



# RiskIQ Digital Footprint® Risk Reporting

## Prioritize Risk Mitigation With Up to Date Threat Indicators and Security Posture

With the explosion of digital engagement, public breaches, and data privacy mandates, information security organizations are challenged with how to quantify risk associated with their digital presence. Organizations need a way to quantify the current state of their external attack surface, how well they are managing exposures within their internet-facing assets, and how their digital business ecosystem affects their overall cyber risk posture.

RiskIQ Digital Footprint® Risk Reporting provides management and security teams with an easy to understand, accurate, and interactive view into their organization's digital risk posture. RiskIQ's risk-reporting capabilities take advantage of advanced internet reconnaissance and predictive analytics technology that deliver comprehensive external asset inventory, threat discovery, and risk insights. As a result, organizations can measure, track and benchmark their digital security posture - with confidence that findings are an accurate depiction of exposure to external threats from an attacker's perspective and allow for efficient corrective action.

### Digital Footprint Risk Reporting is:

**Easy** - simple, numerical score, intuitive findings, and interactive online report

**Extensive** - drill down from executive-level scoring into risk component-levels, and even further to examine external asset and cyber threat elements.

**Accurate** - active reconnaissance, component and threat analytics ensures precise insights

**Actionable** - predictive analytics and detailed inventory provides direct insight into high-risk external assets and active threats to enable corrective action

### Features

- Quantify risk posture and risk exposure of external assets
- Actionable metrics and guidance to improve risk posture
- Comprehensive drill-through of threat indicators and security posture as a part of your digital footprint

### Benefits

- Prioritize threat remediation based on external asset exposure
- Provide executive- and operational-level reporting of risk reduction efficacy
- Included as a part of Digital Footprint Enterprise SaaS solution

**Examples of risk components and suggested remediation tasks:**

- A web page in your inventory was found on a phishing blacklist
  - Evaluate web page for compromise, remove from production
- You have 85 external-facing assets with expired SSL certificates
  - Remove from production, or renew SSL certificates
- There are 90 assets in your inventory with open Remote Access (RA) ports
  - Ensure RA should be available on specific assets, and close unnecessary RA ports

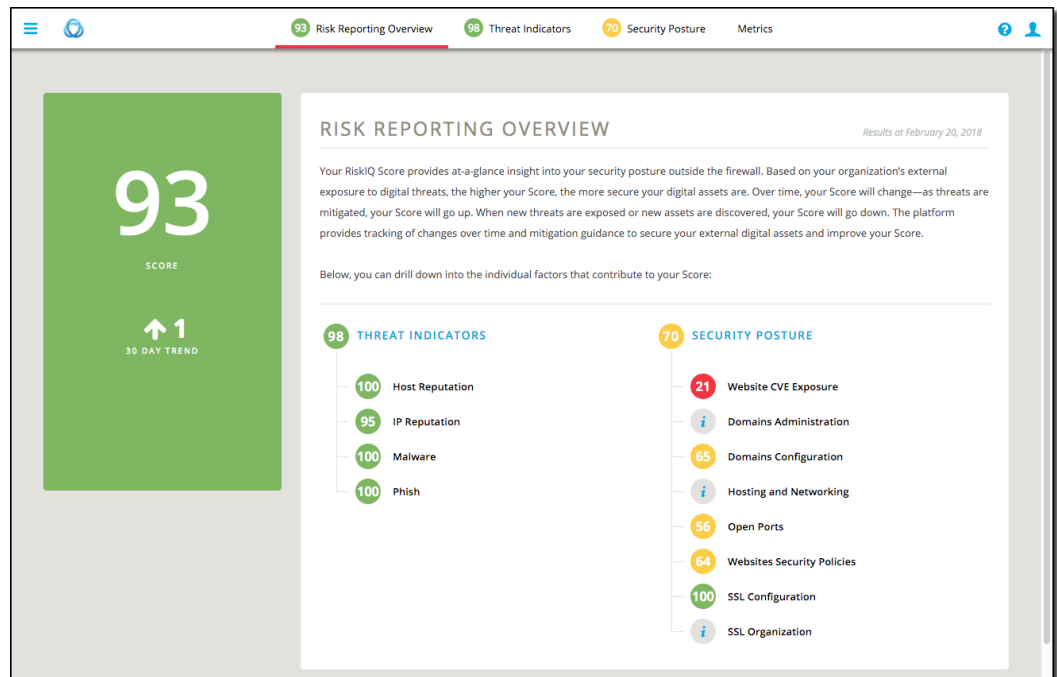


Fig. 1: A Digital Footprint Risk Report of RiskIQ

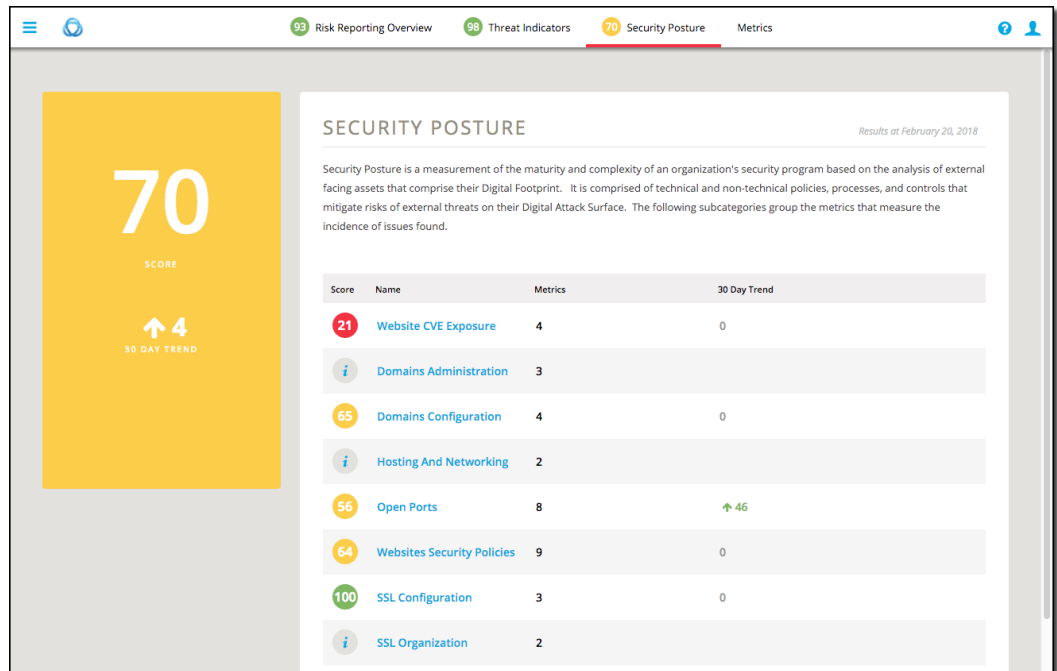


Fig. 2: Asset-level details of at risk security posture

Threat Indicators	Security Posture
<p><i>Threat indicators are active observations of malicious or suspicious activity in an organization's digital footprint. Incidents that occur without remediation serve as indicators that an organization has security management gaps or has not responded effectively.</i></p> <ul style="list-style-type: none"> <li>• Host Reputation</li> <li>• Malware</li> <li>• Phish</li> <li>• IP Reputation</li> </ul>	<p><i>Security Posture is a measurement of the maturity of an organization's security program to properly identify and secure external-facing assets. It is comprised of observing and analyzing exposures against technical best practices and security policies (such as OWASP) that mitigate risk.</i></p> <ul style="list-style-type: none"> <li>• Websites</li> <li>• Domains</li> <li>• SLS/TLS Certificates</li> <li>• Open Ports</li> <li>• Hosting and Networks</li> </ul>



### Gain digital risk management control

Measure, track, and benchmark your digital security posture and accelerate prioritized corrective actions

### Not Just a Score. An Action Plan.

RiskIQ closes the digital risk management gap with easy, accurate, extensive and actionable risk reporting capability built into our Digital Footprint solution. Digital Footprint dynamically generates a map, elements, and insights of external infrastructure and interconnected relationships associated with a business. RiskIQ's breadth and depth of data, combined with advanced analytics technology, ensures that RiskIQ's calculated risk score and underlying component findings for an organization is active, valid, and facilitates efficient corrective action.

Digital Footprint Enterprise enables teams to curate their asset list, provide details about those assets in terms of software, frameworks, and infrastructure, as well as perform crawling for underlying threats that are unable to be seen at the surface level, such as assets that have been compromised to host targeted malware or phishing pages.

At a glance, security leadership can understand trends with regard to risk and security posture over time, and see tangible results from investment in digital threat management. For vulnerability management teams, Digital Footprint Risk Reporting provides a way to add known and at-risk external assets to vulnerability assessment and GRC tools, prioritize remediation activity, and guide remediation efforts to measurably improve their risk.



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

✉ sales@riskiq.net

☎ 1 888.415.4447

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