DATASHEET

DIGITAL FOOTPRINT

Discover and Monitor Your Attack Surface

RISKIQ®

MAP YOUR DIGITAL FOOTPRINT TO IDENTIFY AND PROTECT YOUR WEB ASSETS FROM ATTACK

INCLUDING KNOWN, UNKNOWN, AND ROGUE ASSETS

SECURE YOUR DIGITAL ASSETS

Your organization's brand and digital presence is your largest attack vector. Because of this, cybercriminals 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 all of your known, unknown, and rogue digital assets.

Every day, thousands of websites and servers are compromised, opening backdoors to sensitive customer, employee, and company data. Any organization with an online, digital presence is a target. This exposure damages the trust between brands and their customers and prospects. From phishing to brand infringement and impersonation, it has never been more important to secure your company's digital assets than it is today.

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:

- Domain and subdomain infringement
- Typosquatting
- Website defacement
- Compromised web components
- Broken links
- Any properties that pose a threat to prospects, customers, and your organization

WHAT DOES DIGITAL FOOTPRINT DO?

RiskIQ's Digital Footprint automatically discovers web assets across the internet and experiences them like a real user does. This virtual user technology allows you to accurately identify, monitor, and manage your entire internet attack surface from the outside in.

We scan millions of web pages every day, collecting telemetric data to produce a dynamic index of your web attack surface—illuminating websites, URLs, web page content, ASNs, IPs, and nameservers that you may or may not know about. RiskIQ's Digital Footprint uncovers and inventories all digital assets appearing online that tie back to your organization, enabling your security team to manage assets outside your firewall, 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 web attack surface, your security team can make accurate, comprehensive, and strategic risk management decisions.

DIGITAL FOOTPRINT

DISCOVERY AND INVENTORY

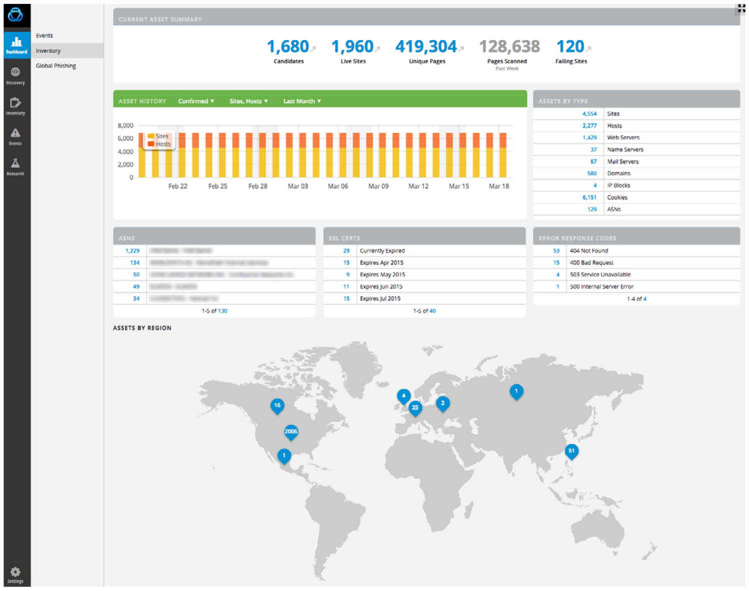
RiskIQ proprietary discovery technology analyzes all the assets associated with your organization,and continuously discovers new, unknown assets that may be legitimate or fraudulent. RiskIQ technology interacts with web assets exactly how a real user would—from different browsers, locations, and device types around the world. This approach evades detection techniques used by malware and phishing campaigns to hide from traditional web crawlers and scanning agents.

Because RiskIQ has the perspective of an attacker, our virtual users see what appears on pages, websites, and mobile sites—just as it appears in users' browsers. This discovery technology captures the DOM and any redirects, external references, dynamic links, and changes made by JavaScript that could signify a potential attack or malicious behavior. Our dynamic inventory system provides full visibility into the state of all the assets and monitors them for unsanctioned changes or compromise.

REPORTING ON ASSETS

RiskIQ provides an intuitive dashboard for monitoring your digital footprint within social media, web and mobile app stores as well as tracking enforcement, which includes:

- Executive summary reports and a snapshot of the current state of an organization's global presence
- Trends and benchmarks of external threat management improvements over time
- Custom reports and data drill-down with key metrics include:
    - Event generation period
    - Current review status and status change history
    - Event uptime until resolution
    - Events by social network
    - Brands associated to events
    - Geographic distribution of events



CURRENT ASSET SUMMARY

1,680	1,960	419,304	128,638	120
Candidates	Live Sites	Unique Pages	Pages Scanned Past Week	Failing Sites

ASSETS BY TYPE

4,554	Sites
2,277	Hosts
1,429	Web Servers
37	Name Servers
67	Mail Servers
580	Domains
4	IP Blocks
6,151	Cookies
129	ASNs

ASNS

1,229	[redacted]
134	[redacted]
50	[redacted]
49	[redacted]
34	[redacted]

1-5 of 130

SSL CERTS

29	Currently Expired
15	Expires Apr 2015
9	Expires May 2015
11	Expires Jun 2015
15	Expires Jul 2015

1-5 of 40

ERROR RESPONSE CODES

53	404 Not Found
15	400 Bad Request
4	503 Service Unavailable
1	500 Internal Server Error

1-4 of 4

ABOUT RISKIQ

RiskIQ is the leader in digital threat management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 80 percent of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social, and mobile exposures. Trusted by thousands of security analysts, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action to protect business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures. Visit RiskIQ.com or follow @RiskIQ on Twitter.