RiskIQ is a cyber security company based in San Francisco, California.[1] It provides cloud-based software as a service (SaaS) for organizations to detect phishing, fraud, malware, and other online security threats.

The company was co-founded in 2009 by Lou Manousos, Chris Kiernan and David Pon. It received $10 million of Series A funding from Summit Partners in February 2013 and $25 million series B funding from Battery Ventures in May 2014.[2][3] RiskIQ is a member of the Cloud Security Alliance (CSA), and ISACA.

RiskIQ monitors advertising networks for malware (malvertising) and spyware[4] and also provides mobile app security services.[5] In May 2018, Standard Bank deployed RiskIQ’s software to automate the threat analysis of brand infringement, cybercrime and web-based attacks against its digital presence.[6]

References


External links

- Official website (http://www.riskiq.com/)
RiskIQ: The Digital Threat Hunter Using AI To Define The Future Of Cyber Security

Just like Google, we crawl and index the entire web -- over 2 billion web pages and 15 million mobile apps every day.

Before, cyber security was practiced within the confines of the firewall, but it should now traverse the entire internet.

Cyber Security is projected to become a $232 billion global market by 2022.
Cyber Security is a rapidly evolving industry, projected to become a $232 billion global market by 2022.

This estimated valuation reflects a significant rise from last year, in which the market value reached $137.8 billion worldwide in 2017. marking an impressive Compound Annual Growth Rate of 11%.

The emergence of mobile platforms and cloud-based enterprise apps, coupled with the increased adoption of advanced technologies such as fingerprint identification and biometrics have collectively fueled a notable spike in the space. Although cyber security is attracting greater attention across the globe, the United States stands as the dominant force leading the charge for innovation.

Founded in 2009, RiskIQ stands as a global leader in cyber security, specializing in digital threat management. Asserting that an estimated 75% of cyber attacks originate outside of the firewall, RiskIQ uses digital threat hunting to help shield customers, companies and brands from breaches across a broad scope of digital channels.

Digital threat hunting refers to proactively analyzing large quantities of data, processing information that is both internal to a business and generated from public internet data sets. By closely examining these relationships, threat analysts can spot new connections, group attack activity, and uncover evidence to legitimize claims. More importantly, this method allows analysts to see the full scope of a targeted attack, enabling threat preventionists to limit the impact of an attempted breach and ultimately block dangerous infrastructure.

YOU MAY ALSO LIKE

Utilizing a combination of machine learning and advanced analytics, RiskIQ uses raw internet data collected by crawlers and internet sensors for the purpose of
mapping and locating threats across various attack surfaces. The company refers to this security method as *In the Wild Threat Detection*, meaning that their proprietary platform experiences the internet identically to real users. This allows RiskIQ to detect visible threats in real-time and alert security teams with substantiated data.

I spoke with RiskIQ President Dan Schoenbaum about the vision behind his company, the future of cyber security and why organizations must protect their data now more than ever.

**What was the void or opportunity you saw in the market that attracted you to join the leadership team at RiskIQ?**

*Dan Schoenbaum:* Security teams are spending more budget than ever before on security products, but they have been powerless to stop the internet-scale attacks that are picking off organizations one by one and causing data breaches that make national headlines. The problem is that companies are spending money in all the wrong places, beefing up their perimeter while hackers hit them in the only place they lack visibility: outside the firewall. But, the market is now realizing that there’s a good reason 75% of the attacks that cause data breaches originate from outside the firewall, and analysts are corroborating that. That’s why RiskIQ presented the perfect opportunity for me. It’s the only company that empowers security teams to fight attacks that traverse the entire internet with data that does the same, so being able to help them accelerate growth during a new age of security was too good to pass up.

**Describe how your digital defense works and the specific tools or methods you use to protect online entities?**

*Dan Schoenbaum:* Just like Google, we crawl and index the entire web -- over 2 billion web pages and 15 million mobile apps every day. Only, instead of doing it to rank websites for search, we’re the only company doing it to detect and expose threats. At the same time, we’re continuously mapping the internet and building a system of record for highly connected internet data that analysts can search to uncover and block attackers targeting their organizations. RiskIQ does
this through a vast global network of crawlers and sensors, essentially virtual users that execute billions of HTTP requests per day, which interact with the web exactly how a real user or hacker would.

These virtual users discover, index, and monitor what we call 'digital assets' -- anything discoverable on the web by users and hackers alike, such as websites, servers, frameworks, mobile apps, social media pages and third-party code. All too often, businesses aren't aware of the scope of servers, web pages, and mobile apps associated with their organization. Both legitimate and malicious assets are created by threat actors with the goal of impersonating the business's digital presence. Due to this lack of visibility, security teams can't protect these assets, which are inroads threat actors use to breach them. How can you protect what you don't know exists? When organizations have an inventory of everything they own, they can process and understand the massive scope of their attack surface and develop an effective threat management strategy to protect it.

What is the biggest blind spot in the cyber security space and what are some of the biggest misconceptions around it?

Dan Schoenbaum: As a military veteran, I like a combat analogy to describe the problem plaguing modern cybersecurity. Like real-world warfare, the cyber battlefield has grown exponentially in size and scope. Before, cyber security was practiced within the confines of the firewall, but it should now traverse the entire internet. Unfortunately, despite needing to defend everything from the corporate network to the outer reaches of the internet, CISOs still spend significant money securing their perimeter, employing an average of 35 tools to do so. But, this is mostly a reactive approach, and it no longer works. In this new age of cyber attacks targeting organizations on the open internet, it doesn't make sense to dig in and wait for the enemy to come to you because there are no more battle lines to defend.

The organizations finding success on today's cyber battlefield are the ones spending money on surveillance and reconnaissance tools that show them their digital presence the way it looks to attackers, a collection of far-flung digital assets hackers can discover as they research their next threat campaigns. Millions
of these digital assets appear on the internet every day, most of which are entirely outside the scope of organizations' security visibility. Think of it as the digital version of eyes in the sky that unmanned drones provide modern soldiers. With this view, organizations can take a proactive approach to defend their organizations and, if necessary, take the fight to the enemy rather than waiting to be breached.

How are you working to improve digital threat hunting practices?

Dan Schoenbaum: RiskIQ PassiveTotal, our threat infrastructure analysis tool, is the go-to threat hunting tool for analysts. Because of this widespread adoption, RiskIQ set up a nationwide tour of threat hunting workshops to teach analysts how to leverage the interconnectivity of the internet to track and expose their attackers. In these workshops, we teach them to use the interconnected datasets derived from our web crawling to efficiently surface threat infrastructure. Amidst a cybersecurity skills shortage reaching crisis levels, the goal is to empower the professionals who are hunting threats with technology that acts like a digital 'mech suit' that supercharges their output so that their organizations have the chance to thrive in digital channels despite this skills gap. Technology that combines advanced internet data reconnaissance and analytics acts as a force multiplier that enables fewer, less-skilled employees to expedite investigations, understand digital attack surfaces, assess risk, and take action against threats with the skill and efficiency of a much larger and more experienced group.

What emerging trends do you expect to see in the space and what should online business and brands be paying attention to?

Dan Schoenbaum: Some of your organization’s most dangerous vulnerabilities may actually belong to someone else, but are still very much your problem. With the widespread lack of visibility into their external-facing assets, supply chain attacks -- attacks on third parties integrated with your digital assets such as third-party tracking and analytics code -- will increase in volume, intensity, and sophistication. Vulnerable third-party components breached by hackers to gain access to thousands of sites at once is a central narrative in recent hacking events,
namely the rise in injected cryptocurrency mining scripts and RiskIQ's research into Magecart -- the threat group responsible for the recent hack of Ticketmaster.

In the case of the infamous breach of Ticketmaster, RiskIQ discovered it wasn't an isolated incident, but a worldwide digital credit card-skimming campaign by the threat group Magecart. By hacking a third-party analytics script found on the Ticketmaster website, Magecart instantly gained access to their site, as well as thousands of others that were running it. The affected brands had no visibility into the code running on their website, so they were unaware and powerless to protect their customers.

**How do you see the space evolving in the next 3-5 years and what impact do you hope RiskIQ has on this shift?**

**Dan Schoenbaum:** With the perimeter becoming less defined by the day, security teams are increasingly responsible for defending against digital threats on the open web, where threat actors target their organizations' brand, employees, and customers with tactics such as phishing, malicious mobile apps, and hacking internet-facing assets like websites and web components. The next 3-5 years will be defined by internet data -- who can get it, who has it, and how long have they been collecting it. 

Because of our ability to essentially be a search engine for threat data and index web pages, which security teams can use to uncover threats, RiskIQ will be incredibly impactful going forward. Since 2008, RiskIQ's global network of sensors has been discovering and indexing assets across the web, collecting an extensive repository of telemetry data that helps our technology operate at a massive scale. I'm looking forward to continuing the journey of empowering organizations around the world so they can grow, innovate, and safely do business on the open internet.

*I'm an award-winning content creator with a passion for adding my perspective to topics in music, media and entertainment. I've spearheaded campaigns and content for brands like American Honda Motors, Wells Fargo, Google, and Magic Johnson Enterprises. I also worked closely ...*
Follow me on Twitter to share your comments and continue the conversation

@Allthingsmith