



# Security Solutions— Integrated or Compatible?

## **Table of Contents**

<b>Executive Summary</b>	<b>3</b>
<b>More For Less</b>	<b>3</b>
<b>Real Cost of Ownership</b>	<b>4</b>
<b>Compatible vs. Integrated: The Spectrum</b>	<b>4</b>
<b>Conclusion</b>	<b>6</b>

# Security Solutions—Integrated or Compatible?

## Executive Summary

Words like “integrated” and “centralized” have been used to describe application software solutions for some years now, often because of marketing messaging that implies more interoperability than the given technology can actually provide to the business customer. The terms are broad enough to be almost meaningless in some instances. In the field of IT security, the sheer range of tools and techniques in the hacker or virus writer’s armory that one must guard against has driven up the number of solutions required to prevent attacks. This has increased the cost of managing these solutions, to where the cost of management typically makes up over half the total cost of ownership (TCO). Reducing this significant cost is achievable, as this paper details. This makes financial sense and, just as importantly, allows a superior level of security even when using multiple vendors. Solutions that truly are integrated and centralized can bring clear benefits if applied correctly.

## More For Less

In today’s competitive security market, vendors are driven to provide more for less. Bundles and suites are a common practice that became popular following the introduction of the Microsoft® Office suite in the 1990s. The aim is to provide exponential discounts as you buy more components from the same vendor, therefore reducing the overall costs for the software. (The diagram below highlights the approximate discount level for some of the key McAfee suites.) Although the purchaser may not use every product included in the bundle, it is still more cost-effective to buy the suite instead of the individual components.

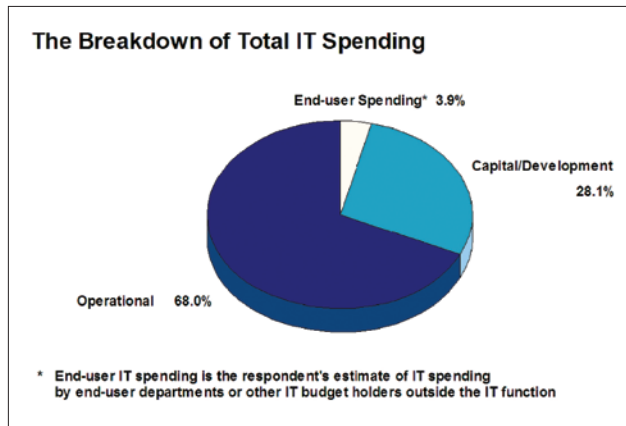
	<b>McAfee Active Virus Defense</b>	<b>McAfee Total Protection™ for Enterprise</b>	<b>McAfee Total Protection for Enterprise— Advanced</b>
<b>Percentage suite discount value over sum of parts</b>	<b>20%</b>	<b>39%</b>	<b>46%</b>
McAfee VirusScan®			
McAfee NetShield® for Netware			
McAfee VirusScan Command Line Scanner			
McAfee ePolicy Orchestrator®			
McAfee GroupShield® for Mail Servers			
McAfee WebShield® SMTP for Gateway			
McAfee AntiSpyware			
McAfee Host Intrusion Prevention (desktop)			
McAfee SpamKiller® for Mail Servers			
McAfee Network Access Control			
McAfee SiteAdvisor™			

To encourage the use of unused suite components, Microsoft started to integrate features and build common interfaces among the component parts of the Office suite. This paper will look at how and why the security industry is doing the same.

### Real Cost of Ownership

The traditional reason for purchasing a security suite—as opposed to purchasing each security component—was to save money. However, purchasing the license(s) for the security software only accounts for about 5 to 15 percent of the real cost of implementing and maintaining that solution (i.e., the TCO) when amortized over three years, as is common practice for a software purchase. This means that real-world savings, which depend on the number of suite components you use, would always be a small percentage of the total cost of using that solution.

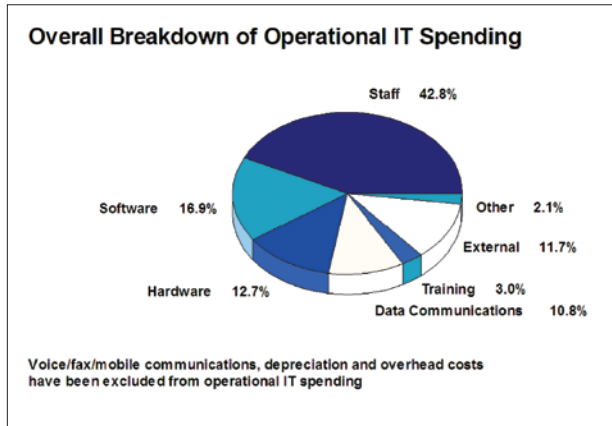
With every company needing to reduce costs, how do you improve efficiency and get more from security investments? To answer this, we need to understand what makes up the real cost of implementing security solutions. The largest cost is in manpower, which can make up between 50 to 70 percent of that TCO. This can include cost of training, implementation, management, maintenance, and support.<sup>1</sup>



In the 2006 report *Benchmark of IT Spending 2006, The Annual Review of IT Spending in the UK*, the National Computer Centre (NCC) validates these figures. (See pie chart entitled “The Breakdown of Total IT Spending” above and the chart in the next column, “Overall Breakdown of Operational IT Spending”). Note that security software traditionally requires more maintenance and training than most other software. This is due to the need for regular updates and reconfiguration to keep up with ever-changing

<sup>1</sup> “In most cases, the price of software proved to be less than 10 percent of the total cost of ownership. Where costs do become significant for all types of software is in the level of staffing needed. By staffing, I mean the training, maintenance, support, administration and other personnel costs necessary to run the software package efficiently. These costs can add up to as much as 50 percent to 70 percent of a software system’s TCO over its useful life.”—“The True Costs of Software” by Alan MacCormack, assistant professor of business administration at Harvard Business School (*ComputerWorld*, May 2003), <http://www.computerworld.com/softwaretopics/os/windows/story/0,10801,81590,00.html?l=x13>

security threats, and because compliance controls require security solutions to be in place 24/7.<sup>2</sup>



If staff and management costs are the biggest part of your TCO, how can security suites help reduce this cost? Many vendors’ security suite collateral use the term “integrated security protection.” The question is, what does “integrated” mean and, if the protection does integrate, how does this help reduce the costs of using a particular security suite?

### Compatible vs. Integrated: The Spectrum

#### Compatible

The most basic integrated security suite provides compatible software components, in which the vendor has verified that each component or product can coexist on the same system. This may include presetting configurations to be sympathetic to one another, such as a desktop firewall being aware of anti-virus software and having predefined rules set to ensure the anti-virus software can communicate with its central manager and update sites through the appropriate protocols and ports of communication.

The value of such an integrated suite is ease of implementation. You spend less time testing the products prior to deployment, since you do not need to test compatibility. Moreover, you do not need to tune the products to function correctly with any of the other security products or components you are using.

#### Common management interface

For each security solution you deploy, you will likely have a corresponding management console to configure, control, update, and view activity logs and reports. The more management interfaces you have, the more costs increase.

These costs include:

- The hardware required to install the management interface

<sup>2</sup> Graphs taken from the National Computing Centre report *Benchmark of IT Spending 2006, The Annual Review of IT Spending in the UK*.

- Product training, which may involve simply reading the manual and spending time with the product or more formal classroom training
- Deploying a client agent to each system you want to manage. This may already be a part of the security product, but in reality, each one creates network traffic and uses system resources. The more agents you deploy, the greater the cost in terms of resource usage. This is known in the industry as the “Agent Wars,” because more system resources are used for managing solutions than for normal processing
- Once a management console and client software are installed and active, the administrator will have to complete daily maintenance. Security solutions are more labor intensive than most other software solutions, as they require stringent compliance to:
  - Ensure that all protected systems have the correct software installed, are using the latest versions, are configured correctly, and have not been tampered with by either the user or an attacker
  - See what attacks or incidents have occurred that may determine whether you take further action, such as validating that data has not been breached or changing the configuration to prevent such incidents from happening again

The more management interfaces you have, the more time will be spent repeating these tasks for each security solution you have deployed. A common management interface allows you to complete these tasks from a single console against all the relevant security products you have deployed.

### **Collective reporting**

You could argue that common reporting is a component of a common management interface— if you have one point from which to manage and configure your security solutions, then surely all the event data will come back to the same interface. However, collective reporting should offer more. It should be able to aggregate and collate the data from each point solution to give you a holistic view of your security posture, as opposed to you having to run multiple reports and then manually paste them together to get that single view.

In security, the volume of data you can receive from one security solution could be far greater than is possible to reasonably understand and assimilate within a 24-hour period. Gathering such security data into a single view, encompassing all your security solutions, can be the difference between responding in a timely fashion and not using the solution due at all to the avalanche of data it can produce.

### **Common process management**

Security should enable businesses. As such, threats and other security challenges should be treated together as a single entity. Traditionally, IT staffs have needed the security expertise and resources to translate what each threat means to their business and determine how to manage it. This would consist of the painstaking process of having to understand if and how each security solution can help manage the threat and what value and risks are associated with each. Too often, this translates into a blanket approach to business security.

An effective security solution should translate a technical threat into the potential business risk it brings to each business. At a simple level, it should highlight the relevancy and areas in which the threat could succeed. At a more advanced level, it should be able to prioritize based on asset value.



An integrated security solution should paint a relevant threat risk picture for customers and help them manage it. It should translate the technical threat knowledge into actual business risk, by comprehending the existing security solutions and correlating where protection already exists and where it is lacking. Based on the technologies deployed, it should provide guidance as to what response to take and help business prioritize these actions.

Having defined business risks and what steps to take to mitigate them, the integrated security solution should manage and report on the processes required to implement the solutions and show the results (i.e., risk management).

Integrated process management can happen among solutions from each vendor, or as part of full integration among all the security components you have deployed. The latter is more complex to achieve but far more beneficial to the business.

### **Security product interaction**

As security solutions become more complex, we see everything from duplication of effort among different solutions—sometimes a good thing, such as a multi-layered defense; others times a waste of effort, such as redundant gathering of data—to solutions that are aware of and can cooperate with other security products.

Integrated security solutions should interact both at a product and management level to minimize unwanted duplication and provide smarter security protection. There already are some clear examples of this.

For example, when using network intrusion prevention systems (IPS), network administrators traditionally have had to decide whether they should drop network packets that the IPS sensor labels a threat. What makes this decision difficult is the fact that the IPS sensor tells you which IP address the attack is coming from and going to, but not whether that attack is relevant to that particular IP address.

Vulnerability assessment and management tools, however, understand the relevancy of threats. If IT staff can share the data from their vulnerability assessment tool with their

In the Gartner report *Use Processes and Tools to Reduce TCO for PCs*, the section entitled “Security Best Practices Can Lower PC TCO” examines “...the TCO impact of using security software, such as personal firewalls, patch management, malware prevention, network access protection, and host-based intrusion prevention products. They highlight looking at the processes to implement and manage these security tools, as well as implementing security policy configuration management. Each of these best practices potentially reduces the TCO between 1

Relevant	Tue Aug 08 11:...	H	HTTP: IIS cmd.exe Execution	10.10.10.9	---	10.10.10.10	---	My Coi
Unknown	Mon Aug 07 13:...	H	BACKDOOR: Back Orifice Trojan	30.1.0.1	1272	30.1.0.2	6666	My Coi

network IPS solution, they can better decide whether the attack in question is relevant and therefore potentially successful.

Equally, the endpoint system being attacked may have local protection in place that could mitigate the attack. When a network administrator can correlate these factors, it greatly reduces the pressure in terms of having to try and block everything that looks potentially insidious. By making the security solutions work together, smarter decisions are possible.

Another example is client security solutions that are aware of each other to avoid conflict and to provide optimal protection. Say an organization’s anti-virus software includes some basic firewall functionality. If the company installs a full client firewall, the anti-virus product should be aware that its firewall features are being superseded and therefore disable that feature. Should that firewall be removed from the system, the anti-virus solution should detect the change and re-enable its more basic firewall functions.

## Conclusion

Traditionally, software suites are positioned to reduce purchasing costs. However, in the real world, management costs of security software solutions make up the largest segment of TCO. Single vendor security products that improve efficiency and effectiveness through integration have great potential to reduce operational costs and increase value by making the component products work together as a solution. Applying this across multiple vendors would also achieve an exponential increase in value.

percent and 5 percent and, when used in combination, can reduce TCO by 14 percent.”<sup>3</sup>

Business savings through integration are both tangible and intangible. The reduction of costs such as training and hardware is tangible, as it affects the largest section of the TCO. Less tangible benefits, such as integration of process management and product integration, are more difficult to measure. Having proper protection against the latest threat enables you to tackle the problem collectively rather than one product at a time. This approach minimizes the overall risk to the business. Product integration leads to smarter security, giving you more from your solutions. Equally, the endpoint system being attacked may have local protection in place that could mitigate the attack. When a network administrator can correlate these factors, it greatly reduces the pressure in terms of having to try and block everything that looks potentially insidious. By making the security solutions work together, smarter decisions are possible.

Today, businesses focus not on each individual threat but instead on managing risk. This requires a truly integrated security strategy to allow each organization to manage its risk relevant to its business and its security solutions from a technology and process standpoint. In this context, the question “How integrated is your security?” takes on some context.

Greg Day  
Security Analyst,  
McAfee

<sup>3</sup> Gartner report *Use Processes and Tools to Reduce TCO for PCs, 2005-2006 Update* by Federica Troni and Michael A. Silver, January 13, 2006.