Cut Through Dark Web Noise. Act on What Matters.

BOLSTER AI

Bolster AI Dark Web Monitoring & Takedowns

Executive exposure, stolen credentials, and leaked data surface on the dark web long before they become incidents. Bolster AI gives security teams visibility into what's tied to your business, so remediation happens before attackers act on it.

Why Dark Web Exposure Matters

Dark Web Exposure Is Hidden in the Noise

Executive exposure, stolen credentials, and leaked customer data are scattered across thousands of sources hidden behind anonymity tools and encrypted channels: difficult to see, harder to act on. In practice, this shows up as:

- Executive and employee credentials traded on illicit forums and paste sites
- Credit card data with full BIN details brokered across carding marketplaces
- Phishing kits and source code targeting your brand listed for sale
- Threat actor coordination across Telegram, IRC, and I2P channels

The Impact

Over $36 billion in stolen credentials are circulating on the dark web [1]

88% of basic web app attacks involve stolen credentials [2]

$4.88m average cost of a data breach in 2024 [3]

How it Works

1 Continuous Source Coverage

Bolster AI continuously monitors hard-to-track dark web sources and validates findings to reduce noise and surface actionable exposure faster.

2 Built Around Your Assets

Findings map directly to your domains, executives, employee identities, payment data, and custom assets by what's new, total exposure, and top leak sources.

3 Prioritized Remediation

Prioritized exposure based on likely business impact

Citation

[1] ReliaQuest, 2024 Annual Cyber-Threat Report

[2] Verizon Data Breach Investigations Report, 2024

[3] IBM Cost of a Data Breach Report, 2024

Key Benefits

Faster Remediation
Move from raw chatter to actionable findings in minutes, with one-click drilldowns to affected entities.

Reduced Investigation Burden
Eliminate manual source research and log parsing. Bolster AI organizes the noise so your team works only what matters.

Executive & Customer Protection
Surface compromised executive, employee, and customer credentials before they're weaponized in takeover or impersonation attacks.

Predicted Risk Visibility
Forward-looking risk levels per asset help prioritize what to act on first, not just what landed last.

No Operational Lift
Bolster AI's analysts and AI handle source curation, validation, and triage. No new hires, tooling, or setup.

What Makes Bolster AI Different

Built Around Your Organization, Not Raw Data
Findings map to your domains, executives, BINs, and assets. Compare domains or scope to a single executive without leaving the dashboard.

Trained In-House LLMs
Sources are curated and prioritized by LLMs purpose-built for dark web analysis. Edge cases and complex threats stay with human analysts.

Connected to the Full Attack Surface
Pairs with Bolster AI's wider lens across phishing, brand impersonation, and marketplace fraud, feeding findings into broader threat context.

Built for Speed
Remediation recommendations and predicted risk are delivered the moment exposure is identified, not after a queue review.

Manual Process vs. Bolster AI

The difference becomes clear when compared to manual approaches:

Process	Manual Approach	With Bolster AI
Source Coverage	Limited public forums and manual scraping	ToR, I2P, IRC, Telegram, paste sites, breach dumps
Time to Identify Exposure	Days to weeks of log parsing	Minutes to identify exposed assets
Data Organization	Raw, unstructured chatter	Findings mapped to your domains, execs, BINs
Future Risk Visibility	Reactive review only	Prioritized exposure based on likely business impact
Remediation Guidance	Ad-hoc, built incident by incident	Recommended next steps for faster remediation

Proven Results

99.999%
detection accuracy rate

Minutes
from exposure detected to actionable finding

Major Dark Web Sources
ToR, I2P, IRC, Telegram, paste sites

Other vendors flood you with chatter. Bolster AI tells you what matters.
See how Bolster AI Dark Web Monitoring surfaces compromised credentials, leaked data, and threat activity tied directly to your assets.

Request a Demo