

Essential Questions for Evaluating ESM Solutions

Security and Compliance Management. Redefined.



Essential Questions for Evaluating ESM Solutions

Table of Contents

- Introduction..... 3**
- Question 1: Data Sources 4**
- Question 2: Correlation 5**
- Question 3: Context 5**
- Question 4: Reporting 6**
- Question 5: Collaboration..... 6**
- Question 6: Investigative Analysis 7**
- Question 7: Data Archival..... 8**
- Question 8: Scalability 8**
- Question 9: Performance..... 9**
- Question 10: Total Cost of Ownership 9**
- Summary..... 10**
- Exhibit A: Security Solution Checklist..... 11**



Essential Questions for Evaluating ESM Solutions

Introduction

You are in the market for a security management solution and you're probably more than a little bewildered by complex product features and wide-ranging vendor claims. This document is offered as an evaluation tool to help you navigate the security management marketplace by quickly drilling into key questions that will help you address vendor claims.

In case you hadn't noticed yet, nearly identical acronyms abound in the security management market. Before proceeding, let's first dispel any acronym confusion by defining SIM, SEM, SIEM and ESM. Gartner Group defines the first three as follows:

- SIM – security information management provides reporting and analysis of data primarily from host systems and applications, and secondarily from security devices to support security policy compliance management, internal threat management and regulatory compliance initiatives. SIM can be used to support the activities of the IT security, internal audit and compliance organizations.
- SEM – security event management improves security incident response capabilities. SEM processes near-real-time data from security devices, network devices and systems to provide real-time event management for security operations. SEM helps IT security operations personnel be more effective in responding to external and internal threats.
- SIEM – security incident and event management is a market that is driven by customer needs to analyze security event data in real time (for threat management, primarily focused on network events), and to analyze and report on log data (for security policy compliance monitoring, primarily focused on host and application events).

In this document, we use the term ESM or enterprise security management because ESM solutions typically incorporate all SIM, SEM and SIEM aspects.

Many of the ESM solutions available today are complex offerings backed by hard-to-prove claims. This can make a product evaluation quite a daunting task, but knowing the right questions to ask during the process will help you evaluate ESM alternatives in a timely and justifiable fashion. The following ten topics present questions and answers that will help you select the best ESM solution for your organization's Network Operations Center (NOC), Security Operations Center (SOC) and Audit teams.

NOTE: [Exhibit A](#) presents these topics in a handy checklist that you can use as a reference during your ESM solution evaluation.



Question 1: Data Sources

Does the ESM solution collect data besides log data, such as vulnerability, configuration, asset, performance or NetFlow data?

Most ESM solutions collect, archive and analyze log and vulnerability data from network devices (hosts, servers, workstations, applications). While collecting and analyzing this data is, in fact, a great starting point for an ESM solution, it becomes vastly more meaningful when examined alongside other gathered security data.

Consider the TJX Companies' breach of 2006 and 2007. It is widely known that TJX used an ESM solution to analyze log and vulnerability data. As such, the solution did not allow TJX SOC and NOC analysts to look beyond this limited data set to view other critical security information that would have revealed configuration, asset and behavioral changes, prohibited access to applications, unauthorized creation of new accounts and more. The TJX lesson is clear: a solution that builds on log and vulnerability data by collecting this data from other data silos such as configuration, asset, performance and NetFlow information will deliver a superior ability to identify and remediate sophisticated and complex breaches such as identity and information theft.

Some ESM solutions are also deployed for IT governance, risk and compliance management and a company concerned with best practices and regulations like PCI DSS, COBIT or SOX should mandate that an ESM solution collect and analyze all security and compliance data across the enterprise. Given evolving security and compliance challenges, the ESM solution you select must have the ability to collect and analyze:

- **Log data**, a fundamental data type for security event detection and analysis
- **Configuration data** with periodic snapshots across network devices and hosts
- **Asset data** on all devices and hosts including hardware and software system specs, applications and processes
- **Performance data** such as network traffic and CPU utilization
- **Vulnerability data** across network devices and hosts
- **NetFlow data** that provides information on network and application resources and user behavior



Question 2: Correlation

Does the ESM solution automatically correlate all data collected from multiple silos in real time over an extended time period?

It is essential that any organization serious about detecting newly evolving, targeted security threats such as identity theft and meeting audit regulations think strategically when evaluating ESM solutions. Meeting security and compliance challenges requires a solution that not only collects multiple silos of data across the enterprise, but also effectively correlates all data collected in real time. If an ESM solution only correlates data once a day rather than around the clock in real time, hours that could be spent detecting and mitigating an attack disappear.

For continuous support, it is also important that data be collected over extended periods of time. If an ESM only correlates data collected over a few days, there is limited historical data to compare the new real-time data against and the correlation may miss slowly evolving, methodical attacks. Thus, only with a correlation engine that performs continuous, real-time analysis of long-term data from multiple data silos can an ESM solution automatically “connect the dots” to quickly mitigate attacks.

Question 3: Context

Does the ESM solution provide a complete context for breaches, incidents and events?

Rapid attack detection is possible only if the ESM solution is able to provide a complete context for each security event. This is accomplished by performing real-time correlation of all security data from multiple data silos over extended periods of time. Furthermore, the ESM solution should provide this complete context in a single console so that, with the click of a button, an analyst can view all relevant data around an incident or breach in one drilldown screen.

Again, because of their limited focus on log and vulnerability data, most of the ESM solutions available today lack the ability to provide complete context. As a result, analysts are forced to use a “swivel-chair approach”. This approach relies on manual management and analysis of multiple point solutions, making it nearly impossible to obtain the complete context of an incident.



Question 4: Reporting

Does the ESM solution deliver all the reports that it advertises as out of the box? Do the reports provide useful, actionable information? Do the reports capture all security and compliance metrics?

As a fundamental ESM solution component, reporting should comprehensively meet the differing requirements of NOC, SOC and Audit teams. These teams typically mandate that ESM reports be useful and actionable, incorporate all important security and compliance data, and be out-of-the-box accessible in different formats based on role. Let's briefly examine each of these requirements in more detail.

Reports should be useful and actionable, presenting a high-level summary of all security and compliance data so a manager or an analyst can immediately see the big picture and understand the context. It should then provide the ability to easily drilldown into more detail to quickly determine root cause.

To be cost-effective, the ESM solution should also provide out-of-the-box reports. Many vendors claim—often in obfuscating terms—that their ESM solutions include a variety of reports. Their customers, however, soon discover only a small set of reports are provided out of the box and the generation of additional reports requires custom coding. This can prove costly as customers are often forced to write their own SQL queries or hire the vendor's professional services to get the reports they need.


As a complement to its ability to report data across all silos, an ESM solution should deliver reports based on user role. That is, the solution should allow a user, regardless of team affiliation, to access the solution and obtain a report of data meaningful to them from anywhere at anytime based on the privileges assigned to the user's role. Finally, the solution should provide report generation flexibility that supports automated report generation and delivery in various formats such as HTML and PDF.

Question 5: Collaboration

Does the ESM solution enable efficient collaboration between NOC, SOC and Audit teams? Can different teams view different metrics through the same console?

Rapid threat analysis and mitigation requires collaboration between NOC, SOC and Audit teams. An effective ESM solution, therefore, should encourage collaboration between different teams so the root cause of a threat can be determined in seconds or minutes instead of in weeks, months or never.

This is often easier said than done. In their quest to stay ahead of a changing environment, IT departments have historically created specialized NOC and SOC teams to manage increasingly



sophisticated threats, evolving regulations and new reporting mandates. These teams continually deploy point solutions that are complemented by best practices to meet the requirements of each area independently. This results in separate silos of incompatible data that hinder effective cross-functional decision making.

If information from all important security and compliance data silos is combined into an integrated solution or platform and then presented to multiple teams through a single console, overall collaboration can be accomplished. In this case, solution access can easily be granted based on the user's role—be they a NOC, SOC or Audit team member—so they can look at the data in different ways to meet individual requirements.

As with reporting, the solution dashboard should also be customizable to meet varying needs. For example, a NOC team member should be able to obtain operational metrics through the console while an SOC team member uses the dashboard to view security metrics. In this way, different teams can effectively collaborate by viewing different metrics through the same interface. A solution that allows all teams to look at the same data collaboratively removes obstacles to resolving problems collaboratively and expeditiously.

Question 6: Investigative Analysis

***Does the ESM solution enable investigative forensic analysis across multiple data silos?
How quickly can the security analyst determine the root cause of an incident or event?***

An effective ESM solution must also enable investigative forensic analysis by multiple teams across all the data silos: log, vulnerability, configuration, asset, performance and NetFlow. In their investigative analysis of an evolving security incident, the teams should be able to move easily between these silos to view—in a single console—all related and relevant data. This requires data integration enabled by a single platform that collects, correlates and analyzes all relevant security and compliance data.

The forensics search function of an ESM solution should allow an analyst to easily search through terabytes of archived data for any parameter. It should also include search-on-search functionality so the analyst can refine a query to zero-in on the root cause quickly. Finally, the ESM solution should provide a mechanism to export results for evidentiary purposes.



Question 7: Data Archival

Does the ESM solution archive all data? Does the ESM solution encrypt and archive data? Does the solution use existing SAN, NAS or DAS storage media?

Whether incident investigation reveals a real attack from an external hacker or an inadvertent policy violation by an internal user, the ESM solution must archive the collected multi-silo data for correlation, analysis and reporting *without* creating a new storage management headache. That means the ESM solution should take advantage of the existing storage infrastructure by archiving data on any storage media whether it be DAS, NAS or SAN.

Of course, in a large enterprise network, the data generated over months and across thousands of nodes can be quite voluminous. So to save storage space and enhance data security, an ESM solution should support compression and encryption of all the data collected over long periods of time. In short, when evaluating an ESM solution's data archival features, you should look for the ability to:

- **Compress** all data to use storage space efficiently
- **Encrypt** all data to maintain data integrity
- **Piggyback** on existing DAS, NAS and SAN infrastructures for data archival
- **Archive** all data for long time periods.

This set of archiving features allows your company to cost-effectively meet security, compliance and audit management requirements.

Question 8: Scalability

How scalable is the ESM solution? Does it scale to support thousands of nodes that are geographically distributed?

In a large scale infrastructure, it is common to see tens of thousands of syslog events per second and NetFlow volumes in the hundreds of thousands of flows per second. Given such a large volume, it is essential that the ESM solution you select be able to scale and simultaneously process data from thousands of nodes. An ESM solution that can be deployed in a distributed architecture is more apt to meet this requirement by maintaining the following capabilities while scaling to cover large, geographically-disbursed networks:

- **Processing and archiving** the data over long periods of time
- **Collecting** all important data across the entire infrastructure to meet security, compliance and audit requirements
- **Correlating, analyzing and reporting** on all data concurrently and in real time



To be cost-effective, this scalability should not come at significant incremental expense such as the cost to add a dedicated DBA to manage the additional data collected as network coverage expands. Rather, the solution should support a self-data management capability. It should also have a built-in ability to adapt to new log formats and, thereby, avoid the expense of custom programming to handle new data formats as the scope of the ESM extends to new types of network nodes.

Question 9: Performance

How is ESM solution performance impacted with an increasing number of nodes and aging of data?

In information security, time is vulnerability so a useful ESM solution needs to collect, analyze and report on all data at a very high-performance rate. In addition, that high-performance rate should not degrade significantly over time or as more nodes are added to the scope of the deployment. Most ESM solutions on the market today exhibit performance degradation resulting from database insert rate limitations. This is why it is crucial that an ESM solution be scalable and not be bound by the insert rate limitations of its database. The performance and report access speeds should be consistent across an increasing number of nodes and aging of the data.

Important ESM performance metrics to be examined include:


- **Standalone ESM server throughput** that reaches 15,000 analyzed events per second
- **Distributed ESM server performance scaling** that reaches performance levels of 100,000 events per second as additional servers are added.
- **Real-time, multi-silo ESM performance scaling** that handles the collection and analysis of data in real time from all the multiple data silos.

Question 10: Total Cost of Ownership

What is the true total cost of ownership (TCO) of the ESM solution? Does it require additional staff to manage? Does it require the purchase of other enterprise applications or data connectors? Does it require a license for each user?

The final consideration, critical to purchasing professionals, is total cost of ownership. As with most IT solutions, the initial deployment price typically comprises the smallest TCO component; the largest component is on-going support and professional services which, in the case of many ESM solutions, may include:

- **A dedicated DBA** – Many ESMs are based on a relational database which may require a dedicated database administrator. What type of database is used by the ESM and is a dedicated administrator required?

- 
- **Additional management staff for new nodes** – Additional people may be required to manage the ESM component on new nodes as they are added to the network and the scope of the ESM solution. Are the ESM node agents self-managing or do they require management?
 - **Custom connectors** – Adding an unsupported device to an ESM network often requires that a custom collector be created to collect syslog data from that device. Does adding an unsupported device require returning to the vendor for custom design work, or can it be easily done in-house?
 - **Additional applications** – Additional applications may be required to make an ESM solution truly useful across the enterprise. Examples of such additional applications include crystal report server and applications to report on vulnerability, asset, configuration or NetFlow data drawn from network nodes. Consider how your users will expect to deploy and use the application. Are any additional third-party applications required to make the ESM solution effective and useful?
 - **Additional licenses** – As nodes and associated users are added in the future, licensing cost can soar if they are licensed individually. Are users licensed in tiers or separately?
 - **Per User Access costs** – Some ESM solutions charge a per user access fee.

To eliminate or minimize these “hidden” expenses, you need an ESM solution that takes a broader, more integrated platform approach: an approach that supports both your security and compliance needs with sufficient flexibility to accommodate your enterprise IT growth without adding significant IT expense.

Summary

This document has provided you with an explanation of key topics and questions that will help you navigate the murky waters of an ESM solution evaluation. By following this guidance, your overall product analysis, understanding and recommendations should be more convincing and sound. The ESM solution that remains standing at the end of this evaluation should prove the best solution for your SOC, NOC and Audit teams. With it, comprehensive security and compliance management will be achievable through end-to-end data collection and correlation, rapid attack mitigation, fast root cause analysis, robust reporting capabilities, high performance and maximum scalability at a minimal TCO.

About eIQnetworks

eIQnetworks, Inc., a leader in integrated security, risk and audit management, enables enterprise, government and MSSP customers to effectively meet security and compliance challenges through a unified framework. More than 2,700 organizations worldwide rely on the power of eIQ’s enterprise security management and IT governance, risk and compliance solutions to proactively detect security breaches, speed incident remediation and support evolving best practices and compliance regulations across the enterprise. For additional information, please visit www.eIQnetworks.com or call +1 877.564.7787.

Exhibit A: Security Solution Checklist

Question Topic	Specific Questions	Notes
Question 1: Data Sources	<ul style="list-style-type: none"> • Log? • Vulnerability? • Configuration? • Asset? • Performance? • NetFlow? 	
Question 2: Correlation	<ul style="list-style-type: none"> • In real time? • Over long periods of time? • Across multiple silos? 	
Question 3: Context	<ul style="list-style-type: none"> • Complete context around security events? 	
Question 4: Reporting	<ul style="list-style-type: none"> • Out-of-the-box reports? • From all data sources? • Actionable, e.g., ability to drilldown? 	
Question 5: Collaboration	<ul style="list-style-type: none"> • Combine all data into a single, role-based console? • Provide access rights for NOC, SOC and audit teams? • Dashboard customization? 	
Question 6: Investigative Analysis	<ul style="list-style-type: none"> • Forensics across multiple data silos? • Ability to determine root cause quickly? 	
Question 7: Data Archival	<ul style="list-style-type: none"> • Archive all data? • Use existing DAS, NAS and SAN storage? • Encrypt and archive data? 	
Question 8: Scalability	<ul style="list-style-type: none"> • Does the solution scale well? • Thousands of geographically distributed nodes? 	
Question 9: Performance	<ul style="list-style-type: none"> • Events per second? • Impact of increasing number of nodes and age of data? 	
Question 10: Total Cost of Ownership	<ul style="list-style-type: none"> • Procurement cost? • Management cost? • Additional applications or connectors? • License needed for each user? 	

© 2008, eIQnetworks, Inc. eIQnetworks and the eIQnetworks logo are registered trademarks of eIQnetworks, Inc. All other trademarks, servicemarks, registered trademarks or registered servicemarks are the property of their respective owners. All rights reserved.