RiskIQ Threat Detection Suite

Visibility from the Attacker's Perspective

RISKIQ®

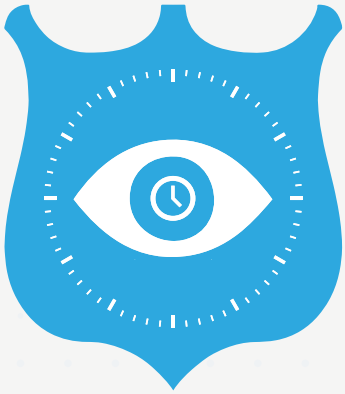
An Attacker's View From Outside Your Firewall Enables Them to Threaten Your Organization by Taking Advantage Its Ever-expanding Web, Mobile, and Social Presence

Powered by our unique virtual-user technology, threat analysis engine, and global proxy network, our External Threat Detection Product Suite gives organizations an actionable, real-time view of both their and their adversaries' infrastructure. With this comprehensive view of their attack surface, organizations can proactively defend against threats that target their websites, mobile applications, customers, employees, and social presences.

Interacting with web, mobile, and social properties as a real user would, RiskIQ technology disarms attackers' evasion techniques while collecting user session data to detect phishing, fraudulent apps and content, domain infringement, malware, and more—all at scale. RiskIQ packages this incredible amount of data into actionable, event-based threat alerts and workflows.

Monitor and Enforce

By continuously monitoring the entire web at scale, RiskIQ technology can reduce personnel resources, improve accuracy and minimize costs. We provide a holistic view of the external threat landscape, at scale, in one pane of glass, enabling cross-team reporting and mitigation. RiskIQ offers:



- A comprehensive, multidimensional view of campaigns enables accurate detection, fast remediation and proactive blocking of attacks. By illuminating what were formerly blind assets, RiskIQ allows you to put policy under them and gain control.
- Industry scoring and vertical comparison tools offer the ability to compare your company's web asset security within your industry and against your competitors to see the business units performing the best and report on ROI.

RiskIQ Anti-Phishing

RiskIQ's Anti-Phishing solution detects and combats phishing attacks and sends automated alerts and analysis to security, cybercrime, and incident-response teams to mitigate phishing's impact on a company.

Our anti-phishing technology continuously scans web pages, industry and proprietary feeds, client-abuse boxes, DMARC feeds, referrer log analysis, and social media for evidence of phishing. Our proprietary machine-learning classification algorithm and virtual-user technology find and confirm unreported phishing pages at unprecedented rates.

With more than 95% accuracy in identifying phish, companies using RiskIQ won't waste time with false positives while live phish await verification. We eliminate the need for large-scale manual reviews associated with alternative solutions, where accuracy rates are in the single digits. RiskIQ Anti-Phishing dramatically shortens not only time to mitigation per phish, but also overall Phish uptime, offering organizations:

- Comprehensive detection of phish targeting their brands and customers across a wide variety of standard and unique sources
- Ability to bypass advanced phishing obfuscation and targeting techniques based on user location, referring URL, browser/device-type, or browsing behaviors that elude other crawling methods
- Unparalleled accuracy of detection and automated workflow to shorten time to mitigation per phish and minimize overall business impact

RiskIQ Mobile Threats

The size, complexity, and dynamic nature of the global app store ecosystem make it increasingly difficult for brands to monitor their mobile presence and protect their customers from fraud. Once published, mobile apps can rapidly proliferate from official stores throughout the app store ecosystem, spreading to new stores and web download locations without the developer's knowledge or consent.

RiskIQ Mobile Threats provides discovery across all major app stores as well as 150+ unofficial app stores, including focused coverage of high-risk stores and regions for brand impersonation, malware, and fraud.

In addition to unparalleled coverage of third-party app stores worldwide, RiskIQ incorporates a unique source of "feral app" binaries, or mobile apps collected outside of dedicated mobile app stores—via drive-by download, for example. With this comprehensive mobile presence knowledge organizations have the unparalleled ability to:

- Monitor Google Play, Apple iTunes, and 150+ high risk, unofficial app stores around the world to uncover rogue mobile apps
- Intelligently sort legitimate apps from modified versions, unauthorized fakes, and look-a-likes
- Go beyond just the title and description, automatically analyzing all app content and code to and discover logos, brand references, and malicious code hidden within app files
- Track app versions and correlate apps across stores for efficient management and enforcement of related incidents

RiskIQ Social Threats

In the age of social media, having an advanced social threat detection strategy is critical. The low barriers to entry and high visibility inherent to social media make it a powerful tool for threat actors seeking large audiences with which to commit fraud.

RiskIQ External Threat Detection: Social Threats taps our proprietary virtual-user technology to offer an enterprise-level solution that detects and eliminates social media-based threats against an organization, its employees, and its customers. Our platform correlates and contextualizes threats in all social media channels with other web and mobile data for comprehensive threat detection.

By experiencing the same content encountered by real social media users, RiskIQ's unique virtual technology uncovers social media-based threats missed by other 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

RiskIQ Domain Threats

As brands increasingly transact business and engage with customers through their website, having an advanced domain infringement detection strategy is critical. Threat actors can register domains using trusted brand names to drive monetizable traffic to other sites, phish for sensitive data, distribute malware, sell counterfeit goods and more.

RiskIQ Threat Detection Suite

Visibility from the Attacker's Perspective

RiskIQ Domain Threats detects the unauthorized use of brands within third-party registered domain names and continuously monitors their site content and behavior so organizations can prioritize infringements according to their brand impact and act quickly to protect itself and its customers.
After identifying an infringing domain, RiskIQ's unique virtual-user crawling infrastructure intelligently analyzes the website associated with it and provides the additional context needed to determine how threat actors may be using each domain, and the risk it poses to the associated organization. Unlike other domain infringement solutions, RiskIQ Domain Threats offers:

- Detect brand impersonation, traffic diversion, phishing, malware distribution, and other types of abuse occurring on infringing domains
- Continuously monitor evolving threats over time and create granular policy controls around site metadata, behavior, and page content to group and prioritize infringements
- Intelligently sort company-owned domains and legitimate web pages from infringement and fraud for more accurate recognition of threats
- Automatically contextualize threats with knowledge of related incidents to gain insight into how criminals are using an infringing domain and how to stop them

Purchase RiskIQ's External Threat Detection Suite for a comprehensive solution or mix and match the offerings to suit your specific needs.

RISKIQ PROTECTS CORPORATE BRANDS AND THEIR CUSTOMERS ON THE INTERNET. The company combines a worldwide proxy network with synthetic clients that emulate real users to monitor, detect and take down malicious and copycat apps, drive by malware and malvertisements. RiskIQ is being used by leading financial institutions and brands in the US to protect their web assets, visitors, employees, and customers from security threats and fraud. To learn more about RiskIQ, visit www.riskiq.com.