SANS ANALYST PROGRAM

Sponsored by McAfee

Data Protection Requirements Worksheets

A SANS Whitepaper – July 2009

Written by Barbara Filkins

Evaluation Criteria

How to Use These Worksheets

Instructions

Summary

Data-centric protections need to address data discovery and classification, incident workflow, policy creation/management and data movement detection. The breadth of the technology required to accomplish all of this is broad, covering:

- Fully-integrated encryption for end points for data in use, in motion and at rest within applications (e-mail, file servers, etc.), including sensitive data transferred onto portable storage devices
- Host-based DLP for localized detection and prevention of data leakage for data in use, data in motion, and data at rest
- Network DLP with data discovery and analysis, network monitoring (with extensive protocol and application parsing support), and prevention capabilities for both inbound and outbound content

How should a management team go about evaluating today's encryption and emerging data leakage prevention (DLP) tools? What questions should they ask of the vendor provider(s)? How does a management team determine which solution being proposed will meet the most requirements for today—and in the future? How do they even set requirements without due diligence and discovery technologies to assist in locating and classifying what it is they need to protect? How do they weigh specific business requirements to product features? How do they gauge the stability of the vendor? How do they compare pricing models (per user, per server) and such additional factors as growth potential and integration with other vendor products to optimize their investments?

Organizations need a way to map business needs against all these technological challenges. To help, SANS has developed the following interactive Data Protection Requirements Worksheet. In it, requirements have been organized into broad categories to include:

- Host/network data leakage protection and encryption (how the product functions)
- Management and support (how the product can be managed)
- Company profile and pricing (how viable the vendor is, what services it offers, and product pricing)

The following pages include our evaluation criteria and instructions for using the Data Protection Requirements Worksheet to compare data collected from potential vendors/providers against organizational requirements.

Evaluation Criteria

The Data Protection Worksheet is part of an Excel workbook that allows individual scoring of up to three vendors and the comparison of all three. When creating this workbook, we used the following elements to score a vendor:

1. **Scope/Priority:** This element is established by the organization, which assigns a weight to each requirement that demonstrates how important that requirement (or group of requirements) is to the organization. For example, A healthcare entity may not weigh requirements in a manner similar to a financial institution and vice versa. What are user population characteristics that define the organizational environment? Is the user population highly mobile, placing an emphasis on data at rest (smart phones/USB devices), data in motion (network), and data in use (files/folders)? Or, even though users are highly mobile, is the access to corporate resources via a thin client with little or no local storage, placing emphasis on data in motion (network) and data in use (cached files/folders, mobile devices)?
2. **Vendor Support:** How well are specific requirements supported by the vendor? This factor should directly influence the decision by the organization to acquire the product in terms of effort and risk for implementation. A score should be assigned with values ranging from a high for "standard" product support to zero for capabilities not supported in any way. (Values are explicitly defined in the following worksheet.) Desired product capabilities available "out of the box" should be scored the highest due to the savings recouped from minimal IT setup and administration.
3. **Availability:** Is the product currently able to meet requirements? Or, does it promise to deliver features in the future? An organization should be cautious in acquiring a product based on a vendor's promise of delivering capabilities in future releases. Organizations should consider the vendor's development roadmap against its own timelines for rolling out functionality and features. The organization then needs to apply weights to availability: Is requirement compliance demonstrable now, or is it close to being in production (i.e., 30 to 60 days from release)? Or would it be safer to think of that feature as being in beta (i.e., 60 days to 6 months)? Or, is it still on the drawing board, meaning it will be 6 months to a year before what is needed could be considered a releasable product?

So, for each requirement, calculate a score in the following way:

Scope x Support x Availability

The resulting scores are summed automatically with these calculations. The higher the score, the more closely the product will meet the needs of the organization. This worksheet also allows a side-by-side product comparison and scoring calculator.

How to Use These Worksheets

This complete Excel workbook, titled "Vendor Requirements Worksheets," is an interactive toolset that can be used to evaluate and compare the integrated DLP/encryption capabilities of up to three vendors. The workbook contains the following tabbed sections (or individual worksheets):

1. **Instructions:** Explains how to use this workbook to evaluate and compare up to three (3) vendors.
2. **Scoring Guidelines:** Describes the scoring, as presented above, to develop an overall vendor score, and contains the tables used to automate the scoring process on the subsequent interactive worksheet.
3. **Requirements, Vendor xx:** Provides scoring for an individual vendor based on vendor or evaluator completion of the interactive worksheet. Worksheet automatically calculates the score for each requirement, major groupings of requirements, and an overall score for that vendor.
4. **Requirements Summary:** Compares up to three vendors. Can be used to collect the results from the static vendor response sheet, or can be completed as described in the instructions below.
5. **Scorecard and Vendor Compare:** Compares up to three vendors in terms of summarizing the responses provided in the Requirements Summary worksheet.

Instructions

Use these worksheets to gather, input and compare features and comparisons of DLP/encryption vendors, SANS recommends the following:

1. Start by downloading the spreadsheet here:
   http://www.sans.org/reading_room/extras/data_protection_reqs.xls
2. Save a copy of this workbook under another name such as "DLP RFP_Vendorname."
   Disclaimer: Some of the worksheets in this workbook contain formulas that support the automated scoring of vendor responses. Be careful in cut and past of the response columns as outlined in the following steps. It is always a good practice to save the original spreadsheets under a different name so that you can return to them in the case of a misstep or mishap!
3. Take this workbook copy and delete the "Instructions,""Requirements Summary," and "Scorecard and "Vendor Compare" tabs. Or, if you'd rather, hide these tabbed pages and make this individual worksheet page the only part that's active. To do this, select "Format/Sheet/Hide" for each of the three sheets named above. (To unhide, select "Format/Sheet/Unhide" and select the name of the spreadsheet.)
4. You now have an individual requirements intake form that can be sent to a prospective vendor, copies of which can be sent to up to three vendors.
5. Upon receiving the completed checklists from prospective vendors, you can copy up to three vendor fields into the master workbook by doing the following:
   a) Open the completed individual vendor worksheet that was returned.
   b) Highlight columns C through I. Right click and select "copy."
   c) Go to the "Requirements Summary" worksheet in the master workbook and select column C.
   d) Right click and select "Paste Special/Values and Number Formats," then click OK.
6. Repeat for two additional vendors but in step 5(c) above, select column O for Vendor Two and column V for Vendor Three.

The forms can also be used by internal employees who intake vendor information by other means, such as over the phone interviews and research of their own.

Conclusion

It's our hope that these worksheets provide a relatively comprehensive starting point for organizations wanting to gain control over their DLP and encryption processes.

As new regulatory demands are made, requirements will change, so consider these worksheets as an evolving set of tools. Expectations will also get higher as the market DLP and encryption market continues to mature. This maturation will drive higher requirements for single point of control over detection, encryption, access controls and usage/handling rules around sensitive data in use, at rest and data in motion. It will have to cover the virtual layers as well as sensitive date going into and out of the cloud in today's service-oriented architectures.

About the Author

Barbara Filkins has done extensive work in system procurement, vendor selection and vendor negotiations in her career as a systems engineering and infrastructure design consultant. Based in Southern California, she sees security as a process that she calls "policy, process, platforms, pipes, AND people." Most recently she has been involved with HIPAA security issues in the health and human services industry. She has clients ranging from federal agencies (DoD and VA) to municipalities and commercial businesses. Her interest in information security comes from its impact on all aspects of the system lifecycle as well as its relation to many of the issues faced by modern society that are dependent on automation—privacy, identity theft, exposure to fraud, and the legal aspects of enforcing information security. She holds the SANS GSEC (Gold), GCIH (Silver, working towards Gold), and GHSC certifications.

SANS would like to thank this paper's sponsor

McAfee®