Signal Sciences

Investing.com Blocks Data Scraping Bots at Scale

CHALLENGE

Investing.com is a global financial portal and internet brand composed of 30 editions in 22 languages and mobile apps for Android and iOS that provide news, analysis, streaming quotes and charts, technical data and financial tools about the global financial markets. Each edition covers a broad variety of local and global financial vehicles including stocks, bonds, commodities, currencies, interest rates, futures, and options. Investing.com is ranked 532 in Alexa Global Rank and is one of the top three financial portals in the world.

An advertising-supported business, Investing.com pays financial exchanges for financial markets data and content to publish to its user base. Investing.com needed a solution that would detect and stop malicious actors deploying bots and scrapers to harvest this data and using it for their exploitative purposes. The team was facing 30-40M content scraper requests per week that they needed to stop.

> "Signal Sciences has proven to be a highly effective solution in terms of reducing false positives in production which is important for us at all times, but especially during extremely high-volume traffic periods."

Gabriel Mizrahi, CTO at Investing.com

SOLUTION

Signal Sciences enabled Investing.com to deploy an application and API defense solution with agents installed on-premise in their data center. Additionally, they utilized Signal Sciences Power Rules that detect and block bots and scrapers from harvesting content Investing.com purchases.

Investing.com's operations staff installed Signal Sciences agents on their highest traffic site web servers. Signal Sciences was able to block high volumes of bad-bot traffic for Investing.com, stopping the data scraping requests from reaching the application and stealing data. Within the first week of Investing.com putting these Power Rules in place, Signal Sciences blocked over 40 million bot requests without a single false positive.

Investing.com had not found a solution to mitigate data scraping bots, but with Signal Sciences gained both the ability to identify the high volume of scraping bots and block them. Signal Sciences ability to deploy in any environment—on premise, in cloud or hybrid environments—made the rollout easy and future-proof since it moves wherever their applications are deployed. Installing Signal Sciences enabled Investing.com to:

Meet European GDPR privacy requirements while protecting customer data

Protecting customer data to be compliant with GDPR privacy requirements meant Investing.com needed a WAF technology. With Signal Sciences, Investing.com can redact the entire contents of commonly-used sensitive headers, parameters, and values as well as those they specify as unique to their application. Signal Sciences enabled them to do this while protecting their portfolio of sites and APIs.

Deploy a future-proof WAF solution on premise without impacting app performance

Publishing real-time stock quotes and financial data requires fast, efficient request processing. Legacy WAFs using a virtual or physical appliance can create bottlenecks as they struggle to process high volumes of web requests. But Signal Sciences can be installed and distributed alongside customer applications without creating a bottleneck: Investing.com installed our technology across their existing servers without deploying any dedicated virtual or physical WAF appliances. Our patented module-agent architecture protects apps with a fail-open design that won't interrupt site performance or impact uptime.

Gain visibility while blocking attacks in production without false positives

Precise details of web requests in production have helped Investing.com's DevOps and network operations teams see how and when scrapers are attempting to steal data from them—and block that activity at scale. They also gained visibility into malicious actors' "below the radar" bot request patterns that are smaller in scope in an effort to avoid detection. With Signal Sciences they also enhanced their security posture by uncovering would-be attacker methods by analyzing granular details about the scraping requests.

> "We now spend less time manually blocking malicious bots and scrapers while reducing our workload with automated attack blocking."
>
> **Gabriel Mizrahi**, CTO at Investing.com