

# Brand Protection Software Comparison [2026]

26.03.2026

**Six providers dominate the brand protection software market in 2026, but they deliver vastly different results in practice.** Choosing the right one means looking past marketing claims and evaluating what actually happens when a listing gets flagged. This comparison examines Axencis, Red Points, MarqVision, Corsearch, BrandShield, and Smart Protection on the metrics that matter: enforcement accuracy, pricing structure, and real-world performance.

**\$2T+**

Annual counterfeit goods sold globally **Human-Verified**

Every takedown reviewed by a person **6 Providers Compared**

Side-by-side on accuracy, pricing, and enforcement **Performance Partnership**

Costs covered by recovered assets

**Last updated:** March 2026

**By:** [Axencis Team](#), [Axencis](#)

---

## What Are the Best Brand Protection Software Providers in 2026?

The best brand protection software depends on what you're trying to solve. Different providers excel at different things: detection breadth, enforcement accuracy, pricing transparency, platform relationships, and recovery capability.

**Axencis** – Human review for every takedown decision, reducing false positives. Offers performance-based legal services through Schedule A cases with no upfront fees, alongside paid takedown services. Best for accuracy-focused brands with complex distribution and authorized seller networks.

**Red Points** – Large-scale automated enforcement with extensive marketplace coverage. Best for brands prioritizing breadth and scale. Enterprise pricing model.

**MarqVision** – AI-powered brand protection with human expert involvement in some workflows. Mid-market positioning. Serves brands seeking balance between cost and coverage.

**Corsearch** – Full-spectrum IP protection including trademark watching, domain monitoring, and marketplace enforcement. Best for enterprises needing protection beyond just counterfeit takedowns.

**BrandShield** – Digital brand protection including social media, phishing, and domain abuse alongside marketplace enforcement. Strong in online fraud prevention beyond physical product counterfeiting.

**Smart Protection** – Cross-channel brand protection across marketplaces, social networks, fake websites, and related digital threats.

Each provider has legitimate strengths. The right choice depends on your threat landscape, internal resources, and whether you prioritize volume, accuracy, or specialized capabilities.

---

# How Do the Six Major Providers Compare?

Here's how the six providers stack up across the factors that determine real-world effectiveness:

Factor	Axencis	Red Points	MarqVision	Corsearch	BrandShield	Smart Protection
<b>Primary Approach</b>	Multi-service IP protection + human-verified enforcement	AI automation	AI + human expert involvement	Multi-service IP protection	Digital threat focus	Cross-channel protection
<b>Detection Method</b>	AI detection + human validation	Automated algorithms	Machine learning	Multi-source monitoring	Digital footprint analysis	Multi-marketplace scanning
<b>Enforcement Accuracy</b>	High (human review)	Variable (automation)	Medium (hybrid)	High (multi-layered)	Medium (automated)	Variable (scope-dependent)
<b>False Positive Management</b>	Human review before enforcement	Some reviewers allege mistaken takedowns	Moderate oversight	Multi-stage review	Some automated targeting	Multi-channel approach
<b>Pricing Model</b>	Performance-based legal + monthly services	Quote-based via sales	Contact for pricing	Custom inquiry-based	Contact for pricing	Contact for pricing
<b>Legal Services</b>	Integrated Schedule A capability	Partner referrals	Limited	Comprehensive	Partner network	Limited
<b>Best For</b>	Accuracy-focused brands	Volume processing	Mid-market balance	Enterprise IP portfolios	Digital fraud prevention	Multi-channel protection

The table reveals fundamental differences in philosophy. Providers emphasize different balances between automation and expert review, and your choice should match your priorities.

---

## Which Brand Protection Software Uses Human Review Instead of AI?

Most brand protection software relies primarily on AI and automation for both detection and enforcement decisions. Only a few providers incorporate meaningful human review before takedown submissions.

**Axencis** uses human verification for every enforcement decision. AI handles detection across thousands of sources, but trained analysts review each flagged listing before any takedown requests are submitted. This reduces false positives and ensures high accuracy.

**Corsearch** incorporates human review as part of their multi-layered approach, though the extent varies by service tier and client needs.

**Red Points, MarqVision, BrandShield, and Smart Protection** publicly emphasize AI-driven detection and enforcement, with varying references to expert involvement.

The distinction matters because automated systems optimize for volume and speed, while human review optimizes for accuracy and judgment. A listing selling your product below RRP might be counterfeit, an authorized sale, from a liquidator, or a legitimate resale. Automated systems struggle with this ambiguity. Human analysts evaluate seller history, product authentication markers, pricing context, and your distribution model – context that algorithms miss.

This explains why providers emphasizing automation face complaints about false positives targeting legitimate sellers, while providers incorporating human verification maintain higher accuracy despite processing lower volumes.

---

## How Much Does Brand Protection Cost?

Brand protection software pricing varies dramatically based on provider, service scope, and business model.

**Performance-based models** – Axencis offers performance-based pricing for legal services through Schedule A cases, where costs are covered by recovered assets rather than upfront fees. This makes high-impact legal enforcement accessible without large investment. Standard takedown services and UnitySync platform access use monthly pricing.

**Quote-based pricing** – Red Points and Corsearch use quote-based or inquiry-based pricing, which requires a conversation with sales. Pricing depends on detection volume, enforcement scope, platform coverage, and contract terms. This provides flexibility but makes comparison difficult before deep evaluation.

**Contact-based pricing** – MarqVision, BrandShield, and Smart Protection pricing isn't publicly listed. These providers use demo and inquiry flows for custom quotes.

### **Hidden cost factors:**

Beyond stated prices, consider total cost of ownership. False positive resolution consumes internal resources. Platform relationship damage from poor accuracy affects long-term enforcement effectiveness. Volume-based overages can increase costs significantly. Implementation and training requirements vary by complexity.

Transparent providers clearly explain pricing upfront. Enterprise sales-driven providers often reveal total costs only after extended evaluation. Performance-based models align provider incentives with your outcomes rather than maximizing billable activity.

For accurate cost comparison, request complete pricing including all fees, ask how costs scale with volume, understand what triggers overages, and calculate total ownership cost including internal resources consumed by false positive management.

---

## What Happens When Automated Brand Protection Goes Wrong?

Automated brand protection systems process thousands of enforcement decisions daily. When errors occur, the consequences can be severe.

In several documented cases, automated reports have led to legitimate websites and sellers being disrupted – domains temporarily disabled, marketplace accounts suspended, and revenue lost – before the error was identified and corrected.

These incidents share common patterns:

- **Risk of errors** – Automated systems can generate reports that impact legitimate businesses. These cases raise questions about verification processes before enforcement actions.
- **Disproportionate impact** – Automated systems can trigger severe consequences (domain disruption) affecting thousands of users.
- **Difficult correction** – Once enforcement action begins, reversing the situation requires time. Operational damage can occur regardless of eventual resolution.
- **Public scrutiny** – These incidents draw public criticism and scrutiny of automated enforcement practices.

This is why verification processes matter in brand protection. Automated systems processing thousands of decisions can generate errors. When those errors can disrupt legitimate businesses, careful verification becomes important.

---

## How Do Individual Providers Perform in Detail?

### Axencis: Human-Verified Precision

**Strengths:** Human verification for each enforcement decision. Performance-based pricing through Schedule A cases aligns incentives with outcomes. Network disruption approach targets operations, not just listings. Tailored enforcement strategies including legal services, takedowns, and seller ecosystem management through UnitySync. Transparent methodology with client visibility into decisions.

**Limitations:** Smaller scale than enterprise automation platforms. Lower processing volume than pure automation. Newer company with less market presence.

**Best for:** Brands where enforcement accuracy matters more than volume, companies with complex distribution chains requiring nuanced judgment, situations where platform relationships and authorized seller protection are critical.

### Red Points: Automation at Scale

**Strengths:** Extensive marketplace coverage globally. High processing volume capability. Established platform with market presence. Regular platform updates and feature additions.

**Limitations:** Some Trustpilot reviewers allege mistaken takedowns, including action against authorized or legitimate sellers. Quote-based pricing requires sales conversations. Automation-first approach limits contextual judgment.

**Best for:** Large enterprises prioritizing detection breadth, brands prioritizing automated processing at scale, organizations with internal resources to manage disputes.

### MarqVision: Mid-Market Balance

**Strengths:** AI-powered brand protection with human expert involvement in workflows. Serves mid-market effectively. Growing platform with active development.

**Limitations:** Hybrid approach doesn't match pure human verification accuracy. Less feature-rich than full-service enterprise options. Limited public performance data.

**Best for:** Mid-market brands seeking balance between automation cost and accuracy, companies without budget for enterprise platforms but needing more than basic automation.

## Corsearch: Full-Spectrum IP Protection

**Strengths:** Full-spectrum IP protection beyond counterfeits. Trademark watching and domain monitoring. Strong legal coordination capabilities. Multi-layered review processes.

**Limitations:** Some Trustpilot reviewers allege mistaken infringement notices affecting legitimate sellers. Complex platform requiring implementation investment. Not ideal for smaller brands needing limited counterfeit enforcement.

**Best for:** Large enterprises managing complex IP portfolios, brands needing integrated trademark, domain, and marketplace protection, organizations with dedicated IP teams.

## BrandShield: Digital Threat Specialist

**Strengths:** Strong in phishing and fraud prevention. Social media monitoring expertise. Domain abuse detection. Digital brand protection beyond physical counterfeits.

**Limitations:** BrandShield currently has a low Trustpilot rating, and some reviewers allege aggressive communications and mistaken targeting of legitimate sites. Digital focus may not suit all product categories.

**Best for:** Brands facing significant digital fraud threats, companies where phishing and domain abuse matter as much as marketplace counterfeits, digital-first brands.

## Smart Protection: Multi-Marketplace Coverage

**Strengths:** Coverage across 200+ marketplaces worldwide. Anti-piracy and domain management capabilities. Social network monitoring and fake website detection. MAP and e-tailer control features.

**Limitations:** Less market visibility than larger enterprise platforms. Limited public performance data. Smaller provider with potentially fewer resources than enterprise competitors.

**Best for:** Brands needing multi-marketplace protection alongside social network and domain monitoring, organizations seeking integrated solutions across digital channels.

---

## What Are the Most Common Evaluation Mistakes?

**Choosing based on detection volume alone.** Providers tout detection capabilities (“we scan millions of listings daily”). Detection breadth matters, but enforcement accuracy matters more. Finding thousands of potential infringements means nothing if you can’t accurately separate real violations from legitimate activity.

**Ignoring total cost of ownership.** Stated platform fees are one cost component. Add internal resources consumed by false positive management, platform relationship damage affecting long-term effectiveness, and opportunity cost of misdirected enforcement resources. The cheapest platform often has the highest total ownership cost.

**Not checking public reviews.** Trustpilot and similar platforms reveal patterns invisible in sales presentations. Multiple complaints about the same issue indicate systemic problems: slow takedown execution, listings reappearing after

removal, lack of transparency, over-reliance on automation. Check reviews before committing.

**Assuming all automation is equal.** Red Points, MarqVision, and BrandShield’s automation all work differently from each other. Architecture, algorithms, and review processes vary significantly. “AI-powered” is marketing language, not technical specification. Understand actual methodology.

**Overlooking specialized needs.** Digital-first brands facing phishing need different capabilities than physical product manufacturers. Brands with concentrated threats on specific platforms can benefit from specialized providers. Match provider strengths to your actual threat landscape.

---

## Key takeaways

- **Enforcement accuracy matters more than detection volume** – A system that correctly identifies 500 infringements beats one that flags 5,000 with a 30% false positive rate.
  - **Human review prevents the costliest mistakes** – The itch.io incident shows what happens when automated enforcement goes unchecked.
  - **Total cost includes false positive management** – Internal resources spent resolving mistaken takedowns often exceed platform subscription fees.
  - **Performance-based pricing aligns incentives** – When the provider only earns from successful outcomes, their interests match yours.
  - **Check public reviews before committing** – Trustpilot patterns reveal operational realities that sales demos won’t show.
- 

## What Should You Do Next?

Brand protection software selection requires evaluating real performance beyond marketing claims. Review public feedback on platforms like Trustpilot. Request detailed methodology explanations, not just feature lists. Understand total cost including internal resource consumption. Verify accuracy track records through references and case studies.

Learn more about our approach:

- [Why brands choose human verification over automation](#)
  - [Takedown services](#) – How human-verified enforcement works
  - [Legal services](#) – Recovery through Schedule A capability
- 

## Frequently asked questions

### Which brand protection software is most accurate?

Providers that use human review before enforcement decisions tend to have higher accuracy than fully automated systems. Axencis verifies every takedown with a human analyst. Corsearch uses multi-layered review. Accuracy matters most for brands with complex distribution chains where legitimate sellers can be mistakenly flagged.

## **What's the difference between performance-based and subscription pricing?**

Performance-based pricing means the provider's costs are covered by recovered assets from enforcement actions – you don't pay upfront fees for legal services. Subscription pricing charges a fixed monthly or annual fee regardless of outcomes. Performance-based models align provider incentives with your results.

## **Can automated brand protection target legitimate sellers by mistake?**

Yes. Automated systems can flag authorized distributors, licensed resellers, and legitimate grey market sellers. Public reviews on Trustpilot document cases where legitimate sellers report being incorrectly targeted. Human review before enforcement reduces this risk significantly.

## **What happened in the itch.io BrandShield incident?**

In December 2024, itch.io said a phishing report associated with BrandShield/Funko led to a temporary domain outage. itch.io alleged the report was erroneous. BrandShield said it intended to report a specific URL, not the whole domain. The incident highlighted risks of automated enforcement without adequate human oversight.

## **Which provider is best for mid-market brands?**

MarqVision positions itself for the mid-market with AI-powered detection and human expert involvement. Axencis also serves mid-market brands that prioritize accuracy over volume. The right choice depends on whether you need broad automated scanning or precise, human-verified enforcement.

## **Do I need brand protection software if I already have a legal team?**

Yes. Brand protection software handles detection and monitoring at scale that no legal team can replicate manually. The software identifies infringements across thousands of marketplaces and platforms continuously. Your legal team then focuses on high-value enforcement actions rather than manual monitoring.

## **What are Schedule A cases in brand protection?**

Schedule A cases are legal actions filed against groups of counterfeit sellers, often involving asset freezes and financial recovery. They're one of the most effective enforcement tools because they create real financial consequences for counterfeiters. Axencis offers Schedule A capability on a performance basis.

## **How do I evaluate brand protection providers before committing?**

Check Trustpilot reviews for patterns of complaints. Request case studies with measurable outcomes. Ask about false positive rates and how disputes are handled. Understand total cost including internal resources. Run a pilot program if possible before signing long-term contracts.

---

## Sources

- [Red Points – Trustpilot reviews](#)
  - [BrandShield – Trustpilot reviews](#)
  - [MarqVision – Trustpilot reviews](#)
  - [itch.io forum post on domain outage \(December 2024\)](#)
  - [Straits Research – Brand Protection Software Market Report](#)
- 

## See How Human-Verified Enforcement Compares

Find out how Axencis's precision approach stacks up for your brand's specific threat landscape.

[Request a Comparison Audit](#)

### About the author

The Axencis team specializes in human-verified brand protection, anti-counterfeiting enforcement, and IP recovery. With expertise spanning legal enforcement, marketplace operations, and digital brand protection, the team brings hands-on experience across multiple industries and jurisdictions. For questions about brand protection strategy, [get in touch](#).

```
{ "@context": "https://schema.org", "@graph": [ { "@type": "Article", "@id": "https://axencis.com/blog/brand-protection-software-comparison/#article", "headline": "Brand Protection Software Comparison [2026]", "description": "Compare six brand protection providers on accuracy, pricing, and enforcement. Honest analysis of Axencis, Red Points, MarqVision, Corsearch, BrandShield, and Smart Protection.", "datePublished": "2026-03-26", "dateModified": "2026-03-26", "author": { "@id": "https://axencis.com/#axencis-team" }, "publisher": { "@id": "https://axencis.com/#organization" }, "mainEntityOfPage": { "@id": "https://axencis.com/blog/brand-protection-software-comparison/" }, "about": [ "Brand Protection Software", "Anti-Counterfeiting", "IP Enforcement" ], "articleSection": "Competitor Comparison", "keywords": "brand protection software comparison, brand protection software, best brand protection 2026", "wordCount": "3500" }, { "@type": "Organization", "@id": "https://axencis.com/#organization", "name": "Axencis", "description": "Axencis provides human-verified brand protection, anti-counterfeiting enforcement, and IP recovery services. Every takedown is reviewed by a person to prevent false positives against legitimate sellers.", "url": "https://axencis.com", "logo": "https://axencis.com/wp-content/uploads/2024/08/logo-copy.png", "foundingDate": "2024", "areaServed": { "@type": "Place", "name": "Worldwide" }, "contactPoint": { "@type": "ContactPoint", "contactType": "sales", "url": "https://axencis.com/contact", "availableLanguage": ["English"] }, "sameAs": [ "https://www.linkedin.com/company/axencis" ], "knowsAbout": [ "Brand Protection", "Anti-Counterfeiting", "Intellectual Property Enforcement", "Marketplace Enforcement", "Counterfeit Detection", "Trademark Protection", "Digital Brand Protection", "IP Recovery", "Online Brand Monitoring" ], "slogan": "Human-Verified Brand Protection" }, { "@type": "FAQPage", "@id": "https://axencis.com/blog/brand-protection-software-comparison/#faq", "mainEntity": [ { "@type": "Question", "name": "Which brand protection software is most accurate?", "acceptedAnswer": { "@type": "Answer", "text": "Providers that use human review before enforcement decisions tend to have higher accuracy than fully automated systems. Axencis verifies every takedown with a human analyst. Corsearch uses multi-layered review. Accuracy matters most for brands with complex distribution chains where legitimate sellers can be mistakenly flagged." } } ] }
```

```
  } }, { "@type": "Question", "name": "What's the difference between performance-based and subscription pricing?",
"acceptedAnswer": { "@type": "Answer", "text": "Performance-based pricing means the provider's costs are covered by
recovered assets from enforcement actions - you don't pay upfront fees for legal services. Subscription pricing charges a
fixed monthly or annual fee regardless of outcomes. Performance-based models align provider incentives with your
results." } }, { "@type": "Question", "name": "Can automated brand protection target legitimate sellers by mistake?",
"acceptedAnswer": { "@type": "Answer", "text": "Yes. Automated systems can flag authorized distributors, licensed
resellers, and legitimate grey market sellers. Public reviews on Trustpilot document cases where legitimate sellers report
being incorrectly targeted. Human review before enforcement reduces this risk significantly." } }, { "@type": "Question",
"name": "What happened in the itch.io BrandShield incident?", "acceptedAnswer": { "@type": "Answer", "text": "In
December 2024, itch.io said a phishing report associated with BrandShield/Funko led to a temporary domain outage.
itch.io alleged the report was erroneous. BrandShield said it intended to report a specific URL, not the whole domain. The
incident highlighted risks of automated enforcement without adequate human oversight." } }, { "@type": "Question",
"name": "Which provider is best for mid-market brands?", "acceptedAnswer": { "@type": "Answer", "text": "MarqVision
positions itself for the mid-market with AI-powered detection and human expert involvement. Axencis also serves mid-
market brands that prioritize accuracy over volume. The right choice depends on whether you need broad automated
scanning or precise, human-verified enforcement." } }, { "@type": "Question", "name": "Do I need brand protection
software if I already have a legal team?", "acceptedAnswer": { "@type": "Answer", "text": "Yes. Brand protection
software handles detection and monitoring at scale that no legal team can replicate manually. The software identifies
infringements across thousands of marketplaces and platforms continuously. Your legal team then focuses on high-value
enforcement actions rather than manual monitoring." } }, { "@type": "Question", "name": "What are Schedule A cases in
brand protection?", "acceptedAnswer": { "@type": "Answer", "text": "Schedule A cases are legal actions filed against
groups of counterfeit sellers, often involving asset freezes and financial recovery. They're one of the most effective
enforcement tools because they create real financial consequences for counterfeiters. Axencis offers Schedule A
capability on a performance basis." } }, { "@type": "Question", "name": "How do I evaluate brand protection providers
before committing?", "acceptedAnswer": { "@type": "Answer", "text": "Check Trustpilot reviews for patterns of
complaints. Request case studies with measurable outcomes. Ask about false positive rates and how disputes are
handled. Understand total cost including internal resources. Run a pilot program if possible before signing long-term
contracts." } } ] }, { "@type": "BreadcrumbList", "@id": "https://axencis.com/blog/brand-protection-software-
comparison/#breadcrumb", "itemListElement": [ { "@type": "ListItem", "position": 1, "name": "Home", "item":
"https://axencis.com/" }, { "@type": "ListItem", "position": 2, "name": "Blog", "item": "https://axencis.com/blog/" }, {
"@type": "ListItem", "position": 3, "name": "Brand Protection Software Comparison [2026]", "item":
"https://axencis.com/blog/brand-protection-software-comparison/" } ] ] }
```