História do cliente da Akamai

Clientes protegidos com o Akamai API Security

O líder de segurança ajuda a manter milhares de clientes em conformidade e dezenas de milhares de APIs seguras

A Netskope é líder global em cibersegurança e está redefinindo a segurança de nuvem, dados e rede. Milhares de clientes, incluindo mais de 25 da Fortune 100, confiam na Netskope para lidar com ameaças em evolução, facilitar mudanças tecnológicas e ajudá-los a cumprir determinações regulatórias.

Entre as muitas áreas essenciais de tecnologia que protege, a Netskope é responsável por proteger dezenas de milhares de APIs globalmente, uma missão para a qual a empresa percebeu que precisava de uma nova abordagem além da segurança tradicional de aplicativos. Depois de descobrir falhas na postura de segurança de APIs de um de seus clientes, a Netskope recorreu à Noname Security (agora uma empresa Akamai) em busca das ferramentas de última geração necessárias para proteger os clientes contra ataques mal-intencionados a APIs.

Para além do firewall

Quer os clientes estejam implantando aplicativos menores ou maiores com miríade de microsserviços, a realidade é que todos estão usando APIs, o que significa que cada uma dessas APIs expostas faz parte da superfície de ataque. Por exemplo, a Netskope descobriu que havia abusos dentro da infraestrutura de APIs de um cliente que não haviam sido detectados e que ela não podia ver. Por essa razão, a equipe de AppSec da Netskope começou uma busca por uma solução que protegesse tanto suas próprias APIs quanto as dos clientes, juntamente com outros ativos digitais voltados para o público.

A Netskope sabia que o problema não era antigo, o que significava que não seria possível usar soluções legadas, como um firewall de aplicativos da Web ou realizar testes convencionais de segurança de aplicativos. O volume de registros, os tipos de ataques que estavam vendo e os tipos de abusos de APIs exigiam uma abordagem diferente.

netskope

Localização

Santa Clara, Califórnia
netskope.com

Setor

Alta tecnologia

Solução

Akamai API Security

Principais impactos

- Ciclo de vida de APIs totalmente seguro
- Ataques a APIs bloqueados em tempo real
- Especificações de APIs criadas automaticamente

Akamai

James Robinson, vice-CISO da Netskope, também entendeu que, ao tentar escalar a nível empresarial, sua equipe precisaria aproveitar o machine learning e ferramentas avançadas para ter visibilidade completa de sua infraestrutura de APIs. No entanto, para integrar uma nova ferramenta, a equipe de segurança estava muito ciente de que precisaria que os desenvolvedores participassem do processo.

Uma vitória para a equipe de segurança

A Netskope decidiu usar a plataforma de segurança de APIs da Noname (agora parte do Akamai API Security) para proteger as APIs na pré-produção e durante a produção. Para proteger as APIs em produção, foi usado o módulo de descoberta no Akamai API Security para acessar um inventário preciso das APIs internas, externas e de terceiros dos clientes, bem como para classificar quaisquer dados confidenciais que atravessassem essas APIs. Depois de ter um inventário preciso, foi usado o módulo de proteção de tempo de execução para detectar anomalias e bloquear ataques a APIs em tempo real.

Do ponto de vista da pré-produção, a Netskope usou a solução de teste de segurança de APIs da Akamai que ajuda as organizações a testarem se as APIs apresentam vulnerabilidades e configurações incorretas antes de serem implantadas. A solução pode executar automaticamente mais de 100 testes dinâmicos que simulam tráfego mal-intencionado, o que não só ajuda os desenvolvedores de uma organização a proteger o código, mas também garante a segurança do produto de API que está prestes a ser lançado para os clientes.

Durante a fase de avaliação, os desenvolvedores imediatamente identificaram recursos que facilitariam suas vidas. Eles viram que a Akamai poderia ajudar quando o desenvolvedor não tiver uma especificação da API por esta ser muito antiga, porque agora eles poderão construir uma rapidamente. Eles não precisam ver o código para entender a API, porque a especificação está sendo criada automaticamente. A mesma experiência é verdadeira para os registros e transações. Os desenvolvedores podem realizar consultas em diferentes sistemas e olhar para linhas de registros.

Não surpreendentemente, a plataforma também foi uma grande vitória para a equipe de segurança. A equipe não só começou a detectar ataques tradicionais, mas também descobriu ameaças mais sofisticadas.

> “Internamente, quando começamos a analisar a solução, vimos que definitivamente precisávamos de desenvolvedores que fizessem parceria conosco. Não é possível entrar nos sistemas críticos, basicamente o coração dos aplicativos, sem a ajuda deles.
>
> – **James Robinson**
> **Vice-CISO, Netskope**

Perspectivas futuras: manter os clientes em conformidade

Pensando nas perspectivas futuras, a Netskope planeja usar a Akamai para abordar a governança de APIs, garantindo que ela e seus clientes permaneçam em conformidade com as leis e determinações de privacidade de dados em expansão global. Também planeja continuar a explorar diferentes casos de uso, pois possui o Akamai API Security implantado tanto na nuvem quanto no local. A implantação no local tem sido um divisor de águas para a Netskope e seus clientes no setor público, além de outros setores altamente regulamentados.

> Não só a Noname foi vencedora, mas também apoiou uma implantação melhor e mais rápida para chegarmos ao mercado mais rápido.
>
> – James Robinson
> Vice-CISO, Netskope

As organizações estão adotando rapidamente uma arquitetura de SASE (edge de serviço de acesso seguro) para proteger os dados onde quer que eles se movam, apoiar os esforços de transformação digital e aumentar a eficiência e o ROI (retorno sobre o investimento) da tecnologia. A Netskope já é uma especialista amplamente reconhecida e inovadora em CASB, SWG, ZTNA, firewall como serviço e outros componentes da SSE (edge de serviço de segurança), que descreve os serviços de segurança necessários para uma arquitetura SASE bem-sucedida.

Apesar da popularidade da SASE, mensagens confusas de fornecedores muitas vezes acompanham conjuntos de produtos fragmentados que são questionavelmente comercializados como "SASE". A maioria desses produtos não é integrada de forma nativa nem é capaz de simplificar ambientes de tecnologia. Além disso, eles não têm recursos críticos de transformação de rede e infraestrutura, sendo que todos arriscam níveis mais altos de incidentes de segurança, tempo de inatividade da rede e baixo ROI.

A Netskope Borderless SD-WAN foi combinada com o Netskope Intelligent SSE em uma plataforma SASE totalmente convergente, abordando exclusivamente esses desafios.

Akamai