BOLSTER

Best Practices for Modern Brand Protection

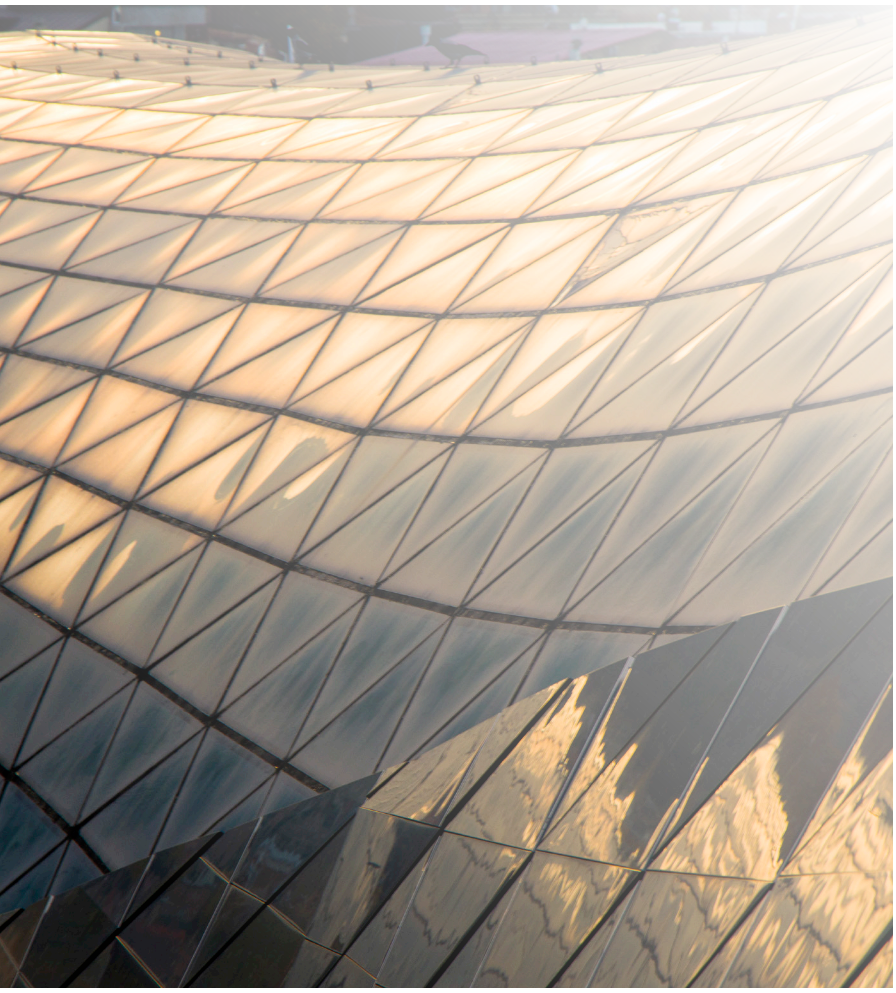
Building More Robust Brands Through Cybersecurity Best Practices

Contents

Foreword

by Shashi Prakash,
Chief Technology Officer and
Cofounder, Bolster.ai

Brand impersonation has been a growing threat for over a decade. In recent years, however, brand impersonation has become a massive issue, and information security (InfoSec) sits at the center of it all. To put it simply, if your brand has an online presence, you need a brand protection program — and that program must be part of your overall cybersecurity strategy.



Traditionally, brand protection was the domain of the legal department. Brand analysts, paralegals, and attorneys worked together to manually investigate and assess potential infringement. At a time when roughly 18,000 fraudulent websites are created[1] *daily*, this approach is more than simply infeasible — it's obsolete.

Modern brand protection demands that we treat infringement and impersonation as new attack vectors, subject to the same principles and processes as any other cyber threat.

Of course, this reality introduces an entirely new set of challenges. Organizations are already struggling to contend with overly complex ecosystems and the growing security skills shortage. Security teams are already short on time, resources, and personnel.

How can they shoulder yet more responsibility?

You'll find the answer in this white paper — along with an overview of the threats your brand faces, best practices for your brand protection program, and guidelines for choosing the right brand protection vendor.

[1] https://www.helpnetsecurity.com/2020/11/25/fraudulent-sites

Why is this 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 2021, phishing and counterfeit pages topped 10.5 million globally[2]. Each day, fraudsters send out approximately three billion phishing emails[3]. 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 new technology instead of new hires.

This is where brand protection and cybersecurity intersect. Security teams have begun leveraging technology such as computer vision, artificial intelligence (AI), machine learning, and natural language processing. These same tools and solutions have the potential to revolutionize brand protection, improving your organization's security posture in the process.

Yet, even the best tools may prove insufficient in unskilled hands. That's why deploying a brand protection solution is only the first step. You must also understand what you're up against, so you know where to direct your time, effort, and attention.

It's now easier than ever for threat actors to engage in fraudulent activity targeting your brand and its customers, creating a surge in both the volume and scope of brand infringement attacks. To survive this tide, you need to fight scale with scale by leveraging expertise and technology.

10.5

million phishing and counterfeit web pages were created in 2021 alone.

3billion

phishing emails are sent out daily.

[2] https://bolster.ai/resources-center/download/report/2022-phishing-online-fraud
[3] https://www.zdnet.com/article/three-billion-phishing-emails-are-sent-every-day-but-one-change-could-make-life-much-harder-for-scammers/

Knowing the risks

Most threat actors aren't interested in a challenging game of cat-and-mouse. They seek the path of least resistance — the easiest way to make a quick buck. By understanding and preparing for their tactics, you can discourage many of them right out of the gate.

Brand infringement encompasses a diverse range of attacks and tactics, many of which are immediately familiar to anyone with a cybersecurity background. It's yet one more reason why brand protection is a security problem. Several of the following use cases overlap with work already occurring in security operations centers (SOCs).

Counterfeit products

Counterfeiting has always been an issue, and not just for luxury brands. The rise of online marketplaces, the popularity of ecommerce, and the proliferation of digital goods have together created a perfect storm for criminals looking to sell cheap knockoffs.

Fake websites

Fraudulent websites have existed for as long as the Internet, though not every fake site is created with the same objective in mind. Some sites may be used to sell counterfeit goods, while others may use your brand in an effort to defraud visitors. Still others may simply be part of a larger phishing campaign.

Copyright infringement

To say that copyright infringement runs rampant online would be putting it lightly. Plagiarists steal anything and everything — videos, product images, logos, artwork, and even text — for brand impersonation or personal gain.

Phishing attacks

Coincidentally, the number-one threat vector for cybersecurity is also one of the most common brand infringement attacks. Phishing can take many different forms, from fake websites designed to steal credentials to targeted scam emails.

Most threat actors aren't interested in a challenging game of cat-and-mouse. They seek the path of least resistance — the easiest way to make a quick buck

The Most Common Brand Infringement Attacks

Business email compromise

A business email compromise (BEC) attack occurs when a criminal attempts to defraud a company by directly targeting its employees. Threat actors typically use a spoofed email address to extort money from or send a malicious payload to their target. They may also leverage stolen credentials or lookalike domains.

Fraud and scam campaigns

A brand infringement attack may be part of a concerted, ongoing effort to defraud a company or its customers. Many infringement programs tend to overlook this fact, defining infringement too narrowly and missing out on both fraudulent activity and larger patterns of attacker behavior.

Typo squatting

When customers enter your business's URL incorrectly, they expect to be redirected to your website. Typo squatting abuses this expectation, leveraging top-level domains and extensions to create fake sites that look nearly indistinguishable from the genuine webpage. Even a simple six-letter domain can spawn over 100,000 fakes.

Social media fraud

Recent events have cast a harsh light on the dangers of unregulated social media use, as fraudulent activity and falsified information are commonplace. In our experience, this problem extends to brand infringement, which tends to be four times worse on social networks than elsewhere on the Internet.

Account takeovers

An account takeover is frequently the second phase of a phishing email or website — the end result of a criminal's efforts in which they use stolen credentials for further fraudulent activity. This often takes the form of identity theft. A criminal may also abuse a compromised account's trusted access to escalate their attacks against a brand by exfiltrating data or installing malicious software.

Malicious apps

Smartphones contain our entire lives, both personal and professional. Their ubiquity makes them a treasure trove for cybercriminals, who have flooded app stores with malicious software that steals information, pushes obtrusive ads, or promotes illegitimate products.

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, you can identify and classify fraud far more efficiently and effectively than any human actor.

Accuracy

False positives are the death of any security solution, making it increasingly difficult to identify and respond to threats. To make matters worse, overwhelmed security teams may cope with the flood of unnecessary alerts by simply ignoring them, potentially overlooking major incident. Find a brand protection tool that leverages and machine learning to discard false positives and intelligently filter notifications.

Proactive remediation

Relying on blacklists is like trying to find broken glass by wandering around barefoot in the dark. Threat actors know these lists exist, and they know how to sidestep them by creating new fraud sites and exploring new tactics. They're counting on targets to wait, which is exactly why you must detect and act on threats as quickly as possible — this is best accomplished through automation and artificial intelligence.

Real-time response

The more time you spend on research, analysis, and decision-making, the longer scammers have to take advantage of your brand. Be prepared to act the moment you identify a new threat. Augment your response capabilities with automation and machine learning.

24/7 monitoring

Criminals and scammers won't do you the courtesy of attacking only during regular office hours. Your business can come under threat at any time and from any location. Look for a tool that actively guards your brand 24 hours a day, 7 days a week, 52 weeks a year, with or without direct human intervention — ideally one with intelligent alerting and a centralized dashboard.

Trusted partnerships

Working with experienced service providers is almost always the right call. Look for companies that are both trusted and well-known in brand protection and cybersecurity. Avoid working with vendors that lack experience, if possible — they may not possess the necessary understanding of your challenges and landscape.

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 own program, focus on the following four pillars:

People

Brand protection may be a security problem, but multiple stakeholders are involved, including

- Chief information security officers
- Security professionals
- Information technologists
- Compliance officers
- Attorneys
- Paralegals
- Investigators
- Analysts

Processes

Design and implement standardized workflows defining

- The threats your brand faces
- Digital detection, monitoring, and enforcement processes
- Roles and responsibilities
- Interconnections between groups
- Handoffs

Partnerships

The best brand protection service providers are technology-focused and knowledgeable, content to let their competence speak for itself. They do not

- Charge based on hours, volume, or takedowns instead of SKU-level pricing
- Lack a tier-based pricing/licensing model
- Speak poorly of competitors
- Pressure prospective clients into a contract
- Make grandiose claims or promises

Technology

Each brand infringement problem has an online component. The right technology goes a long way toward disrupting the criminal supply chain. Look for a solution with

- Image detection
- Keyword detection
- Analysis
- Triage
- 24/7 automated monitoring
- Alerting
- Reporting

Two sides of the same coin

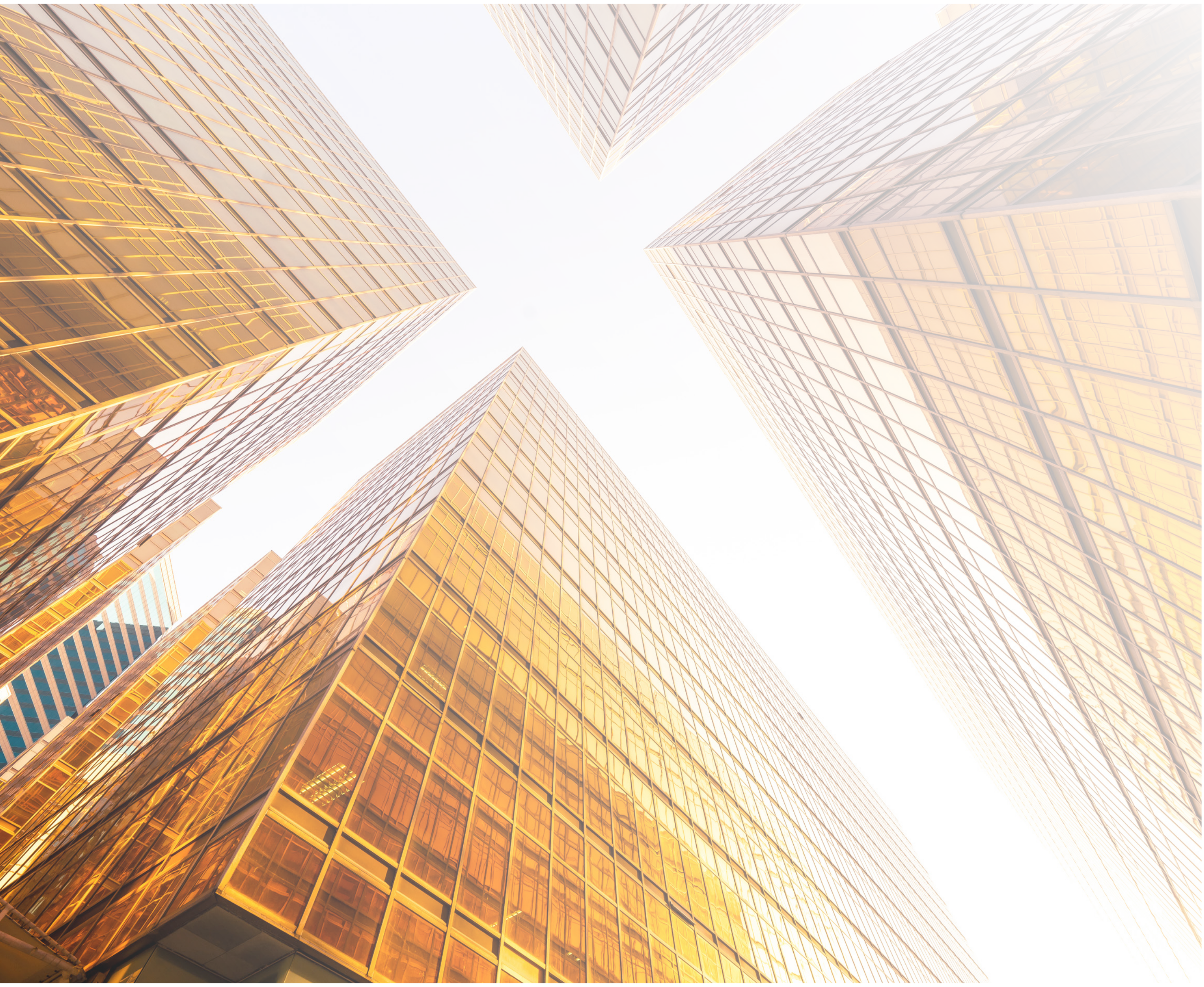
Brand protection is as much a cybersecurity problem as it is a legal problem. Neither side should go it alone; collaboration is the key to success.

Legal brand protection enforcement focuses on taking down infringing content rather than blocking access — a considerably more effective approach in the long-term. Security teams, meanwhile, already have the skillset to monitor and manage organizational risk at scale. The two directly complement one another, particularly when paired with a purpose-built brand protection platform.

Modern brand infringement is very much 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 to contend with. But it's not insurmountable. With the right approach — and with help from an AI-driven brand protection solution — you can stop the runaway train dead on the tracks and regain control of your brand.

Bolster's cutting-edge brand protection software leverages machine learning to detect and take down threats that might target your customers, employees, or partners. Request a demo to learn more about what it can do for your business.



About BOLSTER

At Bolster, our mission is to make the internet safe for everyone. That's why we created the first and only fully automated platform purpose-built from the ground up 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, app stores, and the dark web to combat fraudulent sites and content.

Contact us today:

4940 El Camino Real, Suite
#200, Los Altos, CA, USA 94022
bolster.ai