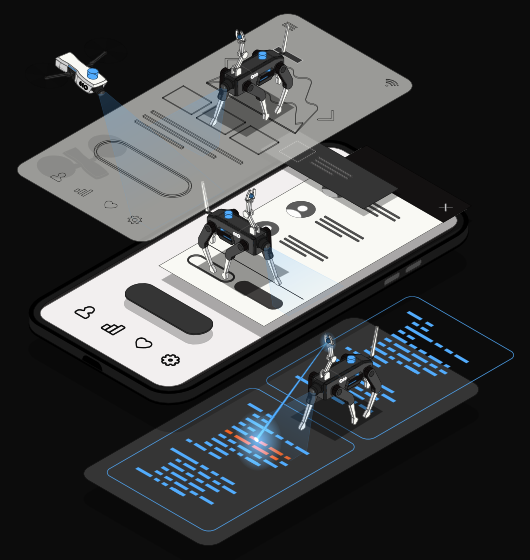
outtake Product Protection

Your product is being sold.
You just don't know where.



Free trials, cloned access, resold storefronts. A parallel market formed around your product. Outtake finds every listing, maps the operation behind it, and takes the network down at the campaign level.

300%
surge in AI bot activity this year

703%
growth in phishing attacks YoY

37%
of internet traffic is bad bots

67%
of leaders say AI expanded attack surface

THE PROBLEM

You find out the same way your customers do. Too late.

01 VISIBILITY

No systematic view into resale.

Free-tier abuse, cloned storefronts, fraudulent reseller listings. Most teams discover them through a support ticket. By then dozens of storefronts are live, brand damage has accumulated, and the revenue lost is unmeasured.

02 REACH

One takedown. The network keeps generating.

A specific URL gets reported. The team moves on. The operators behind that listing are running coordinated activity across multiple platforms, with new infrastructure already staged. Cutting one branch never killed a tree.

03 EVASION

Detection that stops at the keyword.

Listings use your branding through visual logos, paraphrased copy, and pricing patterns instead of clean text matches. Keyword tools cannot read what is happening in the image, the video, or the structured layout.

THE DIGITAL TRUST JOURNEY

From listing to network takedown in hours, not weeks.

STEP 01 →

See Every Listing

Continuous detection across domains, social, marketplaces, and reseller sites.

STEP 02 →

Read the Brand

Visual logos, copy variation, pricing patterns. Multi-modal recognition.

STEP 03 →

Map the Network

Connected domains, shared hosting, linked accounts, operator clusters.

STEP 04 →

Take Down at Scale

Registrars, social, app stores, ad networks. Simultaneous, automated.

STEP 05 →

Quantify the Loss

Revenue lost to abuse becomes visible, measurable, and recoverable.

TRUSTED BY THE BEST

ANTHROP\C · NVIDIA · DUNKIN' DONUTS · OpenAI · Pershing Square Holdings · APPLOVIN

THE PLATFORM

GLOBAL DIGITAL TRUST FOOTPRINT

DARK WEB · DOMAINS · ADS

DIGITAL RESERVOIR™

The more it sees, the more it knows.

THREAT GRAPHING

One signal. Their whole operation exposed.

REMEDIATION

Brand
Impersonation · Fraud

Executive
VIPs · PII · Extortion

Event
Real-time · Threats · VIPs

Product
SaaS abuse · Token fraud

Threats removed in hours, not weeks

SOLUTIONS

Built for every team protecting your product.

Free-Tier & Resale Abuse

Stop the parallel market in your product.

— **Unauthorized Storefronts**
Listings selling access outside authorized channels.

— **Bulk Account Harvesting**
Operators creating accounts to monetize free-tier.

Cloned Apps & Sites

Stop the impersonation that targets your customers.

— **Cloned App Listings**
Mobile stores, sideload distribution, lookalike branding.

— **Spoofed Product Pages**
Sites built to harvest credentials and payment data.

AI Misuse & Output Resale

Stop the resale of access to your AI capacity.

— **API Capacity Reselling**
Harvested keys and capacity sold on grey markets.

— **Generated Output Abuse**
Voice, content, and image output resold under false branding.

PROVEN OUTCOMES

Results that protect revenue and brand integrity.

99%
Takedown confirmation rate

14hrs
Average internet-wide takedown time

100%
Network eradication, not single listings

20M+
Cyberattacks scanned in 2025

Ready to stop unauthorized resale at the network level?

outtake.ai hello@outtake.ai

REQUEST A DEMO →