EMA Radar™ for Digital Threat Intelligence Management: Q4 2017

DomainTools Profile

An Enterprise Management Associates Radar™ Report

Written by David Monahan

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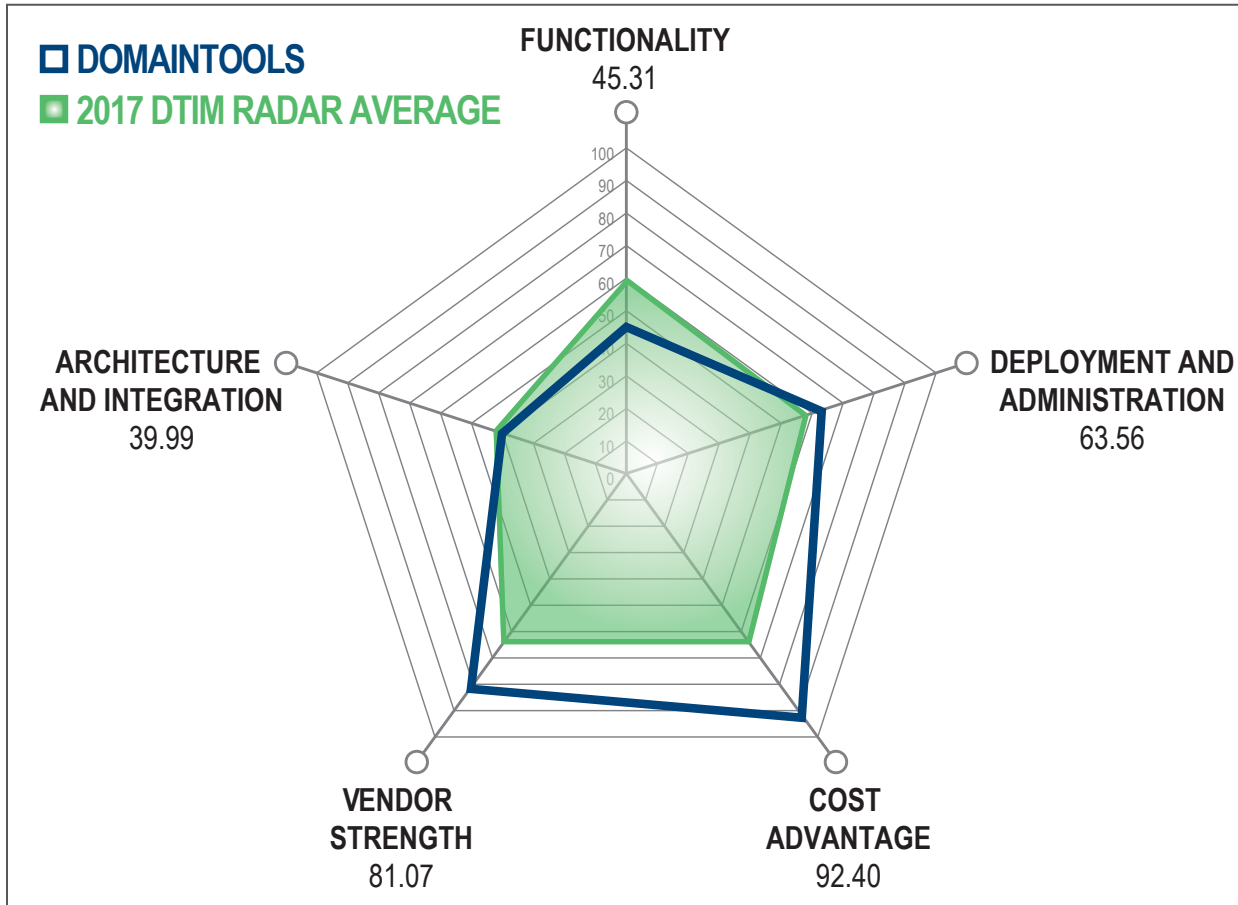
Because DomainTools is focused on threats specifically around DNS, domain, IP, and websites, it is considered more of a niche player. It does not address as wide an array of threats as most of the other vendors; however, it is exceptionally strong at what it does. It has the most detailed and farthest-reaching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

VALUE LEADER: DOMAINTOOLS

RADAR CHART EVALUATION

□ DOMAINTOOLS
■ 2017 DTIM RADAR AVERAGE

FUNCTIONALITY
45.31

DEPLOYMENT AND
ADMINISTRATION
63.56

COST
ADVANTAGE
92.40

VENDOR
STRENGTH
81.07

ARCHITECTURE
AND INTEGRATION
39.99

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

EMA RADAR

VALUE LEADER: DOMAINTOOLS

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.

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-DomainTools.020118

EMA IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING