WAVE REPORT

The Forrester Wave™: External Threat Intelligence Service Providers, Q3 2023

The 12 Providers That Matter Most And How They Stack Up

August 3, 2023

By Brian Wrozek with Merritt Maxim, Caroline Provost, Christine Turley

FORRESTER®

Summary

In our 29-criterion evaluation of external threat intelligence service providers (ETISPs), we identified the 12 most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Additional resources are available in the online version of this report.

External Threat Intelligence Is Necessary For Effective Cybersecurity

Just relying on fundamental security controls and monitoring internal logs is no longer a sufficient strategy for effective cybersecurity. External cyber threat intelligence is now a necessary foundational component of any organization's cybersecurity defenses. Customers need help prioritizing threats efficiently and want long-term guidance about emerging threats for strategic initiative planning. Building a comprehensive, internal threat intelligence team can be challenging, so customers need providers who can offer diverse threat intelligence services. Customers are so hungry for information that they pay for an average of seven commercial threat feeds. To meet this growing demand, ETISPs are expanding the use cases they address, including investments in AI/ML algorithms to collect, process, analyze, and disseminate threat intelligence in machine- and human-readable formats; usability improvements; and more APIs for integration. Some customers want a total threat intelligence platform, some want curated alerts, and others just want the raw data.

As a result of these trends, S&R pros should look for ETISPs that:

- **Gather diverse sources of threat intelligence.** Few organizations have the time, money, and experts to collect, process, and store a vast amount of open source information and keep it up to date. It is even harder to gain access to the dark web and restricted sites. Look for providers who can supplement this information with malware analysis and attack telemetry from honeypot devices and proprietary sources like firewalls and endpoint detection and response (EDR) applications deployed across a global customer base. Some providers can even gather insights learned from responding to incidents or providing managed security services. Ensure the providers have a deep repository of historical data, routinely expand into new areas like Telegram channels, but also refresh existing sources regularly from all regions of the world.
- **Simplify the consumption of threat intelligence.** Indicators of compromise (IOC) feeds are standard offerings but are not enough by themselves. Look for providers who have a rich set of APIs to facilitate integration and automation across your technology portfolio to speed up detection, prevention, and response efforts. Providers should have a robust library of reports about threat actors, malware families, vulnerabilities, and industry trends. These human-readable reports should contain detailed tactics, techniques, and procedures (TTP) suitable for technical and executive audiences. The portal user experience should be rich with visualization and easy to pivot from a fact within a report to supporting information.

Providers should do the heavy lifting of connecting the dots from multiple threat data points to actions by adding contextual information, prioritization, and risk scoring. Give preference to ETISPs that can cut through the noise to deliver complete, accurate, relevant, and timely information with minimal false positives.

- **Act as a force multiplier.** The best providers enhance threat intelligence information with value-added services to promote better decision-making and drive tangible action to mitigate risks. They should provide recommendations based on their analysis of the threat intelligence, offer competitive peer data for benchmarking comparisons, and deliver targeted threat briefings to company executives. Providers should assist organizations in taking down rogue domains, removing masquerading social media profiles, performing threat hunting, and uplifting existing security staff with dedicated research and analyst resources. Providers should regularly solicit feedback on the quality and applicability of their threat intelligence. Organizations that are well informed are better prepared to mitigate cyber risks, but you may need additional support to turn that information into tangible action and results.

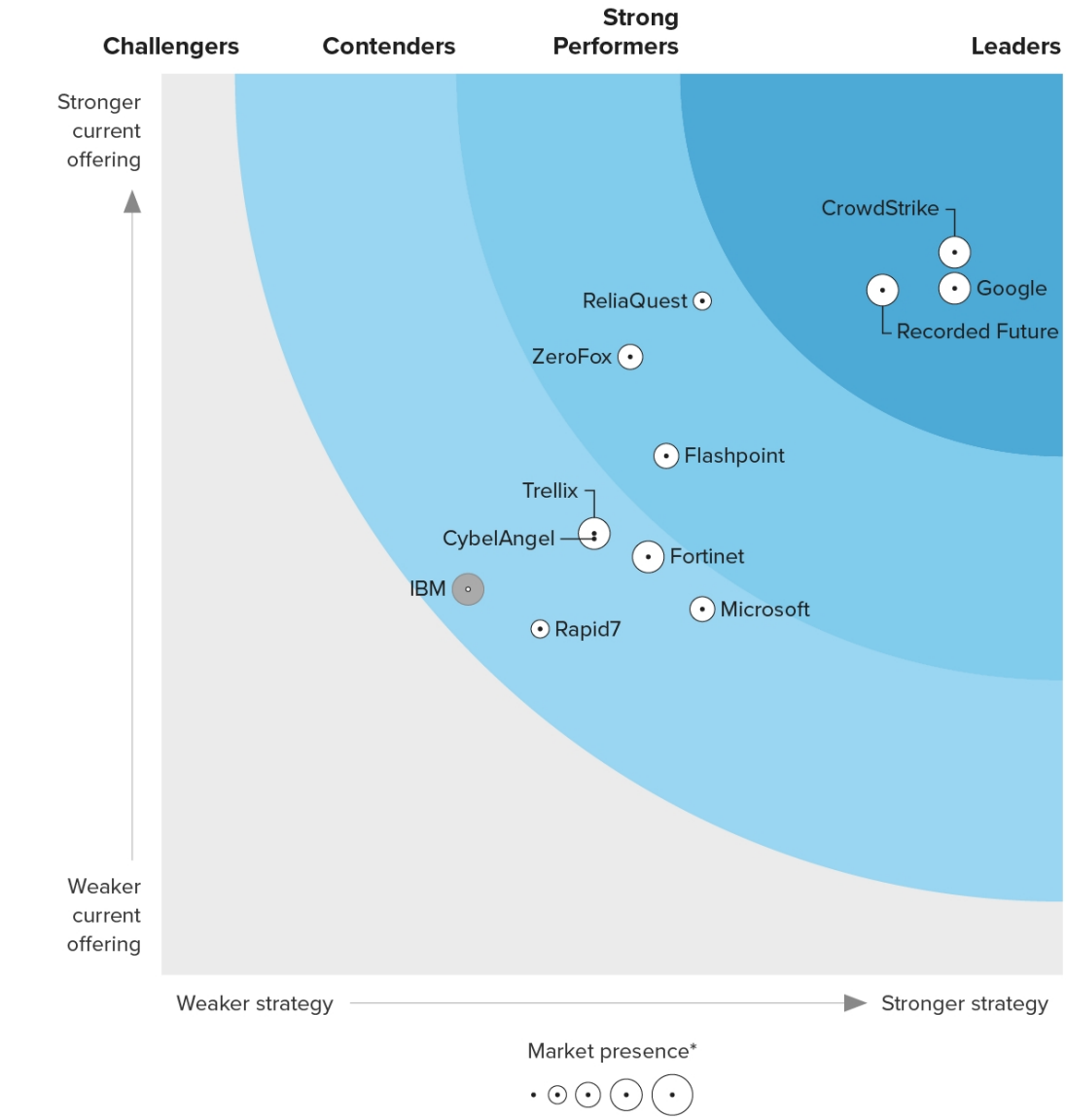
Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market; it doesn't represent the entire vendor landscape. You'll find more information about this market in our reports on threat intelligence.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figures 1 and 2). Click the link at the beginning of this report on Forrester.com to download the tool.

Figure 1

Forrester Wave™: External Threat Intelligence Service Providers, Q3 2023



*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2

Forrester Wave™: External Threat Intelligence Service Providers Scorecard, Q3 2023

	Forrester's weighting	CrowdStrike	CybelAngel	Flashpoint	Fortinet	Google	IBM*
Current offering	50%	4.01	2.42	2.88	2.32	3.81	2.14
Gathering intelligence requirements	4%	5.00	3.00	3.00	1.00	3.00	1.00
Intelligence collection sources	12%	4.00	2.00	3.00	3.00	4.00	2.50
Intelligence processing and analysis	13%	4.00	1.40	3.00	2.00	4.80	3.00
Dissemination	14%	5.00	1.80	3.00	2.80	4.00	3.00
Metrics and feedback	4%	5.00	3.00	3.00	1.00	1.00	1.00
Cyber threat intelligence (CTI)	11%	5.00	1.00	3.00	3.00	5.00	3.00
Digital risk protection (DRP)	11%	3.00	5.00	3.00	3.00	3.00	1.00
Special services	7%	1.00	3.00	3.00	3.00	1.00	1.00
RFIs for ad hoc needs	4%	3.00	3.00	3.00	1.00	3.00	1.00
Portal interface experience and capabilities	6%	3.00	1.00	1.00	1.00	5.00	1.00
Frameworks and models supported	4%	5.00	3.00	3.00	3.00	5.00	3.00
Analyst tradecraft expertise	6%	5.00	3.00	3.00	1.00	5.00	3.00
Privacy and data security controls	2%	3.00	5.00	3.00	3.00	1.00	1.00
Product security controls	2%	5.00	3.00	3.00	1.00	5.00	1.00
Strategy	50%	4.40	2.40	2.80	2.70	4.40	1.70
Vision	10%	3.00	5.00	5.00	3.00	3.00	1.00
Innovation	15%	5.00	3.00	3.00	3.00	5.00	3.00
Roadmap	15%	5.00	3.00	3.00	1.00	5.00	1.00
Partner ecosystem	20%	5.00	1.00	3.00	3.00	5.00	3.00
Pricing flexibility and transparency	20%	3.00	1.00	1.00	3.00	3.00	1.00
Community	20%	5.00	3.00	3.00	3.00	5.00	1.00
Market presence	0%	4.00	1.00	2.50	3.50	4.00	4.00
Revenue	50%	4.00	1.00	3.00	2.00	5.00	5.00
Number of customers	50%	4.00	1.00	2.00	5.00	3.00	3.00

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

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

	Forrester's weighting	Microsoft	Rapid7	Recorded Future	ReliaQuest	Trellix	ZeroFox
Current offering	50%	2.06	1.92	3.80	3.74	2.45	3.43
Gathering intelligence requirements	4%	1.00	1.00	3.00	5.00	3.00	3.00
Intelligence collection sources	12%	4.00	2.00	3.00	3.00	3.50	3.00
Intelligence processing and analysis	13%	2.00	1.80	4.00	3.80	3.20	2.00
Dissemination	14%	1.20	2.00	4.20	3.00	2.20	3.00
Metrics and feedback	4%	3.00	1.00	5.00	3.00	1.00	5.00
Cyber threat intelligence (CTI)	11%	3.00	1.00	3.00	3.00	3.00	3.00
Digital risk protection (DRP)	11%	1.00	3.00	5.00	5.00	1.00	5.00
Special services	7%	1.00	3.00	3.00	5.00	1.00	5.00
RFIs for ad hoc needs	4%	1.00	3.00	3.00	5.00	3.00	5.00
Portal interface experience and capabilities	6%	1.00	3.00	5.00	5.00	1.00	3.00
Frameworks and models supported	4%	1.00	1.00	5.00	3.00	3.00	1.00
Analyst tradecraft expertise	6%	3.00	1.00	3.00	3.00	3.00	5.00
Privacy and data security controls	2%	5.00	1.00	3.00	3.00	5.00	3.00
Product security controls	2%	3.00	1.00	3.00	3.00	3.00	3.00
Strategy	50%	3.00	2.10	4.00	3.00	2.40	2.60
Vision	10%	3.00	1.00	3.00	3.00	1.00	3.00
Innovation	15%	3.00	1.00	5.00	3.00	3.00	3.00
Roadmap	15%	3.00	3.00	5.00	3.00	3.00	3.00
Partner ecosystem	20%	3.00	1.00	3.00	1.00	3.00	3.00
Pricing flexibility and transparency	20%	3.00	3.00	3.00	5.00	3.00	3.00
Community	20%	3.00	3.00	5.00	3.00	1.00	1.00
Market presence	0%	2.50	1.50	3.50	2.00	3.50	3.00
Revenue	50%	3.00	2.00	4.00	2.00	3.00	3.00
Number of customers	50%	2.00	1.00	3.00	2.00	4.00	3.00

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

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor Offerings

Forrester evaluated the offerings listed below (see Figure 3).

Figure 3
Evaluated Vendors And Product Information

Vendor	Product evaluated
CrowdStrike	Falcon Intelligence
CybelAngel	CybelAngel
Flashpoint	Flashpoint Ignite
Fortinet	FortiGuard Threat Intelligence
Google	Google Threat Intelligence
IBM	X-Force Threat Intelligence
Microsoft	Microsoft Defender Threat Intelligence
Rapid7	Threat Command
Recorded Future	Recorded Future Intelligence Cloud
ReliaQuest	GreyMatter Digital Risk Protection
Trellix	Trellix Threat Intelligence
ZeroFox	ZeroFox External Cybersecurity Platform

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

- **CrowdStrike delivers world-class threat intelligence to power its Falcon platform.** CrowdStrike Falcon Intelligence enables an extensive set of threat intelligence use cases integrated into the CrowdStrike Falcon Platform. CrowdStrike is best known for its finely crafted human-written reports with an extensive adversary library plus the operational efficiencies delivered through the Falcon platform. CrowdStrike is researching and implementing large language models (LLMs) and generative AI to help customers more easily consume all the written intelligence they produce while they continue to expand automation workflows. CrowdStrike's cyber threat intelligence is well established, but its

brand-protection threat intelligence needs more development.

CrowdStrike supplements traditional public open sources and underground sources of intelligence with telemetry from its established Falcon Platform customer base, lessons learned from 500-plus incident response engagements, and experience gained by the Falcon OverWatch Threat Hunting teams. CrowdStrike tracks over 200 named nation-state, electronic crime, and hacktivist adversaries. While Falcon Intelligence Recon provides external visibility to stop attacks, CrowdStrike does not offer services such as taking down fraudulent domains that customers need. Reference customers find CrowdStrike's endpoint telemetry compelling, and they rely on the detailed TTPs in threat reports to drive fruitful threat-hunting exercises. CrowdStrike Falcon Intelligence is a comprehensive solution that firms should consider for an overall threat intelligence program even if they are not using the vendor's EDR tools.

- **Google is poised to become the most relevant and dominant threat intelligence provider.** Google Threat Intelligence combines existing Google capabilities with capabilities acquired via the September 2022 Mandiant acquisition. Mandiant Threat Intelligence, together with VirusTotal, delivers a comprehensive suite of solutions at a scale few can match. The Mandiant offerings can now leverage the power, scale, and innovation of Google to discover, personalize, and operationalize threat intelligence for customers. With much to offer, the variety of solution options and pricing models can be complex. Google has big ambitions to leverage its own platform and solutions like Google AI Security Workbench and PaLM, coupled with Google's vast internet visibility, to revolutionize its threat intelligence services.

  In addition to the vast number of suspicious files processed by VirusTotal, threat intelligence is sourced from malicious activity observed across Google's product ecosystem. Another advantage is the visibility provided by Mandiant's robust consulting services, especially incident response as Mandiant performs over a thousand breach response engagements annually. Google relies on third-party services to execute rogue domain and profile takedowns. It still has room to grow with its digital risk protection suite released in 2022. Reference customers were very satisfied with their overall experience using the portal, saying that the interface is intuitive, easy to navigate, and very user friendly. Google Threat Intelligence is ideal for global organizations that need robust cyber threat intelligence information.

- **Recorded Future is an easy-to-use yet powerful threat intelligence solution.** Recorded Future Intelligence Cloud is composed of nine specific threat intelligence modules, strategically designed and grouped for specific use cases and user personas. This allows customers to expand their deployment as they mature, but it requires additional licensing costs if a needed use case is part of another module. Recorded Future plans to aggressively expand data collection and analytics and enable customers to automate threat hunting while growing their geographic coverage deeper into EMEA and APAC. Recorded Future offers free tools like a browser extension, an asset discovery tool, and a free daily newsletter that has over 1.5 million subscribers.

  Recorded Future is best known for its extensive open source threat intelligence boasting over 10 billion entities in its Intelligence Graph ecosystem, which serves as the foundation for the Recorded Future Intelligence Cloud. It lacks the breadth and depth of internal telemetry that some competitors gather from its proprietary technologies and services, like incident response engagements. The portal has multiple ways to provide feedback, and customers can benchmark to see how many alerting rules other Recorded Future customers in their industry have enabled, for example. Reference customers believe that Recorded Future's open source threat intelligence is best in class but felt the dark web threat intelligence wasn't at the same level. The most consistent complaint from references was about the high price tag. Recorded Future Intelligence Cloud is best suited for customers who need comprehensive threat intelligence in an intuitive, user-friendly platform.

Strong Performers

- **ReliaQuest is expanding its already solid threat intelligence capabilities.** GreyMatter Digital Risk Protection is the threat intelligence solution resulting from ReliaQuest's acquisition of Digital Shadows in June 2022. Digital Shadows was primarily known for brand protection, vulnerability management, and threat-hunting capabilities. GreyMatter Digital Risk Protection differentiates itself from competitors with a straightforward, simple pricing model. While ReliaQuest partners with some information-sharing and analysis centers (ISACs) and a few government security agencies, its partner ecosystem is not as expansive as other threat intelligence providers. ReliaQuest's roadmap focuses on balancing enhancements to existing capabilities like expanding data collections and disruption services.

ReliaQuest uses a prescriptive and thorough requirement-gathering process. In addition to open and underground sources, ReliaQuest is now collecting technical telemetry from its GreyMatter security operations platform customers and lessons learned from its incident response and threat-hunting engagements. The portal interface is simple to navigate with an abundance of options that can be configured by the customer. Alert risk scoring is based on the Factor Analysis of Information Risk (FAIR) model and can be adjusted to the customer's risk appetite. GreyMatter Digital Risk Protection includes other use cases like external attack surface management (EASM), but they are not as robust as the rest of the portfolio. Reference customers valued the actionability of the threat intelligence and the triage page specifically but expressed some concerns about missing specific local and regional sources outside of Europe and America. ReliaQuest is an ideal fit for North American and EMEA companies with small to midsize security teams that may not have dedicated threat intelligence analysts.

- **ZeroFox analysts provide valuable disruption services to a growing portfolio.** ZeroFox External Cybersecurity Platform is composed of four main components: protection, intelligence, disruption, and response. ZeroFox is best known for its suite of digital risk protection. However, the vendor has an active history of acquiring companies to expand not only threat intelligence capabilities but also complementary services like incident response. Some of the next steps in this evolution are to further expand into areas like EASM and offer more comprehensive executive-protection capabilities. ZeroFox is not as active in the community as other threat intelligence providers beyond participating in the usual events or publishing free reports.

  ZeroFox collects a substantial amount of information from the dark web and presents it in the main portal dashboard. ZeroFox gathers additional intelligence from its extensive incident response services but lacks telemetry from proprietary technologies. ZeroFox is customer obsessed with active metric, feedback, and quality review initiatives. Its disruption services team is dedicated to performing tens of thousands of disruptive actions per week like domain takedowns, with success rates in the 95%-plus range. Reference customers were very satisfied with brand protection capabilities, especially social media monitoring. References said alerts were timely; however, they complained it took a fair amount of time to reduce the initial volume of false positives. ZeroFox is relevant for customers of any size that need a holistic external cybersecurity platform based on external threat intelligence.

- **Flashpoint excels in fraud and compromised credentials intelligence.** Flashpoint Ignite threat intelligence solutions are grouped into four distinct modules to deliver cyber threat intelligence, vulnerability management, physical security intelligence, and national security intelligence. Flashpoint purchased Risk Based Security in January 2022 to strengthen its vulnerability and data breach intelligence. Flashpoint excels at collecting information from underground and dark web sources but acquired Echosec in August 2022 to enhance its open source intelligence (OSINT) capabilities and strengthen its physical security intelligence. Flashpoint's published roadmap includes a convenient delivery confidence factor. Flashpoint offers a flexible yet complex a la carte pricing model but has introduced value-based bundles to simplify procurement.

  Flashpoint has a strong reputation and deep penetration in the financial services industry, especially for fraud intelligence and compromised credentials. Flashpoint's national security intelligence offering leverages a dedicated team to serve government agencies involved with national security. It also addresses the often-forgotten area of physical security threat intelligence. Portal features and overall user experience need improvement as reference customers wanted enhanced visualization for readability, easier searching, and more intuitive navigation. Reference customers felt the dark web threat intelligence was especially strong. Flashpoint is ideal for customers who need accurate and timely fraud and compromised credentials or bank account information intelligence.

Contenders

- **Microsoft is poised to be a disruptor to the threat intelligence market in the long term.** Microsoft Defender Threat Intelligence (MDTI) was released in 2022 and combines the capabilities and expertise from the prior RiskIQ acquisition, which includes PassiveTotal, along with its existing Threat Intelligence Center and Microsoft 365 Defender security resources. While MDTI currently has limitations, Microsoft continues to enhance overall functionality and usability in the short term by better incorporating its vast telemetry across all product offerings while investing in AI advancements. Microsoft plans to leverage generative AI so customers can use natural language to consume threat intelligence.

  Microsoft has the most expansive source of threat intelligence telemetry considering the reach of its commercial and enterprise cloud, endpoint, and other product customers. Microsoft is focused on integration with Microsoft technologies, but more work needs to be done to make it easier to navigate threat

intelligence across its technology landscape. MDTI is integrated into Microsoft Defender, yet traditional TIP features like mapping threat intelligence to the MITRE ATT&CK framework happens in Microsoft Sentinel. Reference customers are especially excited about the volume of telemetry and use MDTI for enrichment and automation across their existing Microsoft stack. References prefer the IOCs over the written threat reports. Microsoft Defender Threat Intelligence is ideal for existing Microsoft customers who want to consolidate vendors and are already on a path to be all-in with Microsoft. Customers should, however, supplement with another threat intelligence provider in the short term until the services mature and the integration becomes more seamless.

- **Fortinet delivers robust IOC integration, but its standalone portal needs development.** FortiGuard Threat Labs started in 2002 and is the source of FortiGuard Threat Intelligence that powers over 50 different products across the Fortinet landscape. FortiRecon Digital Risk Protection is an additional FortiGuard Threat Intelligence service providing external attack surface monitoring, brand protection, and adversary-centric intelligence. Fortinet is active in industry collaborations and partnerships and was a founding member of the World Economic Forum Centre for Cybersecurity. Fortinet plans to expand its portfolio by offering more industry vertical specific threat intelligence targeting areas like operational technology (OT) environments.

  The power of FortiGuard Threat Intelligence is the telemetry obtained and IOCs delivered across its extensive portfolio of products. FortiRecon still has plenty of maturing to do before it can compete with more established digital risk protection providers. FortiRecon has a standalone UI portal, but the rest of FortiGuard's Threat Intelligence capabilities are dependent on existing Fortinet technologies. For instance, FortiSOAR has the capabilities a threat analyst would expect in a standalone threat intelligence portal. Reference customers rely on the inexpensive and seamless integration of FortiGuard Threat Intelligence across the Fortinet products but do not actively search out and read other written threat intelligence reports on a regular basis. FortiGuard Threat Intelligence is best for customers who already have existing Fortinet technologies.

- **The Trellix portfolio primarily delivers cyber threat intelligence use cases.** Trellix Threat Intelligence is a collection of products and services focused primarily on cyber threat intelligence use cases rather than brand protection. Trellix Insights is delivered as a standalone service and integrated into the Trellix portfolio. Trellix Global Threat Intelligence (GTI) and Threat Intelligence Exchange (TIE) are tightly bundled into its existing products, so only existing Trellix customers can leverage

them effectively. Trellix Advanced Threat Landscape (ATLAS) is available as a standalone product but geared to customers with mature threat intelligence programs. Trellix's vision lacks differentiation, but its roadmap includes a future release of Trellix Insights as a microservice giving customers more flexibility in leveraging threat intelligence.

Trellix collects telemetry from its broad portfolio of proprietary technologies, giving it unique IOCs. Trellix Private GTI is a unique offering, which is designed to bring its Global Threat Intelligence capabilities to highly secure environments that are air-gapped from the internet. Trellix does not directly address the more common digital risk protection use cases and requires going through its RFI process as a special request for takedowns. Reference customers appreciate the richness of the IOCs and seamless integration of threat intelligence with the Trellix technology stack but rely on other vendors to provide other services like brand and domain protection. Trellix Threat Intelligence is suited for customers who need robust IOCs integrated across a broad technology stack to address cyber threat intelligence use cases.

- **CybelAngel is a small company that delivers high efficacy results.** The CybelAngel EASM suite is composed of five distinct modules: data breach prevention, dark web monitoring, account takeovers, domain protection, and asset discovery and monitoring. It's headquartered in Paris, France with two-thirds of its customers based in EMEA. CybelAngel's vision is inspiring, true to its value proposition, and consistent with its core competency. The CybelAngel pricing model requires the customer to articulate their expected volume of detections based on their anticipated exposure to external threats, which is difficult to estimate. CybelAngel's partner ecosystem is not as broad as other threat intelligence service providers. CybelAngel is working to enhance its EASM offering with a live status feature that will provide real-time verification if a particular asset of interest is still online or vulnerable based on the prior alert status.

  CybelAngel relies mostly on a passive approach to sourcing and then subjects the raw data to a rigorous keyword-matching and AI/ML curation process before a human analyst conducts the final analysis, which significantly reduces false positives. The CybelAngel customer portal more closely resembles a ticketing system. CybelAngel has 25 dedicated threat analysts. Customers view curated alerts and associated enrichment data for a monitored asset but cannot perform full-blown, ad hoc searches or general threat research. Reference customers laud the lack of false positives and overall efficacy of the alerts. Some references

observed that the alerting frequency felt cyclical as opposed to real time. CybelAngel is suited for customers who don't want a threat intelligence platform but rather a service to do heavy analysis work so that they only receive actionable, external alerts regarding their targeted assets.

- **Rapid7 addresses multiple use cases, but portfolio integration needs strengthening.** Rapid7 Threat Command is the integration of Rapid7's prior IntSights acquisition and further development of threat intelligence capabilities into its Insight Platform. Customers can purchase Rapid7 Threat Command as a standalone solution. Rapid7 does not have as broad of a partner ecosystem as other providers. It does maintain several well-known and widely popular open source technologies such as Metasploit and Velociraptor. Rapid7 is embedding threat intelligence into its broader portfolio to help customers with their digital transformation and shift to the cloud. Despite Rapid7's new AI/ML R&D team, its vision is focused on enhancing standard functionality like threat identification and remediation in its security operations platform.

  Threat Command includes a TIP so customers can integrate other public or private IOC feeds, including something as routine as ingesting an ISAC email alert. The Rapid7 portal lacks some of the capabilities of other competitors who have tightly integrated threat intelligence with the rest of their technology stack. Reference customers lament that the Threat Command interface is outdated, and little has changed in the UI post-acquisition. References also say that the integration of threat intelligence across the Insight Platform is not as seamless as it should be and felt the information was a commodity. Smaller customers looking for a solid threat intelligence solution and existing Rapid7 customers who need actionable external threat intelligence at a reasonable price should consider Rapid7.

- **IBM's X-Force Threat Intelligence specializes in relevant indicators of compromise.** IBM X-Force Threat Intelligence is one part of the overall X-Force portfolio. IBM strives for a unified and open approach to intelligence-driven security, and this vision is reflected in its extensive partner ecosystem. IBM's worldwide influence is evident in its partnerships with over 40 different countries and a dozen global CERTs. IBM structures its threat intelligence offerings differently and charges primarily on a consumption model, which makes it harder and potentially more expensive to address specific needs. IBM continues to add more source content and plans to enhance its platform and build new services.

  IBM X-Force Threat Intelligence is strong across standard cyber threat intelligence use cases like threat monitoring but weaker in digital risk protection use cases like

brand protection. It has a robust malware analysis team and threat intelligence specialists aligned to the operational technology vertical. Customers have multiple options to obtain IOCs from IBM. The portal includes basic TIP features, but the overall interface experience is underwhelming, harder to navigate, and less customizable than competitors. Customers rely on APIs to ingest IOCs and remark that they are more accurate and relevant than other sources they have tried. IBM is a solid choice for any customer seeking to ingest robust machine-readable threat intelligence. IBM declined to participate in the full Forrester Wave evaluation process.

Evaluation Overview

We grouped our evaluation criteria into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include gathering intelligence requirements, intelligence collection sources, intelligence processing and analysis, dissemination, metrics and feedback, cyber threat intelligence, digital risk protection, special services, RFIs for ad hoc needs, portal interface experience, frameworks and model supported, analyst tradecraft expertise, privacy and data security controls, and product security controls.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated vision, innovation, roadmap, partner ecosystem, pricing flexibility and transparency, and community.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's revenue and number of customers.

Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

- **Product revenue.** Each participant must have at least $20 million in annual threat intelligence services revenue.
- **Core functionality.** Each participant solves multiple threat intelligence use cases and addresses a comprehensive spectrum of threat intelligence use cases such as brand protection, vulnerability management enhancement, compromised asset detection, and threat-hunting enablement to name a few.
- **Diverse skill set.** Each participant has broad threat intelligence experience, including dedicated threat intelligence analysts with multiple skills to gather threat information from a variety of sources and deliver machine- and human-readable

threat intelligence.

- **Forrester 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.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by May 18, 2023, and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with our vendor review policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with our vendor participation policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the integrity policy posted on our website.

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

FOLLOW FORRESTER

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

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