Ovum
TMT intelligence | informa

On the Radar: RiskIQ provides external digital threat defense

RiskIQ helps businesses see, manage, and mitigate web, social, and mobile threats

Publication Date: 11 May 2017 | Product code: IT0022-000966

Andrew Kellett

Summary

Catalyst

The RiskIQ Digital Threat Management Platform is a SaaS-based threat intelligence and integrated application suite that addresses security issues across web, social, and mobile channels. It helps security managers protect their business assets, including their brands, their customers, and their employees, from external exploits that originate from beyond the firewall. The RiskIQ application suite provides unified visibility and protection for enterprise organizations, ensuring that their public-facing digital assets are kept safe from impersonation and illegitimate misuse by malicious threat actors. It also enables security teams to optimize a broad range of investigation, analysis, and mitigation tasks.

Key messages

- RiskIQ deals with web, social, and mobile threats outside the corporate firewall, allowing companies to understand and monitor external exploits, adversaries, and attack infrastructure that can adversely affect its business and publicly available assets.
- RiskIQ intelligence is achieved through advanced Internet reconnaissance techniques that capture detailed Internet data through a global proxy network of collectors, sensors, and web crawlers using virtual user emulation techniques.
- Big data, advanced algorithms, and machine learning (ML) techniques are used to analyze and monitor new and active threat activities, and to dynamically generate and assess a client's digital attack surface.
- Beyond threat intelligence, RiskIQ's suite of threat investigation, brand protection, digital footprint, and threat mitigation applications offer collaboration, monitoring, and workflow that provide a means to optimize resources and consolidate other toolsets.
- The RiskIQ Community Edition allows organizations to have entry-level access to the platform and applications at no charge, contributing machine learning advantages.

Ovum view

Digital threats now account for a significant proportion of security incidents, and businesses therefore need to extend their security capabilities beyond the perimeter and internal defenses. While threat intelligence feeds enrich internal event data, organizations need to consider end-to-end approaches that enable security staff to move to a more systematic, automated approach to help reduce business impact and increase proactive response to digital threats. The RiskIQ Digital Threat Management Platform is relevant to organizations that have a mature security program and support team, as well as organizations that need RiskIQ's resources to protect popular brands. The technology is used to enable threat hunters and incident responders to rapidly investigate threats. It enables asset and vulnerability management teams to identify their organization's external-facing Internet attack surface and identify exposed, exploited, and rogue assets. It creates a security status picture of how an organization's online presence is operating, by capturing, monitoring, and reporting on malicious and threatening activities that are likely to put an organization, its consumers, and its brands at risk. This combined intelligence and SaaS application approach can yield considerable advantages over point-based solutions that are either threat feeds, cover one digital channel, or have limited threat coverage.

Recommendations for enterprises

Why put the RiskIQ Digital Threat Management Platform on your radar?

Businesses continue to increase their investments in public-facing web, social, and mobile activities to get their brand stickier with consumers, and to facilitate customer, employee, and partner interaction. In many organizations, online digital interactions are now of equal or greater importance than traditional trading channels. The resulting digital dynamic and sprawl, more often positioned outside the sight or management of IT, can prove difficult to control and puts business operations and reputation at risk. The RiskIQ Digital Threat Management Platform provides the visibility and protection that these organizations need. It makes use of massive Internet data sets and big data analytics to identify, report on, and protect digital assets (websites and web applications, domains, servers, certificates, mobile applications, and social media accounts) that operate beyond the firewall, and identifies the adversaries that are looking to take advantage. RiskIQ business operations and brand protection benefits are threefold.

- RiskIQ offers security analysts detailed access to broad, correlated, and derived data presented in a way that enables faster, more revealing, threat investigations, as well as enabling collaboration and proactive monitoring.
- RiskIQ provides its clients with a thorough picture of their digital assets and risk profile, and ensures that malicious actions, such as phishing, malware, ransomware, and data extraction, and brand abuse, such as imposter mobile apps, malvertisers, websites, and online personas, issues can be addressed using built-in mitigation capabilities.
- RiskIQ identifies and monitors organizations' visible attack surface to provide external attack surface protection. This is a key issue because the external-facing assets are public, and if left exposed, can be and often are exploited by malicious threat actors.

The combination of RiskIQ's threat intelligence and application suite presents organizations with additional layers of business and brand protection, and the opportunity to make cost savings as a result of this.

Highlights

The RiskIQ Digital Threat Management Platform comprises an Internet intelligence data warehouse and three core applications: RiskIQ Digital Footprint, RiskIQ PassiveTotal, and RiskIQ External Threats.

RiskIQ Digital Footprint is used to discover an organization's web and associated online assets, while RiskIQ PassiveTotal accelerates threat, adversary, and incident investigations. RiskIQ External Threats provides the ability to deal with advanced threats, active exploits, and sophisticated attackers through the identification, assessment, and mitigation phases.

The RiskIQ platform approach provides unified visibility and control over external web, social, and mobile channels, and therefore the digital threats and external asset exposure businesses now face. Its external threat monitoring, search, and analytical capabilities are used to identify, confirm the status of, and legitimize the use of digital assets, and at the same time identify actual exploits or

opportunities for malicious outsiders to engage in digital theft, phishing, malware, social impersonation, and the generation of illegal associations to an organization and its brands.

RiskIQ Digital Footprint (DF)

RiskIQ DF is a digital footprint discovery, generation, and management solution that is responsible for discovering the external web and digital assets associated with an organization. It provides the mapping, monitoring, and management facilities needed to accurately plot an organization's Internet attack surface and therefore its external risk posture. It uses RiskIQ's volumes of telemetric Internet data to generate a dynamic and evolving picture of an organization's threat footprint, assessing at-risk domains, websites, applications, URLs, web page content, autonomous system numbers (ASNs), IP addresses, SSL certificates, and other online associations.

RiskIQ DF uses RiskIQ's virtual user crawling technology to interact with websites as a genuine user would, and performs deep website and web application investigations, without upsetting the equilibrium of each site or alerting detection systems. Inventory, session information, and redirects are captured to provide a complete usage and relationship picture. Security teams use this information to identify potential unsanctioned changes and operational risks, such as expired/expiring certificates, infected web servers, unauthorized or vulnerable applications, malicious site alterations, and to support penetration and vulnerability testing initiatives, and asset management compliance tasks.

RiskIQ PassiveTotal (PT)

RiskIQ PT is a tool that accelerates cyber threat investigations. Security analysts and incident responders benefit from the improved investigative processes available. These include the ability to enrich security events detected in the corporate network with detailed information about a threat, exploit, and an adversary's infrastructure on the open web.

RiskIQ PT provides threat hunters with active and actionable intelligence that adds context to each event. Users can establish and share projects comprised of threat artifacts and research results. RiskIQ PT proactively tracks Internet signals and changes to artifacts to predict new threat actor activity and identify new threats. It has a huge and diverse set of Internet data available to support its investigative capabilities, including passive DNS resolution data, WHOIS information for domain registration details (current and historic), SSL certificate information (current and historic), web tracker information, and more, as well as derived data showing related connections between web pages and access requests.

RiskIQ External Threats (ET)

RiskIQ ET identifies advanced threats, active exploits, and sophisticated attackers targeting a business, and provides triage and threat mitigation. It is used to detect a broad array of web, social, and mobile threats. These include domain squatting and infringement; phishing against customers and employees; imposter social media accounts; compromised and rogue mobile apps; and importantly, the unsanctioned use of corporate brands and logos.

The extensive range of coverage and available data sources, which are a consistent characteristic of the RiskIQ platform, feature strongly within RiskIQ ET's analytical detection and response approach. RiskIQ ET turns the vast amount of online information available into discrete, actionable events, and automates the required threat monitoring, triage, notifications, and mitigations. With the solution's in-app mitigation, security teams can block threats using available third-party reputation management

protocols from the likes of Microsoft, Google, Apple, and also through an organization's firewall, SIEM, or security automation system.

For other threats, such as brand abuse and rogue mobile apps, RiskIQ mitigation workflows help coordinate security and business protection requirements. They can, for example, be used to assist security and legal teams to automatically submit take-down requests made of an adversary's digital infrastructure, such as registrars, certificate authorities, site and app owners, and app stores, and can be subsequently used to monitor take-down fulfillment. This type of request is made to block the actions of threat actors and attackers, and can be undertaken by the client, or where authorized, by RiskIQ itself.

Note: When using the RiskIQ Community Edition, organizations, security analysts, and consultants are given entry-level access to RiskIQ solutions at no charge. With only a daily query limitation, users can access PT to experience guided tours; create, examine and contribute to public research projects; conduct threat investigations; and enrich SIEM events via an API. Aggregate security usage adds to big data analytics advantages such as identifying new trends and threats.

RiskIQ Digital Threat Management Platform (DTMP)

To deliver its range of business and brand protection services, RiskIQ uses advanced Internet data capturing facilities, combining its global proxy network with web crawlers, collectors, and sensor technologies to amass huge amounts of publicly available Internet data. Tens of thousands of virtual users are invoked from a constantly evolving global web and mobile proxy network. They execute billions of HTTP requests daily across millions of web pages, collecting telemetric and session data. The captured data is normalized, and big data, advanced algorithms, and machine learning (ML) techniques are used to continuously analyze the data and report on newly identified exploit activities that put businesses and their brands at risk.

With regard to mobile apps, RiskIQ analytics and intelligence is extensive and deep seated, and interrogates beyond the basics of title, description, and version analysis. It regularly monitors more than 20 million mobile apps across 190 different mobile app stores, and automatically conducts app content and code analysis checks to discover logos, brand references, and malicious code hidden within app files. It can identify legitimate apps and can differentiate these from modified versions, unauthorized fakes, and look-alike versions.

RiskIQ offers monitoring capabilities to identify impersonation and security issues within popular social networks, including Facebook, Twitter, LinkedIn, Google+, YouTube, Instagram, and Pinterest.

Through machine learning and human research, derived data sets are created to yield up-to-date IP reputation, phishing, zero-day attacks, online scams, domain infringements, and associated malware lists. Customers can also take advantage of additional platform features, such as project management, activity monitoring and case management facilities, as well as interoperability with other popular security tools, to automate and extend investigation and mitigation processes.

Background

RiskIQ was founded in 2009 by CEO Elias (Lou) Manousos, CTO Chris Kiernan, and David Pon. The company is headquartered in San Francisco, and is a member of the Cloud Security Alliance (CSA), the Information Systems Audit and Control Association (ISACA), Online Trust Alliance (OTA), and APWG. As of 2016, the company has raised $67.5m in funding from Summit Partners, Battery Ventures, Georgian Partners, and Mass Mutual Venture Capital.

Current position

The RiskIQ Digital Threat Management Platform was developed to detect and deal with external digital threats that emanate from web, mobile, and social media channels. As the commercial investment in Internet and public/customer-facing digital communications continues to grow, so does the velocity and sophistication of threat and fraud opportunities that these channels represent. Threat actors no longer need to breach the firewall to steal from an organization or do damage to its brand. RiskIQ deals with these issues through comprehensive Internet data sets and the use of predictive analytics to enable security teams to efficiently identify, understand, monitor, and take action against threats to an organization's brand, online properties and infrastructure, mobile apps, and social community.

The target market is large to global enterprises across all major industries as well as mid-tier organizations with a significant brand and or digital presence. Typical customers are the more mature, security-conscious organizations, with an existing team of security analysts that recognize the threats that now originate and stem from their online presence. RiskIQ has customers in the Americas, EMEA, and Asia-Pacific, including 17 of the largest 25 banks in North America, eight of the largest 15 European banks, and seven of the world's top 15 consumer brands.

Data sheet

Key facts

Table 1: Data sheet: RiskIQ

Product name	RiskIQ Digital Threat Management Platform	**Product classification**	Cybersecurity and digital defense
Version number	n/a (SaaS technology)	**Release date**	2013
Industries covered	All	**Geographies covered**	All
Relevant company sizes	Large to global enterprises or mid-tier organizations with a large brand/digital presence	**Licensing options**	The Community Edition of RiskIQ is free. Premium Editions of PassiveTotal, Digital Footprint, and External Threats start at $9,000 to $25,000 per year.
URL	www.riskiq.com	**Routes to market**	Direct sales, channel sales, and a fulfilment, free approach for the Community Edition
Company headquarters	San Francisco, CA, US	**Number of employees**	165

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

2017 Trends to Watch: Security, IT0022-000808 (October 2016)

Addressing the Range and Reach of Attacks Across the Cybersecurity Threat Landscape, IT0022-000858 (February 2017)

Author

Andrew Kellett, Principal Analyst, Infrastructure Solutions

andrew.kellett@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo