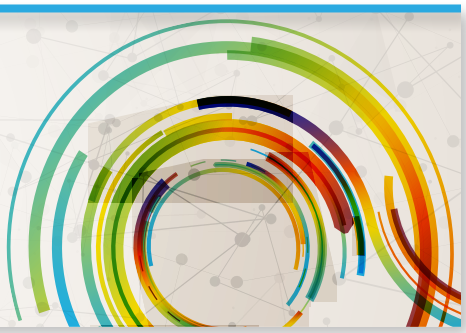
DATASHEET

EXTERNAL THREATS - SOCIAL

Social Threats Aren't Your Friend

MONITOR THE LEADING SOCIAL MEDIA PLATFORMS

Monitor social networks to protect your customers and brand



In the age of social media, having an advanced social threat detection and mitigation strategy is critical. The low barriers to entry and high visibility of social media make it a powerful tool for threat actors seeking large audiences to commit fraud, steal information and credentials, distribute malware, and misrepresent brands and high-profile individuals.

RiskIQ Social Threats solution set taps our proprietary virtual user technology to offer an enterprise-level solution that detects and mitigates social media-based threats against an organization, its employees, and its customers. Powered by advanced analytics, our platform correlates and contextualizes threats in all social media channels for comprehensive threat detection.

SOCIAL MEDIA PRESENTS A UNIQUE ATTACK VECTOR

Social media provides brands with opportunities for customer engagement and feedback that can lead to product and service improvements. However, this two-way accessibility between brands and consumers can be a weakness as well as an advantage—and serve as a powerful weapon in the hands of threat actors.

Social media impersonation, fraud, and abuse are particularly impactful because most users are less aware of threats and fraudulent activity on social media than other attack vectors, such as email. Brands who have a broad customers base, valuable data, or high-profile executives are most vulnerable, especially across industries such as:

- Financial institutions and payment providers
- Health insurance providers
- Internet, e-commerce, tech, and software companies
- Consumer goods and retail companies
- Media and entertainment companies
- Government agencies

ASSESS AND TRIAGE THREATS

Easy-to-access dashboard for security teams to investigate social threats and determine the appropriate response. Rapid assessment of the social threat with full details in a quick snapshot

IN-APP WORKFLOWS TO MITIGATE

Respond quickly with actionable alerts and minimize impact by providing in-app workflows to contact social media platforms for imposter or brand abusing account removal

CONTINUOUS MONITORING

Ensure successful removal of imposter and brand abuse accounts, and monitor for tenacious threats that may pose recurring risk

EXTERNAL THREATS - SOCIAL

HOW DOES RISKIQ SOCIAL THREATS WORK?

Today's cyber threat actors attack brands and their customers through the same social media networks consumers use to interact with trusted brands. RiskIQ Social Threats provides discovery across a broad range of social media networks including Facebook, Twitter, LinkedIn, Instagram, Google+, Pinterest, and YouTube.

By experiencing the same content encountered by real social media users, RiskIQ's unique virtual user technology uncovers social media-based threats missed by less covert detection methods. With it, organizations can:

- Detect brand or executive impersonation aiming to phish for sensitive information or direct users to malware-infected sites
- Prevent unauthorized accounts from undermining social media marketing efforts, which confuses users and competes with authentic profiles
- Detect accounts that associate a brand or executive with offensive or illegal content
- Intelligently sort authentic profiles and legitimate brand mentions from fraudulent accounts and violations of social media usage policies.

REPORT ON SOCIAL THREAT POSTURE

RiskIQ provides an intuitive dashboard and reporting options for monitoring and investigating social threats and enforcement, which includes:

- Executive summary reports and a snapshot of the current state of an organization's social presence
- Trends and benchmarks of social media security improvements over time
- Custom reports and data drill-down with key metrics include:
  - Policy violation type
  - Event generation time period
  - Current review status and status change history
  - Event uptime until resolution
  - Event source and social network
  - Brands associated to events

A HOLISTIC PERSPECTIVE: CONTEXTUALIZE THREATS ACROSS DIGITAL CHANNELS

Effective digital threat management doesn't focus on only one digital channel. Threat actors use the web, mobile, and social channels to phish for credentials, conduct fraud, distribute malware, and carry out abusive activities. Cross-promoting their attack vectors among web, mobile, and social channels maximizes each attack's impact. Solutions that address social threats in isolation cannot contextualize the full extent of the threat.

As a leading provider of security services for phishing, malware, web and mobile application, and digital ad-based threats, RiskIQ is uniquely positioned to provide security teams with an enhanced perspective of social media-based threats. With our platform, organizations gain unparalleled visibility into threats impacting a brand and its customers across all digital channels through a single of pane of glass.

ABOUT RISKIQ

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.

riskiq.com • 22 Battery Street, 10th Floor, San Francisco, CA 94111, USA • sales@riskiq.com • 1.888.415.4447