BOLSTER AI

See what your attack looks like. Request a Demo →

Platform Overview

AI Changed the Attack.
Your Defense Has to Change With It.

Attackers are using AI, automation, and the same digital channels companies use to reach customers to build faster, more convincing attacks at scale.

A fraudulent ad leads to a lookalike website. A fake social account reinforces the deception. Domains, marketplaces, apps, messaging, and manipulated content can become pieces of the same operation.

But most security teams are still forced to investigate these threats one at a time.

Bolster AI helps security teams discover threats across the external attack surface, understand how they're connected, and remove malicious infrastructure before more customers are impacted.



See more of the attack.
Stop more of it.

Fight the Attack, Not Just the Alert.

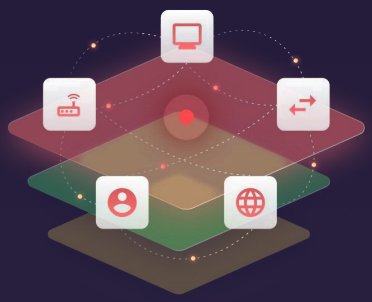
Bolster AI brings discovery, connected intelligence, and takedown together in one platform—helping security teams move beyond isolated threats to understand and disrupt more of the attack.



DISCOVER

Find threats wherever they surface.

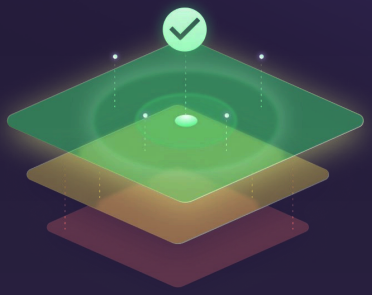
Continuously discover malicious and fraudulent activity targeting your customers across the external attack surface.



REMOVE

Turn intelligence into action.

Automated takedowns and 24/7 security expertise help disrupt malicious infrastructure without adding another queue of alerts for your team.



UNDERSTAND

Connect the pieces.

Reveal relationships between threats and infrastructure so analysts can investigate with greater context and uncover more of the attack.

BOLSTER AI

See what your attack looks like. Request a Demo →

One Platform. Wherever the Attack Surfaces.

Websites & Domains
Find and remove malicious sites and lookalike domains impersonating your brand.

Social Media
Stop fake profiles and accounts attackers use to impersonate your brand and reach customers.

Fraudulent Ads
Detect and remove malicious ads using your brand to acquire victims.

Marketplaces
Find and remove fraudulent listings and storefronts deceiving customers in your name.

App Stores
Detect and remove fake and malicious apps impersonating your brand.

Dark Web
Surface brand abuse, exposed information, and threat activity that may signal or support attacks.

Deepfakes
Detect manipulated media being used to make impersonation more convincing.

Abuse Mailbox
Turn customer-reported threats into actionable intelligence and faster remediation.

The Artifact Isn't the Attack. The Campaign Is the Attack.

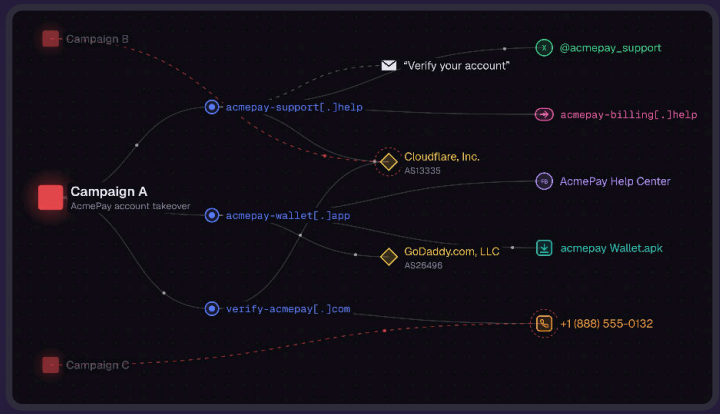
A fake site, fraudulent ad, or spoofed account may only be one piece of a broader operation. **Bolster AI** helps analysts understand what a threat is connected to—so they can investigate beyond the artifact they started with.



Signals

See what's forming earlier.

Surface suspicious infrastructure and activity earlier so your team can investigate emerging threats before they reach greater scale.



Threat Graph

See the campaign behind the threat.

Threat Graph connects related domains websites, ads, social profiles, and other infrastructure to reveal relationships that may otherwise remain hidden.

Finding More Shouldn't Mean More Work.

98%	<10h	20x
Takedown resolved within 72 hours*	Median takedown time*	Lower cost per takedown*

Trusted by the Brands Attackers Want to Be.

Bolster AI helps security teams see the threats targeting their customers, understand the broader attack, and take action against it.

Booking.com · Uber · McAfee · Canva · docusign · AIA