RISKIQ®

# RiskIQ for Government Overview

RiskIQ is the leader in Attack Surface Management (ASM), providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With RiskIQ, organizations can understand their digital attack surface, expedite investigations, assess risk, and take actions to protect their business, brand, and customers from external threats.

The company's Attack Surface Management platform combines advanced internet reconnaissance and analytics to provide unified insight and control for exploits, attacks, and adversaries across web, social, and mobile channels. Beyond superior intelligence, RiskIQ's SaaS-based solution suite allows different security teams to more efficiently identify, triage, monitor, and resolve exposures outside the firewall—taking advantage of greater collaboration, automation, and integration.

RiskIQ's solutions are easy to deploy, have broad application, and yield accelerated time to value. As a result, RiskIQ has been chosen by more than 80,000 security analysts and over 300 enterprises around the world.

## Digital Defense Challenge

Organizations have embraced web, social, and mobile mechanisms to enhance their brand stickiness, to increase customer engagement, and to facilitate employee and market interaction. Cybercriminals have gone digital, too. Today, more than 75% of attacks originate outside the firewall.

Unfortunately, today's diverse and dynamic cyber threats circumvent traditional network and endpoint security tools and place an enormous burden on information security organizations. In addition to securing the network and the assets and data that reside within it, security teams now face questions of:

- Where are, how exposed, and how compliant are my internet-facing assets and digital brand?
- How do external exploits, attackers, and adversary infrastructure relate to internally discovered suspicious activity, security events, and incidents?
- What cyber threats are attacking my business and can I manage the risk, take down external threat, and minimize operational impact?
- To what extent are other entities abusing my brand and customers?
- Is there leaked personal data on the internet that could be used to target and compromise my organisation's executives?

## RiskIQ Answer

While threat intelligence feeds can enrich internal event data, organizations need an end-to-end approach offering a more systematic, automated means to efficiently discover, triage, respond, and preempt external digital threats.

RiskIQ combines advanced internet reconnaissance and analytics, an integrated tool set, and interoperability to automate insight, collaboration and mitigation to address all the above challenges—packaged in a SaaS application suite that optimizes different tasks across security teams.

## Company Snapshot

**Industry**
Cybersecurity

**Solution**
Attack Surface Management

**Customers**
80,000+ security analysts
300+ enterprises

**Markets**
Financial Services
eCommerce
Technology
Service Providers
Retail
Healthcare
Consumer Goods
Media/Entertainment
Manufacturing
Government

**Founded**
2009

**Employees**
160+

**CEO**
Elias (Lou) Manousos

**Investors**
Summit Partners
Battery Ventures
Georgian Partners
Mass Mutual Ventures

### Our Customers are Tackling Digital Threats

RiskIQ is trusted by Fortune 500 companies, security-savvy enterprises, and popular brands across industries, as well as a growing community of thousands of security professionals.

## Mission Impact

**Reduce operational and reputation risk**
Find, monitor, and resolve your external-facing assets to reduce your digital attack surface and business exposure.

**Optimize resources**
Increase productivity through automated intelligence, proactive analytics, and mitigation workflow, as well as consolidate toolsets.

**Reduce MTTD/MTTR**
Decrease threat discovery, triage, and resolution time.

**Fortify compliance**
Proactively identify unsanctioned and malicious brand use, unknown and insufficient external system hygiene, and at risk partners.

## Government Solutions

- **Situational awareness:** Insight on how adversaries, partners, and users of your digital enterprise see you from the internet
- **Internet investigations:** Turn the content of an IOC into the context of a threat with automation and accuracy.
- **Digital orchestration:** Address threats and shadow IT on the internet.
- **Government-specific training and support:** Enable rapid deployment and consistency of internet threat awareness across teams.

## Capabilities

- **Cross-channel intelligence:** Extensive internet data sets covering public internet, deep web, brand abuse, phishing, social impersonation, and mobile telemetrics.
- **Virtual user technology:** Crawlers that emulate users to capture session details, content, relationships, and what's happening under the hood in the browser.
- **Proactive analytics:** Correlation models, data science, and research to identify and monitor new and active threat activities, adversaries, and their infrastructure.
- **Automated footprints:** Auto-generates a connected, internet-facing asset map across large and complex entities, and offers dynamic visual aids and insights.
- **Streamlined analysis:** Intuitive console with correlated data, insights, and derived analytics that expedites investigations and uncovers exploits and attackers.
- **PII/GDPR analytics:** Actively identify, assess, and monitor web assets collecting personal data.
- **Projects:** Designate and group indicators of compromise (IOC), threat artifacts, external infrastructure elements to share, monitor, update, and alert on change.
- **Integrated mitigation:** Built-in blocking, in-app enforcement, and takedown workflows resolve infringements, malicious activity, and attacker infrastructure.
- **Interoperability:** Ready-built integrations and rich API brings data and insights into your existing portfolio; SIEM, VA, GRC, Service Desk, Security Automation.

## Real Results Achieved Through Unified Internet Visibility

RiskIQ enables entry-level cyber warfighters to produce these same results with just hours of training:

- **Expanded investigations:** When Senator Claire McCaskill's staff was spear-phished by Russian actors, RiskIQ data turned one open-source IOC into a trail of breadcrumbs that led to the attacker.
- **Supply Chain attacks:** RiskIQ showed the compromised third-party supplier that helped breach Ticketmaster and identified the thousands of other affected sites.
- **Third-party components:** When a component—any framework, CMS, CDN, widget—is announced to be vulnerable, RiskIQ shows the impacted sites within minutes.
- **Crytominers:** RiskIQ alerts security teams as soon as a crypto miner is discovered on their site and shows every other .gov site running it.
- **Site relationships:** RiskIQ's crawling data showed which Turkish infrastructure and defense websites were used in an espionage waterhole attack, alerting security teams every time the malicious ttp is used anywhere else on the internet.

RISKIQ®

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

sales@riskiq.net

1 888.415.4447

**Learn more at riskiq.com**