EMA Radar™ Summary for Network-Based Security Analytics: Q3 2018

An Enterprise Management Associates Radar™ Report

Written by Paula Musich and David Monahan

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity is a fast-paced, dynamic area. Attackers are developing new and innovative attack methods and combining them with older vectors to create nearly infinite methods of attack. Whether an attack is a single packet exploit, a multiphase user compromise, or a low-and-slow attack drawn out over many days, the defenders are responsible for identifying and stopping the attacks as soon as possible. The speed of detection and mitigation are the true issues today. How fast is as fast as possible? Over the last few years, research like the Verizon Data Breach Investigation Report demonstrated that, "as fast as possible" has not been nearly fast enough. Compromises can happen in hours, but identifying an attack may not take place for months or years.

It is this issue that focused innovators on how to identify and respond to security incidents faster. The first challenge is being able to wade through the incessant and overwhelming noise of alerts, and reduce them to a workable volume of real problems that can be clearly defined and addressed quickly.

Over the past several years, numerous startup companies were established to address the gap in analytics and visibility of real issues in the sea of alerts. Security analytics solutions were initially designed to perform one or more of three primary types of security-focused analytics: User and Entity Behavior Analytics (UEBA), Anomaly Detection, and Predictive Analytics. Since their inception, much of these analytics have merged, leaving only a thin line between combined UEBA/ Anomaly Detection and Predictive Analytics.

This report is the second of a two-part series. Part one, released earlier this year, delved into the platforms, solutions, and products supplying log-based security analytics for the express purpose of providing them with fewer actionable alerts without the side effects that can filter out alerts on actual threat activity. This second report focuses on vendors that use network information, such as net flows, deep packet inspection, and forensic packet analysis, to gather telemetry. This report evaluates vendors across five major categories supported by over 120 KPIs. EMA evaluated and scored each vendor under the same documented criteria. Each participating vendor has a profile that outlines their solution, its strengths and weaknesses, and its performance ratings compared to the other vendors evaluated. It also documents key decision-making factors important to the buying process and ultimately depicts the vendors' relationship to each other based on value vs. functionality.

The Foundations of Security Analytics

Anomaly Detection, Predictive Analytics, and UEBA use similar underlying approaches to achieve their end goals of improved visibility into activities and greater accuracy for identifying and prioritizing threats and risk. They are based on new and old algorithms that include supervised, unsupervised, and reinforced machine learning, deep learning, statistical deviation Bayesian analytics, statistical deviations, and other statistical and probability mathematics to create models of unexpected behaviors or unanticipated outcomes. When something occurs that falls outside the model, the algorithms generate an alert and pass it to the relevant operations team. If the report is deemed accurate and actionable, it is handled. If not, the feedback the operations team provides is usually used to adjust the model to be more accurate.

Though out-of-the-box accuracy is generally 80 percent or higher, model accuracy and the outputs are honed through greater data inputs over time and, in many cases, analyst inputs. Thus, the longer the system is used and properly adjusted with new data and user feedback, the more accurate it becomes at identifying expected outliers.

The Evolution of Security Analytics From SIEM

The SIEM market has existed for nearly 20 years. Despite the improvements made in gathering logs into a single repository and creating a single management and operational interface, SIEM has its difficulties. The largest of these ongoing issues has been the inability to analyze and summarize events on its own.

Alert correlation was SIEM's answer to related or chained events, and was a great advancement in alert conglomeration and response. The problem was that correlation depended on knowing what administrators and operators were looking for and creating rules to look for the related events. If they knew what to look for, they could create a strong system and gain a lot of value. It broke down under the ability to draw relationships without the predetermined rules and thresholds. There were so many alerts that people couldn't readily identify the relationships in all of the noise, so "bad" stuff slipped through. On the other extreme, when systems were over-tuned to reduce the noise, the tuning often filtered out some of the important alerts with the noise, once again allowing some "bad" stuff to be missed.

As time went on, the SIEM vendors' promises were falling short. They were not adapting to the need, so other technologists working to solve this problem created a new market called "security analytics." Numerous groups coming from the private sector and government service applied insightful and revolutionary approaches to solving the problem. Most of these solutions providers did not have the legacy baggage the SIEM vendors were carrying, so they could develop their solutions faster. These solutions have been well received and are growing quickly. They created markets like Advanced Breach Detection, which uses security analytics.

Capability Convergence is Driving the Market

EMA sees the security analytics market paralleling the antimalware market. A few years ago, the endpoint detection and response (EDR) and endpoint prevention platform (EPP) markets separated from the antivirus or antimalware markets. However, in the last year, EMA saw market pressures that caused a recombination of these tools. Vendors who once offered solutions or platforms focusing on one are now creating or acquiring and integrating the other solution capabilities into their existing offerings.

EMA expects the same recombination to happen in security analytics. Security analytics evolved out of the SIEM markets' inability to provide true analytics. The smaller, nimbler companies carved out a nice place for themselves delivering enhanced analytics to address the alert fatigue and accuracy problems. However, in 18 to 24 months, the traditional SIEM vendors responded. They have created or acquired the ability to provide better analytics to their solutions to compete with the startups. They also have the ability to process log and network information within their solutions and platforms. This adaptation requires that the smaller companies focused on either log or network analytics to adapt to having both capabilities. This will happen through merger and acquisition activities or through internal development. With this market pressure, technology consumers should see a good change in the next 12-18 months.

CRITERIA FOR SOLUTIONS EVALUATION

Feature Eligibility

Vendors participating in the research were asked to report on capabilities that were publicly available as of January 31, 2018. The primary inclusion criteria were as follows:

- ✓ Does your solution/platform/product use forms of network packet, network flow collection, and analysis of some kind as a primary mode of data ingestion?
- ✓ Does your solution/platform/product provide any means to reduce workloads on security personnel for situations like incident response and investigations?
- ✓ Does your solution/platform/product correlate multiple, seemingly anomalous events into a single security event without rules, policy, thresholds, or other guidance from an analyst/operator/ administrator?
- ✓ Does your solution/platform/product perform threat detection across hybrid IT infrastructures, including both hybrid cloud and hybrid data center environments?
- ✓ Does your solution/platform/product claim to identify previously unknown threats?
- ✓ Does your solution/platform/product provide any of the following: UEBA, Anomaly Detection, or Predictive Analytics?
- ✓ Does your solution/platform/product provide specialized types of visualizations to easily identify threats and/or risks?
- ✓ Does your solution/platform/product offer support for elastic computing to meet demand spikes?

RESEARCH 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 and the mean value across all evaluated vendors. The same is also displayed for each of the five primary categories.

Summary Rankings Descriptions

The profiles also reveal some of the secondary summary values and their ratings based on a five-level scale. In most cases, the values are converted to one of the following, ranked from highest to lowest: Outstanding, Strong, Solid, Limited, and None, listed from most desirable to least desirable. There were several categories that used other rankings. Costs for training and professional services used the rankings Very High, High, Moderate, Minimal, and Very Low, listed from least desirable to most desirable.

INVITED VENDORS AND NOTABLE ABSENCES

There are quite a few vendors that compete in the security analytics space. This Radar only covers those that focus on analysis of security events through network data acquisition. They may or may not collect and analyze information generated by other security systems to create their picture of the monitored environment.

Listed below are vendors that compete in the network-based security analytics space in some manner, but either voiced a decision not to participate or failed to respond to the request to participate. No qualifying organization that wanted to participate and could return the requested information in the project timeframe was denied the opportunity to do so.

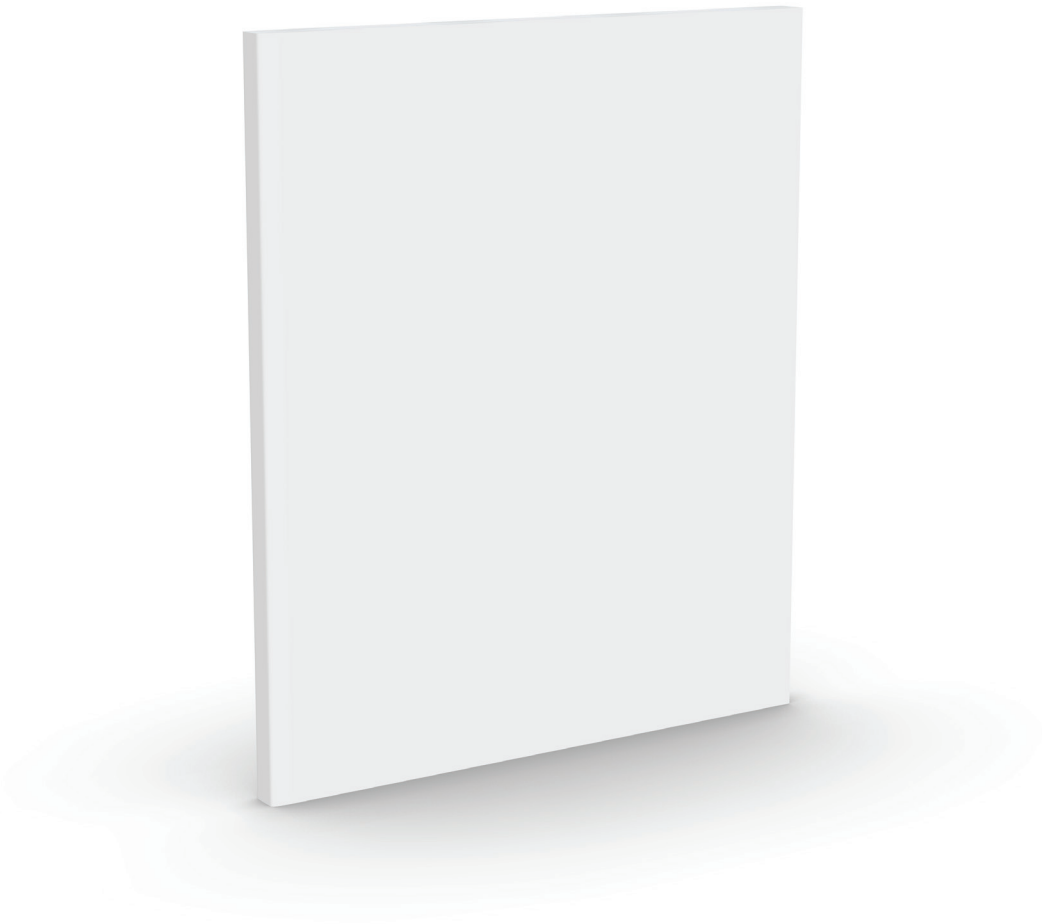
Darktrace did not respond to requests to participate.

FlowTraq was not able to meet requested timelines for data return.

Mantix4 was identified late in the process and was not able to meet requested timelines for data return.

RSA elected not to participate because they were in the middle of a new release and the acquisition of Fortscale, and were not ready to discuss their new features.

LogRythm, QRadar, and Splunk all have analytics capabilities around packets and flows through internal means through partnerships. However, their roots in the log analytics space placed them in the first part of this series, so they were not evaluated in this report.



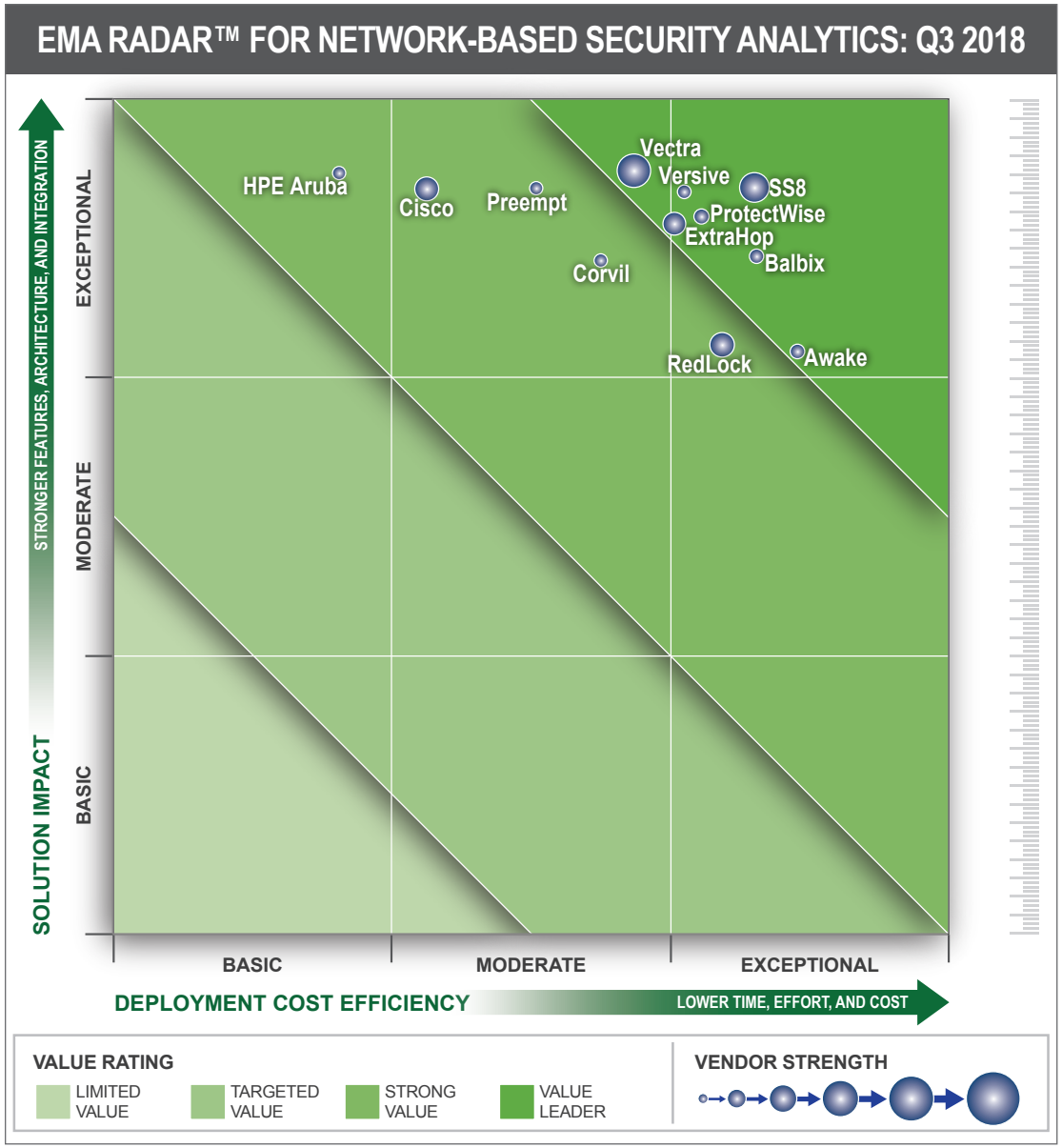


Figure 2: EMA Network-Based Security Analytics Landscape Chart

The EMA Network-Based Security Analytics 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 the market.

In every solution, there are tradeoffs to be made. There are two primary approaches to achieving value leadership. 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 number of use cases in return for commanding premium pricing, thus falling higher on the Y-axis and farther left on the X-axis. The other approach uses the 80/20 rule. This approach means providing somewhere around 80 percent of the features expected to be needed and passing the lower development and maintenance costs on to the customer at a much lower cost, thus landing far to the right on the X-axis and lower on the Y-axis.

Some vendors and consumers have the perception that being in the top right corner is the optimal position. However, that is virtually impossible to attain and though optimal for the consumer, it is not optimal for the vendors. If the solution has maxed out in the features needed for its use, it moves to the top of the Y-axis. If it is also pushing the lowest prices then the consumer gets great value, but the vendor is leaving money on the table because, as a premium solution, it should be demanding a higher price. Given its premium status, the market will bear that higher price. The higher price then moves it to the left on the X-axis. This is highly desirable for the

vendor because it maximizes revenue. However, care must be taken in raising the price. If it inflates too much, the number of prospects willing to accept the increase in price drops, and the solution moves out of optimal revenue. This is represented by an even farther move left on the X-axis and a corresponding transition from a Value Leader to a Strong Value or lower.

For the buyer, having maximum functionality is highly desirable, but so is having lowest cost. This convergence rarely occurs in the real world because with cheap pricing, the company revenue is more limited, meaning R&D investment is limited. With reduced R&D there is a reduced capacity to produce features as quickly as others. The pricing choices the company makes, while possibly maximizing the right position on the X-axis, also limits the vertical positioning on the Y-axis.

Despite its lower cost, if the solution does not maintain the roughly 80 percent level of functionality compared to its competitors as they continue development, it will fall into a lower functionality bracket of the graph, dropping from Value Leader to Strong Value or lower. There is no way it can move up faster on the Y-axis than its competitors without external investment to give it a jump in R&D to increase capacity and comparative feature parity.

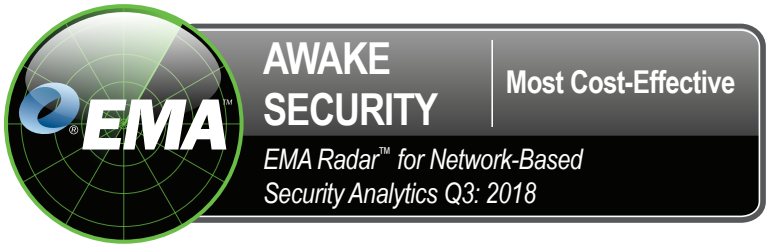
This is why new companies often not only come in at lower prices, but in many cases will provide severely reduced pricing or even free trials to companies designated as “strategic wins.”

In 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 their value range, or be willing to sacrifice features and move to another 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, the vendors in the bottom right corner of the Value Leaders triangle usually maximize profit because even though they have lower pricing, they have a lower development cost for the solution and can attract a sizable customer base.

SPECIAL 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.

Awake Security: Most Cost-Effective



Awake Security delivered a strong product to land in the Value Leader corner. It was also the farthest to the right on the chart. It had the greatest cost-efficiency based on price and features. Some products have many features and charge a premium price. Others deliver a bare bones solution for a rock-bottom price. For organizations that are dabbling and not committed, these are a good try-before-you-buy options. Awake found a solid balance between features and cost for companies that want to move forward, need good features, and are more committed to the endeavor.

OVERVIEW

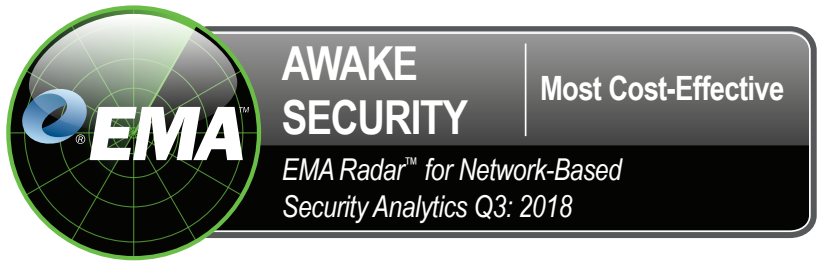
Awake Security is among the newest startups in this evaluation. Although it was founded in 2014, its Network Detection and Response Platform only became available in July 2017, when the company itself came out of stealth mode. Despite its youth, the product reflects significant maturity as a result of the extensive research Awake conducted with hundreds of IT security professionals from over a dozen teams during the product's development, and thanks to the incident response and investigative background of its founders. The company launched with $30 million in venture funding from two veteran cyber security investment firms: Greylock Partners and Bain Capital.

The platform's technology foundation is a three-legged stool that includes the EntityIQ engine, which records and sifts through full packet capture data to extract hundreds of security-relevant data points, and then uses machine learning to correlate, profile, and track entities including devices, users, applications, and domains. The platform also includes the QueryIQ behavioral query language, which can spot anomalous patterns and behaviors by interrogating graph, structured, and raw packet capture data; and DetectIQ libraries of attacker tactics, techniques, and procedures that Awake continually updates.

Thanks to the flexibility of the query language built into the tool and the greater context it brings to investigations, EntityIQ can significantly reduce the time it takes to triage a potential infection from hours or even days down to minutes. Its Security Knowledge Graph data model helps speed investigations because it uses machine learning to predict the questions human operators will ask, and then maintains the answers in a user workflow-oriented user interface. Its workflow design emphasizes groups and entities that exhibit anomalous behavior, allowing analysts to focus their investigations on behaviors and entity profiles, not indicators of compromise. Typical use cases include corporate espionage, insider threats, lateral movement, and data exfiltration.

In this analysis, the strongest attribute for Awake's Security Investigation Platform is its outstanding cost value, thanks largely to their aggressive pricing structure that takes into account the architecture and bandwidth of the protected network. At the same time, Awake received an outstanding rating for its value, based on the fast time to ROI and value demonstrated by the product, as well as the platform's ability to automate much of the often-mundane tasks in investigation and response workflows. Awake is unique among security analytics startups for its comprehensive customer support, which it offers internally.

The platform lacks maturity in its ability to integrate and share information. Although it integrates with a handful of third-party security products, it was the only product in this assessment that scored a limited rating for such integration. It was also unique in its comparatively limited threat mitigation capabilities, both native and through third-party integration.



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 blog.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

3752-AwakeSecurity-Profile.072518