



# RiskIQ Managed Security Services (MSS)

## You Manage Your Business, We'll Mitigate Your External Threats

As business continues to push for digital transformation, threat actors have focused efforts to exploit an organization's growing digital attack surface. With enterprises attempting to make sense from a multitude of tools, threat feeds, and data sets, managing external threats can seem like a daunting, impossible task. The exposure and response capability is exacerbated by the low number and high cost of available qualified cybersecurity professionals.

RiskIQ Managed Security Services (MSS) enables organizations to gain digital threat detection, triage, and protection capabilities in a fast and scalable way, without the burden of training, onboarding, or extended support.

RiskIQ is the leader in Attack Surface Management, providing the most comprehensive discovery, intelligence, and mitigation of external threats associated with an organization's digital presence. Our platform provides unified visibility, insight, and control for exploits, attacks, and adversaries across web, social, and mobile channels. With RiskIQ, organizations can understand, assess, and reduce their digital attack surface, and automate external threat investigation and protection against targeted attacks.

### Rapid Time to Value

RiskIQ Managed Security Services (MSS) ensures that an organization can have an immediate capacity and expertise to mitigate external threats from the moment we activate your detection modules, negating security staffing shortages, program deadlines, or competing internal priorities.

With RiskIQ MSS, security analysts from RiskIQ operate our Attack Surface Management platform on your behalf, monitoring the web, social, and mobile attack vectors for external threat events and responding appropriately based on best practices and your specific requirements. There is no time lost in onboarding or training your team on the platform or processes to detect and mitigate threats using RiskIQ. This allows your organization to almost instantly bring your attack surface management program online and reduce business and reputational risk from external threats.

### Features

- RiskIQ's Incident Response Team (IRT) manages your external threats alerts, triage, and mitigation
- Receive monthly briefings about external threats targeting your organization
- Immediation protection that preserves your security headcount

### Benefits

- Optimize costs associated with your digital threat management program
- Utilize the expertise of RiskIQ analysts to detect and mitigate threats
- Immediately add security response capacity without the need to allocate existing security professionals to the task of digital threat management

### RiskIQ 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

### Expedited Triage and Review of External Threats

With RiskIQ MSS, a RiskIQ security analyst will review any external threat events that are likely to be connected with your organization. These events are tied to the modules that your organization has purchased, such as anti-phishing, social threats, or mobile threats. The RiskIQ security analyst will determine whether your organization is being targeted, attacked, or exploited, and based on policy, can escalate an external threat event for immediate mitigation or for your staff to review if a determination cannot be made.

### Take Automated or Semi-automated Action on Threats

If a RiskIQ security analyst determines that an external threat is targeting your organization, they will take action to resolve the threat from the internet, social media network, or mobile app store. This process can be tailored to your own organization's workflow or can be handled according to best practices.

Action on threats generally takes the form of sending documentation and a takedown request to the hosting provider, ISP, social media network, mobile app store, or platform provider, in addition to documenting the correspondence via the RiskIQ platform. Depending on the threat, RiskIQ can also send malicious URLs and supporting evidence to reputation services from Google and Microsoft to block the threat to customers and employees at the browser level. RiskIQ MSS will monitor threats to ensure that they're removed from being active, as well as monitor for the threats should they come back online in the future.

### Reporting on Program Status and Threats

For RiskIQ MSS customers, our IRT and customer success team will schedule regular meetings with key security personnel at a cadence set by your security organization. Customers can be updated on the status of external threats on a monthly or quarterly basis and have urgent matters escalated when necessary. A complement of management and operational reports are also delivered in scheduled intervals.

\* The State of Enterprise Digital Defense conducted by IDG Connect - 465 survey respondents



#### RiskIQ, Inc.

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

✉ sales@riskiq.net

☎ 1 888.415.4447

[Learn more at riskiq.com](https://www.riskiq.com)

Copyright © 2019 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 11\_19