LISTA DE VERIFICAÇÃO DA AKAMAI

Lista de verificação de segurança de JavaScript do PCI DSS v4.0 com proteção e conformidade no lado do cliente da Akamai

O Padrão de segurança de dados da indústria de cartões de pagamento (PCI DSS, na sigla em inglês) é um padrão de segurança global desenvolvido para proteger a segurança dos dados de cartões de pagamento on-line e facilitar a ampla adoção de medidas consistentes de segurança de dados em todo o mundo. Trata-se de um dos padrões de segurança mais importantes, e a conformidade é exigida por qualquer organização que processa dados de cartões de pagamento on-line.

A versão mais recente do PCI DSS (disponível apenas em inglês), a versão 4.0, entra em vigor em 2025. Ela inclui 12 requisitos básicos de segurança de dados, atualizados com orientações para lidar com as novas e crescentes ameaças à segurança cibernética. Dois requisitos principais adicionados ao PCI DSS v4.0, 6.4.3 e 11.6.1, abordam a segurança do JavaScript e a proteção contra ataques de Web skimming no lado do cliente que roubam informações confidenciais do usuário final de dentro do navegador. A popularidade desses ataques cresceu ao longo dos anos e técnicas sofisticadas tornaram eles cada vez mais difíceis de detectar. Eles podem ter consequências devastadoras para as organizações vitimadas; incluindo multas pesadas, danos à reputação da marca, perda de receita e diminuição da confiança dos clientes.

Vamos examinar uma lista de verificação do que os novos requisitos de segurança de script do PCI DSS v4.0 envolvem e comparar com a proteção e a conformidade no lado do cliente.

Requisitos do PCI DSS v4.0	Como a proteção e conformidade no lado do cliente ajudam
Requisito 6.4.3 — As aplicações da Web voltadas para o público são protegidas contra ataques ☑ Um método é implementado para confirmar se cada script carregado e executado no navegador está autorizado ☑ Um método é implementado para garantir a integridade de cada script carregado e executado no navegador ☑ Um inventário de todos os scripts carregados e executados no navegador é mantido com justificativa por escrito de por que cada um é necessário	**Autorize com um clique** ☑ Gerencie facilmente quais scripts você permite que sejam executados nas páginas de pagamento do seu website diretamente na ferramenta **Garanta a integridade desde o início** ☑ A tecnologia comportamental analisa cada script executado no navegador para detectar e alertar sobre atividades maliciosas ou exfiltração de dados **Rastreie e inventarie todos os scripts automaticamente** ☑ Justificativas predefinidas e regras automatizadas facilitam a justificação da finalidade de cada script carregado e executado no navegador

Requisitos do PCI DSS v4.0	Como a proteção e conformidade no lado do cliente ajudam
Requisito 11.6.1 — Alterações não autorizadas nas páginas de pagamento são detectadas e respondidas **Um mecanismo de detecção de alteração e violação é implantado da seguinte forma:** ☑ Alertar o pessoal para modificações não autorizadas (incluindo indicadores de comprometimento, alterações, adições e exclusões) nos cabeçalhos de HTTP e no conteúdo das páginas de pagamento, conforme recebido pelo navegador do consumidor ☑ O mecanismo está configurado para avaliar o cabeçalho de HTTP recebido e a página de pagamento **As funções do mecanismo são executadas** pelo menos uma vez a cada sete dias ou periodicamente (na frequência definida na análise de risco direcionada da entidade, que é realizada de acordo com todos os elementos especificados no Requisito 12.3.1)	**Mantenha suas páginas de pagamento protegidas** ☑ Monitore, analise e mitigue adulterações maliciosas de páginas de pagamento para garantir que os dados valiosos do usuário final permaneçam seguros **Investigue modificações não autorizadas em tempo real com alertas imediatos e práticos** ☑ Com detecção instantânea, as equipes de segurança podem responder rapidamente a alterações ou modificações não autorizadas em cabeçalhos de HTTP em páginas de pagamento **Proteja com defesa sempre ativa** ☑ A proteção 24 horas por dia assegura as interações do usuário em suas páginas de pagamento

O Akamai Client-Side Protection & Compliance oferece proteção robusta contra ameaças ao JavaScript e permite visibilidade da superfície de ataque no lado do cliente para proteger dados confidenciais no navegador. Os recursos específicos do PCI DSS v4.0 ajudam as equipes de segurança e conformidade a simplificar o processo de auditoria do PCI DSS v4.0 e fornecer fluxos de trabalho dedicados para ajudar a cumprir os requisitos de segurança de script 6.4.3 e 11.6.1.

O Akamai Client-Side Protection & Compliance tem opções de implantação flexíveis e não exige que o Akamai Connected Cloud esteja habilitado.

Saiba mais sobre como esses recursos podem ajudar sua organização a cumprir o PCI DSS v4.0.