EMA Radar™ for Digital Threat Intelligence Management: Q4 2017

An Enterprise Management Associates Radar™ Report

Written by David Monahan

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Threat intelligence has been around in one form or another for many years. Only in the last few years did the information really become digestible for any but the largest organizations. Its most recent form evolved into platforms that collect and analyze information through various automated and manual means. The information is focused on delivering indicators of a valid threat against the company. Rather than terabytes of superfluous data, organizations that invest in the toolset can specify what types of information they are most interested in and begin collection.

Some vendors focus on specific types of infringement, like brand infringement or domain abuse. Others focus on data sources like social media or the dark web. The third group has a broader coverage, looking at many different sources, analyzing and correlating them, and delivering directed information on the infringement. As expected, greater or premium coverage often demands a premium price, so those looking into the solutions should evaluate the scope they really need instead of just what they want.

EMA is seeing a surge of M&A activity, as well as significant infusions of capital in the established companies. Only some of the companies in the space are profitable at this time, though the analysis points to a number of them crossing into profitability later in 2018.

Organizations in sectors that are at high risk for having intellectual property of any sort compromised and do not have something already in place should investigate this technology stack. Remember, this is not going to do anything to protect against internal theft, incursion, or breach, but selecting the right platform for the organization's needs should provide earlier detection of the theft or misuse of IP, thus significantly reducing the impacts.

Definition

Digital Threat Information Management (DTIM) is centered on threat information platforms and their ability to aid organizations with threat identification and risk management. In general, the platforms can gather and assimilate threat intelligence from a variety of sources, including the common Internet, the deep and dark webs, mobile app markets, email, and social media repositories. The majority of this information cannot be gathered by simple web searches and requires more specialized expertise and tooling to locate and access it. There are a range of capabilities that will be discussed in a later section, but within these platforms, there are generally two focuses.

The first group consists of the data aggregators. This group gathers, normalizes, and correlates data from existing lists and feeds from a multitude of open and free sources and closed subscription lists. They even collect data from other DTIM vendors who create their own proprietary information.

The second group has the same general attributes, but they also invested in the means to collect and analyze their own proprietary data by various automated and human-driven methods prior to adding it to the data repository passed on to their clients.

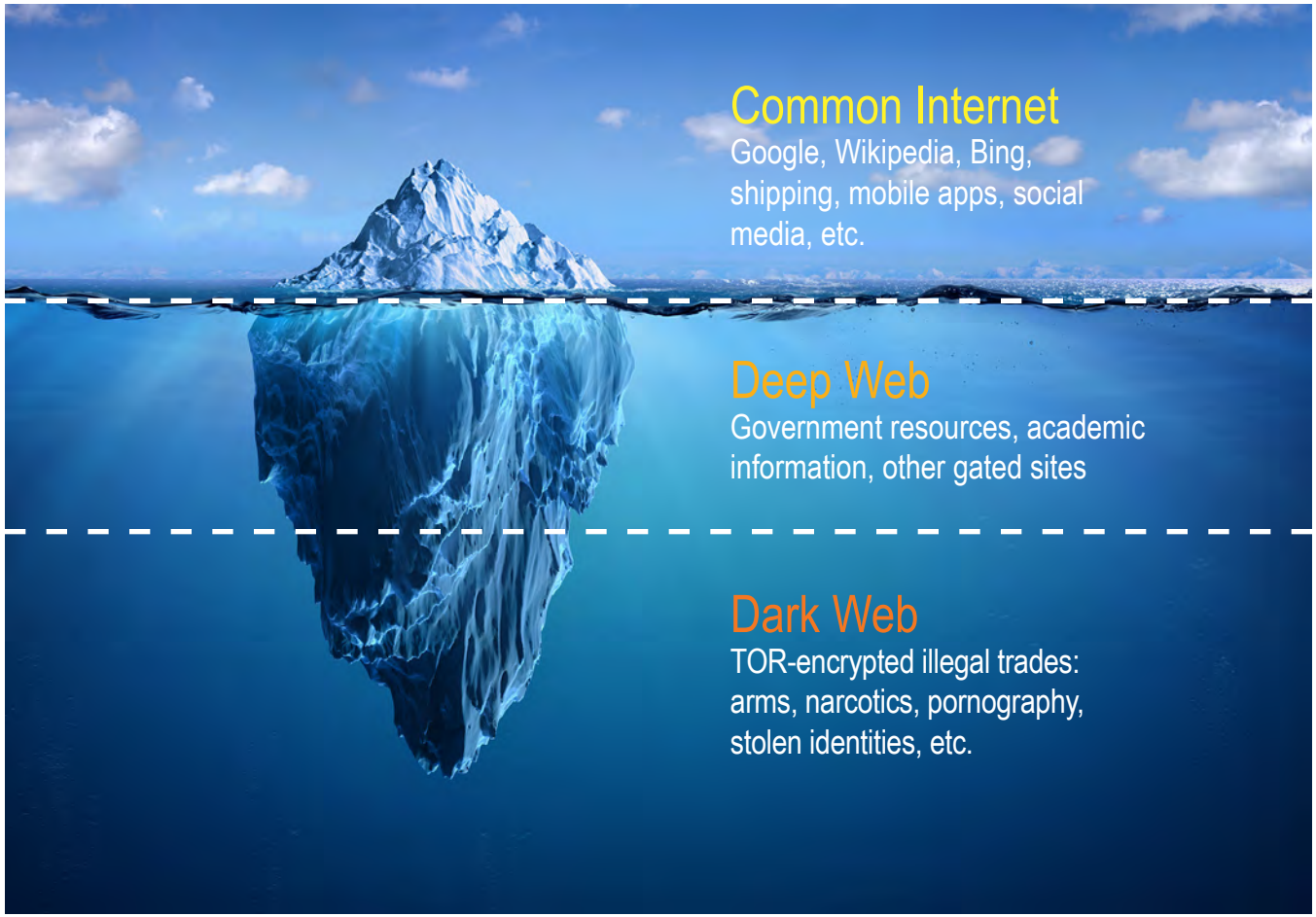


Figure 1

"The Chasm" and Technology Adoption

The market for threat intelligence has been around for a number of years, starting with threat feeds. Threat platforms emerged as a centralized means of not only aggregating huge amounts of data, but also processing it with better analysis, thus creating the Digital Threat Intelligence Management platforms.

Figure 2 depicts the adoption lifecycle of technologies in a market. In another research project,[1] EMA found that in organizations of greater than 1000 personnel, 40 percent of the surveyed organizations had some form of either purchased or home-grown DTIM solution installed. This adoption rate placed DTIM past the Emerging category and "the Chasm." To survive as more than a niche, technologies must reach a market adoption above 25-30 percent to move from Emerging to Growth. If they are unable to gain that market popularity, technologies will linger in Emerging and remain niche technologies, or they will die out altogether. When entering "the Chasm," lackluster competitors will disappear, early mergers will be required for smaller players to continue fighting for market share, and market leaders will begin to appear in the space.

The critical indicators for growth, other than price, are market awareness of the technology and satisfaction of existing customers, which are in turn affected by multiple factors.

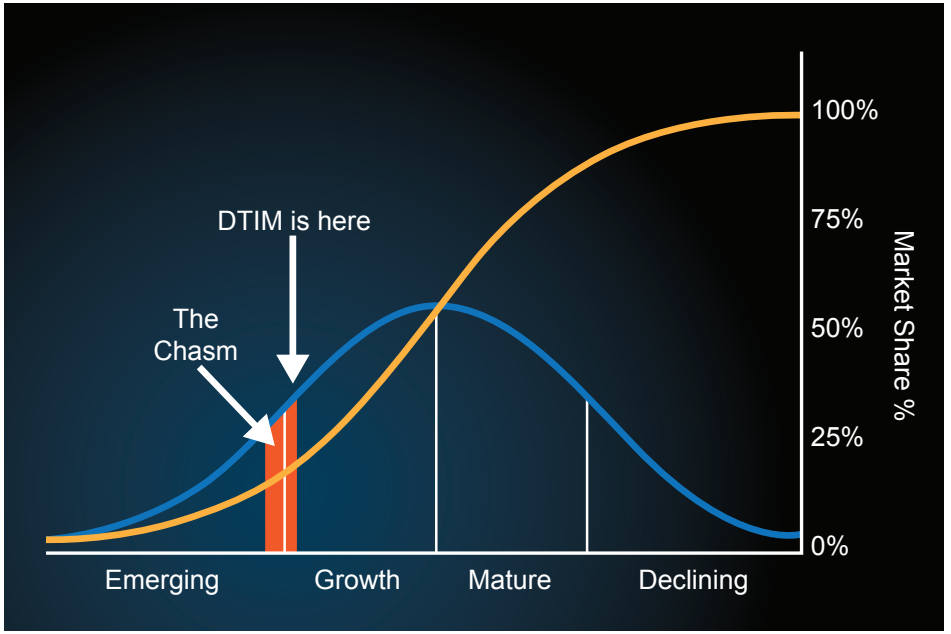


Figure 2

DTIM as a Market

The DTIM market seems to have passed the Emerging phase and overcome "the Chasm." Market awareness is good and adoption is increasing. Some approaches and technologies have fallen by the wayside in figuring out how to locate and deliver the intelligence in a consumable and useful manner. The market spend on DTIM is estimated to be between $550M USD and $600M USD for 2018, with a weighted growth rate of 35 percent from 2016 to 2017 and an estimated growth rate of 40 percent in 2018. Receiving increasing growth expectations is another positive sign of the market and the estimated placement on the maturity curve. If the vendor estimates hold, 2018 should see a market spend between $770M USD and $840M USD. Given the market saturation and the continued expansion of managed DTIM as a service, it is easily foreseeable that the market will exceed $1B USD by 2020.

[1] EMA Research Report, "Data-Driven Security Unleashed: A Look Into the Tools That Drive Security"

Feature Eligibility

In order for a product set to be credited with a feature or capability in EMA's evaluation, it was required to meet three strict criteria:

1. The features needed to be generally available with the solution set at the time of the evaluation. Any features that were in beta testing or were scheduled to be included in later releases of the management suite were not eligible for consideration.
2. All features needed to be self-contained within the included package sets. Any features that were not natively included in the evaluated package sets, but available separately from the same vendor or third-party vendors for an additional cost, did not qualify.
3. All reported features needed to be clearly documented in publicly-available resources (such as user manuals or technical papers) for verification.

Methodology

In the entirety of the evaluation, there were over 100 different KPIs that were collected from a combination of publicly-available information, a vendor questionnaire, and customer interviews. The KPIs were parsed into five primary categories: Deployment and Administration, Cost Advantage, Architecture and Integration, Functionality, and Vendor Strength. Each of these categories had multiple subcategories. The ratings for these categories are presented in the vendor profiles as a spider graph, with the total score for the vendor along with the mean value across all evaluated vendors. The same is also displayed for each of the five primary categories. The profiles also reveal some of the secondary summary values and their ratings based on a five-level scale. The values are converted to one of the following, ranked from highest to lowest: Outstanding, Strong, Solid, Limited, and None. There are two exceptions that did not fit that model. For reliance on professional services, the values were listed from Very Low, Low, Moderate, High, and Very High. For monetary-related items, a scale from one to five dollar symbols was displayed to represent cost or value. In both cases, one symbol provided the least strength or value and five dollar signs represented the greatest.

Key Area for Consideration: Data Collection

As organizations look for a threat intelligence vendor to aid them, it is important that they have a base understanding of the sources the prospective vendor uses. They must determine whether the proprietary data and human researchers add enough value, based on the organizational requirements and goals, for the premium prices they command. In the analysis, EMA deemed much of the proprietary data as having significant additional value, so for organizations with deeper pockets or broader protection needs, it can be worth the investment. On the converse side, some of the platforms have a very high reliance on their proprietary data. No one vendor has the scale to catch everything across all threat surfaces, so overreliance on proprietary data may leave blind spots in the overall threat intelligence net.

Some of the vendors have a tighter focus and more specialized tooling to address certain aspects of threat intelligence, so their information reach may be narrower but substantially deeper. This is another part of the decision-making equation. If the investigating organization aims to focus on protecting a certain aspect of their business (like unauthorized brand usage on the Internet or in email marketing, unauthorized mobile applications in marketplaces, domain infringement, etc.), they can choose a less expensive vendor that focuses on that space rather than buying a solution that covers the broader context.

Deployment and Administration

This section attempts to quantify the ease or difficulty in getting the solution installed and operational. It classifies its KPIs into three areas: Deployment Flexibility, Ease of Administration, and Reliance on Professional Services.

Key Area for Consideration: Deployment Flexibility

Deployment Flexibility evaluates how purchasers can receive the platform. Various factors affect whether the platform is delivered as a managed service, single or multi-tenant cloud SaaS service, software installation, appliance, or image.

Some organizations want everything in the cloud. Others want nothing in the cloud, and there are those in the middle that determine where a tool will reside based on long- or short-term need, data sensitivity, compliance requirements, extent of the need, resilience requirements, lack of available skillset, capital expense vs. operational expense, or other business requirements. Some of the platforms are only available as cloud services, while others are only available with on-premises delivery. A few have both options. Included in that thought process is the option of having a managed service. Any of these platforms can be a primary or cumulative weighted choice for deciding for or against a particular platform.

Key Area for Consideration: Ease of Administration

Ease of Administration evaluates the required care and resources needed to manage and maintain the system during operations.

Some platforms used on-premises require dedicated resources to manage and maintain, while the same platform in the cloud or a managed service may be able to use a shared resource or no additional resources to maintain operations. With skilled people in high demand, the cost of administration is increasing and keeping existing personnel is tricky. In this case, even if prospective buyers have a data center where they could install the platform, they need to consider their ability to maintain and support that platform in that data center. Even if they can, they should evaluate the opportunity cost of that use of human capital to do it. This needs to be maintained in balance with sensitive data management policies.

Key Area for Consideration: Reliance on Professional Services

Whether for installation, upgrades, lifecycle management, policy creation, module reconfiguration, or training, the need for professional services is a significant budgetary consideration. All the vendors offer the option of professional services, but some require them for one to all phases of delivery. This must be managed as a recurring expenditure if a platform is chosen that needs professional services for updates.

Cost Advantage

This is a crucial area for every potential buyer. Cost Advantage was evaluated by both questionnaire and from customer interviews. The customers were most influential in this area, since they can provide information on what they received the most value from in the platform and the level of value they received from the solution compared to what they paid, and how productive they were before obtaining the solution.

Key Area for Consideration: Functionality Increasing Accuracy and Productivity

Though the initial goal of purchase for the platforms is often to get better insights on the threats that may be coming, a core benefit is that they provide enough contextual intersection of information to analyze and correlate the external threat events well enough to deliver high confidence and concise, actionable incidents. The system must wade through huge amounts of data to find the alerts in the Internet that have a high probability of either indicating an asset will be attacked or that a successful attack took place with evidence to back it up. If it just delivers lists of possible threats, it is not really helping, and is probably making the situation worse.

Every DTIM customer EMA spoke with had totally changed their organization's accuracy and productivity model by investing in the solution. Prior to their purchase, their teams spent 80-90 percent of their time gathering data and researching in order to come to a decision on whether their company was at risk from the indicators they uncovered. Ten percent actually worked on the incident. Many indicators were dropped on the floor, never to be investigated. Some of those ended up being real problems. After purchase, all companies interviewed said they were able to reverse that time usage, spending 80-90 percent of their time actually investigating the indicators. By receiving better intelligence through the platform, the volume of individual indicators went down and the ability to investigate more of them rose.

People can agree on certain aspects of a GUI being very good or very poor, or certain aspects of a workflow being very useful or not. However, because people process information differently and even think differently, and because workflows vary considerably in different organizations, it is difficult to get an agreement that one GUI is the best. That said, look for tools with customizable workflows or playbooks that can be adapted for the target environment and role-based dashboards that can be tailored to a specific function or group and may allow individual users to further customize them to be more productive. Platforms with these features often charge a premium, but if it is not too much of a premium for a budget to handle, the future payoffs for productivity are often worth the money upfront.

Architecture and Integration

Platform architecture and integration are going to be crucial for scalability, breadth of data collection, data analysis, workflow collaboration, and incident response (among other things). A lack of forethought on how the platform assimilates and processes data can have a significant effect on future capabilities and impacts on customers. The two most common issues are having to adapt the business to meet the needs of the tool, rather than the reverse, and an inability to scale sufficiently as the business grows.

Failing to create the proper integrations also means tools already in use cannot interface, lowering their value and the platform's value, and creating the inability to automate defensive responses.

Key Areas for Consideration: Data Sources and Integration Partners

Each platform was evaluated on the types of data it consumes. The four areas were open sources, government sources, private subscriptions, and proprietary collection. Each of these sources has value and should be part of the mix. Each also has weaknesses. Overemphasizing or ignoring a particular area could be detrimental to overall visibility or perspective of the indictors. Be sure the vendors being investigated are acquiring a balances dataset and ingests enough data for the industry it is going to be used to monitor.

Organizations mature enough to evaluate a DTIM platform should consider the tools they have in place. SIEM, firewalls, and IDS are some of the most common. A premium platform offers integration with SIEM to facilitate centralized incident management with defensive systems to exchange data as needed.

Functionality

Functionality ratings included questions about how well the platform was able to analyze data, determine threat levels, assign risk, facilitate incident workflows and collaboration, aid remediation of an issue once identified, and deliver reporting.

Key Areas for Consideration: Analysis and Automation, Third-Party Risk

Integrations are crucial for DTIM. Part of the criticality leads to the ability to automate tasks, especially remediation tasks. If the platform has the capability to automate the update, the defensive policies on firewalls or other defensive systems save time and reduce risk by closing attack surfaces or compromises faster. However, an additional consideration is how the platform and the vendor help remediate and clean up incidents on the Internet.

Most of what DTIM identifies occurs outside the perimeter from others usurping assets of one kind or another, so remediation requires working through legal channels with ISPs, domain registrars, app stores, and others to terminate infringement. Engaging a platform provider with relationships in place to address those issues is extremely helpful in reducing the red tape, stress, and delays that are often associated with this sort of remediation work.

Engaging a platform that can aid in identifying risk associated with third-party suppliers, vendors, or other partners is also a benefit. There was a lot of attention on third-party risk in the last few years, and with good reason: organizations have been used to gain unauthorized access to valuable resources. DTIM is not designed to be a full third-party risk management solution at this time, but identifying risks can help organizations be proactive in shoring up defenses or terminating relationships to reduce overall risk.

Vendor Strength

Vendor strength is visualized by the size of the bubble in the bubble chart. It evaluated multiple factors, including but not limited to: company vision and direction in the market, investment in research and development, third-party recognition, company growth, and funding debts.

Key Area for Consideration: Company Stability

When considering which solution to buy, the vendor's vision must align with the company's vision, and customer support for new features and bug fixes must also be considered. There is a tradeoff decision that must be made. Smaller vendors are more flexible with customer requests and generally tend to be more agile in delivering on those requests. However, many security startups either go bust or have their intellectual property acquired by another company that takes it in a different direction, so the vendor's financial stability must be a consideration.

INVITED VENDORS AND NOTABLE ABSENCES

There are quite a few vendors that compete in the DTIM space, both fully and partially. Some vendors specialize in the facets of threat and risk they monitor, while others are much broader. The focal areas vary from types of monitored environments (domain information or social media) to types of analyzed threats (brand infringement, credential, or identity theft).

When EMA invited vendors to participate, they did not discriminate based on any factor. Listed below are vendors that compete in the DTIM space in some manner, but did not respond to the request to complete the KPI survey or responded that they did not have the resources to complete the survey in the requested interval. A few felt that though they are strong in their niche of the space, their solution might not be well-represented to a broader market and decided not to participate. No organization that wanted to participate was denied the opportunity to do so.

BitSight[2]
BrightPoint
Centripetal
Crisp Thinking
CrowdStrike
CyberInt
DigitalShadows
Digital Stakeout
FireEye
Infoblox
Intel471
LifeRaft
ListenLogic
MarkMonitor
OWL Cybersecurity
PhishMe
Proofpoint[3]
Qadium
Recorded Future
Security Scorecard
ZeroFox

[2] BitSight did not respond to requests to validate its profile, so the profile is not included in the report. Data was gathered from available public sources.
[3] Proofpoint did not respond to requests to validate its profile, so the profile is not included in the report. Data was gathered from available public sources.

Value in any solution can be clearly defined by comparing the strength of the platform with its cost effectiveness. The EMA Digital Threat Intelligence Management Landscape Chart provides graphical representations of evaluated industry leader positioning in relation to both critical axes. The Product Strength axis combines evaluation scores for Functionality with Architecture & Integration. Cost Efficiency is calculated by adding the scores achieved for Cost Advantage and Deployment & Administration. The size of each bubble indicates scoring for Vendor Strength.

In every solution, there are tradeoffs to be made. There are two primary approaches to achieving value leaderships. Some vendors approach value leadership by trying to create premium solutions that have "all" of the functionality that can be imagined, thus meeting the broadest possible use cases and also usually commanding premium pricing, thus falling high on the Y axis and lower on the X axis. The other approach uses the 80/20 rule. This approach means providing somewhere around 80 percent of all desired features, but doing it at a much lower cost, thus falling high on the X axis and lower on the Y axis.

There is also a fallacy that should be addressed. Both vendors and consumers have the perception that being in the top right corner is the optimal position. This is not entirely true. Though optimal for the consumers, it is not optimal for the vendors.

Those that gain funding and market share initially tend to do it through innovation and marketing, which create solution differentiation with a premium, feature-leading solution. Others that are not able to collect equivalent findings or maintain a premium feature set parity have to reduce their pricing and research and development costs. If the market is out of the emerging phase but still in the early- to mid-growth phase, there is often enough spend in the market to support the vendors as they fall into place as a feature leader or price leader. If not, companies falter at making a quick decision on their target audience and tend to either go out of business or get acquired in this disruptive transitional phase.

For the buyer, the upper right corner is most desirable. Those companies have maximum functionality and maximum value, and the lowest cost for the desired features. The problem is that solutions don't hover in that spot for long due to feature and economic pressures. As the market matures, solutions tend to polarize into feature leaders that demand a premium price and therefore begin moving left on the X-axis, or price leaders that have fewer features and a lower cost, therefore move down on the Y-axis. Movement either left or right on the X-axis depends on how much they push the price down and what proportion of the key features they maintain.

When making the decision to buy, desire for features often conflicts with budgetary limitations. Buyers are either forced to spend more than they want to, being pushed outside of the Strong Value range, or be willing to sacrifice features, being pushed down the Y-axis, selecting a Value Leader solution at a lower cost. In general, maximum vendor revenue is somewhere around the dividing line between Value Leader and Strong Value at the top left of the Value Leaders triangle. On the other hand, consumers tend to maximize value in the bottom right corner of the Value Leaders triangle because even though they receive fewer features, the significantly lower cost creates a strong option for prospects looking to try the solutions out. The low cost can still support viable vendors in the space due to the sizable customer base.

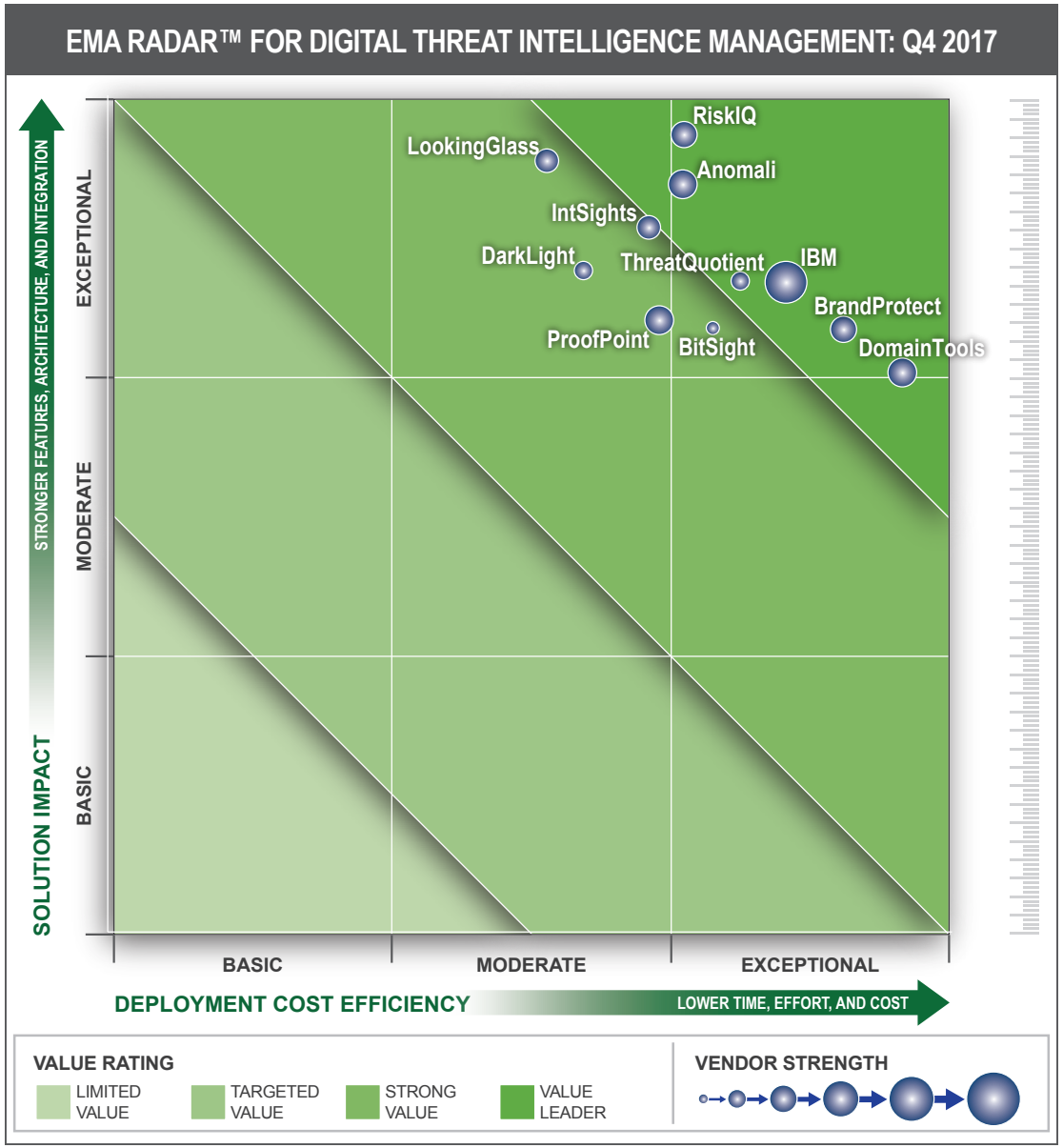


Figure 3: EMA Digital Threat Intelligence Management Market Landscape Chart

OVERVIEW

Anomali is a strategic player in the DTIM space. Founded originally as ThreatStream in 2013, the company changed its name to Anomali in 2015 but retained ThreatStream as its platform name. The company is well-funded, with strong sales history and expectations. It is one of only two smaller companies to receive a 5 out of 5 Financial Strength rating and an overall "strong" vendor rating.

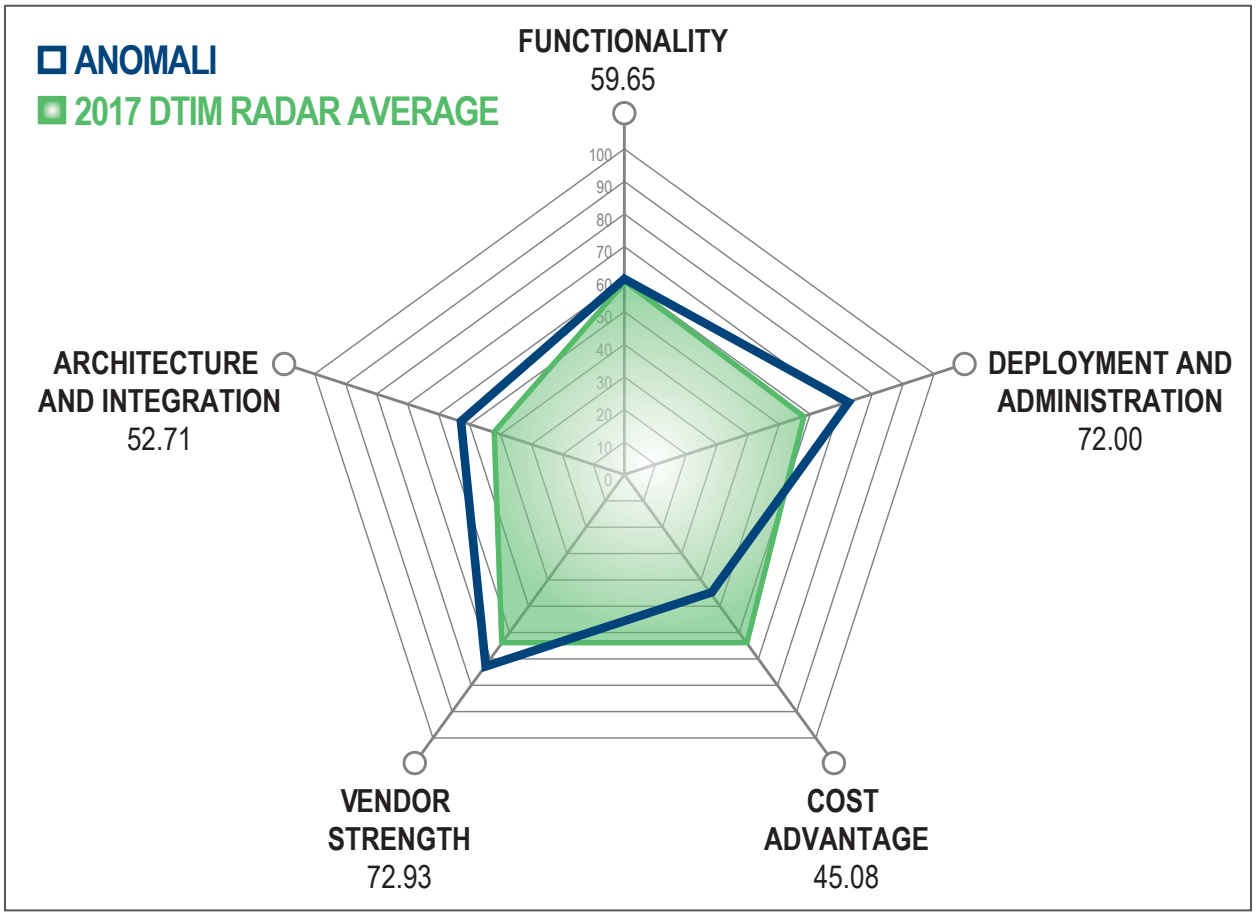
ThreatStream allows organizations to collect, manage, and operationalize external and internal threat intelligence. The ThreatStream platform is a third-party data aggregator and a primary data collector. Its data comes from all four sources identified in the report: proprietary, government, commercially licensed, and subscribed open sources. The program analyzes the data to align the telemetry streams into related and mutually corroborated events, thus eliminating duplicate information, reducing false positives, and delivering actionable events. Anomali was one of only three vendors to receive an overall outstanding Architecture & Integration rating due to its ability to integrate with internal security infrastructure, such as SIEMs, firewalls, IPS, and endpoint systems to deliver threat intelligence to monitoring and blocking tools.

Though professional services are available for onsite installation and configuration, they are not required. The platform can be shared across multiple operations centers and supports multi-team collaboration. The GUI is customizable by role and individual needs, and delivers a beautiful dashboard for daily work or for specialized activities. Most key operations are less than four clicks away, and the ThreatStream platform supports context-sensitive drilldown for easier workflow.

Anomali was rated lower than average in cost advantage, meaning it is more expensive than average. It is not the only solution to be ranked this way, nor is its standard pricing out of range for a premium service.

All of the Anomali customers interviewed indicated they received greater than expected value from the platform, and much of this was because Anomali is so receptive to their needs from the tool. As they identify new workflows and use cases, Anomali is quick to add many of them to the platform. These customers indicated that on average, they increased investigation case throughput by three to five times. They shifted their focus from information gathering to incident response due to the platform's data ingestion and analysis capabilities.

RADAR CHART EVALUATION



STRENGTHS AND WEAKNESSES

Anomali strengths are:

- Strong financial base
- Cloud/SaaS and on-premises deployment options
- Broad array of solution and protocol integrations
- Strong GUI usability
- Very fast to adapt to customer needs and suggestions

Anomali limitations are:

- Potentially high reliance on third-party, open-source information
- Detection solution, no remediation or takedown
- Currently limited support for mobile application- and social media-based threats
- Phone and live web chat support are 5x24

RATING SUMMARIES

DEPLOYMENT & ADMINISTRATION: STRONG	
Deployment Flexibility	Outstanding
Ease of Administration	Outstanding
Need for Professional Services	Strong
Licensing Options	Strong

ARCHITECTURE & INTEGRATION: OUTSTANDING	
Architecture	Strong
Integration	Outstanding
Trigger-Based Automation	Strong
Data Source Management	Outstanding
Detection, Identification, and Analysis of Threat Types	Outstanding

FUNCTIONALITY: STRONG	
Threat and Risk Identification and Assessment	Solid
Digital Threat Management	Strong
Data Management	Solid
Feature Differentiation	Outstanding
Remediation	Limited
Management Console	Outstanding
Out-of-Box Reporting	Outstanding
Report Flexibility	Solid

VENDOR STRENGTH: STRONG	
Vision, Strategy, and Direction	Strong
Financial Strength	$$$$$

OVERVIEW

BrandProtect has been delivering digital threat intelligence longer than any other company in the Radar Report. Delivering its first solution in 2002, BrandProtect expanded its protection solution into a suite consisting of five components for monitoring persons, places, and things across the Internet, including domains, email, mobile, and social media. BrandProtect identifies sites on the surface web and theft across the web and deep web.

To protect companies from the significant risks arising from fraudulent or unauthorized online activities, BrandProtect uses a seasoned team of experienced intellectual property (IP) threat analysts to deploy a unique combination of advanced proprietary technology, incident-oriented workflow, advanced reporting, and threat forensics. BrandProtect can quickly identify and take action on illegal, infringing, or threatening online incidents involving IP, trusted brands, and trademarks.

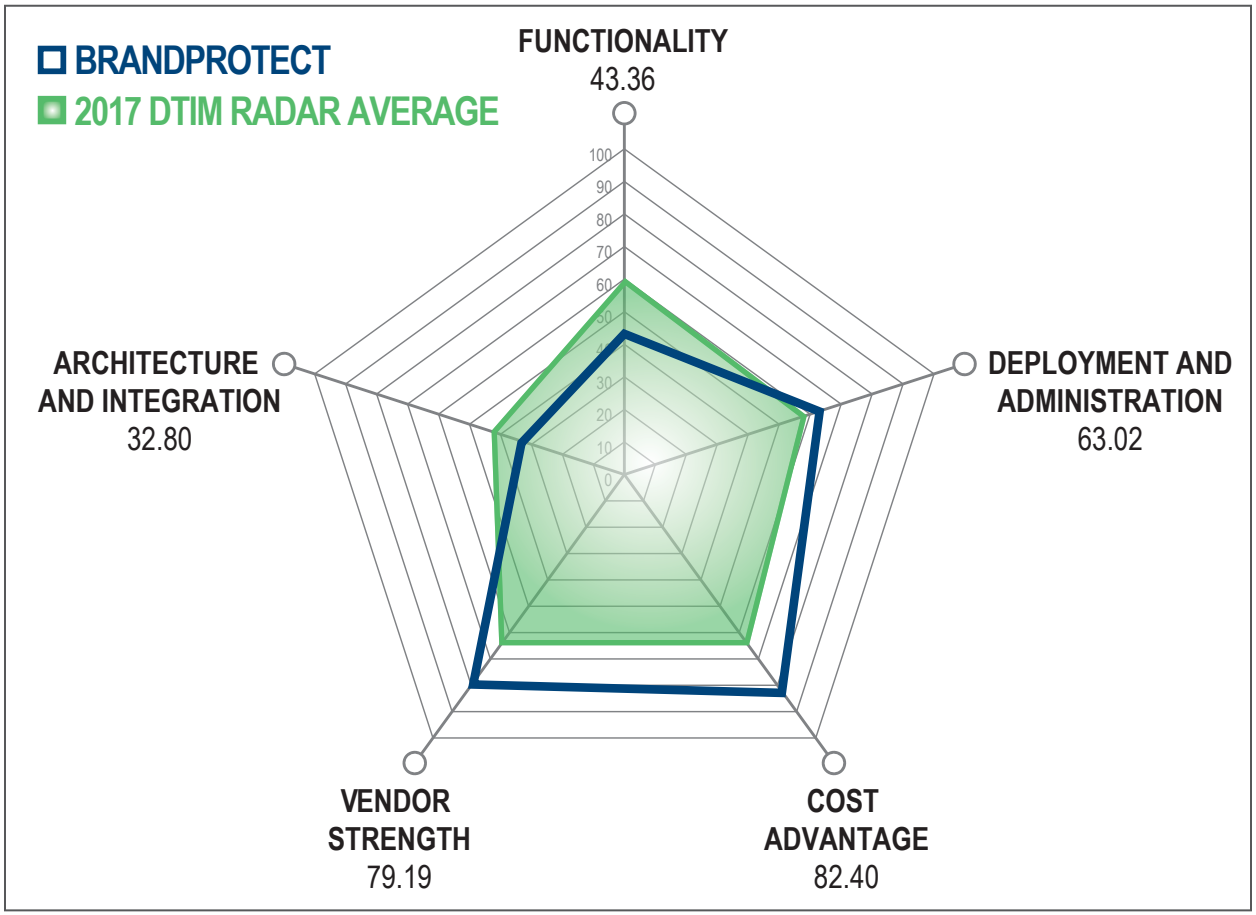
BrandProtect is focused specifically on threats around operational, reputational, revenue, legal, and compliance business risk. Its focus on these areas make it a standout among other vendors in this report. Though it does not address as wide an array of threats as most of the other vendors, it earned a Specialized Technology award because it is very strong at what it does. BrandProtect is not well known compared to other, much newer companies in the report. This lack of visibility in the marketplace may be due to being primarily bootstrap-funded and thus spending more on technology delivery, with very little spent on marketing. They sell primarily by word-of-mouth and tradeshows, with only a small outside sales force. These choices had the advantage of allowing the BrandProtect team to focus on developing the platform based on customer feedback rather than the decisions of a third-party funding organization.

BrandProtect's vision of the threat universe is somewhat compartmentalized. Given what they focus on, their vision could be upgraded to "strong" or even possibly "outstanding." Looking at the broader marketspace and their competition, it is ranked as "solid." Their Detection, Identification, and Analysis of Threat Types are in the same position. In their focal area, they deliver in an "outstanding" manner for clients across numerous verticals. However, given the current evolution of the broader threat intelligence market, their detection was only "strong."

One of the primary aspects that made BrandProtect a Value Leader is its overall competitive cost. Notice in the vendor placement bubble chart, it is very far to the right. Compared to most of the other solutions, BrandProtect is far less expensive. For organizations focused on brand and personnel protection, this service has a more significant value proposition.

VALUE LEADER: BRANDPROTECT

RADAR CHART EVALUATION



STRENGTHS AND WEAKNESSES

BrandProtect strengths are:

- Assisted clients in over one million mitigations
- Outstanding variety of reporting
- Wide array of integration protocols
- Support, on-premises, cloud/SaaS, and managed service delivery

BrandProtect limitations are:

- High focus on its proprietary data causes it to ignore some other useful data streams with no government-supplied data sources
- Detection breadth (not depth) could be expanded
- Major updates only semi-annually

RATING SUMMARIES

DEPLOYMENT & ADMINISTRATION: STRONG	
Deployment Flexibility	Outstanding
Ease of Administration	Strong
Need for Professional Services	Solid
Licensing Options	Outstanding

ARCHITECTURE & INTEGRATION: SOLID	
Architecture	Strong
Integration	Outstanding
Trigger-Based Automation	Strong
Data Source Management	Solid
Detection, Identification, and Analysis of Threat Types	Strong[1]

FUNCTIONALITY: STRONG	
Threat and Risk Identification and Assessment	Strong
Digital Threat Management	Solid
Data Management	Strong
Feature Differentiation	Solid
Remediation	Strong
Management Console	Solid
Out-of-Box Reporting	Strong
Report Flexibility	Outstanding

VENDOR STRENGTH: STRONG	
Vision, Strategy, and Direction	Solid[2]
Financial Strength	$$$

[1] See notes in BrandProtect Overview, fourth paragraph
[2] Ibid.

OVERVIEW

DomainTools was founded in 2002 to provide DNS research tools that monitor brand infringement, domain monitoring and valuation, and website change histories. However, the growth of the threat intelligence market in the last three years fueled DomainTools' focus on expanding into three solutions to fight cyber-crime in the same areas. This evaluation focuses on the Iris solution.

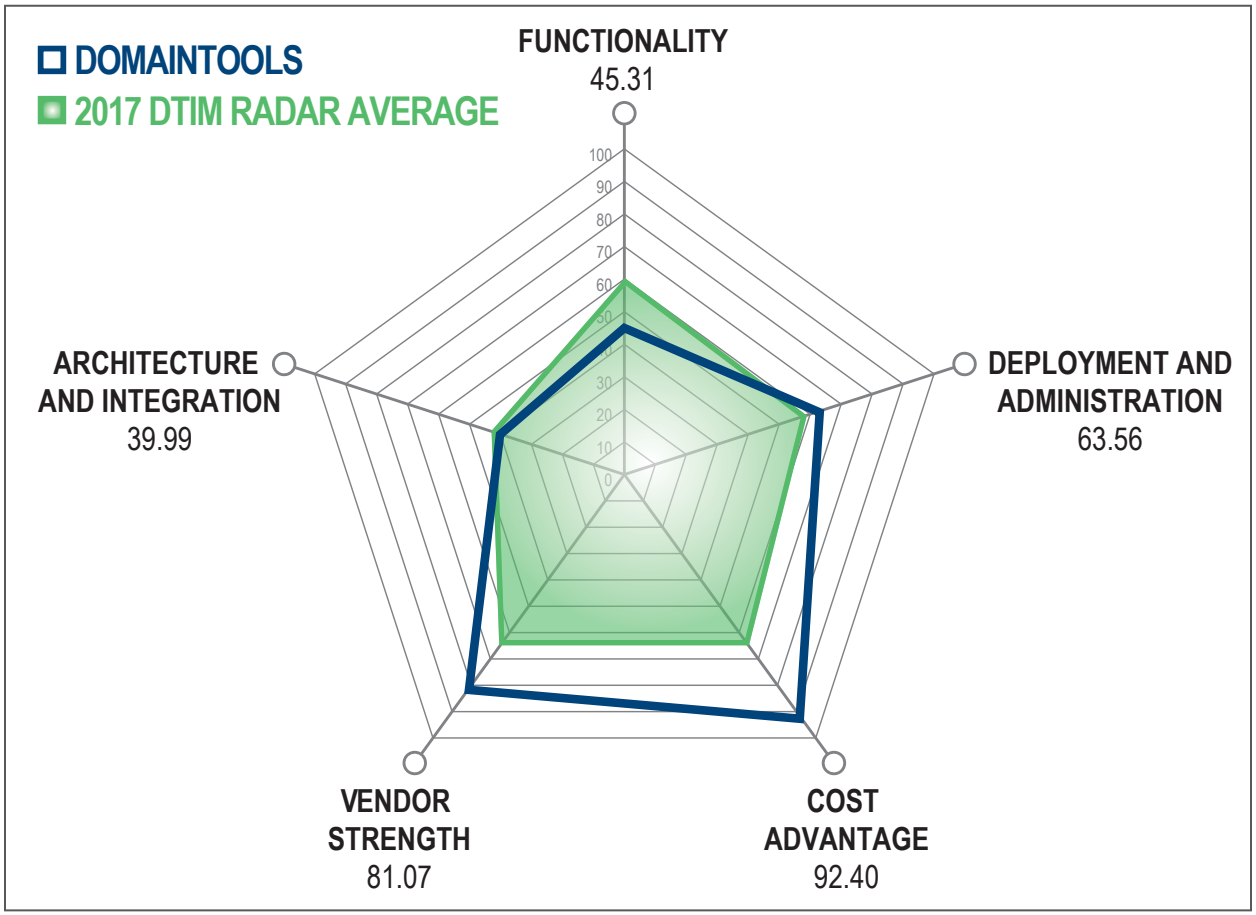
DomainTools helps security analysts turn threat data into threat intelligence. Its solutions give organizations the ability to create a forensic map of criminal activity, assess threats, and prevent future attacks. The Iris solution ingests data into a huge repository of historical information, giving customers access via portal and API. Customers use the information to detect risks arising from fraudulent or unauthorized online activities involving DNS, domains, IP addresses, and websites. DomainTools' information is so extensive that it is used as a data source for other threat intelligence feeds.

Because DomainTools is focused on threats specifically around DNS, domain, IP, and websites, it is considered more of a niche player. It does not address as wide an array of threats as most of the other vendors; however, it is exceptionally strong at what it does. It has the most detailed and farthest-reaching archive of DNS, domain, IP, and website information, earning it a Specialized Technology award.

DomainTools' vision of the threat universe is very focused. They received a "strong" rating on their Vision, Strategy, and Direction due to that focus being narrower than the current market direction. However, in the context of what it focuses on, its Vision, Strategy, and Direction could be upgraded to "outstanding." Their Detection, Identification, and Analysis of Threat Types are also in the same position. Though rated as "solid" for the across-the-market view, in their focal area, they deliver in an "outstanding" manner for clients across numerous verticals.

In the vendor placement bubble chart, DomainTools is very far to the right. However, it is not as high compared to most of the other solutions. One of the primary aspects that made DomainTools a Value Leader is its overall competitive cost. Its narrower focus pushes it down in the analysis, but its lower cost pushes it to the right, nudging it into the Value Leader area. For organizations that are focused on using current and historical domain information to augment their threat intelligence or protect their brand, this service has a much higher value proposition.

RADAR CHART EVALUATION



STRENGTHS AND WEAKNESSES

DomainTools strengths are:

- Depth of delivery in domain, DNS, IP, and web
- Strong threat and risk identification and analytics
- Solid financial base

DomainTools limitations are:

- Only leverages three of four main data sources
- Detection solution, no remediation or takedown
- Limited integrations for trigger-based automation

RATING SUMMARIES

DEPLOYMENT & ADMINISTRATION: STRONG	
Deployment Flexibility	Outstanding
Ease of Administration	Solid
Need for Professional Services	Strong
Licensing Options	Strong

ARCHITECTURE & INTEGRATION: STRONG	
Architecture	Outstanding
Integration	Solid
Trigger-Based Automation	Limited
Data Source Management	Strong
Detection, Identification, and Analysis of Threat Types	Solid[1]

FUNCTIONALITY: SOLID	
Threat and Risk Identification and Assessment	Strong
Digital Threat Management	Strong
Data Management	Solid
Feature Differentiation	Strong
Remediation	Limited
Management Console	Solid
Out-of-Box Reporting	Limited
Report Flexibility	Solid

VENDOR STRENGTH: STRONG	
Vision, Strategy, and Direction	Solid[2]
Financial Strength	$$$$$

[1] See notes in DomainTools Overview, fourth paragraph
[2] Ibid.

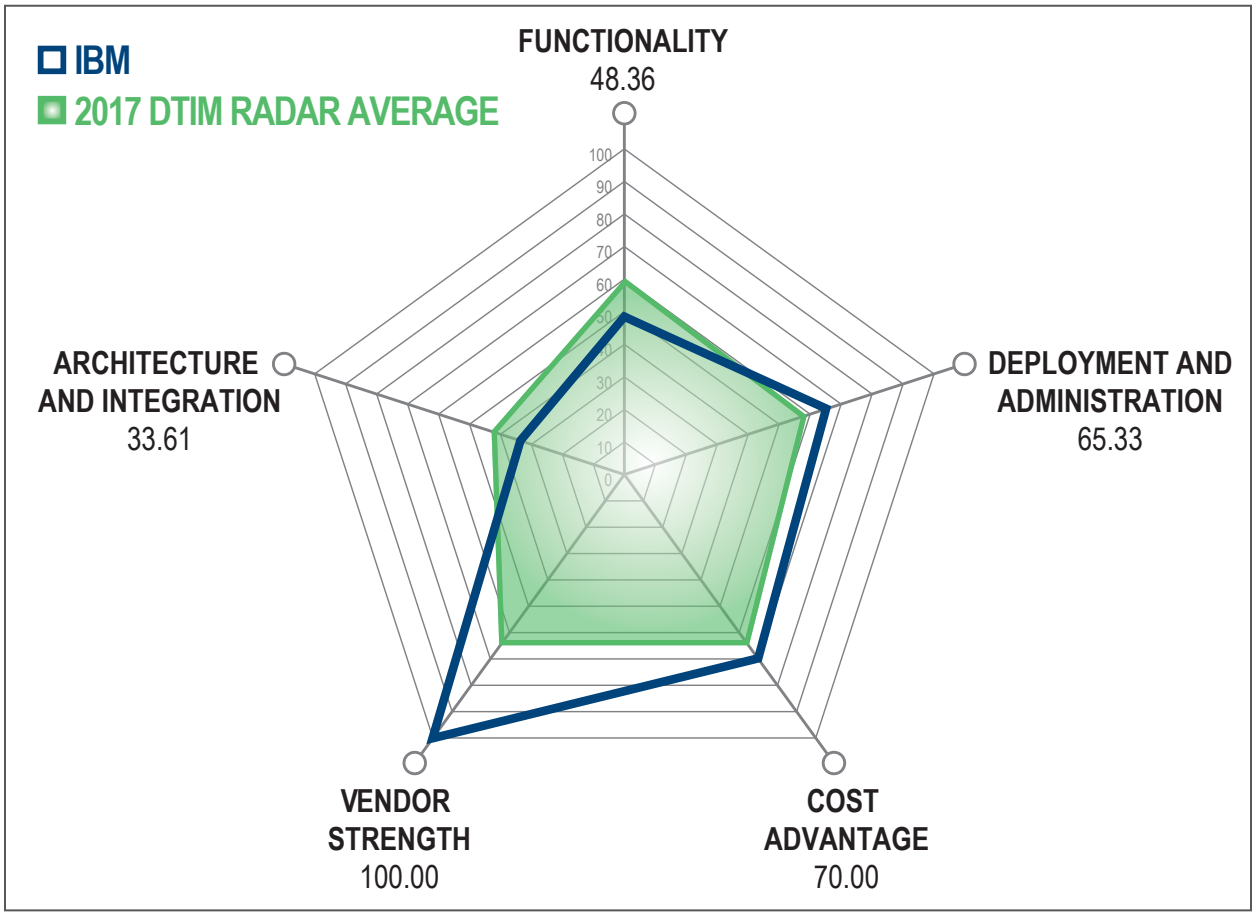
OVERVIEW

The IBM X-Force Exchange is a cloud-based platform offering both free and paid-for versions of access to the platform and the use of APIs for backend interaction. The subscription is delivered as a managed service and as a portal with access to a robust commercial API, while providing access to an SDK for further integration development. The platform is designed to facilitate security analyst access to and sharing of threat information to increase efficiency of incident investigation and response.

IBM entered the threat intelligence arena in full force, and in a less than one year deployed a formidable platform for the security community. However, it is important to note that though IBM is highly effective in identifying numerous threat types, the focus of the service does not include areas such as brand infringements, exposures of company content, IP, or credentials on the web. Despite not having every form of threat embedded in the platform, its open access approach has drawn the largest subscriber base, with tens of thousands of subscribers from every imaginable industry vertical. Customers using the service are happy with its content delivery, interface, and reporting. Due to this accelerated adoption and overall satisfaction with the platform, EMA identified IBM as a Market Driver.

IBM X-Force Exchange was only identified as "limited" in three areas. The first was deployment flexibility, which is because of a strictly cloud-based offering. The second was due to a small range of licensing and usage options for the paid services. As seen by the platform adoption, these are not deal breakers for many perspective users. The third was because of the boundaries around brand, IP, content, and user credentials that are not identified. The threat identification could be remedied in a future release if IBM decides to focus resources on them.

RADAR CHART EVALUATION



STRENGTHS AND WEAKNESSES

IBM X-Force Exchange strengths are:

- API available for both the free and subscription versions
- Both public and private collaboration communities can be leveraged
- Broad range of collected data
- Threat telemetry is collected from thousands of points globally

IBM X-Force Exchange limitations are:

- Strictly an intelligence service, no enforcement and takedown assistance
- High focus on its proprietary data ignores some other useful data streams, with no government-supplied data sources
- Current limitations in types of threat detection

RATING SUMMARIES

DEPLOYMENT & ADMINISTRATION: STRONG	
Deployment Flexibility	Limited
Ease of Administration	Outstanding
Need for Professional Services	Outstanding
Licensing Options	Limited

ARCHITECTURE & INTEGRATION: OUTSTANDING	
Architecture	Outstanding
Integration	Outstanding
Trigger-Based Automation	Outstanding
Data Source Management	Outstanding
Detection, Identification, and Analysis of Threat Types	Limited

FUNCTIONALITY: SOLID	
Threat and Risk Identification and Assessment	Solid
Digital Threat Management	Solid
Data Management	Strong
Feature Differentiation	Solid
Remediation	Limited
Management Console	Solid
Out-of-Box Reporting	Outstanding
Report Flexibility	Solid

VENDOR STRENGTH: OUTSTANDING	
Vision, Strategy, and Direction	Strong
Financial Strength	$$$$$

OVERVIEW

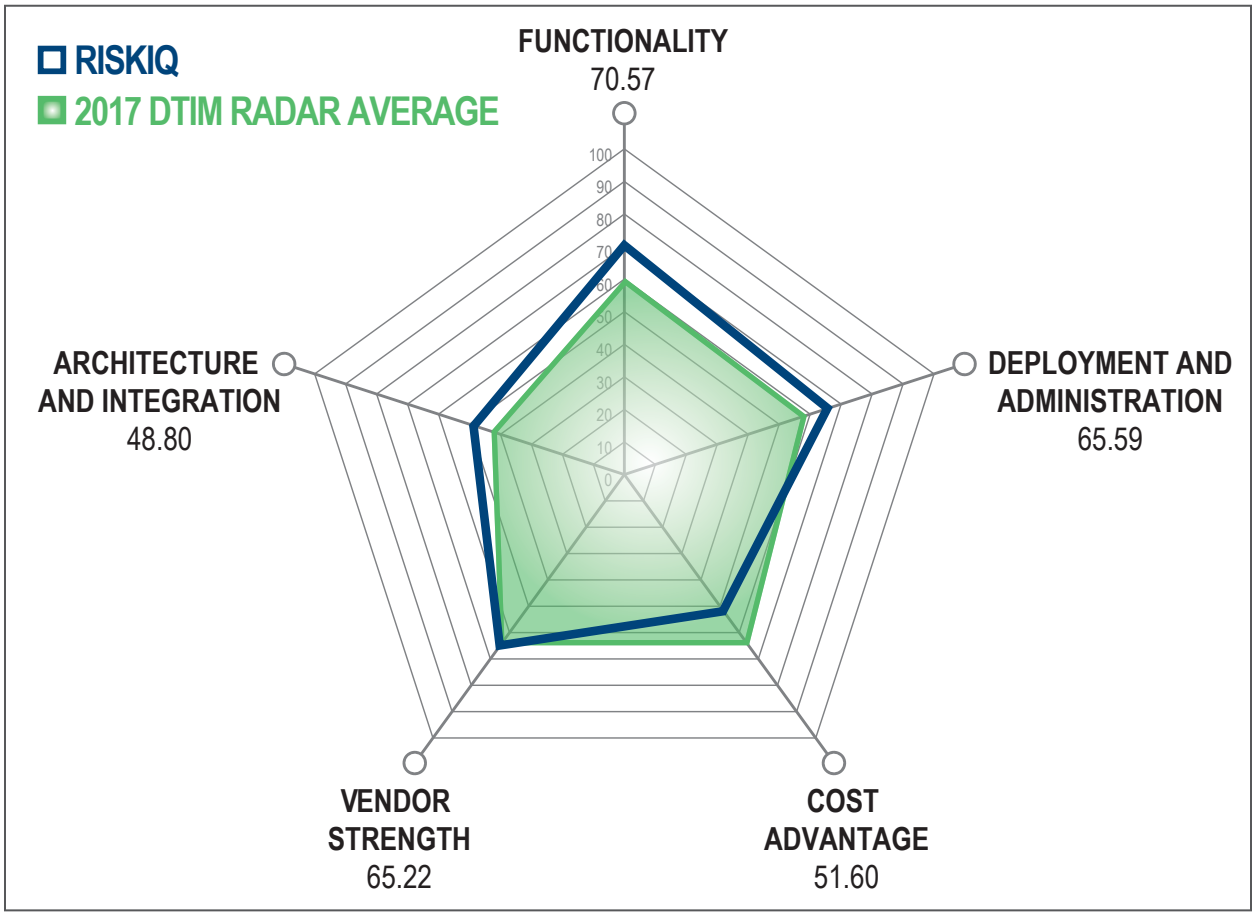
RiskIQ delivers a solution suite in a platform designed to maximize intelligence gathering, analytics, and external threat protection. In dissecting the platform capabilities, Enterprise Management Associates identified a great breadth of gathered data, including collection of deep web, social media, mobile, and open-source artifacts. By applying correlation models, RiskIQ provides derived data in the form of blacklists and external asset insights. This highly-enriched metadata intelligence saves analysts considerable time. Using a combination of largely proprietary means, RiskIQ collects and maintains vast correlated web asset, exploit, attacker, and threat information. By using RiskIQ's task-driven web applications, organizations can optimize data use across teams for incident response, SOC, and vulnerability analysis. A mature API and built-in integrations are available to augment internal security telemetry with external threat context.

Customer interviews with large global companies across major industries including finance and banking, manufacturing, and media all provided a common theme. By engaging RiskIQ, they were able to turn their cyber-risk management program around, moving from spending between 80 percent and 90 percent of the team's time gathering data to 90 percent or greater time spent on actual analysis and response actions. The banking and finance customers were pleased with RiskIQ's analytics for exposures such as PII/GDRP, while each of the industries had use cases for leveraging its new internal risk scoring. All interviewed customers reported they gained greater than expected value from the platform and saw large improvements in their work accuracy, broad use cases, and case throughput, making investing in the platform a strong value.

RiskIQ was identified as a Technology Leader due to its completeness of vision moving forward, as well as its ability to implement safeguards against that vision. RiskIQ's gathering and analysis of data were highly regarded by its customers, especially those that previously used other solutions.

EMA RADAR

RADAR CHART EVALUATION



STRENGTHS AND WEAKNESSES

RiskIQ strengths are:

- Very high data confidence
- Broad range of data collected globally
- Ease of use with advanced analytics
- Broad threat takedown capabilities
- Free community edition available (here)

RiskIQ limitations are:

- Strictly SaaS, cloud-based deployment
- No dark web or government-supplied data sources
- Desire for even more accelerated takedown timeframe
- Dashboards for different roles, but not customizable
- Focus on proprietary data may limit use of other data streams

RATING SUMMARIES

DEPLOYMENT & ADMINISTRATION: STRONG	
Deployment Flexibility	Limited
Ease of Administration	Outstanding
Need for Professional Services	Solid
Licensing Options	Solid

ARCHITECTURE & INTEGRATION: OUTSTANDING	
Architecture	Outstanding
Integration	Outstanding
Trigger-Based Automation	Solid
Data Source Management	Solid
Detection, Identification, and Analysis of Threat Types	Outstanding

FUNCTIONALITY: OUTSTANDING	
Threat and Risk Identification and Assessment	Outstanding
Digital Threat Management	Outstanding
Data Management	Outstanding
Feature Differentiation	Outstanding
Remediation	Outstanding
Management Console	Outstanding
Out-of-Box Reporting	Strong
Report Flexibility	Outstanding

VENDOR STRENGTH: STRONG	
Vision, Strategy, and Direction	Outstanding
Financial Strength	$$$

VALUE LEADER: THREATQUOTIENT

OVERVIEW

ThreatQuotient started delivering its ThreatQ platform in 2013. The team decided to focus on a centralized threat data management platform, which ingests one of the broadest data sets in the report of nearly 200 integration partners. Its primary focus was internal threat management, taking feeds from virtually all mainstream security tools from the perimeter to the endpoint and everywhere in between (most of which are bidirectional to maintain the updated information). However, it also receives data from nearly 100 external threat intelligence feeds with the click of a mouse, provided the client has the applicable licensing from the feed owner.

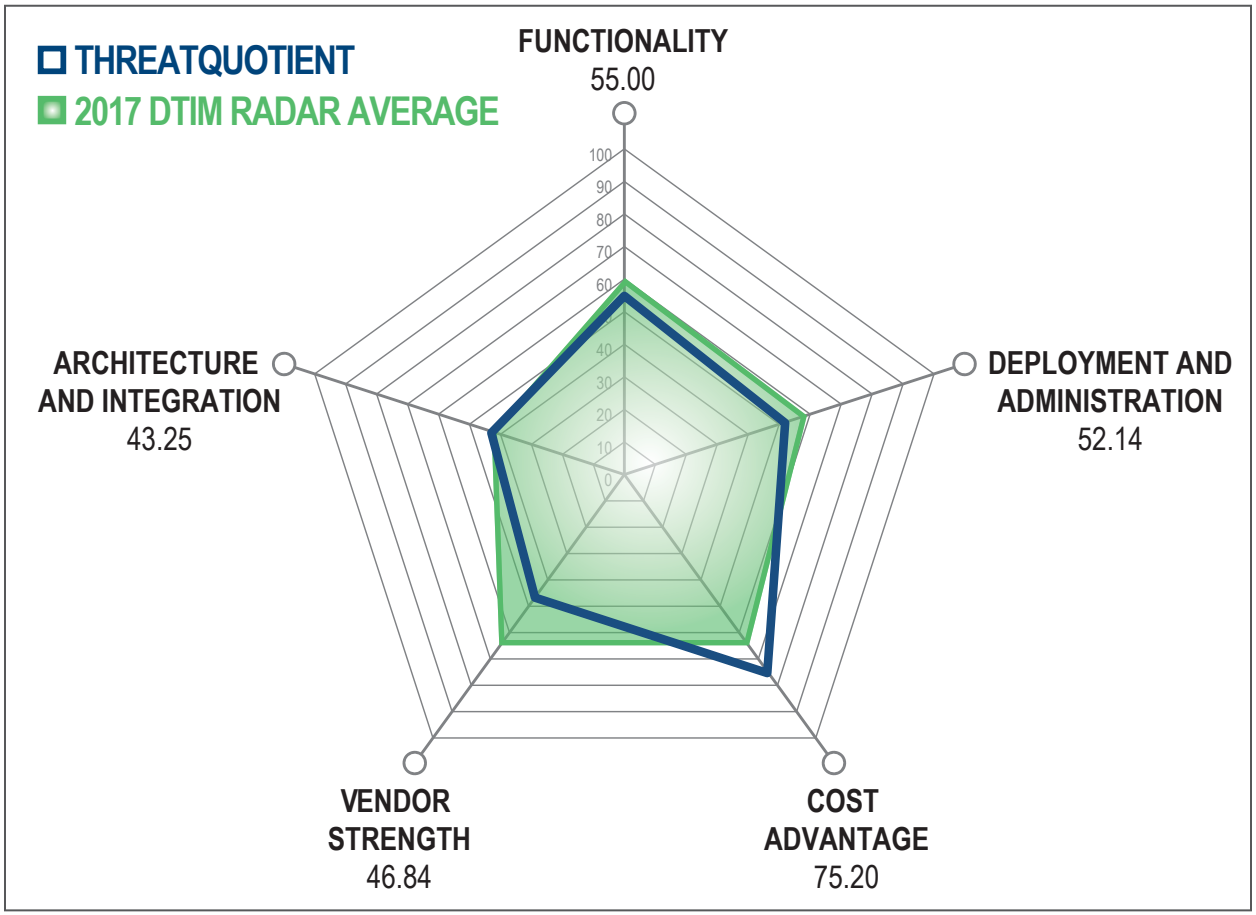
ThreatQuotient made a decision not to create its own proprietary data to maintain lower product costs and provide a data platform that could be used in conjunction with other risk or threat platforms. The foundation of this decision is ThreatQuotient's goal to create a continuous threat assessment lifecycle that shifts organizations from operating in a reactive and tactical mode into a proactive and strategic mode. The lifecycle transformation consists of creating understanding through better information assimilation and context, improving prioritization driven by customer definition, driving action through automation and orchestration with existing tools, and developing a learning platform that improves environmental awareness using a self-tuning threat library that improves as more data and context enter the system.

The most significant impacts to ThreatQuotient's placement in the Radar Report are not architectural or performance-related, but driven by the platform's newness. The development team can only move so fast to increase functionality and maintain stability, so they had to make feature prioritization choices. With few wizards for setup and configuration, ThreatQuotient recommends professional services for installation, system tuning and customization, and providing custom integrations. Its internal reporting is extremely limited, but it does provide the broadest data export capability in the report and can readily move information into an existing reporting system like crystal reports. The platform is delivered via software, VM images, and/or an appliance that can be installed on-premises or in the cloud. However, they do not currently offer their own hosted, multi-tenant SaaS/cloud solution.

On the other hand, ThreatQuotient's data collection and dissemination architecture seem "outstanding" and ready for large-scale integration. Its directional vision for the ThreatQ platform is well-defined, and its ability to correlate threat data into a single, actionable event is "outstanding." ThreatQuotient leads to minimal false identifications and creates the foundation for confident automatic actions to minimize threat incursion and subsequent damage.

VALUE LEADER: THREATQUOTIENT

RADAR CHART EVALUATION



STRENGTHS AND WEAKNESSES

ThreatQuotient strengths are:

- Strong cash flow (new funding round)
- Outstanding integrations for data ingestion and integrations for data export to tools
- Excellent GUI usability
- Very good integrations for automating response with internal security systems

ThreatQuotient limitations are:

- No proprietary data (business choice)
- No external takedown relationships
- Limited internal reporting flexibility
- Support is currently only in business hours

RATING SUMMARIES

DEPLOYMENT & ADMINISTRATION: SOLID	
Deployment Flexibility	Strong
Ease of Administration	Limited
Need for Professional Services	Very Low
Licensing Options	Limited

ARCHITECTURE & INTEGRATION: OUTSTANDING	
Architecture	Outstanding
Integration	Outstanding
Trigger-Based Automation	Strong
Data Source Management	Solid
Detection, Identification, and Analysis of Threat Types	Outstanding

FUNCTIONALITY: STRONG	
Threat and Risk Identification and Assessment	Solid
Digital Threat Management	Outstanding
Data Management	Solid
Feature Differentiation	Strong
Remediation	Strong
Management Console	Outstanding
Out-of-Box Reporting	Limited
Report Flexibility	Strong

VENDOR STRENGTH: LIMITED	
Vision, Strategy, and Direction	Strong
Financial Strength	$$$

STRONG VALUE: DARKLIGHT CYBERSECURITY

OVERVIEW

DarkLight Cybersecurity was founded in 2013. It is a bit of an anomaly in the report and was difficult to classify in some ways. It is not a pure-play threat intelligence platform; nor does it supply its own data. However, it is an artificial intelligence-based expert system for active cyber defense and trusted information sharing. DarkLight is a force-multiplier for cyber analysts to codify their processes and workflows in order to execute them at machine-speed. As such, it intakes virtually any security data in a company's infrastructure.

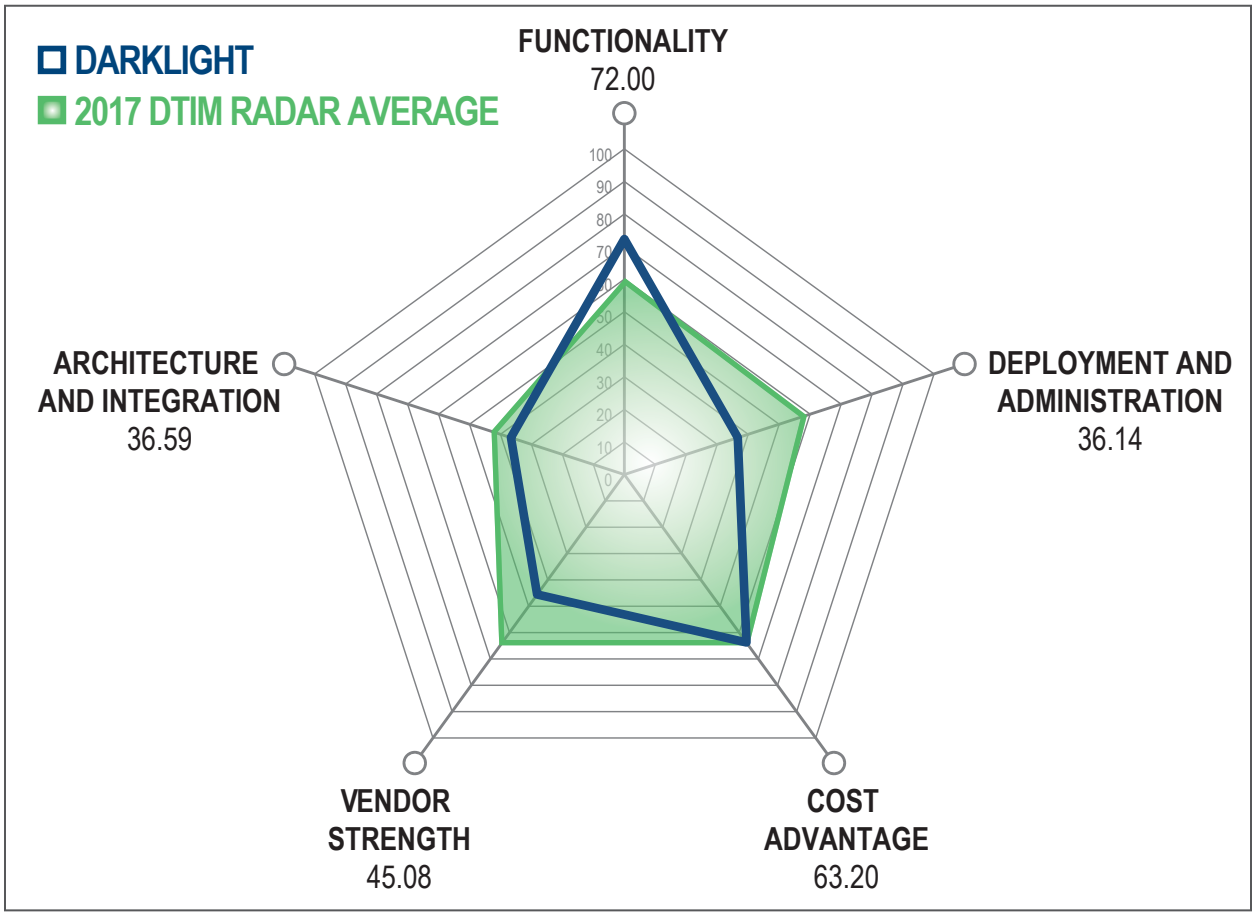
DarkLight is radically different from the typical DTIM solution in several ways, and is most frequently aligned with security orchestration and automation platforms. It is entirely reliant upon data provided by other systems for analysis. Because of that, DarkLight delivers focused insights into the areas of threat in which the customer concentrates their data gathering. If the DarkLight analysis engine is fed external threat information, it will incorporate that information into the analysis to show relationships between external and internal activities. Interestingly, DarkLight had the broadest range of threat detections in the reviewed vendors. Given the right data, it has the possibility of producing some of the best results. When provided with the organizational security telemetry, it was rated as "outstanding" at Detection, Identification, and Analysis of Threat Types with very low, if any, false positives. The underlying systems and data architecture was rated as "strong."

The artificial intelligence analysis engine is one of the more advanced AI-labeled tools. It is a true expert system designed to learn directly from an organization's cyber security team through the use of its AI-driven playbooks. DarkLight's expert system is designed to emulate the sense and decision-making of humans, and apply knowledge and reasoning to solve complex problems. Users may share their playbooks (including the mapping and knowledge models for the datasets used by the playbook) within trusted communities. ISAC and ISAO groups can move from sharing actionable intelligence to also sharing playbooks that can automate decisions and actions that should be taken based on that intelligence.

Once DarkLight works on a threat, the company provides orchestration of a response via any product supporting OpenC2. DarkLight can provide explainable, evidence-based results for further action by the analyst or legal team. It also has the ability to execute tasks and scripts, access other solutions via API, and send emails to MSSPs or others to initiate response or takedown actions.

STRONG VALUE: DARKLIGHT CYBERSECURITY

RADAR CHART EVALUATION



STRENGTHS AND WEAKNESSES

DarkLight Cybersecurity strengths are:

- Strong data ingestion integrations
- AI-driven playbooks for cyber investigations
- Outstanding incident collaboration
- Largest range of detected threats

DarkLight Cybersecurity limitations are:

- Does not offer a cloud/SaaS option
- Requires significant initial professional services
- More focused on internal threat management

RATING SUMMARIES

DEPLOYMENT & ADMINISTRATION: LIMITED	
Deployment Flexibility	Limited
Ease of Administration	Limited
Need for Professional Services	High
Licensing Options	Limited

ARCHITECTURE & INTEGRATION: STRONG	
Architecture	Solid
Integration	Strong
Trigger-Based Automation	Solid
Data Source Management	Limited
Detection, Identification, and Analysis of Threat Types	Outstanding

FUNCTIONALITY: STRONG	
Threat and Risk Identification and Assessment	Strong
Digital Threat Management	Strong
Data Management	Solid
Feature Differentiation	Outstanding
Remediation	Outstanding
Management Console	Outstanding
Out-of-Box Reporting	Solid
Report Flexibility	Solid

VENDOR STRENGTH: LIMITED	
Vision, Strategy, and Direction	Solid
Financial Strength	$$

OVERVIEW

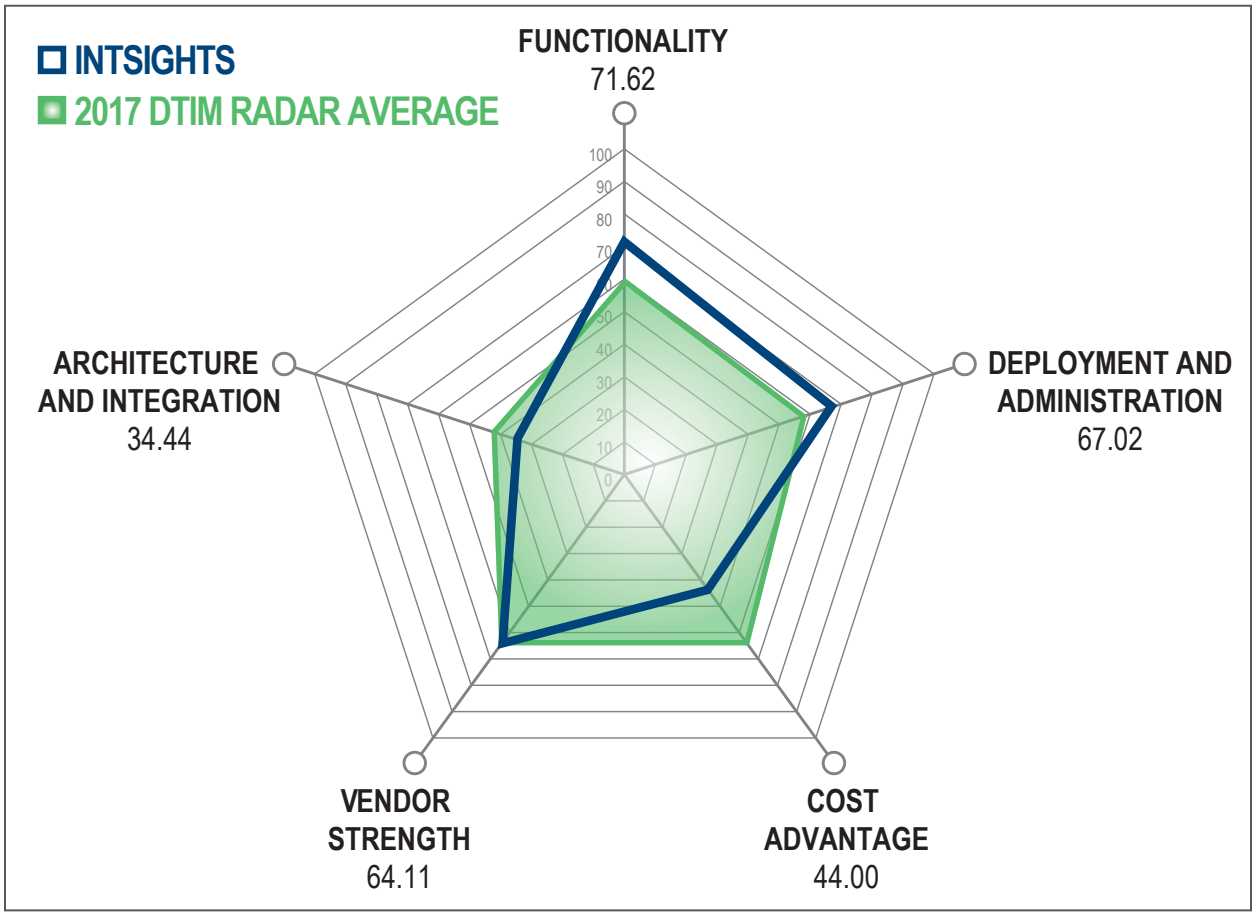
Coming on the threat intelligence scene in 2015, IntSights Cyber is the newest player in the report. The IntSights Enterprise Threat Intelligence & Mitigation platform delivers tailored enterprise threat intelligence gathered from dark, deep, and clear webs, including social media. With IntSights, enterprises have complete visibility into attack supply chains targeting operations, employees, and assets. This intelligence, combined with third-party feeds, powers one-click threat remediation via integration with existing protection tools, keeping customers one step ahead of potential attacks.

IntSights constantly monitors numerous digital channels (e.g., dark web, black markets, forums, social media, etc.) to collect its proprietary data. A variety of sources and channels are monitored, including IM platforms, such as Telegram, Whatsapp, social media, app stores, cybercrime forums, paste sites, IRC channels, file sharing websites, and search engines. Each of the sources and channels are monitored for customers' names, brand names, domains, VIPs, sensitive business information, etc. IntSights also collects data from government and commercial subscriptions, as well as publicly-available sources. IntSights captures information from the source to identify all the relevant context about each specific threat. The ingested data is analyzed by a proprietary artificial intelligence engine developed specifically to identify cyber threats. Once a threat relevant to the customer is detected, an alert is generated and delivered to the customer. Due to the level of analysis using multiple source corroboration, when available, IntSights delivers very few false positives (one of the lowest rates seen).

IntSights was rated as "strong" in every aggregate category and received more "outstanding" ratings on the KPI subsections than any other vendor. For its age, it is well ahead of the curve, delivering capabilities that even some of the more established vendors are still working on. This is why it was awarded a Vendor to Watch. If it stays on its current trajectory, EMA expects that by the next iteration of this DTIM Radar Report, IntSights will move into the Value Leader segment and become a major challenger to the existing incumbents.

STRONG VALUE: INTSIGHTS CYBER SOLUTIONS

RADAR CHART EVALUATION



STRENGTHS AND WEAKNESSES

IntSights Cyber strengths are:

- Offered in cloud/SaaS, on-premises, and managed services
- Automated remediation capabilities
- Outstanding threat and risk identification and analytics
- Outstanding system architecture built for volume and speed

IntSights Cyber limitations are:

- Small company may be in danger of being acquired for technology stack
- Management console and workflows are still evolving
- May not be able to keep up with rapidly expanding customer base

RATING SUMMARIES

DEPLOYMENT & ADMINISTRATION: STRONG	
Deployment Flexibility	Outstanding
Ease of Administration	Strong
Need for Professional Services	Very Low
Licensing Options	Outstanding

ARCHITECTURE & INTEGRATION: STRONG	
Architecture	Outstanding
Integration	Outstanding
Trigger-Based Automation	Strong
Data Source Management	Solid
Detection, Identification, and Analysis of Threat Types	Outstanding

FUNCTIONALITY: OUTSTANDING	
Threat and Risk Identification and Assessment	Outstanding
Digital Threat Management	Outstanding
Data Management	Outstanding
Feature Differentiation	Strong
Remediation	Outstanding
Management Console	Solid
Out-of-Box Reporting	Strong
Report Flexibility	Outstanding

VENDOR STRENGTH: STRONG	
Vision, Strategy, and Direction	Strong
Financial Strength	$$$$

STRONG VALUE: LOOKINGGLASS CYBER SOLUTIONS, INC.

OVERVIEW

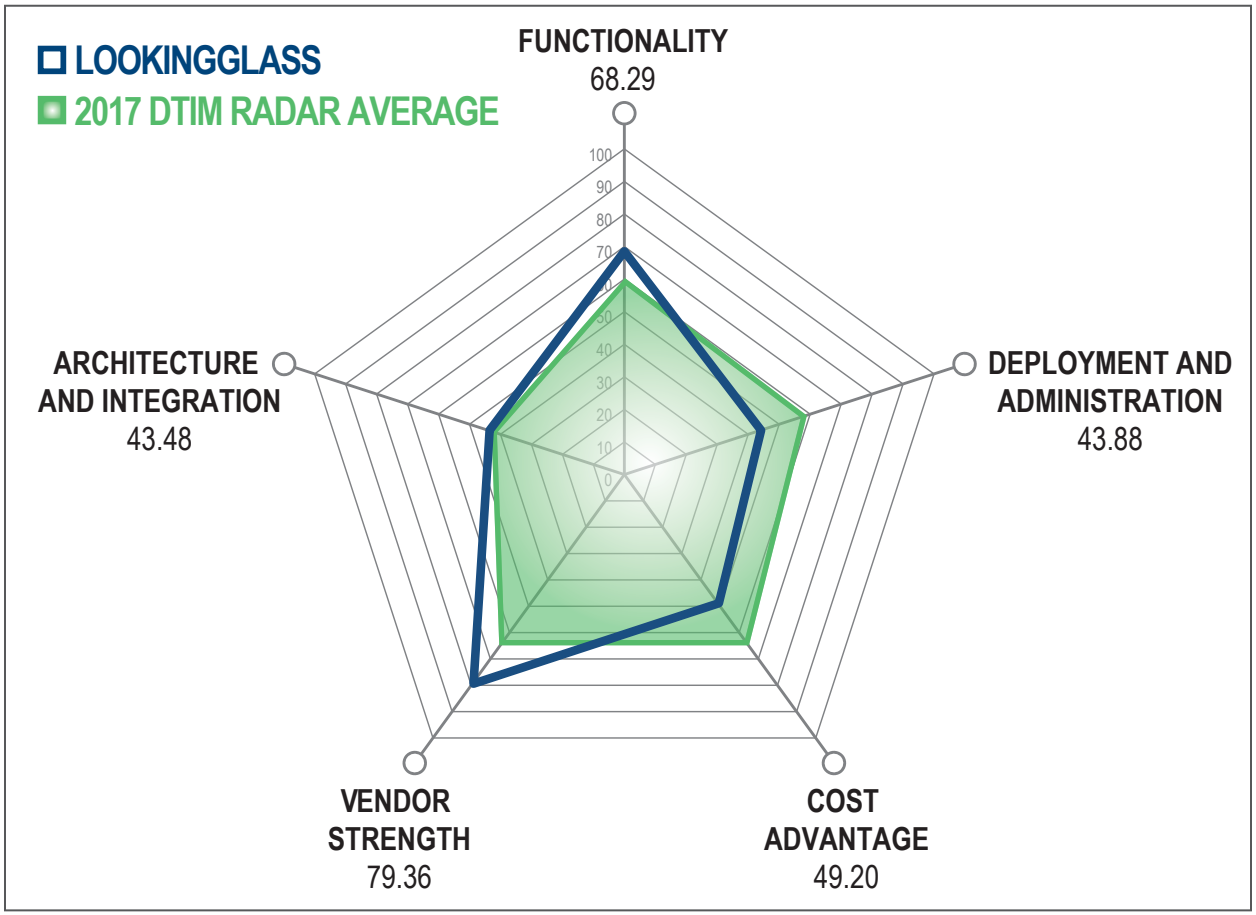
Founded in 2006, LookingGlass is one of the most mature companies in the digital threat management space. Since inception, it has evolved its offerings and expanded through acquisitions of CloudShield Technologies, Cyveillance, and Kleissner & Associates in 2015. Operating on its own capital and revenue for the first five years, LookingGlass accepted outside funding for debt financing in 2011. Since that time, it has absorbed over $108 million USD in multiple rounds, with the most recent in August of 2017. Though over $45 million was used for acquisitions and a substantial amount was poured into product development, this debt load negatively affected its Financial Strength, reducing its rating to "solid."

LookingGlass has one of the three largest customer bases. Clients come from numerous verticals, but LookingGlass seems to attract most of its clients from the government, financial, and oil and gas industries. The Fortune 500 tend to be proportionately larger consumers of threat intelligence due to their greater need to identify and thwart threats earlier in the threat lifecycle. Though premium platforms in the threat intelligence space most often come at a price, the LookingGlass suite comes with a hefty standard price tag that impacted its overall value. That said, it was still considered a "strong" value.

LookingGlass received numerous "strong" ratings and multiple "outstanding" ratings, the most notable of which are for its data collection and overall architecture, which comprise multiple aspects of its functionality. The original vision and technology stack were developed from the expertise of former intelligence agency personnel using a wholly different approach from the other vendors. Their concept was to use massive amounts of information (big data) from proprietary, government, commercial, and public sources, and use associative threat modeling to identify relationships between that data and their customers. Federal intelligence and law enforcement agencies use a similar model to detect relationships between known terrorists and other people they come into contact with to determine the possible threats created by those relationships and related activities. It is for LookingGlass's longevity, and more so, its approach for data analysis, that LookingGlass received a Technology Pioneer award.

STRONG VALUE: LOOKINGGLASS CYBER SOLUTIONS, INC.

RADAR CHART EVALUATION



STRENGTHS AND WEAKNESSES

LookingGlass strengths are:

- Unique threat identification and analysis model
- Provides remediation capabilities and facilitates post-incident workflow
- Processes and analyzes big data

LookingGlass limitations are:

- High focus on proprietary sources may diminish its view into other useful data streams
- Most of its components are not cloud/SaaS
- Though robust, user interface can be difficult to navigate

RATING SUMMARIES

DEPLOYMENT & ADMINISTRATION: LIMITED	
Deployment Flexibility	Limited
Ease of Administration	Strong
Need for Professional Services	Solid
Licensing Options	Limited

ARCHITECTURE & INTEGRATION: STRONG	
Architecture	Strong
Integration	Outstanding
Trigger-Based Automation	Strong
Data Source Management	Solid
Detection, Identification, and Analysis of Threat Types	Strong

FUNCTIONALITY: OUTSTANDING	
Threat and Risk Identification and Assessment	Outstanding
Digital Threat Management	Strong
Data Management	Outstanding
Feature Differentiation	Strong
Remediation	Strong
Management Console	Strong
Out-of-Box Reporting	Outstanding
Report Flexibility	Outstanding

VENDOR STRENGTH: SOLID	
Vision, Strategy, and Direction	Solid
Financial Strength	$$$$

2017 DTIM RADAR AWARDS

The EMA Radar evaluation process involves a review of many different aspects of platform capabilities and features. During the evaluation process, several reviewed solutions were identified as being worthy of special recognition for specific areas of strength and/or unique areas of innovation. Each of the characteristics discussed in this section contributed significantly to the solutions' overall ratings. The following are the special award winners:

BrandProtect is one of the specialized players in the market. As its name indicates, it focuses on identifying brand infringement for its clients. Its recognition is for its specialized depth in delivering brand infringement protection.

DarkLight received the Vendor to Watch. Its technology is not specific to DTIM, but its architecture allows it to compete in the space, along with a few others involving analytics. It is still a new solution, so it has some growing to do. It ranked solidly and has the distinct possibility of being a key player across what are currently seen as separate technology stacks.

DomainTools was farthest right on the chart and still in the Value Leaders category, so it achieved the greatest Cost Efficiency in the report. Its award is for its Specialized Technology. DomainTools focuses on threats related to domain and similarly-related infringement. Its historical database is the oldest in the DTIM business, allowing clients to see the change in behavior and content for the longest period of time.

IntSights is a small company that delivers big. It just missed the Value Leader category, primarily because of its age. It is the newest entrant in the DTIM field in the report. However, EMA has no doubt that in the next report it will push itself over the line. The management and technical teams have a solid vision of where they want IntSights to go in the marketspace and are consistently delivering to achieve those goals.

2017 DTIM RADAR AWARDS

IBM was identified as a Market Driver in the DTIM space for several reasons. First, it has the largest subscriber base for threat intelligence by a large margin. The X-Force exchange free subscription is 100x bigger than any other player in the space. Additionally, users are signed up and a large majority of those practitioners are actively involved with the platform community, driving information sharing and creating insights that the larger community can benefit from.

LookingGlass is a pioneer in the DTIM industry, delivering its DTIM solutions since 2006. Its vision at the time largely exceeded technology's ability to deliver, and they had to bide time for certain aspects of technology to catch up. Its vision and ability to execute that vison have been excellent. Many of the current companies looked to LookingGlass as the standard to build from.

RiskIQ has been pushing the boundaries of the DTIM market to achieve a well-recognized Technology Leader platform. It developed a premium solution to address a significant problem for larger companies ready or needing to tackle the problems of external threat management.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3640.011218

IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING