

# SECURITY ANALYTICS FOR THREAT DETECTION AND BREACH RESOLUTION IN 2019



EMA Top 3 Report and Decision Guide  
Focus Vendor: Gigamon

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

Q1 2019



IT AND DATA MANAGEMENT  
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

# CONTENTS

Introduction.....1

What are the EMA Top 3 Reports? .....3

Use Case: Enhancing Incident Investigation .....4

Use Case: Identifying Advanced Threats .....5

Conclusion.....6

Vendor Profile: Gigamon .....7



# 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.

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 activities 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.

## EMA TOP 3:

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



# 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
Gurukul	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.

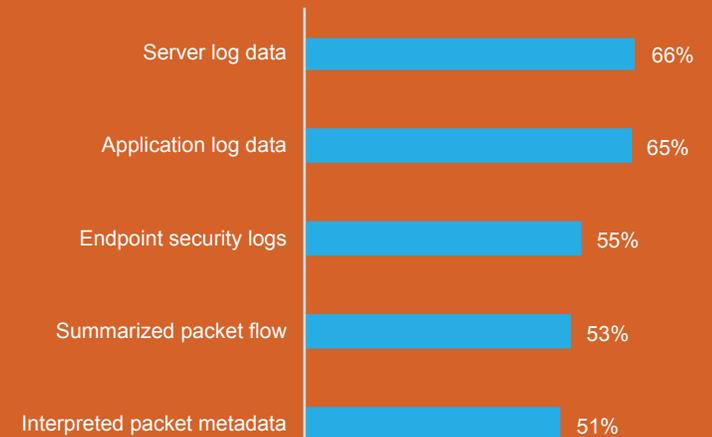
# USE CASE: ENHANCING INCIDENT INVESTIGATION



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

## Gigamon

### Top five most common inputs to security analytics



*EMA "Data-Driven Security Unleashed" research*

## QUICK TAKE

Investigations are a reaction to a detected incident. Once an alert is made on an activity, analysts go to work to gather more information. Solutions in this use case must have access to and be able to utilize a broad array of data, provide increased automated data assimilation for the identified incident, and provide strong data presentation and interaction capabilities. The last part is somewhat subjective because different people process information differently, so the presentation is not one-size-fits-all.

## BUYER'S NOTE

Research shows that packet and flow data are underutilized for investigations. Fast information gathering and increased investigation speed will reduce impacts and costs, so there is an ROI discussion that can be made for this area. This is another use case that is subject to perception so not only a demo, but also a test drive, are in order. Ensure that the user interface meets with the approval of the people who will be using it.

# USE CASE: IDENTIFYING ADVANCED THREATS



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

## Gigamon

**53%** of organizations stated that they have not established comprehensive baselines to understand whether they are in a state in which they can identify threats in their environment.

EMA "Data-Driven Security Unleashed" research

### QUICK TAKE

“Advanced threats” is a term thrown around far too often to incite fear, uncertainty, and doubt (FUD), which is problematic because FUD sells products. Most attacks are executed using advanced threats. Advanced threats are simply those that are better designed to hide, disguise themselves, and execute in a stealthy manner. They leave as little a footprint on the systems as possible and layer additional protections to obfuscate their network presence.

In their first phase, advanced threats are most often targeted at specific marks requiring a large amount of research to construct and test. This requires a significant amount of time and money to initially develop, and therefore nation states and cybercrime syndicates with significant resources most often develop and deploy advanced threats. The latter often act as hired guns for the highest bidder.

In general, identifying threats is not difficult for any of the numerous security analytics solutions evaluated in the report, since all of the solutions are based on the same pool of machine learning algorithms. However, each uses their own specialized intellectual property they have applied to their solution to achieve their final results. It is the development and application of the intellectual property combined with the common foundation that creates the unique analytics engines that are each more suited to different collections of use cases.

### BUYER'S NOTE

It cannot be stressed enough that detection of advanced threats has everything to do with the data becoming available to the engine for analysis.

Gigamon is specifically designed to get the right data to the right places at the right time.

# 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. Assess 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.

# VENDOR PROFILE: GIGAMON

Security operations teams face tremendous challenges in combating cyberattacks due to the compounding complexity of managing and securing infrastructure. As networks get faster, become more distributed, and carry more data across physical data centers and the public cloud, their attack surfaces—and therefore risks—increase.

Gigamon is changing the game on how SecOps and NetOps see and contextualize traffic across physical, virtual, and cloud networks. Gigamon solutions reduce complexity and costs to support business and innovation needs while reducing risk by delivering powerful visibility and insights into the organization's network-based activities.

The Gigamon next-generation approach to security is keeping pace with the rapidly-evolving threat landscape to provide pervasive visibility across the entire connected ecosystem. Gigamon simplifies the security architecture to better protect the organization by shifting control and the advantage away from attackers and back to the defender. A key part of this approach involves [Gigamon Insight](#), a SaaS-based network detection and response (NDR) solution built for rapid detection, investigation, and threat hunting, combined with their [Applied Threat Research](#) team. According to one customer, Insight provides them with a single source of truth with rich contextual data to better understand what is happening in their network, and helps them deliver a mean time to detection that is five times faster than previous solutions.

Gigamon has been a recognized leader in network visibility solutions for years, delivering the powerful insights needed to see, secure, and empower enterprise NetOps and SecOps. Its solutions accelerate threat detection and incident response by funneling the right data to the right tools as it is available, empowering customers to maximize their infrastructure performance.

Since 2004, Gigamon has cultivated a customer base that includes more than 80 percent of the Fortune 100, leading service providers, and over 2,800 NetOps and SecOps teams globally.

For the full story on how Gigamon can help reduce risk, complexity, and cost to meet your business needs, visit its [website](#), follow their [blog](#), and connect with the company on [Twitter](#), [LinkedIn](#), and [Facebook](#).



# Gigamon®

## 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](http://www.enterprisemanagement.com) or [blog.enterprisemanagement.com](http://blog.enterprisemanagement.com).

Please follow EMA on:



This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2019 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

### Corporate Headquarters:

1995 North 57th Court, Suite 120

Boulder, CO 80301

Phone: +1 303.543.9500

Fax: +1 303.543.7687

[www.enterprisemanagement.com](http://www.enterprisemanagement.com)

3796-Gigamon.011619