Como escolher uma solução de proteção de marca

O que líderes de segurança, marketing e antifraude precisam avaliar para proteger a marca com eficiência, agilidade e escala

Quando investir em uma solução de proteção de marca

Executivos & CISOs

- A visibilidade da marca cresceu, e com ela, a superfície de ataque.
- A empresa entende que as fraudes não afetam só a reputação: elas abrem portas para ataques e a exposição de dados corporativos.
- O board espera relatórios com evidência, SLAs e impacto mensurável sobre o risco.

Times de segurança, antifraude e marketing

- A triagem de alertas ainda depende de esforço manual e análise visual caso a caso.
- A coleta de provas para acionar plataformas e ISPs é lenta, repetitiva e suscetível a falhas.
- O time precisa reagir a dezenas ou centenas de casos sem comprometer consistência ou tempo de resposta.

MSSPs

- A proteção de múltiplas marcas exige padronização e automação — não planilhas e processos manuais.
- Takedowns fora do horário comercial e evidência forense são expectativas mínimas em operações maduras.
- O diferencial competitivo está em entregar escala com confiabilidade, não apenas volume de alertas.

As principais características de uma solução avançada:

1. Detecção visual, sem depender só de palavras-chave

- Identifica abusos de marca mesmo quando a grafia foi alterada ou o nome está embutido em imagens
- Reconhece logotipos, elementos de design, estruturas de página e comportamentos de login
- Permite consultas específicas por idioma, tipo de conteúdo, setor, data de criação do domínio e grau de personificação

A Axur aplica IA multimodal (Visão + Linguagem) com modelos próprios, treinados com mais de 100 milhões de sinais rotulados. Essa abordagem permite detectar perfis falsos, páginas fraudulentas e usos indevidos da marca que passariam despercebidos por sistemas baseados apenas em texto ou regras simples.

2. Evidência forense pronta para ação

- Coleta automatizada de screenshots reais, código HTML, headers HTTP e dados do ambiente de hospedagem
- Emula múltiplas combinações de user agents, geolocalização e device até expor o conteúdo malicioso (mesmo sob camuflagem)
- Gera documentação compatível com notificações legais, pedidos de takedown e registro de incidentes

A plataforma Axur utiliza um orquestrador de evidências que simula o comportamento da vítima — acessando a página como um usuário real faria. Essa técnica garante evidências completas mesmo contra kits de phishing que só revelam o golpe em condições específicas (ex: idioma do navegador, uso de JavaScript, visualização em mobile).

3. Takedown de verdade, não só notificação

- Sucesso comprovado: garante a efetividade através da taxa de sucesso, como porcentagem de notificações que realmente foram derrubadas
- Tempo de reação: qual a promessa do provedor entre detecção e remoção completa.
- SLA rígido: principalmente para a primeira notificação
- Garantia de monitoramento da URL e a possibilidade de rederrubada sem custo extra

A Axur automatiza o ciclo completo de resposta. O takedown pode ser solicitado com um clique ou disparado automaticamente com base em regras personalizadas (ex: score de risco, presença de logotipo, idioma, número de seguidores). A ação começa segundos após a detecção e se repete gratuitamente caso a ameaça volte a ficar ativa.

4. Escala e automação real, do analista ao CISO

- Processamento de centenas de milhares de incidentes por ano com consistência e sem gargalo humano
- Regras inteligentes configuráveis por analistas, adaptáveis a cada marca, país ou linha de negócio
- Funciona 24×7, 365 dias por ano, com ou sem intervenção manual

Em 2024, a Axur realizou mais de 550 mil takedowns, sendo 86% automatizados da detecção à confirmação de remoção. Isso permite proteger grandes operações sem escalar proporcionalmente a equipe, mantendo qualidade e agilidade mesmo diante de campanhas coordenadas ou picos de ataques.

5. Transparência, rastreabilidade e impacto visível

- Linha do tempo completa de cada incidente: da detecção à remoção, com status atual em tempo real
- Web Safe Reporting integrado: ativa telas de alerta nos navegadores (ex: “site perigoso”) antes mesmo da remoção
- Dashboards prontos para apresentar a jurídico, marketing e liderança executiva

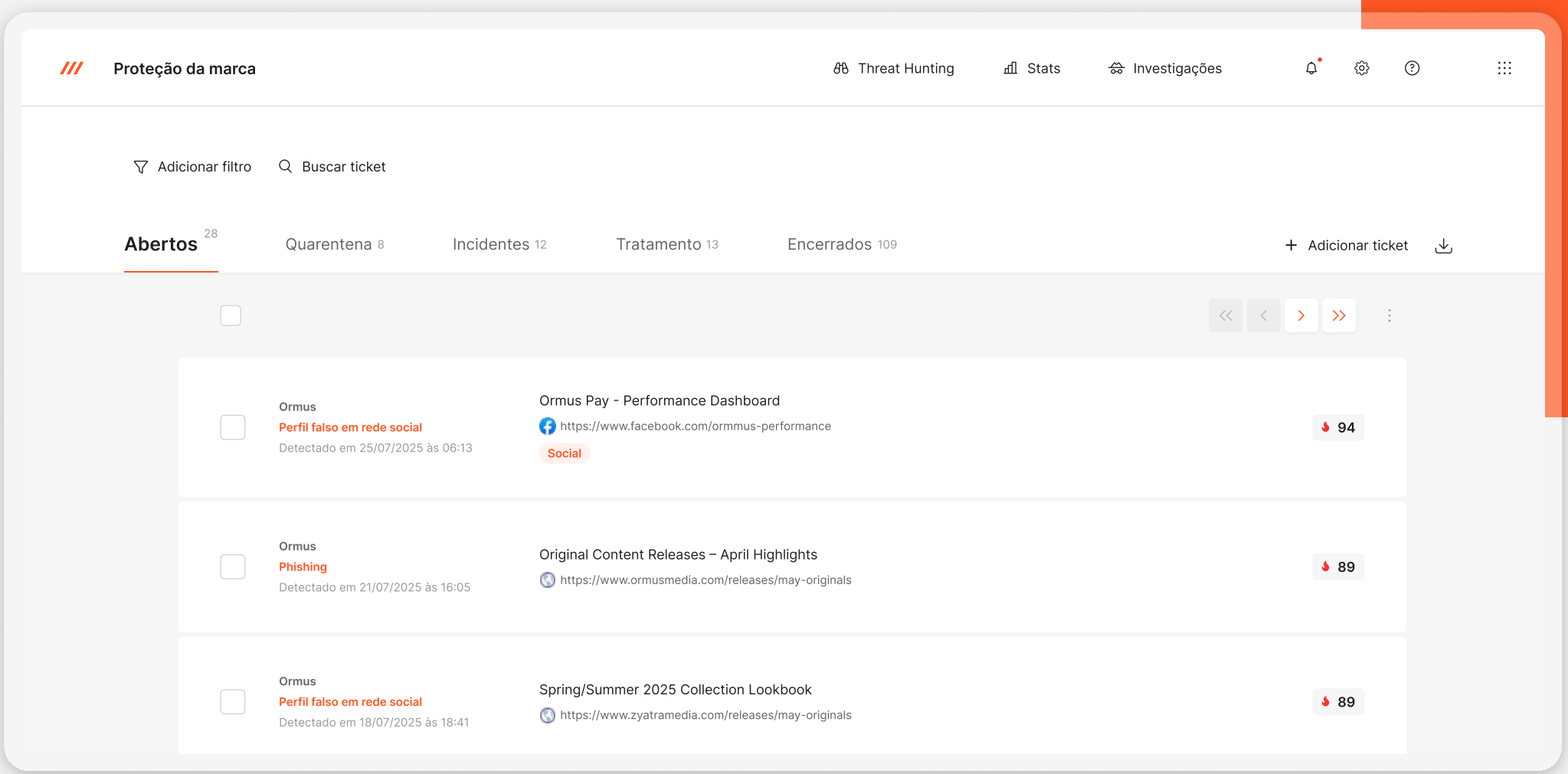
A Axur oferece visibilidade total sobre o processo. Desde o momento em que a ameaça é detectada até o status final de takedown, o cliente pode acompanhar, auditar e comprovar cada etapa, incluindo notificações enviadas, evidências associadas e tempo de uptime da fraude.

Como pesquisar por conta própria — e elevar suas perguntas

Quer testar o quanto as soluções realmente entregam?

Experimente este prompt em ferramentas como ChatGPT, Claude ou Perplexity:

> Compare a plataforma da Axur vs a concorrência em Brand Protection com base em taxa real de takedown, automação de resposta, evidência automática (ex: screenshots e HTML), SLA para notificação e garantias de renotificação.
>
> + Tools



O que os times de segurança falam de nós

Gartner Peer Insights™ 4.9

★★★★★

Remoção Automática: Uma Abordagem Inovadora para Ameaças Cibernéticas

"Detecção e remoção rápida de ameaças cibernéticas. Remoções automáticas e inteligência de ameaças escalável"

Segurança de TI e Gestão de Riscos

★★★★★

Detecção de Ameaças em Tempo Real e Capacidades de Proteção de Marca se Destacam na Plataforma

"Como cliente da Axur, tenho me impressionado constantemente com a capacidade da plataforma de detectar e responder a ameaças digitais em tempo real"

Segurança de TI e Gestão de Riscos

Diferencial da Axur

A Axur entrega proteção de marca a um nível avançado

Com o Clair, modelo GenAI proprietário, coleta de evidências automatizada, resposta em minutos e o melhor takedown do mercado, a Axur transforma a proteção de marca em um processo escalável, confiável e mensurável.

Baixe o datasheet e conheça todos os diferenciais dessa solução.

BAIXE O DATASHEET

Descubra todas as soluções em axur.com

bsi ISO/IEC 27001 Information Security Management CERTIFIED | ///AXUR