RISKIQ®

Five Security Intelligence Must-Haves For Next-Gen Attack Surface Management

How Deep Knowledge of Digital Relationships Can Help Defend the Extended Digital Enterprise

Security intelligence describes the practice of collecting, standardizing, and analyzing data generated by networks, applications, and other IT infrastructure to assess and improve an organization's security posture. Traditionally, security intelligence helped us keep an eye on our networks, traffic, and endpoints to take action when and where necessary. However, as recent events have forced us to reassess core concepts and long-held perspectives on cybersecurity itself, it's also time to revisit the impact of security intelligence to protect the enterprise.

Today's global internet attack surface has transformed dramatically into a dynamic, all-encompassing, and completely entwined ecosystem that we're all a part of—your organization, my organization, good guys, bad guys, and every online entity in-between. If you have an internet presence, you interconnect with everyone else, including those that want to do you harm.

It's these digital infrastructure connections that attackers leverage to attack organizations where they lack visibility and situational awareness. However, these connections can also tell your security team your attack surface's story, such as its composition and areas of risk and vulnerability. These connections also illuminate cyber adversaries and their tools—which organizations they've compromised, how they're rotating infrastructure, and more. It's these connections that bring security intelligence to life.

YOUR CURRENT SECURITY INTELLIGENCE PROBABLY ISN'T GOOD ENOUGH

Like a massive battlefield, your organization's digital presence can be a crowded, chaotic, and dangerous place. However, the right security intelligence can cut through this fog of war to help your security team understand the threats and vulnerabilities that matter most and address them.

> "War is ninety percent information."
>
> - Napoleon Bonaparte

The more real-time information you have about yourself, your adversary, and your surroundings—anything that can affect an outcome of a battle—can be the difference between victory and defeat. However, static security intelligence that doesn't account for your organization's attack surface, threat infrastructure, global attack surface, and the constantly changing variables in each only adds to the confusion.

In this white paper, we'll review the five fundamental tenets of a next-gen security intelligence program that give your organization a distinct advantage over its cyber assailants.

Five Key Tenets of a Next-Gen Security Intelligence Program

In today's cyberthreat landscape, those who understand these infrastructure relationships best, good guy or bad guy, are the ones who win. This white paper will detail the importance of modern, dynamic security intelligence focused on these digital connections. In addition, it shares five critical elements all security teams must have fully loaded and operationalized to stay ahead of their adversaries and win the cybersecurity battle:

1. **Know Yourself: Attack Surface Intelligence**
   Awareness of your digital attack surface, its composition, and unique placement amid the global attack surface. Having complete visibility into each asset and connection across your digital footprint is vital.

2. **Know Your Allies: Third-Party Intelligence**
   Your attack surface is full of dependencies. Understanding the risks across your digital supply chain allows you to gain early visibility of threats that could compromise your partners and, through them, impact your organization.

3. **Know Your Enemies: Cyber Threat Intelligence**
   Like your attack surface, your adversary's digital footprint is continuously evolving. With access to real-world observations, insights into digital relationships, and internet connections to threat systems and threat actors, you gain the intelligence necessary to scale your defenses.

4. **Know Your Ever-Changing Surroundings: Security Operations Intelligence**
   Enriching core security solutions with extended enterprise intelligence improves investigation and response.

5. **Know Your Weaknesses: Vulnerability Intelligence**
   New common vulnerabilities and exposures (CVEs) are announced every day. Identify which vulnerabilities matter, how critical they are, and how to align all the teams in your organization so that you're working together toward a common goal.

A Rapidly Shifting Threat Landscape, a Growing Battlefield

The rapid growth of internet-exposed assets has dramatically broadened the spectrum of threats and vulnerabilities affecting the average organization. Sophisticated APTs and petty cybercriminals alike threaten businesses' safety, targeting their data, brand[1], intellectual property, systems, and people. Today, 375 new threats emerge each minute[2].

However, unlike years past, most cyberattacks originate miles away from the network—external-facing web applications comprised the vector category most commonly exploited in hacking-related breaches[3].

In 2020, the COVID-19 pandemic dispersed the enterprise and grew the size and complexity of the global attack surface even more. With most of the world adopting a work-from-home policy, the global remote desktop software market size, $1.53 billion USD in 2019, is now projected to reach $4.69 billion USD by 2027[4]. Meanwhile, dozens of new vulnerabilities in remote access software and devices have given attackers footholds they never had before.

In 2021, landmark cyberattacks told us just how exposed we really were. Mere months removed from the SolarWinds[5] breach, a watershed attack some thought would set the standard for the impact a vulnerability could have, we dealt with the Microsoft Exchange vulnerability. The Exchange incident was exploited by potentially dozens of APTs and signified yet another critical global-scale incident some thought we'd only see once in a decade. It affected more than 300,000 servers and hundreds of thousands of organizations worldwide, and many organizations are still exposed[6].

The sheer scale of these now-commonplace security issues makes them just as much of a big data problem as a cybersecurity problem. They've made us rethink the value of security intelligence to the organization and what security teams and the rest of the enterprise need to operate safely in the age of global-scale threats.

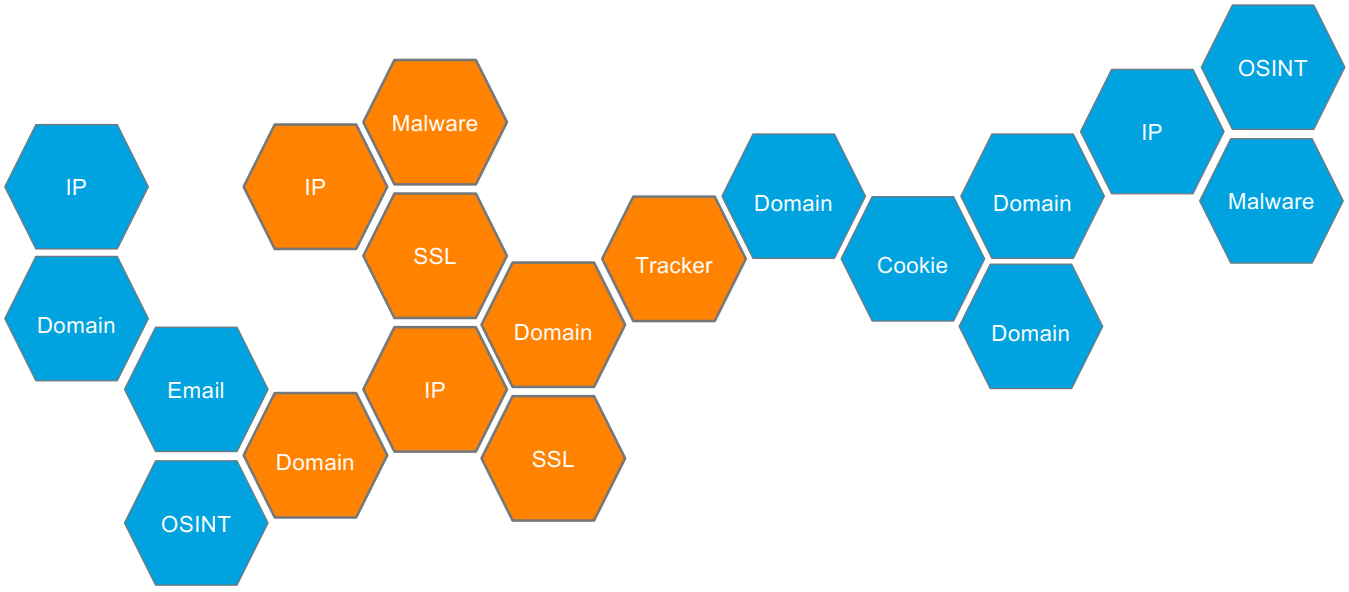
Security intelligence must shrink the global attack surfaces down to size, showing security teams what matters most and how best to act quickly and decisively in the face of each new threat.

Welcome to the age of next-gen security intelligence. Welcome to the age of relationships.

---

1. https://www.riskiq.com/solutions/brand-protection/
2. https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/
3. https://www.scmagazine.com/home/security-news/data-breach/six-need-to-know-takeaways-from-the-verizon-breach-report/
4. https://www.fortunebusinessinsights.com/remote-desktop-software-market-104278
5. https://www.riskiq.com/blog/external-threat-management/solarwinds-orion-hack/
6. https://www.riskiq.com/blog/external-threat-management/microsoft-exchange-server-landscape/

The Awesome Power of Relationships



The new cyberthreat landscape has made static security intelligence dangerously myopic. Whether it be a hack of a digital partner upstream, a forgotten website, or vulnerability in a code library or remote access program, organizations can be susceptible in ways we rarely thought about before.

Internal logs and third-party feeds alone don't provide enough information about the attackers most likely to target your organization, nor the vulnerabilities and security gaps they're most likely to exploit. Extending security and IT protection for the extended enterprise requires mapping the billions of relationships between the internet components belonging to every organization, business, and threat actor on Earth. Security intelligence built from these relationships—the connective tissue between websites, IP addresses, components, frameworks, and code—brings the near-infinite global attack surface into scope, giving security teams real-time situational awareness.

Relevant, actionable threat intelligence gives security teams line-of-sight to attackers and threat systems and infrastructure. Delivering robust and strategic attack surface intelligence starts with hard observations from the internet, including attackers, enterprise, and third parties. These connections illuminate the entire internet and provide a 360-degree view of your organization's attack surface as well as the tools and infrastructure used against you.

1. Know Yourself

Attack Surface Intelligence

The global attack surface is a fluid and dynamic system connecting everything on the internet. “Knowing yourself,” especially better than the enemy does, is the first step to achieving true situational awareness in this chaotic global threat landscape.

Knowing themselves is precisely what attack surface intelligence affords organizations who adopt it, but becoming an expert on your organization’s unique digital footprint isn’t easy. With staggering amounts of infrastructure, brands, companies, apps, services, and systems attached to the enterprise, much of the attack surface is outside the purview of different teams across the organization. This gap creates massive exposures that soon turn into exploits.

As individual attack surfaces get more complicated with each passing day, their complexity goes up, and “non-standard” becomes the norm. Today’s enterprise attack surface is defined by nearly infinite attacker targets, diverse assets, and continuous change and expansion. This elastic, dynamic reality is what security and risk teams must mitigate if their organizations will thrive in the new digital era.

In many organizations, pinpointing CVEs, misconfigurations, and exposures, as they appear, can take days or longer, enabling adversaries to work at their leisure. And for too many enterprise security teams, they are left making poor decisions—slowly. For instance, thousands of Microsoft Exchange servers around the world remain unpatched for the critical HAFNIUM vulnerability, all because of an overwhelming lack of knowledge and intelligence for their attack surface.

Digital Relationships Find, Expose, and Mitigate Risk

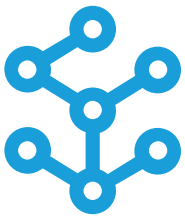
Attack surface intelligence identifies digital relationships within and throughout an organization's unique slice of the worldwide attack surface. All the organization's internet-exposed hardware, software, and underlying components become visible to security and risk teams, enabling them to better collaborate and track how their attack surface evolves, potentially introducing new risks.

This real-time view speeds up triage, analysis, and incident-response by identifying how threats and vulnerabilities connect to your organization.

A Rapidly Expanding Enterprise Digital Attack Surface

- The global remote desktop software market is projected to reach $4.69 billion USD by 2027, a CAGR of 15.1%[7]
- Cloud IT infrastructure is expected to grow at a five-year CAGR of 10.6%, reaching $110.5 billion USD in 2024 and accounting for 64.0% of total IT infrastructure spend[8]
- Attacks on web applications represent 39% of all breaches[9]

7. https://www.fortunebusinessinsights.com/remote-desktop-software-market-104278
8. https://cloudcomputing-news.net/news/2021/feb/01/public-cloud-demand-accelerates-during-the-pandemic-idcs-analysis/
9. https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report&sa=D&source=editors&ust=1624405573386000&usg=AOvVaw1Sfmh0BDvAISeTxRIWPpzT



2. Know Your Allies

Third-Party Intelligence

The enterprise has never been more dependent upon the digital alliances that form the modern supply chain. While these dependencies are essential to operating in the 21st century, they also create a cluttered, layered, and highly complicated web of third-party relationships, many of which are outside the purview of security and risk teams to protect and defend proactively. As a result, quickly identifying vulnerable digital assets that signal risk is a massive challenge.

Often, security and risk teams rely on vendor questionnaires and surveys or antiquated methods for scoring a third-party's risk via credit score models that do not account for the interconnectedness and systemic risk of the global attack surface. A lack of understanding and visibility into these dependencies have made attacks through third parties one of the most frequent and effective vectors for threat actors. More than seventy-five percent of attacks now come through the digital supply chain.

Third-party attacks are now commonplace because even resource-constrained security and risk teams have difficulty keeping up with their attack surface as it grows and evolves both up and downstream. But, more critically, they also lack insight into the digital relationships that provide a layered view of risk in the digital supply chain[10].

75%

More than seventy-five percent of attacks now come through the digital supply chain.

Third-Party Intelligence Finds Risk in All Layers of the Digital Supply Chain

With a real-time graph of the internet, organizations can go far beyond just a static reputation score that uses potentially murky or inconsistent criteria. This third-party intelligence powered by digital relationships can provide a layered view of risk across your digital supply chain using precise indicators of exposure from IP and non-IP resources, hosts and host pairs, apps, pages, ports, data, NetFlow, content, components, and code.

This deep, nuanced, and contextualized view of third-party dependencies destroys silos in the organization and acts as a lingua franca across all teams.

The Enterprise Has Never Been More Reliant on the Digital Supply Chain

- 70% of IT professionals indicated a moderate-to-high level of dependency on external entities that might include third, fourth, or fifth parties[11]
- 53% of organizations have experienced at least one data breach caused by a third party[12]
- 40% of security breaches are now indirect, as threat actors target the weak links in the supply chain or business ecosystem[13]
- Less than 10% of deals globally contain cybersecurity due diligence today[14]

10. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/asus-supply-chain-attack
11. https://www.prnewswire.com/news-releases/as-organizational-reliance-on-third-parties-increases-extended-enterprise-risk-management-to-be-a-focus-in-2019-300778258.html
12. https://securityboulevard.com/2020/06/automation-in-compliance-why-its-a-business-imperative-and-where-to-start/
13. https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf#zoom=40
14. https://www.aon.com/unitedkingdom/insights/top-5-cyber-risks-in-mergers-and-acquisitions.jsp

3. Know Your Enemies

Cyber Threat Intelligence

Today's universe of cybercriminals, hacktivists, and nation-state threats seems nearly infinite. And like a Hydra, even when security teams are successful against a single threat, two (or more) will emerge to make the challenge of scalable defense all the more elusive.

Understanding the many threat groups and keeping track of new ones as they emerge is crucial to situational awareness. And, of course, every organization has a laundry list of credible threats about which they need to be concerned. Still, the sheer scale of the threat landscape creates doubt, uncertainty, and persistent false alarms and alerts that hinder the resolute and decisive action that creates meaningful outcomes for stronger resilience.

Again, diving into the infrastructure relationships that comprise the global attack surface can cut through the constant noise and distractions. By understanding threat infrastructure and the organization-owned infrastructure it targets, next-gen cyber threat intelligence can illuminate only the threats that truly matter to a particular organization, including organizations with similar attack surfaces and in related industries.

Leveraging digital relationships is particularly important in understanding how threat actors evolve tactics, techniques, and procedures (TTPs) to improve their malicious capabilities. Here, open-source intelligence, threat feeds, and other static intelligence provide, at best, a superficial view of threat actors; a static, incomplete list of indicators of compromise (IOCs). At worst, they can leave teams completely blind as threat operators switch up and rotate infrastructure and evolve their tools and TTPs, with new actors picking up where old ones left off.

In many cases, tracking threat infrastructure is more important than the threat groups themselves. To use a metaphor, it's tracking the guns rather than the shooters. This take on security is essential because different groups will recycle and share infrastructure—IPs, domains, and certificates—and borrow each other's tools, such as malware, phish kits, and C2 components, tweaking and improving them to fit their unique needs. And with the rise of economies that sell crimeware-as-a-service and other cybercrime commodities, threat infrastructure can transcend threat actors and groups.

Cyber Threat Intelligence Unpacks Adversary Threat Infrastructure

Knowing the infrastructure and its connections helps security teams map, monitor, and track adversary-threat infrastructure and its composition—malware, suspicious activity, threat capabilities, shareable attack tools, and their relationships within the worldwide attack surface. With this view, they see adversaries for what they really are, illuminating all of a group's infrastructure to eliminate doubt and leave no ambiguity.

The Global Attack Surface Has Exploded

- 560,000 new pieces of malware are detected every day[15]
- In 2020, the number of detected malware variants rose by 62%[16]
- The number of phishing kits advertised on underground cybercrime marketplaces doubled between 2018 and 2019[17]
- RiskIQ detects a Cobalt Strike C2 server every 49 minutes[18]

15 https://dataprot.net/statistics/malware-statistics/
16 https://dataprot.net/statistics/malware-statistics/
17 https://dataprot.net/statistics/malware-statistics/
18 https://www.riskiq.com/resources/infographic/evil-internet-minute-2021/

4. Know Your Ever-Changing Surroundings

Security Operations Intelligence

Seventy percent of cybersecurity professionals claim the cybersecurity skills shortage impacts their organization[19]. The true strength of security intelligence infused by digital relationships is its ability to empower organizations' ecosystem of people, processes, and technology to overcome the skills gap and keep pace with the elastic, continuously changing global attack surface.

The digital enterprise and threat actors alike create digital relationships every second—new domains, hosts, and other elements of threat infrastructure constantly appear and morph. RiskIQ observed 3,495,267 new domains (249,662 per day) and 77,252,098 new hosts (5,518,007 per day) across the internet over a two-week period[20]. The sheer scale of the attack surface can be debilitating for security organizations. However, when these connections are precomputed and fed into the security operations tech stack via APIs—SIEM, SOAR, EDR, and MSSP—it becomes something of a digital mech suit for understaffed and overworked team members.

Security Operations Intelligence Is Premium Fuel for Effective Security Operations

Knowledge of relationships translates to security knowledge at scale. Precomputed relationships across the global attack surface provide the instant reputation of any infrastructure. For instance, next-gen SecOps intelligence:

- Illuminates all hosts and domains related to an organization via dynamic DNS providers
- Instantly informs teams if domains and IPs to which outbound traffic is going and inbound is coming are malicious or suspicious
- Shows host relationships showing connections to malicious infrastructure
- Flags phish and other malicious hosts before they're added to feeds

SecOps intelligence built with precomputed digital relationships creates knowledge at scale, a guided path for security teams. This way, they can then focus only on what matters to their organization, shrinking the global attack surface from impossibly large to manageable—and shrinking their unreasonable workload in the process.

The Global Attack Surface Is Highly Dynamic. Is Your SOC Plugged In?

- Every 6 minutes, a phishing domain was detected across a sample of 478 unique brands[21]
- Every minute, 5.5 domain infringements were detected across a sample of 170 unique brands[22]
- 14.6 Every minute, 14.6 COVID-related hosts were created[23]
- RiskIQ has observed 61,651,839,751 new hosts over the past year[24]

19 https://www.esg-global.com/esg-issa-research-report-2020?utm_campaign=ESG%20Research&utm_source=slider
20 https://www.riskiq.com/research/anatomy-of-an-attack-surface/
21 https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/
22 https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/
23 https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/
24 https://www.riskiq.com/blog/external-threat-management/internet-intelligence-graph/

5. Know Your Weaknesses

Vulnerability Intelligence

Sun Tzu comes up often in infosec literature, and sometimes for a good reason: modern threat actor tactics perfectly exemplify his advice on strength and weakness. He suggests that, in war, "avoid what is strong, and strike at what is weak." At the most basic level, this is how today's cyber attackers operate. If organizations are weak somewhere, attackers will find out about it—even if that organization wasn't one of their primary targets.

With the outbreak of COVID-19, the digital enterprise went into hyperdrive. Almost overnight, workforces and business operations decentralized and were flung worldwide, widening the protection gaps and giving attackers more access points to probe or exploit. Remote work due to the pandemic has increased the average cost of a data breach by $137,000[25].

Breaches via new internet-connected assets are happening at an unprecedented rate, many of them resulting from compromised assets that organizations weren't aware even existed. The average time to identify a breach in 2020 was 207 days[26]. Even now, thousands of organizations are still exposed to the Hafnium vulnerabilities, and patching is wildly inconsistent across the world.

This dangerous gap between breach and response is also likely due to different teams across the organization not sharing data, preventing them from seeing the big picture of their organization's attack surface.

Vulnerability Intelligence the Lingua Franca for Different Teams across the Organization

Next-gen vulnerability intelligence is the glue that connects all the teams across an organization. The flow of vulnerability intelligence gets everyone speaking the same language and enables them to correlate one another's information quickly.

Vulnerabilities can lie throughout every layer of the enterprise attack surface, at a depth that only security intelligence fortified with internet intelligence can illuminate, such as those in frameworks, page contents, third-party components, and code. With feeds showing these vulnerabilities and where they lie across an organization, teams can stay ahead of early-stage vulnerabilities and speed up remediation with risk-based priorities for what's relevant, preventing downtime and wasted effort by focusing on critical exposures.

Vulnerabilities Are Rampant and Global in Scale

- Over 18,000 vulnerabilities were published in 2020[27]
- Microsoft Exchange Vulnerability affected more than 300,000 servers[28]
- 18,000 government and private users downloaded compromised SolarWinds Orion versions[29]

25 https://www.ibm.com/security/data-breach

26 https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

27 https://www.scmagazine.com/home/security-news/cves-break-record-in-2020-topping-18000/

28 https://www.riskiq.com/blog/external-threat-management/microsoft-exchange-server-landscape/

29 https://www.cpomagazine.com/cyber-security/solarwinds-backdoor-affected-18000-customers-microsoft-warns-40-actively-targeted-organizations/

Gain Deeper Knowledge of Your Digital Relationships

Leverage RiskIQ to Prepare for, and Win, the Battle against Global Adversaries

With RiskIQ, you can access a precomputed relationship database of internet intelligence that is updated daily. Tapping into the Internet Intelligence Graph[30] provides a complete picture of the entire internet to show your own organization's internet attack surface, including known, unknown, and attacker-owned assets. This view also includes external third-party infrastructure, OSINT, and resources on which your organization, users, and customers depend. The graphic helps analysts map cyber threats to the enterprise to prioritize response and fully extinguish compromises.

Organizations can infuse their security stack with next-gen security intelligence built on digital relationships via the RiskIQ Illuminate® Internet Security Intelligence Platform. This security intelligence evolves as fast as threat actors because it's fortified with trillions of observations of both an organization's unique attack surface and threat groups and their tools and tactics. This real-time data gives security leaders, researchers, analysts, and teams on-the-ground visibility into their digital presence from every angle to understand how they're being targeted. In addition, this intelligence provides context that prioritizes the most critical exposures, future-proofs security programs against emerging threats, and optimizes precious security resources.

RiskIQ Illuminate helps you take the first step by bringing together global visibility for both your attack surface, your third parties, and the threats and threat actors targeting you—all in a single platform. Organizations want to pull intelligence into the products and security stack—to make those systems smarter and orchestrate a rapid, coordinated, cross-functional response. The RiskIQ platform has modules for everyone in the security team from the CISO, SecOps, CTI, Brand Intelligence, and Vulnerability Teams, enabling a unified view of internet threats that ultimately speed up decision-making and response times to reduce overall risk.

RiskIQ Illuminate® Internet Security Intelligence Platform

One Platform: Multiple Solutions

Want to see how next-gen security intelligence can help you win on the cybersecurity digital battlefield?

Request a free trial today:
https://community.riskiq.com/learn-more

30 https://www.riskiq.com/blog/external-threat-management/internet-intelligence-graph/

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 75%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, security teams, and CISO's, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action to protect the business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures.

Try RiskIQ Community Edition for free by visiting https://www.riskiq.com/community/. To learn more about RiskIQ, visit www.riskiq.com.

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com