The Forrester Wave™: Digital Risk Monitoring, Q3 2016

The Nine Vendors That Matter Most And How They Stack Up

by Nick Hayes

September 28, 2016

Why Read This Report

In our 27-criteria evaluation of digital risk monitoring (DRM) solutions, we identified the nine most significant ones — BrandProtect, Crisp Thinking, Digital Shadows, DigitalStakeout, ListenLogic, LookingGlass, Proofpoint, RiskIQ, and ZeroFox — and researched, analyzed, and scored them. This report shows how each provider measures up, helping security and risk (S&R) professionals and their peers select the right solution for their companies.

Key Takeaways

ZeroFox, Proofpoint, RiskIQ, And Digital Shadows Lead The Pack

We uncovered a market in which ZeroFox, Proofpoint, RiskIQ, and Digital Shadows lead the pack. DigitalStakeout, LookingGlass (which recently acquired Cyveillance), and BrandProtect offer competitive options. Crisp Thinking is a relevant Contender, and ListenLogic lags behind.

S&R Pros Need Capabilities To Persistently Monitor For Risk Across Digital Channels

Whether it's to spot a major data leak, prevent a brand impersonation, or monitor a closed conversation threatening physical harm of key personnel, digital risk monitoring solutions are increasingly valuable for S&R pros who need to scour countless digital (i.e., social, mobile, web) channels and rapidly remediate these burgeoning crises before severe, long-lasting damage occurs.

Data Coverage, Risk Analytics, And Digital Governance Features Are Key Differentiators

As manual, in-house, and generic online and social media monitoring options struggle to address risk management needs, DRM solutions that continue to expand their data coverage, develop unique techniques to track and identify risk, and enhance their automated control capabilities will become clear standouts in this budding digital risk market.

The Forrester Wave™: Digital Risk Monitoring, Q3 2016

The Nine Vendors That Matter Most And How They Stack Up

by Nick Hayes
with Christopher McClean, Claire O'Malley, and Peggy Dostie

September 28, 2016

Table Of Contents

Notes & Resources

Forrester conducted product evaluations in March 2016 and interviewed 55 vendor and user companies. The vendors were: BrandProtect, Crisp Thinking, Digital Shadows, DigitalStakeout, ListenLogic, LookingGlass, Proofpoint, RiskIQ, and ZeroFox.

Related Research Documents

Build Digital Risk Insight

Four Ways Cybercriminals Exploit Social Media

TechRadar™: Risk Management, Q4 2015

FORRESTER®

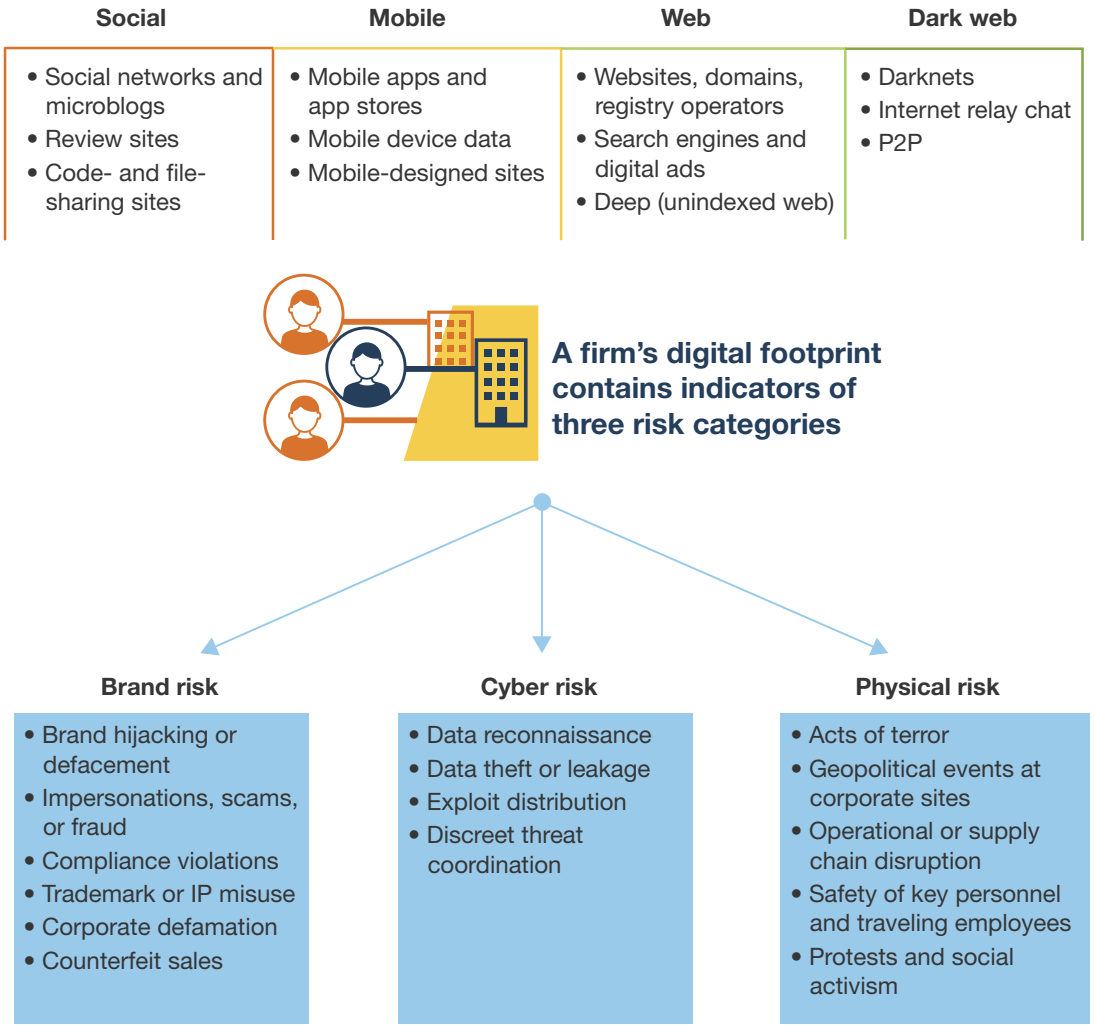
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Major Digital Risk Blind Spots Leave Companies Exposed

When it comes to the myriad risks companies face across digital channels — social, mobile, and web — security and risk (S&R) pros track a much smaller portion of their environment than they realize. Without comprehensively and persistently monitoring risk in digital channels, companies remain susceptible to a wide variety of brand, cyber, and physical risk events (see Figure 1). Despite the high stakes, many organizations struggle to improve digital risk visibility and mitigate related risks because:

- **Digital footprints are incredibly vast and chaotic.** A firm's digital footprints encompass every touchpoint, mention, and affiliation that links to the company.[1] Given the large number of social networks, mobile apps, and websites where this activity can occur, the number of associated corporate accounts, sites, apps, and ads can easily rise into the thousands for large organizations. When you account for unowned, but associated digital elements — including those owned by affiliated third parties, associated with current and former employees, and created fraudulently — manual tracking becomes untenable.
- **From malware to brand hijacking, digital risk comes in countless shapes and sizes.** Cybercriminals use a variety of tactics to weaponize social media, impersonate or embed malware into mobile apps, deface websites, and collude in dark channels.[2] Beyond these nefarious cybertactics, digital channels are often the fastest way to detect a slew of other brand and physical risks, such as compliance violations, corporate defamation, protests, supply chain disruption, and safety threats to personnel. Given the wide variety of risk on digital channels, identifying relevant risk is a deeply complicated task.
- **Companies are at the mercy of digital channels for control and enforcement.** Many digital risk events occur beyond the corporate network and outside a company's legal jurisdiction. For example, Target was caught off guard by a Facebook account impersonating its customer service group; this fraudulent account antagonized already upset customers on the day of a particularly contentious corporate announcement before Facebook finally took it down — after 16 hours![3] Beyond brand impersonations, other events beyond corporate control include hashtag takeovers, employee defamation, malware distribution, and threat coordination.
- **Generic online or social media monitoring provides a false sense of security.** Many S&R (and marketing) pros remain naïve about serious risks in their organization's digital presence, because they believe their existing social media monitoring or cyberthreat intelligence (CTI) tools will detect them. That notion, however, is increasingly misguided. Most social monitoring technologies focus on marketing initiatives; they fail to address risk needs, lack appropriate risk analytics, and don't even cover many important digital channels, such as code- and file-sharing sites, dark web domains, and communities. Meanwhile, most CTI tools don't offer continuous monitoring and focus exclusively on cybersecurity-related issues.

FIGURE 1 Risk Runs Rampant On Every Digital Channel



Digital Risk Monitoring Is Critical For Effective Prevention, Mitigation, And Remediation

Digital risk monitoring tools help customers reduce the impact of risk events with quicker detection and remediation while minimizing the likelihood of such events with better governance and automated controls. In particular, DRM solutions provide the following capabilities:

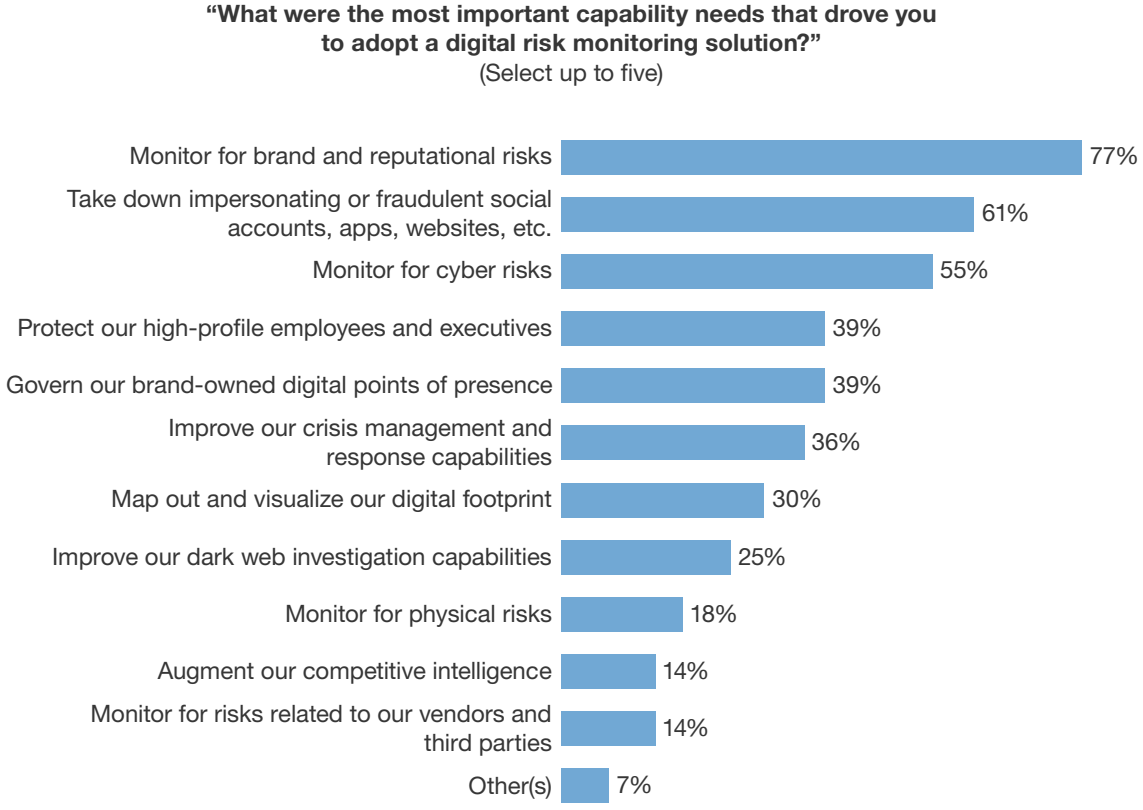
› **Sophisticated intelligence delivers relevant risk data.** DRM solutions aggregate and analyze data from a range of intelligence sources, including open source intelligence (OSINT), technical intelligence (TECHINT), signals intelligence (SIGINT), human intelligence (HUMINT), and covert human intelligence sources (CHIS) (see Figure 2).

- **Continuous monitoring improves event detection and response.** DRM solutions continuously monitor known digital assets and routinely scour all monitored digital channels to ensure that relevant risk events and threats are discovered quickly and with sufficient context to determine the appropriate response.
- **Vendor analysts fine-tune configurations and perform deeper investigations.** Behind every DRM platform and dashboard are experienced analysts who optimize these products based on their deep understanding of digital risk and the ever-changing threat landscape. They may tune the analytics to ensure clients receive only the most relevant events, or they may let customers manage their own DRM solutions and just offer strategic support when needed. In addition, some vendors offer analyst services for special or covert investigations, to go beyond what even advanced technical tools can offer.
- **Strong ties with major channels can expedite requests and takedowns.** Takedown capabilities are the second most sought-after feature of surveyed DRM customers (see Figure 3). DRM vendors routinely interact with cyber, fraud, and compliance stakeholders at major digital channel providers such as Amazon, eBay, Facebook, Google (search engine), Google Play (app store), LinkedIn, Twitter, and Yahoo, along with registrars and registry operators such as Verisign. These frequent interactions reduce the time it takes to submit and complete related requests. In specific cases, DRM vendors establish technical partnerships that expedite their submissions.

FIGURE 2 Sources Of Risk Intelligence That Feeds Into DRM Solutions

Source	Abbreviation	Explanation	Examples
Open source intelligence	OSINT	Data collected from publicly available or subscription-based sources, often via API or web crawlers and bots	• Social media data sources • Paste sites • Code-or file-sharing sites • Surface web harvesting
Technical intelligence	TECHINT	Data containing technical indicators associated with malicious cyberactivity, typically sourced from corporate or third-party forensic efforts	• Threat intelligence feeds • DNS sinkholes and traffic • Honeypots • Pen testing results
Signals intelligence	SIGINT	Data gathered by intercepting communications or other information in transit	• Data flow analysis • Cluster analysis • Wireless IDS/IPS • Log monitoring and vulnerability scanning
Human intelligence	HUMINT	Data gathered or verified by experienced, human intelligence analysts	• Event and incident management • Sock puppets and personas • Law enforcement relationships
Covert human intelligence sources	CHIS	Data gathered covertly by intelligence agents, who manually infiltrate hidden, underground, or otherwise closed-off channels	• Undercover cyberinvestigations • Regional insider recruitment

FIGURE 3 DRM Customers Need The Most Help With Brand Risk And Digital Governance



Base: 46 global security and risk professionals that use digital risk monitoring software
Source: The Forrester Digital Risk Monitoring Wave Customer Reference Survey, 2016

Digital Risk And The DRM Vendor Landscape Are Still In Early Days

It's important to remember how quickly our use of digital channels and technologies has evolved, because the related risks are only beginning to emerge. To put this into context, the average time people spend on smartphones on a daily basis more than doubled since 2013, rising from 58 minutes to 126 minutes every day in 2015.[4] This rapid digital evolution is drastically altering consumer behavior and expectations, blurring digital and physical experiences, and creating new vulnerabilities and ways for malicious actors to exploit these trends.[5] For example, the augmented reality app phenomenon, Pokémon Go, has ushered in a surge of fraudulent mobile apps and social accounts that aim to manipulate unsuspecting users with inconspicuous spam and malware, while sinister bots target popular hashtags like #PokemonGo to effectively take advantage of massive audiences.[6]

We are only at the start of this digital era, and the same can be said for the DRM vendor landscape. As digital risks continue to proliferate and become even more detrimental to the business, Forrester expects the growth of the DRM market to accelerate in turn. Beyond those included in this Forrester Wave™, Forrester is tracking an emerging group of vendors that are either just surfacing or in the process of building out full DRM capability suites, including 4iQ Solutions, Brandle, Buguroo, Cyberint, Cytegic, InfoArmor, Social Safeguard, and Surfwatch Labs.

Digital Risk Monitoring Solutions Evaluation Overview

To assess the state of the digital risk monitoring market, Forrester evaluated the strengths and weaknesses of nine top vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of 27 evaluation criteria, which we grouped into three categories:

- **Current offering.** To assess current offerings, we evaluated how the solutions stack up in terms of data coverage, digital governance, risk analysis, and the overall dashboard and user experience.
- **Strategy.** To evaluate strategy, we analyzed how well aligned and developed each vendor's vision is for the future of the DRM market, along with the degree to which their product strategies, financial resources, and staff expertise will enable them to execute on their strategic vision.
- **Market presence.** To determine the vendors' market presence, we looked at their annual product revenue, customer base, and number of employees.

Evaluated Vendors And Inclusion Criteria

Forrester included nine vendors in the assessment: BrandProtect, Crisp Thinking, Digital Shadows, DigitalStakeout, ListenLogic, LookingGlass, Proofpoint, RiskIQ, and ZeroFox. Each of these vendors has (see Figure 4):

- **A strong focus on risk management use cases and functions.** Through its solution offering, marketing collateral, and technical vision, each vendor must demonstrate a strong understanding of and focus on helping customers in various risk functions address a range of risk challenges and use cases, such as information security, compliance, brand and reputational risk, and fraud.
- **Capabilities to actively scan and uncover risk across a broad set of digital channels.** The solution must continuously surveil digital channels — social, mobile, and web — to measure, detect, and mitigate all forms of corporate risk online.
- **Unique data access or data-gathering techniques.** The vendor must provide pay-for-access, proprietary, or otherwise differentiating data sources or data-gathering techniques to monitor for risk.
- **Functionality to detect digital and physical risk events.** The vendor's solution must apply advanced data science techniques to analyze and identify a variety of risk types, including both digital and physical risk, in an automated fashion.

› **Demonstrated success and relevance to the market.** The vendor must have an active, growing customer base and must routinely appear in competitive situations in the market and among Forrester clients.

FIGURE 4 Evaluated Vendors: Product Information And Selection Criteria

Vendor	Product evaluated
BrandProtect	Digital Risk Monitoring Platform
Crisp Thinking	Social Media Risk Monitoring
Digital Shadows	SearchLight
DigitalStakeout	Digital Risk Intelligence Platform v2.9
ListenLogic	Enterprise Risk Sensing Solution
LookingGlass Cyber Solutions	Cyber Threat Center Version 1.12
Proofpoint	Digital Risk Suite
RiskIQ	External Threat Management Platform
ZeroFox	Enterprise Spring ’16

Vendor selection criteria

A strong focus on risk management use cases and functions. Through its solution offering, marketing collateral, and technical vision, each vendor must demonstrate a strong understanding of and focus on helping customers in various risk functions address a range of risk challenges and use cases, such as information security, compliance, brand and reputational risk, and fraud.

Capabilities to actively scan and uncover risk across a broad set of digital channels. The solution must continuously surveil digital channels — social, mobile, and web — to measure, detect, and mitigate all forms of corporate risk online.

Unique data access or data-gathering techniques. The vendor must provide pay-for-access, proprietary, or otherwise differentiating data sources or data-gathering techniques to monitor for risk.

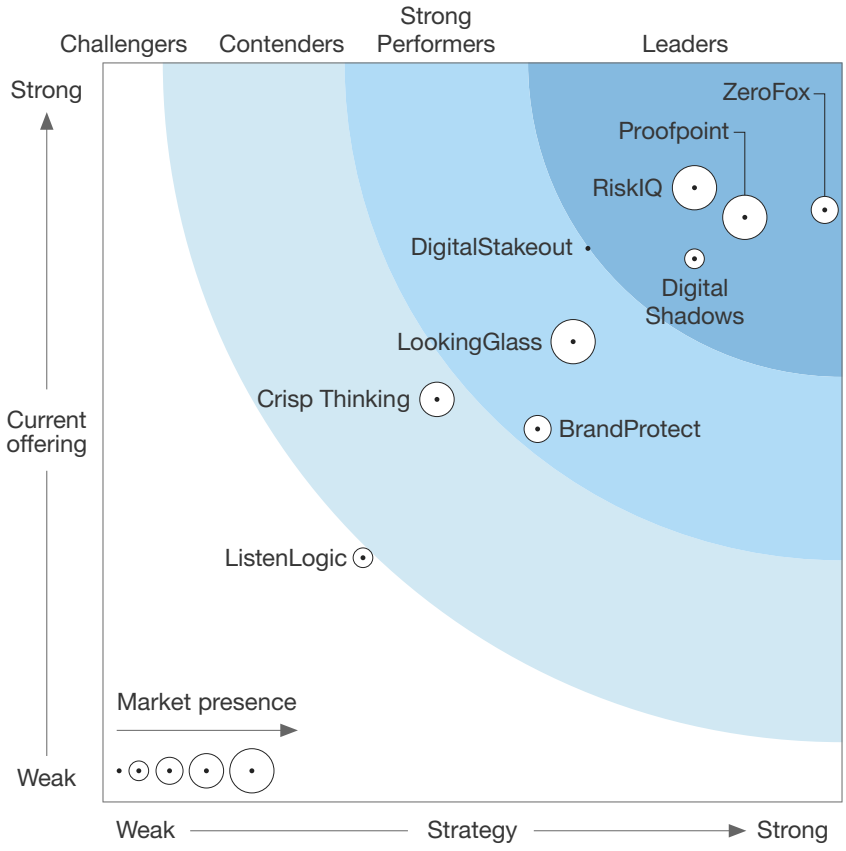
Functionality to detect digital and physical risk events. The vendor’s solution must apply advanced data science techniques to analyze and identify a variety of risk types, including both digital and physical risk, in an automated fashion.

Demonstrated success and relevance to the market. The vendor must have an active, growing customer base and must routinely appear in competitive situations in the market and among Forrester clients.

Vendor Profiles

This evaluation of the DRM market is intended to be a starting point only. We encourage clients to view the detailed product evaluations and adapt criteria weightings to fit their individual needs using the Forrester Wave Excel-based vendor comparison tool (see Figure 5).

FIGURE 5 Forrester Wave™: Digital Risk Monitoring, Q3 '16



FORRESTER® **RESEARCH**
The Forrester Wave™

Go to Forrester.com to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.

FIGURE 5 Forrester Wave™: Digital Risk Monitoring, Q3 '16 (Cont.)

	Forrester's weighting	BrandProtect	Crisp Thinking	Digital Shadows	DigitalStakeout	ListenLogic	LookingGlass	Proofpoint	RiskIQ	ZeroFox
Current offering	50%	2.52	2.72	3.67	3.74	1.65	3.11	3.95	4.15	4.00
Background information	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Data coverage	40%	2.75	2.55	3.40	3.80	1.55	3.40	3.85	4.50	3.50
Digital governance	20%	3.30	3.80	3.50	2.60	1.10	2.70	4.40	3.70	4.30
Risk monitoring and remediation	30%	2.20	2.40	3.70	4.40	2.10	3.30	3.70	4.10	4.40
Dashboards and user interface	10%	1.00	2.20	5.00	3.80	1.80	2.20	4.20	3.80	4.20
Strategy	50%	2.94	2.26	4.00	3.28	1.76	3.18	4.34	4.00	4.88
Corporate strategy and vision	60%	2.90	3.10	4.00	2.80	1.60	3.30	3.90	4.00	4.80
Customer references	40%	3.00	1.00	4.00	4.00	2.00	3.00	5.00	4.00	5.00
Implementation size and cost of ownership	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Market presence	0%	3.00	3.80	1.80	0.80	1.80	4.20	4.60	4.60	3.00
Annual revenue	40%	4.00	4.00	2.00	1.00	2.00	5.00	5.00	5.00	3.00
Number of customers	40%	3.00	3.00	1.00	1.00	0.00	3.00	5.00	5.00	3.00
Number of employees	20%	1.00	5.00	3.00	0.00	5.00	5.00	3.00	3.00	3.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Leaders

› **ZeroFox fuses superior social data coverage with fast-paced analytics.** ZeroFox has innovated rapidly since its inception in 2013, offering a solution for customers to analyze and discover cyber and brand risks, predominantly via social media channels. Sticking to its strategic focus on social media security, ZeroFox has expanded its coverage of social channels, added further flexibility for

customers to configure or integrate their own data sources through its Foxscript API, improved its cybersecurity acumen with new analysis techniques, and built out a number of strategic security partners, including FireEye, Maltego, and Splunk.

ZeroFox still has work to do to further expand its coverage of digital channels, particularly for mobile app stores and the unindexed web. It also lacks automated control enforcement capabilities to safeguard known and brand-owned accounts and sites. That said, S&R pros looking to improve the way they monitor and detect a plethora of cyber and brand risks should certainly consider ZeroFox.

- **Proofpoint offers unparalleled control enforcement for covered digital channels.** Since its acquisition of Nexgate in October 2014, Proofpoint has invested heavily in social media security and compliance capabilities — and the strategy is starting to pay off. Proofpoint continues to integrate its own security capabilities with Nexgate to offer an even more comprehensive digital risk monitoring solution capable of correlating internal communications, such as email, with external social media threats. Proofpoint stands above the rest of the pack with its strong portfolio of patents related to digital risk monitoring, including capabilities to automatically lock down brand-owned social media accounts when malicious activity is detected.

  Proofpoint must continue to integrate its disparate social media and security products —NetCitadel, Nexgate, Sendmail, and Socialware, and, most recently, Return Path — for a more consistent end user experience and to deliver value at higher levels of the organization. Those seeking advanced capabilities to safeguard their company's known digital presence while actively monitoring a sufficient set of digital channels to identify risks should put Proofpoint on their vendor shortlist.

- **RiskIQ provides the broadest coverage of social, mobile, and web data.** Leveraging its proprietary sensor network and virtual web crawlers — which use behavior characteristics to mimic real users — RiskIQ covers a practically endless list of digital channels to provide customers a comprehensive digital system of record. Beyond that, RiskIQ monitors a large set of official and unofficial mobile app stores, and it's one of the only vendors in this Forrester Wave to cover malvertising, including analysis of Facebook's ad ecosystem. RiskIQ's deep partnership with Facebook also benefits RiskIQ customers, who can expect expedited takedown requests with Facebook.

  RiskIQ's virtual web crawler approach, however, does have some limitations. For instance, outside of Facebook, RiskIQ isn't able to track all private activity of client-owned social media accounts. Clients may also experience some inconsistencies in their data since RiskIQ's aggregation techniques circumvent some digital channels' APIs. Even so, S&R pros looking to detect malicious, external cyberactivity across a wide gamut of digital channels will want to take a close look at RiskIQ.

- **Digital Shadows showcases the digital risk dashboard of the future.** Digital Shadows' SearchLight offering provides granular, automated cyberthreat intelligence typically only found in primarily analyst-driven offerings — even using proprietary techniques to monitor and search open and dark web channels. Rather than publishing regularly scheduled, static reports, Digital

Shadows' platform offers real-time, detailed insight into the data it aggregates, the events and leaked data it discovers, and the behavioral attributes and motivations of dozens of adversaries and hacker groups. It also applies its own risk scoring method to offer a business-level view into clients' current digital risk posture.

While Digital Shadows' platform, data coverage, and threat detection techniques are solid, it still needs broader and/or deeper coverage across social, mobile, and web channels. It should also look to improve its digital governance capabilities, particularly in the area of takedowns and control enforcement over managed digital accounts and sites. The company's limited data coverage, however, shouldn't deter S&R pros. Digital Shadows' analytics, data classifiers, and dashboard give it a solid foundation onto which it will ultimately add more data sources.

Strong Performers

› **DigitalStakeout boasts a robust data model for high-caliber digital risk analysis.** While lesser known than many of the other vendors included in this Forrester Wave, DigitalStakeout offers a powerful digital risk monitoring solution. In particular, DigitalStakeout has an extremely flexible data model capable of aggregating information from a broad set of digital channels — including several dark web sources — and automatically applying a nearly limitless set of metadata and classifiers. Moreover, its dashboard is highly intuitive and can produce advanced data visualizations, including sophisticated location analysis and geofencing capabilities.

DigitalStakeout still has more to do from a data coverage standpoint, especially for mobile channels and the unindexed web. Some of its technology partners can cover its gaps in control monitoring, takedown, and remediation capabilities, but that means customers will require two separate tools for what other vendors are offering in one solution. These should be viewed as areas for improvement, but not dealbreakers, for S&R pros looking for a way to monitor digital, physical, and brand risks in an accurate, detailed, and efficient fashion.

› **LookingGlass impresses with decades of analyst expertise and integration potential.** LookingGlass entered the digital risk monitoring market in full force when it announced its acquisition of Cyveillance in December 2015. The combination of its own threat intelligence and mitigation capabilities, coupled with Cyveillance's well-established digital risk monitoring capabilities and strong analyst expertise, creates the potential for LookingGlass to offer one of the broader solutions, providing capabilities for detection, mitigation, and prevention.

The jury is still out on how well this acquisition will go. Cyveillance's heavy reliance on an analyst-driven solution may not conform well to the rest of the primarily technology-focused LookingGlass portfolio. Beyond that, Cyveillance has some legacy shortfalls that LookingGlass will have to address, especially the need to enhance the user portal and dashboard for a better end user experience. S&R pros seeking a well-known commodity in the market with strong potential to add valuable features through deeper product integration will do well to consider LookingGlass.

› **BrandProtect prevails in managed service scenarios for North American SMBs.** Founded in 2001, BrandProtect was one of the first vendors to offer online brand protection services. Since then, it's expanded its product portfolio to monitor for a much broader range of digital risks, with data coverage across social, mobile, and web channels. BrandProtect is largely an analyst-driven solution with proprietary crawlers to aggregate relevant digital risk data for clients. It covers thousands of ISPs globally and has strategic partnerships with Thomson Reuters for country code top-level domain (ccTLD) data. The company maintains strong customer relationships with quick response times, providing references with longer relationships, on average, than any other vendor in this Forrester Wave.

BrandProtect offers adequate capabilities and coverage in most areas but lacks any truly differentiating technical features. Its customer portal is fairly unintuitive, with most clients choosing to rely on the company's experienced threat analysts, receiving reports and charts via PDF. S&R pros looking to cover most digital channels sufficiently should consider BrandProtect. This is especially true for heavily regulated small and medium-size businesses (SMBs) (e.g., financial services and healthcare) in North America, which represents a large portion of BrandProtect's current customer base.

Contenders

› **Crisp Thinking differentiates with clear SLAs and reliable customer support.** Based in the UK, Crisp Thinking provides a managed digital risk monitoring solution. Supported by its proprietary natural language processing (NLP), machine learning, and moderation capabilities, the company's analysts refine results to ensure that clients only review highly relevant risk events. Primarily covering social media channels, Crisp Thinking differentiates from most other vendors in this Forrester Wave with well-defined SLAs for risk detection, ranging from a 95% accuracy rate to as high as 99.999% with its platinum package.

Crisp Thinking has several capability gaps, including lackluster data coverage for mobile, web, and dark web channels; poor end user experience; and relatively poor customer satisfaction compared with other vendors in this Forrester Wave. S&R pros with major personnel resource constraints that still require global capabilities and a high degree of confidence in the accuracy and speed of digital risk detection for social media, such as those in regulated industries, should be sure to consider Crisp Thinking.

Challengers

› **ListenLogic goes beyond keyword searches, but success hinges on automation.** ListenLogic offers a primarily analyst-driven, managed digital risk monitoring service. The company has a solid vision of the serious challenge that cyber, physical, and brand threats pose organizations and how its solution can help customers mitigate those risks with continuous tracking and persistent analyst oversight. ListenLogic monitors digital channels with a combination of automated

data ingestion and experienced analysts who scour online channels and search engines using complex, predeveloped search techniques. It's maintained some success with several enterprise organizations, primarily in pharma and healthcare.

There remain major capability gaps for ListenLogic across the broad, including data coverage, risk analysis, and digital governance. And while it can scale to meet the coverage requirements for any client, its standard offering only covers 16 hours a day, seven days a week. S&R pros needing basic coverage to monitor digital channels more comprehensively than assigning internal resources to conduct manual keyword searches can consider ListenLogic.

Supplemental Material

Online Resource

The online version of Figure 5 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by or prior to March 31, 2016:

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality, as well as provide us an overview of their current product offerings, go-to-market strategy, and future road map. We also requested online access to the demo environment for further independent review. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also fielded an online survey to at least three customer references per vendor, and conducted one 30-minute phone interview with one of the references who completed the survey.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and

market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, go to http://www.forrester.com/marketing/policies/forrester-wave-methodology.html.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

Endnotes

[1] There are four main categories of digital risk data: 1) points of presence (POPs); 2) actors; 3) assets; and 4) affinities. POPs are the company-owned or company-sponsored domains that publicly represent an organization and where they conduct business online or in person. Actors are the people directly or indirectly associated with an organization, including employees, customers, third parties, and more. Assets are the organization's property, information, and other material items that hold intrinsic or strategic value. Affinities are the tangible and intangible connections among POPs, actors, and assets, often understood as relationships, interactions, sentiment, or processes. See the "Build Digital Risk Insight" Forrester report.

[2] Sophisticated social engineering, efficient data reconnaissance, software exploits, targeted spearphishing, account takeovers, spam — this is just a small sample of how cybercriminals and other adversaries are weaponizing social media. This report explains four ways social media is currently a major cyberthreat, what's really at stake for you organization, and practical steps security and risk pros can take to mitigate the risk. See the "Four Ways Cybercriminals Exploit Social Media" Forrester report.

[3] Source: Tim Nudd, "Man Poses as Target on Facebook, Trolls Haters of Its Gender-Neutral Move With Epic Replies," Adweek, August 13, 2015 (http://www.adweek.com/adfreak/man-poses-target-facebook-trolls-haters-its-gender-neutral-move-epic-replies-166364).

[4] Between 2013 and 2015, the percentage of US online adults owning a personal computer, a tablet, and a smartphone grew from 6% to 37%. Consumers now rely on and are empowered by technology to accomplish everyday tasks: US online adults spent an average of 1 hour a day using their mobile phone in 2013; by 2015, the daily average had grown to just over 2 hours. See the "The Rise Of The Empowered Customer" Forrester report.

[5] Given mobile technology's high penetration rates and increasing sophistication, empowered customers rarely think of digital experiences as separate from their physical ones — the two are becoming seamlessly integrated. For example, a growing 17% of US online adults now use their mobile phone to get additional product information while walking through a brick-and-mortar store, while 46% want to use in-store tools to visualize a product in their home today. See the "The Rise Of The Empowered Customer" Forrester report.

[6] Source: Teri Robinson, "Bogus Pokemon GO Ultimate app on GooglePlay locks screen, trawls porn ads," SC Magazine, August 2, 2016 (http://www.scmagazine.com/bogus-pokemon-go-ultimate-app-on-googleplay-locks-screen-trawls-porn-ads/article/513621/).

Source: Phil Muncaster, "Malware Fears as Pokémon Threats Go Social," Infosecurity Magazine, September 8, 2016 (http://www.infosecurity-magazine.com/news/malware-fears-as-pokemon-threats/).

Source: Kaveh Waddell, "The Twitter Bot That Sounds Just Like Me," The Atlantic, August 18, 2016 (http://www.theatlantic.com/technology/archive/2016/08/the-twitter-bot-that-sounds-just-like-me/496340/).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.