BOLSTER AI

MAY 2026

Best Practices for Modern Brand Protection

Building More Robust Brands Through Cybersecurity Best Practices

By Bolster AI Research Team

Table of Contents

I. Why is Brand Protection Important?

Fraud tactics have evolved. Online impersonation and infringement now occur at light speed. The longer you take to respond to these threats, the greater the potential for reputational damage and revenue loss as threat actors victimize customers, prospects, and partners through your brand.

In 2025, phishing and counterfeit pages topped 10.5 million globally. Each day, fraudsters send out approximately three billion phishing emails. A single brand may be the target of hundreds, perhaps even thousands, of incidents overnight.

People-focused brand protection solutions simply cannot operate at this scale — and criminals know it. Some even intentionally flood targets with fraudulent activity intending to overwhelm them.

To keep pace, your organization needs a new approach to brand protection — one that addresses the issue through technology instead of new hires.

Security teams have begun leveraging computer vision, artificial intelligence (AI), machine learning, and natural language processing. These same tools have the potential to revolutionize brand protection, improving your organization's security posture.

To survive this tide, you need to fight scale with scale; leveraging expertise and technology rather than headcount.

3.8M
Phishing attacks in 2025 [1]

3.4B
fake/impersonation emails sent daily [2]

18K
fraudulent sites created daily [3]

Citation

[1] APWG, Phishing Activity Trends Report, Q4 2025

[2] More than 3 Billion Fake Emails Are Sent Worldwide Every Day," Valimail Spring 2019 Email Fraud Landscape report, 2019

[3] Bolster AI, 2026 Fraud Trends & Predictions Report,2026

II. Knowing the Risks

Brand infringement encompasses a diverse range of attacks and tactics — many immediately familiar to anyone with a cybersecurity background. It's yet one more reason why brand protection is fundamentally a security problem.

Counterfeit Products

The rise of online marketplaces and digital goods has created a perfect storm for criminals looking to sell cheap knockoffs at scale.

Typosquatting

Even a simple six-letter domain can spawn over 100,000 fake variants. Criminals exploit user typos to redirect to fraudulent sites.

Phishing Attacks

The number-one threat vector for cybersecurity. Phishing takes many forms, from fake credential-harvesting sites to targeted scam emails.

Copyright Infringement

Plagiarists steal videos, product images, logos, and text for brand impersonation or personal gain across the web.

Account Takeovers

Frequently the second phase of a phishing attack — stolen credentials used for identity theft or further escalation against a brand.

Social Media Fraud

Brand infringement on social networks tends to be four times worse than elsewhere on the Internet — and growing.

Fake Websites

Fraudulent websites have existed as long as the Internet — used to sell counterfeits, defraud visitors, or serve as phishing entry points.

Malicious App

App stores are flooded with software that steals information, pushes obtrusive ads, or promotes illegitimate products under trusted names.

Business Email Compromise

Criminals use spoofed addresses or lookalike domains to extort money or deliver malicious payloads directly to employees.

III. Best Practices for Brand Protection

Automation

The scope and scale of modern brand infringement attacks are impossible to tackle manually. By combining automation with properly trained AI, Bolster AI can identify and classify fraud far more efficiently than any human actor.

Proactive Remediation

Relying on blacklists is like trying to find broken glass by wandering barefoot in the dark. Detect and act on threats as quickly as possible through Bolster AI's automation and artificial intelligence.

24/7 Monitoring

Criminals won't do you the courtesy of attacking only during regular office hours. Bolster AI actively guards your brand around the clock, 365 days a year — with intelligent alerting and a centralized dashboard.

Accuracy

False positives are the death of any security solution. Bolster AI's platform leverages machine learning to discard false positives and intelligently filter notifications, keeping security teams focused on real threats.

Real-Time Response

The more time spent on research and decision-making, the longer scammers have to exploit your brand. Bolster AI augments your response capabilities with automation and machine learning for near-instant action.

Trusted Partnerships

Working with experienced service providers is almost always the right call. Bolster AI is trusted and well-known in both brand protection and cybersecurity, with a proven track record across industry-leading brands.

IV. The Pillars of Modern Brand Protection

Every brand's needs are a little different. However, the DNA of an effective brand protection program is unchanging. When implementing your program with Bolster AI, focus on these four pillars:

People

Brand protection involves multiple stakeholders: CISOs, security professionals, IT, compliance officers, attorneys, paralegals, and analysts — all aligned through Bolster AI's unified platform.

Processes

Design and implement standardized workflows covering the threats your brand faces, digital detection and enforcement processes, roles, responsibilities, and hand-offs between teams.

Partnerships

Bolster AI is technology-focused and knowledgeable, offering tier-based pricing without pressure. We let our results speak for themselves: industry-leading accuracy and speed.

Technology

Each brand infringement problem has an online component. Bolster AI's solution includes image detection, keyword detection, AI-powered analysis, triage, 24/7 automated monitoring, alerting, and reporting.

V. Two Sides of the Same Coin

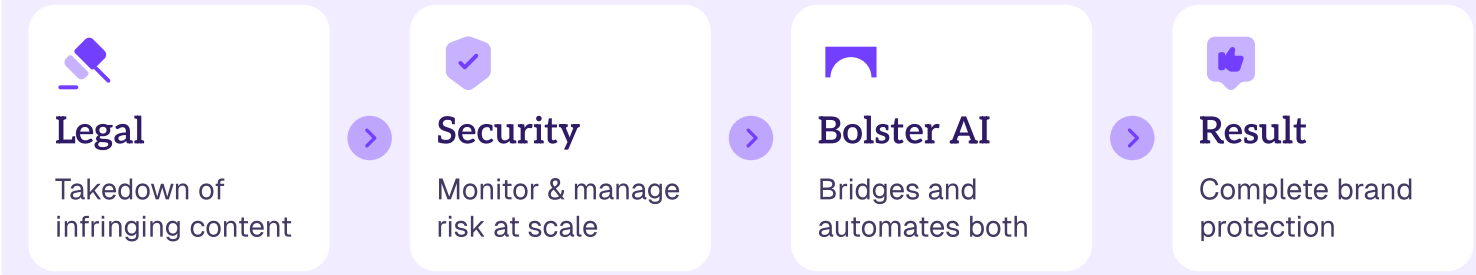
Brand protection is as much a cybersecurity problem as it is a legal problem. Neither side should go it alone — collaboration, powered by Bolster AI, is the key to success.

Legal brand protection enforcement focuses on taking down infringing content rather than blocking access — a considerably more effective long-term approach. Bolster AI gives security teams the tools to monitor and manage organizational risk at scale.

Modern brand infringement is akin to a runaway train: the more digital touchpoints you maintain, the more difficult it becomes to protect them. A never-ending stream of threat actors looks to illicitly profit from your organization and its customers.

It's a daunting prospect, but not insurmountable. With Bolster AI's automated detection and takedown capabilities, you can stop the runaway train dead on the tracks and regain control of your brand.

Legal + Security Together



Ready to protect your brand with Bolster AI?

Request a Demo

https://bolster.ai

BOLSTER AI

Making the Internet Safe for Everyone.

At **Bolster AI** our mission is to make the internet safe for everyone. That's why we created the first and only fully automated platform purpose-built to detect, monitor, and take down fraudsters on the Internet. We call it Automated Digital Risk Protection.

Our comprehensive platform offers the most efficient protection across web, social media, marketplace, app stores, and dark web — helping the world's most recognizable brands combat fraudulent sites, phishing, and digital impersonation at scale.

Contact Bolster AI today:

2880 Lakeside Dr, Ste 150, Santa Clara,
CA 95054

https://bolster.ai

Request a Demo