PANDA CLOUD OFFICE PROTECTION

*Simply... **Evolution***

TOTAL COST OF OWNERSHIP OF PANDA CLOUD OFFICE PROTECTION

PANDA CLOUD OFFICE PROTECTION

PANDA CLOUD EMAIL PROTECTION

PANDA CLOUD INTERNET PROTECTION

Index

1. Executive Summary

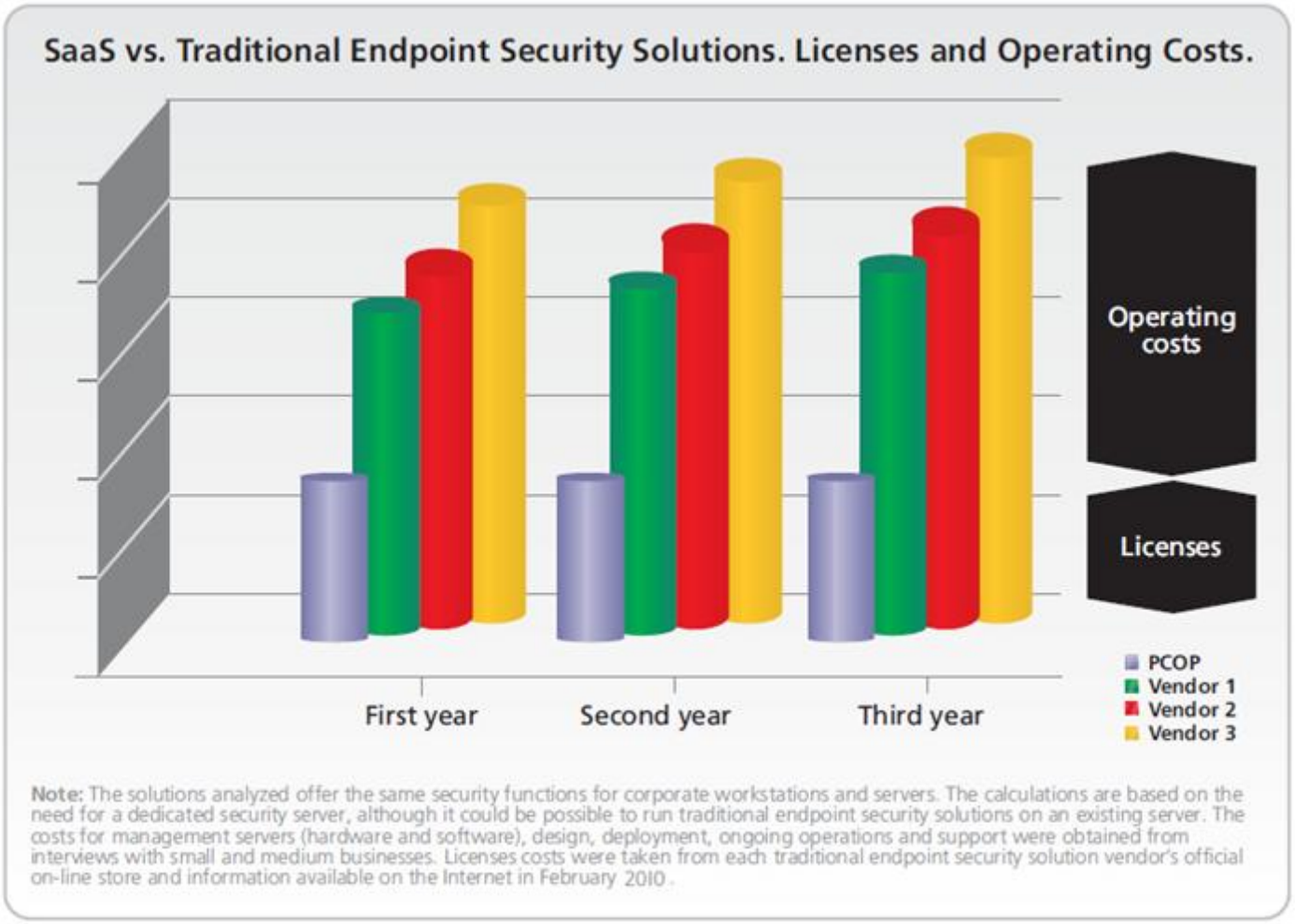
Businesses of all sizes are increasingly dependent on their IT systems to run their operations and, as a result, have become more sensitive to IT vulnerabilities and other security concerns. Add to that the increasing mobility of the workforce, the explosion in the use of mobile devices, and the inherent difficulties in managing those mobile devices, and we have a scenario in which the security management is becoming a major challenge. Much of today's IT system failures and consequent downtime is caused by human errors in the management of in-house IT and especially security solutions.

In order to address these challenges, Software-as-a-Service (SaaS) solutions have emerged which can partially or completely replace traditional, on-premise products. In the security space, the SaaS approach solves a multitude of problems around the availability of expertise in house and the need for dedicated security infrastructure. A good example is Panda Cloud Office Protection (PCOP), which provides robust anti-malware and other threat protection technologies to endpoints and can be managed by a trusted external source such as a reseller with no need for internal expertise or infrastructure.

The most obvious benefit of a SaaS solution like PCOP, when compared to traditional endpoint protection, is the lack of need for upfront investment in hardware, software, or expertise to implement it. Traditional endpoint security solutions require on-premise hardware and software investment (management and repository servers and databases), which in itself introduces the potential for additional points of failure and vulnerabilities, as well as recurring maintenance and upgrade costs. The management infrastructure for a SaaS endpoint security solution, on the other hand, is hosted by the vendor and/or the vendor's trusted partner network. The more distributed the business environment, the greater the savings to be gained from switching to this approach. Considering a typical endpoint security solution implementation of an anti-malware solution in a medium-sized business with three sites, the savings generated by a SaaS-based solution can easily reach 50% of the total cost. Example cost justification which can be adapted for use in any type of business can be found later in this document.

A second important benefit of SaaS solutions accrues to the channel, which can provide value-added services to businesses associated with the SaaS installation. In the case of Panda Cloud Office Protection, channel partners can make use of a specially-designed "Partner Console", which enables them to efficiently manage the security solution across multiple customers from a single Web console, remotely, and without requiring any hardware or software investment. Those business customers in turn benefit from the aggregated knowledge gained by the reseller in managing multiple security installations.

The last primary benefit is in supporting the application of standardized policies across mobile and multi-site users. Today, controlling and managing travelling employees with laptops is a source of concern for administrators. With a solution like Panda Cloud Office Protection, the centralized, web-based, anytime anywhere management console enables businesses and their channel partners to change and apply new security policies on the fly to combat a new security threat.



2. Cost Drivers in the Total Cost of Ownership Analysis

There are a number of different cost drivers businesses should consider when estimating the total cost of ownership and consequent return on investment for any new adoption.

2.1 Capital expenses

Traditional Security Solutions
Adopting or upgrading to new security solutions frequently entails the acquisition of additional software and/or hardware, network infrastructure enhancements, monitoring and testing tools, and more. This capital expense is an up-front cash outlay before any benefit is seen from the acquisition of the security solution itself.

SaaS Security Solutions
With SaaS, 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. There are no perpetual software licenses to buy. The nature of SaaS is that you pay only for what you use.

2.2 Design and deployment costs

Traditional Security Solutions
When planning the introduction of a new security solution, much time and IT expertise is required to design, integrate and test the solution before deployment can take place. Server and networking capabilities must be assessed for capacity, evaluated for compatibility, and upgraded if necessary. Then there is training for staff, pilots to complete, and only then can final deployment be undertaken.

SaaS Security Solutions
Because the infrastructure for the solution is all external to the end user customer organization, none of the preparation work associated with deploying a traditional solution applies; the most that's likely to be needed is distribution of client agent software, which can be automated through the central management console. On the downside, there are fewer options for customization of a SaaS installation because the back end exists in a multi-tenanted environment at the vendor's data center.

2.3 Infrastructure maintenance 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, and allowances must be made for hardware repair and replacement costs.

SaaS Security Solutions
Other than possible additional Internet bandwidth requirements, there are almost no incremental infrastructure costs required to handle the growth of a SaaS security solution. The only cost incurred in scaling up an installation is the cost of additional licenses; scaling the infrastructure and the costs associated with growth are the responsibility of the SaaS provider.

2.4 Ongoing operational and support costs

Traditional Security Solutions
To ensure a traditional security solution operates at optimum efficient over time, IT organizations must allocate resources for monitoring, supporting and maintaining the solution. Typically a big hidden cost in the ongoing management of IT security is the cost of implementing patches and upgrades, all of which need to go through the same testing routine as the original installation prior to deployment across a production system. Support can also be a time and resource sink, particularly when a new security system is introduced.

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. Patching and upgrading is handled outside of the end user customer's environment, and support requirements are normally minimal.

2.5 Intangible costs

While intangible costs are by their nature harder to measure and more difficult to include in a Total Cost of Ownership analysis, they are no less real. Some questions businesses should ask themselves about intangible cost factors that can impact Total Cost of Ownership include:

Reliability and availability: System failures mean lost employee time and possibly lost business opportunities. What service level does the SaaS vendor offer and how does it compare with the internal service level an IT department can provide?

Interoperability: How easy is it to integrate with other applications?

Extensibility: How easy is t 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 can impact business productivity. How well can the SaaS vendor accommodate growth, and what are the costs associated with growing the use of an in-house installation?

Capacity: Usage and adoption within the organization is hard to predict, making managing capacity requirements difficult. The tradeoffs are poor performance on the one hand or underutilized infrastructure on the other. SaaS may require additional capacity at the outset but because most of the “heavy lifting” of the installation is handled offsite, capacity issues may balance out over time.

Opportunity costs: The human resource and capital expenditures required by an in-house implementation may come at the expense of other projects or could delay the roll-out of new products and services, both of which have a direct impact on the company's bottom line.

3. The Total Cost of Ownership calculation and comparison

To illustrate the difference or percentage between the Total Cost of Ownership of traditional anti-virus solutions and Panda Cloud Office Protestation, we will use the following scenarios.

3.1 A single site with 50 seats

The first scenario is a SMB company with 50 workstations and servers that require anti-virus security solution to protect against the increasing malware. It is a single site that has no internal IT staff and limited IT infrastructure. We have compared three on-premise traditional security solutions versus Panda Cloud Office Protection. Because on-premise traditional security solutions require hardware / software and are more complex in installation and management we have considered the cost of these expenses. As Panda Cloud Office Protection is hosted SaaS solution no hardware or software investment is required.

On-premise solutions require implementation (installation, integration and configuration) which we have estimated between 4-6hrs, we also have considered yearly software upgrade maintenance which we estimated between 2-4hrs. With Panda Cloud Office Protection, the time required for implementation is reduced by more than 50% compared to on-premise solutions, minimizing the time and cost of implementation.

Cost Analysis One Site - 50 seats	Vendor 1 Traditional Security Solution A	Vendor 2 Traditional Security Solution B	Vendor 3 Traditional Security Solution C	Panda Cloud Office Protection
Initial Cost				
Capital Expensive				
Software or License costs	$1,786	$2,087	$2,293	$1,918
Hardware (management server)	$1400	$1400	$1400	$0
Operating System (management server)	$250	$250	$250	$0
Design and Deployment Costs				
Integration/Deployment	4-6hrs	4-6hrs	4-6hrs	1-2hrs
Integration/Deployment (cost)	$400	$400	$400	$200
Software Upgrade Maintenance	2-4 hrs	2-4 hrs	2-4 hrs	Automatic
Software Upgrade Maintenance (cost)	$300	$300	$300	$0
Total Cost	**$4136**	**$4437**	**$4643**	**$2118**

3.2 Central office with two branch offices (Distributed workforce)

Scenario 2 looks at distributed workforce. An international company with 500 workstation and servers, central office is located in US with two branch offices in China and Spain needs anti-virus and firewall for endpoints and servers. Most of the IT infrastructure is located at the central office with 20% of workstations and servers dispersed to the branch offices.

In this scenario the on-premise solution will require a central administration server at the central office with two additional update servers at each branch offices.
This design will require additional investment in server hardware and server operating software. In addition to the required infrastructure the implementation (installation, integration and configuration) will require extended planning and hours/days to deploy, we have estimated 10-12 hrs for initial implementation and 4-6 hrs for yearly software upgrades.

Panda Cloud Office Protection eliminates the need for on-premise security infrastructure, no hardware or software investment is needed. Panda Cloud Office Protection is a hosted solution that is managed by Panda Security, allowing the administrator to deploy protection, manage and administer from anywhere, anytime from a single internet browser.

Cost Analysis	Vendor 1 Traditional Security Solution A	Vendor 2 Traditional Security Solution B	Vendor 3 Traditional Security Solution C	Panda Cloud Office Protection
Initial Cost				
Capital Expensive				
Software or License costs	$14,000	$14,665	$19,245	$15,140
Hardware (management server)	$4200	$4200	$4200	$0
Operating System (management server)	$750	$750	$750	$0
Design and Deployment Costs				
Integration/Deployment	10-12 hrs	10-12 hrs	10-12 hrs	2-3 hrs
Integration/Deployment (cost)	$1200	$1200	$1200	$300
Software Upgrade Maintenance	4-6 hrs	4-6 hrs	4-6 hrs	Automatic
Software Upgrade Maintenance (cost)	$800	$800	$800	$0
Total Cost	**$20,950**	**$21,615**	**$26,195**	**$15,540**

Conclusion

If we take into account all the factors that play a role in a security solution, the analysis of the total cost of ownership of Panda Cloud Office Protection compared to on-premise solutions illustrates that services managed from the cloud save considerable time and money.

Panda Cloud Office Protection is an easy-to-use, cost- effective proactive endpoint security solution, delivered by and managed from the cloud. It provides comprehensible protection and ease of management addressing the needs of today's distributed networks and mobile workforces.

Choosing a security service in the cloud guarantees a service quality, security and continuity that on-site solutions cannot offer.