The Insider's Guide to Evaluating Security Incident and Event Management Appliances

DCIG

2014-15 SIEM APPLIANCE BUYER'S GUIDE

By Evan Francen and Jerome Wendt

FRSECURE
Information Security Experts

DCIG

2014-15 SIEM APPLIANCE BUYER'S GUIDE

The Insider's Guide to Evaluating Security Incident and Event Management Appliances

Table of Contents

© 2014 DCIG, LLC. All rights reserved.

Introduction

Technology is a major driving force in the march forward of progress. As it continues this advance, it constantly evolves to push the boundaries of where and how it is used. While technology's expansion is generally viewed as positive, its expansion also exposes security holes and weaknesses that hostile third parties probe and look to exploit.

Large companies regularly issue warnings to customers that critical information may have been compromised. Last year saw several seemingly secure companies breached. This included even the Federal Reserve which exposed the personal data of 4,000 bank executive.[1] When these events occur, it can take organizations several days, weeks or even longer to discover the breach and what data was compromised and much longer to sort out who is responsible.

Security Information and Event Management *(SIEM)* appliances provide a fix to this problem by acting as a watchdog as it tails intruders and immediately alerts administrators of any suspicious activity. In short, these appliances give security administrators visibility into what is going on in their environment.

Frost and Sullivan's Network Security Research and Consulting practice forecasts that sales of the SIEM appliance market will hit $1.3 billion by 2014 though this estimate may be low.[2] While many larger organizations already use SIEM solutions, smaller organizations have been slower to adopt them due to the price of these solutions, the commitment required to implement such a solution and their lack of understanding about the SIEM appli

The *DCIG 2014-15 SIEM Appliance Buyer's Guide* focuses solely on SIEM solutions that are available as appliances that include both the hardware and software needed to deploy them. That said, SIEM appliances are still anything but *"plug and play."* They can require significant investments, time and expertise to properly and successfully deploy them into a business. While appliances certainly help to expedite their installation and deployment, organizations still face an uphill battle in understanding and sorting through the options available to them and then choosing the right product for them

This Buyer's Guide does the heavy lifting that IT organizations normally would have to perform in order to understand the vendor landscape and the scope of available solutions. By using this Buyer's Guide, IT organizations can immediately understand what features and functions are available so they can move more quickly to making a buying decision. This Buyer's Guide lists those solutions from which DCIG could reliably obtain information, the features that are supported on each product, weights those features and then scores and ranks each SIEM solution.

We hope this Buyer's Guide serves its intended purposes in your environment.

Evan and Jerome

1. SC Magazine, "Top five data breaches in 2013...so far." http://www.scmagazine.com/top-five-data-breaches-in-2013so-far/slideshow/1387/#4
2. Frost & Sullivan. "Marketwired." Marketwire. Marketwire, L.P., 14 Mar. 2011. Web. 27 Mar. 2014. http://www.marketwired.com/press-release/Frost-Sullivan-Greater-Sophistication-Cyber-Crimes-Encourages-Adoption-Security-Information-1410638.htm.

© 2014 DCIG, LLC. All rights reserved.

Executive Summary

Data security is a part of the IT infrastructure that should take care of itself. Companies have enough to worry about without always looking over their shoulder to make sure no one is stealing vital information.

As most organizations recognize, this is ***NOT*** the case. Security specialists are never without work for the simple reason that almost every day a headline reads *"International Company [you fill in the blank] Suffers Massive Data Breach."* Read deeper into those articles and a company representative is often quoted as saying something akin to, *"The breach happened a couple days ago and we just caught it. We're still trying to figure out how many of our customers were affected and who is responsible."*

The truth of the matter is that data security does not take care of itself. But Security Information and Event Management (SIEM) solutions take the edge off of these concerns by acting as a constant watchdog that performs several services:

- Logging information
- Correlating data
- Alerting security administrators as soon as a breach is detected
- Providing a dashboard to provide a picture of what is happening in the environment at any given time

Simply put, SIEM solutions gives organizations visibility into their security posture by providing usable and actionable information.

Large enterprise organizations are leading the charge into the adoption of SIEM appliances. Many of these organizations implemented SIEM solutions in large part due to their size and to meet internal and external compliance requirements but a growing number of smaller organizations are adopting these solutions due the sensitive information they handle.

The U.S. Commerce Department's National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity in early 2014. It outlined five (5) ways organizations with critical systems could protect themselves and their data from a cyberattack.[1] The five areas that this Framework outlined included:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Without an SIEM solution, step 3 or detection is nearly impossible. Without detection, response and recovery are entirely impossible.

The hard truth is that it is impossible to prevent all breaches. The next best thing to all-out prevention is a good protection system and a planned, swift course of action in the case of

1. NIST, "NIST Releases Cybersecurity Framework Version 1.0." 12 February 2014. http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

© 2014 DCIG, LLC. All rights reserved.

Executive Summary (continued)

a breach. SIEM solutions play a large role in quickly detecting breaches and many can be customized to provide immediate responses upon detection of a breach.

SIEM solutions do not prevent breaches. They are not force fields. They do not attack intruders. Rather they provide immediate, real-time alerts to security administrators and the organizations for which they work. In addition, they provide a tangible, measurable picture of where a company stands in the once-vague area of data security.

Organizations often cling to illusions of security with no hard data to back up their perceptions. Only when its clients ask for security assurances and proof that their data is secure that these illusions are exposed. Yet it is not entirely the organization's fault as no one has created a standard unit of measurement that they can use to illustrate their company is doing everything it can to provide the maximum level of protection or to detect breaches or threats as they occur.

SIEM solutions and the dashboards they offer put a big dent in addressing that problem. When a breach is detected, an administrator can pull up a dashboard that breaks down every user session that has taken place by login name, location, applications launched, and more. Using these dashboards, the security administrator can make short work of finding those responsible.

This information is presented in easily accessible charts and lists that can be used for personal protection and also for forensic investigations should the need arise. Further, they may be shown to potential customers worried about security and who want proof that the company is doing everything it can to protect and secure their data.

Every SIEM appliance contained in the *DCIG 2014-15 SIEM Appliance Buyer's Guide* performs the following primary functions:

1. Data and log aggregation
2. Data correlation
3. Alerting
4. Dashboarding
5. Log and data retention and protection.

Many also perform three (3) secondary functions:

1. Forensic analysis on the information
2. Serve as an incident management tool
3. Perform compliance monitoring

It is important that prospective buyers keep in mind their organization's security requirements as they look to acquire one of these SIEM appliances. What might be the best SIEM solution for a large, international company might be too robust for a smaller organization. A company must be aware of its own security needs before investing time and money in an SIEM solution.

The *DCIG 2014-15 SIEM Appliance Buyer's Guide* is designed to shorten the time needed in the product research phase. DCIG invested hundreds of hours designing a survey that would

© 2014 DCIG, LLC. All rights reserved.

Executive Summary (continued)

capture the data that matters most to prospective SIEM appliance purchasers by gathering the relevant data associated with each SIEM appliance and then analyzing the results.

While compiling this Buyer's Guide, DCIG spoke to various end-users to get a sense of how the end-user would weight their needs in various areas and coupled that with the expertise of the analysts putting together this Buyer's Guide. DCIG then evaluated each product by applying weightings to its features based upon our conversations with end-users and our own knowledge and expertise.

It is in this context that DCIG presents its *2014-15 SIEM Appliance Buyer's Guide.* As prior Buyer's Guides have done, it puts at the fingertips of organizations a comprehensive list of SIEM solutions and the features they offer in the form of detailed, standardized data sheets that can assist them in this important buying decision. This Buyer's Guide is the result of a multi-month effort that involved communicating with multiple providers and evaluating over 100 features on 29 different SIEM appliances.

Each provider was given the opportunity to complete a survey with over 85 questions that examined how its solution delivered on features associated with management, hardware, scalability and support.

In instances where vendors did not respond, DCIG completed the surveys on the vendor's behalf and then sent the completed survey to the vendor for their review. In every case, every vendor had the opportunity to review and respond to the survey and the information regarding their product displayed on the data sheets included in this Buyer's Guide.

This *DCIG 2014-15 SIEM Appliance Buyer's Guide* accomplishes the following objectives:

- Provides an objective, third party evaluation of SIEM solutions that weights, scores and ranks their features from an end user's viewpoint
- Includes recommendations on how to best use this Buyer's Guide
- Scores and ranks the features on each SIEM appliance based upon criteria that matter most to end users so they can quickly know which products are the most appropriate for them to use and under what conditions
- Provides data sheets for 29 SIEM appliances from nine (9) different providers so end users can do quick comparisons of the features that are supported and not supported on each product
- Gives any organization the ability to request competitive bids from different providers of SIEM appliances to do *apples-to-apples* comparisons of these products

© 2014 DCIG, LLC. All rights reserved.

How to Use this Buyer's Guide

In determining how to best use the information contained in this Buyer's Guide, it is important to note that it is intended to help users accelerate the product research and selection process—driving cost out of the research process while simultaneously increasing confidence in the results. The purpose of this Buyer's Guide is ***NOT*** to tell users exactly which product(s) to purchase. Rather it is to help guide them in coming up with a short list of competitive products that have comparable features that meet their specific needs.

It is also important to note that just because a product scored the highest in a particular category or is ranked a certain way does not automatically mean that it is the right product for their organization. If anything, because of the scope of the products evaluated and analyzed, it may have features that are too robust for the needs of an individual department or organization.

However, what this Buyer's Guide does is give users some sense of how each product compares to other products classified in this guide, as well as offers additional insight into what product offerings are available on the market.

DCIG recommends that you use this Buyer's Guide in the following seven (7) ways:

1. ***Eliminate the painstaking research associated with coming up with a short list of products that meet their needs.*** This Buyer's Guide ranks, scores and contains data sheets for 29 different products from nine (9) different vendors. Each product is scored and then ranked as *Best-in-Class, Recommended, Excellent, Good* and *Basic* based upon its score. In each product, over 100 different features were evaluated, weighted, scored and then ranked. All an organization has to do is look at the scores and features of each product in order to come up with a short list of products for consideration.
2. ***Do apples-to-apples comparisons of products from different vendors.*** In today's crowded SIEM appliance market, it behooves organization to get competitive bids from multiple vendors. After all, *when they compete, you win!* But that tactic only works well when organizations know that they are receiving competitive bids on products that are roughly comparable. Using this Buyer's Guide, organizations can do a better job of accomplishing that objective.
3. ***Separate the apples from the oranges.*** Just as important as doing apples-to-apples comparisons is identifying when an orange is thrown into the mix. Sometimes it is very difficult for an organization to know if it is truly getting a good deal when bids come in from vendors that include different products. Now organizations can refer to the scores and rankings of each product in this Buyer's Guide so they know if the features on the appliances they are comparing are apples-to-apples comparisons or apples and oranges.
4. ***Provides perspective on how products from less well known vendors compare against established and better known brands.*** Anyone involved with information security systems has probably at least heard of IBM, but many of the companies providing these innovative products are less well known.

   This Buyer's Guide helps to remove some of that apprehension about buying from a less well known vendor or even a less well known model from an established vendor. Using this Buyer's Guide, organizations can see how these products from lesser known vendors as well as lesser known products from established vendors stack up.
5. ***Normalizes complex terminology.*** Every segment across industries has a proclivity to adopt acronyms and jargon that is specific to it. The SIEM appliance segment is no exception. In this dynamic and relatively young market, vendors often refer to the same capability in different ways. This Buyer's Guide sifts through the acronyms and jargon and then normalizes these terms, providing a foundation for meaningful comparisons. Definitions for the terms on the data sheets in this Buyer's Guide are provided in the Glossary, included as Appendix A.
6. ***Creates a standardized data sheet.*** The product data sheets available from the different vendors are rarely laid out in the same way or contain the same information. Some vendors even have data sheet formats that vary from product to product within their own portfolio. This Buyer's Guide tackles this problem by creating a standard, easy to read data sheet for every product. In this way, product data sheets for individual products can be printed out, laid down side by side and then the features on them quickly compared.

© 2014 DCIG, LLC. All rights reserved.

7. ***Helps justify buying recommendations to business teams.*** Nothing is easier for those on the business side to understand than a number when doing comparisons. At the top of every product data sheet, a product score is included so the business side of the house can quickly see how the different product models compare.

Disclosures

Over the last few years the general trend in the US has been for both large and boutique analyst firms to receive some or all of their revenue from vendors.

DCIG is no different in that respect as it also receives payment for the different services it performs for vendors. The services that DCIG provides include blogging, competitive advantage reports, customer validations, white papers and head-to-head product special reports. It also makes all of the information found in its published Buyer's Guide available online by a paid subscription through its Interactive Buyer's Guide (IBG).

In that vein, there are a number of important facts to keep in mind when considering the information contained in this Buyer's Guide and its merit.

- No vendor paid DCIG any fee to develop this Buyer's Guide.
- DCIG did not guarantee any vendor that its product would be included in this Buyer's Guide.
- DCIG did not imply or guarantee that a specific product would receive a good score on this Buyer's Guide, before or after completion.
- All research was based upon publicly available information, information provided by the vendor and the expertise of those evaluating the information.
- Because of the number of features analyzed, how these features were weighted and how these products were then scored and ranked, there was no way for DCIG to predict at the outset how individual products would end up scoring or ranking.
- DCIG wants to emphasize that no vendor was privy to how DCIG did the scoring and ranking of the products. In every case the vendor only found out the scores and rankings of its product after the analysis was complete.

Inclusion and Exclusion Criteria

This *DCIG 2014-15 SIEM Appliance Buyer's Guide* incorporates input from users and vendors to assist in defining the inclusion criteria for this Buyer's Guide. DCIG attempts to take into consideration as many variables as possible, though likely fails to account for all of them. This may have even resulted in a specific model not being covered in this Buyer's Guide when it rightfully belonged. DCIG will continue to refine both the variables for which we collect data and the inclusion criteria for future editions of the DCIG SIEM Appliance Buyer's Guide.

The rationale that was used to determine the inclusion and exclusion of specific models in this Buyer's Guide is as follows:

- ***The appliance must be available as hardware solution and ship as a single SKU.*** A number of SIEM solutions are sold and/or are available as software. To best address the most common SIEM appliance products that serve the widest range of business needs, only solutions that shipped with both hardware and software as a single SKU were considered for this Buyer's Guide.
- The SIEM appliance must provide traditional SIEM capabilities, such as:
  - ***The SIEM appliance must offer data and log aggregation.***
  - ***The SIEM Appliance must support log data protection and prevention.***
  - ***The SIEM Appliance must provide correlation abilities.*** An appliance must be able to correlate data together from various sources to produce a holistic snapshot of the information that it gathers about an environment.
  - ***The SIEM Appliance must contain alerting capabilities.*** It has to have ability to alert security administrators of unusual activity in the network.
  - ***The SIEM appliance must present a dashboard.*** A dashboard gives a brief, high-level picture of what is happening in the security environment.
- ***Must be generally available by January 1st, 2014.*** A cut-off date had to be put in place or this Buyer's Guide would never be published.

© 2014 DCIG, LLC. All rights reserved.

The 8-Step Process Used to Score and Rank SIEM Appliances

To score and rank each flash memory storage array model, DCIG went through an eight (8) step process to come to the most objective conclusion possible.

1. ***DCIG listed out all of the features available on all of the SIEM Appliances.*** Prior to selecting the features that were included in the final evaluation in the Buyer's Guide, DCIG went through and quantified what features SIEM Appliances this process, DCIG *"normalized"* the list of features available on SIEM Appliances such that a common name for each feature was established.

2. ***DCIG established which features would be included in the Buyer's Guide and which ones would not.*** One of the goals of this Buyer's Guide was to try to only include features on each SIEM Appliance model that could be objectively and authoritatively analyzed.

   For example, *"Event Process Rate (Max)"* was evaluated as a feature instead of *"Peak Events per Second."* While the measurement of Peak Events per Second (EPS) may ultimately be a more important metric, SIEM Appliance providers cannot objectively measure a "peak event" which negated the use of this terminology. Therefore, *"Event Process Rate (Max)"* was selected as the feature to be evaluated since a more objective answer could be ascertained and supported.

3. ***The features were broken down into four general categories.*** The features included in this Buyer's Guide broke down into a total of four broad categories that are reflected on each SIEM Appliance data sheet. These four categories include Hardware, Software, Management and Support.

4. ***Each feature had a weighting associated with it.*** The weightings were used to reflect if a feature was supported and potentially how valuable the feature is to an end-user compared to other options. For example, the *"Custom Branded Report"* feature is more of a *"Yes"* or *"No"* type of response whereas *"Total Raw Capacity (Max TB)"* covers a range of storage capacity options. Each of these options is weighted and scored differently.

5. ***A survey that asked about all of the features scored in this Buyer's Guide was sent to each storage provider.*** Vendors were invited to complete the online survey. The survey elicits more data than was available on any vendor website to provide a more thorough analysis of each SIEM Appliance. If a vendor did not respond to the invitation, a DCIG analyst filled out the survey on their behalf using the vendor's web site, other reliable publicly available information, and prior DCIG research where available.

6. ***All vendors were given the opportunity to review their data sheets before the final scores and rankings were determined.*** To ensure the information presented in this Buyer's Guide is as complete and correct as possible, DCIG provided each vendor a copy or copies of their filled-out surveys and the data sheets that appear in this Buyer's Guide *without the scores and rankings on them.* In this way they had the opportunity to validate the information and correct it before it was publicly released.

7. ***All of the features were scored based upon the information that was gathered.*** The weighting and scoring of the features were done by a DCIG analyst.

8. ***The SIEM Appliances were ranked using standard scoring techniques.*** One of the goals of this Buyer's Guide is to establish clear lines of differentiation between SIEM Appliances with conclusions that are arrived at objectively. To accomplish this goal, the mean or average score for each classification was first determined and then the standard deviation.

Using the mean of the scores from all of the SIEM Appliances from which the standard deviation was calculated, DCIG developed a ranking for each model based upon the following in each classification:

- Those models that were .5 or greater standard deviations below the mean were given the rank of *Basic.*
- Those models that were .5± standard deviations above or below the mean were ranked as *Good.*
- Those models that were .5 – 1.25 standard deviations above the mean were ranked as *Excellent.*
- Those models that were greater than 1.25 standard deviations above the mean were ranked as *Recommended.*
- The model(s) with the highest score in each category were given the designation of *Best-in-Class.*
- It is for this reason that in each category the number of models that achieved a certain ranking varied.

© 2014 DCIG, LLC. All rights reserved.

Comments & Thoughts on…

Struggles with SEIM Appliances

The SIEM appliance market is rapidly evolving and feature appliances that provide a wide range of capabilities. Those without extensive experience with SIEM can easily find the market, appliance capabilities, and features available to be confusing. This section seeks to help organizations understand the many options available.

The question every practicing information security professional wants answered when it comes to SIEM is: *"Which SIEM solution is the best one for me?"* This is a question that has no easy answer. Despite all efforts to answer it conclusively, the best answer is *"It depends."*

Information security consultants often see customers struggle with:

- ***Determining the specific requirements for an SIEM appliance in their respective environments.*** SIEM solutions have many features. Before investing in a specific SIEM appliance, spend time determining your specific needs.
- ***Understanding how an SIEM appliance will satisfy the specific requirements.*** Map your specific requirements to the specific features supported by SIEM appliances.
- ***SIEM appliance implementation.*** Not all SIEM appliances are the same when it comes to implementation and integration which results in organizations being improperly prepared for a successful SIEM deployment. Organizations should develop and implement prerequisites like secure builds, standard configurations, and sound change control processes as well as intimately understand how the SIEM appliance integrates with your organization's broader information security strategy.
- ***SIEM appliance support.*** Some SIEM appliances are more *"plug and play"* than others, but this often comes with a price in terms of the appliance's functionality, flexibility and usability. While *"plug and play"* is desirable, how the SIEM appliance is supported and what process changes it requires are more desirable and will provide a higher level of security and protection over time than simply deploying an SIEM appliance for the sake of having one as this represents a wasted investment and may leave your organization exposed.

SIEM Appliance Implementation Considerations

The only way to have any assurance that you are compliant with most information security regulations is to understand how your other controls are working and if they are functioning as intended. An SIEM appliance, if deployed and maintained properly, can give a security administrator insight into the moment-by-moment technical compliance status of his/her organization. At the same time, it can give executive management the insight they need to plan strategically.

The deployment and maintenance of the chosen solution, however, is often the most challenging part of choosing and using an SIEM appliance. Implementation of an SIEM appliance varies greatly between the available solutions. Some of the SIEM solutions presented in this Buyer's Guide are more *"plug-and-play,"* while others can be very difficult for a novice to implement. Due to the potential complexities, it makes sense to obtain a demo appliance if possible and try out the appliance before purchasing or implementing it.

SIEM Appliance Starting Point

As already noted, it is vital to consider which SIEM appliance fits your organization's unique needs prior to even examining the SIEM solutions available on the market. Determine how you will use SIEM for all that it can provide your organization. If you are unsure of where to start, consider the following:

- ***Educate yourself.*** Understanding what an SIEM appliance offers is the first step. The acquisition of an SIEM appliance should be based upon sound security decisions in accordance with business requirements. Verify the SIEM will be used in such a way to improve your organization's broader information security and represents more than just completing a check box.
- ***Define your own requirements before you start shopping around for a solution.*** Define your requirements first and then compare the features on the available solutions against your pre-defined criteria. This Buyer's Guide includes many of the criteria any need to consider and will serve as an excellent starting point to determining the features available on these products and identifying the right product for your environment.
- ***Define or redefine process.*** Prepare for how you are going to use and support SIEM ***before*** the purchase and implementation. You should put processes in place to adequately support you SIEM solution to include determining if a FTE or specialist is needed to maintain

© 2014 DCIG, LLC. All rights reserved.

the solution and interpret its messages. Organizations should also put in place processes to respond to alerts generated by the SIEM solution as well as differentiate between what constitutes a formal incident response process versus ignoring *(or tuning out)* an alert.

The Maturity of the SIEM Appliance Market

The SIEM appliance market is still young and immature, though less so in terms of the technology. Rather this immaturity is reflected more in terms of consumer readiness and understanding. Too many organization buy SIEM solutions before completing all of the necessary education and readiness checks. Any technology provider will gladly sell a company a solution to a problem that it may (or may not) have. Ultimately it is the company's problem if it does not know how to use the solution.

The roots of SIEM solutions are in centralized logging systems and devices. The first devices did little more than store (and protect) log files. It was up to the security administrator to review log files with most of these reviews done manually. As the solutions matured, additional features on SIEM appliances began to emerge.

Today's SIEM appliances do much more than collect and protect log files. They aggregate, correlate, and provide active protection based on the intelligence gleaned from the environment. This has make SIEM appliances more useful but at the same time more complex. The introduction of these new features has resulted in this technology maturing at a faster pace than the understanding of many people using it.

The number of security breaches and the increased concern that organizations have about unauthorized access to their information has contributed to making an already hot market for SIEM appliances even hotter. This concerns coupled with increased compliance demands are pushing more organizations to adopt these appliances.

SIEM Appliance Evaluation Challenges

A lack of understanding on the part of consumers acquiring SIEM appliances is not the only place where immaturity exists in this market place. The terminology used to describe and benchmark the features on these appliances is in a number of cases also equally immature. Among them:

1. ***Benchmarks for the measurement of SIEM performance or features are still very subjective.*** Event Peak Processing is an agreed upon means to measure Events per Second (EPS). The challenge is that SIEM vendors use a variety of methods to arrive at this metric. One vendor claims a peak EPS of 5,000 while another claims a peak EPS of 50,000. Both may be technically correct though they may use different tools to arrive at these figures. This makes it is nearly impossible to validate the accuracy of these metrics or what metrics an organization may obtain when the appliance is deployed in their environment.
2. ***There is a great deal of subjectivity associated with choosing the right solution for any given organization.*** In order for organizations to objectively evaluate SIEM appliances, some standards need to exist as to how features on SIEM appliances from different providers are described. This Buyer's Guide represents the first concerted effort to provide such a common set of definitions for these features.
3. ***Providers reluctant to share information.*** DCIG still had to rely very heavily on press releases, data sheets, vendor web sites and other generally available industry sources to evaluate the SIEM appliances in this Buyer's Guide. It is DCIG's hope that in the future more SIEM appliance providers will respond to DCIG inquiries. This will in turn lead to better information in future DCIG Buyer's Guides.
4. ***Some solutions initially slated to be included were removed.*** DCIG originally identified 36 products that met the established inclusion criteria. However some of these solutions were later excluded either because the provider came out with a new product or, after closer evaluation and inspection, these appliances were only available as software or as virtual appliances (SIEM software running on dedicated virtual machines.) This led to these solutions being dropped from inclusion in this Guide.

DCIG Observations & Recommendations

Best-in-Class Ranking

LogRhythm All-in-One (XM) 6300

Observations

The **LogRhythm All-in-One (XM) 6300 SIEM** appliance achieved the *Best-in-Class* ranking in this inaugural *DCIG 2014-15 SIEM Appliance Buyer's Guide.* Scoring at or near the top in every category (Hardware, Management, Software and Support) evaluated in this Buyer's Guide, it represents the best of what SIEM appliances currently have to offer.

© 2014 DCIG, LLC. All rights reserved.

Its strong showing in the Management category is of particular note. Organizations want SIEM appliances to promptly alert them should any type of breach occur and the All-in-One (XM) 6300 stood head and shoulders above the competition in its ability to detect breaches and then respond and recover from them. Able to monitor in excess of 2,000 systems, collect over 10,000 events per second, and provide multiple ways in which to collect data, generate alerts and even be configured to automatically take action, it provides enterprise organizations with a robust solution to centrally monitor and manage a large number of devices.

Recommendations

The LogRhythm All-in-One (XM) 6300 is the best SIEM appliance fit for the broadest range of environments and organizations as it provides the most comprehensive set of features among the SIEM appliances evaluated. Large enterprises should especially consider this solution for adoption in their environments as the LogRhythm All-in-One (XM) 6300 is about as close to a *"can't miss"* option as there is in the SIEM appliance market.

Recommended Ranking

LogRhythm All-in-One (XM) 4300

Observations

The LogRhythm All-in-One (XM) 4300 SIEM appliance achieved the only *Recommended* ranking in this Buyer's Guide. Like its big brother; the LogRhythm All-in-One (XM) 6300, the (XM) 4300 possesses most of the 6300's feature functionality and shares the Best-in-Class ranking in the Software category with it.

The primary difference between this model and the XM 6300 is that the 6300 has more hardware features to support higher levels of performance. This makes the XM 4300 better suited for midsized, small and remote offices as organizations get all of the 6300's management, software and support features available but at a lower price point.

Recommendations

The LogRhythm All-in-One (XM) 4300 SIEM appliance is an excellent fit for most small to mid-sized organizations. The features provided by the appliance give small and midsize organizations all of features and performance that they are likely to need an SIEM appliance to provide with relative ease of implementation and support.

Excellent Ranking

Observations

The SIEM appliances ranked as Excellent generally shared the following characteristics:

- ***Contain ample built-in storage.*** All SIEM appliances rated excellent and above came with 2TB or more of storage capacity in a RAID configuration.
- ***Display a distinct ease of management.*** Each of the SIEM appliances rated *Excellent* and above offer a wide variety of flexible management solutions including co-admin features, strong and flexible access control, and excellent incident management support.
- ***Offer wide range of data collection capabilities.*** These capabilities include configurable agent installations and agentless data collection.
- ***Show excellent performance.*** They can achieve event processing rates of at least 1,000 EPS and collection rates averaging up to 10,000 EPS.
- ***Provide strong implementation support.*** They include a range of support options with average installation able to be supported with less than five hours or training. These products also boast large install bases.

Recommendations

The organizations best suited for the SIEM appliances rated *Excellent* are those with pressing compliance needs and those with dedicated information security personnel. While these SIEM appliances may meet the needs of many organizations, organizations should have a good handle on exactly what challenges they confront and can map them to the features available on these appliances.

Only four (4) SIEM appliances achieved an *Excellent* ranking: The Hewlett-Packard ArcSight AE-7581 and AE-7566 models, the McAfee ETM-6000 and the TIBCO LogLogic MX4025. These SIEM appliances offer most if not all of the features available on the *Best-in-Class* and *Recommended* SIEM appliances. These appliances may prove to be most attractive to small and midsized businesses that have needs for higher levels of capacity and/or performance as these appliances generally have more robust hardware than the other models evaluated in this Buyer's Guide.

© 2014 DCIG, LLC. All rights reserved.

Good Ranking

Observations

The SEIM appliances ranked as *Good* generally shared the following characteristics:

- ***Support for the most important SIEM features.*** These features include event/log collection, aggregation, correlation and presentation *(alerts and dashboards).*
- ***Offer data collection capabilities for the most common event and log sources.*** These appliances generally did not support as wide a range of sources as SIEM appliances with higher rankings.
- ***Offer good performance.*** They can achieve event processing rates ranging from 500 EPS to more than 1,000 EPS and collection rates ranging from 1,000 to 10,000 EPS.
- ***Provide more limited implementation, training and management support option.***

Recommendations

The majority (16) of the SIEM appliances evaluated in this Buyer's Guide achieved the ranking of *Good.* These appliances are well-suited for organizations that can match specific needs and requirements to specific features provided. In most cases, the organizations adopting these appliances will employ personnel with specific information security responsibilities and in some cases should employ personnel dedicated to SIEM.

Basic Ranking

Observations

In general, the SIEM appliances ranked as *Basic* shared the following characteristics:

- Provide support for basic SIEM features.
- Offer limited flexibility in data collection, event processing, incident management support, and training opportunities.
- Display performance that is generally less than adequate for the most demanding network environments.

Recommendations

The SIEM appliances ranked as *Basic* could be an appropriate entry-level option for organizations that have certain compliance needs to fill and are not all that interested in fully leveraging all of the features that SIEM appliances have to offer. However due to the comparable price points between SIEM appliances rated as *Basic* and those with higher rankings, organizations should have a very compelling business case for deploying these models over higher ranked models in this Guide.

© 2014 DCIG, LLC. All rights reserved.

SIEM APPLIANCE SCORES AND RANKINGS

The scores and rankings for the security incident and event management appliances contain the following information:

- A chart that includes the scores and rankings for all of the products
- The mean and the standard deviation that were used to establish how each integrated backup appliance solution was ranked
- A summary of the primary findings

© 2014 DCIG, LLC. All rights reserved.

OVERALL SCORES AND RANKINGS

	SIEM APPLIANCES	SCORE	RANKING
1.	**LogRhythm All-in-One (XM) 6300**	**95.86**	**Best-in-Class**
2.	LogRhythm All-in-One (XM) 4300	91.28	Recommended
3.	Hewlett-Packard ArcSight AE-7581	85.83	Excellent
4.	McAfee ETM-6000	85.56	Excellent
5.	Hewlett-Packard ArcSight AE-7566	84.93	Excellent
6.	TIBCO LogLogic MX4025	83.77	Excellent
7.	IBM Security QRadar SIEM 3124 All-In-One	81.55	Good
8.	IBM Security QRadar SIEM 3105 All-In-One	81.48	Good
9.	Hewlett-Packard ArcSight AE-7526	81.23	Good
10.	BlackStratus MIDWAY	80.84	Good
11.	Hewlett-Packard ArcSight AE-7551	80.43	Good
12.	McAfee ETM-5600	79.92	Good
13.	BlackStratus ENTERPRISE	79.00	Good
14.	IBM Security QRadar SIEM 2100 All-In-One	78.94	Good
15.	TIBCO LogLogic MX3025	78.91	Good
16.	McAfee ETM-4600-ELM	77.92	Good
17.	BlackStratus RANGER	76.41	Good
18.	Solarwinds Log & Event Manager	75.94	Good
19.	Alienvault USM Standard & Enterprise	75.83	Good
20.	BlackStratus EXPRESS	75.13	Good
21.	Trustwave LME 5	74.96	Good
22.	Hewlett-Packard ArcSight AE-7511	74.73	Good
23.	Hewlett-Packard ArcSight AE-7506	72.23	Basic
24.	Trustwave LME 4	71.16	Basic
25.	AlienVault USM All-in-One	70.98	Basic

continued on next page

© 2014 DCIG, LLC. All rights reserved.

OVERALL SCORES AND RANKINGS (continued)

	SIEM APPLIANCES	SCORE	RANKING
26.	Trustwave LME 3	68.52	Basic
27.	Trustwave LME 2	65.76	Basic
28.	Trustwave LME 2-20	65.66	Basic
29.	Trustwave LME 2-10	65.46	Basic

Total Number of Products **29**

		Rankings	
Highest Score	**95.86**	Recommended	**88.81 – 95.86**
Lowest Score	**65.46**	Excellent	**81.57 – 88.80**
Average (Mean)	**77.94**	Good	**74.32 – 81.56**
Standard Deviation	**7.24**	Basic	**65.46 – 74.31**

© 2014 DCIG, LLC. All rights reserved.

Management Scores and Rankings

	SIEM APPLIANCES	SCORE	RANKING
1.	**LogRhythm All-in-One (XM) 6300**	**58.00**	**Best-in-Class**
2.	LogRhythm All-in-One (XM) 4300	56.80	Recommended
3.	Hewlett-Packard ArcSight AE-7581	53.85	Excellent
4.	Hewlett-Packard ArcSight AE-7566	53.15	Excellent
5.	TIBCO LogLogic MX4025	52.25	Excellent
6.	McAfee ETM-6000	52.20	Excellent
7.	Hewlett-Packard ArcSight AE-7526	50.25	Good
8.	TIBCO LogLogic MX3025	50.05	Good
9.	BlackStratus ENTERPRISE	49.90	Good
10.	BlackStratus MIDWAY	49.60	Good
11.	BlackStratus RANGER	49.55	Good
12.	Hewlett-Packard ArcSight AE-7551	49.45	Good
13.	BlackStratus EXPRESS	49.05	Good
14.	McAfee ETM-5600	48.80	Good
15.	Solarwinds Log & Event Manager	48.70	Good
16.	Alienvault USM Standard & Enterprise	48.55	Good
17.	McAfee ETM-4600-ELM	48.50	Good
18.	IBM Security QRadar SIEM 2100 All-In-One	48.30	Good
19.	IBM Security QRadar SIEM 3105 All-In-One	47.60	Good
20.	IBM Security QRadar SIEM 3124 All-In-One	47.15	Good
21.	Hewlett-Packard ArcSight AE-7511	46.85	Good
22.	Hewlett-Packard ArcSight AE-7506	46.25	Good
23.	AlienVault USM All-in-One	45.20	Good
24.	Trustwave LME 5	42.20	Basic
25.	Trustwave LME 4	40.50	Basic

continued on next page

© 2014 DCIG, LLC. All rights reserved.

Management Scores and Rankings (continued)

	SIEM APPLIANCES	SCORE	RANKING
26.	Trustwave LME 3	39.80	Basic
27.	Trustwave LME 2	37.90	Basic
28.	Trustwave LME 2-20	37.80	Basic
29.	Trustwave LME 2-10	37.60	Basic

Total Number of Products 29

		Rankings	
Highest Score	58.00	Recommended	55.71 – 58.00
Lowest Score	37.60	Excellent	50.43 – 55.70
Average (Mean)	47.79	Good	45.15 – 50.42
Standard Deviation	5.28	Basic	37.60 – 45.14

© 2014 DCIG, LLC. All rights reserved.

Software Scores and Rankings

	SIEM APPLIANCES	SCORE	RANKING
1.	**LogRhythm All-in-One (XM) 6300**	**16.90**	**Best-in-Class**
2.	**LogRhythm All-in-One (XM) 4300**	**16.90**	**Best-in-Class**
3.	IBM Security QRadar SIEM 2100 All-In-One	16.70	Recommended
4.	IBM Security QRadar SIEM 3124 All-In-One	15.50	Excellent
5.	IBM Security QRadar SIEM 3105 All-In-One	15.50	Excellent
6.	TIBCO LogLogic MX4025	14.10	Good
7.	TIBCO LogLogic MX3025	14.10	Good
8.	AlienVault USM All-in-One	14.00	Good
9.	McAfee ETM-6000	13.60	Good
10.	McAfee ETM-5600	13.60	Good
11.	McAfee ETM-4600-ELM	13.60	Good
12.	Hewlett-Packard ArcSight AE-7581	13.40	Good
13.	Hewlett-Packard ArcSight AE-7566	13.40	Good
14.	Hewlett-Packard ArcSight AE-7551	13.40	Good
15.	Hewlett-Packard ArcSight AE-7526	13.40	Good
16.	Hewlett-Packard ArcSight AE-7511	13.40	Good
17.	Hewlett-Packard ArcSight AE-7506	13.40	Good
18.	Solarwinds Log & Event Manager	13.20	Good
19.	BlackStratus MIDWAY	13.10	Good
20.	BlackStratus RANGER	12.90	Basic
21.	Alienvault USM Standard & Enterprise	12.80	Basic
22.	BlackStratus EXPRESS	12.70	Basic
23.	Trustwave LME 5	12.70	Basic
24.	Trustwave LME 4	12.70	Basic
25.	Trustwave LME 3	12.70	Basic

continued on next page

© 2014 DCIG, LLC. All rights reserved.

Software Scores and Rankings (continued)

	SIEM APPLIANCES	SCORE	RANKING
26.	Trustwave LME 2	12.70	Basic
27.	Trustwave LME 2-20	12.70	Basic
28.	Trustwave LME 2-10	12.70	Basic
29.	BlackStratus ENTERPRISE	11.90	Basic

Total Number of Products **29**

		Rankings	
Highest Score	**16.90**	Recommended	**15.71 – 16.90**
Lowest Score	**11.90**	Excellent	**14.39 – 15.70**
Average (Mean)	**13.71**	Good	**13.05 – 14.38**
Standard Deviation	**1.33**	Basic	**11.90 – 13.04**

© 2014 DCIG, LLC. All rights reserved.

SIEM APPLIANCE MODELS

© 2014 DCIG, LLC. All rights reserved.

AlienVault USM All-In-One

Approximate Starting List Price: $3,600

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
70.98	7.58	14.00	45.20	4.20
BASIC	GOOD	GOOD	GOOD	BASIC

HARDWARE

Virtual Appliance Option	✓
Raw Storage *MAX*	1.8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	2
Rated Throughput	Up to 200 Mbps/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✗
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✓
Dashboard Mobile Platforms *TOTAL #*	3
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	2
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	2
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	7
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	>10
Supported Load Exceeded	Dropping
Data Types *TOTAL #*	8
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✗
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	17
Base Event Collection Rate	Up to 2,500 eps
Maximum Event Collection Rate	Up to 5,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 2,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	6
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	1 – 2 hours
Recom'd Training *MANAGE & MAINTAIN*	5 – 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Free of Charge
Support Performance Tracking	✗
% Support Resolution w/o Escalation	✗
% Support Resolution on 1st Contact	✗
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

AlienVault USM Standard & Enterprise

Approximate Starting List Price: $50,000 – $75,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
75.83	9.08	12.80	48.55	5.40
GOOD	EXCELLENT	BASIC	GOOD	BASIC

HARDWARE

Virtual Appliance Option	✓
Raw Storage *MAX*	1.8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 1Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	2
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	5
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	7
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	Up to 2,000
Concurrent Admin Logins	>10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	10
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✗
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	18
Base Event Collection Rate	>10,000 eps
Maximum Event Collection Rate	Up to 5,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	7
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	5 – 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	3
24x7x365 Telephone	✗
New Software Versions	Incl. in support contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	✗
% Support Resolution on 1st Contact	81 – 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

BlackStratus ENTERPRISE

Approximate Starting List Price: $50,000 – $75,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
79.00	8.90	11.90	49.90	8.30
GOOD	GOOD	BASIC	GOOD	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	10 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 1Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✗
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	3
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP, HTTP
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	Yes
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	> 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	10
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	✗
Software Agent Standard Inputs *TOTAL #*	17
Base Event Collection Rate	> 10,000 eps
Maximum Event Collection Rate	> 10,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	> 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	7
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	> 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	3
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in support contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	81 – 90%
% Support Resolution on 1st Contact	> 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✗
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

BlackStratus EXPRESS

Approximate Starting List Price: Less than $10,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
75.13	4.08	12.70	49.05	9.30
GOOD	BASIC	BASIC	GOOD	EXCELLENT

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	2 TB
RAID	✗
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 200Mb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	2
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	Yes
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✗
Software Agent Configurable	✓
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	18
Base Event Collection Rate	Up to 5,000 eps
Maximum Event Collection Rate	Up to 7,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	3
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	5 – 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	3
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in support contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	81 – 90%
% Support Resolution on 1st Contact	> 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✓
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

BlackStratus MIDWAY

Approximate Starting List Price: $10,000 – $25,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
80.84	9.24	13.10	49.60	8.90
GOOD	EXCELLENT	BASIC	GOOD	GOOD

HARDWARE

Virtual Appliance Option	⊗
Raw Storage *MAX*	6 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	⊗
Dashboard Mobile Platforms *TOTAL #*	3
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	⊗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	⊗

✓ Supported ⊗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	Yes
LDAP Authentication	⊗
# of Monitored Systems *SINGLE APPLIANCE*	> 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	⊗
Software Agent Remote Installation	✓
Software Agent Remote Update	⊗
Software Agent Configurable	✓
Software Agent Remotely Configurable	⊗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	19
Base Event Collection Rate	Up to 10,000 eps
Maximum Event Collection Rate	Up to 7,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	1
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	5 – 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	⊗
DISA UC Approved Product	⊗
Tuning Services *TOTAL #*	3
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	81 – 90%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✓
Web-based Training	✓
Instructor-led Training	✓
Product Certification	⊗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

BlackStratus RANGER

Approximate Starting List Price: $10,000 – $25,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
76.41	4.66	12.90	49.55	9.30
GOOD	BASIC	BASIC	GOOD	EXCELLENT

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	4 TB
RAID	✗
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 5Mb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	1
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	3
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	Yes
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✗
Software Agent Configurable	✓
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	20
Base Event Collection Rate	> 10,000 eps
Maximum Event Collection Rate	> 10,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	1
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	5 – 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	3
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	81 – 90%
% Support Resolution on 1st Contact	> 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✓
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Hewlett-Packard ArcSight AE-7506

Approximate Starting List Price: $25,000 – $50,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
72.23	4.58	13.40	46.25	8.00
BASIC	BASIC	GOOD	GOOD	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	1.8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	✗
Rated Throughput	Up to 500Mb/sec
Event Process Rate *MAX*	Up to 500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	3
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	5
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	8
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✗
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	>10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✗
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	22
Base Event Collection Rate	Up to 500 eps
Maximum Event Collection Rate	Up to 1,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	3
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	> 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	3
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	81 – 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Hewlett-Packard ArcSight AE-7511

Approximate Starting List Price: $50,000 – $75,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
74.73	6.08	13.40	46.85	8.40
GOOD	BASIC	GOOD	GOOD	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	1.8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 1Gb/sec
Event Process Rate *MAX*	Up to 1,000 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	3
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	5
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	8
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✗
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✗
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	21
Base Event Collection Rate	Up to 500 eps
Maximum Event Collection Rate	Up to 2,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	5
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	3
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	81 – 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Hewlett-Packard ArcSight AE-7526

Approximate Starting List Price: $50,000 – $100,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
81.23	9.08	13.40	50.25	8.50
GOOD	EXCELLENT	GOOD	GOOD	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	1.8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	3
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	5
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	8
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✗
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	21
Base Event Collection Rate	Up to 2,500 eps
Maximum Event Collection Rate	Up to 2,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	5
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	5 – 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	81 – 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Hewlett-Packard ArcSight AE-7551

Approximate Starting List Price: $100,000 – $250,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
80.43	9.08	13.40	49.45	8.50
GOOD	EXCELLENT	GOOD	GOOD	GOOD

HARDWARE

Virtual Appliance Option	⊗
Raw Storage *MAX*	1.8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	⊗
Dashboard Mobile Platforms *TOTAL #*	⊗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	3
FIPS 140-2	⊗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ⊗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	5
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	8
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	⊗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	21
Base Event Collection Rate	Up to 2,500 eps
Maximum Event Collection Rate	Up to 5,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	5
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	> 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	⊗
DISA UC Approved Product	⊗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	81 – 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	⊗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	⊗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Hewlett-Packard ArcSight AE-7566

Approximate Starting List Price: Over $250,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
84.93	10.08	13.40	53.15	8.30
EXCELLENT	EXCELLENT	GOOD	EXCELLENT	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	1.8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	2
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	3
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	5
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	8
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	Up to 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	21
Base Event Collection Rate	Up to 5,000 eps
Maximum Event Collection Rate	Up to 10,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 2,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	5
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	> 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 500 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	81 – 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Hewlett-Packard ArcSight AE-7581

Approximate Starting List Price: Over $250,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
85.83	10.08	13.40	53.85	8.50
EXCELLENT	EXCELLENT	GOOD	EXCELLENT	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	1.8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	2
Rated Throughput	> 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	3
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	5
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	8
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	Up to 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✗
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	21
Base Event Collection Rate	Up to 10,000 eps
Maximum Event Collection Rate	> 10,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 2,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	4
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	> 10 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✗
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	81 – 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

IBM Security QRadar SIEM 2100 All-In-One

Approximate Starting List Price: $50,000 – $75,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
78.94	7.04	16.70	48.30	6.90
GOOD	BASIC	RECOMMENDED	GOOD	BASIC

HARDWARE

Virtual Appliance Option	✓
Raw Storage *MAX*	1.3 TB
RAID	✓
Appliance Growth Options *TOTAL #*	4
Rated Throughput	Up to 200Mb/sec
Event Process Rate *MAX*	Up to 1,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✓
Dashboard Mobile Platforms *TOTAL #*	0
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ⊗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	2
Standard Basic SIEM Capabilities	14
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	3
Data Export Options *TOTAL #*	6
Report Distribution Interface(s)	SMTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	7
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	⊗
Software Agent Data Encryption	⊗
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	1
Software Agent Standard Inputs *TOTAL #*	3
Base Event Collection Rate	Up to 2,500 eps
Maximum Event Collection Rate	Up to 2,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 1,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	6
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	1 – 2 hours
Recom'd Training *MANAGE & MAINTAIN*	2 – 5 hours
Est. Current Installation Base	Up to 500 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	2
Common Criteria Validation	⊗
DISA UC Approved Product	⊗
Tuning Services *TOTAL #*	1
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	More than 90%
% Support Resolution on 1st Contact	⊗
Professional Training Available	✓
Professional Training Included in Support Contracts	⊗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✓

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

IBM Security QRadar SIEM 3105 All-In-One

Approximate Starting List Price: $100,000 – $250,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
81.48	9.28	15.50	47.60	9.10
GOOD	EXCELLENT	EXCELLENT	GOOD	EXCELLENT

HARDWARE

Virtual Appliance Option	✓
Raw Storage *MAX*	6.5 TB
RAID	✓
Appliance Growth Options *TOTAL #*	4
Rated Throughput	Up to 200Mb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✓
Dashboard Mobile Platforms *TOTAL #*	0
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ⊗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	2
Standard Basic SIEM Capabilities	14
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	3
Data Export Options *TOTAL #*	6
Report Distribution Interface(s)	SMTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	7
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	⊗
Software Agent Data Encryption	⊗
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	1
Software Agent Standard Inputs *TOTAL #*	3
Base Event Collection Rate	Up to 2,500 eps
Maximum Event Collection Rate	Up to 7,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 1,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	7
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	3
Common Criteria Validation	⊗
DISA UC Approved Product	✓
Tuning Services *TOTAL #*	1
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	More than 90%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	⊗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✓

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

IBM Security QRadar SIEM 3124 All-In-One

Approximate Starting List Price: $100,000 – $250,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
81.55	9.80	15.50	47.15	9.10
GOOD	EXCELLENT	EXCELLENT	GOOD	EXCELLENT

HARDWARE

Virtual Appliance Option	✓
Raw Storage *MAX*	20 TB
RAID	✓
Appliance Growth Options *TOTAL #*	4
Rated Throughput	Up to 200Mb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	0
Dashboard Mobile Platform	✓
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	2
Standard Basic SIEM Capabilities	14
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	3
Data Export Options *TOTAL #*	6
Report Distribution Interface(s)	SMTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	7
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	3
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✗
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	1
Software Agent Standard Inputs *TOTAL #*	4
Base Event Collection Rate	Up to 2,500 eps
Maximum Event Collection Rate	Up to 7,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	7
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	3
Common Criteria Validation	✗
DISA UC Approved Product	✓
Tuning Services *TOTAL #*	1
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	More than 90%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✓

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

LogRhythm All-in-One (XM) 4300

Approximate Starting List Price: $25,000 – $50,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
91.28	8.08	16.90	56.80	9.50
RECOMMENDED	GOOD	BEST-IN-CLASS	RECOMMENDED	EXCELLENT

HARDWARE

Virtual Appliance Option	✓
Raw Storage *MAX*	2 TB
RAID	✓
Appliance Growth Options *TOTAL #*	3
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	Up to 1,000 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	2
Dashboard Mobile Platform	✓
Dashboard Mobile Platforms *TOTAL #*	3
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ⊗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	2
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	4
Data Export Options *TOTAL #*	6
Report Distribution Interface(s)	SMTP
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	7
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	5
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	> 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	4
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	28
Base Event Collection Rate	Up to 1,000 eps
Maximum Event Collection Rate	Up to 10,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	7
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	6
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	2
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 500 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	3
Common Criteria Validation	✓
DISA UC Approved Product	⊗
Tuning Services *TOTAL #*	3
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	81 – 90%
% Support Resolution on 1st Contact	81 – 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✓
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✓

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

LogRhythm All-in-One (XM) 6300

Approximate Starting List Price: $50,000 – $75,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
95.86	10.66	16.90	58.00	10.30
BEST-IN-CLASS	EXCELLENT	BEST-IN-CLASS	BEST-IN-CLASS	EXCELLENT

HARDWARE

Virtual Appliance Option	✓
Raw Storage *MAX*	4 TB
RAID	✓
Appliance Growth Options *TOTAL #*	3
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	2
Dashboard Mobile Platform	✓
Dashboard Mobile Platforms *TOTAL #*	3
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ⊗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	2
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	4
Data Export Options *TOTAL #*	6
Report Distribution Interface(s)	SMTP
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	7
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	5
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	> 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	4
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	28
Base Event Collection Rate	Up to 5,000 eps
Maximum Event Collection Rate	> 10,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	> 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	7
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	6
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	2
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 500 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	3
Common Criteria Validation	✓
DISA UC Approved Product	⊗
Tuning Services *TOTAL #*	3
24x7x365 Telephone	Part of Support Contract
New Software Versions	Part of Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	81 – 90%
% Support Resolution on 1st Contact	81 – 90%
Professional Training Available	✓
Professional Training Included in Support Contracts	✓
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✓

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

McAfee ETM-4600-ELM

Approximate Starting List Price: $25,000 – $50,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
77.92	6.62	13.60	48.50	9.20
GOOD	BASIC	GOOD	GOOD	EXCELLENT

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	3 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	Up to 1,000 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	3
Data Export Options *TOTAL #*	6
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	8
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 499
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	26
Base Event Collection Rate	Up to 1,000 eps
Maximum Event Collection Rate	Up to 2,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	7
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	1 – 2 hours
Recom'd Training *MANAGE & MAINTAIN*	5 – 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	81 – 90%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

McAfee ETM-5600

Approximate Starting List Price: $50,000 – $75,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
79.92	8.32	13.60	48.80	9.20
GOOD	GOOD	GOOD	GOOD	EXCELLENT

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	2
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	Up to 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	3
Data Export Options *TOTAL #*	6
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	8
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✗
Software Agent Configurable	✗
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	26
Base Event Collection Rate	Up to 2,500 eps
Maximum Event Collection Rate	Up to 2,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 1,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	7
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	1 – 2 hours
Recom'd Training *MANAGE & MAINTAIN*	5 – 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	81 – 90%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

McAfee ETM-6000

Approximate Starting List Price: $75,000 – $100,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
85.56	10.56	13.60	52.20	9.20
EXCELLENT	EXCELLENT	GOOD	EXCELLENT	EXCELLENT

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	14 TB
RAID	✓
Appliance Growth Options *TOTAL #*	2
Rated Throughput	> 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	3
Data Export Options *TOTAL #*	6
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	8
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	> 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✗
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	26
Base Event Collection Rate	Up to 5,000 eps
Maximum Event Collection Rate	Up to 5,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	7
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	1 – 2 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	81 – 90%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

SolarWinds Log & Event Manager

Approximate Starting List Price: Less than $10,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
75.94	8.54	13.20	48.70	5.50
GOOD	GOOD	GOOD	GOOD	BASIC

HARDWARE

Virtual Appliance Option	✓
Raw Storage *MAX*	1 TB
RAID	✗
Appliance Growth Options *TOTAL #*	4
Rated Throughput	> 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✗
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	14
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	1
Data Export Options *TOTAL #*	6
Report Distribution Interface(s)	✗
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	4
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	3
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	> 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	2
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	2
Software Agent Standard Inputs *TOTAL #*	13
Base Event Collection Rate	Up to 10,000 eps
Maximum Event Collection Rate	> 10,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	> 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	5
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	3
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	5 – 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✗
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✓
Tuning Services *TOTAL #*	1
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	Not Disclosed
% Support Resolution w/o Escalation	Not Disclosed
% Support Resolution on 1st Contact	Not Disclosed
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✓
Instructor-led Training	✗
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

TIBCO LogLogic MX3025

Approximate Starting List Price: $25,000 – $50,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
78.91	6.66	14.10	50.05	8.10
GOOD	BASIC	GOOD	GOOD	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	4 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	Up to 1,000 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✓
# of Monitored Systems *SINGLE APPLIANCE*	Up to 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	20
Base Event Collection Rate	Up to 1,000 eps
Maximum Event Collection Rate	Up to 5,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 2,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	4
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	2
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	> 90%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✗
Professional Training Included in Support Contracts	✗
Web-based Training	✗
Instructor-led Training	✗
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

TIBCO LogLogic MX4025

Approximate Starting List Price: $50,000 – $75,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
83.77	9.32	14.10	52.25	8.10
EXCELLENT	EXCELLENT	GOOD	EXCELLENT	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	8 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	4
FIPS 140-2	✓
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✓

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	15
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	2
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP, HTTP, HTTPS
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	4
Distributed Search	✓
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	> 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	11
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	2
Software Agent Data Compression	✓
Software Agent Data Encryption	✓
Software Agent Remote Installation	✓
Software Agent Remote Update	✓
Software Agent Configurable	✓
Software Agent Remotely Configurable	✓
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	20
Base Event Collection Rate	Up to 5,000 eps
Maximum Event Collection Rate	Up to 10,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 5,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	4
Stored Log Compression Ratio	8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	2
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	5 – 10 hours
Est. Current Installation Base	> 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	> 90%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✗
Professional Training Included in Support Contracts	✗
Web-based Training	✗
Instructor-led Training	✗
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Trustwave LME 2-10

Approximate Starting List Price: $10,000 – $25,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
65.46	6.36	12.70	37.60	8.80
BASIC	BASIC	BASIC	BASIC	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	9 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	Up to 500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	2
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	12
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	1
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	3
Distributed Search	✗
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 200
Concurrent Admin Logins	Up to 5
Supported Load Exceeded	Caching
Data Types *TOTAL #*	7
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✗
Software Agent Configurable	✗
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	15
Base Event Collection Rate	Up to 500 eps
Maximum Event Collection Rate	Up to 1,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	4
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✗
Instructor-led Training	•
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Trustwave LME 2-20

Approximate Starting List Price: $25,000 – $50,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
65.66	6.36	12.70	37.80	8.80
BASIC	BASIC	BASIC	BASIC	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	9 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	Up to 500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	2
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	12
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	1
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	3
Distributed Search	✗
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 200
Concurrent Admin Logins	Up to 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	7
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✗
Software Agent Configurable	✗
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	15
Base Event Collection Rate	Up to 500 eps
Maximum Event Collection Rate	Up to 1,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	3
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✗
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Trustwave LME 2

Approximate Starting List Price: $50,000 – $75,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
65.76	6.36	12.70	37.90	8.80
BASIC	BASIC	BASIC	BASIC	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	9 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	Up to 500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	2
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	12
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	1
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	3
Distributed Search	✗
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 200
Concurrent Admin Logins	Up to 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	7
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✗
Software Agent Configurable	✗
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	15
Base Event Collection Rate	Up to 500 eps
Maximum Event Collection Rate	Up to 1,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	4
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✗
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Trustwave LME 3

Approximate Starting List Price: $50,000 – $75,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
68.52	7.22	12.70	39.80	8.80
BASIC	GOOD	BASIC	BASIC	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	18 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	Up to 2Gb/sec
Event Process Rate *MAX*	Up to 1,000 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	2
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	12
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	1
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	3
Distributed Search	✗
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 499
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	7
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✗
Software Agent Configurable	✗
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	15
Base Event Collection Rate	Up to 1,000 eps
Maximum Event Collection Rate	Up to 1,000 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	4
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✗
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Trustwave LME 4

Approximate Starting List Price: $75,000 – $100,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
71.16	9.16	12.70	40.50	8.80
BASIC	EXCELLENT	BASIC	BASIC	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	29 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	> 2Gb/sec
Event Process Rate *MAX*	Up to 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	2
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	12
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	1
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	3
Distributed Search	✗
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 999
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	7
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✗
Software Agent Configurable	✗
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	15
Base Event Collection Rate	Up to 2,500 eps
Maximum Event Collection Rate	Up to 2,500 eps

MANAGEMENT (CONTINUED)

# Devices w/o Performance Degradation	Up to 750
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	4
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✗
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

Trustwave LME 5

Approximate Starting List Price: $75,000 – $100,000

DCIG Scores and Rankings

OVERALL SCORE	Hardware	Software	Management	Support
74.96	11.26	12.70	42.20	8.80
GOOD	RECOMMENDED	BASIC	BASIC	GOOD

HARDWARE

Virtual Appliance Option	✗
Raw Storage *MAX*	44 TB
RAID	✓
Appliance Growth Options *TOTAL #*	1
Rated Throughput	> 2Gb/sec
Event Process Rate *MAX*	> 2,500 eps

SOFTWARE

Benchmarking From All Data	✓
Scheduled HTML Reports	✓
Dashboard Customizable	✓
Dashboard Updated in Real-Time	✓
Dashboard Drilldown Capabilities	✓
Dashboard Standard Browser Support	✓
Dashboard Technologies *TOTAL #*	1
Dashboard Mobile Platform	✗
Dashboard Mobile Platforms *TOTAL #*	✗
Canned Reports Built-in	✓
Customized Reports	✓
Basic (if/then) Event Correlation	✓
Cross-device Event Correlation	✓
Advanced Event Correlation	✓
Correlation Difficult Use Cases *TOTAL #*	2
FIPS 140-2	✗
Collector/Agent/Connector Local Cache	✓
Automated Backup Routines *BUILT-IN*	✗

✓ Supported ✗ Unsupported

MANAGEMENT

Licensing Options *TOTAL #*	1
Standard Basic SIEM Capabilities	12
Co-Admin Flexibility	✓
Access Control Options *TOTAL #*	1
Data Export Options *TOTAL #*	3
Report Distribution Interface(s)	SMTP
Custom Branded Reports	✓
Privileged User Logging	✓
Incident Management Options *TOTAL #*	6
Query Options *TOTAL #*	5
Query Audit History Options *TOTAL #*	3
Distributed Search	✗
Analyst Software Install Required	No
LDAP Authentication	✗
# of Monitored Systems *SINGLE APPLIANCE*	Up to 2,000
Concurrent Admin Logins	> 10
Supported Load Exceeded	Caching
Data Types *TOTAL #*	7
Agentless Log Collection	✓
Software Agent	✓
Software Agent Caching	✓
Limited Bandwidth *TOTAL #*	1
Software Agent Data Compression	✓
Software Agent Data Encryption	✗
Software Agent Remote Installation	✓
Software Agent Remote Update	✗
Software Agent Configurable	✗
Software Agent Remotely Configurable	✗
Database DBA Logging *TOTAL #*	4
Software Agent Standard Inputs *TOTAL #*	15
Base Event Collection Rate	Up to 5,000 eps
Maximum Event Collection Rate	Up to 5,000 eps

MANAGEMENT (CONTINUED)

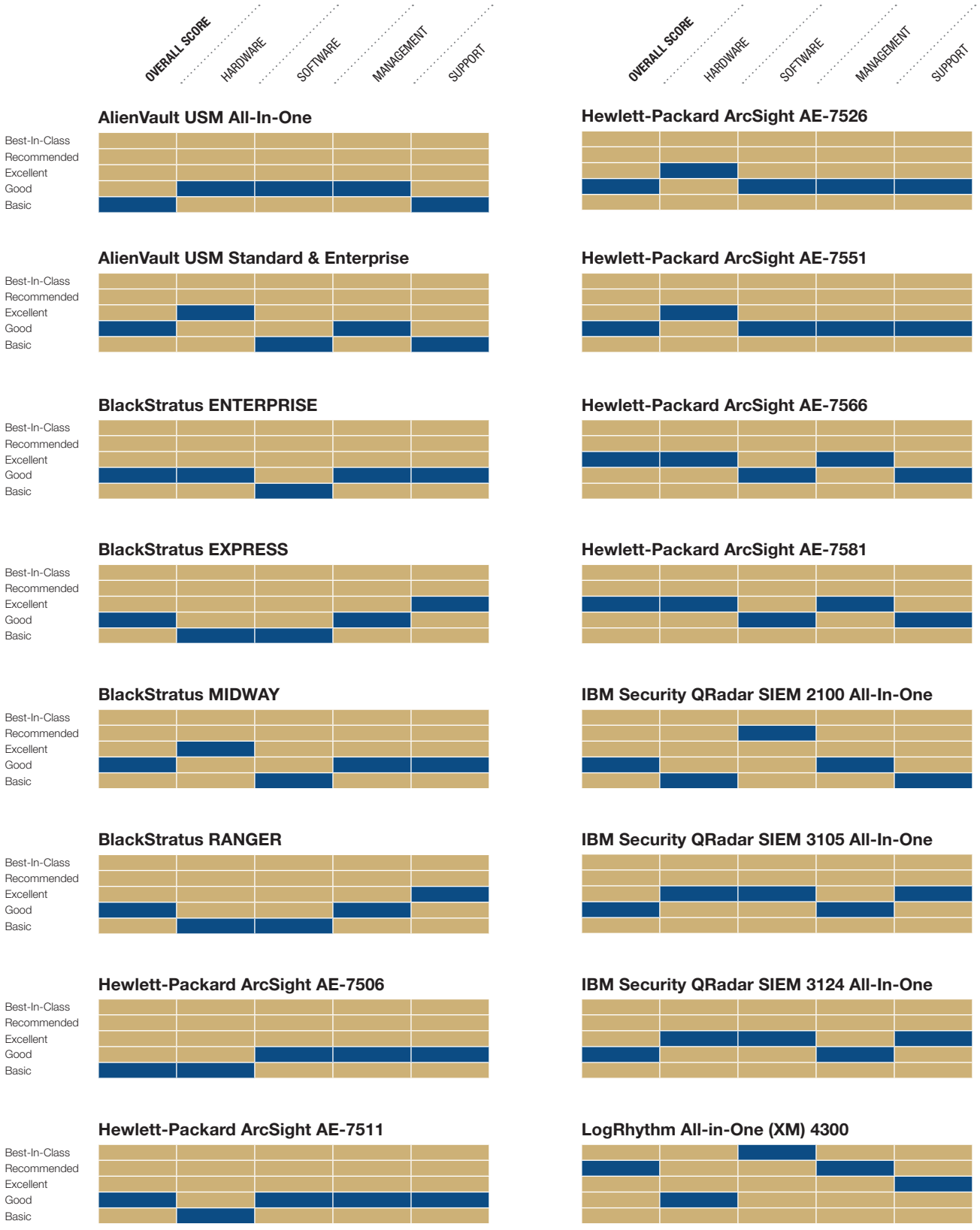
# Devices w/o Performance Degradation	Up to 2,000
Automatic Hotlist Updates	✓
Correlation Rule Updates Provided	✓
Log Time Stamp Normalization	✓
Real-Time Actions *TOTAL #*	4
Stored Log Compression Ratio	> 8:1
Raw Log Storage Format(s) *TOTAL #*	1
Raw Data Archival	✓
Log Data Protection Options *TOTAL #*	1
Normalized and Raw Data Accessibility	✓
Search Results Drilldown	✓
Content Package Updates *TOTAL #*	6

SUPPORT

Recom'd Training for Install	2 – 5 hours
Recom'd Training *MANAGE & MAINTAIN*	> 10 hours
Est. Current Installation Base	Up to 1,000 customers
Hardware/Software Asset Management	✓
Alerting Mechanisms *TOTAL #*	1
Common Criteria Validation	✓
DISA UC Approved Product	✗
Tuning Services *TOTAL #*	4
24x7x365 Telephone	Part of Support Contract
New Software Versions	Incl. in Support Contract
Support Performance Tracking	✓
% Support Resolution w/o Escalation	71 – 80%
% Support Resolution on 1st Contact	71 – 80%
Professional Training Available	✓
Professional Training Included in Support Contracts	✗
Web-based Training	✗
Instructor-led Training	✓
Product Certification	✗

©2014 DCIG, LLC. All rights reserved. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. The information, product recommendations and opinions made by DCIG, LLC are based upon public information and from sources that DCIG, LLC believes to be accurate and reliable.

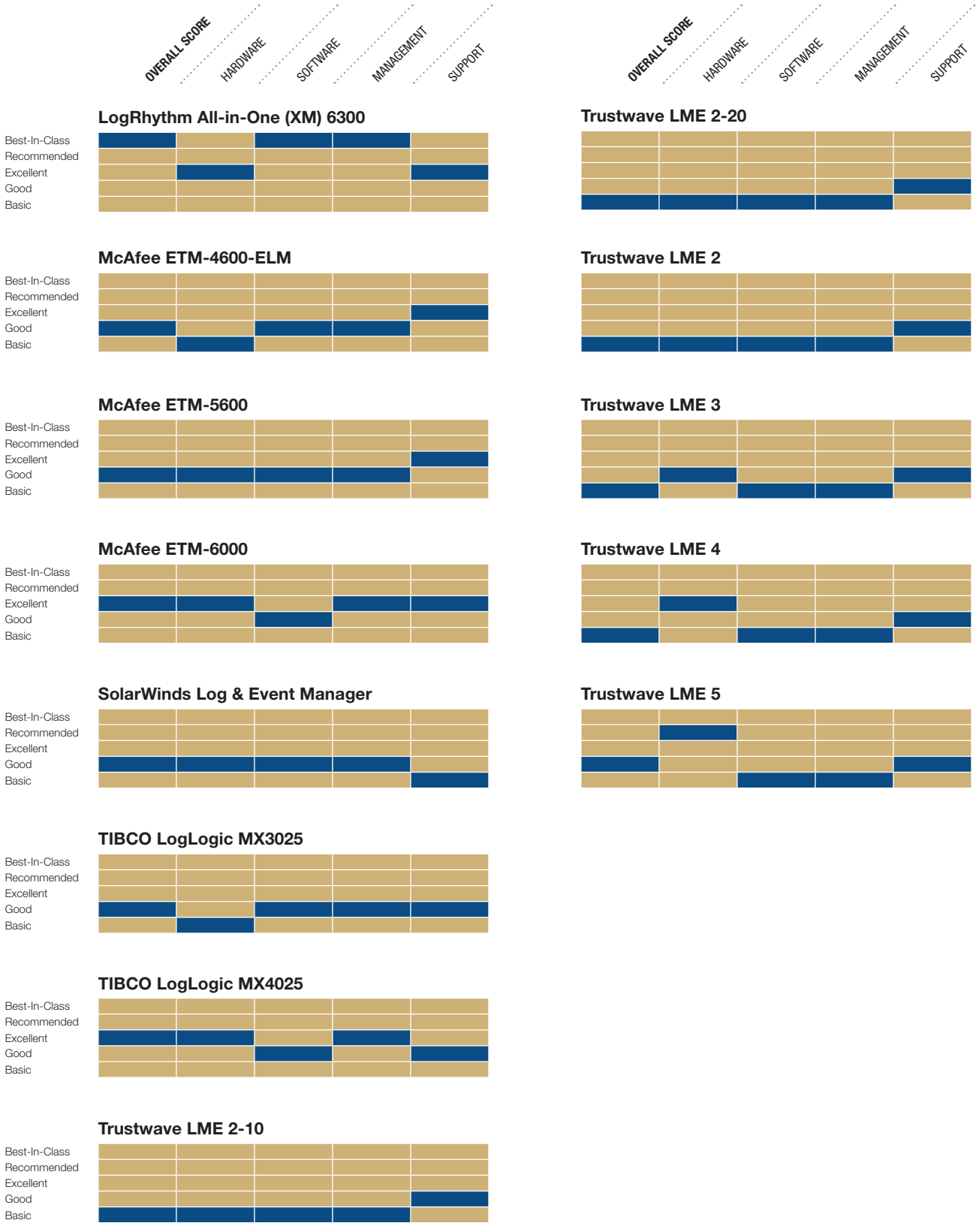
Product Rankings Dashboard



continued on next page

© 2014 DCIG, LLC. All rights reserved.

Product Rankings Dashboard (continued)



© 2014 DCIG, LLC. All rights reserved.

APPENDICES

© 2014 DCIG, LLC. All rights reserved.

Definitions, Explanations and Terminology

This section contains brief definitions and/or explanations of the terms used when developing the data sheets found in the *DCIG 2014-15 Security Information and Event Management (SIEM) Appliance Buyer's Guide.*

Hardware

Virtual Appliance Option

Indicates whether or not this appliance is available as a virtual appliance, in addition to a physical appliance.

Raw Storage MAX

The number of terabytes of raw data storage available within the appliance.

RAID

Indicates whether or not the appliance includes built-in disk/storage redundancy.

Appliance Growth Options (TOTAL #)

Indicates the number of options available for expansion and growth without appliance replacement. For a detailed list of exactly which growth options are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Rated Throughput

Indicates the maximum network throughput supported by the appliance.

Event Process Rate (MAX)

Indicates the maximum number of events that can be processed by the appliance, noted as events per second (eps).

Software

Benchmarking From All Data

Indicates whether or not the SIEM appliance has the ability to create benchmarks from all network data, including types of data, amount of data, and origin/destination information.

Scheduled HTML Reports

Indicates whether or not the SIEM appliance supports scheduled HTML reports.

Dashboard Customizable

Indicates whether or not dashboards are customizable within the SIEM appliance.

Dashboard Updated in Real-Time

Indicates whether or not dashboards operate/update in real-time.

Dashboard Drilldown Capabilities

Indicates whether or not dashboards within the SIEM appliance provide drill down capabilities.

Dashboard Standard Browser Support

Indicates whether or not web-based dashboards for this SIEM appliance are accessible with a standard browser.

Dashboard Technologies (TOTAL #)

Indicates which technologies drive the SIEM appliance dashboard. For a detailed list of exactly which dashboard technologies are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Dashboard Mobile Platform

Indicates whether or not the SIEM appliance dashboard supports mobile device access and manipulation.

Dashboard Mobile Platforms (TOTAL #)

Indicates which mobile device platforms are supported natively by the SIEM appliance. For a detailed list of exactly which dashboard mobile platforms are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Canned Reports Built-in

Indicates whether or not the SIEM appliance includes standard (canned) reports built-in.

Customized Reports

Indicates whether or not the SIEM appliance supports the creation and distribution of customized reports.

Basic (if/then) Event Correlation

Indicates whether or not the SIEM appliance supports basic correlation (e.g. identify a known "Bad" using if/then statements).

© 2014 DCIG, LLC. All rights reserved.

Appendix A—Definitions, Explanations and Terminology (continued)

Cross-device Event Correlation

Indicates whether or not the SIEM appliance supports cross device correlation (e.g. events from system x and y can be matched no matter where they were collected).

Advanced Event Correlation

Indicates whether or not the SIEM appliance supports or employs advanced correlation across reporting devices (immediate and over time, referencing host, referencing application, vulnerabilities, asset information, exclusion/inclusion lists, and previous rule output all with "if/then/else" logic).

Correlation Difficult Use Cases (TOTAL #)

Indicates the total number of difficult use-cases for correlation that the SIEM appliance supports. For a detailed list of exactly which difficult use-cases are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

FIPS 140-2

Indicates whether or not the SIEM appliance supports a FIPS 140-2 certified configuration.

Collector/Agent/Connector Local Cache

Indicates whether or not the SIEM appliance event collector/agent/connector keeps a local cache of events so that events are not lost in case of application or connectivity issues.

Automated Backup Routines (built-in)

Indicates whether or not automated backup routines are built into the SIEM appliance.

Management

Licensing Options (TOTAL #)

Indicates the number and types of licensing options that are available for the appliance. For a detailed list of exactly which licensing options are supported and available, please access the DCIG Interactive Buyer's Guide *(IBG).*

Standard Basic SIEM Capabilities (TOTAL #)

Indicates the number of basic SIEM capabilities that are built into the appliance. For a detailed list of exactly which basic SIEM capabilities are built into the appliance, please access the DCIG Interactive Buyer's Guide *(IBG).*

Co-Admin Flexibility

Indicates whether or not the appliance allows different teams to view different metrics through the same console (e.g. netflow data, bandwidth statistics, number of incidents, etc.).

Access Control Options (TOTAL #)

Indicates the number of appliance access control options that are supported. For a detailed list of exactly which access control options are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Data Export Options (TOTAL #)

Indicates the number of ways in which data may be exported by the SIEM appliance. For a detailed list of exactly which data export options are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Report Distribution Interface(s)

Lists the report distribution interface options supported by the SIEM appliance.

Custom Branded Reports

Indicates whether or not the SIEM appliance supports the ability for customers to upload business graphics and create custom-branded reports.

Privileged User Logging

Indicates whether or not all user and privileged user account (e.g. admin) actions are logged and monitored within the SIEM appliance.

Incident Management Options (TOTAL #)

Indicates the total number of options available for the SIEM appliance to serve as an incident management tool. For a detailed list of exactly which incident management options are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Query Options (TOTAL #)

Indicates the number of query type options are available within the SIEM appliance. For a detailed list of exactly which query type options are available within the SIEM appliance, please access the DCIG Interactive Buyer's Guide *(IBG).*

Query Audit History Options (TOTAL #)

Indicates the number of detailed query execution audit history options that are available. For a detailed list of exactly which query execution audit history options are available, please access the DCIG Interactive Buyer's Guide *(IBG).*

Distributed Search

Indicates whether or not the SIEM appliance supports distributed search across multiple data stores.

© 2014 DCIG, LLC. All rights reserved.

Appendix A—Definitions, Explanations and Terminology (continued)

Analyst Software Install Required
Indicates whether or not the analyst interface requires software to be installed on their workstation(s).

LDAP Authentication
Indicates whether or not the SIEM appliance supports LDAP integration for authentication.

# of Monitored Systems (SINGLE APPLIANCE)
Indicates the total number of systems that can be monitored by a single SIEM appliance, before the need to integrate additional appliances.

Concurrent Admin Logins
Indicates the number or simultaneous administrator logins that are supported by the SIEM appliance.

Supported Load Exceeded
Indicates how the SIEM appliance handles peak loads above those supported by the appliance itself.

Data Types (TOTAL #)
Indicates the number of data types supported by the SIEM appliance (in addition to standard log data). For a detailed list of exactly which data types are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Agentless Log Collection
Indicates whether or not the SIEM appliance supports agentless options for log collection.

Software Agent
Indicates whether or not the SIEM appliance can be supported by software agents that are installed on systems.

Software Agent Caching
Indicates whether or not the SIEM appliance software agent is able to cache events locally in case of network or system outage.

Limited Bandwidth (TOTAL #)
Indicates the total number of methods that are supported by the SIEM appliance to handle limited bandwidth situations. For a detailed list of exactly which limited bandwidth support options are available, please access the DCIG Interactive Buyer's Guide *(IBG).*

Software Agent Data Compression
Indicates whether or not the software agent is able to compress data being forwarded to the SIEM appliance.

Software Agent Data Encryption
Indicates whether or not the software agent is able to encrypt data being forwarded to the SIEM appliance.

Software Agent Remote Installation
Indicates whether or not the software agent can be installed without physical access to the system (if deployed as a server resident software package).

Software Agent Remote Update
Indicates whether or not the software agent software can be updated from a centralized management system within the SIEM appliance.

Software Agent Configurable
Indicates whether or not the software agent has configuration options.

Software Agent Remotely Configurable
Indicates whether or not configuration settings for the software agent can be updated from a centralized management system within the SIEM appliance.

Database DBA Logging (TOTAL #)
Indicates which SQL and file system-based sources for which the software agent supports database administrator (DBA) logging. For a detailed list of exactly which SQL and file system-based sources are supported by the SIEM appliance, please access the DCIG Interactive Buyer's Guide *(IBG).*

Software Agent Standard Inputs (TOTAL #)
Indicates which standard data inputs are supported by the software agent. For a detailed list of exactly which standard data inputs are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Base Event Collection Rate
Indicates the base collection rate supported by the SIEM appliance in terms of events per second (eps).

Maximum Event Collection Rate
Indicates the maximum collection rate supported by the SIEM appliance in terms of events per second (eps).

 # Devices w/o Performance Degradation
Indicates the number of devices supported by a single SIEM appliance for event collection without performance degradation.

© 2014 DCIG, LLC. All rights reserved.

Appendix A—Definitions, Explanations and Terminology (continued)

Automatic Hotlist Updates

Indicates whether or not the SIEM vendor provides automatic hotlist updates for the SIEM appliance and whether or not the SIEM appliance supports this feature.

Correlation Rule Updates Provided

Indicates whether or not the SIEM vendor provides correlation rule updates for the SIEM appliance and whether or not the SIEM appliance supports this feature.

Real-Time Actions (TOTAL #)

Indicates that number of specific actions that can be initiated by the SIEM appliance, based upon real-time alerts. For a detailed list of exactly which actions can be initiated, please access the DCIG Interactive Buyer's Guide *(IBG).*

Stored Log Compression Ratio

Indicates the compression ratio used by the SIEM appliance for log storage.

Raw Log Storage Format(s) (TOTAL #)

Indicates the total number of raw log storage formats supported by the SIEM appliance. For a detailed list of exactly which storage formats are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Raw Data Archival

Indicates whether or not the SIEM appliance archives all of the data it receives in raw form.

Log Data Protection Options (TOTAL #)

Indicates the number of options that are available to protect log data in storage. For a detailed list of exactly which protection options are available, please access the DCIG Interactive Buyer's Guide *(IBG).*

Normalized and Raw Data Accessibility

Indicates whether or not there is accessibility to internal, centralized log sources, in normalized and raw form.

Search Results Drilldown

Indicates whether or not the SIEM appliance supports the ability to drilldown into raw log data from search results.

Content Package Updates (TOTAL #)

Indicates the total number of content package update types are available for this SIEM appliance. For a detailed list of exactly which content packages are available for this SIEM appliance, please access the DCIG Interactive Buyer's Guide *(IBG).*

Support

Recom'd Training for Install

Indicates the recommended number of training hours for internal technical staff prior to installation of the SIEM appliance.

Recom'd Training (MANAGE & MAINTAIN)

Indicates the recommended number of training hours for internal technical staff to manage and maintain the SIEM appliance in the first year.

Est. Current Installation Base

Indicates the estimated number of customers who use this SIEM appliance.

Hardware/Software Asset Management

Indicates whether or not the SIEM appliance can be used to maintain an up-to-date hardware and software asset database.

Alerting Mechanisms (TOTAL #)

Indicates the number of alerting mechanisms that are natively supported by the SIEM appliance. For a detailed list of exactly which alerting mechanisms are supported, please access the DCIG Interactive Buyer's Guide *(IBG).*

Common Criteria Validation

Indicates whether or not the SIEM appliance is common criteria validated.

DISA UC Approved Product

Indicates whether or not the SIEM appliance is listed on the DISA Unified Capability Approved Product List.

Tuning Services (TOTAL #)

Indicates whether or not and how tuning services are made available to customers. For a detailed list of exactly which tuning services are supported, please access the DCIG Interactive Buyer's Guide *(IBG)*.

24x7x365 Telephone

Indicates whether or not 24x7x365 telephone support is available for the SIEM appliance.

New Software Versions

Indicates whether new versions of software are available free of charge or are included as part of a standard support contract.

© 2014 DCIG, LLC. All rights reserved.

Appendix A—Definitions, Explanations and Terminology (continued)

Support Performance Tracking

Indicates whether or not the SIEM manufacturer tracks customer support metrics.

% Support Resolution w/o Escalation

Indicates the percentage of support contacts that result in resolution without escalation to a 2nd level (or higher) support engineer.

% Support Resolution on 1st Contact

Indicates the percentage of support contacts that result in a resolution on the first call/contact.

Professional Training Available

Indicates whether or not professional product training is available for the SIEM appliance.

Professional Training Included in Support Contracts

Indicates whether or not professional product training is included in standard support contracts.

Web-based Training

Indicates whether or not Web-based training is available for the SIEM appliance.

Instructor-led Training

Indicates whether or not instructor-led training is available for the SIEM appliance.

Product Certification

Indicates whether or not professional, product-specific certification is available for professionals who support the SIEM appliance.

© 2014 DCIG, LLC. All rights reserved.

Appendix B—Vendor Contact Information

Vendor Contact Information

AlienVault, Inc.
1875 S. Grant Street, Suite 200
San Mateo, CA 94402
http://www.alienvault.com/
Phone: +1.650.713.3333

BlackStratus
1551 South Washington Avenue, Suite 401
Piscataway, NJ 08854
http://blackstratus.com
Phone: +1.732.393.6000
Phone: +1.866.525.5666
Email: info@blackstratus.com

Hewlett-Packard Corporation
3000 Hanover Street
Palo Alto, CA 94304
http://www.hp.com
+1.866.625.0242

IBM Corporation
1 New Orchard Rd
Armonk, NY 10504-1722
http://www.ibm.com/storage
+1.800.426.4968
Email: callserv@ca.ibm.com

LogRhythm, Inc.
4780 Pearl East Circle
Boulder, CO 80301
https://www.logrhythm.com
+1.303.413.8745
Email: info@logrhythm.com

McAfee, Inc.
2821 Mission College Blvd.
Santa Clara, CA 95054
http://www.mcafee.com
+1.866.622.3911

SolarWinds, Inc.
3711 South MoPac Expressway
Building Two
Austin, TX 78746
http://www.solarwinds.com
+1.866.530.8100

TIBCO Software Inc.
TIBCO LogLogic
3307 Hillview Avenue
Palo Alto, CA 94304
http://www.tibco.com
+1.650.846.1000

Trustwave Holdings, Inc.
70 W. Madison St., Suite 1050
Chicago, IL 60602
http://www.trustwave.com
+1.312.873.7500

© 2014 DCIG, LLC. All rights reserved.

Appendix C—Author Contact Information

Author Contact Information

DCIG, LLC
7511 Madison Street
Omaha, NE 68127
+1.402.884.9594

FRSecure
141 W 1st Street
Waconia, MN 55387
+1.888.676.8657

CONTACT
Evan Francen
frsecure@dcig.com

Jerome Wendt
jerome.wendt@dcig.com

WEBSITE
www.dcig.com
www.frsecure.com

© 2014 DCIG, LLC. All rights reserved.