

Brand Guardian

Digital trust is now a frontline security issue. Artificial intelligence (AI) has industrialized brand impersonation, enabling attackers to launch convincing phishing sites, counterfeit domains, and scam campaigns in minutes. The result: rising fraud losses, customer churn, and erosion of brand trust. Traditional brand monitoring approaches cannot keep pace. Organizations need a continuous, intelligence-driven solution that detects and disrupts abuse at internet scale.

To protect customers and preserve trust, organizations must treat brand abuse as a core security issue, delivering continuous visibility, intelligent prioritization, and rapid automated response across multiple attack surfaces.

The reality of protecting a digital brand

Fraud and brand abuse are no longer niche security issues — they are large-scale operations fueled by automation and generative AI. These technologies have dramatically lowered the barrier to entry for attackers, enabling them to create convincing scams, phishing content, and counterfeit digital experiences at unprecedented speed and volume.

Today, it can take minutes for attackers to spin up a counterfeit website, complete with realistic branding, language, and customer flows. Large enterprises routinely face thousands of active look-alike scams and impersonation variants, most of which exist entirely outside the visibility of traditional security tools.

At the same time, fake experiences are difficult for users to distinguish from legitimate ones. AI-generated content, cloned websites, and polished social engineering tactics make fraudulent social profiles, emails, and login pages look authentic. As a result, customers are more likely to engage, share credentials, or complete transactions before realizing they've been deceived, if they realize it at all.

Legacy brand protection models are reactive, manual, and siloed. Modern brand security must be continuous, automated, and integrated into core security operations. These legacy workflows are slow, resource-intensive, and poorly suited to an environment where attackers continuously rotate domains, hosting providers, and identities. By the time one fraudulent site is identified and removed, multiple replacements have already gone live, perpetuating the cycle.

Benefits for your business

Protect brand trust

Proactively remove counterfeit sites and impersonations to ensure your brand remains safe, reliable, and authentic across every digital channel.

Reduce customer fraud

Eliminate phishing and scam infrastructure before engagement to protect customers from sophisticated AI-driven attacks.

Accelerate threat response

Replace manual workflows with automated discovery and enforcement to shorten takedown timelines.

Lower customer churn

Prevent brand-related scams that drive dissatisfaction and attrition, helping to retain customers.

Scale without headcount

Handle thousands of look-alike domains and scam variants simultaneously using automation and intelligence.

Improve risk prioritization

Focus resources on the most critical threats by ranking brand abuse based on customer impact, financial risk, and reputation.

Strengthen executive visibility

Deliver clear, measurable insights into brand risk, takedown effectiveness, and trend analysis, helping leaders understand exposure.

Unify brand protection

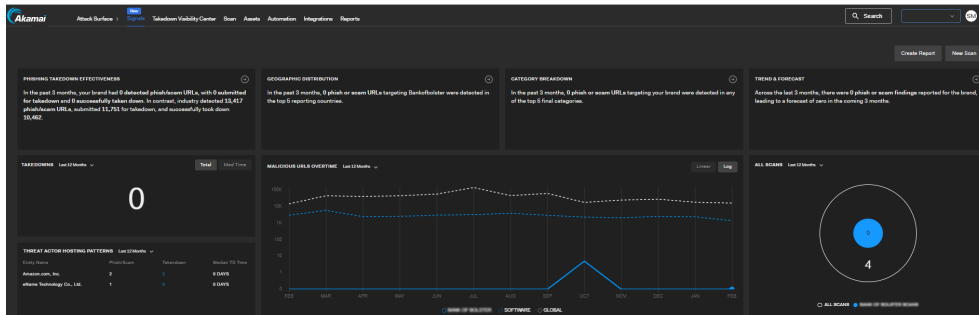
Break down silos between security, fraud, legal, trust/safety, and marketing teams by providing a shared view of brand abuse.



How Akamai Brand Guardian helps

Brand Guardian addresses this new reality by treating brand abuse as a continuous, high-scale security problem, one that requires automation, intelligence, and internet-wide visibility. Utilizing AI-powered detection and internet-scale infrastructure visibility, Brand Guardian enables organizations to detect, prioritize, and disrupt brand-based attacks at the speed they are created.

Rather than relying on customer reports or manual searches, Brand Guardian continuously discovers brand impersonation across domains, websites, social media, app stores, and dark web sources in real time. Advanced analysis correlates signals to distinguish low-risk noise from high-impact threats, helping teams focus on activity that puts customers and revenue at risk.



Signals dashboard provides AI-powered insights and threat feeds to track phishing and impersonation

Response is automated and scalable

Integrated workflows accelerate investigation, evidence collection, and takedown actions across registrars, hosting providers, and other online platforms. AI models trained on real-world brand abuse patterns separate genuine threats from legitimate brand usage, minimizing false positives and ensuring your team focuses on what matters. Where automation handles routine takedowns, experienced security analysts focus on the complex cases that require human judgment.

That protection extends beyond brand monitoring alone. By integrating brand threat intelligence with Akamai's broader DNS posture and security capabilities, organizations gain a unified view of external risk, enabling stronger governance, faster response, and clearer executive accountability.

Key product capabilities:

- **Continuous brand abuse discovery**
Automatically identifies brand impersonation across look-alike domains, phishing sites, fraudulent social profiles, fake apps, email, and emerging digital channels.
- **AI-first threat detection**
Uses advanced AI to detect brand abuse in milliseconds while minimizing false positives.
- **Automated investigation and takedown**
Automated takedown workflows accelerate evidence collection and enforcement across registrars, hosting providers, and platforms, significantly reducing time to removal.

- **Risk-based threat prioritization**
Ranks threats based on likelihood of customer harm, fraud enablement, and reputational impact, allowing teams to focus on the most critical risks first.
- **Broad multichannel visibility**
Monitors across domains, websites, social platforms, app stores, search engines, email, and dark web sources in one platform.
- **Unified brand and security posture**
Integrates brand threat intelligence with Akamai's broader security and DNS posture capabilities, enabling organizations to manage brand abuse as part of a holistic security strategy.

By matching the scale and speed of modern fraud, Brand Guardian helps organizations protect customers, reduce churn, and preserve brand trust, wherever their brand is targeted across the internet.

Request a brand assessment from your Akamai team or visit akamai.com to learn more.