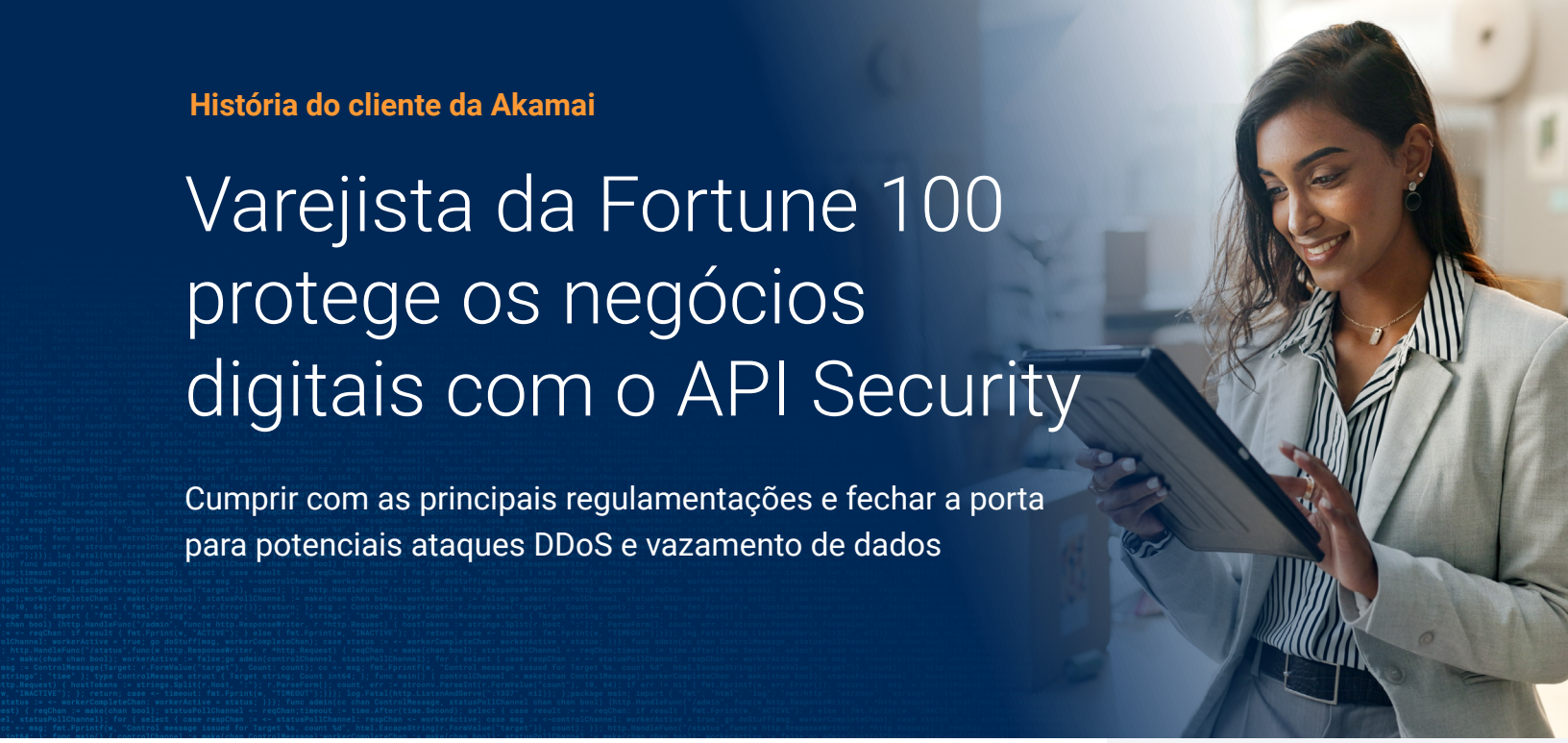
História do cliente da Akamai

Varejista da Fortune 100 protege os negócios digitais com o API Security

Cumprir com as principais regulamentações e fechar a porta para potenciais ataques DDoS e vazamento de dados



O varejo está passando por uma transformação significativa com a adoção de processos digitais impulsionados pelo poder das APIs (interfaces de programação de aplicativos). As APIs estão revolucionando a forma como os varejistas operam, interagem com os clientes e gerenciam seus negócios.

Os varejistas estão integrando seus sistemas com vários aplicativos e serviços de terceiros por meio de APIs, permitindo interações perfeitas em diferentes plataformas. Por exemplo, as APIs permitem que os varejistas integrem suas plataformas de comércio eletrônico com gateways de pagamento, transportadoras e sistemas de gerenciamento de estoque. No entanto, à medida que esse ecossistema se expande, ele cria uma grande quantidade de potenciais vulnerabilidades de segurança.

A segurança de APIs é fundamental no cenário digital atual. À medida que as organizações dependem cada vez mais de APIs para conectar sistemas, compartilhar dados e possibilitar integrações, assegurar a segurança dessas interfaces se torna fundamental. Por essa razão, este varejista da Fortune 100 recorreu à Noname Security (agora uma empresa Akamai) para proteger sua superfície de ataque a APIs.

Descoberta da superfície de ataque a APIs

A descoberta de APIs desempenha um papel essencial no controle da multiplicação de APIs, que se refere à proliferação descontrolada de APIs dentro de uma organização. À medida que as empresas adotam cada vez mais APIs para permitir a transformação digital e impulsionar a inovação, ter uma abordagem sistemática para descobrir e gerenciar efetivamente essas APIs se torna essencial. Além disso, no ecossistema de varejo digital em rápido crescimento, garantir que suas APIs estejam protegidas é um primeiro passo vital.

Designer Merchandise Retailer

Localização

Estados Unidos

Setor

Varejo

Solução

Akamai API Security

Principais impactos

- Prevenção da exposição de dados
- Descoberta da superfície de ataque a APIs
- Redução de riscos e de custos

Akamai

Este líder de varejo estava enfrentando uma falta de visibilidade do inventário e do tráfego de APIs. Sem governança sobre plataformas diferentes (no local e na nuvem), não foi possível desenvolver uma proteção escalável do SDLC de APIs. A empresa se envolveu com a nossa equipe para que ela fornecesse descoberta contínua de ativos de API para reduzir riscos e custos, identificando configurações incorretas, vulnerabilidades e não conformidade e integrando-se com seu fluxo de trabalho existente de SecOps (por exemplo, Splunk).

Prevenção da exposição de dados confidenciais

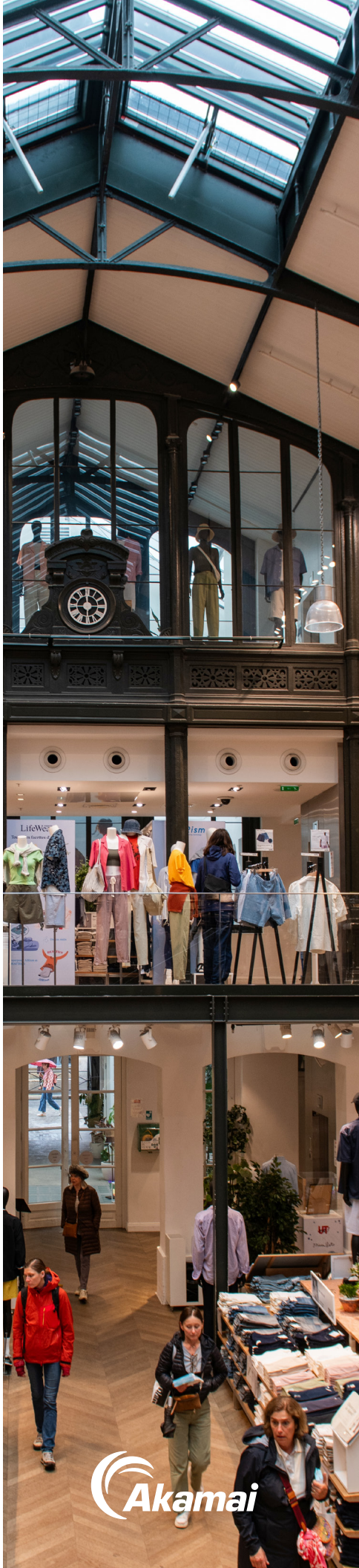
No setor de varejo, existem várias regulamentações de conformidade às quais as organizações devem aderir. Essas regulamentações têm como objetivo proteger os direitos dos consumidores, garantir práticas comerciais justas e manter a privacidade e a segurança dos dados. As empresas devem ser capazes de ver e de proteger APIs que lidam com dados confidenciais para cumprir as principais regulamentações e padrões do setor, e evitar consequências legais e danos à reputação.

A equipe da Akamai ajudou o varejista da Fortune 100 a impedir que dados confidenciais fossem expostos publicamente. O varejista estava usando uma versão antiga do Jira, o que resultou em um bug que expôs publicamente nomes de funcionários, nomes de usuários do Jira e endereços de e-mail. As APIs voltadas para o público também apresentavam risco de postura para a empresa.

A solução Akamai API Security resolveu lacunas na postura de segurança de APIs da empresa e corrigiu erros de configurações em seu ambiente. Por exemplo, a configuração de arquitetura ineficiente deixava a porta aberta para um risco expandido por meio de ataques DDoS e vazamento de dados.

Daqui para a frente

O cliente interage ativamente com a equipe da Akamai toda semana para impulsionar a adoção organizacional. Também está muito interessado em explorar novas integrações com seus fluxos de trabalho existentes. O Akamai API Security identifica e prioriza de forma inteligente vulnerabilidades potenciais, que podem ser corrigidas manualmente, de forma semiautomática ou totalmente automática por meio de integrações em WAFs, gateways de APIs, SIEMs, ITSMs, ferramentas de fluxo de trabalho ou outros serviços. Além disso, devido à rápida expansão da pilha de tecnologia do cliente, há uma série de integrações que estão sendo analisadas.



 | Publicado em 08/24