



COVID-19: The Expanded Attack Surface

Secure the distributed enterprise

THE CHALLENGE: Rapid Change to COVID-19, Keep It Secure

COVID-19 put digital growth into hyperdrive. Fluid conditions and remote access are evolving the attack surface every moment, outpacing security's ability to keep it protected. Digital expansion instantly became the only way to enable a distributed workforce, consumer base, partner ecosystem, and supply chain. But this breakneck pace pushes the enterprise outside the firewall, becoming more exposed to cybercriminals.

COVID-19 related threat actors target fears and vulnerabilities; hit with the hard cost of theft, takeover, skimming, and breach clean-up—along with lost customers, trust, and revenue. IT and security teams must look through billions of logs, events, triggers, alerts, and assets to see where they need to focus.

But this manual process is time-consuming and almost instantly obsolete, subject to the ever-changing digital attack surface. Not to mention the fog surrounding compromised third parties, code, and components.

Specific challenges include:

- Increased shadow-IT; systems move fast to be productive
- Boost in remote access, global distribution and support
- Threat, compliance risk: misconfigured new, on-demand infrastructure
- Multiple cloud providers, controls, permissions, and services
- Growing cyberattacks, exploiting the crisis

THE SOLUTION: Discover Unknowns, Investigate Threats

RiskIQ has been absorbing the internet for 10+ years, and transforms it into a single internet intelligence graph—enabling security teams to scale and adapt to this crisis. Discover hidden risks and threats outside the firewall: clouds and eComm, mobile and websites, users and apps.

Whether you're exploring billions of web components or millions of IP addresses or spotting risky VPN services, RiskIQ gets you from data to insights to action in just a few clicks.

WHY RISKIQ?



Complete Cloud Intelligence

from full DOM capture, analysis and simulated human-web activity



Always-on Monitoring to identify exposures outside the firewall, prioritize for scale



Continuous Inspection discovering attack-exposed assets and exploitable components

Internet Intelligence Graph

RiskIQ absorbs the internet and leverages attacker-aware machine learning to create an intelligent graph of the digital attack surface—enabling secure expansion beyond the firewall by uncovering risks and threats in the layers of the internet assets: pages, apps, ports, services, infrastructure, components, and code.

SOLUTION OVERVIEW

RiskIQ helps safeguard the distributed enterprise by discovering attacker-facing assets—known, unknown, malicious—and investigating threats. Visibility and control for the expanding digital attack surface.



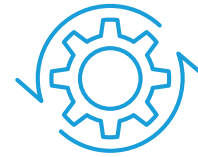
No-Agent Sensor Network

human-web simulation to identify hosts, pages, apps, services, and ports—uncovering COVID-19 related risk and threats



Connected Cloud Services

automated internet graphing, uncovering the global internet fabric—including third-parties, apps and services



Automated Change Detection

code-level detection and smart graphing across infrastructure, services, apps, code, and components



Pre-built Risk Indicators

including COVID-19 exploits and exposures, custom metrics across 200+ risk/threat indicators



Internet Intelligence Graph

attack surface composition, digital layers: hosts, services, apps, ports, pages, components, code, and behavior



RiskIQ gives our team detailed visibility into our thousands of assets and extends control over exposures outside the firewall, previously hidden. Alongside the digital visibility, RiskIQ brought us from a zero-level capability to complete Javascript monitoring coverage to protect our customers.

Director of Security Operations
Discovery, Inc.



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

✉ sales@riskiq.net

☎ 1 888.415.4447

Learn more at riskiq.com

Copyright © 2020 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. 04_20