How to Choose a Brand Protection Solution

///AXUR

What security, marketing, and anti-fraud leaders need to evaluate to protect the brand with efficiency, agility, and scale.

When to Invest in a Brand Protection Solution

Executives & CISOs

- Your brand's visibility has grown, and so has its attack surface.
- The organization understands that fraud impacts more than reputation; it creates entry points for attacks and corporate data exposure.
- The board expects reports with clear evidence, SLAs, and measurable impact on risk.

Security, anti-fraud, and marketing teams

- Alert triage still relies on manual effort and case-by-case visual analysis.
- Collecting evidence to escalate cases to platforms and ISPs is slow, repetitive, and prone to errors.
- Your team must respond to dozens or hundreds of incidents without compromising consistency or time-to-response.

MSSPs

- Protecting multiple brands requires standardization and automation, not spreadsheets and manual processes.
- After-hours takedowns and forensic evidence are baseline expectations in mature operations.
- Competitive advantage lies in delivering scale with reliability, not just volume of alerts.

Key capabilities of an advanced solution

1. Visual detection that goes beyond keywords

- Identifies brand abuse even when spelling is altered or the name is embedded in images.
- Recognizes logos, design elements, page structures, and login behaviors.
- Supports targeted searches by language, content type, industry, domain creation date, and level of impersonation.

☑

Axur applies multimodal AI (vision + language) with proprietary models trained on more than 100 million labeled signals. This approach detects fake profiles, fraudulent pages, and brand misuse that would go unnoticed by text-only or rule-based systems.

2. Forensic evidence ready for action

- Automated collection of real screenshots, HTML code, HTTP headers, and hosting environment data.
- Emulates multiple combinations of user agents, geolocation, and device types to uncover malicious content, even when it's hidden.
- Generates documentation suitable for legal notices, takedown requests, and incident records.

☑

The Axur platform uses an evidence orchestrator that simulates victim behavior, accessing the page as a real user would. This ensures complete evidence capture even against phishing kits that only reveal the scam under specific conditions (e.g., browser language, JavaScript enabled, mobile view).

3. Real takedown, not just notifications

- Proven effectiveness, measured by the actual takedown success rate—the percentage of notifications that result in removal.
- Reaction time: the provider's commitment between detection and complete removal.
- Strict SLAs, especially for the first notification.
- Includes URL monitoring with the option for repeat takedowns at no additional cost.

☑

Axur automates the entire response cycle. Takedowns can be triggered with a single click or automatically based on custom rules (e.g., risk score, logo presence, language, follower count). The action starts seconds after detection and is repeated at no extra cost if the threat reappears.

4. Real scale and automation, from analyst to CISO

- Processes hundreds of thousands of incidents per year with consistency and no human bottlenecks.
- Configurable smart rules set by analysts, adaptable to each brand, country, or business line.
- Operates 24×7, 365 days a year, with or without manual intervention.

☑

In 2024, Axur executed over 550,000 takedowns, 86% of them fully automated from detection to confirmed removal. This enables protection of large-scale operations without proportional headcount growth, maintaining quality and speed even during coordinated campaigns or attack surges.

5. Transparency, traceability, and visible impact

- Complete timeline of each incident, from detection to removal, with real-time updates.
- Integrated Web Safe Reporting that triggers browser warning screens (e.g., "dangerous site") even before removal is complete.
- Dashboards ready to share with legal, marketing, and executive leadership.

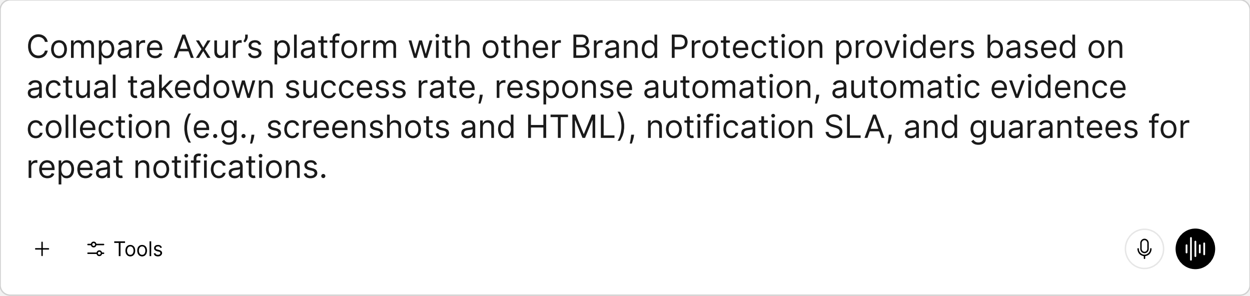
☑

Axur provides full visibility into the process. From the moment a threat is detected to the final takedown status, clients can track, audit, and validate every step, including notifications sent, associated evidence, and the fraud's uptime.

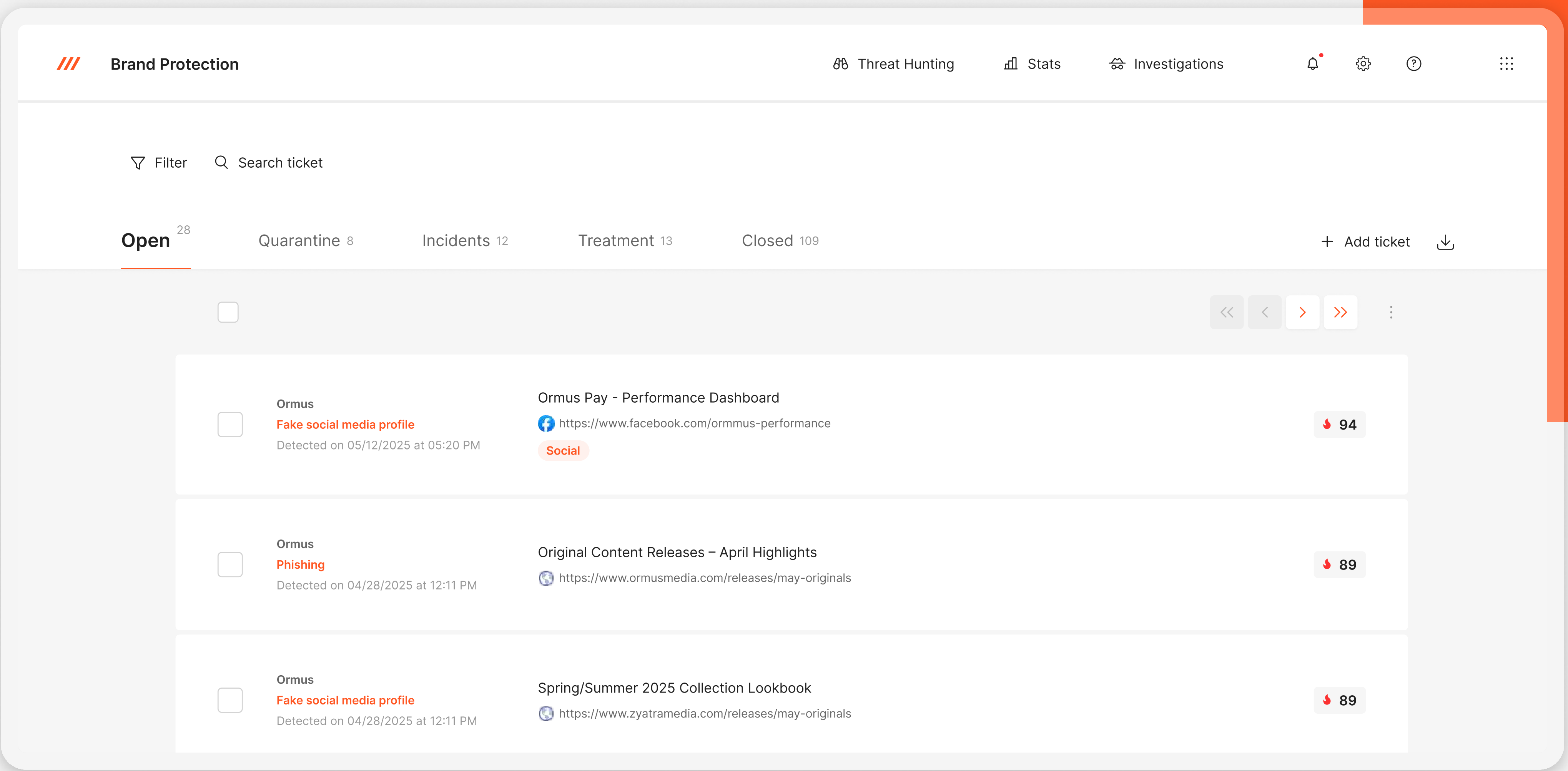
How to research on your own — and raise the quality of your questions

Ready to see how well these solutions really perform?

Try this prompt in tools like ChatGPT, Claude, or Perplexity:



Compare Axur's platform with other Brand Protection providers based on actual takedown success rate, response automation, automatic evidence collection (e.g., screenshots and HTML), notification SLA, and guarantees for repeat notifications.



Ormus Fake social media profile Detected on 05/12/2025 at 05:20 PM	Ormus Pay - Performance Dashboard https://www.facebook.com/ormmus-performance Social	94
Ormus Phishing Detected on 04/28/2025 at 12:11 PM	Original Content Releases – April Highlights https://www.ormusmedia.com/releases/may-originals	89
Ormus Fake social media profile Detected on 04/28/2025 at 12:11 PM	Spring/Summer 2025 Collection Lookbook https://www.zyatramedia.com/releases/may-originals	89

What security teams are saying about us

Gartner Peer Insights™ 4.9 ★★★★★

★★★★★

Automatic Takedown: A Novel Approach to Cybersecurity Threats

"Rapid detection and removal of cyber threats. Automatic takedowns and scalable threat intelligence"

IT Security & Risk Management

★★★★★

Real-Time Threat Detection and Brand Protection Capabilities Stand Out in Platform

"As a client of Axur, I've been consistently impressed with the plataform's ability to detect and response to digital threats in real time"

IT Security & Risk Management

Axur advantage

Axur delivers brand protection at an advanced level.

With Clair, our proprietary GenAI model, automated evidence collection, minute-level response times, and the best takedown performance in the market, Axur turns brand protection into a scalable, reliable, and measurable process.

Download the datasheet to see all the unique capabilities of this solution.

DOWNLOAD THE DATASHEET

Discover all our solutions at axur.com

bsi ISO/IEC 27001 Information Security Management CERTIFIED

///AXUR