Signals

See What's Connected. See What's Forming.

Individual threats rarely tell the whole story.

Bolster AI Signals turns activity across your external attack surface into connected intelligence—helping security teams understand relationships between threats, uncover additional infrastructure, and investigate emerging activity earlier.

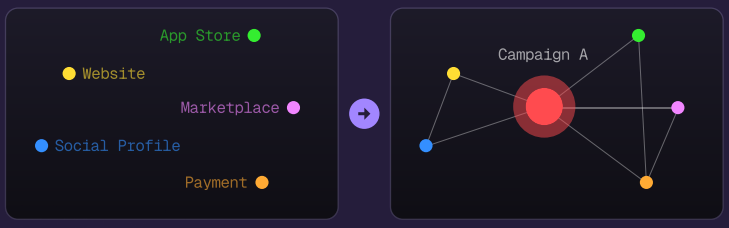


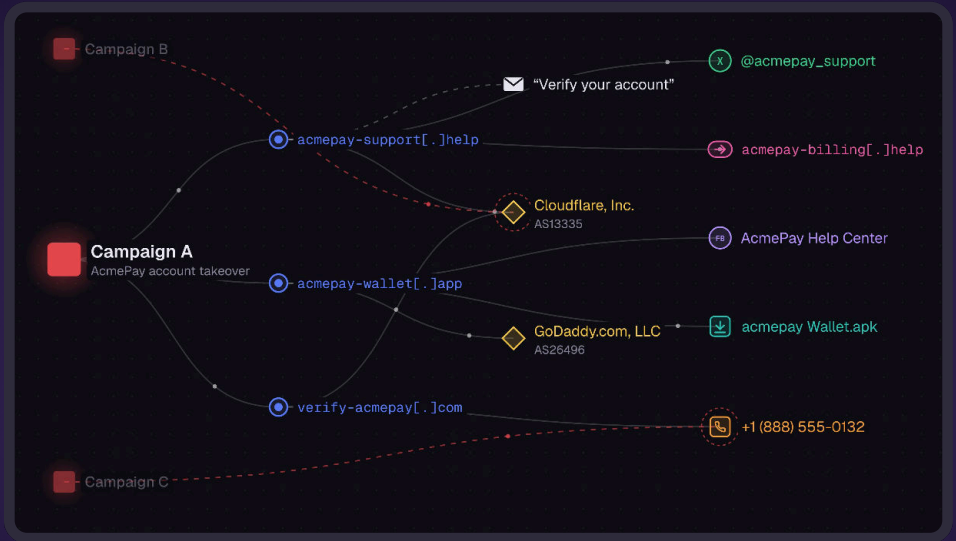
The Artifact Isn't the Attack. The Campaign Is the Attack.

You found the fake website. What else is connected to it?

A fraudulent website, lookalike domain, malicious ad, or spoofed social account may be only one piece of a broader operation. Looking at each threat in isolation can leave the infrastructure and activity around it hidden.

Bolster AI Signals helps analysts connect the pieces and investigate beyond the artifact that first caught their attention.





Threat Graph

See What's Connected. See What's Forming.

Individual threats rarely tell the whole story.

Bolster AI Signals turns activity across your external attack surface into connected intelligence—helping security teams understand relationships between threats, uncover additional infrastructure, and investigate emerging activity earlier.

Connected Intelligence for a Changing Attack Surface

Signals

What should I investigate earlier?

Surface suspicious activity and infrastructure that deserves investigation, helping analysts identify emerging threats earlier.

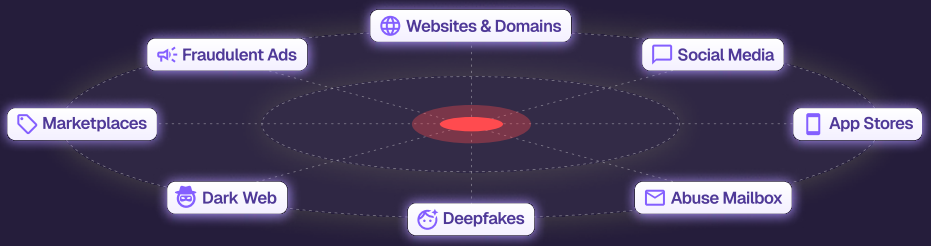
Threat Graph

What is this connected to?

Explore relationships between threats and infrastructure to uncover additional activity and understand the broader campaign.

Connect Intelligence Across the Attack Surface.

Attackers don't limit themselves to one channel. Signals brings intelligence from across the Bolster AI platform into a more connected view of the threats targeting your customers.



Go From Question to Context Faster.

Signals gives analysts faster way to investigate threat activity without manipulate piecing together information across disconnected tools and data sources.

Ask Bolster

Query threat intelligence in plain language to quickly get the context you need.

Threat Hunting

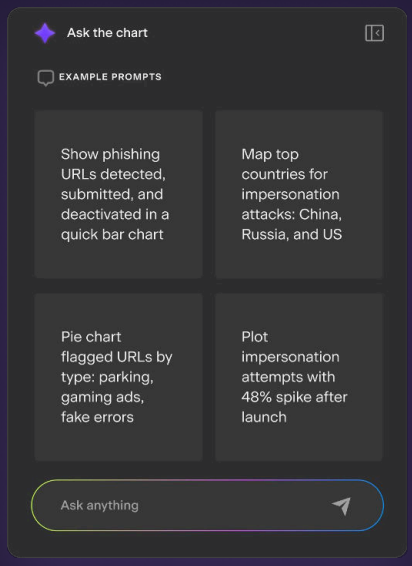
Explore suspicious infrastructure and relationships to investigate activity beyond the initial finding.

Peer Benchmarking

Compare your threat landscape with similar organizations to understand where your exposure stands.

Executive Visibility

Turn threat activity into clearer context for security leaders and stakeholders.



Don't Just Understand the Attack. Disrupt It.

Connected intelligence matters when it leads to action.

Because Signals is part of the Bolster AI platform, security teams can move from discovery and investigation to takedown and remediation without turning intelligence into another alert queue.

- Discover the threat.
- Understand the connections.
- Take action against the malicious infrastructure behind it.

98%
Takedown resolved within 72 hours*

<10h
Median takedown time*

20x
Lower cost per takedown*

Built for Security Teams That Need Answers, Not More Alerts.

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

One Threat Can Tell You a Lot More Than You Think.

See how Bolster AI Signals helps your team uncover connections, investigate emerging activity, and disrupt more of the attacks targeting your customers.

Request a Demo →