AXUR

Digital Fraud

Detect and Neutralize Frauds Impersonating Your Company

Axur's platform offers automated monitoring, enhanced AI-driven inspection, and ultra-precision takedown to neutralize external attack vectors.

Problem

Cybercriminals exploit sophisticated techniques to impersonate your brand across various vectors, whether through phishing campaigns, fake profiles, disguised malware, or domain names closely resembling the original. Security teams are challenged by the increasing prevalence of these persistent threats, draining resources and prolonging response times. These risks undermine customer trust and loyalty, and digital frauds not only erode brand integrity but also escalate operational costs such as chargebacks.

Solution

Axur's platform alleviates operational burdens by identifying and eliminating digital frauds impersonating your brand. Our advanced AI-based inspection examines advanced signals like logo similarities and automatically initiates takedown flows without the need to wait for human action. By drastically reducing mean time to containment (MTTC) and configuring customized automation rule sets, Axur strengthens your defenses, ensuring a resilient, streamlined, and proactive cybersecurity posture.

Phishing

Axur's platform detects a phishing attempt and automatically triggers removal in just 5 minutes — the fastest response time in the market.

With our unique OnePixel technology, coverage increases by up to 52%.

Brand Impersonating

Identify brand impersonation of your company's name, ensuring protection against improper associations that may deceive or confuse your customers.

Fake Social Profiles

Our platform implements predictive models to quickly identify unauthorized use of your brand name and visual assets, such as logos and mascots, on major social networks. Automatic takedowns with notifications in 3 minutes for:

Malware

Monitor the spread of Trojan-Banker malware and protect your consumers from data theft for financial transactions and fraudulent purchases. Data may contain the C&C (Command & Control) server details of the infected machine.

Typosquatting

Inspect new domain registrations related to your brand and keep them under surveillance. You will be the first to know if these domains host phishing campaigns or register suspicious activities.

Brand Use in Paid Search

Prevent competitors and fraudsters from exploiting your brand in top paid search engine ads, such as Google.

Fake Mobile Apps

Get complete visibility of official stores and app websites to track fake apps impersonating your brand or posing any risk to your consumers.

The world's best Takedown. And we have the evidence to back it up.

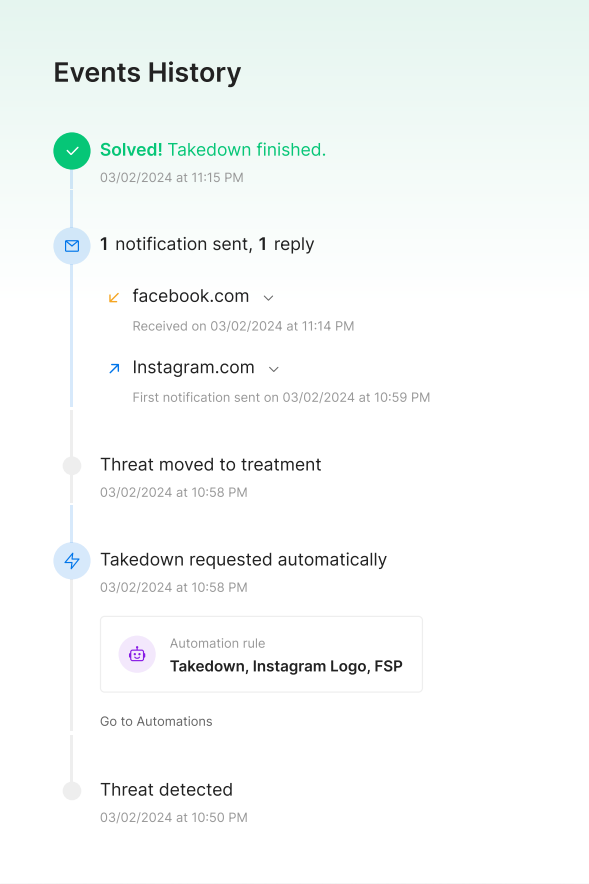
5 minutes
For the first notification in phishing cases and up to 30 minutes for all other incidents.

98.9% success rate
Guaranteed removal if the content reappears within 15 days.

9 hours of uptime
Average time for content removal with Axur's takedowns.

Trigger Takedowns with Automated Flows

Every second counts to mitigate a threat. You don't need to wait for human intervention when you need action the most. In 2023, 86% of Axur detections were managed without any human intervention.



AI-driven Inspection and Removal

Axur's platform deeply analyzes signals to categorize and prioritize threats. By empowering takedown automation, actions are fast and accurate, minimizing exposure and strengthening cyber resilience.

Key inspection attributes:

- **89** Risk score
- Brand logo similarity
- Content language
- Brand name disambiguation
- VIP facial recognition
- Presence of password fields
- and several more!

Keep Watch with Re-up

Axur's takedown is not limited to initial remediation but rather a commitment to ensuring threats against your business remain neutralized. If any removed content reappears within a 15-day period, it will be immediately detected and treated as a new incident — at no additional cost.

Maximize Defense with Websafe Reporting

Axur collaborates with leading cybersecurity entities to reduce the reach of malicious content, reducing exposure time to fraud. We are integrated with over 30 leading cybersecurity organizations.

Effortless Evidence Compilation

Allow automation to streamline evidence collection, from HTML copies and screenshots to domain data, aiding decision-making.

See all of this in action.

Discover all our solutions at axur.com

Get a custom demo

///AXUR