

Data Scraping Risk Assessment Service for Online Businesses

Almost all companies in the online business dependant on making information available to the public suffer from data scraping attacks. During these attacks scrapers systematically steal information from the company's website and use it to boost competing businesses – in clear breach of the site's terms and conditions.

Where none existed before, Sentor has developed a sharp tool for assessing the scraping risk any online company is subjected to.

Why is data scraping a threat to the online business?

Because it's your intellectual property being stolen. Numerous online businesses around the world are subjected to data scraping every day and enormous amounts of data is downloaded every hour and used by the scrapers for personal or commercial gain.

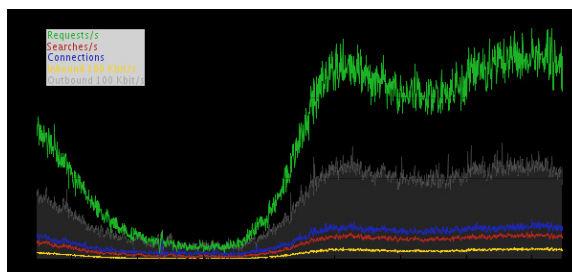
The total damage of ongoing scraping is hard to estimate since it affects diverse parts of your business. For example:

- A competing company may draw users and advertisers away from you by systematically downloading large amounts of information from your website using it to offer a better, more complete service to their customers.
- Scraping can directly affect your company's revenue when prospective customers, instead of buying data lists from you, simply download what they want without paying.
- Your relation with your advertisers can be seriously damaged when one of the effects their ad at your site has, is them being contacted by telemarketers who has scraped your site for prospect lists.
- Massive distributed scraping will also affect the performance and availability of your site to legitimate users. During one Scraping Risk Assessment we carried out for a client, two scrapers were responsible for nearly 10% of all searches on the site, consuming resources for legitimate users.

How can I assess the scraping risk my company is subjected to?

Assessing the scraping risk is not an easy task. The manual tools for detecting data scraping that exist today are time-consuming and inadequate. Adding insult to injury, scrapers become more and more sophisticated every day, masking themselves as search engine robots or normal users, which makes satisfactory manual scraping detection near impossible.

You need an automated system backed with human analysis, running around the clock, in order to have a fighting chance at detecting and blocking serious data scrapers.



With Scraping Risk Assessment you will get a crystal clear view of the scraping activity at your website.

Learn about your risk with Sentor's Scraping Risk Assessment service

With Sentor's Scraping Risk Assessment service you can get a crystal clear view of how much scraping your online business is subjected to, thereby assessing your need to protect your intellectual property. The service is based on ASSASSIN – Sentor's unique service which detects and blocks scraping attacks in real time for clients all over the world.

How does Scraping Risk Assessment work?

Sentor runs historical log data from your web-servers through ASSASSIN. The amount of log data needed varies but we typically recommend two months worth of data in order to comprehensively assess your scraping risk.

The data is replayed in the system just as if it was real time data, allowing our operators to detect and analyse scraping incidents in the same manner as if you were protected by ASSASSIN.

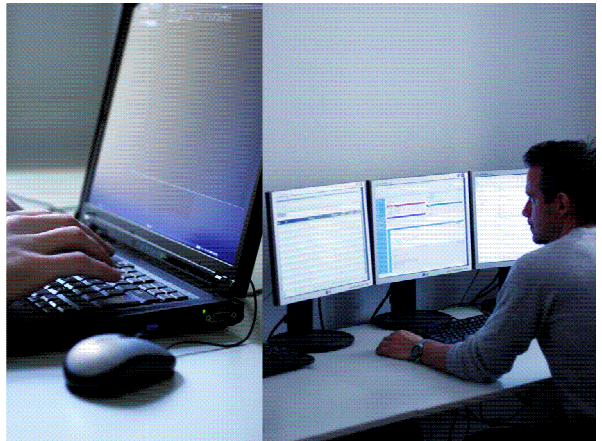
After completion of the analysis you receive a report summarising all scraping incidents at your web-site, along with other abusive behaviour. This report may serve as a foundation for a thorough risk analysis of the need to further protect the intellectual property of your online business. The report includes information such as:

- Number of scraping incidents
- Estimated volume of data stolen
- General statistics of abuse

What are the benefits?

Simply put, the benefits of Sentor's Scraping Risk Assessment service are:

- *Risk assessment.* Enables you to detect 100% of all scraping attacks on your website during the test period. With this information you assess your need to further protect your intellectual property from scraping attacks.
- *Instant access to reports.* Ad hoc reports are available to you "24/7", allowing you to monitor scraping activity at your website during the test period, just as if you had real time protection with Sentor's ASSASSIN.



Sentor's security operators are ever vigilant, guarding our clients' information assets against data scraping.

- *Comprehensive summary report.* A comprehensive report about scraping incidents as well as other abusive traffic is delivered after the test period. This report allows you to evaluate your protection needs in depth.
- *Transparent service.* Access to our Security Management Portal during the test period gives you full insight into our work.

Need more protection?

If your risk analysis – based on the Scraping Risk Assessment summary report – shows that you need to take strong countermeasures in order to protect yourself against data scrapers you may step up your defences by implementing ASSASSIN into your systems.

ASSASSIN detects and blocks scraping attacks in real time according to predefined response processes which we draw up together based on your specific needs. Having already done a risk assessment prior to implementing ASSASSIN benefits you, as the results of the assessment will be used in the process.

Contact us today

Call us at +46 8 545 333 00 or email assassin@sentor.se. We look forward to explain the full benefits of Scraping Risk Assessment to you.