10 Lies you Tell your Security Vendors – And what to do instead

Michael Adler
VP, Products
RSA
Who am I?

• 15 Years Building and Implementing Security Products
  – IMLogic – Secure Private and Public Instant Messaging
  – Symantec – Email Gateways, Endpoint, Mobile
  – RSA – Advanced Threat Detection and Response

• Implementations at Enterprises of all sizes
  – 500 employee companies
  – 400k employee companies

• Not only on the Vendor side, but as a customer as well
Maybe Vendors Can Help?
“We understand our needs and our environment and just need you to tell us what your product does.”
Setting Context – Take time to

- Explain the environment – Physical and Organizational
- Explain the challenges and needs – What are the problems you are looking to solve?
- Ask Vendors to describe their solution, not their product.
“We understand our needs and our environment and just need you to tell us what your product does.”

“Here is our environment, we have a problem with X. How do you help your customers solve this problem?”
“We know our security requirements but can’t share them.”
Product Security Requirements

• There are organizational requirements –
  – Everyone has them
  – Be honest with them up front.

• We are transitioning workloads to _________
  – Does your solution allow to be run in the appropriate ways?

• We restrict internet access for security tools
  – What are the impacts?

• We require SLAs for included product security fixes

• We require the following certifications
"We know our security requirements but can’t share them."

"These are the certifications and security requirements required to operate in our environment, do you or can you meet these?"
“All of these features are required to qualify for the RFP.”
<table>
<thead>
<tr>
<th>Area</th>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection - Client</td>
<td>Does your solution automatically generate alerts when a user creates an alert?</td>
<td>Yes. RSA NetWitness Platform (NWP) can deploy RSA NetWitness Log within private, public, or hybrid cloud architectures. In addition, you can monitor Office 365 environments or Salesforce applications. Module components can be deployed virtually and other public clouds, including AWS and Azure, to enable security across cloud environments.</td>
</tr>
<tr>
<td>Alerting</td>
<td>What type of alerting mechanisms are used, such as emails, auto-generation of SMS messages, and such notifications?</td>
<td>Yes, based on the enabled NetFlows, scripts on the log collectors, and correlation rules on RSA. RSA NetWitness Platform supports real-time notifications triggered by RSA correlation rules. These can consist of alerts, SNMP, SMTP, or SMS for any event.</td>
</tr>
<tr>
<td>Prioritization</td>
<td>What prioritization is used?</td>
<td>The RSA NetWitness Platform (NWP) includes native capabilities to support analytics and alert prioritization. Prioritization is based on the RSA NetWitness Platform. It supports real-time prioritization of alerts based on the incident data.</td>
</tr>
<tr>
<td>Data Collection - On-premise</td>
<td>Does your solution allow for the storage of data for a pre-determined period of time?</td>
<td>Yes, RSA NetWitness Platform has two models for storing the collected data: logs, networks, or endpoint or network data, either as a rule or a log rotation policy. Data can also be archived using the RSA NetWitness platform.</td>
</tr>
<tr>
<td>Software Defined Networks</td>
<td>Does your solution allow for the storage of data for a pre-determined period of time?</td>
<td>Yes, RSA NetWitness Platform has two models for storing the collected data: logs, networks, or endpoint or network data, either as a rule or a log rotation policy. Data can also be archived using the RSA NetWitness platform.</td>
</tr>
<tr>
<td>Design Model</td>
<td>Does your solution allow for the storage of data for a pre-determined period of time?</td>
<td>Yes, RSA NetWitness Platform has two models for storing the collected data: logs, networks, or endpoint or network data, either as a rule or a log rotation policy. Data can also be archived using the RSA NetWitness platform.</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Does your solution allow for the storage of data for a pre-determined period of time?</td>
<td>Yes, RSA NetWitness Platform has two models for storing the collected data: logs, networks, or endpoint or network data, either as a rule or a log rotation policy. Data can also be archived using the RSA NetWitness platform.</td>
</tr>
<tr>
<td>Analytics</td>
<td>Does your solution allow for the storage of data for a pre-determined period of time?</td>
<td>Yes, RSA NetWitness Platform has two models for storing the collected data: logs, networks, or endpoint or network data, either as a rule or a log rotation policy. Data can also be archived using the RSA NetWitness platform.</td>
</tr>
</tbody>
</table>
“All of these features are required to qualify for the RFP.”

“Our Needs are labeled Must, Shall, Optional and also labeled with Priority 1-3.”
# A well formed RFP Example

<table>
<thead>
<tr>
<th>Area</th>
<th>Need</th>
<th>Requirement</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log management</td>
<td>We have requirements around access to information for different organizations and need to be able to keep Event and Log Data Segregated for separate partied.</td>
<td>The Solution <em>Shall</em> enforce data segregation such that users in certain organizations do not have access to another organizations data. The solution <em>may</em> segregate at storage time</td>
<td>P2</td>
</tr>
</tbody>
</table>
“I can POC this next week”
Can you really setup a product next week?

If you could, do you know what success would look like?
“I can POC this next week”

“How long does it take to start a successful POC? What do you need from us?”
“Budget isn’t a factor in our decision”
“Budget isn’t a factor in our decision”

“We will purchase the tool that gives us the greatest value”

Or

“We are looking for the greatest value at the best price”
“We don’t need training or professional services”

Or

“We will do the installation ourselves”
I DON'T NEED YOU OR ANYBODY ELSE!
“We don’t need training or professional services”

Or

“We will do the installation ourselves”

“What value do I receive if I use your professional services?”

Or

“What training is required to be successful with the product?”
Get the right kind of help.

- Implementations need quick strong wins
- Getting started correctly is critical
  - How many times has the start of a project determined its success?
- What training will users of the solution need to get the most out of it?
- Services starts training but won’t complete it
“We can plan/budget for increased usage/growth later”
Budget for the Future

• Does any company really plan to shrink?
• You do need to plan for a full deployment
• You should plan for future expansion
• Design and Understand the architecture now and in the future
  – Negotiate the future impacts of growth
“We can plan/budget for increased usage/growth later”

“How do we design for increased usage/growth now and can we understand those costs?”
“We can get this through purchasing/legal”
Getting the Purchase through...

- Are there any Procurement teams or Lawyers in the Room?

- Let your vendor help, vendors do this all the time....
  - Protect your internal brand, let the vendors track the individual pieces

- Read the legal agreements – There shouldn’t be any surprises for either side.
“We can get this through purchasing/legal”

“Can you help me get this through purchasing/legal?”
“I need references to make a decision”
References

- What are reference checks for?
  - Confirm what you should have learned through your own process
  - Look for concerns that you won’t be able to see in your evaluation process
    - How does the product scale?
    - How long did the rollout take?
    - How well was the training received?
“I need references to make a decision”

“We have made a decision, but I would like to hear from references to validate our decision”
#10

“We don’t plan on upgrading regularly”

Or

“You need to help us with that upgrade”
“We don’t plan on upgrading regularly”

Or

“You need to help us with that upgrade”

“What costs should I expect to perform an upgrade?”
10 Things

- Context and needs
- Non-Functional requirements and certifications
- Write a real/good RFP
- Prioritize success over fast RFP
- Know your budget and how it impacts your purchase

- Get the right kind of help
- Plan for growth
- Let vendors help with purchasing and legal
- Use references to validate decisions not make decisions
- Plan for upgrades
Maybe Vendors Can Help?

*Not all Vendors or representatives of Vendors will behave perfectly all of the time......
In Summary

• Security Vendors Want to Help
  – Look to identify those who you can partner with
  – Don’t look at purchases as transactions

• Be honest with your vendors
  – Vendors do a better job when they really understand needs and what success looks like
  – Don’t be embarrassed or hide information. Vendors have seen it all.

• Don’t try to solve every problem with a single solution
  – Find the right mix of products that provide solutions to the problems you actually have
  – Understand the organizational complexities of deploying a security solution
In the next 90 days

- Document your real needs in a format that you can share with vendors
- Document non-functional requirements for any security solution that you bring into the environment
- Review your RFP procedures and templates
- Understand your staffing, training, and skills strategies to prepare for your next purchase
Thank You