SECURITY ANALYTICS FOR THREAT DETECTION AND BREACH RESOLUTION IN 2019

EMA Top 3 Report and Decision Guide
Focus Vendor: ExtraHop

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) REPORT
WRITTEN BY DAVID MONAHAN

Q1 2019

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

CONTENTS

INTRODUCTION

Understanding Security Analytics

The need for better analysis at the front of an incident inspired the creation of security analytics. Over the past five to seven years, lag times in identifying and remediating threats created not only dissatisfaction with the commercially available systems, but also stemmed significant creativity. Much of the advancements evolved from applying the concepts that have been driving advancements in business processes and IT analytics for a significantly longer period of time. Both the algorithms and the models had to be adjusted to form security analytics.

Security analytics were created to provide advanced data analysis using multiple analysis techniques, the most popular of which is a class of adaptive outcome algorithms called machine learning (ML), also now being dubbed artificial intelligence (AI). These algorithms and models supply individual and community behavioral analysis combined with protocol, packet stream, and big data interrogation and risk profiling techniques. Combined, they identify, prioritize, and aid in containing threat actors.

To deliver increased detection and accelerated response and containment, security analytics can ingest data from packet streams and flows, perimeter defense, authentication, application, endpoints, and any other of the myriad of IT and security technologies. Security analytics also interface with other monitoring and alerting systems, like security incident and event management systems (SIEM). This data, along with the good algorithms and the proper application thereof, can produce extremely high-fidelity intelligence for rendering the context of an event, provide a previously unobtained level of visibility into activities in the environment, and supply excellent prioritization of incidents.

EMA TOP 3:
EMA PRESENTS ITS TOP 3 AWARD TO VENDORS THAT ARE BEST ALIGNED WITH TODAY'S CUSTOMER PRIORITIES AND PAIN POINTS

Each vendor uses publicly available ML and has its own intellectual property and proprietary approach that, when combined, create a unique solution. The combination of their integrations for data collection, the back-office analysis approach, and the user interface make each product different, thus making it imperative for each organization to understand their requirements and discuss them with prospective vendors prior to purchasing a solution of this type.

A crucial aspect of this whole genre is that these technologies look for patterns and anomalies within those patterns. Not all anomalies are bad and not all seemingly normal actives are good. That is why the quality and volume of data and the means of modeling and analysis are so crucial. Each environment has different systems that provide the data, and each vendor has different ways of analyzing that data, so different vendors may perform with somewhat different degrees of efficacy between those dissimilar environments.

Security analytics tools are not a silver bullet. Though they all create a myriad of metadata to aid analysis, all of them also rely on other technologies to provide them with relevant source data for that analysis. If an organization is missing the technologies that provide that source data, tools silos, or a pathway to get that data to the analytics engine and data silos, then security analytics will be hampered and simultaneously provide a false sense of security.

Security Analytics and SIEM

SIEM evolved over twenty years. Some people felt it was unable to adapt, which is why disruptive technologies that are now labeled as security analytics burst onto the scene.

Some of the vendors that provide security analytics are trying to take over the role of the central interface for security operations, thus also identifying as SIEM 2.0 or Next-Gen SIEM. At the same time, some of the traditional SIEM vendors have been working diligently to incorporate ML/AI and new models into their SIEM technology to provide equal capability and defend their market share. Many of the traditional SIEM vendors did very well in addressing use cases, and many of the new vendors did as well. Given this, setting aside preconceived notions and biases is important for identifying the best tool for the organization.

INTRODUCTION

Why You Should Read This Research Report

This report is a time-saving guide. It is designed to help decision-makers who have identified problematic security use cases to select analytics tools that best address those use cases to aid in narrowing selection choices for proof of concept testing or other interviews.

If the security team has invested in the proper tools and still is not able to render a solid defense, and reaches a point where they have been able to break down data silos and address the political silos that impede information flow and cooperation, then this report can aid in choosing a vendor to take the security practice to the next level.

Evaluation Methodology

This report comes from hundreds of man hours of data collection and review based on vendor interviews, product demos, customer interviews, and documentation review.

It is also important to note that while these vendors all provide security analytics, many of them compete in different solution spaces, so not all use cases are applicable to all vendors and therefore not all vendors were evaluated against all use cases.

Evaluated Vendors

Awake	Huntsman Security	SecBI
Balbix	IBM QRadar	Seceon
Barac	IronNet	Securonix
Bay Dynamics	Lastline	Splunk Phantom
Corvil	LogRhythm	SS8
Dtex	Mantix4	STEALTHbits
empow	ObserveIT	Sumo Logic
ExtraHop	Preempt	Teramind
Gigamon	ProtectWise	Vectra
Gurucul	Palo Alto Networks (RedLock)	Versive
HPE Niara	RSA	

About the Use Cases

The use cases in the report were gathered from management and frontline security professionals of current customers, non-customers, and vendors. Current customers and non-customers indicated their perceived needs from analytics, while the customers also provided details on use cases that they discovered they could address once they started using their chosen solution. Vendors provided insights on advanced use cases they address. Over sixty use cases were identified, with just over 40 published in the report.

The evaluated solutions focus on security analytics in different ways. The approaches to data collection and the types of data they collect affect not only the applicability, but the efficacy of the solutions in the various use cases. Given this variance, it is conceivable that more than one solution meets the organization's needs or that given a wide breadth of needs, multiple solutions could be warranted.

WHAT ARE THE EMA TOP 3 REPORTS?

EMA Top 3 reports identify the leading priorities organizations face with resolving challenges and meeting enterprise requirements in particular IT management focus areas. The intent of this report is to inform and inspire influencers and decision makers in their project planning and vendor selection process.

While EMA internally conducted a detailed analysis of solutions that help support the identified IT management priorities, this report is not designed to provide a feature-by-feature comparison. In certain cases, EMA recognized products for their innovative approach rather than their ability to meet a predetermined checklist of features. Additionally, some popularly adopted approaches may not be represented in this report because EMA's analysis did not indicate that they fully address emerging market requirements. This guide was developed as a resource for organizations to gain insights from EMA's extensive experience conducting hundreds of product briefings, case studies, and demonstrations.

Solution Qualifications

In order for a product to be considered for recognition as an EMA Top 3 secure access enablement solution, all evaluated features and capabilities were required to conform to the following rules:

- Reported features must be generally available on or before December 1, 2018. Features that are in beta testing or are scheduled for inclusion in later releases do not qualify.
- Reported features must be self-contained within the included package sets. Any features that are not natively included in the evaluated package sets, but available separately from the same vendor or a third-party vendor, do not qualify (except where explicitly noted as points of integration).
- Reported features must be either clearly documented in publicly-available resources (such as user manuals or technical papers) or be demonstrative to confirm their existence and ensure they are officially supported.

How to Use This Document

It is important to recognize that every organization is different, with a unique set of IT and business requirements. As such, EMA strongly recommends that when using this guide to create a shortlist, each organization conduct its own evaluation to confirm that other aspects of the solutions will best match its business needs or that the disclosed use cases also meet other requirements, like business workflows and full reporting necessities. This guide will assist with the process by providing information on key use cases common to many prospective buyers to review during the selection process, and an associated shortlist of vendors with solutions that meet them.

For each use case, EMA provides the following sections offering insights for use in the platform selection process:

- **Quick Take** – This is an overview of the use case, why it is important, and how the solutions address it.
- **Buyer's Note** – Key considerations prospective buyers should be aware of, and questions they should ask during the evaluation process.
- **Top 3 Solution Providers** – By identifying and recognizing the most innovative vendor solutions that address the greatest business priorities for secure access enablement, the table in this section provides a brief overview of each platform and the respective capabilities. Within the Top 3, the solutions are listed alphabetically by vendor, so the order in which they appear is not an indication of EMA's preference. It is highly recommended that organizations seeking to adopt solutions addressing a particular priority investigate each of the corresponding Top 3 vendors to determine which best meet their full and unique requirements.

USE CASE: ASSET INVENTORY/CLASSIFICATION

Note: Solution providers are listed alphabetically without other preference assigned.

ExtraHop

During asset discovery, in any given organization there are at least **25%** more assets connected to the network than are cataloged.

ForeScout Technologies research

QUICK TAKE

Virtually every environment has more assets on the network than they have accounted for in their asset databases or network diagrams. IT and business personnel are constantly adding and removing end-user devices and new systems to support business needs. Virtual computing and cloud, with pressures from shadow IT and agile delivery models, have exacerbated this problem.

Accurately identifying everything that is connected to the infrastructure should be a critical concern since each application and system is part of the potential attack surface that can be leveraged as a beachhead for incursion or data exfiltration.

BUYER'S NOTE

There are numerous specialized systems that provide asset inventory or classification services, such as CMDB and NAC tools. Identifying a security analytics tool that will double up to provide this feature can deliver cost avoidance by alleviating the need for the adoption of a separate system or a cost reduction. It does this by allowing the discontinuation of the purpose-built solution. Do a thorough analysis of the business requirements to determine the features used within the organization now and those that may be needed in the next three to five years prior to discontinuing an existing solution.

USE CASE: EARLY BREACH DETECTION

Note: Solution providers are listed alphabetically without other preference assigned.

ExtraHop

197 days is the mean time to identify a breach.

Identifying a breach in <100 days **saves > $1 million** compared to those taking >100 days.

IBM/Ponemon 2018 "Cost of a Data Breach" Report

QUICK TAKE

One of the foundational goals of security analytics solutions is early breach detection. Depending on the attack vector used to achieve that end, the breach may start on an endpoint and expand outwardly, or it may start with network communications and be directed inward to create a landing point. Except for one scenario where an insider logs on to a local station, extracts data from only that station's local disk, loads it on to removable storage, and walks away, all infiltrations and data extractions touch the network at some point. If the incursion starts from a malicious download or other remotely triggered event, the network has the opportunity to see the attack's earliest stages. Depending on the circumstances, it may not see the full details of the landing and host compromise, but it can see the incursion, reconnaissance, lateral movement, data aggregation, and ultimately data exfiltration. This was a major factor in the final outcome of the choices for the top three solutions for early breach detection.

BUYER'S NOTE

Whether choosing a system or a network-focused system, the placement and maintenance of detections are paramount for early detection. Many organizations make the mistake of placing network detections only at the gateway. Cost and a flawed perception that detection at the gateway is sufficient drive this mistake. While budgets are an internal matter out of scope for this report, the perception that gateway detection is enough, is in scope.

Failure to place detections at all differing zones of trust and between all major intersections leaves the organization with considerable blind spots, thus vulnerable to attack. Take careful thought on placement of network sensors and endpoint sensors to avoid creating blind spots that allow for undetected lateral movement and data aggregation. If the attack is brought inside the perimeter by a system that was compromised externally, or initiated from a malicious insider and monitoring is only performed at the gateway, sophisticated and automated or well-planned attacks may be able to compromise considerable portions of the internal network before making a signal through the gateway.

USE CASE: ENCRYPTED TRAFFIC ANALYSIS

Note: Solution providers are listed alphabetically without other preference assigned.

ExtraHop

80% of U.S. Internet traffic is now encrypted. This is a >2x increase over 18 months ago.

Symantec Internet security threat report

QUICK TAKE

This is one of the most difficult areas for analysis. With current browsers and secure remote connection technology using AES256 or AES512 as their standard encryption, there is little hope of being able to crack open packets without proper authorization. The authorization may not be available due to privacy concerns, regulations, or fear that intercepting and opening encrypted traffic will put too much strain on latency-intolerant applications.

Vendors that attempt to analyze encrypted packets and produce intelligent results have chosen a hard road. Without the payload contents, they have to rely on the source and destination addresses, metadata they can glean, and the strength of their algorithms. This is a significant challenge, but one that a number of vendors have taken head on.

Being able to get a high degree of confidence in the analysis at high-line speeds without impacting traffic latency is a boon for security and ITOps, keeping the two from being at odds, as they often seem to be.

BUYER'S NOTE

Those interested in this use case should ask the prospective vendors to supply customer references that will hold a candid conversation about their perspectives on accuracy, efficacy, and overall value for their security program. Even with that, skeptical buyers may want to prove this approach with a proof of concept test. Vendors asked to provide sample products for POCs will most likely ask for written outcome expectations or success criteria to participate. This is only fair if they have to put in man hours to support the testing.

USE CASE: FORENSIC ANALYSIS LEVERAGING PACKET STREAMS

Note: Solution providers are listed alphabetically without other preference assigned.

ExtraHop

71% of organizations stated that they thought using network traffic content, such as flows and packets, was very valuable to extremely valuable in forensic investigations.

EMA "Data-Driven Security Unleashed" research

QUICK TAKE

Forensics are a huge cost in mega breaches, such as Target, Anthem, etc. Specialists are paid by the hour to gather and organize information to tell the story of the scope and duration of the incident. The post-incident forensics can take months and may never be truly complete due to a lack of data because of blind spots in coverage or a failure to retain the necessary information long enough. Solutions in this Top 3 use case are addressing the use of live or stored network packets to identify the source and scope of an incident or breach. Since most attacks traverse the network in some manner, packets are very useful in this endeavor. However, they can take up a large amount of storage for a relatively short period of time compared to logs. There are tools like Wireshark that can collect live packets and open packet capture files for investigation. While they have filtering and some other basic tools, they provide little in the way of analysis capabilities and rely on the analyst for expertise in discerning what happened. Improved analytics within forensics reduce the analyst's workload by providing a better way to collect, store, and organize information. By processing packets as they are received with the goal of supporting forensics, the information is ready when and how analysts need it.

BUYER'S NOTE

With packet analysis of any kind, the largest concern is meeting the line speed requirements of the environment in order to be able to analyze the packets and to avoid introducing any latency into network transmissions. The analytics dissect every aspect of the packet and the protocols passing it to create valuable metadata. Those investigating forensic packet stream analytics should delve into the metadata that is created and used, since there is some differentiation in this area.

Aside from how the vendors process, organize, and present information, it is incumbent on the buyer to properly scope storage requirements for the information they want to provide in the forensic process. If data is removed or not captured, forensics can be impossible. Buyers must make a conscious choice of how much data they want to store in order to maintain forensic readiness. While there is no reason to maintain data for the sake of data, maintaining several months of historical information is a necessary part of forensic preparedness.

USE CASE: IDENTIFYING NETWORK PROTOCOL MISUSE/ABUSE

Note: Solution providers are listed alphabetically without other preference assigned.

ExtraHop

81% of major APT campaigns hide their command and control (C2) in common web ports.

Trend Micro infographic, "Connecting the APT Dots"

QUICK TAKE

To perform effectively on this use case, it is highly advantageous for the analytics system to be at least somewhat aware of OSI network layers three through seven. If it does not or cannot understand how a standard IP transport protocol, a custom Internet protocol, or application protocol is supposed to operate, there is no way for it to identify that something is amiss.

The data hidden with the transmission employing this type of technique would be analogous to a network protocol steganography. To attempt this type of attack, attackers can use protocol tunneling or other methods to try to fool perimeter and internal firewalls and other detection solutions into allowing or otherwise ignoring the communication stream because it looks benign. In reality, the attacker is hiding the actual nature of a communication.

This approach began gaining popularity in the last ten years or so, but recently hit a plateau as attackers began moving to more TLS. A popular attack method is to tunnel communication through common network communications ports like HTTP or DNS. These ports are commonly allowed through firewalls and other perimeter security devices because they provide business-critical functions. While unsuspecting monitoring devices believe the traffic is HTTP or DNS traffic, it is actually something else. The attacker is misusing the protocol because ports 80 and 53 that should be communicating HTTP and DNS, respectively, are actually being used to communicate in a different manner.

BUYER'S NOTE

In most environments, this may not be seen as a primary use case. However, ignoring it would be a mistake if the organization does not have a full application layer proxy in place.

USE CASE: RANSOMWARE DETECTION

Note: Solution providers are listed alphabetically without other preference assigned.

ExtraHop

51% of data breaches involved the use of malware.

350% increase in ransomware attacks from 2016-2017 (2018 numbers were not available).

2018 Verizon DBIR and NTT Security 2018 Global Threat Intelligence Report

QUICK TAKE

Today, ransomware is a serious problem for organizations of all sizes. Once an infection is activated, every second counts when trying to detect it. Solutions in this use case are adept at detecting the characteristics common to many types of malware not by signature, but by behavior. Though aspects of how actions are performed may vary, ransomware variants share characteristics in the way they perform reconnaissance and encrypt files. Many of these characteristics are patterned in the machine learning detection models. Remember, these are not signatures or rules. They are more like methodologies for behaviors. Characteristics of behavior are identified as the ransomware steps out to do its thing. These characteristics are combined with currently known and established behavioral models for the normal operating environment watching for unusual communications.

BUYER'S NOTE

First, buyers must understand that ransomware has certain operating characteristics that are unique from other malware. This use case is not a blanket statement that security analytics is an early detection mechanism for all malware. At the current time, EMA does not recommend using security analytics as a standalone replacement for endpoint defense against malware or ransomware in which a current antimalware solution can be deployed. It is a secondary detection mechanism or failsafe defense. That said, it is extremely useful for detecting ransomware activity in environments where endpoint agents cannot be deployed. These systems include facilities where there are medical devices, manufacturing systems, SCADA systems, and other OT-, IIoT-, and IoT-rich environments. The systems can aid in early detection to stop the spread of ransomware to other devices and data repositories in the network vicinity of the infected system, but host zero could still suffer significant losses.

Lastline has a rich history in broader malware detection capabilities, which further bolsters its ability in this use case. Lastline analysis expands to analyze inbound files and URLs in a sandbox as they enter the environment, exposing all of the intended behaviors to blocking the ransomware from taking root in the first place (this is not endpoint protection). Stopping ransomware involves both a sandbox and network behavioral analysis.

VENDOR PROFILE: EXTRAHOP

ExtraHop has a long history in the network and application performance management markets, but its formal history in the network-based security analytics market dates back only to January 2018. The company officially launched its Reveal(x) purpose-built security analytics solution based on its technology, which can monitor and analyze detailed network activity. The fast-growing, privately-held company counts a number of blue chip companies among its customer base, including Lockheed Martin, Credit Suisse, Caesars Entertainment, and Liberty Global. ExtraHop is backed by venture capital firms to the tune of $61.6 million, including a $41 million Series C round in 2014 designed to help bring ExtraHop into new markets.

Reveal(x) is the culmination of a multiyear effort to exploit the unique insights extracted from wire data to detect behavioral anomalies. Its machine learning models take advantage of thousands of features from network traffic, including endpoint activities on the wire, to detect threat behavior. It automatically correlates related indicators of compromise and presents them with contextual details and visualizations that enable security analysts to validate, investigate, and resolve incidents faster. Reveal(x) also automatically discovers, classifies, and prioritizes any device, client, or application traversing the network. Discovery and classification extend to encrypted traffic, thanks to ExtraHop's passive SSL and TLS decryption, which supports perfect forward secrecy ciphers. Reveal(x) exhibited strong functionality due to its impressive feature differentiation, out-of-box reporting, and high-performance sustained data capture and processing (which was the highest of all competitors in this analysis).

Reveal(x) also benefits from an extensive network of existing channel partners, who can resell the security analytics product. In that particular metric, ExtraHop rivaled Cisco, which is no small feat for a comparatively small, privately-held company. Flexible pricing models and fairly aggressive volume discounts give Reveal(x) a strong cost advantage.

Downsides to the security analytics product are the amount of time it takes to train its machine learning models to meet advertised accuracy levels and the requirement to obtain network traffic, usually with the cooperation of the network operations team. This last point has been made easier by several Reveal(x) customers that allow the network operations team to use the product for performance troubleshooting as well. It is important to note that this evaluation was compiled based on ExtraHop's product version from early 2018, which has been updated. Additionally, this is a new product line for ExtraHop. Scoring as highly as it did with a new solution in a new space is very uncommon and says a lot for ExtraHop.

CONCLUSION

Security analytics tools are a significant strategic and tactical investment. They are significant both from the potential costs and from the potential benefits. The ability to identify a myriad of threats earlier in the attack process is a crucial part of the security arsenal. Each of the tools listed in this report can provide a great deal of value for the organization provided it is adopted while evaluating the larger picture. Below are the top considerations when investigating a security analytics tool:

1. Identify the use cases most pertinent to your organization, both presently and for the next 3-5 years.
2. Evaluate current workflow processes and the tool's ability to adjust to work within those processes or the organization's ability to adapt to the tool, whichever is more appropriate.
3. Consider the organization's ability to collect and centralize the necessary data so the tool can do its job.
4. Asses the ability to retain the necessary data for a sufficient length of time if forensics is part of the operations plan.

While there is no security silver bullet, security analytics is a great step forward for any organization to improve its ability to detect threats. When purchased without the proper research, these tools can create unnecessary overhead and actually impede performance by creating a false sense of security. However, security analytics is the perfect operational example of prior planning averting negative performance. When the proper tool is selected, customers will see great benefits.

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.

Please follow EMA on:

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

3796-ExtraHop.020319