RISKIQ®

Think Outside the Firewall™

RiskIQ® Attack Surface Management Solutions

Take Charge of Your Digital Presence and Combat Threats to Your Organization

Business Benefits

- Defend your attack surface - web, mobile, social, and deep and dark web
- Reduce operational and reputation risk
- Optimize staff and technology resources
- Accelerate time to detect and respond to targeted attacks
- Fortify risk assessment and compliance
- Prioritize risk and security gaps based on real exposure

"The intelligence provided by RiskIQ has enabled visibility and collaboration between our central and decentralized teams to continually improve our security posture and protect the bank and our customers from cyber threats."

– Robin Barnwell
Head: PBB IT Security
Standard Bank

RiskIQ catalogs, maps, and enriches the structure of the internet to let you take charge of your digital presence and combat threats to your organization.

Today's diverse cyber threats, from malware, Magecart, phishing, and targeted attacks to domain infringement, rogue mobile apps, social impersonation, and brand abuse circumvent traditional security tools and place an enormous burden on information security organizations. In fact, according to recent research, 75% of attacks on organizations originate outside the firewall. To help organizations with this immense task, RiskIQ helps answer the questions:

- What does our business look like on the internet and where are susceptible, non-compliant, or exploited internet-facing assets?
- How do internally-discovered suspicious activity and security events relate to external exploits and attackers?
- Are attackers targeting my business, employees, and customers?
- How can we automate attack surface reduction, targeted attack detection, and external threat take-down tasks?

The RiskIQ platform provides unified visibility, insight, and control for exploits, attacks, and adversaries across web, social, and mobile channels. With RiskIQ, organizations can reduce their digital attack surface and automate external threat detection to protect against targeted attacks.

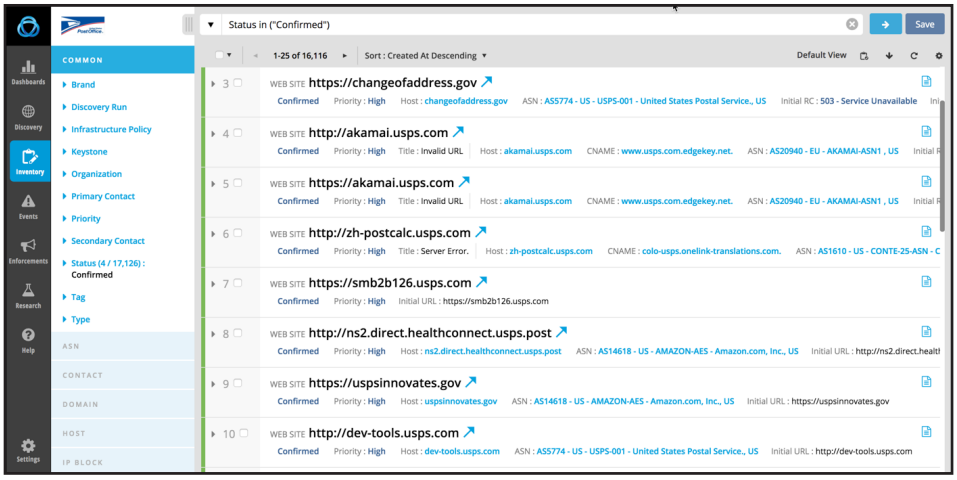
Defending Digital Transformation

As organizations embrace digital channels to enhance products and deepen customer and employee engagement, their online presence and attack surface has grown beyond the protection of the firewall. Attackers take advantage of web, social, and mobile attack vectors to gain user access credentials, obtain sensitive information, and propagate malware. Unfortunately, the sheer volume of cyber threats and exposed internet-facing digital assets have surpassed traditional defenses and security staff capacity. While security teams have amassed multiple tools and threat intelligence feeds to enrich investigation and risk analysis, their results have been lacking and breaches continue to occur. Organizations need a more automated, force-multiplier approach that includes broad internet data set collection and correlation, and a systematic means to identify and respond to targeted external threats.

RiskIQ combines advanced internet reconnaissance and analytics, an integrated toolset, and interoperability to help organizations automate attack surface visibility and targeted threat protection. RiskIQ's solutions are easy to deploy and have been chosen by more than 35,000 security analysts and over 220 enterprises around the world.

RiskIQ Digital Footprint™

Discover and Monitor your Digital Attack Surface



- Discover all internet-facing assets
- Prioritize remediation efforts using risk scores and interactive reporting
- Inventory assets and components
- Monitor assets for change or compromise
- Report on asset compliance with policies

Digital Footprint continuously discovers an inventory of your internet-exposed assets and helps reduce risk associated with your attack surface. A digital footprint is comprised of known, unknown, unsanctioned, and often poorly maintained internet-facing assets that may be susceptible to attack by external threat actors. Attackers perform reconnaissance to find and exploit unknown, vulnerable, and unmonitored internet-facing websites, applications, forms, and underlying infrastructure. The more a company extends its digital presence—directly and through affiliates—the more onerous it becomes to reduce its attack surface.

In the wild, RiskIQ detects an average of

30%

more external assets than an organization had accounted for

Digital Footprint provides automated discovery and active mapping, inventory, and monitoring capabilities needed to accurately reveal an enterprise's external risk posture. Discovered external assets are indexed, classified, and assessed in a RiskIQ inventory, providing a dynamic system of record of web infrastructure, web applications, and third-party dependencies. Digital Footprint includes the discovery and monitoring of:

- Domain names
- Websites
- Hostnames
- Web pages
- IP addresses and blocks
- Services running on over 110 ports
- Name servers
- Autonomous System Networks (ASNs)
- SSL certificates
- WHOIS contact details
- Third-party web components
- PII collection pages and forms
- Malicious or suspicious redirects
- Vulnerable web components
- and more

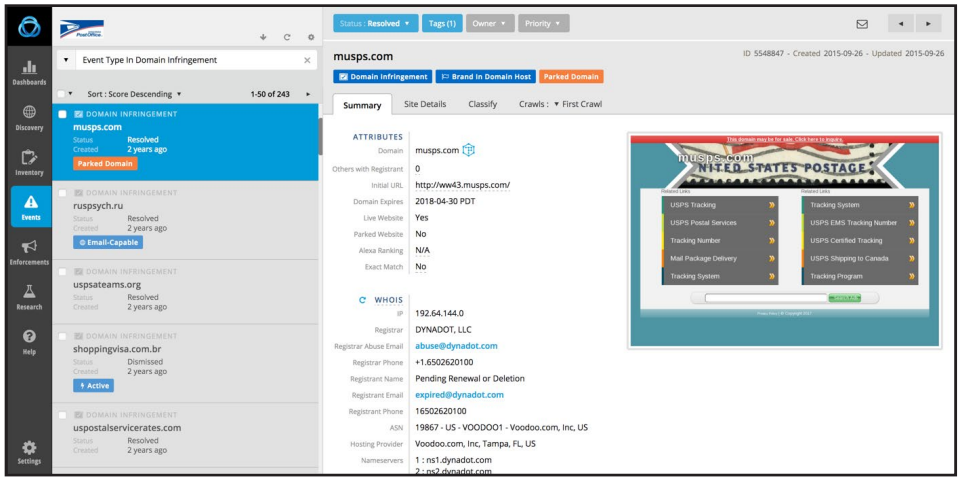
Delivering Business Value

RiskIQ is trusted by Global 1,000 companies, security-savvy enterprises, and popular brands across industries, as well as a growing community of thousands of security professionals. Our platform enables customers to:

- **Reduce operational and reputation risk.** Discover, inventory, and monitor internet-exposed assets to increase the visibility of your digital attack surface and reduce business exposure.
- **Optimize resources.** Increase productivity through automated intelligence, proactive analytics, and mitigation workflows, as well as realize toolset and data set consolidation.
- **Accelerate time to detect, respond, and preempt.** Decrease time to discover, triage, and resolve targeted external threats, even as threats are being weaponized.
- **Increase defense effectiveness.** On-demand intelligence via integration with other defense, protection, and compliance systems providing timely, accurate, and contextual awareness of external threats.
- **Fortify risk assessment and compliance.** Proactively identify unsanctioned and malicious brand use, pinpoint managed, unmanaged, and rogue external infrastructure, as well as at-risk affiliates and brand abuse that can potentially expose your business.

RiskIQ External Threats™

Detect and Mitigate Targeted Threats Across Digital Channels



- Identify targeted attacks
- Gain cross-channel threat coverage
- Automate malicious IP blocking
- Preempt threats and expedite takedowns
- Automate workflows across multiple departments

RiskIQ External Threats automates the detection, monitoring, and remediation of digital threats posed by malicious actors to your organization, employees, and customers. External Threats provides a centralized system to protect against a broad array of active attacks across web, social, and mobile vectors. Using integrated workflows, SOC and incident response analysts can take action on.

Leveraging automated analytics and workflow, External Threats eliminates manual threat detection and resolution tasks—dramatically reducing mean-time-to-resolve (MTTR). The solution automates the process of pinpointing, validating, and responding to:

- Targeted phishing
- Malicious websites
- Domain infringement
- Typosquatting
- Malware sites
- Fake social media profiles• Rogue and exploited mobile apps
- Unsanctioned brand use
- Monitoring of the deep and dark web for reference of your brand or keywords
- and more

RiskIQ can automatically block

98%

of web browsers from accessing verified phishing pages targeting your brand

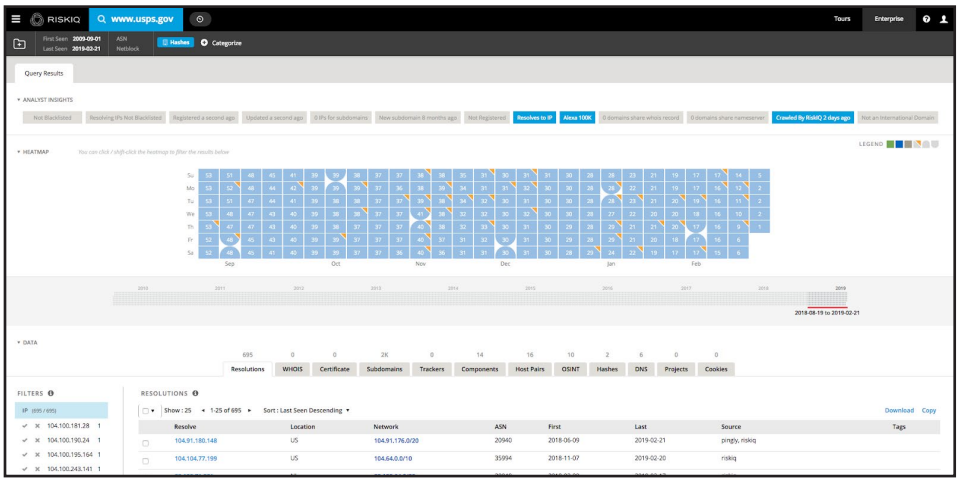
As threats are detected and confirmed, External Threats' in-app mitigation can dynamically block malicious URL access at the browser level through Google and Microsoft reputation management services. An extensive API can be used to block attacks behind the perimeter via a company's existing firewalls, proxies, SIEM, and security automation systems. RiskIQ mitigation workflows include response templates to expedite corrective actions with third party digital infrastructure providers—coordinating staff, tracking notification and correspondence, and monitoring take-down fulfillment. This type of takedown can be done within External Threats, or where authorized, by RiskIQ as a managed security service (MSS).

RiskIQ Advantages

- **Unrivaled Intelligence** Tap into the deepest, broadest internet data sets available and harness the power of RiskIQ's award-winning research, data science, and automation.
- **Force Multiplier** Give security teams and analysts access to a platform that allows them to operate more effectively by automatically correlating data across multiple data sets.
- **Work Smarter** Enable collaboration between security and incident response teams to expedite investigations and reduce time to response through workflow and project capabilities.
- **Context Matters** Enrich investigations and quickly pivot between multiple data sets in a single platform, allowing connections to be made between disparate information and data sources.

RiskIQ PassiveTotal™

Investigate, Uncover, and Analyze Internet Infrastructure



RiskIQ PassiveTotal, used by a growing community of more than 35,000 security analysts, unifies internet data sets into a single threat analysis platform, empowering security teams to accelerate investigations and eliminate threats.

Threat hunters, incident responders, and research teams need diverse internet data to understand exploits, attackers, adversary infrastructure, and their tactics, techniques, and procedures (TTPs). PassiveTotal centralizes and continuously correlates the industry's most comprehensive internet data sets and provides an easy-to-use visual interface that empowers analysts to more proficiently examine, validate, share, and monitor digital threats.

Analysts can take advantage of derived intelligence, threat classifications, and historical record preservation—enabling them to rapidly pivot across sources and time to understand past, immediate, and imminent threats. The solution correlates extensive internet data sets, including:

- Passive DNS and historical resolutions
- WHOIS registration and contact details, including historic data
- Website components and web trackers found within web pages
- New domains, subdomains, and hosts
- SSL certificate information
- Host pairs derived from web crawlers to see internet relationships
- Website cookie and tracker information
- Malicious sites, exploits, and actors
- Open source intelligence (OSINT)
- and more

- Expedite investigations and reduce incident response time
- Gain comprehensive threat and adversary infrastructure intelligence
- Enrich context of internal security systems
- Escalate and share research findings
- Monitor artifact and insight changes

84%

of surveyed organizations found PassiveTotal to be more comprehensive than other security data sources and 46% reduced response times of validating incidents by 25-50% or more

PassiveTotal® Projects permit analysts to share and contribute investigations publicly or privately within their organization—with means to monitor and be alerted to any changes including new contributions or changes in artifacts. In addition, API and integrations allow PassiveTotal to enrich threat context for other systems.

RISKIQ®

RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn how the RiskIQ could help protect your digital presence by scheduling a demo today.

22 Battery Street, 10th Floor
San Francisco, CA. 94011

sales@riskiq.net
RiskIQ.com
1 888.415.4447
@RiskIQ