RESUMO DO PRODUTO DA AKAMAI

Client-Side Protection & Compliance

Proteja-se contra vulnerabilidades de JavaScript no lado do cliente e simplifique a conformidade regulatória.

O JavaScript é uma ferramenta essencial para aplicações Web modernas. Desde a otimização da experiência do usuário até o aprimoramento da funcionalidade e do desempenho, o uso de JavaScript próprio e de terceiros cresceu exponencialmente ao longo do tempo. Embora existam inúmeros benefícios que vêm com seu uso, uma cadeia de fornecimento digital de JavaScript também pode deixar websites vulneráveis a ataques no lado do cliente, que visam roubar informações confidenciais do usuário final dentro do navegador, incluindo dados de cartão de pagamento, por meio da injeção de código mal-intencionado.

Como esses ataques não têm visibilidade no lado do servidor e contornam as medidas de segurança tradicionais, as organizações podem facilmente ser vítimas, resultando na diminuição da confiança do cliente, multas regulatórias devastadoras, penalidades de conformidade e danos à reputação da marca.

Akamai Client-Side Protection & Compliance

A solução Akamai Client-Side Protection & Compliance ajuda a proteger contra a exfiltração de dados do usuário final e protege websites contra ameaças de JavaScript. Ela foi projetada para detectar comportamentos mal-intencionados de scripts e fornecer alertas acionáveis para que as equipes de segurança mitiguem atividades prejudiciais em tempo real.

Com recursos de conformidade com o padrão PCI DSS v4.0, a Client-Side Protection & Compliance ajuda as organizações a atender aos novos requisitos de segurança de script e protege os dados de cartões de pagamento contra ataques no lado do cliente. Gerencie facilmente o inventário de scripts de sua página de pagamento, simplifique o processo de auditoria por meio de um único painel abrangente e receba alertas dedicados de PCI para responder rapidamente a eventos relacionados à conformidade.

Principais recursos

Proteção contra a exfiltração de dados confidenciais no lado do cliente

Os cibercriminosos estão à procura de informações confidenciais dos seus usuários finais. Ao explorar vulnerabilidades nas cadeias de fornecimento de JavaScript, os agentes mal-intencionados são capazes de injetar código em websites para extrair informações confidenciais e exfiltrá-las para uso fraudulento. A solução Client-Side Protection & Compliance combina machine learning e pontuação heurística para analisar o comportamento do script em tempo real para detectar atividades mal-intencionadas e recursos vulneráveis. Ela fornece às equipes de segurança alertas acionáveis imediatos para se defender rapidamente contra ataques no lado do cliente, incluindo skimming na Web, Magecart e formjacking.

BENEFÍCIOS PARA SUA EMPRESA

Detecção e proteção Monitore o comportamento do script em sessões de usuários reais para detectar atividades suspeitas

Fluxos de trabalho do PCI DSS v4.0
Ajuda a atender aos requisitos de segurança do JavaScript 6.4.3 e 11.6.1

Alertas priorizados em tempo real Mitigue imediatamente eventos de alto risco com alertas acionáveis

Visibilidade no lado do cliente
Obtenha visualizações abrangentes da superfície de ataque no lado do cliente

Gerenciamento de políticas
Gerencie o comportamento do script e a execução do JavaScript em tempo de execução

Detecção de vulnerabilidade
Identifique CVEs (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) respaldadas pela inteligência de ameaças da Akamai

Opções flexíveis de implantação
Implante facilmente por meio da Akamai Connected Cloud ou diretamente no servidor de origem

Akamai

Suporte dedicado à conformidade com o PCI DSS v4.0

Os requisitos de segurança de script do PCI DSS v4.0 6.4.3 e 11.6.1 impõem a necessidade de as organizações protegerem os dados de cartões de pagamento contra ataques no lado do cliente e garantirem o gerenciamento de scripts em páginas de pagamento. A solução Client-Side Protection & Compliance rastreia e faz o inventário de todos os scripts nas páginas de pagamento, garantindo sua integridade e autorização. Ela fornece justificativas predefinidas e regras automatizadas para justificar facilmente todos os scripts carregados. A solução também monitora as alterações nos cabeçalhos HTTP e na proteção da página de pagamento para se defender contra adulteração da página. Um painel abrangente e alertas dedicados de PCI permitem que as organizações respondam rapidamente a eventos relacionados à conformidade e garantam a proteção dos dados de cartões de pagamento dentro do navegador. Com esses recursos, as equipes de segurança e conformidade podem reduzir a carga do processo de auditoria de PCI e agilizar os fluxos de trabalho.

Ampla visibilidade das ameaças de JavaScript

As proteções tradicionais de aplicações Web, como firewalls de aplicações Web, monitoram apenas o tráfego no lado do servidor e não podem fornecer visibilidade da atividade executada no lado do cliente. As abordagens baseadas em normas para proteção contra tais ameaças, como as políticas de segurança de conteúdo, são difíceis de gerenciar e fornecem proteção limitada contra cargas perigosas introduzidas na cadeia de fornecimento de scripts fora do controle dos operadores de páginas da Web. Isso cria um ponto cego para as organizações, fazendo com que o código prejudicial não seja detectado por dias, semanas ou até mesmo meses enquanto continua o roubo de dados confidenciais. A Client-Side Protection & Compliance fornece uma visão incomparável da superfície de ataque no lado do cliente do seu website, incluindo o comportamento, as vulnerabilidades, o alcance e o impacto de cada script, bem como os dados acessados ou a ameaça existente.

Como funciona

A Client-Side Protection & Compliance é executada no navegador do usuário final para monitorar execuções de scripts no lado do cliente em uma página da Web protegida. Quando os scripts exibem alterações nos comportamentos, as técnicas de machine learning são empregadas para avaliar o risco de ações não autorizadas ou inadequadas. Elas alertam as equipes de segurança sobre eventos de alto risco, permitindo a investigação imediata e a mitigação de possíveis ameaças.

Configuração São injetados scripts simples em cada página monitorada sem impacto significativo no desempenho.

Monitoramento e avaliação Os dados de atividade JavaScript são coletados do navegador da Web de um usuário e monitorados. As técnicas de machine learning são empregadas para avaliar o risco de ações não autorizadas ou inadequadas, se encontradas.

Alertas Alertas em tempo real com informações detalhadas para mitigar ameaças são enviados se uma ameaça ou ataque ativo for encontrado.

Mitigação O JavaScript mal-intencionado é imediatamente impedido de acessar e de exfiltrar dados confidenciais em páginas protegidas com um simples clique.

Agilize a conformidade com requisitos de segurança de script PCI DSS v4.0

Integridade e autorização do script (6.4.3)

Garanta a integridade e a autorização de todos os scripts carregados em páginas de pagamento protegidas.

Inventário e justificativa do script (6.4.3)

Rastreie e faça inventários de scripts carregados em páginas de pagamento protegidas. Justifique rapidamente todos os scripts, aproveitando as justificativas predefinidas e as regras automatizadas.

Proteção de páginas de pagamento (11.6.1)

Detecte e responda imediatamente a alterações não autorizadas em páginas de pagamento protegidas.

Painel intuitivo

Simplifique o processo de conformidade e auditoria do PCI DSS v4.0 por meio de um painel dedicado com informações detalhadas sobre tarefas relacionadas e alertas para requisitos de segurança do script 6.4.3 e 11.6.1.

Alertas de PCI acionáveis

Receba e registre alertas detalhados para eventos relacionados à conformidade com PCI, incluindo scripts não autorizados, exfiltração de dados de pagamento e adulteração de página de pagamento.

Para saber mais, acesse nossa página de produtos ou entre em contato com a equipe de vendas da Akamai.

 | Suporte | | Publicado em 09/23