Protect Your Brand From External Threats


THE CHALLENGE:

Your brand is your business in the digital age. RiskIQ helps protect your brand with active mapping, monitoring, mitigating, and managing external threats and schemes against your digital identity. Security intelligence makes it easy to find and take down.

- Typosquat domains
- Phishing
- Mobile App Impersonation
- Exposed Credentials
- Bank Numbers
- Brand Impersonation via Social Media
- Code Breaks
- Weaponized Impersonations
- Domain Infringement

RiskIQ virtual users search for web content using a combination of threat feeds and configured search engine searches for brand keywords to encounter threats the same way real users targeted by them do.

THE SOLUTION:

Discover and Eliminate Typosquatting
Attacker-aware machine learning and open search, including DNS change detection and history. RiskIQ monitors for typosquat domains that can be used in phishing campaigns. Along with integrated GSB services, RiskIQ is at your command to take down brand threats to stop them in their tracks.

Unify Intelligence, Pinpoint Data Leaks
The frequency of brand attacks can overwhelm security teams. RiskIQ discovers sensitive data, including PII, PFI, and corporate information from leaks—precisely tuned to your unique brand. Security teams can gain visibility over their digital footprint to extend protection to their public-facing assets.

Pinpoint Abuse, Take Action
Security Intelligence from RiskIQ generates alerts and reports that provide key insights on how to remediate and take down brand attacks with focus on:

- Typosquatting sites, domains, and hosts
- Misleading social media accounts
- Other forms of brand abuse
- Attribution

WHY RISKIQ?

Complete Cloud Intelligence
from full DOM capture, analysis and simulated human-web activity

Always-on Detection to pinpoint cloud and digital changes, encoded insights for rapid response

Continuous Inspection discovering attack-exposed assets and exploitable components

Global Internet Graph
RiskIQ extracts and normalizes internet-scale data and includes 10+ years of data history, active crawling, asset inspection and machine learning to encode security expertise. Secure expansion beyond the firewall and identify hidden risks and threats to safeguard digital strategies.
SOLUTION OVERVIEW

With RiskIQ, enterprises safeguard digital strategies by discovering their assets outside the firewall and commanding the attack surface with global visibility and control.

No-Agent Sensor Network
identifies cloud infrastructure, apps and services, edge connections, full DOM extraction and human-web simulation

Connected Cloud Services
automated internet graphing, uncovering the global internet fabric—including third-parties, apps and services

Automated Change Detection
encoded detection logic and smart graphing across infrastructure, services, apps, code, and components

Pre-built Risk Indicators
readymade and custom metrics with statistical analysis across 200+ risk/threat indicators

Trusted Data Internet Graph
enriched asset intelligence—open ports, hosts, pages, components, CVEs, and relationships

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
Social Media Company

“...”