RISKIQ®

Find and Eliminate JavaScript Threats

Pinpoint malicious code, Magecart, and threat actors

THE CHALLENGE: Enable Digital Commerce, Shielded from Threats

Digital assets—outside the firewall—are difficult to find and protect, leaving the attack surface open to compromise by cybercriminals. Hidden exposures are a breeding ground for stealing payment card details, PII and other personal financial data.

Meanwhile, threat actors exploit unnoticed gaps with easy, cheap tools like JavaScript injections to execute techniques such as cross-site scripting and component compromise. These threats harm the enterprise through the hard costs of theft, takeovers, skimming, and breach clean up—along with lost customers, lost trust, and lost revenue.

Specific challenges include:

- Constantly changing pages, scripts—new risk every moment
- Limited, or no line-of-sight into third party compromise
- Unknown attacker-accessible pages and infrastructure: enterprise and third party
- Cannot identify inner workings of infrastructure, websites, pages, apps, components or code
- Long dwell times, malicious JavaScripts linger and spread

THE SOLUTION: Find and Eliminate JavaScript Threats

Security teams can find and eliminate JavaScript threats automatically, leveraging RiskIQ's global sensor network and patented machine learning tailored for JavaScript threats.

RiskIQ stops guesswork with JavaScript threats by absorbing relevant data from every pocket of the internet—IP and non-IP space—to fingerprint assets, connections, codes, and components, including JavaScripts threats. Our global sensor network and human-web simulation continuously stream asset intelligence, pinpoint JavaScript threats, and automate detection: enterprise and third party dependencies.

WHY RISKIQ?

Complete Intelligence from full DOM capture, uncover code exposures and access

Always-on Detection and live change monitoring: apps, pages, code, enterprise, third party

Attacker-aware Machine Learning to pinpoint accessibility and prioritize risky attack paths

Global Internet Graph

RiskIQ collects and rapidly dissects internet-scale data with machine learning to encode security expertise, 10+ years of internet history, and live JavaScript detection—no hosting required. Shield customers, partners, and the digital enterprise with the only view of your entire internet presence, including clode and component threats.

SOLUTION OVERVIEW

RiskIQ is the only attack surface solution designed to discover unknowns and eliminate threats; guided by attack-aware machine learning and continuous detection to root out malicious JavaScripts.

No-Agent Sensor Network

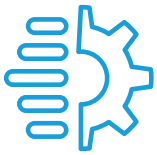
identifies JavaScript and credential, access risk in apps, resources, code, and services via full DOM extraction

Attack Surface Visualization

intuitive, flexible UI simplifies internet visualization—data to insights to action in just a few clicks

Live, Always-on Change Detection

synchronized code and component inspection, automating change detection for assets and malicious JavaScripts



Autonomous Orchestration

enforce business and security logic, trigger downstream workflows for speedy response with zero human touch

"The additional insight RiskIQ provides, helps us protect the integrity of our global network and create a trusted environment for the people on our platform. RiskIQ helps Facebook detect and block threats planted in third-parties that violate our policies or put our people at risk."

Director of Security Operations
Facebook

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com