RISKIQ®

RiskIQ vs. Digital Shadows

Internet-scale Automation vs. Manual Threat Intel

How an organization looks online is always changing via a wide range of factors, both legitimate and malicious.

As companies grow, it's increasingly challenging for security teams to stay on top of the day-to-day activities of far-flung partners, vendors, and internal teams and business units. These groups continuously create and alter digital assets, many of which are outside the official protocol. At the same time, threat actors create rogue assets meant to mimic their brands, such as fake branded websites, mobile apps, and social media accounts that fool customers and prospects and steal sensitive information or distribute malware.

In response, security teams have turned to a handful of vendors claiming to provide visibility into the immensity of the internet so they can understand their own presence as well as detect attacks happening in the wild. Two of these vendors are Digital Shadows and RiskIQ.

These two vendors claim to do similar things in the space of attack surface reduction and digital risk management, but in this article, we'll outline three enormous differences in how they go about it, which may affect your decision about which is right for your organization.

1. Monitoring

Businesses want a real-time view of their internet-exposed attack surface as it appears to hackers. With a catalog of everything that's part of their infrastructure, security teams can bring previously unknown assets under management, verify the security and compliance of what belongs to them, and identify what may be fraudulent, including websites, mobile apps, URLs, web page content, ASNs, IPs, and nameservers. They can also know when and how they're being targeted on the open internet.

How RiskIQ and Digital Shadows go about doing these things for their customers is the first key difference between them.

Digital Shadows takes a "managed service"-oriented approach to monitor a customer's attack surface exposure online. Customers submit their keyword assets to be monitored to Digital Shadows, which then monitors for mentions of exposures against third-party data sources on the open web, dark web, and social media as well as infrastructure search engines such as Shodan.io. Digital shadows analysts compose reports for each textual exposure they find, along with detailed guidance about how to mitigate or eliminate the exposure.

RiskIQ takes a different approach. Instead of relying on querying keywords against third-party sources, RiskIQ acts as the search engine itself, crawling and indexing the internet on a telemetric level, collecting web data from interactions with internet infrastructure so it can build connections and identify unseen relationships

between what your organization owns. Rather than only monitoring assets that have been mentioned textually, RiskIQ uses a network of crawlers, sensors, and proxy users to crawl and download web pages, experiencing them like a real user (or attacker performing reconnaissance) does from a variety of different perspectives, at scale.

With a network of tens of thousands of these virtual users, RiskIQ scans millions of web pages per hour, creating telemetry data to produce a dynamic index of an attack surface, all branching out from one keystone asset. In essence, rather than customers telling RiskIQ about their attack surface, RiskIQ tells them about it while going beyond the use of exposed text.

2. Detection

As similar to many threat intelligence outfits, Digital Shadows' detection is based around detection of keywords and textual mentions—they search for indications of attacks, leakage of data, and brand abuse on the open internet, social media and dark web much like how you would type a term into Google. Digital Shadows' analysts review the search results and build reports around each finding so your team can assess the threat or exposure and take action. Consider it a comprehensive threat intelligence report; an encyclopedia of things that could harm your business.

In contrast, after mapping your attack surface via relationships between web components beyond textual mentions, RiskIQ actively monitors it for threats with the telemetric internet data collected by its networks of crawlers. These crawlers emulate human users with a fully instrumented browser and algorithms to simulate human-like mouse movements and click behavior. This automation stores the entire chain of events that may have led to an attack, such as a redirect sequence on a phishing page to determine when, where, and how an attack is taking place. Basically, instead of writing an encyclopedia of threats that may be targeting your business you can reference, RiskIQ writes an encyclopedia of your business.

3. Analysis

Attackers use automation to launch sophisticated attacks by cheaply developing and rotating infrastructure at internet scale. Correlating threat data extracted from a broad set of data sources across channels helps uncover these threats. Digital Shadows takes an analyst-driven approach to this endeavor.

Viewing the process through the lens of the classic intelligence cycle, analysts at Digital Shadows are part of the processing, analysis and dissemination stages, filtering through hits on keyword searches to generate alerts for security teams. For each alert, analysts give customers context and guidance, including intelligence gathered from open source channels around each threat.

RiskIQ believes in an internet-scale approach to defense, with advanced analytics and machine learning built into its platform to process the data its crawling infrastructure collects in near real time with as little false positives as possible. This automatically triages and addresses security events and tracks changes in threat infrastructure to help predict new attack vectors as they emerge. While human analysts are a part of the process for RiskIQ, their role is mainly to hone the machine learning models and enable the customer to action events in scenarios where manpower is limited.

4. Data

Data is crucial in defending an attack surface from modern internet-scale threat campaigns, and there are hundreds of data sources available to security vendors. Digital Shadows relies on data from a variety of sources on the open web and social media to create their alerts.

A key feature of RiskIQ's Attack Surface Management platform is its worldwide network of web crawlers, which continuously crawl the internet collecting rendered pages and the entire sequence of requests and responses that make up a web page—the composition of webpage, the full DOM, javascript, headers, dependent requests, certificates, components, trackers, etc.

These crawls have been collecting internet data for over ten years, which is stored and owned by RiskIQ. RiskIQ aggregates these massive repositories of telemetry data in datasets that enable them to map customers' attack surfaces and monitor them for threats. As opposed to relying on third-party data, RiskIQ is the source and owner of the telemetry and data used to enable customers to reduce their risk online tangibly.

RiskIQ vs. Digital Shadows

for Attack Surface Management

Solution Coverage

Low ..... High

	RiskIQ	Digital Shadows
Monitoring	●	◔
Detection	●	◔
Analysis	●	◕
Data	●	◔

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

sales@riskiq.net
1 888.415.4447

Learn more at 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