

White Paper



Planning and Executing
Enterprise Security Management

Planning and Executing Enterprise Security Management

Introduction

It is very easy to attempt to justify the purchase of a network security product by claiming that if it prevented just one major failure, the cost avoidance would more than cover the price of the product. In truth, there is certainly value in the security introduced by new products but this type of justification ultimately leads to an unrealistic expectation of a blank check. In today's climate of razor-thin operating margins and heavy competition for capital, the winning investment must not only increase protection, but also support clear business goals while demonstrating conclusive financial return on an operating basis.

Because there is a high threshold of justification for security investment, the adoption of comprehensive enterprise security management has greatly accelerated in the last year based on the clear ROI and increased protection that it provides. For large organizations with geographically-dispersed operations, security management means software that can consolidate, analyze and report on the millions of security events that they see each day so that the right actions can be taken at the right time. Industry analysts who advise clients on security technology report that security management has gone from a part-time interest to an active practice that now consumes their attention full time.

The emergence of ESM comes from many areas:

- ❖ New laws and regulations establishing goals and measurements for the security function
- ❖ Board-level concern over the validity of business data
- ❖ Expanding use of e-business techniques to drive revenue and profit
- ❖ The need to audit and report on the security function
- ❖ The increasing threat environment which drives the workload of the security staff

ArcSight has worked with a number of customers to identify not only the intrinsic security benefit of its products but also the real operational value of installing ArcSight solutions. This insight is captured in cases and examples so that new or prospective customers can easily establish the value of ArcSight's enterprise security management software.

Planning and Justifying the ESM Solution

Planning and preparation are critical to a successful implementation of an enterprise security management solution and the security function is often in the lead position in justifying the need and recommending a solution. Based on today's environment, the major preparation steps include:

1. Understanding the business objectives and how they drive security needs
2. Pinpointing the major security "stakeholders" within the organization and defining their major requirements
3. Projecting the security implications of strategic business initiatives
4. Identifying the resource and process bottlenecks that are reducing the efficiency and effectiveness of the security function
5. Preparing the ROI case for an ESM investment
6. Specifying the key features of an ESM solution

Items 1-3 are very specific to the organization but in general are based on the list of environmental factors listed in the Introduction section (above). Steps 4-6 are largely under the control of the security group.

Identifying and Calculating the Need for ESM

A customer ready for ArcSight typically is experiencing these problems:

- ❖ Extreme data overload from IDSes, firewalls, system logs, etc.
- ❖ A plethora of false positives that sap the security staff resources
- ❖ Under-utilized ("de-tuned") devices that have become that way because of the two previous problems
- ❖ Inefficient incident response due to poor tools and incomplete information
- ❖ Incomplete reporting that often consumes several days per month to supply the lines of business and senior management with the security summaries they need.

Each of these issues not only reduces the amount of protection that an organization experiences, but they also have a specific economic impact. By capturing the dollar value of solving these problems, a clear and pragmatic ROI calculation can be done with the benefit of ArcSight's improved security result as an added bonus. For examples of ROI calculations that are relevant to the overall ESM solution, see APPENDIX 2.

Finding the Right Solution

Sorting through the claims and comparisons of ESM software packages can be confusing and time-consuming. As a result, many organizations develop a checklist, or Request For Information process that is intended to generate a short list of options that will be investigated in more detail. Consequently, it is difficult to generalize a complete solution set that will apply equally in all circumstances. However, ArcSight has worked with many large organizations to define and implement ArcSight software and as a result can draw some conclusions about which areas are most important:

- ◆ **Enterprise Capabilities.** Enterprise Security Management software follows in the footsteps of Systems and Network Management solutions. Consequently, scalability and ease of deployment are important attributes of the solution. There are however, numerous difference between security management and the other management solutions. One is that security event traffic dwarfs what the other products must handle. It is not unusual to see several hundred security events per second in a fully-deployed security management solution, far greater than system or network management traffic. However, security management software can be an effective partner for other IT subsystems such as network management or job-ticketing systems by sending them only the most important security-related information and tasks. Another key difference is that a well-crafted security management solution should deploy within a matter of days and produce immediate results. It is no longer acceptable for enterprise-class solutions to require large amounts of consulting fees for installation and customization.
- ◆ **Correlation and Analytics.** The goal of a successful security management solution is to optimize the use of the most precious security resource-people. With millions of individual alarms and alerts flowing through the network each day, it is impossible for even the most experienced and expert group of security analysts to see and integrate the small number of events that constitute a true threat or attack. The security management software must have the ability to look across events, across vendors, across time to distill out those relatively few alarms and alerts that the security staff should investigate and resolve. A key tool in the analysis arsenal is real time correlation that performs as an expert system for the security staff by using its awareness of threatening trends and behaviors and the current vulnerability of the targeted asset to calculate a precise threat index.
- ◆ **Complete Process Coverage.** The position of a security analyst covers a wide range of activities, hence the security management software should map to those job functions. Comprehensive ESM software begins with the collection of 100% of the alarms and alerts that come from the various firewalls, intrusion detection systems and other sources of security-relevant information. Those events are then persisted in a relational database while they are processed by the correlation engine described above. A full range of display options provides the flexible views into security status that individual operators need and once an incident is identified, a fully-integrated case management system provides the mechanism to investigate and resolve it quickly. Equally important, the both the security staff and the organization at large can easily summarize and report on the security activity across the organization.

A quick summary of the key ESM software requirements is listed in Appendix 1.

APPENDIX 1. THE ESM RFI STARTER KIT

Security management used to mean setting up a few firewalls and installing anti-virus software. Now you have a global security infrastructure populated by many types of security devices from many different vendors. To deal with the resulting data overload, false alarms, multiple displays and isolated databases you need centralized, enterprise-class security management software.

Here's a starter list of requirements compiled from major corporations, government agencies, and service providers who have surveyed the market, tested the options and successfully implemented an ESM software solution on their way to increased protection, improved staff utilization and better reporting from their security function.

1. An architecture that can scale to handle constantly increasing workloads
2. Security device neutrality to manage best-of-breed infrastructure
3. Event correlation with cross-device real time alerts combined with asset vulnerability and asset value data
4. Multiple real time display options to support a Security Operations Center
5. One click switch between real time monitoring and forensic investigation.
6. Integration with network management systems and IT trouble ticket systems
7. Complete reporting infrastructure with both an authoring system and pre-configured reports
8. Full case management workflow to track incidents from notification to closure
9. 100% capture and normalization of raw alarms and alerts
10. Rapid installation with immediate results.

For more information about how ArcSight satisfies these requirements in addition to many other features and benefits for both the security function and organization at large, visit www.arcsight.com.

APPENDIX 2. ROI CASES

Scenario One: Event Consolidation Cuts Monitoring Overhead

Each security point product typically has its own console and log. Even with the trend for individual vendors to consolidate their devices into a single console, the heterogeneous nature of edge defense means that the security staff must juggle numerous data streams and formats. This means that every time a new device is installed, more staff resource is likely required to manage it.

One of the primary missions of ArcSight is to capture, normalize and store every event from every device in a database that the ArcSight Manager uses for analysis, display and reporting. With ArcSight, the security staff has a single unified view of the entire infrastructure together with the tools necessary to either drill down for more detail or summarize for purposes of reporting. ArcSight customers have indicated that each staff member can oversee and manage three times the number of devices than they could before the installation. This enables them to perform higher-value tasks such as incident response, security reconnaissance, and infrastructure update. From a financial standpoint, this means that security can be improved without additional staff.

An ArcSight customer is forecasting the installation of 50 IDS' and firewalls without the additional two senior staff members that previously would have been required, resulting in a savings of over \$100,000 per year.

Scenario Two: Correlation Dramatically Reduces False Positives

On a day-in, day-out basis, expert security professionals can spend hours working on an incident. If it is a false alarm, the effort is wasted. Factors that determine the specific cost associated with false positives include:

- ◆ The rate at which false positives are received
- ◆ The amount of time it takes to verify that it is false
- ◆ The level of individual required to do the analysis

Consider the organization that handles 10 incidents per day that are false alarms which the intrusion detection system or firewall could not properly identify. For example, an attack that only threatens Unix directed at an NT system. Based on testing and customer feedback, the ArcSight correlation and SmartRules engine typically reduces this kind of false positive by 80%. If it takes 30 minutes of a senior security analyst's time to resolve each incident, then the daily savings would be 4 hours per day or over 800 hours per year. Depending on the hourly rate of the security specialist, the yearly savings can exceed \$75,000.

Scenario Three: ArcSight Facilitates More Efficient Incident Response

Once the monitoring time and the false positives are reduced, the next point of efficiency is the investigation, resolution, and reporting for true threats and attacks. The ArcSight closed-loop incident response workflow has reduced the resolution time per incident by as much as 50%. This is accomplished through a comprehensive Case Management system, an integrated Knowledge Base, and notification via console, pager or cell phone.

One area that has also yielded significant savings is the formal reporting that organizations do each month. Customers have found that two days of reporting activity per month have been reduced to two hours with the ArcSight Reporting System of pre-packaged and custom reports. This translates to a savings of up to \$25,000 per year.

Scenario Four: More Efficient Capital Expenditures

Even though security budgets are increasing there is still a need to stretch capital. With ArcSight organizations can utilize the most cost competitive and technologically advanced products without the worry of adding administrative or management overhead. Open-source security products such as Snort can be introduced in a controlled manner to ensure that they produce the desired results as monitored by the ArcSight management system.

The combination of competitive bidding and low-cost open source solutions have saved as much as 10% of a \$1 million security capital budget.

Summary

ArcSight delivers cost savings and improved security results in many different areas. Those that are highlighted in this document can lead to a payback for an ArcSight installation of 12 months or less. Each organization will have its own set of values to fit into the model but in every case the improved financial performance and increased security produce a compelling Return on Investment.