LANDSCAPE REPORT

The External Threat Intelligence Service Providers Landscape, Q1 2023

Forrester's Overview Of 28 Providers

March 8, 2023

By Brian Wrozek with Merritt Maxim, Caroline Provost, Ian McPherson

FORRESTER®

Summary

You can use threat intelligence to reduce physical and cyber risks, improve you and your team's decision-making capabilities, and complement internal security threat intelligence. But to realize these benefits, you'll first have to select from a diverse set of providers that vary by size, type of offering, geography, and use case differentiation. Security and risk (S&R) professionals should use this report to understand the value they can expect from external threat intelligence service providers (ETISP), learn how providers differ, and select one based on size and market focus.

Market Definition

The need for threat intelligence has never been greater. IT environments have become increasingly complex. The number of vulnerabilities continues to grow, and the expanding sophistication of threat actors has heightened the need to improve decision-making, allocate resources more efficiently, and enhance cyber resiliency. S&R professionals are looking for external threat intelligence providers (ETISPs) that have the right visibility into the most relevant threats to their organization and industry. Forrester defines ETISPs as:

> Services that provide information and analysis about potential or active threats against a specific organization, industry, or geography. They collect information from multiple sources and add valuable enrichment to enable organizations to make better decisions to reduce physical and cyber-attacks and mitigate risk.

ETISPs improve decision-making capabilities by prioritizing vulnerabilities for remediation, identifying and mitigating threats to your organization's brand, and tracking and analyzing cyberthreats.

Business Value

Information is valuable when it improves the outcomes and reduces the uncertainty of our actions. S&R pros implement ETISPs' offerings to:

- **Reduce physical and cyber risks.** ETISPs address a broad array of physical and cyber risks. They increase their clients' knowledge of the general threat landscape and those threats targeting their specific regions, industries, and organizations. S&R professionals use this information to answer corporate-level questions about their organizations' cyber risk posture. This information is crucial in developing and executing an effective cyber security strategy.
- **Improve the decision-making capabilities of security professionals.** Today, security resources are limited and overburdened. Complete, accurate, relevant, and timely threat intelligence can be used tactically to assist in triaging new alerts, prioritizing vulnerabilities, and enabling more efficient incident response. S&R pros can use it operationally to facilitate threat modeling and attack analysis for effective allocation of controls. They can also use it strategically to align business goals and security priorities to assessments of likely threats.

- **Complement internal security threat intelligence.** Threat intelligence that you obtain from internal resources, such as system logs and security alerts, should be the foundation of your threat intelligence program. Internal threat intelligence is available and reliable because it reflects what is happening to your organization — but that is only half the picture. You should enrich this internal information with external information for a more accurate picture of the threats your organization faces. External threat intelligence provides early warning of pending threats, adds context to existing threats, and educates you about the overall threat landscape.

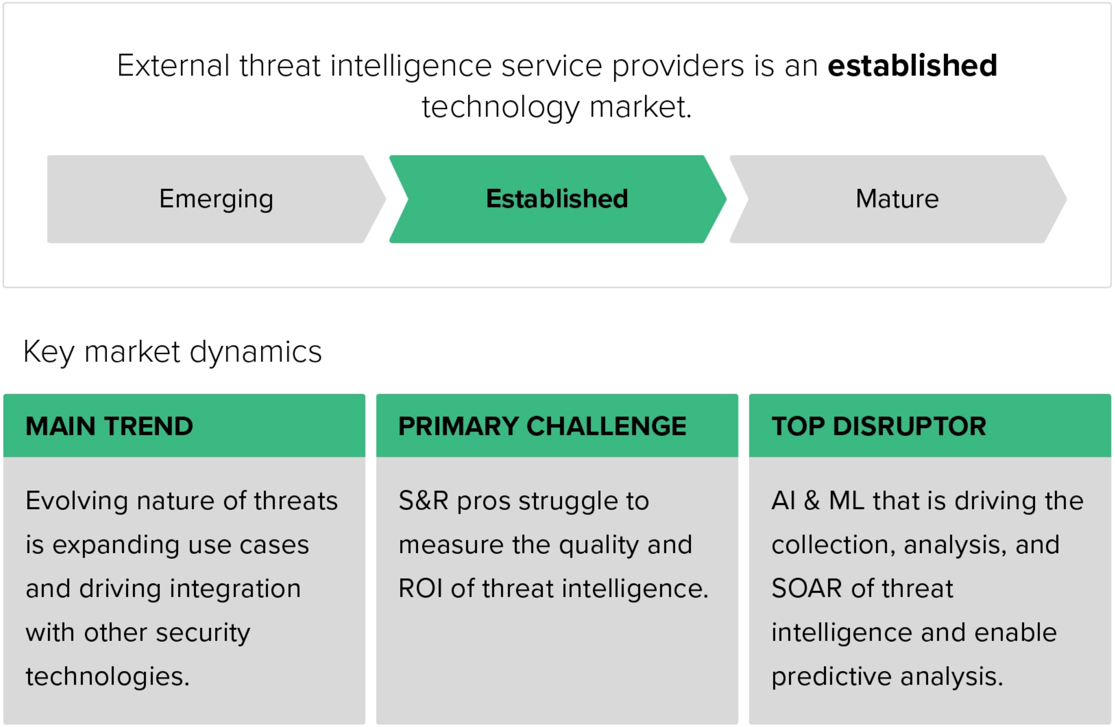
Market Maturity

Gathering and using threat intelligence to aid in decision-making is not new, but the collection, analysis, and presentation of threat intelligence continue to improve (see Figure 1). ETISPs have evolved into an established market that:

- **Augments IOCs data with TTP information.** Indicators of compromise (IOCs) are an important source of raw data, but increased complexity of attacks and the sheer volume of possible IOCs leads to false positives and alert fatigue. ETISPs deliver more than IOC feeds by providing analysis and detailed intelligence reports with tactics, techniques, and procedures (TTP) information. These reports provide insight into the methods and tools threat actors use to aid security teams in detecting, mitigating, and responding to attacks. S&R pros can use TTP information to proactively model attacks, providing insight into the effectiveness of your security controls.
- **Provides additional context to existing information.** More IOCs do not automatically result in better threat intelligence, but adding relevant contextual information provides clarity and insight into security events. Knowing who is conducting an attack may help you understand their motivations and goals. Early warning that a threat actor is actively exploiting a vulnerability may encourage you to escalate the deployment of that patch over others with a similar CVE rating. ETISPs enhance raw data with contextual information and analysis so security teams can make better decisions on where to focus their resources.
- **Delivers targeted and specific information in addition to general trends.** Not all threat intelligence is equal. ETISPs use added contextual information to target threat intelligence for a particular global region or industry vertical. They can offer more granularity by monitoring corporate assets such as domain names and providing information related to a specific target like an upcoming sporting event. Targeted threat intelligence allows you to focus on the most relevant and likely threats.

Figure 1

External Threat Intelligence Service Providers: Market Maturity And Key Dynamics



External threat intelligence service providers is an **established** technology market.

Emerging → **Established** → Mature

Key market dynamics

MAIN TREND	PRIMARY CHALLENGE	TOP DISRUPTOR
Evolving nature of threats is expanding use cases and driving integration with other security technologies.	S&R pros struggle to measure the quality and ROI of threat intelligence.	AI & ML that is driving the collection, analysis, and SOAR of threat intelligence and enable predictive analysis.

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

Market Dynamics

S&R pros will encounter a plethora of ETISPs and should pay attention to the following market dynamics.

- **Main trend.** The evolving nature of threats is expanding use cases and driving integration with other security technologies. Reports about another cyberattack or newly discovered vulnerabilities have become daily occurrences. Information without the ability to turn it into meaningful action is useless. To keep up with the barrage of threat information, S&R professionals are integrating threat intelligence into all facets of their security programs, including security operations, vulnerability management, brand protection, and incident response.
- **Primary challenge.** S&R professionals struggle to measure the quality and ROI of threat intelligence. ROI for much of cybersecurity has always been a challenge. How much would you pay to learn that a certain IP address is part of a botnet? If

you learn that IP address is part of a ransomware campaign targeting your industry, how much does this additional context increase the value of the information? We intuitively know the information is useful, but it is difficult to quantify.

- **Top disruptor.** AI and machine learning (ML) are driving the collection; analysis; and security orchestration, automation, and response of threat intelligence and enable predictive analysis. More of the right information provides greater context about a threat, but the sheer volume of potential IP addresses, domain names, malware versions, vulnerabilities, and threat actors is too much to handle manually. New AI and ML algorithms will facilitate the collection, analysis, and automation of threat intelligence. The goal is to shift the use of threat intelligence from a reactive process to a predictive analysis approach to address threats before they materialize.

Notable Providers

S&R professionals can start shortlisting specific providers based on their market, with large providers having over $55 million, medium providers having $20 million to $55 million, and small providers having $5 million to $20 million in annual product revenue. They should also take into consideration geographic focus, industry focus, and type of offering. The list doesn't include providers with under $5 million in product revenue (see Figure 2).

Figure 2

The External Threat Intelligence Service Providers Landscape, Q1 2023

Provider	Geographic focus	Industry focus	Type of offering
LARGE >$55M			
Accenture	NA; EMEA	Financial services Oil and gas Telecommunications	General-purpose platform that can be used to build any domain application
CrowdStrike	NA; EMEA	Financial services Government High-tech products	General-purpose platform that can be used to build any domain application
Flashpoint	NA	Financial services Government High-tech products	Domain-specific solution/application
Google[1]	NA; EMEA	Financial services Government Healthcare	General-purpose platform that can be used to build any domain application
IBM[1]	NA; EMEA; APAC	Financial services High-tech products	Domain-specific solution/application
Microsoft[1]	NA	Financial services Media Retail	General-purpose platform that can be used to build any domain application
Recorded Future[1]	NA; EMEA	Financial services Government High-tech products	Domain-specific solution/application
Tencent[1]	APAC	Financial services Government High-tech products	General-purpose platform that can be used to build any domain application
ZeroFox	NA; EMEA	Financial services Government Retail	Domain-specific solution/application

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

Provider	Geographic focus	Industry focus	Type of offering
	MEDIUM >$20M-$55M		
Booz Allen Hamilton[1]	NA	Financial services High-tech products Pharmaceuticals and medical equipment	General-purpose platform that can be used to build any domain application
Claroty[1]	NA	Consumer products Healthcare Oil and gas	Domain-specific solution/application
CybelAngel[1]	EMEA	Industrial products Pharmaceuticals and medical equipment Telecommunications	Domain-specific solution/application
Dragos	NA	Oil and gas Primary production Utilities	Domain-specific solution/application
Everbridge	NA	Financial services High-tech products Pharmaceuticals and medical equipment	General-purpose platform that can be used to build any domain application
Fortinet	NA; EMEA; APAC	Financial services Government Oil and gas	General-purpose platform that can be used to build any domain application
QI-ANXIN	APAC	Financial services Government Oil and gas	Domain-specific solution/application
Rapid7[1]	NA	Financial services Healthcare Retail	Domain-specific solution/application

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

Provider	Geographic focus	Industry focus	Type of offering
	MEDIUM >$20M-$55M		
ReliaQuest	NA; EMEA	Financial services High-tech products Retail	General-purpose platform that can be used to build any domain application
ThreatBook	APAC	Financial services Government Oil and gas	Library of APIs, API services
ThreatQuotient[1]	NA; EMEA	Financial services Government High-tech products	Domain-specific solution/application
Trellix	NA; EMEA	Financial services Government Healthcare	Domain-specific solution/application
Trend Micro	NA; EMEA; APAC	Financial services Government Healthcare	Domain-specific solution/application

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

Provider	Geographic focus	Industry focus	Type of offering
SMALL $5M-$20M			
360 Digital Security Group	APAC	Financial services Government Telecommunications	General-purpose platform that can be used to build any domain application
Cybersixgill	NA; EMEA; APAC	Financial services Government High-tech products	General-purpose platform that can be used to build any domain application
GreyNoise Intelligence[1]	NA	Financial services Government Healthcare	Domain-specific solution/application
LookingGlass Cyber	NA	Financial services Government Transportation	Domain-specific solution/application
NSFOCUS	APAC	Financial services Government Telecommunications	General-purpose platform that can be used to build any domain application
Yoroi[1]	EMEA	Financial services Industrial products Oil and gas	Domain-specific solution/application

Note: Geographic focus indicates regions where the provider's product revenue in this category is greater than or equal to 15% of its total product revenue.
1. The provider did not provide complete information for this table; this table includes Forrester's estimates.

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

Top Use Cases

Threat intelligence supports a variety of use cases. We have identified the following core use cases for this market: compromised asset detection, vulnerability management enhancement, general threat landscape monitoring, targeted threat monitoring, and enabling threat hunting and modeling. These are the use cases most frequently sought after by buyers and addressed by ETISP solutions. We have identified the following use cases as extended: physical asset protection, brand and domain reputation or impersonation protection, attack surface discovery and management, fraud and counterfeit detection, and third-party risk monitoring. These are use cases for which some buyers look to address in addition to the core use cases but are less commonly addressed by ETISP solutions (see Figure 3 and see Figure 4).

Figure 3

External Threat Intelligence Service Providers: Core Use Cases

Use case	Objective	Top differentiators
Compromised asset detection	Find and share detailed evidence of compromised assets to facilitate incident response efforts.	• Find compromised company assets quickly
Vulnerability management enhancement	Provide additional context and analysis regarding vulnerabilities to enable customers to prioritize remediation.	• Add context and analysis • Risk scoring • Recommendations
General threat landscape monitoring	Search public and private sources and report about existing and potential threats to enhance decision making.	• Breadth of sources and coverage • Publishing frequency
Targeted threat monitoring	Focus on threats by assets, regions, industry verticals or other criteria for what customers cares about the most.	• Focus on specific criteria • Uniqueness and accuracy of data
Enable threat hunting and modeling	Provide detailed indicators of compromise (IOCs) and tactics, techniques, procedures (TTPs) on threats and threat actors.	• Consumable IOCs • TTPs on actors and attacks • Map to Mitre

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

Figure 4

External Threat Intelligence Service Providers: Extended Use Cases

Use case	Objective	Top differentiators
Physical asset protection	Find and report about existing and potential malicious and natural threats specifically targeting and impacting physical assets.	• Address physical threats • Cover human and natural threats
Brand and domain reputation or impersonation protection	Search open and restricted sources about indications of threats targeting or compromising a customer brand.	• Focus customer brand • Assist in domain takedowns
Attack surface discovery and management	Discover and enumerate both known and unknown internet facing assets so customers can account for them in their operational security efforts.	• Identify and profile company assets that are internet facing
Fraud and counterfeit detection	Provide information about threats or evidence of potentially fraudulent activities and transactions.	• Discover credit card numbers • Identify fraud abuse
Third-party risk monitoring	Identify, assess, and monitor on risks to the company stemming from their third-party relationships to ensure continuity of their supply chain.	• Risk scoring of third-party partners and suppliers

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

Functionality By Use Case

Each organization’s need for threat intelligence is different based on their unique risk profile and capacity to act upon the information. Buyers expect ETISPs to provide a variety of functionalities to support each use case. Select the use cases that are most relevant to your business requirements, then use the following tables as a guide to choose the functionalities that align with your company culture, risk appetite, capabilities, and overall needs of the business (see Figure 5 and see Figure 6).

Figure 5

External Threat Intelligence Service Providers: Functionality By Core Use Case

Functionality	Compromised asset detection	Vulnerability management enhancement	General threat landscape monitoring	Targeted threat monitoring	Enable threat hunting and modeling
Collect general information from open sources	●	●	●	●	●
Collect proprietary information from your own products	○	○	○	○	○
Collect specific information from closed sources	●	●	○	●	●
Perform data deduplication, clean-up, formatting, enrichment	○	●	○	●	●
Perform intelligence analysis and provide additional context	●	●	●	●	●
Perform malware (sandboxing) analysis	◌	○	○	○	○
Perform threat actor profiling and analysis	◌	○	○	●	●
Perform vulnerability and risk scoring	●	○	◌	●	○
Deliver automated, raw indicators of compromise (IOC) feeds	○	○	●	●	●

● **Primary functionality** required for a given use case

○ **Secondary functionality** required for a given use case

◌ **Little to no functionality** required for a given use case

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

Functionality	Compromised asset detection	Vulnerability management enhancement	General threat landscape monitoring	Targeted threat monitoring	Enable threat hunting and modeling
Portal or platform integration with searching and reporting	○	●	●	●	●
Deliver finished tactics, techniques, procedures (TTP) reports	○	○	●	●	●
Deliver finished threat trending reports	◍	○	○	●	●
Provide consulting services for program development	◍	◍	◍	○	○
API integrations to facilitate orchestration and automation	●	●	●	●	●
Provide domain takedown and malicious asset tagging	◍	◍	◍	◍	◍

● **Primary functionality** required for a given use case

○ **Secondary functionality** required for a given use case

◍ **Little to no functionality** required for a given use case

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

Figure 6

External Threat Intelligence Service Providers: Functionality By Extended Use Case

Functionality	Physical asset protection	Brand and domain reputation or impersonation protection	Attack surface discovery and management	Fraud and counterfeit detection	Third-party risk monitoring
Collect general information from open sources	●	●	●	●	●
Collect proprietary information from your own products	◌	◌	◌	◌	◌
Collect specific information from closed sources	●	●	◌	●	○
Perform data deduplication, clean-up, formatting, enrichment	○	●	○	○	○
Perform intelligence analysis and provide additional context	●	●	○	●	○
Perform malware (sandboxing) analysis	◌	◌	◌	◌	◌
Perform threat actor profiling and analysis	○	○	◌	○	○
Perform vulnerability and risk scoring	○	○	●	○	●
Deliver automated, raw indicators of compromise (IOC) feeds	◌	●	○	◌	○

● **Primary functionality** required for a given use case

○ **Secondary functionality** required for a given use case

◌ **Little to no functionality** required for a given use case

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

Functionality	Physical asset protection	Brand and domain reputation or impersonation protection	Attack surface discovery and management	Fraud and counterfeit detection	Third-party risk monitoring
Portal or platform integration with searching and reporting	○	●	●	●	○
Deliver finished tactics, techniques, procedures (TTP) reports	○	○	◍	●	◍
Deliver finished threat trending reports	○	○	◍	○	◍
Provide consulting services for program development	○	○	◍	○	◍
API integrations to facilitate orchestration and automation	○	○	●	○	◍
Provide domain takedown and malicious asset tagging	◍	●	◍	○	◍

● **Primary functionality**
required for a given use case

○ **Secondary functionality**
required for a given use case

◍ **Little to no functionality**
required for a given use case

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

Extended Use Cases By Vendor

We asked each provider included in this report to select its top use cases for which customers select that provider's service. From this, we determined the extended use cases that highlight differentiation among providers. The following table shows how each provider's responses map to those. This table represents the provider-reported use cases for which clients select them, not available functionality (see Figure 7).

Figure 7

External Threat Intelligence Service Providers: Extended Use Case By Vendor

Providers	Physical asset protection	Brand and domain reputation or impersonation protection	Attack surface discovery and management	Fraud and counterfeit detection	Third party risk monitoring
Accenture					●
Claroty			●		
CybelAngel	●	●	●	●	●
Cybersixgill		●			
Everbridge	●	●			●
Flashpoint	●	●		●	
Fortinet		●	●		
Google			●		
IBM			●		
LookingGlass Cyber			●		●
NSFOCUS			●		
QI-ANXIN			●		●
Rapid7		●	●		

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

Providers	Physical asset protection	Brand and domain reputation or impersonation protection	Attack surface discovery and management	Fraud and counterfeit detection	Third party risk monitoring
ReliaQuest		●			●
Tencent Security			●	●	
Trend Micro			●		
ZeroFox	●	●		●	

Note: The following vendors selected most or all use cases in our questionnaire: 360 Digital Security Group, Booz Allen Hamilton, Crowdstrike, Recorded Future

Note: The following vendors selected core use cases only in our questionnaire: Dragos, GreyNoise Intelligence, Microsoft, ThreatBook, ThreatQuotient, Trellix, Yoroi

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

Supplemental Material

Methodology

To complete our review, Forrester requested information from providers. If providers didn't share this information with us, we made estimates based on available secondary information. We've marked all estimates with a note. Forrester fact-checked this report with providers before publishing.

Companies We Researched For This Report

Forrester researched the following companies for this report.

360 Digital Security Group

Accenture

Booz Allen Hamilton

Claroty

CrowdStrike

CybelAngel

Cybersixgill

Dragos

Everbridge

Flashpoint

Fortinet

Google

GreyNoise Intelligence

IBM

LookingGlass Cyber

Microsoft

NSFOCUS

QI-ANXIN

Rapid7

Recorded Future

ReliaQuest

Tencent

ThreatBook

ThreatQuotient

Trellix

Trend Micro

Yoroi

ZeroFox

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