Typosquatting

Sheer volume of typosquat domains is daunting

Typosquatting has been plaquing online businesses for years, but the growing number of top-level domains has expanded the attack surface, drastically outpacing traditional defense mechanisms and techniques. It's a problem virtually all online businesses can't solve for given the current scope and scale of the problem. It's not economically feasible to try to purchase all domain variants. What's more, traditional detection systems aren't fast enough or accurate enough to do the job, resulting in painstakingly long verification and take down processes.

Game up with 24×7 monitoring, detection and automated takedown of typosquat attack sites

Our typosquatting solution is designed to help you identify and monitor typosquat domains that are being used for nefarious activity. We seek out typosquat domains of any length, assess them for malicious content using natural language processing, deep learning, and logo detection and computer vision. If deemed fraudulent, we simply take them down automatically—on average in two minutes. The system then monitors the domains taken down to ensure they stay down in addition to monitoring registered domains that have suspicious activity but have not been activated yet. To keep an eye on it all, our platform provides rich widget-based dashboarding for easy-to-use visualization and reporting tools.

Real-time scanning & detection

Our detection engine uses deep learning to render a typosquatting verdict within 100 milliseconds with a false positive rate of 1 in 100,000.

Detect known & newly registered domains

Our threat intelligence feeds are augmented with algorithms to detect and monitor newly registered domains for malicious activity.

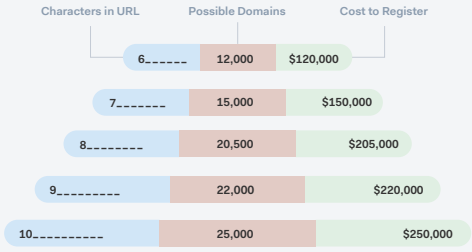
Fully-Automated Zero-Touch Takedown

Our electronic integration with hosting companies allows us to take down more than 95% of typosquat sites used for phishing as quickly as 2 minutes globally

Rich Threat Intelligence/Playbooks

Use pre-built SOAR playbooks to feed typosquatting events into your SIEM or other systems so your analysts can take action.

Legacy approaches can't keep up with the growing problem



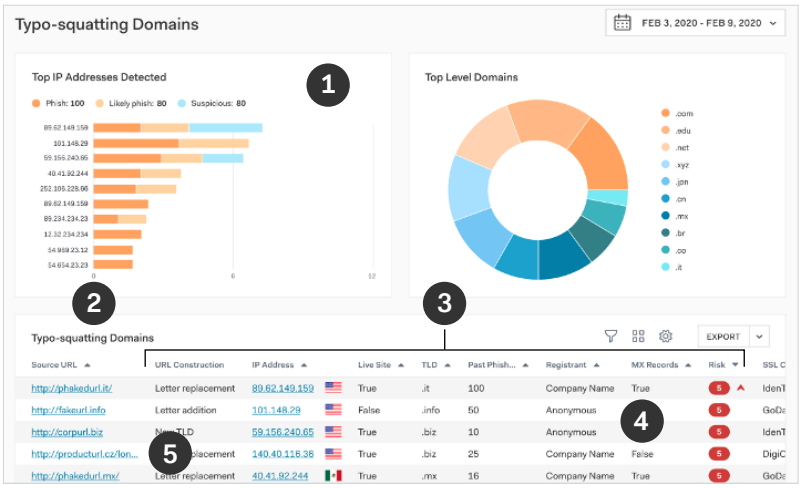
Unmatched Results

60 sec	2 min	95%	6.5 sec	24/7
Mean Time to Response (MTTR)	Avg API based takedown time	Without manual intervention	Submission to global blocklists	Automated monitoring

Real-time Dashboard

Actionable typosquatting information in real time

1. Configurable widgets graph volume of typosquatting by IP address, TLD, or geography
2. Detailed, actionable breakdown displayed for each typosquatting domain
3. See URL construction, TLD, company name, MX record detection and more
4. Real-time phishing & scam detection reveals risk level and trending status
5. Click to view detailed scan results based on natural language processing & computer vision



Customer Success at Scale

Dropbox

"My favorite thing about Bolster – I don't have to do a thing. No diverted employee time; no new hires; no setup; no admin. Plus there's full visibility into results and impact."

Devdatta Akhawe
Director of Security Engineering

1+ Million	**1/100,000**	**99%**
Number of sites scanned daily	False-positive rate	Takedown rate in the first 24 hours

About

Bolster builds AI/ML technology to protect regular citizens from bad actors on the internet. Your favorite brands from technology to eCommerce use our software to detect and takedown threats that might attack their customers, employees, or partners.
Learn more at: www.bolster.ai

4966 El Camino Real, Suite #101
Los Altos, CA, USA 94022
info@bolster.ai