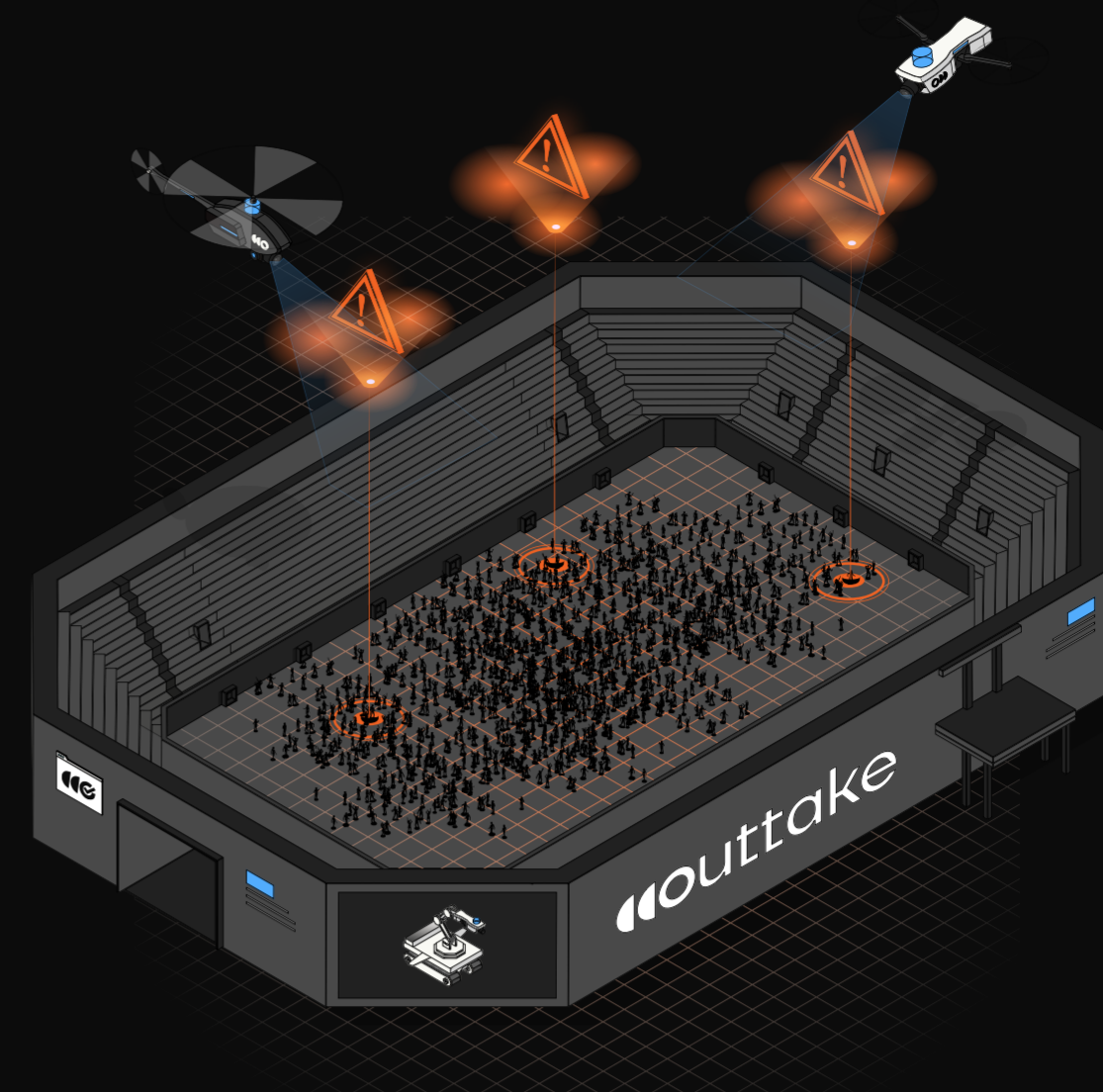


# See it. Before it shows up.

Every location is a window of exposure. The schedule is public. The venue is known. Adversaries are organizing online before your team finishes the briefing. Outtake closes the gap.



**703%**

increase in phishing attacks YoY

**9 hr**

manual detection lag

**15 min**

Outtake detection cadence

## THE PROBLEM

### Manual monitoring was built for a slower internet.

#### 01 SPEED

**The threat moves faster than the monitor.**

Activist groups coordinate on Telegram and WhatsApp before your pre-event briefing is finished. Coded language. Cross-platform fragmentation. Manual review catches what is loud and recent. It misses the rest.

#### 02 SCOPE

**Always-on tools, time-bound risk.**

Standard tools are not scoped to a venue, route, or schedule. They generate noise outside the event context, do not spin up cleanly, and do not archive when it ends. Teams improvise. Coverage suffers.

#### 03 GEO

**Physical exposure without digital visibility.**

A protest on a driving route. An unannounced gathering near the venue. Without geolocation parsing tied to the event footprint, all of it stays invisible until it is physically present.

## THE DIGITAL TRUST JOURNEY

### From event configured to threat neutralized, in real time.

#### STEP 01 →

##### Scope the Window

Configure venue, route, executives, and schedule. Monitoring deploys on demand.

#### STEP 02 →

##### Listen Everywhere

Social, fringe forums, dark web. Multi-modal. Across every relevant language.

#### STEP 03 →

##### Map to Geography

Location signals parsed and mapped to landmarks, intersections, and routes.

#### STEP 04 →

##### Alert in Minutes

Real-time delivery to Slack, Teams, email. On-site and ops center get it together.

#### STEP 05 →

##### Archive Cleanly

When the window closes, monitoring archives. No persistent overhead.

## TRUSTED BY THE BEST

ANTHROPIC



DUNKIN' DONUTS

OpenAI



APPLOVIN

## THE DIGITAL TRUST PLATFORM

### GLOBAL SIGNAL NETWORK



### DIGITAL TRUST 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

#### Location

Real-time Threats ·  
Crowd signals

#### Product

SaaS abuse · Token  
fraud

Threats removed in hours, not weeks

## SOLUTIONS

Built for every team running high-stakes events.

### Conferences & Appearances

Multi-day coverage scoped to venue and schedule.

#### — Activist & Protest Detection

Coordinated activity, coded language, cross-platform.

#### — Venue Proximity Monitoring

Surrounding landmarks, routes, access points.

### Executive Travel

Coverage that follows the motorcade.

#### — Route-Level Intelligence

Driving routes, stopovers, hotel proximity.

#### — Cross-Language Detection

Local platforms, local languages, local context.

### Earnings & Shareholder Meetings

Scoped windows around financial milestones.

#### — Coordinated Disruption

Activist investor activity, planned protest infrastructure.

#### — Influence Operations

Narrative manipulation timed to the event.

## PROVEN OUTCOMES

Results the world's most exposed events depend on.

# 15min

Detection cadence in event window

# 14hrs

Average internet-wide takedown time

# 99%

Takedown confirmation rate

# 20M+

Cyberattacks scanned in 2025

Ready to see the threat before it arrives?

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

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

REQUEST A DEMO →

