WHITE PAPER

Four Factors Not to Overlook When Trying to Save on Security

Author: Mark Bouchard

AimPoint Group

keeping IT on target

Executive Summary

Unrelenting pressure to do more with less has CIOs worldwide aggressively pursuing cost-saving techniques and technologies such as datacenter consolidation, server virtualization, and software-as-a-service (SaaS). And, perhaps, for no domain is the pressure greater than for IT security. Risk levels continue to escalate at the same time that the resources available to contain associated threats remain, at best, constant.

Once again, consolidation is a reasonable response. Implementing multi-function security systems – such as web security gateways, email security gateways, or even unified threat management (UTM) devices – and focusing on solution suites in favor of point products, will typically yield positive returns. One significant trap that IT/security managers must take caution to avoid, however, is placing too much emphasis on initial acquisition, licensing, and maintenance costs when evaluating these solutions. The true cost of any solution and, therefore, its potential to deliver savings relative to available alternatives, also depends on four additional factors: security effectiveness, administrative and operational efficiency, breadth of coverage, and adaptability – each of which can vary considerably from one solution to the next.

The Information Security Landscape

The challenge faced by modern organizations is a daunting one. Achieving greater operational efficiency and remaining competitive essentially dictates that information technology be fully embraced. Steadily rolling out new applications and communications technologies and increasingly exposing them to external constituents is basically a business imperative. Organizations, however, must simultaneously provide an effective level of confidentiality, integrity, and availability for *all* of the associated infrastructure, applications, and, most importantly, data. Moreover, they must continue to do so even as risk levels rise and resources – financial and otherwise – remain in short supply.

Risks Levels Continue to Rise

One need only consider the three components that comprise the classical risk equation – threats, vulnerabilities, and resource value – to understand what's going on here.

- **Threats.** The presence of an underground economy for valuable information has sparked an explosion in the sheer quantity of threats being released, as well as the speed with which they are developed and launched.
- **Vulnerabilities.** The surface area open to attack continues to expand as competitive pressures drive organizations to steadily adopt emerging technologies, buy or build new applications, and embrace greater degrees of user mobility, interconnectivity, and third-party access to networked systems.
- **Value.** The value of information resources is rising in lockstep with the growing dependence that modern organizations have on electronic information and associated systems. The Web, for example, has become an ingrained part of how business is conducted.

Resources Remain Constrained

IT security budgets, however, are not growing at a commensurate rate. In some instances they're even shrinking. This is due in no small part to the weakened economy and the challenges it presents to the majority of businesses worldwide. Other forces that are also at work here include complacency and a growing sense of futility.

In the first case, relatively few major attacks have made the headlines in recent years, leading some management teams to conclude that further investments in information security are not really necessary at this time.

Concurrently, frustration levels are mounting as significant incidents and breaches continue to occur on a regular basis despite progressively larger sums having been committed to information security for several years now. As a result, some management teams are basically ready to capitulate – at least to the extent that obtaining substantially greater assurance of solution's effectiveness is now a prerequisite for further investments.

Reality Rules

Although the specific causes are certainly debatable, the bottom line is not: when it comes to IT security, the vast majority of organizations are having to get more done with less. Naturally, many of these organizations are looking for ways to cut costs.

Given this situation, it is not surprising that low-priced security products hold a certain degree of attraction. The issue, however, is that all too often solutions that appear great on the surface exhibit a plethora of hidden costs that become painfully obvious once they are put into production. Fixed cost elements – those associated with hardware, licensing, and maintenance – represent just one aspect of a solution's overall cost of ownership, and placing too much emphasis on them is extremely short-sighted. Indeed, organizations that fail to account for this fact risk having their cost reduction efforts backfire.

Earth-shattering news by no means, this is a message that deserves repeating, particularly during periods of tough economic conditions when competition among vendors is likely to be at its fiercest.

Reducing Security Costs The Right Way

Further to the point initiated in the previous section, the right way to achieve enduring and even more substantial cost savings when selecting information security solutions is to look beyond obvious, fixed costs. Four factors that IT/security managers should focus on in particular based on their capacity to reduce costs on a recurring basis are a solution's effectiveness, efficiency, breadth of coverage, and adaptability.

Fixed cost elements – those associated with hardware, licensing, and maintenance – represent just one aspect of a solution's overall cost of ownership, and placing too much emphasis on them is extremely short-sighted.

Effectiveness is Job #1

First and foremost among the factors that determine a security solution's true cost is effectiveness, or stopping power. Products that are unable to consistently prevent the introduction or execution of both known and unknown threats can ultimately cost an organization dearly. At a minimum, each event carries with it the substantial cost of "cleanup", or the effort required to restore systems to an appropriate and hopefully stronger configuration[1]. Major incidents are likely to also entail substantial costs in the form of customer notification, loss of data, regulatory fines, punitive damages, loss of customer confidence, and/or loss of competitive advantage.

To be clear, "ineffectiveness" in this case is measured on a relative basis. No security product will ever be 100 percent effective. On the other hand, one that trails the top performers by even just 5 to 10 percent will not save an organization money in the long run – no matter how much less it cost initially.

And although relative effectiveness is difficult to definitively determine – in no small part because it varies over time – it is simply too important to ignore. Accordingly, some imperfect-yet-useful indicators that organizations can use to evaluate a solution's effectiveness include the following:

[1] Each year in an enterprise of 5,000 employees, nearly two-thirds of endpoints get infected resulting in IT labor cost of over $197,000 for endpoint cleanup/restoration – *The Cloud-Client Enterprise Security Impact Report,* Osterman Research, January 2009.

- **What is its track record?** Beyond a solid heritage and history, there must also be proof of continued/current success. Ideally this should take the form of side-by-side, real-world pilot testing. But given the associated cost, it may be necessary to settle for test results published by independent sources.
- **Does it employ innovative techniques?** What techniques and "special sauce" does the solution include to counteract the prevailing characteristics of the threat landscape – greater speed, diversity, and elusiveness? For example, being backed by an extensive threat intelligence network and leveraging a cloud-client architecture (which reduces reliance on local updates for the very latest protection) enables a solution to "know more threats sooner"[2]. Complementary to these capabilities, employing application-aware access control, vulnerability-oriented intrusion prevention signatures, and heuristic detection algorithms fall into the camp of enabling greater stopping power without the need for threat-specific details.
- **To what extent are its components integrated?** It makes sense that sharing information among the individual countermeasures that comprise a solution should increase its effectiveness. A simple example is where the detection of malware in material downloaded from a site results in a complementary URL filtering capability automatically preventing other users from accessing the responsible page/domain[3].

The Many Faces of Efficiency

The second-most powerful contributor to a solution's ability to effectively reduce costs is efficiency. Some aspects of efficiency are fairly clear – such as ease of management and the capacity for automation – whereas others are somewhat less obvious. The following suggestions for items to evaluate in this regard include a bit of both.

- **At what point are threats being thwarted?** Generally speaking, threats such as malware can be thwarted in different stages: by blocking access to the resources that contain them in the first place; detecting and eliminating them at the time of download; or thwarting them once they reach an endpoint and begin to execute. Having capabilities across all of these stages is absolutely necessary. However, those focused on the earlier stages – such as dynamic/reputation-augmented URL filtering and spam blocking – are, arguably, more important. This is based on the fact that they minimize the workload placed on downstream infrastructure, including network bandwidth, security gateways, and endpoint systems.
- **How does the solution impact its environment?** Closely related to the previous item, this one deals with the presence of innovative techniques that help reduce resource and administrative requirements. For instance, for anti-malware and endpoint security solutions, having a cloud-client architecture provides a distinct advantage: it eliminates the need to push conventional signature updates with ever-increasing frequency to ensure the greatest degree of protection is provided – a task that would otherwise require considerable effort on the part of IT staff, consume substantial bandwidth and network device capacity, and significantly impede end-user productivity. Adding file reputation and associated caching capabilities extends these gains even further by helping control the size of signature files that need to be maintained on local systems and improving the efficiency of cloud-client interactions.

[2] A cloud-client architecture is one where a substantial amount of threat intelligence is housed in the cloud. Security solutions using this architecture do not retain a full set of content-based resources (e.g., signatures or URLs) at each local component, but instead supplement a partial listing and cached entries by making real-time calls to a comprehensive, centralized repository that is constantly being updated.

[3] Although the examples included herein focus predominantly on anti-malware, content, and endpoint security, the general principles, rationale, and guidance are applicable to most (if not all) other domains of information security as well.

- **Is it easy to operate and maintain?** Configuration and monitoring capabilities that are centralized and unified are table stakes and the key to a truly scalable solution. So is the ability to automatically distribute and implement content and firmware updates. Less common, but quite powerful from a cost reduction perspective, is the ability to automatically remediate a malware infection.

The Art of Covering Multiple Bases at Once

Technically this third factor could also be classified as another "face of efficiency." But treating it separately helps emphasize its significance. The general idea is that, so long as they do not introduce compromises with regard to the previous factors, solutions that provide broad coverage can help reduce the overall cost of security. Indeed, strategic use of multi-function security gateways and well-structured software suites avoids the need to juggle multiple management tools, maintain and integrate a collection of disparate point products, and negotiate and navigate a large number of vendor relationships. There are even tie-ins that help to further bolster effectiveness and efficiency. For instance, centralized visibility across multiple controls can speed threat detection, confirmation, and response, while unified reporting simplifies the otherwise onerous task of compiling proof for compliance audits.

In terms of the actual scope of coverage that a given solution provides, there are three dimensions that IT/security managers need to evaluate.

- **Functional coverage.** Matching the increasing diversity of threats requires multiple countermeasures featuring a blend of positive-model, negative-model, and type-specific (e.g., rootkit) detection techniques, as well as both prevention and monitoring capabilities.
- **Logical coverage.** Ultimately, protection needs to span all layers of the computing stack, from network to application and even the data itself.
- **Physical coverage.** Similarly, protecting just the perimeter is not enough. Coverage should ideally extend from end-to-end, which means having countermeasures at external *and* internal chokepoints, as well as near or on individual endpoints.

Flexibility and Adaptability = Low-Cost Security in the Future

Security solutions that are highly adaptable and therefore able to remain applicable despite changing conditions can definitely reduce the need for additional investments in the future. In contrast, solutions that are inescapably tied to a piece of hardware, difficult to upgrade, or unable to accommodate step-function increases in demand and changing modes of operation (e.g., cloud computing) will ultimately drive security expenditures upward due to their significantly shorter service life.

Flexible configuration options, broad platform support, seamless integration with 3rd-party solutions, and the ability to fully support other cost-reduction initiatives the organization may be pursuing are all important considerations in this area.

Another item that makes increasing sense these days is support for virtualization. Having a virtual appliance version for network-based countermeasures conveys several advantages. In addition to typically costing less initially, the need to only develop software – versus an entire system – and the fact that deployment only involves software and/or a license key means that new controls for counteracting new threats can be released and implemented more quickly than with conventional appliances.

Virtual appliances, however, are only a start. Virtualization is a much broader trend with many additional facets, most of which are being pursued due to their potential to yield substantial cost savings. What cost-conscious IT/security managers need to evaluate, therefore, is how well candidate security solutions align with the bigger picture by providing multiple options not just for protecting virtualized infrastructure but also for becoming part of it.

Conclusion

Rising risk levels and shrinking budgets have many of today's organizations in a bind: they can ill afford to stop embracing and investing in information technology, but managing to do so in a relatively secure manner is rapidly moving beyond their reach. Finding ways to reduce costs and using this as a means to stretch available resources is certainly an appropriate response. What is not appropriate, however, is ignoring total cost of ownership elements above and beyond licensing and maintenance costs. In particular, IT/security managers need to focus on effectiveness, efficiency, breadth of coverage, and adaptability, for it is these four factors that determine a security solution's true cost and its ultimate potential to help organizations do more with less.

IT/security managers need to focus on effectiveness, efficiency, breadth of coverage, and adaptability, for it is these four factors that determine a security solution's true cost and its ultimate potential to help organizations do more with less.

About The Author

Mark Bouchard, CISSP, is the founder of AimPoint Group, an IT research and analysis firm specializing in information security, compliance management, application delivery, and infrastructure optimization strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security and networking topics for more than 13 years. During this time, he has assisted hundreds of organizations worldwide with strategic and tactical initiatives alike, from the development of multi-year strategies and high-level architectures to the justification, selection, and deployment of security and networking solutions. A veteran of the U.S. Navy, Mark is passionate about helping enterprises address their IT challenges.