



Bolster AI Deepfake Detection

Bolster AI brings deepfake detection into investigations. Verify suspicious media, see the campaign behind it, and reach an evidence-backed decision, inside your existing workflows.

Why Deepfake Impersonation Matters

AI-Generated Impersonation Is Moving From Novelty to Operational Risk

Deepfake impersonation rarely shows up as a single suspicious clip. It spans coordinated campaigns: synthetic media distributed through fake profiles, phishing pages, and spoofed channels. In practice, that looks like:

-  Fake executive videos used in fraud, extortion, and social engineering
-  Manipulated images impersonating brands, products, and employees
-  Fake executive profiles and synthetic accounts across social media
-  Synthetic media embedded in phishing and scam campaigns
-  Suspicious media scattered across channels that analysts can't quickly verify
-  Verification handled in separate tools, disconnected from the investigation itself

The Impact



\$1.65B in deepfake-enabled fraud losses reported in 2025 alone ¹



\$25.6M deepfake fraud — finance employee deceived by an AI "CFO" ²



41% of businesses faced executive deepfake incidents in 2025 ³

Key Benefits

Faster Investigations

Reduce the time required to analyze suspicious media and make operational decisions.

Better Investigation Context

Understand whether media is authentic, manipulated, or AI-generated before escalating or enforcing.

Stronger Enforcement Actions

Support takedowns and escalation workflows with investigative evidence and media validation.

One Investigation Workflow

Investigate impersonation campaigns and suspicious media in a single platform.

Full Campaign Visibility

Connect suspicious media to the domains, accounts, ads, and infrastructure behind the campaign.

What Makes Bolster AI Different

Beyond Deepfake Detection

Most vendors flag manipulated media. Bolster AI connects it to the broader impersonation campaign.

Embedded in the Investigation Workflow

Deepfake analysis happens directly inside impersonation investigations — no separate tools.

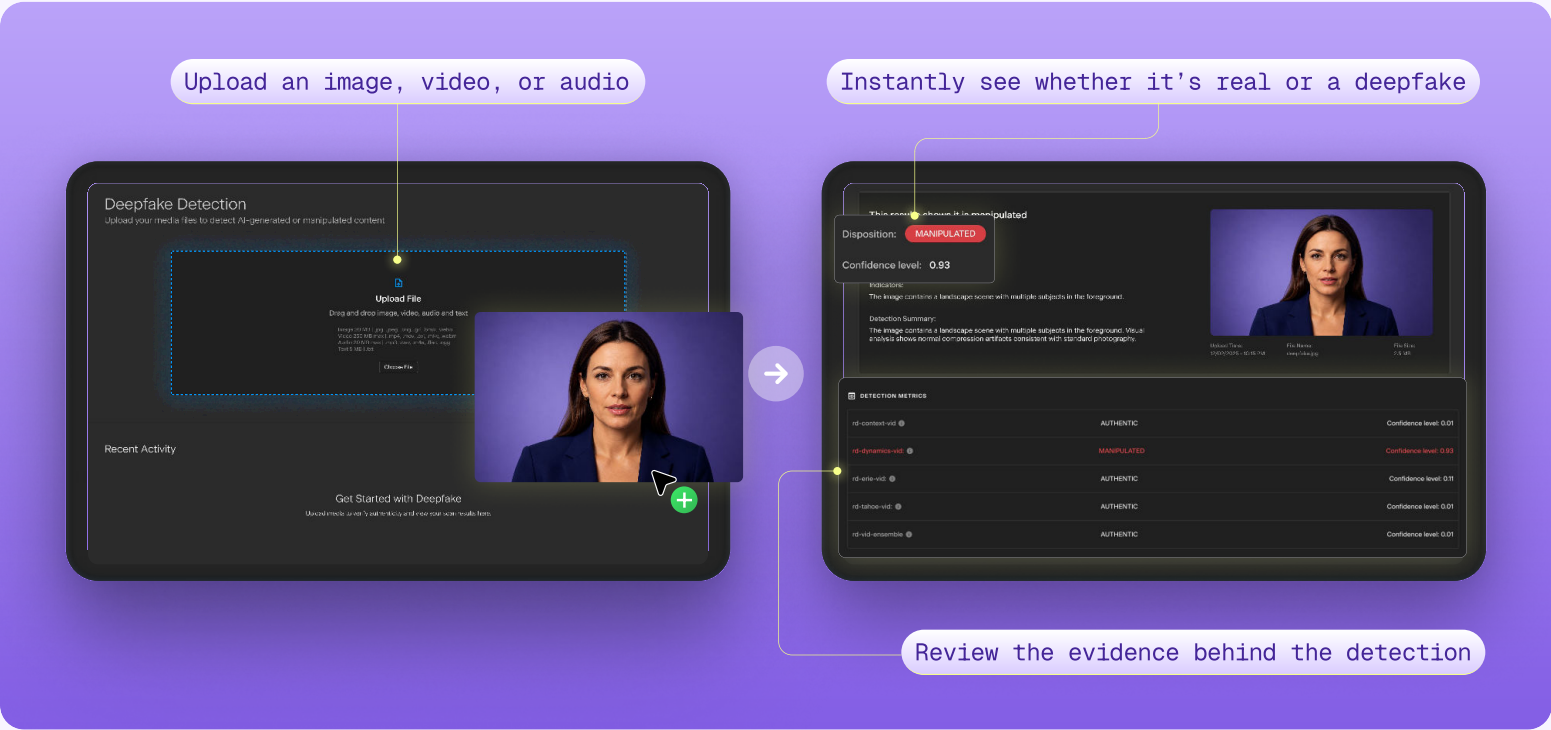
Cross-Channel Infrastructure Visibility

Connect suspicious media to domains, social accounts, marketplaces, email, apps, and the wider attack surface.

Built for Operational Teams

Designed for security, fraud, trust, and legal teams driving investigation, enforcement, and takedown.

Deepfake Detection Workflow



STEP 1

Surface

Upload suspicious files or check ones Bolster AI has already surfaced from web and social in one workflow.

STEP 2

Validate

Quickly check if media is AI-generated — inside the impersonation investigation your team is running.

STEP 3

Connect

Deepfakes rarely travel alone. Bolster AI traces phishing domains, fake accounts, and spoofed channels.

STEP 4

Take Down

Turn findings into action. Evidence-backed takedowns end investigations in disruption, not alerts.

What Changes for Your Analysts

70 minutes⁴
average investigation time per alert

600% ROI
delivered to customers

98.6% Manual Reduction
manual workload reduction

Other vendors stop at the verdict. Bolster AI investigates and disrupts the campaign behind it.

See how Deepfake Detection lives inside impersonation investigations — turning suspicious media into evidence.

Request a Demo

Citation

¹ Deepfake Fraud Losses," Surfshark research (Resemble AI Deepfake Incident Database), 2025

² Cybercrime: Lessons learned from a \$25m deepfake attack," World Economic Forum, 2025

³ Ponemon Institute, cited in BlackCloak, "The Evolving Executive Threat: Understanding and Countering Deepfakes in 2025

⁴ Deepfake-Eval-2024: A Multi-Modal In-the-Wild Benchmark," Chandra et al. (arXiv:2503.02857), 2025