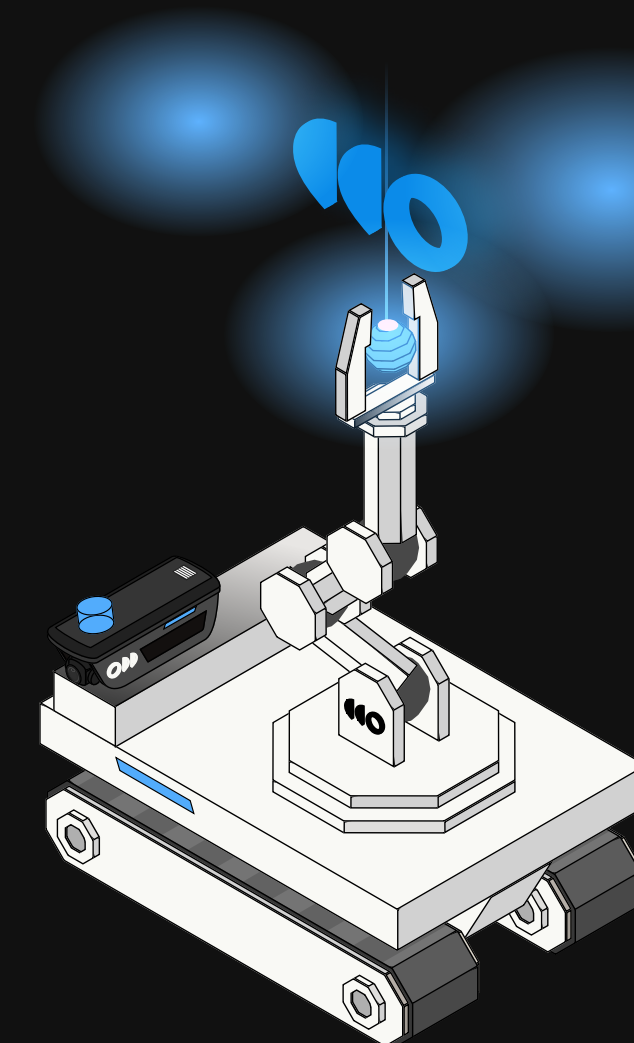


# Detect Every Impersonation. Dismantle the Campaign Behind It.



Your brand is being used against you across domains, social, ads, and apps. Outtake finds the operation, maps the network, and eliminates it.

**51%**

of global internet traffic is now automated bots

**703%**

increase in phishing attacks YoY

**300%**

surge in AI bot activity this year

**67%**

of security leaders say AI has expanded attack surface

## THE PROBLEM

### Your brand is being weaponized. Most teams can't keep up.

**01**

#### Coverage Gaps in Detection

Impersonation campaigns use logos in images, brand identity in video, and cloned experiences with no keywords. Keyword-based tools are blind to them, threats run until a customer reports harm.

**02**

#### Point Solutions Stop at the Node

Taking down one domain without understanding what is behind it is brand whack-a-mole. Adversarial campaigns are coordinated systems. Remove one node, the rest keeps running.

**03**

#### Manual Workflows Cannot Scale

Attackers spin up infrastructure faster than any manual process can clear it. Alert queues grow, high-severity threats sit in noise, and the human bottleneck never goes away.

## THE PLATFORM

### See everything. Dismantle everything.

Agentic OSINT



#### Multi-Modal Detection

Monitors domains, social, app stores, and ads simultaneously, analyzing text, images, video, and audio. No impersonation hides behind a format.

Threat Graph



#### Full Network Mapping

Autonomous agents trace shared hosting, registration patterns, and analytics IDs. One signal becomes a complete map of the full adversarial operation.

Agentic DRP

#### Automated Takedowns at Scale

Takedowns execute automatically across registrars, social platforms, app stores, and ad networks. No manual coordination. No human bottleneck.

# Built for every team protecting your brand.

## Brand Impersonation Takedowns

- Lookalike domains diverting your customers
- Fake social accounts across all platforms
- Fraudulent ads using your brand identity
- Cloned app listings in mobile stores

## Fake Storefront Detection

- Fake storefronts impersonating your brand
- Counterfeit listings on major platforms
- Fake employee profiles on LinkedIn
- Unauthorized brand use in paid advertising

## Campaign Intelligence

- Pre-staged infrastructure before activation
- Cross-platform signal correlation
- Operator attribution with high confidence
- Threat Graph enrichment over time

## HOW IT WORKS

# From exposure to eradication in hours, not weeks.



### See Abuse

Agentic OSINT surfaces all threats across your digital footprint



### Understand Risk

Threat correlation ranks what matters most to your business



### Stop Attacks

Agentic DRP auto-dismantles full adversarial networks



### Prove ROI

Analytics quantify impact and justify investment



### Predict Next

Unified intelligence keeps you ahead of the next wave

## PROVEN OUTCOMES

# Results the world's top brands rely on.

**99%**

Takedown confirmation rate

**14hrs**

Average internet-wide takedown time

**100%**

Network eradication, not just single links

**20M+**

Potential cyberattacks scanned in 2025

## TRUSTED BY



Ready to protect your brand at the speed of AI?

[outtake.ai](https://outtake.ai)

[hello@outtake.ai](mailto:hello@outtake.ai)

REQUEST A DEMO →

