Doppel

Weaponize customer feedback. **Dismantle attacker infrastructure.**

Transform public reports–abuse inboxes, tickets, or complaints–into a direct intelligence pipeline. Instead of sitting idle, those signals activate real-time disruption across Doppel Vision.

Doppel Vision: **Brand AbuseBox**

Capture user reported scams and validate automatically.

Scams are often spotted by people before they're flagged by platforms. Brand ThreatBox bridges that gap—turning early human signals into instant, automated disruption. Instead of letting manual queues slow things down, Doppel drives rapid enforcement. While traditional email security and DRP tools stop at detection, Brand ThreatBox goes further: it dismantles. The result? Threats aren't just flagged—they're neutralized across everv channel thev touch.

Signal Ingestion

Public abuse inboxes and reporting tools feed into Doppel Vision.

AI Parsing + IOC Extraction

Links, domains, phone numbers, and threat artifacts are extracted and analyzed.

Cross-Channel Correlation

Doppel Vision links each report to broader attacker infrastructure.

Automated Enforcement

Validated threats are takedown-ready in seconds.

Shared Threat Grid Contribution

Every takedown makes future detection faster for everyone.

Trusted by

USAA · UNITED · OpenAI · ConocoPhillips · ROBLOX

Brand AbuseBox Powers the Doppel Vision Ecosystem

Brand AbuseBox is not a siloed tool. It amplifies the entire platform.

- **Powers brand impersonation takedowns**
- **Feeds intelligence to Doppel Vision**
- **Strengthens Doppel's Threat Grid for all customers**
- **Contributes to the dismantling of entire attacker networks**

Unify threat insights across attack surfaces into a single Threat Grid.

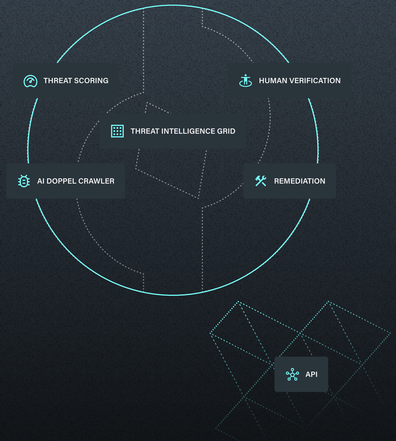
Always-On Protection - Doppel Vision's AI crawler continuously scans domains, social media, and the dark web to identify threats in real time.

Unified Threat Intelligence - A single source for cross channel intelligence that adapts to evolving tactics, delivering dynamic real-time protection.

Advanced Threat Mapping - AI-driven intelligence uncovers hidden attacker infrastructure, ensuring proactive defense.

Rapid Disruption - dismantle attacker operations, preventing future threats.

AI + Human Expertise - Hybrid defense combines machine learning with expert validation, ensuring unmatched accuracy and response.



Book your demo at www.doppel.com/request-a-demo

The first cybersecurity platform purpose-built to defeat social engineering by dismantling the infrastructure behind impersonation attacks—at machine speed.