AKAMAI PRODUCT BRIEF

Content Protector

Protect your revenue from increasingly sophisticated scraper attacks

There's money to be made (by attackers) and lost (by you) in scraping your content. While sharing content publicly is a strategic choice, it's crucial to differentiate between consumer engagement and harmful scraping activities. Competitors and attackers can exploit scraped data, undermining your pricing strategy and harming your customers. Akamai Content Protector promptly identifies and halts scrapers at first sight, using detections tailored to the unique tooling and techniques of scraper attacks. Safeguard your business and revenue without compromising speed or performance.

Scraping attacks present a continuous challenge for online businesses. Unlike typical cyberthreats that have clear start and end points, scrapers can persistently access your site, leading to significant implications if not addressed. These include:

- **Website performance impact:** Persistent scraping activities can slow down your site, leading to user frustration and reduced conversion rates.
- **Competitive disadvantages:** Competitors may use scraping to monitor and undercut your pricing, affecting your revenue.
- **Brand reputation risks:** Counterfeiters could misuse scraped content, selling fake products under your brand's name.

Of course, scrapers have been around for many years. Why are they worse now? The urgency to combat scrapers has intensified recently. The events of 2020, including the pandemic and subsequent supply chain disruptions, have increased the financial incentives for scraping. High-demand items, ranging from everyday essentials to luxury goods and travel services, have become prime targets for sophisticated scraping operations.

With more potential money to be gained, bot operators began innovating feverishly, specializing in pieces of the tooling (like telemetry) and then chaining those together with pieces made by other bot operators to create highly specialized bots unique to scraping attacks. That makes the scrapers more dangerous and also more difficult to detect. And worse, scraping can also occur using other methods like plug-ins, so you need more than bot management to stop scrapers.

But you can't just block all scrapers — search bots look for new content that you want to show up in public searches, some consumer shopping bots can highlight your products in comparison sites, and partners can efficiently gather the latest product information to share with their customers.

BENEFITS FOR YOUR BUSINESS

Raise conversion rates
Remove the bots slowing down your site and apps, keeping more customers on your site and improving sales

Reduce costs
Don't pay to serve bot traffic

Thwart scalpers
Prevent scrapers from pinging your site to see when hot inventory becomes available, lowering the bot operators' ability to get to the next step in an inventory hoarding attack chain

Frustrate competitors
Stop the automated scraping that lets your competitors undercut your prices and lower your sales

Mitigate counterfeiting
Stop the relentless scraping counterfeiters use to grab your content and then pass themselves off as you

Market yourself better
Remove bot traffic from your site analytics to ensure you're optimizing for real users

Akamai Content Protector has detections uniquely designed to detect scrapers and stop them. And it does this while taking advantage of the Akamai network's visibility, our global strength in bot management, and continuous development of leading-edge detections. Updating your protection as threats evolve, we automatically incorporate insights from our threat intelligence researchers and data scientists, so Content Protector continues to lead in tailored detections for scrapers.

Once you stop the scrapers, you can focus on getting the most from your digital presence — such as improving your site performance and conversion rates, and reducing the impact of competitors.

Key capabilities

- **Detections:** A set of ML-powered detection methods that assesses the data collected client-side and server-side.
  - **Protocol-level assessment:** Protocol fingerprinting evaluates how the client establishes the connection with the server at the different layers of the OSI model: TCP, TLS, and HTTP — verifying that the parameters negotiated align with the one expected from the most common web browsers and mobile applications.
  - **Application-level assessment:** Evaluates if the client can run some business logic written in JavaScript. When the client runs JavaScript, Content Protector collects the device and browser characteristics and user preferences (fingerprint). These various data points will be compared and cross-checked against the protocol-level data to verify consistency.
  - **User interaction:** Behavioral metrics evaluate that a human interacts with the client through standard peripherals like a touch screen, keyboard, and mouse. Lack of interaction or abnormal interaction is typically associated with bot traffic.
  - **User behavior:** Analyzes the user journey through the website. Botnets typically go after specific content, resulting in significantly different behavior than legitimate traffic.
  - **Headless browser detection:** A custom JavaScript running client-side looking for indicators left behind by headless browsers even when running in stealth mode.
- **Risk classification:** Provide a deterministic and actionable low-, medium-, or high-risk classification of the traffic based on the anomalies found during the evaluation.
- **Response actions:** A set of response strategies, including the simple monitor-and-deny action, and more advanced ones such as tarpit, which simulates a server hanging or various types of challenge actions. Crypto challenges are generally more user-friendly than CAPTCHA challenges for dealing with possible false positives.

The foundation of Content Protector: the Akamai ecosystem

Akamai makes the internet fast, smart, and secure. Our comprehensive solutions are built on the globally distributed Akamai Connected Cloud, managed through the unified, customizable Akamai Control Center for visibility and control, and supported by Professional Services experts who get you up and running easily and inspire innovation as your strategies evolve.

Sign up for a demo or contact the Akamai sales team.