Resumo do produto da Akamai

Brand Guardian

Confiança digital agora é uma questão crítica de segurança. A inteligência artificial (IA) industrializou a falsificação de marcas, permitindo que invasores lancem sites de phishing convincentes, domínios falsificados e campanhas fraudulentas em minutos. Isso resulta em maiores prejuízos com fraudes, perda de clientes e enfraquecimento da confiança na marca. As abordagens tradicionais de monitoramento de marca não conseguem acompanhar esse ritmo. As organizações precisam de uma solução contínua e orientada por inteligência que detecte e interrompa violações em escala global da Internet.

Para proteger clientes e preservar a confiança, as organizações devem tratar a violação de marca como uma questão central de segurança, oferecendo visibilidade contínua, priorização inteligente e resposta automatizada rápida em várias superfícies de ataque.

A realidade da proteção de uma marca digital

Fraude e violação de marca já não são mais questões de segurança de nicho, mas operações em grande escala impulsionadas por automação e IA generativa. Essas tecnologias reduziram drasticamente a barreira de entrada para invasores, permitindo que criem golpes convincentes, conteúdo de phishing e experiências digitais falsificadas em velocidade e volume sem precedentes.

Hoje, pode levar apenas minutos para que invasores coloquem no ar um site falsificado, com identidade visual, linguagem e fluxos de clientes realistas. Grandes empresas lidam regularmente com milhares de golpes ativos que imitam suas marcas e variações de falsificação de identidade, a maioria totalmente fora do alcance das ferramentas de segurança tradicionais.

Ao mesmo tempo, usuários têm dificuldade para distinguir experiências falsas das legítimas. Conteúdo gerado por IA, sites clonados e táticas sofisticadas de engenharia social fazem com que perfis falsos em redes sociais, e-mails e páginas de login pareçam autênticos. Como resultado, aumenta a probabilidade de clientes interagirem, fornecerem credenciais ou concluírem transações antes de perceberem que foram enganados, se é que chegam a perceber.

Os modelos tradicionais de proteção de marca são reativos, manuais e isolados. A segurança de marca moderna deve ser contínua, automatizada e integrada às principais operações de segurança. Esses fluxos de trabalho legados são lentos, exigem muitos recursos e não conseguem acompanhar a dinâmica de um ambiente em que invasores mudam constantemente de domínios, provedores de hospedagem e identidades. Quando um site fraudulento é identificado e removido, vários substitutos já entraram no ar, perpetuando o ciclo.

Benefícios para a sua empresa

Proteja a confiança na marca
Remova proativamente sites falsificados e imitações para garantir que sua marca permaneça segura, confiável e autêntica em todos os canais digitais.

Reduza a fraude contra clientes
Elimine infraestruturas de phishing e golpes antes que haja interação para proteger os clientes contra ataques avançados impulsionados por IA.

Acelere a resposta a ameaças
Substitua fluxos de trabalho manuais por descoberta e execução automatizadas para encurtar o tempo de desativação.

Reduza a perda de clientes
Evite golpes relacionados à marca que geram insatisfação e abandono, contribuindo para a retenção de clientes.

Escale sem ampliar a equipe
Gerencie simultaneamente milhares de domínios semelhantes e variações de golpes usando automação e inteligência.

Melhore a priorização de riscos
Concentre recursos nas ameaças mais críticas ao classificar a violação de marca com base no impacto para clientes, no risco financeiro e na reputação.

Fortaleça a visibilidade executiva
Forneça insights claros e mensuráveis sobre o risco de marca, a eficácia das remoções e a análise de tendências, ajudando a liderança a compreender o nível de exposição.

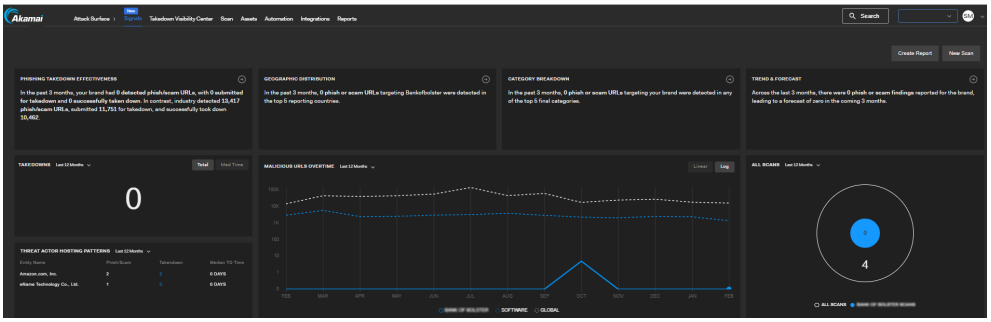
Unifique a proteção de marca
Elimine os silos entre as equipes de segurança, fraude, jurídico, confiança/segurança e marketing ao fornecer uma visão unificada da violação de marca.

Akamai

Como o Akamai Brand Guardian ajuda

O Brand Guardian aborda essa nova realidade tratando a violação de marca como um problema contínuo de segurança em larga escala, que requer automação, inteligência e visibilidade em toda a Internet. Com detecção baseada em IA e visibilidade de infraestrutura em escala da Internet, o Brand Guardian permite que as organizações detectem, priorizem e neutralizem ataques baseados em marca na velocidade em que surgem.

Em vez de depender de relatórios de clientes ou pesquisas manuais, o Brand Guardian identifica continuamente a falsificação de marca em domínios, sites, redes sociais, lojas de aplicativos e fontes da dark web em tempo real. Uma análise avançada correlaciona sinais para distinguir ruído de baixo risco de ameaças de alto impacto, ajudando as equipes a focarem em atividades que colocam clientes e receita em risco.



O painel Sinais fornece insights baseados em IA e feeds de ameaças para monitorar phishing e falsificação de identidade

A resposta é automatizada e escalável

Fluxos de trabalho integrados aceleram a investigação, a coleta de evidências e as ações de desativação em registradores, provedores de hospedagem e outras plataformas on-line. Modelos de IA treinados com padrões reais de violação de marca separam ameaças reais do uso legítimo da marca, minimizando falsos positivos e garantindo que sua equipe se concentre no que realmente importa. Enquanto a automação cuida das remoções rotineiras, analistas de segurança experientes se dedicam aos casos mais complexos que exigem análise humana.

Essa proteção vai além do simples monitoramento de marca. Ao integrar a inteligência contra ameaças à marca com a postura de DNS e os recursos de segurança mais amplos da Akamai, as organizações passam a ter uma visão unificada do risco externo, permitindo uma governança mais eficaz, respostas mais rápidas e maior clareza na responsabilização executiva.

Principais recursos do produto:

- **Descoberta contínua de violações de marca**
  Identifica automaticamente a falsificação de marca em domínios semelhantes, sites de phishing, perfis falsos em redes sociais, aplicativos falsos, e-mails e novos canais digitais.
- **Detecção de ameaças por IA**
  Usa IA avançada para detectar violações de marca em milissegundos e minimizar falsos positivos.
- **Investigação e desativação automatizadas**
  Fluxos automatizados de desativação aceleram a coleta de evidências e a aplicação de medidas em registradores, provedores de hospedagem e plataformas, reduzindo significativamente o tempo de remoção.

- **Priorização de ameaças baseada em risco**
  Classifica as ameaças com base na probabilidade de causar danos aos clientes, viabilizar fraudes e impactar a reputação, permitindo que as equipes priorizem os riscos mais relevantes.
- **Ampla visibilidade multicanal**
  Monitora domínios, sites, plataformas sociais, lojas de aplicativos, mecanismos de pesquisa, e-mails e fontes da dark web em uma única plataforma.
- **Postura unificada de marca e segurança**
  Integra a inteligência contra ameaças à marca com os recursos mais amplos de segurança e postura de DNS da Akamai, permitindo que as organizações gerenciem o abuso de marca como parte de uma estratégia de segurança holística.

Ao acompanhar a escala e a velocidade das fraudes modernas, o Brand Guardian ajuda as organizações a proteger os clientes, reduzir a perda de clientes e preservar a confiança na marca, onde quer que ela seja alvo na Internet.

Solicite uma avaliação de marca com sua equipe da Akamai ou acesse akamai.com para saber mais.

© 2026 Akamai Technologies | Suporte |
| Publicado em 03/26