# RiskIQ External Threats®

## Brand Protection

Business has evolved. More processes and interactions happen online, cybercriminals are exploiting digital channels to launch new types of attacks. This includes a two-fold threat: directly on assets and shadow attacks like ***phishing sites, typosquatting, rogue mobile apps, impersonation on social media, scams,*** and ***brand-trap malware*** that hijack the organization's digital identity and replace it with fakes to steal data, and in some cases, cash.

Unlike incomplete and outdated intel feeds, RiskIQ includes full internet history and curated intelligence to identify threats faster and eliminate the hijackers. RiskIQ gives customers confidence, speed, and scale to find and remediate these external threats—backed by 10+ years of mapping the whole internet.

## Dashboards and Reporting

RiskIQ provides intuitive dashboards and robust reporting to provide insights into threat detection across all threat-types and channels, as well as the effectiveness of triage and mitigation processes in every stage of the threat event life cycle.

- On-demand executive summary reports and real time snapshot of the current state of an organization's global presence and active threats against it
- Custom reports and data drill-down with key metrics include:
    - Event generation for a specific period
    - Current review status and status change history
    - Event uptime until resolution and time elapsed during each stage of the threat lifecycle
    - Events grouped by website, app store, social network, or other shared characteristic
    - Events grouped by brand, priority, or other custom tags
    - Geographic distribution of events

## Benefits

- Automatic monitoring and enrichment to continually contextualize threats to your environment
- Full visibility into threats to your business, brand, and customers
- Fewer false positives, more efficient threat triage
- Faster, more holistic risk and threat response
- Integrate, enrich and scale existing security tools
- Decreased event uptime and customer exposure to live threats
- Insights into threat sources and/or response bottlenecks to inform resource investment and improve processes

## Only from RiskIQ: Detecting External and Brand Threats

RiskIQ absorbed internet security intelligence via human-web simulation and smart crawling—a unique combination to detect threats to brands and customers.

Powered by the RiskIQ Illuminate® Platform, infrastructure associated with your brand and organization—including third parties. Detection logic for brand-related infrastructure that creates a complete and adaptive watchlist, so teams can take down threats and spend less time sorting through false-positives or alerts from benign shadow IT.

RiskIQ simulates human-web interactions to discover threats across the internet: search and click websites, social media profiles, and mobile apps around the world. And since there are multiple attack paths, RiskIQ explores the broad range of egress points, browsers, device-types, and behavior algorithms to optimize detection; unraveling obfuscation techniques such as geo-targeting or browser fingerprinting.

Our no-agent sensor network records the full browser session, including all redirects, script calls and executions, along with links or embedded page content, components and code—providing actionable digital forensics capture for observed malicious behavior and fraud.

Finally, RiskIQ's attacker-aware machine learning infused security expertise, transforms internet observations into discrete scoring for reputation, weaponization, and services history to contextualize and verify who is attacking and the tools they're using against you.

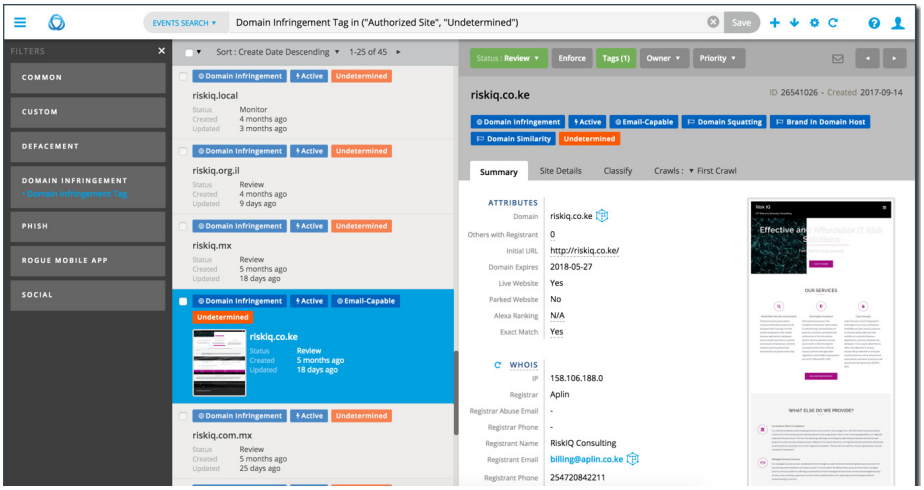


Fig. 1: External Threats user interface showing event details, screenshots, and event history.

## Featured Solutions

- Comprehensive, ongoing detection across web, mobile, and social channels
- Comprehensive and customizable reporting on threat lifecycle metrics and metadata
- Efficient case management and response
- Integrations with SIEM, SOAR, and Remediation endpoints
- Includes support for your team from dedicated team of experts in the field
- Customizable reporting on threat lifecycle metrics and metadata
- Efficient case management and remediation workflow
- Flexible policy framework and granular controls to customize and fine-tune detection rules
- Robust API access and easy integrations with SIEM, SOAR, and other security tools

## Easy Mitigation and Response Workflow

Once threats are detected, they must be addressed—and fast. RiskIQ provides a range of alerting options and UI or API-based workflows to easily assign ownership, add notes and tags, get feedback from other business units, and automatically generate and send takedown notifications or content removal requests to the appropriate parties as well as track all responses and correspondence.

RiskIQ has direct relationships with some of the largest hosting providers, social networks, and mobile app stores. The platform also integrates into Google Safe Browsing and Microsoft SmartScreen to enable automated blocking of phishing pages to 95 percent of internet users across the internet to neutralize phishing threats within minutes at the browser level.

Automated continuous monitoring of online resources lets customers know when events have changed threat level or been successfully remediated, and RiskIQ's post-resolution monitoring automatically alerts you and reopens events for threats reemerging from previous detection.

## Available Add-Ons:

### Managed Intelligence Services (MIS)

The External Threats - Advanced add-on enables organizations to adapt the broad capabilities of the RiskIQ platform and the expertise of RiskIQ Solutions Architect and Managed Intelligence Services (MIS) teams to automate detection and monitoring for use-cases that require a deeper understanding of the business to identify and respond to appropriately, including:  compromised data, fraudulent social media posts, and brand tarnishment (association of brand names or trademarks with illegal or offensive content).

### Deep and Dark Web

The External Threats - Deep and Dark Web add-on provides clients visibility into mentions of their company names or other keywords of interest on the deep and dark web. Data is sourced via Flashpoint, a RiskIQ partner organization specializing in monitoring the deep and dark web, and sent to the RiskIQ platform, so that it can be viewed side-by-side with threats on the open web. Viewing different pieces of the puzzle together enables organizations to draw additional insights from connections in the data and track a threat from planning and discussion stages in forums through to the actions taken and infrastructure used on the open web to launch the attack. This add-on is available for free to mutual customers of RiskIQ and Flashpoint with an existing valid Flashpoint API key, or API access can be purchased through RiskIQ, provided the customer has not terminated a contract with Flashpoint within the last 12 months.

RISKIQ®

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

sales@riskiq.net
1 888.415.4447

**Learn more at riskiq.com**