Brand Protection, Why Threat Actors Target Your People?

Plus 360 Degree Coverage Protecting Company, People and Assets

Senior executives and/or highly sensitive access individuals (HSA's) are a valuable and too often easy target for threat actors. If left unprotected they can represent a significant vulnerability in a company's security posture. Threat actors exploit the human attack surface, including PII, financial data, social impersonation or other identifiable information regarding these individuals in order to extort or attack individuals and the companies at which they work.

Why Are People An Easy Target For Brand Threats?

The internet contains a wealth of information. Online sources such as social media platforms, real estate websites, and people search engines provide hackers with all they need to target you. Your home address, phone number, email address, employment, education, associates, family members, children's names, and frequented restaurants or places of interest may all be public.

Public figures, executives, and high-net-worth individuals often have a more extensive public footprint than the average citizen. Because they are already a high-value target, this outsized exposure makes them even more vulnerable.

Your digital footprint is your and your company's presence in cyberspace. Many of your assets exist, change, and become vulnerable in cyberspace, often without your knowledge. Attackers performing digital surveillance will often find unknown, unprotected, or unmonitored corporate executives' assets or other critical employees to use as attack vectors. In today's Internet of Things (IoT), where our society is highly connected and more social, this information is available. With enough time, research, and data triangulation, you and your key personnel run the risk of becoming a target.

As technology becomes more interconnected and access to information expands, we must adopt a holistic approach to bridge the gap between cybersecurity's inner and outer worlds. In short, we need to focus on cyber bodyguards.

RiskIQ continuously discovers and maps the attack surface to provide an

WHY RISKIQ?

Automated Discovery with 10+ years of real-world internet observations to enable fast

Automated Discovery with 10+ years of real-world internet observations to enable fast takedown

Full API access for use with multiple tools and platforms.

Global Internet Graph

RiskIQ absorbs and normalizes internet-scale data and includes 10+ years of data history, active crawling, asset inspection, and machine learning to encode security expertise. Secure expansion beyond the firewall and identify hidden risks and threats to safeguard digital strategies.

'outside-in' view, identifying where the extended, digital enterprise collides with external threats. This visibility enables security and risk teams to pinpoint relevant threats, attackers, and their infrastructure and prioritize risk so exposures don't become exploits.

RiskIQ's patented discovery capabilities include:

- Domain Names
- Hostnames
- Web Pages
- IP Blocks
- IP Addresses
- ASNs
- SSL Certificates
- WHOIS Contacts
- Mobile Apps
- Social Media Profiles

Discovered assets are indexed and classified in your personal RiskIQ workspace, providing an adaptive system of record for all web infrastructure under the organization's management currently or historically, including web applications, third-party dependencies, and other asset connections.

Enterprise security and risk teams get attack surface awareness, simplifying threat detection and mapping the most relevant attacker-exposed pathways and affected resources, like tools, third parties, mechanisms, components, implications, and action-oriented guidance to safeguard your digital enterprise from external threats targeting brand attacks and abuse.

How Can We Protect Our Company Brand?

Automate detection and protect your brand with active mapping, monitoring, mitigation, and takedown against cyber threats and attacks—phishing sites, typosquatting, domain abuse, rogue mobile apps, impersonation on social media, scams, and brand-trap malware.

RiskIQ gives you command over external threats by leveraging real-world observations of your digital terrain. This includes a deep and dark web for early-stage threat chatter and planning to incident response when attackers attempt to disrupt, deny, or degrade your digital identity and brand.[1]

Brand protection from external threats includes monitoring fluid and stealthy threat activity:

- Typosquat domains and subdomains used for phishing campaigns
- Rogue mobile app impersonation protection
- Identify of exposed credentials
- Alert and monitor bank and financial identifiers
- Uncover brand impersonation via social media and logos
- Listen for coming attacks via deep and dark web monitoring
- Real-time alerts and reports
- Attribute and identify attackers, including takedown services
- Continuously monitor of data leakage
- Scale Threat Discovery for Alerts and Included Takedown Services

[1] Deep/Dark Web sources derived from listeners, including integrations such as Flashpoint.

RiskIQ Managed Intelligence Services is human-driven intelligence, curated and tailored to your attack surface and includes calibrating detections and watchlists and reporting, along with alert triage and mitigation support or takedown services.

When threats are detected, RiskIQ automatically creates alerts—events—within the platform and re-examines the threat at scheduled intervals and documents real-world observations to track the entire threat lifecycle. The Managed Intelligence Service team also includes takedown services and assistance for the events.

i3 Services, Support For Any RiskIQ Product

In addition to our product suite, RiskIQ offers a range of services and immediate support from our Incident Investigation and Intelligence (i3) team for a deeper dive with a more customized solution. These services combine best-in-class technology with expert human analysis from former national security and intelligence officers and trained analysts, acting as a force-multiplier to maximize the value customers can gain from their investment in RiskIQ.

- Reliable and consistent support for security teams
- Nimble and able to act with immediate requests
- Automated identification of vulnerabilities and exposures on the open web and dark web

SOLUTION OVERVIEW

RiskIQ safeguards digital strategies by discovering attacker-exposed assets—people and technologies. Internet-scale security intelligence that identifies and eliminates threats.

24/7 Incident Investigation

Rapid threat reporting or time-sensitive info to be communicated in an escalated manner.

Scale Security Teams

Experienced, high-demand intelligence and counterintelligence analysts and operators.

Automated Change Detection

Encoded detection logic and smart graphing across infrastructure, services, apps, code, and components.

Proactive Threat Intelligence

Readymade with custom metrics and statistical analysis across 200+ risk/threat indicators.

Take Down Services

Built in request removal of threats, content or domains impersonating your company's brand.

WHAT OUR CUSTOMERS SAY

"What I like about RiskIQ is the ease of the dashboard you can log in to at your convenience and see everything in one place. On top of this the i3 team is quick to contact me when there is a digital threat as well we have monthly meetings and that have become critical to our team. It used to take us months to mitigate these incidents and knowing that we are now protected gives our company peace of mind for me."

Marina Beauregard, Vice President
Arcoplast

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

✉ sales@riskiq.net
☎ 1 888.415.4447

Learn more at riskiq.com