SOLUTION BRIEF

RISKIQ®

RiskIQ for Compliance

Know Where You’re Covered, and Where You’re Not

With the drastic increase in cyberattacks against organizations and customers, regulatory agencies and governing bodies are strictly enforcing compliance requirements and holding organizations accountable for violations of those rules and regulations.

Organizations that implement frameworks or regulations from NIST, NERC, FISMA, or PCI are all required to maintain asset inventories that detail the location, accessibility, patch level, and ownership of the assets. These requirements cover all digital assets, including those that exist outside the firewall and outside traditional vulnerability scanning technologies.

To meet these requirements, organizations need a complete and continuously updated view of their digital assets across web, mobile, and social environments through a single pane of glass.

> “The company has grown tremendously in recent years and keeping track of all our digital properties is a challenge—especially the legacy assets. We’re moving so fast that we need tools like those from RiskIQ to help us grow in a healthy way.”
>
> – Vanessa Pegueros, VP and Chief Information Security Officer
> DocuSign

Be Proactive with Compliance

To provide a continuously updated inventory of external-facing digital assets, RiskIQ’s proprietary discovery technology automatically identifies and indexes company-owned digital assets—including shadow IT, third-party code, and component relationships and dependencies between assets. With this view, organizations know:

- What networks the digital assets live on, and where they’re hosted
- Which digital assets are running weak software or configurations
- Which digital assets violate internal and external regulatory policies

Diving into the Data

>80%

Percentage of the incidents that lead to data breaches come from external sources, According to the 2016 Verizon Data Breach and Incident Report

50%

Approximate percentage of those incidents target unknown (and thus unmanaged) digital assets

76%

Percentage of the corporate websites they scanned had vulnerabilities, according to Symantec's 2016 Threat Report

With RiskIQ, Be Able To:

Verify compliance with a given policy in real time. Prepare for audits and perform reporting on the inventory and the state of assets under management.

Reduce the burden of compliance audits. With additional visibility for page-level policies, organizations can instantly search and pivot within asset inventory to locate or remediate all pages containing issues such as vulnerable frameworks or unauthorized third-party web components.

Enrich existing governance tools. Continuous monitoring from the perspective of end-users interacting with company websites, social media profiles, and branded mobile apps complements compliance tools and provides added visibility into their current state and behavior in-the-wild.

Automate the task of tracking all owned assets such as SSL certificates, which sites they are associated with, and their expiration status. The RiskIQ External Threat Management platform sends real-time alerts about gaps in security and compliance.

Support the initial audit process for mergers and acquisitions with RiskIQ, identifying all websites belonging to an organization, including pages that collect data. RiskIQ also flags situations where data collection is not encrypted, or SSL is configured incorrectly.

RiskIQ also helps the acquiring organization identify the shadow IT and applications unknown to the security team of the organization being acquired, as well as applications not listed in spreadsheets.

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

✉ sales@riskiq.net
☎ 1 888.415.4447

Learn more at riskiq.com