TOTAL COST OF OWNERSHIP OF ENDPOINT PROTECTION

panda

pandasecurity.com

01 Executive Summary

Businesses of all sizes today are increasingly dependent on their IT systems to run their operations and, as a result, they have become more sensitive to vulnerabilities and other IT security concerns. Add to that the increasing mobility of the workforce and the inherent difficulties in managing roaming devices, and what we have is a scenario in which the management of security operations becomes ever more complex, costly and sophisticated. In fact, many IT system failures and downtimes are caused by human errors due to the manual nature of managing traditional, onpremises IT management solutions.

To make matters worse, according to Gartner, IT security staff are the most difficult to find and retain for SMBs , which represent the majority of the businesses today.

In order to address these challenges, new Software as a Service (SaaS) solutions are emerging which can replace or extend the capabilities of traditional, on-premise products. In particular, SaaS management solutions for desktop anti-malware, such as Endpoint Protection, can be leveraged at anytime, from any Web browser, providing simple, easy to use management of anti-malware and personal firewall protection.

The needs of the companies that are driving the take up of the combined model

The first benefit of a SaaS solution like Endpoint Protection, when compared to traditional anti-malware protection for desktops, is the absence of upfront investments to implement it. Traditional protection for desktops requires on-premises hardware and software investment (administration servers, repository servers, databases), introducing additional points of failure, added vulnerabilities and recurring maintenance and upgrading costs. a SaaS desktop anti-malware solution, on the contrary, hosts all the management infrastructure within the vendor's infrastructure.

The savings in this regard will be greater, the more distributed the environment is (usually each location in a distributed environment requires at least one server in the on-premises model).

Considering an average implementation of an anti-malware solution in a medium sized business, the savings generated by a SaaS based solution could reach 50% of the total costs. This document details how such a saving is possible.

A second important benefit is that it enables the channel to provide value added services to end users, so mething many of them are actively searching for, trying to regain the profitability they lost due to the shrinking margins in hardware suffered during the past few years. In the case of Endpoint Protection, channel partners can leverage a purpose built "Partner Console", which allows them to efficiently manage the security solution across multiple customers, from one single Web console, remotely, and without requiring any hardware or software investment either. Thus, SMBs have now the opportunity to outsource the management functions to the channel partner (an MSSP).

Finally, a third benefit consists of the natural suitability of the SaaS approach in dealing with an increasingly mobile workforce. Today, controlling and managing travelling employees with laptops is a source of concern for administrators. With a solution like Endpoint Protection an administrator (or the MSSP) can remotely monitor and configure the anti-malware and personal firewall protections in laptops, regardless of their location or the type of Internet connection.

02 Cost Drivers in the Total Cost of Ownership Analysis

What are the cost drivers that companies need to look at when completing a Total Cost of Ownership analysis?

Capital expenses

Traditional Security Solutions

Upgrades to other security solutions that may be required bring additional capital expense.

Software and hardware, network infrastructure enhancements, monitoring and testing tools, supplies, facilities and other required infrastructure are part of the typical capital acquisition expenditure. This capital expense is an up-front cash outlay.

SaaS Security Solutions

With SaaS, there are no perpetual software licenses to buy. The nature of SaaS is that you pay for what you use. SaaS models allow a recurring cost structure. You pay a monthly or annual service fee for as long as you use the service.

This service fee includes maintenance, support, updates and upgrades and is inclusive of all hardware, networking, storage, database, administration and other costs associated with SaaS delivery.

Design and deployment costs

Traditional Security Solutions

- Staff and contract labor needed to design, integrate, test, tune and launch is a significant cost associated with deploying a traditional security solution.
- Server and network capabilities must be reassessed and augmented.
- Server hardware, operating systems and applications have to be evaluated for compatibility with the selected security solution and upgraded if necessary.
- System testing and tuning are necessary to make sure performance is acceptable for launch.
- Training for IT staff will be required.
- Launch activities, awareness and pilots all require IT resources.

SaaS Security Solutions

SaaS security solutions can be deployed and put into production much faster and for a fraction of the cost compared to a traditional software solution.

This is very important when the opportunity costs of getting the application out are high. On the flip side, because a SaaS security solution is a multitenant application, there are less ways to customize the application to fit the business architecture.

Ongoing infrastructure costs

Traditional Security Solutions

- For ongoing operation, network monitoring and management tools are often required to enable real-time problem diagnosis and responsiveness.
- Yearly software maintenance and support contracts and system updates and upgrades make a large contribution to the total cost of ownership.
- Scaling the infrastructure, multiple redundant systems, and add on feature sets further increase cost.
- Hardware repair and replacement and recurring environmental costs.

SaaS Security Solutions

Other than possible additional Internet bandwidth needs, there are almost no incremental infrastructure costs required to handle the growth of a SaaS security solution, and in some cases, as with Endpoint Protection, the SaaS security solution is designed in order to avoid even this cost.

IT organizations may also have to deploy a desktop application to allow the endpoint protection to run and communicate with the servers hosted by the vendor.

Scaling the infrastructure and the costs associated with growth are fully the responsibility of the SaaS provider.

Ongoing operations and support costs

Traditional Security Solutions

- IT organizations will have to allocate resources for monitoring, supporting and maintaining the security solution.
- If the solution is new to the company, the IT organization will have to train and certify existing personnel and/or recruit new personnel with or without preexisting application knowledge.
- In addition, every time a patch or upgrade needs to be deployed, additional IT resources will be required.
- This is typically the biggest hidden cost that needs to be considered when making the decision to buy a new application. If this cost is incorrectly estimated, any effect on revenue or cost reduction can greatly change.
- Support is the final and most critical success factor to the successful adoption and ongoing use of a new security solution: whenever there is a problem, this can lead to a loss in productivity or in the worst case a refusal to use the security solution.

SaaS Security Solutions

SaaS vendors are responsible for the end to end delivery of the solution and operate the infrastructure which hosts the SaaS security solution.

Intangible costs

While the intangible costs are harder to measure and therefore are more difficult to include in a Total Cost of Ownership analysis, they are no less real. Some of the intangible cost factors that affect Total Cost of Ownership include:

- **Reliability and availability:** Failed interactions mean lost employee time and lost opportunities, and may require repeated efforts to persuade users to retry the technology with increasing resistance. What service level does the SaaS vendor offer and how do they compare to the internal service level the IT organization offers?
- **Interoperability:** How easy is it to integrate with other applications?
- **Extensibility:** How easy is it to customize the application to meet the needs of the organization?
- **Scalability:** As users' needs grow, the original system may not keep up. "Busy signals" or functional limitations consume employee time and mean lost opportunities. How well can the SaaS vendor accommodate growth and what are the costs associated with growing the internal application?
- **Capacity:** Usage and adoption within the enterprise is difficult to predict, making management capacity difficult. The tradeoffs are poor performance on the one hand or underutilized infrastructure on the other. With SaaS this is more easily managed when compared to an internal application.
- **Opportunity costs:** The human resource and capital expenditures required by an in house implementation come at the expense of other projects or could possibly delay the rollout of new products and services, both of which have a direct impact on the company's bottom line.

03 The Total Cost of Ownership calculation and comparison

Example I: A single site with 50 seats

This first example concerns a medium sized business with 50 workstations and servers that must be protected against malware, and compares the cost of three on-premise traditional security solutions with that of using Endpoint Protection, Panda Security's SaaS security solution.

Around two man-days should be estimated for implementing a traditional security solution (installation, integration and configuration), with an additional half-day for the upgrade every year. With Endpoint Protection, this time is reduced to approximately one half-day, which is required to configure the solution. With an on-premise security service, regular maintenance is limited to maintaining the configuration, i.e. modeling corporate security regulations on the solution.

As this type of solution presents considerably greater challenges to administrators, significant time for monitoring and for further training must also be factored in. All in all, around 6 man-days a year should be estimated for maintaining an on-premise traditional security solution. While with Endpoint Protection, a SaaS security solution, no time is needed for training, monitoring and administrating the server and the software, this time is therefore is reduced to around 2 man-days a year.

If we estimate the cost of a man-day at €400, it becomes apparent that the administrative costs alone for a traditional solution are equal to the acquisition cost.

This example is not, however, a true like for like comparison, as a SaaS service such as Endpoint Protection uses redundant technology to ensure continuous uptime, while an on-premise solution represents a single point of failure. Companies wishing to implement more redundant systems will need to invest in a second machine, this increasing the administration costs accordingly.

In order to simplify the analysis, we have not considered the benefit of scalability, extensibility and the opportunity cost saving that a hosted service offers.

The Total Cost of Ownership analysis shown in this example demonstrates that the Endpoint Protection service requires €4,150 for the first year and €6,525 for two years. The traditional security solutions demand higher first year expenses due to the management server and maintenance costs.

Even with a conservative estimate of the cost associated for Vendor 1, Vendor 2 and Vendor 3, the company needs to spend €7,189 during the first year for the traditional Security Solution A, €7,315 for the Solution B and €7,663 for the Solution C.

Two-years expenses with Endpoint Protection come to €6,525 while with on-premise traditional solutions expenses are, €10,853, €10,867 and €13,797 respectively.

For one-year licenses, Endpoint Protection Service is cheaper by about 42% than the traditional Security Solution A, 43% cheaper than the traditional Security Solution B and 46% cheaper than the traditional Security Solution C.

For two-year licenses, Endpoint Protection is 40% cheaper than the Security Solution A and B and 53% cheaper than Solution C.

Cost Analysis	Traditional Security Solution A	Traditional Security Solution B	Traditional Security Solution C	Endpoint Protection
Initial Cost				
Capital Expensive:				
Software or License costs	0 €	0 €	0 €	0 €
Hardware (management server)	1.400 €	1.400 €	1.400 €	0 €
Operating System (management server)	250 €	250 €	250 €	0 €
Design and Deployment Costs:				
Design and Engineering (days)	1	1	1	0
Design and Engineering (cost)	400 €	400 €	400 €	400 €
Integration/Deployment (days)	1	1	1	1
Integration/Deployment (cost)	400 €	400 €	400 €	200 €
Year 1				
Capital Expensive:				
Software or License costs	3.203 €	3.218 €	6.147 €	4.725 €
Design and Deployment Costs:				
Integration/Deployment (days)	1	1	1	0
Integration/Deployment (cost)	200 €	200 €	200 €	0 €
Ongoing Infrastructure, Operations and Support Costs:				
IT Staffing (days)	6	6	6	2
IT Staffing (cost)	2.400 €	2.400 €	2.400 €	800 €
Year 2				
Design and Deployment Costs				
Integration/Deployment (days)	0,5	0,5	0,5	0
Integration/Deployment (cost)	200 €	200 €	200 €	0 €
Ongoing Infrastructure, Operations and Support Costs:				
IT Staffing (days)	6	6	6	2
IT Staffing (cost)	2.400 €	2.400 €	2.400 €	800 €
Total Cost (2 Years)	**10.853 €**	**10.868 €**	**13.797 €**	**6.525 €**

Note: The solutions analyzed offer the same security functions for corporate workstations and servers. The calculations are based on the need for a dedicated security server, although it could be possible to run traditional endpoint security solutions on an existing server. The costs for management servers (hardware and software), design, deployment, ongoing operations and support were obtained from interviews with small and medium businesses. Licenses costs were taken from each traditional endpoint security solution vendor's official on-line store and information available on the Internet in February 2009.

Example II: Three sites with 50 seats

The discrepancy between on-premise traditional security solutions and Endpoint Protection, Panda Security's SaaS security solution, becomes considerably clearer when we look at a company with multiple offices. If we imagine that the 50 users from the aforementioned example are distributed among three company sites, each site will need its own management server, which must then be installed and maintained.

While it is certainly possible to install lowerspec systems at each location than the 50 user system installed at the main office, the total acquisition costs still increase considerably.

Administration costs are also much higher for companies with distributed environments and multiple locations. As many administrative tasks can, however, be performed centrally for all locations, the costs do not increase in proportion to the number of installations. Support costs and costs incurred due to lost productivity remain the same, as these factors depend largely on the number of employees and the type of solution.

The cost of implementing an on-premise traditional security solution in a company with three sites is around 50% higher than supporting the same number of users at a single location. With Endpoint Protection the number of locations makes no difference to the service costs, as these are based solely on the number of users. The administration costs, too, remain the same, as the service can be wholly managed centrally from a single office.

Even with a conservative estimate of the cost associated for Vendor 1, Vendor 2 and Vendor 3, the company needs to spend €9,774 during the first year for the traditional Security Solution A, €9,900 for Solution B and €10,248 for the Solution C.

Two years' expenses with Endpoint Protection are €6,525, while with traditional solutions expenses are €14,703, €14,717 and €17,647 respectively.

For one year licenses, Endpoint Protection Service is cheaper by about 42% than the traditional Security Solution A, 43% cheaper than the traditional Security Solution B and 46% cheaper than the traditional Security Solution C.

For two year licenses, Endpoint Protection is 40% cheaper than the Security Solution A and B and 53% cheaper than Solution C.

Cost Analysis	Traditional Security Solution A	Traditional Security Solution B	Traditional Security Solution C	Endpoint Protection
Initial Cost				
Capital Expensive:				
Software or License costs	0 €	0 €	0 €	0 €
Hardware (management server)	2.250 €	2.250 €	2.250 €	0 €
Operating System (management server)	250 €	250 €	250 €	0 €
Design and Deployment Costs:				
Design and Engineering (days)	2	2	2	0
Design and Engineering (cost)	600 €	600 €	600 €	0 €
Integration/Deployment (days)	2	2	2	1
Integration/Deployment (cost)	600 €	600 €	600 €	200 €
Year 1				
Capital Expensive:				
Software or License costs	3.203 €	3.218 €	6.147 €	4.725 €
Design and Deployment Costs:				
Integration/Deployment (days)	0,8	0,8	0,8	0
Integration/Deployment (cost)	300 €	300 €	300 €	0 €
Ongoing Infrastructure, Operations and Support Costs:				
IT Staffing (days)	9	9	9	2
IT Staffing (cost)	3.600 €	3.600 €	3.600 €	800 €
Year 2				
Design and Deployment Costs				
Integration/Deployment (days)	0,8	0,8	0,8	0
Integration/Deployment (cost)	300 €	300 €	300 €	0 €
Ongoing Infrastructure, Operations and Support Costs:				
IT Staffing (days)	9	9	9	2
IT Staffing (cost)	3.600 €	3.600 €	3.600 €	800 €
Total Cost (2 Years)	**14.703 €**	**14.718 €**	**17.647 €**	**6.525 €**

Note: The solutions analyzed offer the same security functions for corporate workstations and servers. The calculations are based on the need for a dedicated security server, although it could be possible to run traditional endpoint security solutions on an existing server. The costs for management servers (hardware and software), design, deployment, ongoing operations and support were obtained from interviews with small and medium businesses. Licenses costs were taken from each traditional endpoint security solution vendor's official on-line store and information available on the Internet in February 2009.

panda

pandasecurity.com