Think Outside the Firewall™

External Threats™

Detect and Respond to Digital Threats

Features

- Web, mobile, and social digital channel coverage
- Built-in blocking and mitigation technology to remediate threats
- Monitoring to ensure takedowns are effective and don't resurface
- API integration to ticketing and SIEM systems to manage threats

Benefits

- Comprehensive detection of threats to your business, brand, and customers
- Near real-time, browser-level blocking of time-sensitive threats
- In-app mitigation workflow to enable fast triage and takedown of threats

External Threats Modules:

- Domain threats
- Phishing threats
- Mobile app threats
- Social threats to brand
- Social threats to executives
- Brand tarnishment
- Data leakage
- Phone phishing
- Email spoofing
- Remote Deposit Capture fraud

Business is Embracing Digital—so are Cybercriminals

As business evolves and moves more processes and interactions online, cybercriminals are exploiting these digital channels to phish and scam customers for data and money, infringe on your brand's value, hijack mobile apps, and impersonate your brand and your executives.

RiskIQ provides the comprehensive coverage across all digital channels to detect threats against your business, brand, and customers that might impact your organization. Utilizing virtual user technology, advanced machine learning, and petabytes of RiskIQ internet data, RiskIQ External Threats™ finds imposters to your domain and branded terms, social profiles, and mobile apps.

Active Monitoring of the Internet

Detecting threats across the vastness of the internet is a daunting task. With hundreds of thousands of new web pages created every day—not to mention the billions that already exist—understanding which of these pages, apps, and social profiles are a threat to your business is critical to protecting your organization.

RiskIQ provides this insight by crawling and indexing millions of pages every day with our virtual users, automatically detecting threats that are present on pages while evading the detection of advanced adversaries.

RiskIQ External Threats provides organizations the capability to monitor digital channels and detect advanced threats like:

- Domain squatting and typosquatting
- Phishing against customers
- Imposter social media accounts
- Data leakage
- Compromised and rogue mobile apps
- Brand tarnishment and misuse
- Remote deposit capture and card cracking fraud

How Does RiskIQ Detect External Threats?

RiskIQ External Threats uses virtual user technology as it crawls the internet, experiencing websites, social media profiles, and mobile apps just like a real user does. RiskIQ virtual users visit websites from thousands of IP addresses originating from around the world, using different browser and device types. This technique evades detection from advanced threat actors who are watching for automated crawling technology, leaving the threat actors nowhere to hide.

When virtual users arrive at a page, they capture and catalog everything that happens when that page is loaded. The perspective of a virtual user provides visibility into known bad or blacklisted sites, drive-by downloads, or other malicious redirects. This allows you to accurately identify, monitor, and mitigate digital threats against you across the internet.

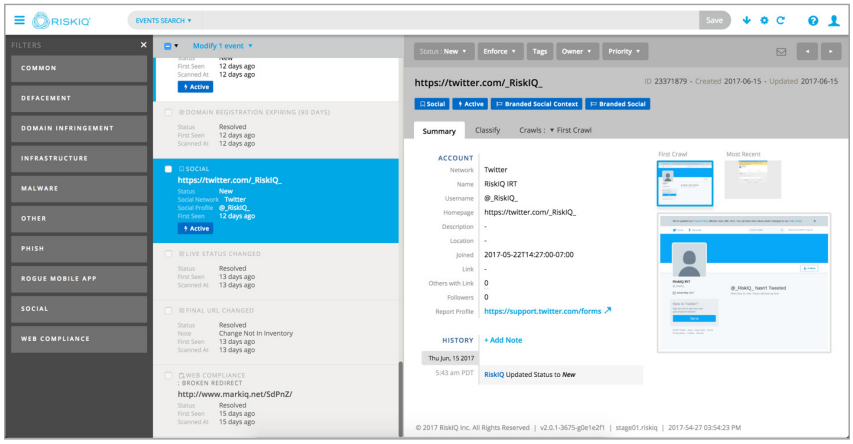

Fig. 1: External Threats user interface showing event details, screenshots, and event history.

Across other digital channels, RiskIQ has integrations with the most popular social media platforms and over 150 app stores around the world to enable visibility and fast, comprehensive response to threats.

Easy Mitigation and Response Workflow

Once threats are detected, they must be addressed—and fast. Depending on the type and location of the threat, the response needs to be dynamic. Domain Threats that directly infringe on your brand and identity must be addressed from both a takedown and legal perspective to protect your organization. Social and Mobile Threats need to have the infringing profile or mobile app removed from the social platform or app store. Phishing pages need to be blocked and taken down as quickly as possible.

RiskIQ has direct relationships with some of the largest hosting providers, social networks, and mobile app stores. The platform also integrates with Google Safe Browsing and Microsoft SmartScreen to enable automated blocking of phishing pages to 95% of internet users across the internet faster than a takedown request.

RiskIQ can automatically block

98%

of web browsers from accessing verified phishing pages

External Threat Dashboard and Reporting

RiskIQ provides an intuitive dashboard for monitoring the internet for External Threats across social media, web, and mobile app stores as well as tracking enforcement and resolution. The reporting includes:

- Executive summary reports and a snapshot of the current state of an organization's global presence and threats against it
- Trends and benchmarks of threat management improvements over time
- 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
  - Events by website, app store, and social network
  - Brands associated to events
  - Geographic distribution of events

RISKIQ

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

RiskIQ is the leader in digital threat management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 75 percent of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social, and mobile exposures. Trusted by thousands of security analysts, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action to protect business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures.

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

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