API por períodos mais longos. A técnica de análise comportamental determina um comportamento normal de linha de base do usuário e monitora continuamente esse comportamento para detectar anomalias.
Nº 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. As organizações eliminaram a necessidade de antecipar todos os métodos de ataque possíveis tornando a abordagem de monitoramento de segurança mais abstrata.

Nº 8 Respostas personalizadas e automatizadas	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.
Nº 9 Investigação proativa e busca de ameaças	Muitas organizações não têm o luxo de esperar que um incidente de segurança ativo ocorra antes de agir. Uma abordagem mais eficaz é identificar situações indesejadas e procurar ativamente por elas.
Nº 10 Data lake observável	A melhor maneira de manter contexto suficiente para observar ameaças, identificar potenciais vulnerabilidades e solucionar problemas em caso de um ataque é registrar todo o comportamento da API e manter um histórico dessa atividade. Isso pode ser feito com um data lake associado à sua plataforma de segurança de API.

Se você achou isso útil, a próxima etapa é explorar a solução de segurança de API da Akamai para garantir que você tenha a estratégia de segurança de API mais robusta possível.