RISKIQ®

RiskIQ Digital Footprint®

Discover and Monitor Your Attack Surface

Secure Your Digital Assets

Your organization's brand and digital presence is your largest attack vector. Because of this, cyber criminals will easily uncover and attack external-facing digital assets. In order to protect your organization, you need an accurate picture of how you look to an attacker, including an inventory of your known, unknown, and rogue digital assets. Utilizing RiskIQ's advanced reconnaissance and analytics to make connections between assets, RiskIQ Digital Footprint® software provides an active, comprehensive inventory of all of your IPs, domains, and hosts.

Why Your Digital Footprint Matters

Expanding attack surfaces and the rise of global adversaries leave companies vulnerable—and security teams blind—to threats that exploit customers, users, and networks via the internet.

Companies are devoting more resources to securing web assets, but with agile development teams and easy access to cloud infrastructure, the speed at which those assets are coming online makes them easy prey for bad actors looking to take advantage.

Companies usually counter cyber threats using several different tools, including firewalls, endpoint devices, and service-based solutions. But these approaches don't provide a complete view of an organization's attack surface, especially outside the firewall. Because certificates expire, software requires patching, and assets associated with partner infrastructure can be compromised, that blind spot can leave your organization at serious risk. Digital threats outside the firewall include:

- Unknown and unmanaged assets
- Website defacement
- Compromised or vulnerable web components
- Broken links
- Any assets that have been blacklisted, currently or historically, as hosting phish or malware

How Does Digital Footprint Work?

RiskIQ scans millions of web pages and IPs every day, collecting telemetric data to produce a map of the internet. Digital Footprint uncovers and inventories all digital assets appearing online that tie back to your organization and that you depend on for your digital presence. Digital Footprint enables your security team to manage assets outside your firewall,

Features

- Continuous inventory of your internet-facing assets, such as hosts, IPs and open ports, websites, mobile apps, and social profiles
- Categorize assets to business unit, brand, or owner
- View details on assets such as IP, registrant details, web components, associated CVEs
- API integration with GRC, CMDB, and vulnerability management applications
- Risk Reporting based on key Threat Indicators and Security Posture

Benefits

- Gain visibility into your digital attack surface from the outside in
- Quickly pinpoint vulnerable assets for remediation
- On demand reporting on asset compliance
- Interoperability with existing asset and vulnerability management tools
- Easily prioritize efforts to improve your security posture based on risk and exposure

Reporting on Assets

Digital Footprint provides an intuitive dashboard for monitoring your digital footprint, as well as tracking enforcement, which includes:

- Executive summary reports and a snapshot of the current state of an organization's global digital presence
- Custom reports and data drill-down
- Digital Footprint Risk Reporting which provides easy prioritization of remediation activities to reduce your attack surface

bring unknown assets under management, and survey your digital footprint from the view of the global adversary.

With a full understanding of the scope of your digital presence—and continuous visibility into your internet attack surface, your security team can make accurate, comprehensive, and strategic risk management decisions.

Discovery and Inventory

RiskIQ proprietary discovery technology analyzes all the assets associated with your organization, and continuously discovers new, unknown assets that may be legitimate or fraudulent.

Digital Footprint consolidates all of your internet-exposed assets into an easy to manage inventory. These assets include websites, domains, hosts, web page content, ASNs, IPs and active services on over 110 ports, nameservers, social media profiles, and mobile applications.

Our dynamic inventory system provides full visibility into the state of all the assets and actively monitors them for unsanctioned changes or compromise.

Asset Details

Internet-facing assets present attack vectors into your organization if not known, monitored, and patched with the latest updates. Along with the type of asset, Digital Footprint displays details about digital assets, such as open ports, server type, software, OWASP headers, ownership information. Once these details are known, we can correlate other important information with them, like associated CVEs for vulnerabilities, or allow security teams to filter based on out-of-date frameworks. RiskIQ never enters sensitive information into search engines to prevent the generation and propagation of unwanted content.

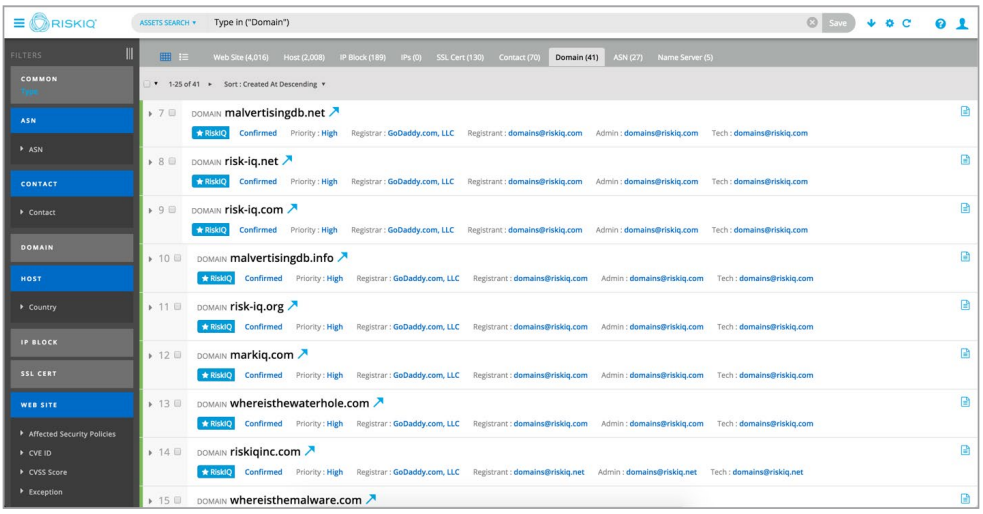

Fig. 1: A view into an asset inventory, looking at domains owned by an organization and high-level details

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com