Security Intelligence Empowers Global Protection

Relevant and Actionable Security Intelligence via Attack Surface Insights, Threat Fingerprinting, and Real-World Machine Learning

Digital, cloud-centric transformation creates hidden risks and threats for the extended enterprise—a fluid and entangled threat landscape reshaping security and risk strategies. However, it is challenging to see threats relevant to the global attack surface, which wastes time and energy while adversaries remain concealed. The ever-increasing number of threats is magnified by easy, universal access to malicious systems, kits, and infrastructure capable of effective cyberattacks that adversaries from even the best security professionals.

Highlights | RiskIQ Illuminate®

- Live discovery for real-time attack surface intelligence and complete visibility to your digital footprint
- Relevant insights for faster analysis and response, prioritized for threats tuned to you
- Actionable outcomes driven by unique cyber threat fingerprinting to scale global defense with authentic identifiers
- Reputation scoring and one-click lookups across the open internet and deep/dark web, removing the guesswork from threat intelligence
- Increase the value across your ecosystem of people, processes and technology via flexible APIs, apps, and integrations with 100+ security products and service providers

Cyber threats have a long history of disrupting, denying, and degrading victims. Meanwhile, faster digital growth and criminal ambitions have meshed in the global attack surface to hide the real source of threats: malicious infrastructure.

Relevant, actionable security intelligence is hard to come by. Attack surface intelligence and adversary fingerprinting is the solution. Pairing attack surface intelligence with unique identifiers for threat systems gives security teams better results.

By combining threat intelligence with knowledge of your worldwide digital footprint, detection and analysis capabilities can now uncover what matters most to you. Layered with durable threat indicators that pinpoints threat infrastructure, it gives security teams a long-awaited unfair advantage against cyber threats.

Simply gathering intelligence from open sources or network telemetry and anti-malware is not enough to solve current security challenges. Unraveling what's you from what is another; what's good from what's bad, and adversaries from allies require relevant, actionable intelligence to discern what's real and important to you.

Intelligence that empowers global defense.

Attack Surface Intelligence

Active and historical discovery for complete visibility

Attack surface intelligence identifies and distinguishes resources and digital systems across the open and closed web—brands, infrastructure, third parties, dependencies, peers, industries, and the whole digital supply chain.

Using active and historical discovery enables trillions of observations to be transformed into a unique digital footprint, the DNA of today's enterprise.

- Attack surface intelligence uses automated discovery and human-web simulation to gather reality-based observations and if/then behaviors when provoked by virtual users.
- Live discovery completes your baseline view of the global attack surface. However, attack surface intelligence's greatest strength comes from providing real-world exposures pinned to threats looking to exploit them in real-time.
- Historical and active observations enable meaningful change detection and risk priorities based on what's most relevant to your personal digital presence.
- Attack surface intelligence can also be used to integrate security programs and operations by enabling a single, common threat view that is 100 percent unique to your organization.

Key Benefits

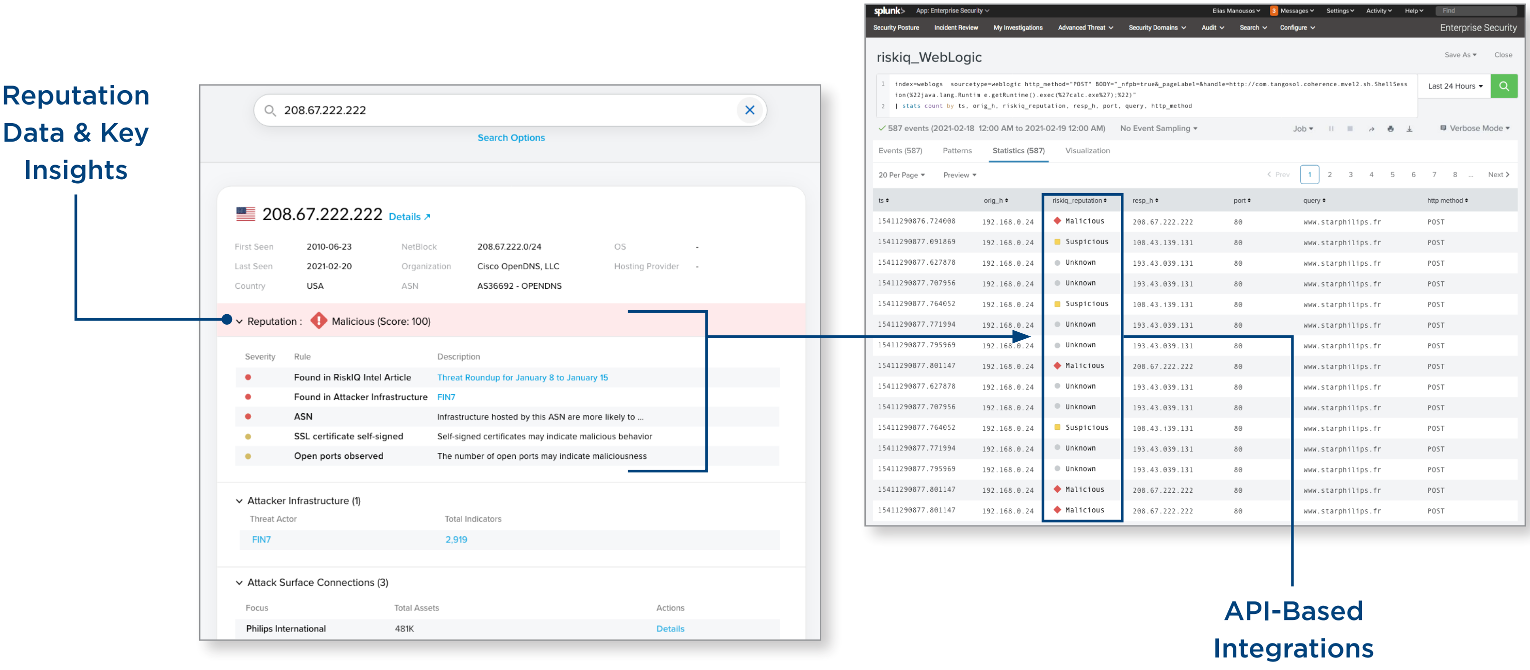
RiskIQ Attack Surface Intelligence

- Attack surface intelligence provides real-world observations of your exploitable digital footprint, elevating your ability to prioritize risks and threats with confidence.
- Speed up analysis, triage, and response and enables security teams to keep pace with digital growth by eliminating threats that matter.
- If malicious activity is detected, you can quickly determine which pieces of the attack surface are also impacted.
- Rapidly classify threats relevant to the attack surface's layered composition—hosts, URLs, apps, components, and code.
- Achieve smarter, faster security and business decisions based on real-world, factful intelligence

Level-up existing SOC resources and people

Security intelligence that combines attack surface insights with relevant observed threats makes security operations more efficient and effective to mitigate the volume of threats at the speed of digital growth.

- Integrated real-world attack surface and threat observations enable reputation summaries and graded scoring to make better sense of alerts. Using composition analysis informs even novice analysts and core security teams to immediately identify alerts pegged with malicious reputations and expanded indicators to streamline triage and downstream workflows.
- Automated discovery distills key insights, pushed via enriched APIs throughout the security ecosystem. Keep pace with digital transformation with details for newly observed hosts (NOH), newly observed domains (NOD), phishing and malware intelligence streams.



Reputation Data & Key Insights

208.67.222.222

Search Options

208.67.222.222 Details ↗

First Seen	2010-06-23	NetBlock	208.67.222.0/24	OS	-
Last Seen	2021-02-20	Organization	Cisco OpenDNS, LLC	Hosting Provider	-
Country	USA	ASN	AS36692 - OPENDNS		

Reputation : Malicious (Score: 100)

Severity	Rule	Description
●	Found in RiskIQ Intel Article	Threat Roundup for January 8 to January 15
●	Found in Attacker Infrastructure	FIN7
●	ASN	Infrastructure hosted by this ASN are more likely to ...
●	SSL certificate self-signed	Self-signed certificates may indicate malicious behavior
●	Open ports observed	The number of open ports may indicate maliciousness

Attacker Infrastructure (1)

Threat Actor	Total Indicators
FIN7	2,919

Attack Surface Connections (3)

Focus	Total Assets	Actions
Philips International	481K	Details

riskiq_WebLogic

```
index=weblogs  sourcetype=weblogic http_method="POST" BODY="_nfpb=true&_pageLabel=&handle=http://com.tangosol.coherence.mvel2.sh.ShellSess
ion(%22java.lang.Runtim e.getRuntime().exec(%27calc.exe%27);%22)"
| stats count by ts, orig_h, riskiq_reputation, resp_h, port, query, http_method
```

✓ 587 events (2021-02-18 12:00 AM to 2021-02-19 12:00 AM)

ts	orig_h	riskiq_reputation	resp_h	port	query	http method
15411290876.724008	192.168.0.24	◆ Malicious	208.67.222.222	80	www.starphilips.fr	POST
15411290877.091869	192.168.0.24	■ Suspicious	108.43.139.131	80	www.starphilips.fr	POST
15411290877.627878	192.168.0.24	● Unknown	193.43.039.131	80	www.starphilips.fr	POST
15411290877.707956	192.168.0.24	● Unknown	193.43.039.131	80	www.starphilips.fr	POST
15411290877.764052	192.168.0.24	■ Suspicious	108.43.139.131	80	www.starphilips.fr	POST
15411290877.771994	192.168.0.24	● Unknown	193.43.039.131	80	www.starphilips.fr	POST
15411290877.795969	192.168.0.24	● Unknown	193.43.039.131	80	www.starphilips.fr	POST
15411290877.801147	192.168.0.24	◆ Malicious	208.67.222.222	80	www.starphilips.fr	POST
15411290877.627878	192.168.0.24	● Unknown	193.43.039.131	80	www.starphilips.fr	POST
15411290877.707956	192.168.0.24	● Unknown	193.43.039.131	80	www.starphilips.fr	POST
15411290877.764052	192.168.0.24	■ Suspicious	108.43.139.131	80	www.starphilips.fr	POST
15411290877.771994	192.168.0.24	● Unknown	193.43.039.131	80	www.starphilips.fr	POST
15411290877.795969	192.168.0.24	● Unknown	193.43.039.131	80	www.starphilips.fr	POST
15411290877.801147	192.168.0.24	◆ Malicious	208.67.222.222	80	www.starphilips.fr	POST
15411290877.801147	192.168.0.24	◆ Malicious	208.67.222.222	80	www.starphilips.fr	POST

API-Based Integrations

Key Benefits

Intelligence for SecOps

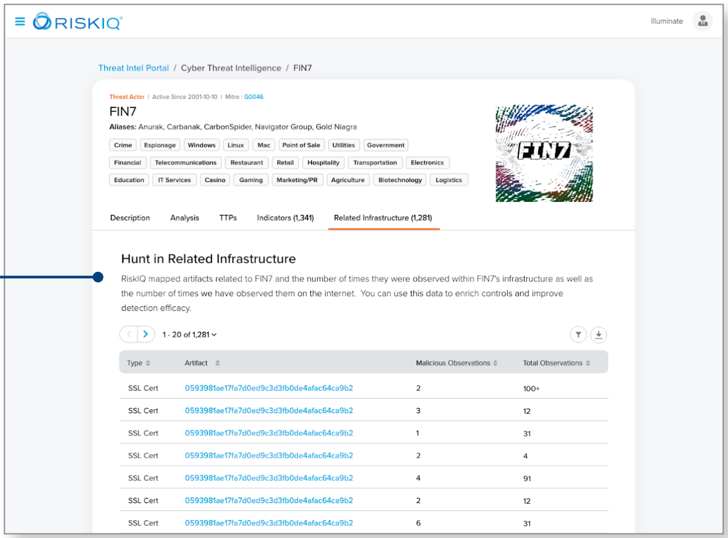
- Easy-to-integrate feeds and simple APIs for SIEM, SOAR, XDR, EDR, IPS, and any other security tools
- Quickly determine priorities based on real-world observations of your attack surface and related threats
- Amplify the productivity of the entire security and risk team by surfacing exposures, threats, and risk tailored to your organization.
- Increase protection coverage with smart defenses, fed by active streams of new and changing threats to your digital footprint.

Find and eliminate attacker systems

Cybercriminals, hacktivists, and nation-state threats all evolve tactics, techniques, and procedures (TTPs) to improve their malicious capabilities. But sustainable, scalable threat indicators come from observing threat infrastructure and behavior, regardless of the threat actor operating it.

- Fingerprint adversary infrastructure to scale defense, even when infrastructure is reused or repurposed by many threat actors. Leverage cyber threat intelligence to assign an identity to threat infrastructure, security teams can future-proof global defenses against threats today and those yet to be deployed.
- Map the composition of threat infrastructure to identify malicious activity, embedded capabilities, and shareable attack tools (e.g. kits, C2 components).
- Use one-click pivots to find related infrastructure, including certificates, hashes, malware, netflow, and deep/dark web reconnaissance to get ahead of threats that matter—from a single threat actor to thousands with access and opportunity to leverage attacker systems.

Related Indicators Discovered Through RiskIQ Intelligence Graph



Threat Actor | Active Since 2001-10-10 | Mitre : G0046

FIN7

Aliases: Anurak, Carbanak, CarbonSpider, Navigator Group, Gold Niagra

Hunt in Related Infrastructure

RiskIQ mapped artifacts related to FIN7 and the number of times they were observed within FIN7's infrastructure as well as the number of times we have observed them on the internet. You can use this data to enrich controls and improve detection efficacy.

Type	Artifact	Malicious Observations	Total Observations
SSL Cert	0593981ae17fa7d0ed9c3d3fb0de4afac64ca9b2	2	100+
SSL Cert	0593981ae17fa7d0ed9c3d3fb0de4afac64ca9b2	3	12
SSL Cert	0593981ae17fa7d0ed9c3d3fb0de4afac64ca9b2	1	31
SSL Cert	0593981ae17fa7d0ed9c3d3fb0de4afac64ca9b2	2	4
SSL Cert	0593981ae17fa7d0ed9c3d3fb0de4afac64ca9b2	4	91
SSL Cert	0593981ae17fa7d0ed9c3d3fb0de4afac64ca9b2	2	12
SSL Cert	0593981ae17fa7d0ed9c3d3fb0de4afac64ca9b2	6	31

▼ Learn More

For more on the advantages of relevant, actionable security intelligence, read the RiskIQ white paper:
5 Questions Threat Intelligence Must Answer

Forrester Research:
Forrester Wave, External Threat Intelligence, Q1 2021

RiskIQ:
The Evil Internet Minute, 2020

LogoKit: Actor Deep Dive

▼ Watch & Join

RiskIQ Illuminate Overview

Cyber Threat Workshops

Get Started

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

✉ sales@riskiq.net
☎ 1 888.415.4447

Learn more at riskiq.com