Cómo elegir una solución de protección de marca

Qué deben evaluar los líderes de seguridad, marketing y antifraude para proteger la marca con eficiencia, agilidad y escala.

Cuándo invertir en una solución de protección de marca

Ejecutivos y CISOs

- La visibilidad de su marca ha crecido, y con ella, su superficie de ataque.
- La organización entiende que el fraude impacta más allá de la reputación: crea puntos de entrada para ataques y la exposición de datos corporativos.
- La junta directiva espera informes con evidencias claras, SLA y un impacto medible en el riesgo.

Equipos de seguridad, antifraude y marketing

- La clasificación de alertas todavía depende de trabajo manual y de un análisis visual caso por caso.
- La recolección de evidencias para escalar casos a plataformas y proveedores de servicios de internet (ISP) es lenta, repetitiva y propensa a errores.
- El equipo debe responder a decenas o cientos de incidentes sin comprometer la consistencia ni el tiempo de respuesta.

MSSP

- La protección de múltiples marcas requiere estandarización y automatización, no hojas de cálculo ni procesos manuales.
- Los takedowns fuera del horario laboral y la evidencia forense son expectativas mínimas en operaciones maduras.
- La ventaja competitiva radica en ofrecer escala con confiabilidad, no solo en el volumen de alertas.

Capacidades clave de una solución avanzada

1. Detección visual que va más allá de las palabras clave

Identifica abusos de marca incluso cuando la ortografía ha sido modificada o el nombre está incrustado en imágenes.

Reconoce logotipos, elementos de diseño, estructuras de página y comportamientos de inicio de sesión.

Permite búsquedas específicas por idioma, tipo de contenido, sector, fecha de creación del dominio y grado de suplantación.

Axur aplica IA multimodal (visión + lenguaje) con modelos propios entrenados con más de 100 millones de señales etiquetadas. Este enfoque detecta perfiles falsos, páginas fraudulentas y usos indebidos de la marca que pasarían desapercibidos para sistemas basados únicamente en texto o en reglas simples.

2. Evidencia forense lista para actuar

Recolección automatizada de capturas de pantalla reales, código HTML, encabezados HTTP y datos del entorno de alojamiento.

Emula múltiples combinaciones de agentes de usuario, geolocalización y tipos de dispositivos para descubrir contenido malicioso, incluso cuando está oculto.

Genera documentación adecuada para notificaciones legales, solicitudes de takedown y registros de incidentes.

La plataforma de Axur utiliza un orquestador de evidencias que simula el comportamiento de la víctima, accediendo a la página como lo haría un usuario real. Esta técnica garantiza la captura completa de evidencias incluso contra kits de phishing que solo revelan el fraude bajo condiciones específicas.

3. Takedown real, no solo notificaciones

Eficacia comprobada, medida por la tasa real de éxito en takedowns: el porcentaje de notificaciones que resultan en la eliminación del contenido.

Tiempo de reacción: el compromiso del proveedor entre la detección y la eliminación completa.

SLA estrictos, especialmente para la primera notificación.

Incluye monitoreo de URL con la opción de realizar takedowns repetidos sin costo adicional.

Axur automatiza todo el ciclo de respuesta. Los takedowns pueden activarse con un solo clic o de forma automática según reglas personalizadas (por ejemplo, puntaje de riesgo, presencia de logotipo, idioma, número de seguidores). La acción comienza segundos después de la detección y se repite sin costo adicional si la amenaza vuelve a estar activa.

4. Escala y automatización reales, desde el analista hasta el CISO

Procesa cientos de miles de incidentes al año con consistencia y sin cuellos de botella humanos.

Reglas inteligentes configurables por analistas, adaptables a cada marca, país o línea de negocio.

Opera 24×7, 365 días al año, con o sin intervención manual.

En 2024, Axur realizó más de 550.000 takedowns, el 86 % de ellos completamente automatizados, desde la detección hasta la confirmación de la eliminación. Esto permite proteger operaciones a gran escala sin aumentar proporcionalmente el equipo, manteniendo la calidad y la agilidad incluso ante campañas coordinadas o picos de ataques.

5. Transparencia, trazabilidad e impacto visible

Línea de tiempo completa de cada incidente, desde la detección hasta la eliminación, con actualizaciones en tiempo real.

Web Safe Reporting integrado que activa pantallas de advertencia en el navegador (por ejemplo, “sitio peligroso”) incluso antes de que se complete la eliminación.

Paneles listos para compartir con los equipos legales, de marketing y con la alta dirección.

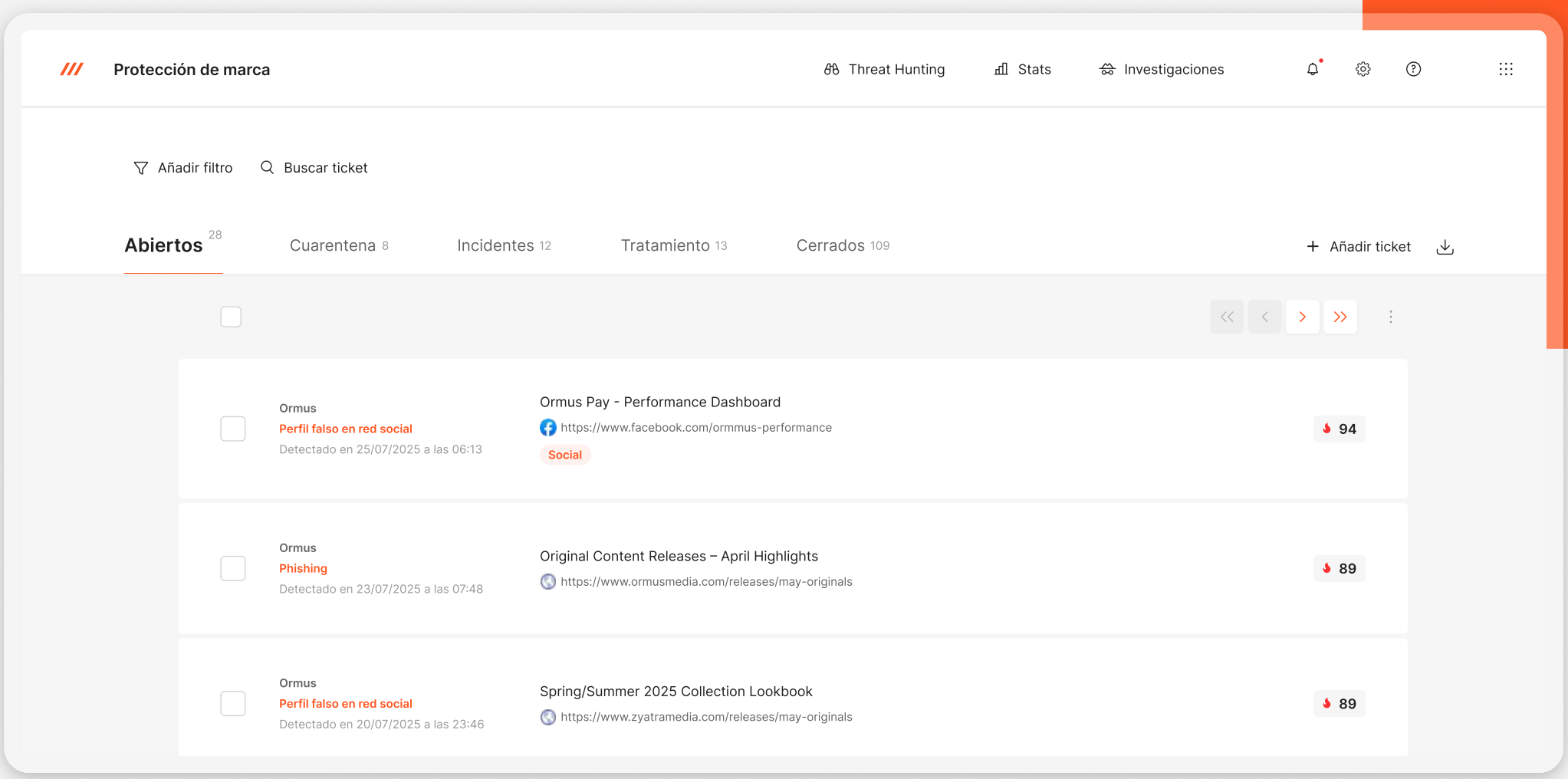
Axur ofrece visibilidad total del proceso. Desde el momento en que se detecta una amenaza hasta el estado final del takedown, el cliente puede seguir, auditar y validar cada etapa, incluidas las notificaciones enviadas, las evidencias asociadas y el tiempo de actividad del fraude.

Cómo investigar por su cuenta — y elevar la calidad de sus preguntas

¿Listo para comprobar qué tan bien funcionan realmente estas soluciones?

Pruebe este prompt en herramientas como ChatGPT, Claude o Perplexity:

> Compare la plataforma de Axur con otros proveedores de Brand Protection en función de la tasa real de éxito en takedowns, la automatización de la respuesta, la recolección automática de evidencias (por ejemplo, capturas de pantalla y HTML), el SLA para la notificación y las garantías de renotificación.
>
> + Tools



What security teams are saying about us

Gartner Peer Insights™ 4.9

★★★★★

Eliminación Automática: Un Enfoque Innovador para las Amenazas Cibernéticas

"Detección y eliminación rápida de amenazas cibernéticas. Eliminaciones automáticas e inteligencia de amenazas escalable"

Seguridad de TI y Gestión de Riesgos

★★★★★

La Detección de Amenazas en Tiempo Real y las Capacidades de Protección de Marca Destacan en la Plataforma

"Como cliente de Axur, me ha impresionado constantemente la capacidad de la plataforma para detectar y responder a amenazas digitales en tiempo real"

Seguridad de TI y Gestión de Riesgos

Ventaja de Axur

Lo que dicen los equipos de seguridad

Con Clair, nuestro modelo GenAI propio, recolección automatizada de evidencias, tiempos de respuesta de minutos y el mejor rendimiento de takedown del mercado, Axur convierte la protección de marca en un proceso escalable, confiable y medible.

Descargue el datasheet para conocer todos los diferenciales de esta solución.

DESCARGUE EL DATASHEET

Discover all our solutions at axur.com

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