AKAMAI PRODUCT BRIEF

Brand Protector Product Brief

Detect and disrupt phishing sites, fake stores, and brand impersonations to prevent harm to your customers and reduce the risk of large-scale fraud and abuse attacks.

Your recognizable brand creates measurable value both outside and inside your organization. Protecting your brand elements enables your organization to retain and grow customer loyalty while minimizing losses, productivity drops, and bad customer reviews. From a security point of view, controlling brand impersonation stops the kill chain in its tracks, preventing credential harvesting and account abuse.

Not all attacks appear at an organization's front door. Across the web, attackers impersonate your brand with digital lookalikes to steal your customers' sensitive data, credentials, and direct payments. Brand impersonation and phishing are a growing challenge, due to their short-lived campaign tactics that turn on and off and move locations to make detection and mitigation a resource-intensive challenge.

Akamai Brand Protector leverages one of the largest threat intelligence databases, combining both first-party and third-party data feeds to speed detections and improve accuracy. Integrated mitigation capabilities make Brand Protector an effective and essential tool for early evasion of fraud and abuse attacks.

Akamai Brand Protector detects and mitigates targeted attacks including phishing, impersonations, and brand abuse across sites, social media, and app marketplaces. Most importantly, Brand Protector allows you to safeguard your trusted relationships.

More than 50,000 new phishing websites are created every week. Brand Protector inspects trillions of digital activities a day, across internal and external sources, to discover abuse of your organization's brand and brand elements with speed and efficiency — often before an attack campaign launches.

To accomplish all this, Brand Protector addresses the problem of fraudulent impersonations with a four-step approach: intelligence, detection, visibility, and mitigation.

Benefits for your business

Trusted attack detection
Our proprietary global network and additional feeds provide a unique advantage to detect brand impersonations

Accuracy and speed
Our speedy algorithmic detection can deliver alerts before attack campaigns launch and can minimize false positives

Actionable insights
Comprehensive data is delivered as actionable insights with risk scoring that summarizes the severity and reach of attack in a single glance

Per-customer visibility
Dedicated intel collection for your brand, products, and associated elements across websites, social media, and app marketplaces

Ease of use
Gain real-time insights and initiate remediation into this growing attack vector in minutes

Takedown and mitigation
To stay productive, leverage the integrated takedown service within Brand Protector, or choose to disrupt traffic with a browsing alert

Akamai

Intelligence

The challenges with detecting phishing and brand impersonation attacks begin at the intelligence and data collection phase.

As the largest global edge and cloud platform, Akamai's proprietary view across the worldwide web traffic analyzes more than 788 TB of data a day. The depth of intelligence in Brand Protector is enhanced with third-party data feeds for holistic visibility into attacker actions. Additionally, you can add your own URL and domains for analysis by the Brand Protector detection cloud.

Detection

Brand Protector's detection strength and speed comes from a combination of Akamai's proprietary intelligence feed and analysis algorithms to increase detection confidence and lower false positives.

Brand attacks automate malicious, short-lived websites. Most technology is not fast enough to detect and mitigate these attack assets before they have impacted your customers. Akamai's approach is different because we trace live traffic to detect brand abuse instead of relying on refreshed lists or delayed feeds. With Brand Protector, your security team can detect phishing sites when the first HTTP/HTTPS request occurs — often before the campaign has reached your customers.

Visibility

Customer-centric engineering and design give your team expansive security insight in a single dashboard view.

After receiving intelligence, data signals are run through a series of heuristic and artificial intelligence detectors. Although an overwhelming amount of data and evidence is collected, Akamai's simplified user interface provides an instant understanding of active threats to your customers via impersonations.

Customer-specific traffic, detections, and threat data are distilled into actionable insights within the Akamai customer portal. The findings are ranked by a summarized threat score. Click into an alert to view analyzed threat data including confidence score, severity rating, number of affected users, and a timeline of attack events.

Each detection is supported by evidence — you can view code, screenshots, detection indicators, and domain details in a single detection screen.

Mitigation

Integrated takedown services close the loop to combat brand fraud.

Brand Protector allows your team to issue a takedown request of the abusive site right in the detection screen. Takedown requests (sent to an Akamai third-party partner) for Brand Protector automatically attach the detection's evidentiary support and additional details for ease of use. You can track and view mitigation status in the portal.

Built for your brand

Zone Protection
This solution from our edge protection portfolio can extend your security team's view into early kill chain protection. It proactively searches for permutations of your brand's domains that could be used to turn customers into phishing victims.

Social Media Monitoring
With the rise of brand impersonation on social media, our new enhanced social media monitoring capability detects and neutralizes online fraud, protecting your brand and its customers on various platforms.

Rogue App Detection
App marketplace monitoring is a new feature that scans official and unofficial app repositories to detect deceptive applications that misuse brand identity, offering a comprehensive defense across the digital landscape.