Brand protection vendor scorecard

Ask every vendor the same nine questions. Score each answer 0–3, multiply by the weight (1–3), and compare totals. Then run a two-week pilot on your own brand.

VENDOR A _____ VENDOR B _____ VENDOR C _____

QUESTION	GOOD ANSWER	RED FLAG	WT	A	B	C
1. Who files the takedowns?	The vendor files and follows up without your involvement for standard cases	You file, or every takedown needs your approval	☐	☐	☐	☐
2. How many takedowns are included per month and what happens above that?	Unlimited or sized to your volume with clear overage pricing	Single-digit monthly caps, vague 'fair use'	☐	☐	☐	☐
3. What is the median and 90th-percentile time from detection to browser warning and to removal?	Both numbers with how they are measured and over what period	Only 'average' or 'as fast as hours' with no data	☐	☐	☐	☐
4. What does 'resolved' mean?	Offline and verified from several locations with evidence	'Report submitted' counted as resolved	☐	☐	☐	☐
5. What do you monitor and how often?	New domains, certificates, DNS, pages, social, marketplaces continuously	Weekly or monthly scans, limited sources	☐	☐	☐	☐
6. Which steps are automated and which go through an analyst queue?	A clear workflow showing what is automated end to end	No answer or only marketing terms	☐	☐	☐	☐
7. What evidence do you capture and can we reuse it?	Screenshots page source DNS and registration records timestamps exportable	Screenshots only, not exportable	☐	☐	☐	☐
8. How do you define and measure false positives?	A definition a measured rate and who triages them	No definition, you triage everything	☐	☐	☐	☐
9. Can we run a pilot on our own brand?	A 2-week pilot on your brand with the same threats given to every vendor	Canned demo only	☐	☐	☐	☐

TOTAL (SCORE × WEIGHT) _____

PILOT RESULTS: REAL DETECTIONS, REMOVALS, TIME TO WARNING AND REMOVAL _____

BUYING ALERTS OR REMOVED THREATS?

Decide first. A tool that stops at detection leaves the takedown work (lookups, reports, follow-ups) with your team, and that is most of the effort.