



Extend Vulnerability Control Beyond the Firewall

Map, monitor, and mitigate risks across your digital footprint.

THE CHALLENGE: More Digital, More Vulnerabilities

Enterprises continue to chase digital strategies—customers and clouds, partners and portals, users and apps. With so much going outside the firewall, it's only natural to lose sight of it all. The ever-expanding and evolving attack surface creates hidden risk and exposures.

Cybercriminals, with their outside-in view, can find and exploit these vulnerabilities. But security teams are left in the dark because traditional scanner and pentesting techniques lack the ability to discover unknown internet assets. Avoidable risks linger and accumulate and grow without notice.

Specific challenges include:

- Unable to discover and inventory attacker-facing, internet assets
- Limited scanning outside the firewall, unseen exposures build-up
- No change detection, missing new inventory and vulnerabilities
- Long windows of vulnerability, more breaches from unchecked exposures

THE SOLUTION: Extend Vulnerability Control Beyond the Firewall

RiskIQ continuously discovers internet assets and scores risk across the digital attack surface—no agents required. By leveraging human-web simulation and smart crawling, security teams get an 'outside-in' view of their attack surface and expand vulnerability control outside the firewall. With a clear view of their digital attack surface, vulnerability and security teams can identify unknowns, prioritize risk, and eliminate threats.

RiskIQ's Digital Footprint cuts out guesswork by automating analysis and change detection across internet assets: enterprise owned and third parties. With 10+ years of internet-scale collection and deep intelligence—full website DOM extraction, graphed relations, 157 billion connections—RiskIQ is the only solution capable of expanding vulnerability control outside the firewall: enterprise-owned assets, third parties, supply chain systems, components, and code.

WHY RISKIQ?



Comprehensive Intelligence
from a global network of smart crawlers



Always-on Monitoring to
identify changes and exposures
outside the firewall



Risk Modeling from attack
paths based on accessible
exposed assets

World-Class Architecture

RiskIQ consumes and normalizes internet-scale data, enabling vulnerability and risk teams to see internet assets and history, then continuously indexes the attack surface via change detection and automated risk analysis.

SOLUTION OVERVIEW

RiskiQ helps safeguard the digital enterprise by discovering attacker-facing, internet assets—known, unknown, or malicious—global reach to extend vulnerability risk control.



No-Agent Sensor Network

discovers attacker-facing assets—enterprise and third-party controlled and owned



Global Internet Graph

encoded logic and smart graphing: infrastructure, IP and non-IP devices, services, apps, code and components



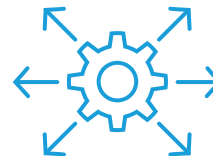
Pre-built Risk Indicators

out-of-the-box Layer-7 asset identifiers and risk indicators, custom metrics with easy-to-use visualization



Synchronous Change Detection

continuous crawling and machine learning for rapid change detection



Intelligent Integrations

extensible APIs to enriched SOC tools and workflows with context, observations, history, and insights



“RiskIQ helps us keep a handle on the growing attack surface. The company has grown tremendously in recent years and keeping track of all our digital properties is a challenge—especially the legacy assets.

We’re moving so fast that we need RiskIQ to help us grow in a healthy way.”

Chief Information Security Officer

DocuSign



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

✉ sales@riskiq.net

☎ 1 888.415.4447

Learn more at riskiq.com

Copyright © 2020 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 03_20