

Tips on Selecting an IT Security Software Vendor

By Mark Azzolina

Each year, many new security software solutions are introduced by a myriad of vendors. Selecting the most appropriate security software solution and a reputable vendor can be a tedious chore.

The IT security software market grew to \$7.4 billion in 2005, according to Gartner¹, and the growth is expected to continue. Each year, many new security software solutions are introduced by a myriad of vendors. Some of these vendors are large, well established and reputable; some are small startup companies with limited funding desperately trying to reach profitability; and still others are small- to medium-sized companies trying to cash in on the growing IT security market. The security solutions offered by these companies are as diverse as they are numerous, ranging from “point” solutions that satisfy one need or requirement, to enterprise-wide solutions designed to satisfy many different technical controls required for securing today’s IT environments. As you can imagine, selecting the most appropriate security software solution and a reputable vendor can be a tedious chore.

If your organization is required to follow a particular IT security “best practices” framework or regulatory directives, consult those documents for specific requirements when procuring IT security software and selecting a vendor. If you don’t have in-house expertise for these regulations and implementations, consider using a regulatory compliance and best-practices consultant to help you with

your selection process. The table below lists some of the frameworks and guidance, and where you can find information on acquiring and integrating any type of software into the network configuration baseline.

Beyond any best-practices framework, the goal of this article is to provide practical advice on how to accomplish a thorough and systematic evaluation of security solutions and vendors. The advice in this article is not intended to replace any of the best-practice frameworks, or suffice for a well documented and structured selection process. However, it may help you avoid selecting a poor-quality product or a vendor that is ill equipped to satisfy your needs.

Build a weighted requirements list

Acquiring an IT security solution should be based on need. What determines that need is a risk assessment that clearly shows where current security controls are inadequate to mitigate the identified risk. Once you’ve determined you want to mitigate a particular risk by purchasing a security solution, you ought to follow a disciplined process in your effort to make the best decision. The due diligence required for this process should be directly proportional to the amount of risk to be mitigated and the cost of the solution itself. Keep in mind that the cost of the software solution includes not only the

purchase and implementation price, but also training of the administrators and users; the complexity of the solution; the amount of time and resources necessary to maintain, operate and administer the system; and the number of bugs encountered in the code.

Once it is clear that a security software solution will be required to mitigate a risk factor, a list of requirements should be developed and weighted to aid in your decision process. The best way to develop a comprehensive set of requirements is to get input from your company’s senior managers, internal auditors, end users, customer support personnel, and of course the IT organization. If this wide group comes

¹ “Market Share: Security Software, Worldwide, 2005” by Nicole S. Latimer-Livingston, August 2006, http://www.gartner.com/DisplayDocument?doc_cd=142510

Framework or Guideline	Relevant Sections	
COBIT 4.0	A11 through A17	<ul style="list-style-type: none"> Acquire and Implement
ISO 17799:2005		<ul style="list-style-type: none"> Information systems acquisition, development and maintenance
IT Infrastructure Library (ITIL)		<ul style="list-style-type: none"> Service Support Service Delivery ICT Infrastructure Management Application Management* Software Asset Management
FFIEC IT Examination Handbook	IT Booklets	<ul style="list-style-type: none"> Development and Acquisition
Payment Card Industry Data Security Standard	Requirement 6	<ul style="list-style-type: none"> Develop and maintain security systems and applications*
* Requirements contained in these sections cover “in-house-developed applications.” These same requirements can also be used to evaluate potential third-party application providers		

Guidance on software selection and acquisition

up with overlapping requirements, ensure that the documented requirements represent the needs of the entire group. If there are conflicts between requirements, they need to be resolved before they are used for a product evaluation.

The requirements list should identify all the major functionality required by the software. The list should also include any applicable regulatory directives, and define the network environment in which the solution must operate. Other requirements to consider are the “ease of use” of the software and the expertise of the IT staff that will be supporting the application. If the application will be used by end users, then training and user interfaces will also be an important factor in your analysis.

Once you have a list of requirements, you must identify potential vendors who can provide the type of security software you need. You will find it easier to learn about the functionality of software products available from large vendors with a broad client base, than that of new security products from smaller vendors. Research on the Internet and in software buyers’ guides can help identify potential applications and vendors.

Working with vendors should be an easy process, but you would be surprised how resistant some vendors are to providing the information you need to make the best selection. The more secretive and less cooperative the vendor is, the more likely they have something they don’t want you to know. Those vendors that will provide you information about their product should do so under the protection of a non-disclosure agreement (NDA). Depending upon the sensitivity of your requirements and the vulnerabilities they expose, you should sign a mutual NDA so that both you and the vendor can speak freely.

Beware of marketing literature

One of the major sources of information you will receive from solution vendors is their marketing literature. Unfortunately, this information often fails to provide you with enough data to make an informed decision. Many vendors claim for marketing purposes that they satisfy regulatory requirements, but only a few document how the requirements are satisfied. Take, for example, a system backup solution. All the regulatory requirements and best-practice frameworks require controls for business continuity and disaster recovery. However, many other requirements appear in these regulations and frameworks. The vendor’s solution may satisfy several required controls, but might not address many others. Access controls, training requirements, configuration and change management requirements – to name a few – need to be satisfied by the implementation of additional technical controls.

Analyze the vendor’s roadmap

If a vendor’s solution does not currently include some of the functionality you require, you may be able to have your requirements included in the vendor’s product roadmap. However, vendors have the prerogative to change the direction of their software product at any time. The only thing to guarantee that you get your needed functionality is making the successful delivery of that functionality a contractual requirement, with clear deadlines for its design, testing and implementation. Vendors that will not or cannot provide you with a detailed product roadmap should be dropped from consideration. This is often a huge red flag indicating the vendor has no clear product direction.

Evaluate security software engineering practices

Many of the best-practice frameworks address application development processes. If these are requirements imposed on your organization when you develop in-house applications, you should also expect these practices from your software vendors. Therefore, use your best-practice frameworks for vendor evaluation criteria.

Poorly engineered security software solutions can introduce new vulnerabilities upon their implementation. Regardless of the software development method used, both the effectiveness of the security solution and the security of the application itself must take prominence as considerations in the product’s definition, design, development, test, implementation and ongoing support. Secure software solutions are supported by clearly documented security engineering activities throughout the software development life cycle.

Documentation should also be a factor in your decision process. Under protection of an NDA, the vendor should share with you samples of the product roadmap, design documentation, user’s manuals and administrator’s manuals. The quality and currency of these documents will often determine how much difficulty you will have supporting the application and how many calls you’ll make to the vendor’s customer support center. While evaluating the design documentation, pay careful attention to the level of consideration for security. Security is a consideration that must be included in every step of the vendor’s engineering process.

You should understand the vendor’s software release cycle and what is contained in each release. Ask the vendor for historical data on software releases over the past few years.

- How often are new releases provided to the vendor's customers, and how does their schedule fit into your IT project schedule?
- Did the vendor's previous releases require a complete reinstall of the software, or were simple software upgrades made available?
- Were upgrades accomplished by customers, or did upgrading require the support of the vendor's engineers?

Evaluation of the location, size and structure of the vendor’s software engineering organization will also provide you with valuable information. In this era of offshore outsourcing, many security vendors are opting to ship some or all of their software engineering efforts overseas. This practice should result in the following questions:

- Does the vendor still maintain control over the security engineering processes of the offshore development team? If so, how?
- What safeguards does the vendor have in place to ensure that the engineers working on the project are ethical?
- How are product requirements articulated to the offshore team? Are there any language barriers?
- How is the quality and “cleanliness” of the source code validated prior to compiling?

Considering the current world political environment, it isn’t hard to imagine a Chinese software engineer writing code for a US software security vendor in Shanghai and hiding malicious instruction in his source code. Although this threat also exists in open market

economies, we can depend on laws to deter malicious activity and prosecute engineers for malicious acts. The ability of a software vendor to prosecute malicious engineers in an offshore development facility is limited by the laws of the foreign country hosting the facility, and the effectiveness of the vendor's legal team in that country.

The structure of the vendor's software engineering team, software test team and customer support team may also provide clues into the quality of the software and support you will receive.

- Are the teams staffed adequately with the engineering expertise necessary to develop and support secure and quality code?
- Does the vendor have seasoned software engineers with security engineering experience?
- Who performs unit, integration and functional testing?
- Do the vendor's implementation team and customer support team sign off on releases or bug fixes prior to their general availability?
- Does the customer support organization report to software engineering, or is it autonomous?
- How many lines of source code are contained in the product, compared with the number of engineers?

Ask for descriptions of the vendor's test environment as well. If the test environment isn't robust enough to handle the complexity of the solution, don't expect the solution to be well tested.

Try to determine financial solvency

The financial solvency of the vendor should also be explored. If the company is publicly traded, its financials are readily available. If it is privately owned, you will need to request an audited copy of the financials. Unfortunately, many of today's smaller security software vendors are not profitable, so don't be surprised if they resist sharing their financials with you. If you can't obtain a copy of these, insist on speaking with a principal from the vendor's funding source to get an indication of the source's commitment to the vendor and their product. The longer the vendor has been in business, the more profitable it should be.

If you are suspicious of a vendor's financial solvency but still select them as your security software vendor, insist that they deposit their product source code in escrow. In the event that the vendor company folds or decides to abandon the product, you retain the right to access source code held in escrow.

Schedule on-site product evaluations

Before committing to any major security software purchase, you should "kick the tires." Request that the vendor provide you with a trial version of the software or an in-depth demonstration of the application in your lab and on your standard equipment. If special hardware is required to run the software, you may have to upgrade your existing equipment or purchase new equipment in order to conduct the on-site trial. Use your requirements list to validate the successful satisfaction of each major requirement. Don't follow any demonstration script or test procedure supplied by the vendor. Instead, follow your requirements list, and ensure that all the functionality you require is demonstrated in the application. Remember, they're your requirements, so you need to validate how each requirement is satisfied by the vendor's software solution.

Get customer references

Ask the vendor for several customer references, and call them! Have a set of questions for the references that provide you insight into the quality of the software and the vendor's customer support. If the reference is in your local area, or if the software purchase is significant enough, you may want to ask if you can visit the reference's facility to see the security solution in action. If you do get to spend time with a vendor's existing customer, have a list of questions for them regarding their experiences with the vendor's personnel, product implementations, upgrades and customer support.

Put it in the contract!

A contract is your most effective protection from poor-quality software and vendors. It should include language that ensures you get what the vendor promised during your evaluation or product trial. If you discussed new functionality, include a hard delivery date for this new functionality, with penalties for missed deadlines or failure to deliver.

Problem resolution should also be contained in the contract. Software bugs you encounter should be categorized by severity. You should expect any critical bugs that render the software inoperative to be acknowledged in an hour or two, and corrected in a matter of days. Bugs that are less critical also need to be defined, and response times set in your software license agreement. Ensure that senior managers in the vendor's organization will be made quickly aware, through a documented escalation plan or guidelines, of any critical issues you may encounter with the software. The speed of escalation throughout the vendor's organization is determined by the severity of the bug. Naturally, critical bugs should filter up to senior management very rapidly, while minor bugs are escalated to functional managers without the sense of urgency of critical issues.

Conclusion

Although your investigation process may provide you with many answers, be careful not to alienate the vendors under investigation. Your exploration into each software solution and company should be a cooperative effort. The way they respond and communicate with you can provide deep insight into the relationship you'll share with them after you become their customer. This is a two-way street. Some vendors will drop a potential prospect if they perceive that the amount of work to capture the deal outweighs the probability of winning the deal. The best way to avoid this is to keep the communication between you and your potential vendors open, honest and frequent.

There are some great security solutions available today from great vendors. It's up to you to make the correct choice, and remember, let the buyer beware!

About the Author

Mark Azzolina, CISSP-ISSMP, is the CEO and Principal Consultant for Compliant IT Services, an IT security and compliance consulting firm. Mark has also been a member of the ISSA-Colorado Springs chapter since 2001. He can be reached at mark@compliant-its.com or (719) 282-1823.