The Forrester New Wave™: External Threat Intelligence Services, Q3 2018

Tools And Technology: The Security Architecture And Operations Playbook

by Josh Zelonis
September 7, 2018

Why Read This Report

In Forrester's evaluation of the emerging market for external threat intelligence, we identified the 15 most significant providers in the category — Accenture, CrowdStrike, Digital Shadows, FireEye, Flashpoint, Group-IB, Hold Security, Intel 471, IntSights, Kaspersky Lab, Proofpoint, PwC, Recorded Future, Secureworks, Verint — and evaluated them. This report details our findings about how well each vendor scored against 10 criteria and where they stand in relation to each other. S&R pros can use this review to select the right partner for their needs.

Key Takeaways

FireEye Leads The Pack

Forrester's research uncovered a market in which FireEye is a Leader; CrowdStrike, Hold Security, Recorded Future, Flashpoint, Kaspersky Lab, Group-IB, and Intel 471 are Strong Performers; PwC, Accenture, Proofpoint, and Secureworks are Contenders; and Digital Shadows, Verint, and IntSights are Challengers.

Vendor Collection Strategies Are The Biggest Differentiator In The Market

Different vendors have access to different types of information based on the focus of their business and other services offered. The way they collect and use this information has a broad impact on the type of intelligence they can produce.

The Forrester New Wave™: External Threat Intelligence Services, Q3 2018

Tools And Technology: The Security Architecture And Operations Playbook

by Josh Zelonis
with Stephanie Balaouras, Nick Hayes, Madeline Cyr, and Peggy Dostie

September 7, 2018

Table Of Contents

Related Research Documents

Job Description: Director Of Threat Intelligence

The State Of The Threat Intelligence Platform Market, Q3 2018

Vendor Landscape: External Threat Intelligence, 2017

FORRESTER®

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

The Threat Intelligence Market Needs Better Outcome-Based Messaging

Many organizations struggle with selecting an external threat intelligence vendor because of the myriad vendors claiming to provide the service and the lack of objective messaging; as a result, prospective customers struggle to build an effective collection strategy. Journeymen in the space will have had experience with many of the vendors in this report, but they may be less familiar with others — who might actually provide better results. Keep in mind that:

- **Your collection strategy dictates what can be delivered.** Much like fishing with the wrong bait, without the right collection strategy, you aren't going to catch what you want. In seeking to better understand the individual offerings these vendors provide, we started by looking at the sources of information they were using to generate intelligence. This helped differentiate between claims of capability and believability of these claims.
- **This Forrester New Wave™ is comparing vendors with a wide variety of services.** According to the Forrester Analytics Global Business Technographics® Security Survey, 2018, global network security decision makers who have seniority level of manager or above and are working at enterprise organizations (of 1,000 employees or more) pay to subscribe to an average of 4.2 commercial threat intelligence feeds.[1] Don't look at the New Wave graphic and think there's a single best vendor for everyone reading this report. This research is not intended to help you select only one threat intel vendor; it's trying to help you understand how to assemble the best 4.2 vendors to fulfill your particular need.[2]
- **The surface and dark web criteria were difficult and highly differentiating.** Someone saying something on the dark web doesn't make it true. Anyone with a TOR browser can access the dark web and visit markets to see all manner of items and services for sale. In these "open" marketplaces, you have to assume lot of the most sordid material is either grifting or law enforcement (read: low confidence). To obtain higher confidence intelligence, you need to access private forums. Because the dark web has become such a focal point of vendor marketing, it was important to allow vendors to demonstrate an understanding of these concepts and provide examples of how they leverage private or closed sources to help cut through the noise.

External Threat Intel Evaluation Overview

The Forrester New Wave differs from our traditional Forrester Wave™. In the New Wave evaluation, we evaluate only emerging technologies, and we base our analysis on a 10-criteria survey and a 2-hour briefing with each evaluated vendor. We group the 10 criteria into current offering and strategy (see Figure 1). We also review market presence.

We included 15 vendors in this assessment: Accenture, CrowdStrike, Digital Shadows, FireEye, Flashpoint, Group-IB, Hold Security, Intel 471, IntSights, Kaspersky Lab, Proofpoint, PwC, Recorded Future, Secureworks, Verint (see Figure 2 and see Figure 3). Each of these vendors has:

- **At least 75 enterprise threat intelligence customers.** Each participant has a minimum of 75 enterprise customers.
- **Significant dedicated dark web collection capabilities.** Participants have a strong focus and a significant team of analysts dedicated to dark web collection.
- **Forrester client mindshare.** Forrester clients often discuss the participating vendors during inquiries and interviews. Alternatively, the participating vendor may, in Forrester's judgment, have warranted inclusion because of technical capabilities and market presence.

FIGURE 1 Assessment Criteria

Evaluation criteria	Criteria explanation
Surface web intelligence	What specific outcomes does the vendor's surface web capabilities enable? How does the vendor measure the efficacy of this collection strategy? How does the vendor leverage analysts and technology to fulfill this collection strategy?
Dark web intelligence	How well does the vendor articulate its expertise with regard to the dark web? What specific outcomes does this capability enable? How does the vendor measure the efficacy of this collection strategy? How does the vendor leverage analysts and technology to fulfill this collection strategy?
Technical intelligence	How well does the vendor articulate expertise with regard to malware analysis and collection using sensor networks and DFIR capabilities? What do its technical intelligence capabilities enable? How does the vendor measure efficacy? How does the vendor use analysts and technology to fulfill this purpose?
Threat feeds	What contextual intelligence does the vendor provide to enrich threat and indicator data? Do threat feed indicators include confidence scores? How well does the true positive/false positive ratio mirror the assigned confidence? How well is this feed helping organizations detect and identify threats?
Nation-state focus	How well does the vendor demonstrate expertise regarding state-sponsored actors to help organizations defend themselves against this type of attack? How does the vendor's collection strategy support a focus on nation-state actors? What unique and differentiating capabilities enable it to stand out from its peers?
Cybercriminal focus	How well does the vendor demonstrate expertise regarding cybercriminal trends and actors? How does the vendor's collection strategy support a cybercriminal focus? How do client references value this capability? What unique and differentiating capabilities enable it to stand out from its peers?
Financial crime focus	How well does the vendor demonstrate expertise regarding financial crimes and associated actors to serve this buyer persona? How does the vendor's collection strategy support a focus on financial crime? What unique and differentiating capabilities enable it to stand out from its peers?
Vision and execution	How well does the vendor execute its vision for its threat intelligence (TI) capability? How does the vendor articulate the importance of its TI capability to overall business? What SLAs are in place for requests for intelligence (RFIs)? How well do they execute on RFIs? What is its road map for improving the delivery of TI?
Global reach	What languages and dialects are the vendor's analysts fluent in, and how does this help the vendor achieve its mission? How does the vendor use regional presence to its advantage with regard to the entire intelligence cycle? How does the vendor leverage threat intelligence to reach a global audience?
Strategic partnerships	How does the vendor supplement its collection strategy with partnerships? Is this vendor seen as a source of threat intelligence that it is partnered with by other vendors in the space? How does the vendor support the community at large in valuing and understanding how to work with threat intelligence?

FIGURE 2 Forrester New Wave™: External Threat Intelligence Services, Q3 2018

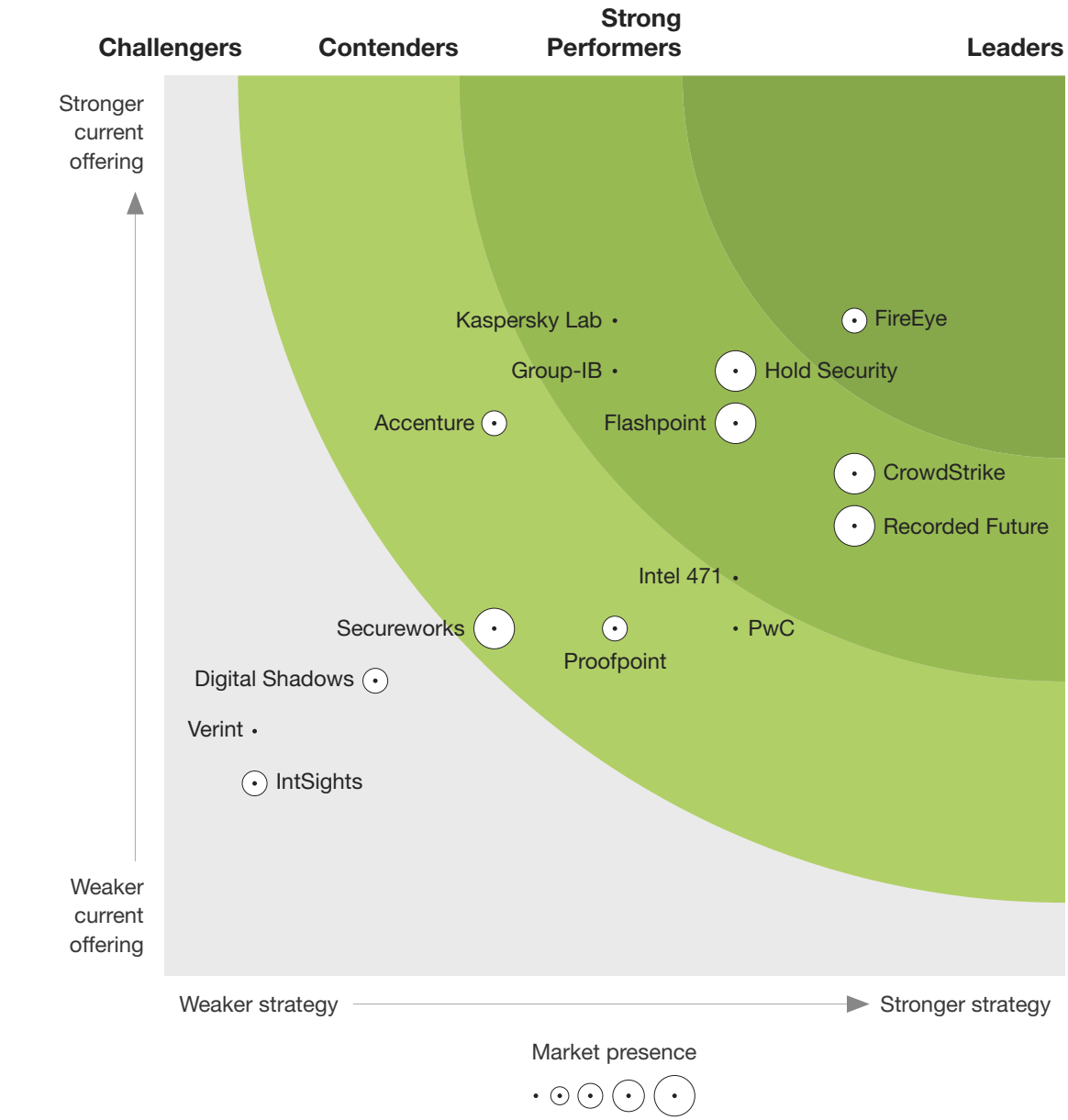


FIGURE 3 Vendor QuickCard Overview

Vendor QuickCards

Forrester evaluated 15 vendors and ranked them against 10 criteria. Here's our take on each.

FireEye: Forrester's Take

Our evaluation found that FireEye (see Figure 4):

- **Leads the pack with its collection capabilities.** The importance of iSight Partners and Mandiant cannot be overlooked when assessing FireEye's threat intelligence capabilities, which marry digital forensics, human intelligence (HUMINT), and a global sensor network.
- **Still needs to do a better job enriching its threat feeds.** FireEye doesn't include confidence scores with its threat feeds, so it's difficult to know if alerts are actionable. The aging process, which allows you to understand how time may impact confidence, is functional but could be better implemented.
- **Is the best fit for companies desiring a breadth of outcomes from a single vendor.** Quilting together commercial vendors to accommodate your intelligence requirements can be a challenge. FireEye simplifies this process with an internationally recognized offering based on a wide collection capability.

FireEye Customer Reference Summary

FireEye customer references were impressed with the depth of analysis on a wide range of topics; however, FireEye scored low on RFI responsiveness compared to other vendors.

FIGURE 4 FireEye QuickCard

FireEye

Wave position
LEADER

- **Surface web intelligence**
- **Dark web intelligence**
- **Technical intelligence**
- **Threat feeds**
- **Nation-state focus**
- **Cybercriminal focus**
- **Financial crime focus**
- **Vision and execution**
- **Global reach**
- **Strategic partnerships**

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"They have great resources and in-depth analysis on a wide breadth of topics."

"Their reporting on Russian state-sponsored actors is quite good."

Products evaluated
Cyber Threat Intelligence Services

CrowdStrike: Forrester's Take

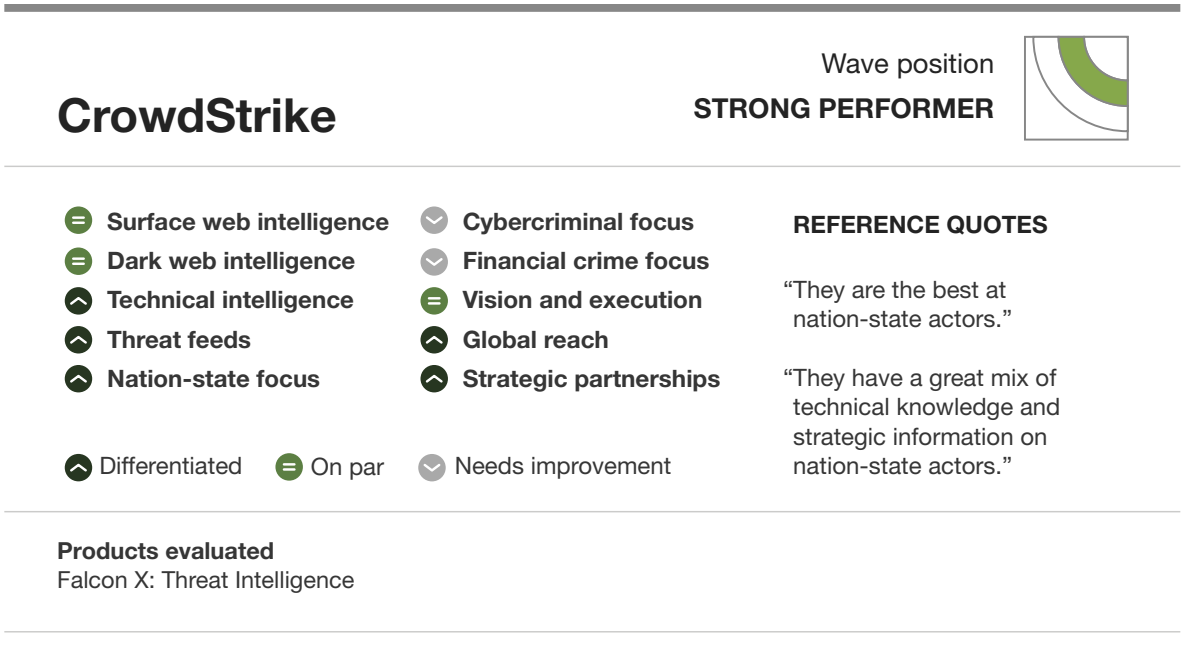
Our evaluation found that CrowdStrike (see Figure 5):

- **Leads the pack with its coverage of nation-state actors.** CrowdStrike's nation-state capability is built on a forensic service that brings it into many of the world's largest breaches, and visibility provided by a global sensor network resulting from its endpoint detection and response (EDR) and threat hunting offerings.
- **Still needs to improve its coverage of cybercriminal actors.** While CrowdStrike has the necessary technical collection capabilities and strong messaging in support of its cybercrime coverage, clients report this is still a commodity offering.
- **Is best for organizations looking for analytical coverage of advanced threat activity.** CrowdStrike provides an engaged threat intelligence partner that is responsive to RFIs and brings a focus on nation-state threats, specifically those targeting western organizations.

CrowdStrike Customer Reference Summary

CrowdStrike wows customers with its well-developed focus on nation-state actors and personalized engagement, although its API integrations are reported to be limited.

FIGURE 5 CrowdStrike QuickCard



Hold Security: Forrester's Take

Our evaluation found that Hold Security (see Figure 6):

- **Leads the pack with the ability to uncover and investigate cybercrime.** Hold Security has impressive collection capabilities, not only leveraging analyst expertise for infiltrating closed sources, but having them train machine learning models to scale their capabilities.
- **Doesn't provide indicator threat feeds.** Hold Security is able to provide a lot of depth in its provided intelligence, but it's not structured to provide traditional threat indicator feeds.
- **Is best for companies requiring human expertise in surface- and dark-web capabilities.** Hold Security has leading HUMINT capabilities and is differentiated by its commitment to diversity.

Hold Security Customer Reference Summary

Hold Security customers were impressed by its ability to monitor the dark web and return actionable intelligence. Hold Security also scored high on its reliable RFIs process. However, references noted that the business is a bit distributed, which can confuse messaging.

FIGURE 6 Hold Security QuickCard

Hold Security

Wave position
STRONG PERFORMER

- **Surface web intelligence**
- **Dark web intelligence**
- **Technical intelligence**
- **Threat feeds**
- **Nation-state focus**
- **Cybercriminal focus**
- **Financial crime focus**
- **Vision and execution**
- **Global reach**
- **Strategic partnerships**

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"They provide great insight on threat-actor pricing strategy, motivations, and mentalities."

"They are extremely reliable, and their intelligence is actionable."

Products evaluated
Hold Security

Recorded Future: Forrester's Take

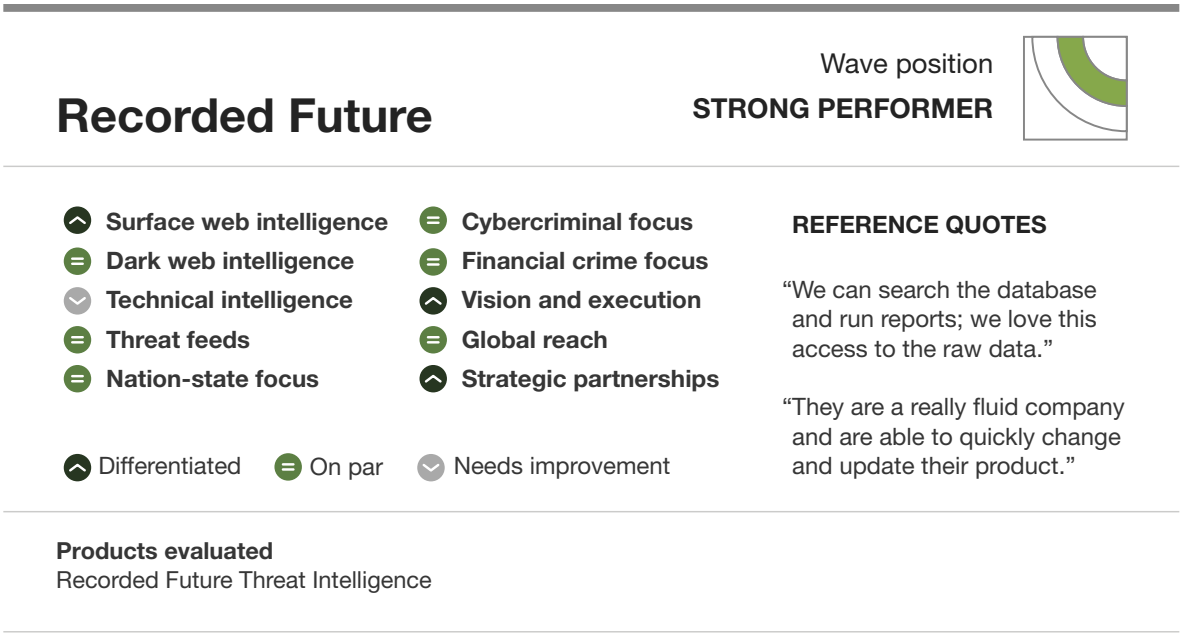
Our evaluation found that Recorded Future (see Figure 7):

- **Leads the pack with robust collection and access to raw intelligence.** Recorded Future prides itself on technical innovation using a combination of technologies such as machine learning and natural language processing to enable it to perform automated collection and processing of data at massive scale.
- **Is weaker with technical collection.** Recorded Future doesn't have access to global sensor networks the way endpoint vendors or managed security service providers would, and, as a result, it doesn't have as much visibility into campaign-level data.
- **Is the best fit for organizations looking for raw intelligence.** The most important reason to choose Recorded Future is that it makes all its raw intelligence available, organizing it into "Intelligence Cards" that enhance the ability for analysts to consume information. In short, Recorded Future makes your analysts better.

Recorded Future Customer Reference Summary

Recorded Future customers were impressed with its speed of innovation and access to raw intelligence; however, they noted a need to communicate changes to its product better.

FIGURE 7 Recorded Future QuickCard



Flashpoint: Forrester's Take

Our evaluation found that Flashpoint (see Figure 8):

- **Leads with closed-source analysis of cybercrime activities.** Flashpoint is focused on providing finished intelligence to inform business risk, based on a dark web collection strategy to uncover cybercrime and hacktivism targeting its clients.
- **Still needs to develop its nation-state capabilities.** While Flashpoint has the ability to obtain insights into nation-state activity, its collection capabilities don't directly support this objective.
- **Is the best fit for companies requiring finished intelligence reporting on business risk.** Flashpoint intelligence is grounded in the dark web, but it will develop custom collection strategies, even deploying custom infrastructure, to meet customer intelligence requirements.

Flashpoint Customer Reference Summary

Customer references have rated Flashpoint high on financial crime and responsiveness to RFIs. Customers are impressed at its access to obscure sources and hope to see its front-end web portal improve.

FIGURE 8 Flashpoint QuickCard

Flashpoint

Wave position
STRONG PERFORMER

- **Surface web intelligence**
- **Dark web intelligence**
- **Technical intelligence**
- **Threat feeds**
- **Nation-state focus**
- **Cybercriminal focus**
- **Financial crime focus**
- **Vision and execution**
- **Global reach**
- **Strategic partnerships**

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"They provide great insights on cybercrime on the dark web and hacktivism."

"RFI responsiveness has been tremendous."

Products evaluated
Flashpoint Intelligence Platform

Kaspersky Lab: Forrester's Take

Our evaluation found that Kaspersky Lab (see Figure 9):

- **Leads with a strong collection strategy and nation-state intelligence.** Kaspersky Lab has a lot to offer in terms of an international research and analysis team and global sensor network of endpoint agents, and its ability to collect and analyze information is exceptional.
- **Is still developing a messaging strategy for the current political landscape.** It's been a rough couple of years in the geopolitical spotlight, which has undoubtedly cost it prospective clients, but its attempts to do damage control distracts from its overall messaging.
- **Is best for nation-state intel that is not necessarily aligned with western governments.** Much like the importance of reading international newspapers to understand differing perspectives on what's happening in the world, for a broader perspective that is independent of western sources, you need sources from outside of those countries.

Kaspersky Lab Customer Reference Summary

Customers of Kaspersky Lab value its wide global reach and ability to monitor and locate threats in all parts of the world. Its intelligence team of analysts and researchers is recognized for its talent. References would like more information on how to use the data Kaspersky Lab provides.

FIGURE 9 Kaspersky Lab QuickCard

Kaspersky Lab

Wave position
STRONG PERFORMER

^ **Surface web intelligence**	^ **Cybercriminal focus**
^ **Dark web intelligence**	= **Financial crime focus**
^ **Technical intelligence**	= **Vision and execution**
^ **Threat feeds**	^ **Global reach**
^ **Nation-state focus**	^ **Strategic partnerships**

^ Differentiated = On par ^ Needs improvement

REFERENCE QUOTES

"Kaspersky Lab is a global company with the ability to monitor all parts of the world."

"Useful for strategic intel on threat actor campaigns and more-granular indicators."

Products evaluated
Kaspersky Lab Threat Intelligence Services

Group-IB: Forrester's Take

Our evaluation found that Group-IB (see Figure 10):

- **Leads the pack with intelligence on Russian-speaking cybercrime.** Group-IB is a Russian company specialized in cybercrime investigation and incident response. It is deeply connected with Russian infrastructure, running an accredited computer incident response team (CIRT) responsible for neutralizing fraudulent .ru top-level domains (TLDs).
- **Still needs to develop better customer communication.** A complaint from customers is it can occasionally be difficult to communicate with representatives of Group-IB due to language barriers.
- **Is best for companies that need visibility into the Russian-speaking underground.** Group-IB performs digital forensics on a majority of high-profile cyberattacks against Russian institutions, allowing insights into attack trends before the adversaries begin to target western organizations.

Group-IB Customer Reference Summary

Group-IB scored high with its customers on informing them of general cybercrime trends. Customers would like it to improve RFI responsiveness speed.

FIGURE 10 Group-IB QuickCard

Group-IB

Wave position
STRONG PERFORMER

- **Surface web intelligence** (On par)
- **Dark web intelligence** (On par)
- **Technical intelligence** (Differentiated)
- **Threat feeds** (On par)
- **Nation-state focus** (On par)
- **Cybercriminal focus** (Differentiated)
- **Financial crime focus** (Differentiated)
- **Vision and execution** (On par)
- **Global reach** (Needs improvement)
- **Strategic partnerships** (Differentiated)

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"Group-IB discovered malware targeting our customer and allowed us to take action."

"Their threat intelligence reports are actionable and have been put together by real people."

Products evaluated
Threat Intelligence

Intel 471: Forrester's Take

Our evaluation found that Intel 471 (see Figure 11):

- **Leads the pack with robust closed-source collection.** Intel 471 has robust HUMINT capabilities with a boots-on-the-ground approach to having analysts geographically located in the regions they are responsible for monitoring, to ensure local perspective and cultural understanding.
- **Is still improving its technical threat feed capabilities.** Currently limited to bulletproof hosting information, Intel 471 is developing a malware analysis capability to better take advantage of code and sample binaries that are acquired through its collection capabilities.
- **Is best for companies requiring closed-source intelligence on cybercriminals.** Intel 471 has one of the largest analyst pools focused on dark web intelligence in the industry, singularly tasked with obtaining and elevating access to mapping out the underground and developing relationships with targeted actors.

Intel 471 Customer Reference Summary

Intel 471 customers are happy with its ability to monitor financial crime and how hard it works for its customers.

FIGURE 11 Intel 471 QuickCard

Intel 471

Wave position
STRONG PERFORMER

- Surface web intelligence
- Dark web intelligence
- Technical intelligence
- Threat feeds
- Nation-state focus
- Cybercriminal focus
- Financial crime focus
- Vision and execution
- Global reach
- Strategic partnerships

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"They are willing to go all out for customer questions and complete RFIs."

"Intel 471 provided us with chatter about our brand that led to actionable intelligence."

Products evaluated
Adversary Intelligence

PwC: Forrester's Take

Our evaluation found that PwC (see Figure 12):

- **Leads with a nation-state capability grounded in its technical intelligence.** PwC combines its digital forensics consultancy with the internal intelligence gathered from managed security services customers, which enables robust outcomes.
- **Is reliant on strategic partnerships for a lot of its collection.** This impacts its ability to do next-level analysis and directly engage adversaries. As a result, client feedback indicates a commodity level of threat intelligence regarding cybercriminal activities.
- **Is the best fit for companies that wish to outsource their threat intelligence capability.** PwC has a broad collection capability, achieved through partnership as well as resulting from services it provides, which allows its clients to benefit from having the threat intelligence capability of a much larger organization.

PwC Customer Reference Summary

PwC received praise from its customer references on its size and reach as well as its technical abilities like reverse engineering indicators of compromise. Its customers would like to see it invest in building out its platform.

FIGURE 12 PwC QuickCard

PwC

Wave position
CONTENDER

Surface web intelligence	Cybercriminal focus
Dark web intelligence	Financial crime focus
Technical intelligence	Vision and execution
Threat feeds	Global reach
Nation-state focus	Strategic partnerships

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"PwC is a thought leader on nation-state actors."

"Their strengths are size, reach, analyst core, and technical ability."

Products evaluated
PwC's Threat Intelligence Service

Accenture: Forrester's Take

Our evaluation found that Accenture (see Figure 13):

- **Leads with tailored threat feeds and a focus on cybercrime.** A major focus of the Accenture offering is being able to tailor intelligence to your organization, from information about actors targeting your vertical, to vulnerabilities and malware being leveraged to do so.
- **Overprioritizes the presentation layer when highlighting its capabilities.** Accenture struggles to communicate the value of the intelligence product and instead relies on impressing clients with how the intel is organized in its platform to establish value.
- **Is the best fit for companies looking for a single source of truth for their intel.** It's probably not an accident that Accenture values its portal so highly; that is also what its clients recommend the most about the offering.

Accenture Customer Reference Summary

Customer references found Accenture's RFI process, portal, platform, and intelligence gathering to be very mature. Customers did note that they wish that they had access to the raw data.

FIGURE 13 Accenture QuickCard

Accenture

Wave position
CONTENDER

= **Surface web intelligence**	^ **Cybercriminal focus**	
= **Dark web intelligence**	= **Financial crime focus**	
= **Technical intelligence**	v **Vision and execution**	
^ **Threat feeds**	= **Global reach**	
= **Nation-state focus**	= **Strategic partnerships**	

^ Differentiated = On par v Needs improvement

REFERENCE QUOTES

"They have a mature RFI process."

"Overall, they are quite advanced with the portal, the platform, and how they organize intelligence."

Products evaluated
IDefense

Proofpoint: Forrester's Take

Our evaluation found that Proofpoint (see Figure 14):

- **Leads with email-centric insight into the threat landscape and situational awareness.** It's no secret that a majority of attacks leverage email as a vector. By focusing on these types of campaigns, Proofpoint can provide insight into attacks before they hit the endpoint.
- **Relies on partnerships for collection beyond its customer networks.** Proofpoint does most of its collection using sensors deployed across its customer networks and supplements this with partner feeds for additional context. When further insight is required, it has a small team of reputable analysts dedicated to external collection.
- **Is best for product customers looking to add internal context to external intel.** Proofpoint leverages its global sensor network and malware analysis capabilities to help you detect threats, but it also adds context as internal intelligence, allowing you to understand who is most targeted within your organization and, therefore, most at risk.

Proofpoint Customer Reference Summary

Proofpoint customers look to it to understand high-level strategic threats on their landscape; however, they would like to see its intelligence focus on being more individualized and tailored.

FIGURE 14 Proofpoint QuickCard

Proofpoint

Wave position
CONTENDER

- Surface web intelligence
- Dark web intelligence
- Technical intelligence
- Threat feeds
- Nation-state focus
- Cybercriminal focus
- Financial crime focus
- Vision and execution
- Global reach
- Strategic partnerships

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"They are great at exposing new campaigns."

"They give a raw view of the threat landscape to help us understand the data we are seeing."

Products evaluated
Proofpoint Threat Information Services

Secureworks: Forrester's Take

Our evaluation found that Secureworks (see Figure 15):

- **Leads with robust technical collection and nation-state intelligence.** Secureworks has a technical collection capability built on its managed security services and digital forensic investigations, which allows it to use client data to generate intelligence.
- **Still needs to develop its cybercriminal intelligence.** Clients recognize Secureworks for its brand monitoring but express concerns about its cybercrime capabilities and lack of threat intelligence integration.
- **Is the best fit for MSS customers looking for a dedicated in-house intel team.** Secureworks has a dedicated threat intel capability it calls its Counter Threat Unit, and makes its threat intelligence services to available to non-MSS customers, but the primary use case or this service is to supplement its MSS offering.

Secureworks Customer Reference Summary

Secureworks customers are impressed with its brand-monitoring abilities and its ability to do independent research. Customers would like better API access instead of being tied into the Secureworks portal.

FIGURE 15 Secureworks QuickCard

Secureworks

Wave position
CONTENDER

Surface web intelligence	Cybercriminal focus
Dark web intelligence	Financial crime focus
Technical intelligence	Vision and execution
Threat feeds	Global reach
Nation-state focus	Strategic partnerships

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"Secureworks provides top-tier brand protection."

"Their researchers are able to find the needle in the haystack."

Products evaluated
Secureworks Threat Intelligence Services

Digital Shadows: Forrester's Take

Our evaluation found that Digital Shadows (see Figure 16):

- **Leads the pack with robust brand monitoring capabilities.** Digital Shadows has a very tailored offering combining automated collection and HUMINT to provide customers with intelligence targeted toward their organizations.
- **Needs to improve its closed-source collection capabilities.** While Digital Shadows does have a HUMINT capability and does have a dark-web presence, it doesn't have the maturity or depth of relationships of other vendors in this space.
- **Is the best fit for companies looking for an engaged threat intelligence partner.** Digital Shadows provides robust collection capabilities of open sources, making it a great partner for brand monitoring. Further, it is an engaged partner, with the analyst expertise needed to research and respond to RFI in a level of detail dictated by the customer.

Digital Shadows Customer Reference Summary

Digital Shadows customers scored it high on tailoring the threat intelligence to their needs. They also praised its customer engagement. Customers would like to see presentation of data on the portal improve.

FIGURE 16 Digital Shadows QuickCard

Digital Shadows

Wave position
CHALLENGER

▲ **Surface web intelligence**	= **Cybercriminal focus**
▼ **Dark web intelligence**	= **Financial crime focus**
▼ **Technical intelligence**	▼ **Vision and execution**
▼ **Threat feeds**	▼ **Global reach**
▼ **Nation-state focus**	= **Strategic partnerships**

▲ Differentiated = On par ▼ Needs improvement

REFERENCE QUOTES

"They have great customer engagement."

"Digital Shadows is great at tailoring its intelligence and helping us monitor our digital assets."

Products evaluated
Digital Shadows SearchLight

Verint: Forrester's Take

Our evaluation found that Verint (see Figure 17):

- **Leads with monitoring cybercriminal forums and language expertise.** In 2017, Verint acquired SenseCy to add threat intelligence capabilities to its portfolio. These capabilities are primarily focused on brand protection and fraud intelligence provided by monitoring the surface and dark web.
- **Provides limited threat intelligence.** While Verint has over 60 analysts on staff, ranging from malware researchers to physical security researchers, its primary outcomes fit better as digital risk monitoring or fraud detection than as a specialized threat intel vendor.
- **Is best fit for orgs concerned about being targeted by hactivists or cybercriminals.** Verint is specialized in providing around-the-clock coverage, providing you visibility into emerging threats as well as the overall threat landscape as it applies to your organization.

Verint Customer Reference Summary

Verint customers praised its 24x7 availability and language expertise; however, customers would like it to share more threat intelligence.

FIGURE 17 Verint QuickCard

Verint

Wave position
CHALLENGER

- **Surface web intelligence**
- **Dark web intelligence**
- **Technical intelligence**
- **Threat feeds**
- **Nation-state focus**
- **Cybercriminal focus**
- **Financial crime focus**
- **Vision and execution**
- **Global reach**
- **Strategic partnerships**

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"They provide intelligence feeds for us against our industry and geolocation to help target what is a threat to us."

"The context makes the intelligence actionable."

Products evaluated
SenseCy Cyber Threat Intelligence Solutions

IntSights: Forrester's Take

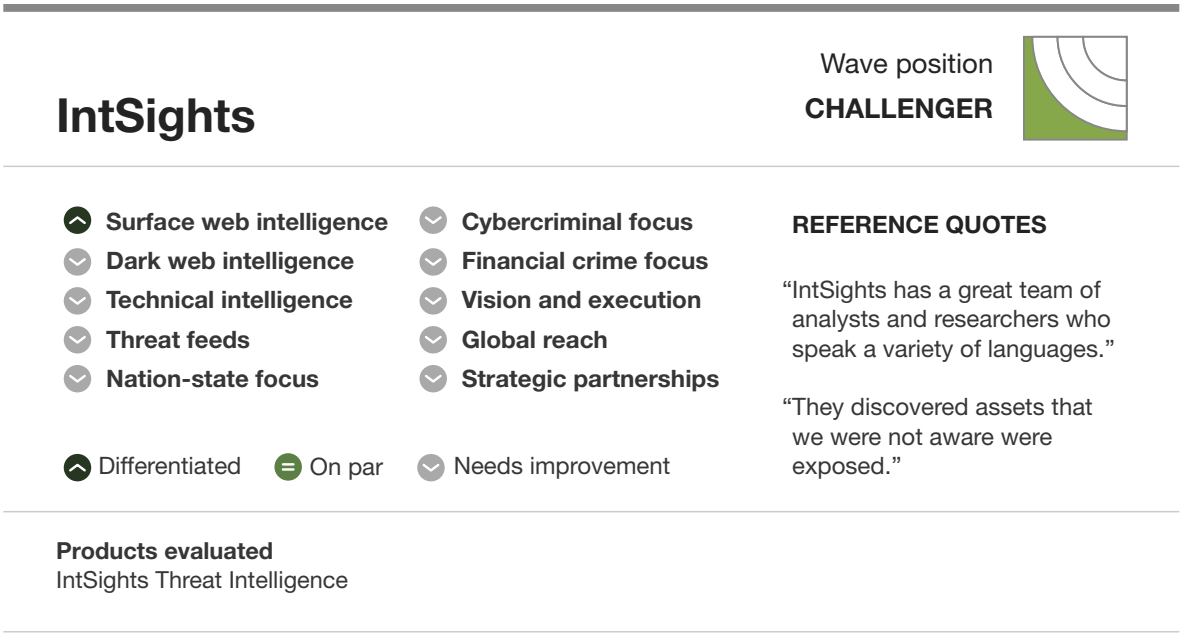
Our evaluation found that IntSights (see Figure 18):

- **Leads with a threat intelligence portal (TIP) and brand protection.** IntSights combines brand monitoring and alerting into one of the most widely deployed commercial TIPs.
- **Is overly focused on threat intel as a product and not a service.** The majority of organizations are going to have multiple feeds and need to centralize them in a TIP. While IntSights is both a provider of external threat intelligence and a TIP, the scoring in this New Wave only reflects its external threat intelligence offering and not its TIP capabilities.
- **Is the best fit for fraud and risk teams outside an organization's threat intel teams.** The largest percentage of its client base is in financial services. Given the general maturity of this vertical, the type of intelligence produced, and the TIP focus, this offering makes the most sense for teams focused on fraud detection, brand monitoring, and digital risk protection, which frequently reside outside an organization's threat intelligence capability.

IntSights Customer Reference Summary

IntSights customers mentioned that it is great at providing attack indicators and brand security. Customers said that they wished it provided more context to alerting.

FIGURE 18 IntSights QuickCard



Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Supplemental Material

The Forrester New Wave Methodology

We conducted primary research to develop a list of vendors that met our criteria for the evaluation and definition of this emerging market. We evaluated vendors against 10 criteria, seven of which we based on product functionality and three of which we based on strategy. We also reviewed market presence. We invited the top emerging vendors in this space to participate in an RFP-style demonstration and interviewed two customer references. We then ranked the vendors along each of the criteria. We used a summation of the strategy scores to determine placement on the x-axis, a summation of the current offering scores to determine placement on the y-axis, and the market presence score to determine marker size. We designated the top-scoring vendors as Leaders.

Integrity Policy

We conduct all our research, including Forrester New Wave evaluations, in accordance with the Integrity Policy posted on our website.

Survey Methodology

The Forrester Analytics Global Business Technographics Security Survey, 2018, was fielded between May and June, 2018. This online survey included 3,089 respondents in Australia, Canada, China, France, Germany, the UK, and the US.

Forrester Analytics Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Verizon

Rapid7

Hyperion Gray

Endnotes

[1] Source: Forrester Analytics Global Business Technographics Security Survey, 2018.

[2] See the Forrester report "Vendor Landscape: External Threat Intelligence, 2017."

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.