

5 Steps to Protecting Beauty Brands Online

As the online counterfeiting landscape becomes more complex, brands need a protection partner that can identify the threats that matter, support effective enforcement, and turn infringement data into **actionable intelligence**.

For beauty brands in particular, protection needs to reflect the way consumers discover and buy products today. From social commerce and marketplaces to paid advertising, search, and closed messaging apps, threats can appear anywhere across the digital customer journey.

This checklist sets out seven questions to help you assess whether a brand protection provider can deliver the coverage, intelligence, and enforcement your brand needs.

Question 1: Can you protect our entire digital ecosystem?

Ask exactly where the provider monitors. Do not settle for a generic list of marketplaces.

Ask about social media, search, websites, domains, paid advertising, marketplaces, and emerging commerce channels.

Then compare that coverage with your actual customer journey. Ideally, they will ask you to share this information with them in the interest of ensuring the brand protection programme is tailored to your needs.

Question 2: How smart is your detection?

Ask how the provider identifies threats that do not use your exact brand name.

Can it detect:

- Copied product imagery?
- Logo misuse?
- Altered brand names?
- Similar product listings?
- Unauthorised sellers?
- Impersonation?

The potential provider should be able to explain not just **what** it detects, but also **how**.

Question 3: What happens after detection?

This is a critical question. A provider that sends you alerts through a complicated dashboard is not necessarily a provider that protects you.

Ask them:

- Who gathers the evidence?
- Who submits the takedown?
- Who deals with the platform?
- Who follows up when the seller reappears?
- Who escalates difficult cases?

The closer the provider can get to managing the enforcement process, the less the operational burden will fall on your internal team.

Question 4: How do you prioritise threats?

Ask to see how potential infringements are scored and ranked. You want to know whether the system can help distinguish between:

A low-risk duplicate listing with limited visibility

and

A high-reach counterfeit operation targeting a hero product.

Volume is not the same as value.

Question 5: Can you identify counterfeit networks?

Individual listings can be symptoms of a much larger problem.

Ask whether the provider can connect sellers, listings, domains, imagery, and platforms to identify patterns and share this information.

This can help you move from repeatedly removing individual infringements to disrupting repeat offenders and wider networks.

Question 6: What does success look like?

Ask for meaningful KPIs that reporting will track and whether they include ROI impact.

For example:

- Time to detain
- Time to enforcement
- Successful removals
- Repeat infringement rates
- High-risk threats identified
- Seller networks uncovered
- Geographic coverage
- Internal hours saved

Question 7: What intelligence will be shared?

Your provider should not disappear behind a dashboard.

You should be receiving insights and regular reports that help your wider business understand the threat landscape and intergrate this knowledge into growth plans.

Contact Us

Every fake listing or imitation product takes a share of your hard-earned sales.

SnapDragon combines AI-powered detection, expert enforcement, and global experience to keep counterfeits off the market and your genuine products where they belong – in customers' hands.

Talk to SnapDragon about how proactive brand protection can drive stronger, more sustainable growth.



www.snapdragon-ip.com



UK & RoW: +44 131 466 9249

US: +1 857 400 7041



thelair@snapdragon-ip.com

LinkedIn



SnapDragon