

# Take threats down with Agentic AI precision: fast, end-to-end, and at scale.

Harmful content across platforms puts brand, revenue, and data at risk. Axur's agentic takedowns detect, classify, and eliminate threats autonomously — fast, precise, nonstop.

## AI as the engine, not as a feature.

Our proprietary AI model detects brand abuse in visual assets — even when there are no keywords, logos, or direct references to your company.

Clair understands visual context, flags infringing content, and feeds those decisions into a fully agentic takedown workflow.

Impersonated brands AI  
Citizens Bank, high impersonation level AI

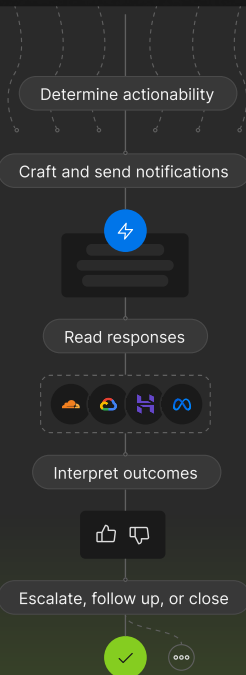
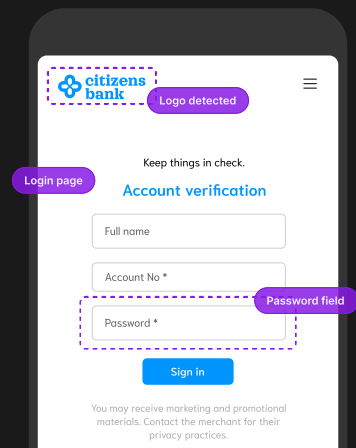
Company logos AI  
Citizens Bank

Content type AI  
Login Page AI

Languages AI  
English, Japanese

Credential request AI  
Yes AI

Password request AI  
Yes AI



## From detection to decision-making.

Next, Axur's agentic takedowns kick in to:

- Determine if a threat is actionable — filtering out false positives, legit content, and fraud that falls outside enforcement scope.
- Craft and send notifications,
- Read responses from hosts and platforms,
- Interpret outcomes, and
- Act accordingly: escalate, follow up, or close.

All with minimal human input.  
This is what the next generation  
of takedowns looks like.

# Yes, the **best** takedown. Here's the evidence.

## ✦ One-click or Zero-Touch Takedowns

No need for screenshots, explanations, or proof of ownership. Just click a button — or set up AI workflows to trigger takedowns automatically.

## ✦ 98,9% success

We don't just notify, we eliminate. Scale your response with a platform proven by over 2 million takedowns.

## ✦ Web Safe Reporting

Automatic notifications to 15+ top-tier entities that help trigger the well-known red screen alert on malicious pages, even before the URL's content is fully removed.

## ✦ 15-day stay down guarantee

We monitor the URL taken down for 15 days straight. If it resurfaces, we take it down again— and at no extra cost.

## ✦ Notification in <5min

The faster the provider gets the takedown request, the most you reduce the time window of the threat. That's why we have the best SLAs for the first notification.

Phishing

Typosquatting

Brand impersonating

Counterfeit

VIPs impersonating

If your current vendor isn't covering this, maybe it's time to upgrade your protection.

## ✦ 9h median uptime

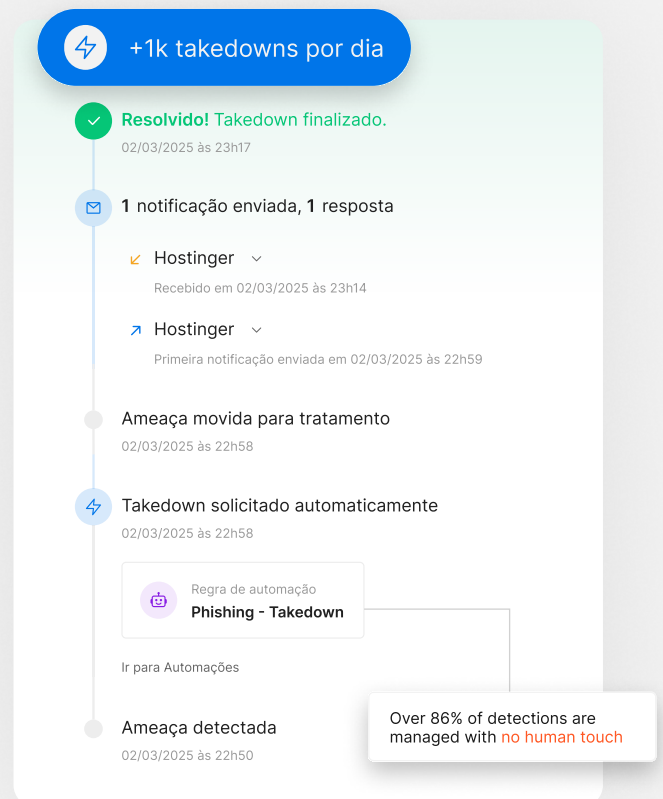
The main reason for the low uptime and high success rate is the takedown automation.

## ✦ Follow up the whole process

Track your takedown request from start to finish—notifications, progress updates, and average removal time are all at your fingertips.

## ✦ We charge only for successful takedowns

We know, it should be the standard. But it is not: other vendors charge for notifications, no matter the outcome.



## Experience the next generation of takedowns

Request a demo

Discover all our solutions at [axur.com](https://axur.com)

Gartner  
Peer Insights.. 4.8  
★★★★★



///AXUR