

RESUMO DA SOLUÇÃO DA AKAMAI

Conformidade com o PCI DSS v4.0 através da Akamai

A conformidade com o PCI significa a adesão a um conjunto global de requisitos de segurança para proteger ambientes com dados de contas de cartões de pagamento. Qualquer empresa que processa, transmite ou armazena dados de titulares de cartões online tem a responsabilidade de aderir ao PCI DSS (Payment Card Industry Data Security Standard). Desenvolvido em 2004, o padrão é atualizado regularmente para atender às mudanças do setor e lidar com as crescentes ameaças à cibersegurança. O padrão mais recente, PCI DSS v4.0, foi lançado em março de 2022 com alterações significativas e contém 12 requisitos essenciais que as organizações precisam cumprir até março de 2025.

Você está preparado para atender aos requisitos do PCI DSS v4.0?

Embora a não conformidade com os padrões do PCI não seja punível por lei, as empresas de cartão de crédito podem impor multas às organizações que não cumprem o padrão. Além disso, a falta de proteção de dados de titulares de cartões pode deixar as marcas vulneráveis a ataques cibernéticos que resultam em violações de dados devastadoras, com multas pesadas e a perda permanente da confiança dos clientes.

Estamos aqui para ajudar. A Akamai não só mantém conformidade de Nível 1 com o PCI DSS, mas também oferece uma variedade de soluções de segurança líderes do setor para ajudar as organizações a estar em conformidade com o PCI DSS v4.0. Algumas soluções ajudam até mesmo a reduzir o escopo de uma auditoria do PCI, economizando tempo e dinheiro valiosos que seriam gastos para atender a requisitos de certificação.

App & API Protector com proteção contra malware

Mantenha a conformidade com os requisitos de registro e proteja-se contra o vazamento de informações pessoalmente identificáveis, ataques de dia zero e CVEs, bem como outros ataques baseados em edge para atender aos requisitos 6.4.2, 6.5.3 e 11.5.

"Todos os dias, 560 mil novos tipos de malware são detectados, somando-se aos mais de 1 bilhão de programas de malware já em circulação."

Fonte: Getastra | 30+ Malware Statistics You Need to Know In 2023

Benefícios



Simplifique fluxos de trabalho de equipes de segurança e conformidade



Reduza a carga das auditorias com recursos dedicados e específicos do PCI



Receba e registre alertas acionáveis do PCI para eventos relacionados à conformidade



Consolide fornecedores para atender aos requisitos do PCI com o abrangente portfólio de soluções de segurança da Akamai



API Security

Detecte e mitigue violações de comportamento e lógica de APIs, registre a atividade de APIs e implemente proteção responsiva e automatizada para suas APIs para facilitar o cumprimento dos requisitos de conformidade 6.2.3, 6.2.4, 6.3.2, 6.4.1, 6.4.2, 10.2.1, 10.5.1 e 11.3.2.

"Até 2024, as violações de APIs e dados praticamente dobrarão."

Fonte: [Gartner: Top 10 Aspects Software Engineering Leaders Need to Know About APIs](#) (disponível apenas em inglês)

Client-Side Protection & Compliance

Atenda aos novos requisitos [6.4.3](#) e [11.6.1](#) de segurança de JavaScript para ajudar na proteção contra ataques do lado do cliente, como web skimming ou Magecart, que exfiltram dados de cartões de pagamento de páginas online de finalização de compras através da injeção de código mal-intencionado no navegador.

"81% de grandes varejistas online relatam que sua organização foi alvo de um comportamento suspeito de scripts em 2022."

Fonte: [From Bad Bots to Malicious Scripts: The Effectiveness of Specialized Defense | 2023](#) (disponível apenas em inglês)

Akamai Guardicore Segmentation

Segmente os ativos regulamentados de forma mais eficiente aproveitando várias tecnologias integradas em uma única plataforma para ajudar a atender a [muitos requisitos do PCI](#). Obtenha visibilidade de rede e ativos, um firewall distribuído, aplicação de políticas até a camada 7 e detecção e resposta a violações.

"A segmentação definida por software nos permitiu criar e aplicar políticas de segmentação no nível dos processos, melhorando significativamente nossa postura de segurança e a capacidade de atender aos requisitos técnicos do PCI DSS."

— Senior Infrastructure Engineer, The Honey Baked Ham Company

Para saber mais sobre como impulsionar a conformidade com o PCI DSS v4.0 através da Akamai, entre em contato com nossa [equipe de especialistas](#).