FORTRA

Brand Protection Buyer's Guide

Find the right partner to elevate your brand protection

In our digital-first world, protecting your brand has never been more critical. As brands expand their reach across borders and platforms, they're up against a growing wave of threats, everything from counterfeit products and online impersonation to IP theft and digital piracy. These risks not only jeopardize revenue and market share but undermine consumer trust and long-term reputation.

The data speaks for itself. Brand protection has never been more essential:

- Phishing is exploding. Since 2020, new phishing sites have surged by 700%, with close to one million appearing every single month.
- Hackers are increasingly targeting business executives, with attacks rising from 43% in 2023 to 51% in 2025.
- Scams impersonating businesses and U.S. government agencies led to $2.95 billion in consumer losses in 2024.
- According to the World Economic Forum, 72% of survey respondents say cyber risks have gone up over the past year, mainly driven by more cyber-enabled fraud, phishing scams, social engineering, and identity theft.
- The average global cost of a data breach in 2025 is $4.44 million, while in the United States, it has surged to an all-time high of $10.22 million, the highest of any region.

Additionally, AI is amplifying brand impersonation attacks, making it easier than ever for cybercriminals to create convincing fakes. With generative AI, they can automate phishing, mass produce counterfeit assets, and mimic trusted brands with striking accuracy to bypass traditional trust signals and defenses. Even inexperienced actors can launch credible fraud campaigns using low-cost, off-the-shelf AI tools.

This buyer's guide helps organizations navigate the complex world of brand protection. Whether you're a global enterprise or a growing business, understanding the right tools and strategies is key to safeguarding your brand's identity and value. We'll cover common pain points, must-have features, and best practices to help you choose the right partner so you can proactively protect what you've worked hard to build.

Lack of Comprehensive Visibility Across Digital Channels

One of the most pressing challenges in brand protection today is the lack of comprehensive visibility into external digital threats. Many organizations remain unaware of phishing attacks, impersonation attempts, or brand misuse until they're alerted by customers or employees and, at this point, the damage may already be underway.

This fragmented visibility severely limits an organization's ability to detect, assess, and respond to threats quickly and effectively. A striking 79% of cybersecurity professionals report making decisions the majority of the time without access to adversary insights from threat intelligence which highlights a widespread lack of visibility into attacker motives, tactics, and infrastructure. Compounding the issue, 47% of surveyed leaders cite "applying threat intelligence throughout the security organization" as one of their top challenges. Without this critical context, security teams are left reacting to threats rather than anticipating them, making proactive defense difficult, if not impossible.

Without real-time visibility into the threats targeting their brand, organizations are essentially operating in the dark as they are unable to anticipate, detect, or respond to attacks with the speed and precision needed to protect their reputation and assets.

Assessing Visibility: What to Ask Potential Brand Protection Providers

To deliver strong protection, a brand protection solution must continuously scan massive volumes of data across the surface web, dark web, social media, mobile apps, and email. Comprehensive, real-time coverage across these digital channels is key to detecting a higher volume of emerging threats before they reach customers or damage brand reputation.

Advanced tools like web beacons and crawlers should play a critical role by uncovering threats others may miss. These tools provide deep visibility into where and how a brand is being targeted, allowing organizations to detect and mitigate threats before they escalate. Ultimately, effective brand protection depends on this kind of expansive, proactive data collection to safeguard both the organization and its customers.

When evaluating a brand protection solution, be sure to ask:

- What sources do you rely on to collect domain data, such as SSL certificate registrations, passive DNS, or DNS zone files?
- Do you monitor for abusive mobile applications? If so, how do you find them?
- Which social media platforms do you monitor?
- What data are you collecting first-hand? What data is collected via third-party sources (including feeds)?
- How do you deal with modern obfuscation techniques that hide fraudulent or malicious content from crawlers or other detection tools?
- Do you monitor lookalike domains, trademark misuse, and executive impersonation?
- Do you have a dedicated team providing continuous threat analysis that actively hunts threats beyond automated alerts?
- What's your strategy for staying ahead of new brand exploitation techniques and emerging attacks?

The Hidden Threat of Noise

Security teams today face an overwhelming number of alerts from a variety of cybersecurity tools and monitoring systems. While these systems are vital for defending against cyber threats, the sheer volume of irrelevant or false alerts has become a significant barrier to effective brand protection.

Modern brand protection operates in noisy digital environments including social media, e-commerce platforms, and messaging apps where impersonators and malicious actors thrive. Organizations need tools that cut through this noise and deliver actionable insights, not just more data.

The volume of alerts only adds to the challenge. Security Operations Centers (SOCs) typically receive between 3,800 and 10,000 alerts daily, with the majority proving irrelevant or false positives. Studies show that 55% to 80% of alerts are ignored or found to be non-actionable. Faced with a flood of low-value alerts, analysts can become overwhelmed and desensitized, resulting in slower responses and the potential to overlook critical threats.

The consequences of this are severe: Missed threats such as phishing scams, brand impersonation, or counterfeit product listings can cause lasting damage to brand reputation, erode customer trust, and weaken an organization's overall security posture.

Assessing the Noise: What to Ask Potential Brand Protection Providers

An effective brand protection solution blends advanced automation with expert human analysis to cut through the noise and focus on real threats. Machine-filtered alerts are enriched by skilled analysts who apply context-specific processes to review, validate, and categorize results — delivering expert-vetted, curated threat intelligence. This human-driven refinement reduces false positives and provides clear visibility into external threats.

Core capabilities include advanced phishing detection that identifies sophisticated attacks often missed by standard defenses, along with proactive credential theft protection to reduce the risk of compromise. By integrating automation with human expertise, the solution not only improves detection accuracy but also eases the operational burden on security teams. Analysts continuously tune intelligence to the organization's unique risk profile, enabling faster response times, minimizing the impact of attacks, and allowing security teams to focus on strategic priorities.

When evaluating a brand protection solution, be sure to ask:

- Are threats validated solely through automation, or do experts review them as well?
- How does your service guarantee accuracy and reliability?
- How do you manage and eliminate duplicate alerts for similar threats appearing across multiple platforms like social media, the dark web, and domains?
- Can you provide metrics for your alert accuracy?
- Do you provide reporting and dashboards that show alert quality, incident prioritization, and operational metrics?
- Can you tune or customize alert thresholds and rules specifically for our environment?
- How often do you update your detection rules, signatures, and data sources to keep false positives low?
- How do your experts vet and curate the intelligence collected?
- Are you able to distinguish between benign activity and clearly malicious? How do you classify activity that's not clearly malicious but is also not clearly benign?
- On average, what percentage of cases require customer input to make a final determination?
- Provide examples of cases that typically do not require customer review, as well as examples of those that do.

The High Cost of Slow Mitigation

What makes mitigation so difficult is the lack of streamlined processes across platforms and jurisdictions. There's no standardized process across registrars or platforms, and internal security teams must attempt to manage countless external relationships with limited visibility or authority. Attackers exploit this gap, hosting malicious content in hard-to-reach corners of the internet and shifting infrastructure faster than defenders can respond.

As a result, only 25% of phishing sites are taken down within 24 hours. Every delay increases the risk of data breaches, financial loss, and brand damage.

Traditional security tools built for internal defense often miss external threats across email, web, and social channels. Without a purpose-built, automated brand protection strategy, organizations remain vulnerable.

Spotting threats is just the first step. What really matters is having the right people and processes in place to take them down, quickly and at scale. Without that, threat actors stay active, and the organization pays the price.

Assessing Ineffective Mitigation: What to Ask Potential Brand Protection Providers

An effective brand protection solution must rapidly detect, disrupt, and remove threats to your brand's integrity. Human expertise is essential as analysts enrich machine-generated alerts with context-driven intelligence, delivering accurate visibility into real threats.

Rapid, large-scale threat mitigation requires a global takedown network, browser-blocking, and automated integrations to take down thousands of threats daily. Leading solutions take it further as they leverage proprietary killswitch technology and direct API connections with service providers to instantly remove threats, eliminating delays caused by manual takedown requests.

Unlimited takedowns with no hidden fees allow aggressive, flexible responses without cost-related delays. Around-the-clock incident response ensures rapid recovery and minimal operational impact.

When evaluating a brand protection solution, be sure to ask:

- Do you have established vendor relationships or integrations with major service providers, registrars, or hosts to expedite takedowns?
- Can you describe your global takedown network?
- What steps are involved in your threat takedown process look like?
- On average, how long does it take you to successfully take down a malicious asset after detection?
- Can remediation steps be automated or orchestrated via your platform?
- How does your service integrate with our existing SIEM, SOAR, incident management, or alerting workflows?
- Is there a limit on the number of takedowns performed with the service?

Strained Security Teams Pose Organizational Risk

Internal security teams are under immense pressure, burdened by an overwhelming volume of threats and alerts, many of which are false positives. With limited staff and time, they're forced into a reactive mode, which disrupts daily operations and compromises brand protection efforts. Staffing shortages only intensify the strain; in 2024 alone, over 4.7 million cybersecurity roles went unfilled, leaving teams under-resourced and overwhelmed.

Alert fatigue and burnout are rampant. Nearly one in four CISOs are considering stepping down due to stress, and high turnover continues to erode institutional knowledge. Alarmingly, 83% of security leaders report that burnout has directly contributed to breaches through human error.

Limited internal resources are creating a bottleneck that severely impacts the capability to proactively defend against external threats. To protect brands effectively, organizations need solutions that reduce the burden through automation, intelligent threat prioritization, and expert external support. Without it, internal teams will continue to drown in noise and critical threats will slip through the cracks.

Reducing Operational Burden: What to Ask Potential Brand Protection Providers

A truly effective brand protection solution should be a managed service, one that proactively detects and mitigates external threats while removing the burden on internal security teams. It goes far beyond software alone, delivering end-to-end threat management that removes the operational load from in-house resources.

By taking on detection, investigation, and takedown, the solution allows internal teams to focus on strategic initiatives instead of constant reactive firefighting. A 24/7 Security Operations Center provides continuous monitoring and rapid response, with experts trained to identify and neutralize threats in real time.

Organizations benefit from avoiding the cost and complexity of building this expertise internally. With predictable pricing and unlimited takedowns, the solution ensures there are no surprise fees, just consistent, comprehensive brand protection.

When evaluating a brand protection solution, be sure to ask:

- Can your service handle the entire threat detection and mitigation process while reducing my team's workload?
- Can you share examples or reports that demonstrate the range and detail of threats detected for current clients?
- Do you operate an in-house security operations center to support threat monitoring and incident response for clients?
- Is your SOC staffed 24/7 with qualified security analysts?
- Does your SOC provide real-time escalation and support for critical incidents?
- How do you streamline collection, curation, and mitigation into a single process for clients?
- How do you minimize the client's need to triage alerts internally?
- How scalable is your service if our business grows?

Brand Protection Begins with the Right Partner

The threats on your brand are becoming more complex and harder to detect and mitigate. From phishing and impersonation to lookalike domains and fake social profiles, the risks are too significant to ignore. Protecting your brand must be a critical element of your cybersecurity strategy.

The right brand protection solution partner doesn't just provide superior technology. They deliver end-to-end support that includes threat detection, real-time visibility, alert curation, and rapid takedown capabilities.

When evaluating brand protection providers, ask the challenging questions. Look for a solution that offers broad visibility, cuts through the noise with expert validation, mitigates threats swiftly, and alleviates pressure on your internal security team.

At Fortra, we break the attack chain of fraud and brand impersonation. We collaborate with organizations so they can disrupt the infrastructure used in a broad range of online attacks targeting their brands, employees, and customers.

Take the next step toward proactive brand protection.

Connect with **Fortra Brand Protection** to stop threats before they impact your brand, your people, or your customers.

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

0825-fta-gd-r1-vm