WHITE PAPER

The Cost Advantages of Virtual Security Appliances

An Osterman Research White Paper

Published March 2011

SPONSORED BY

TREND MICRO™

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

OSTERMANRESEARCH

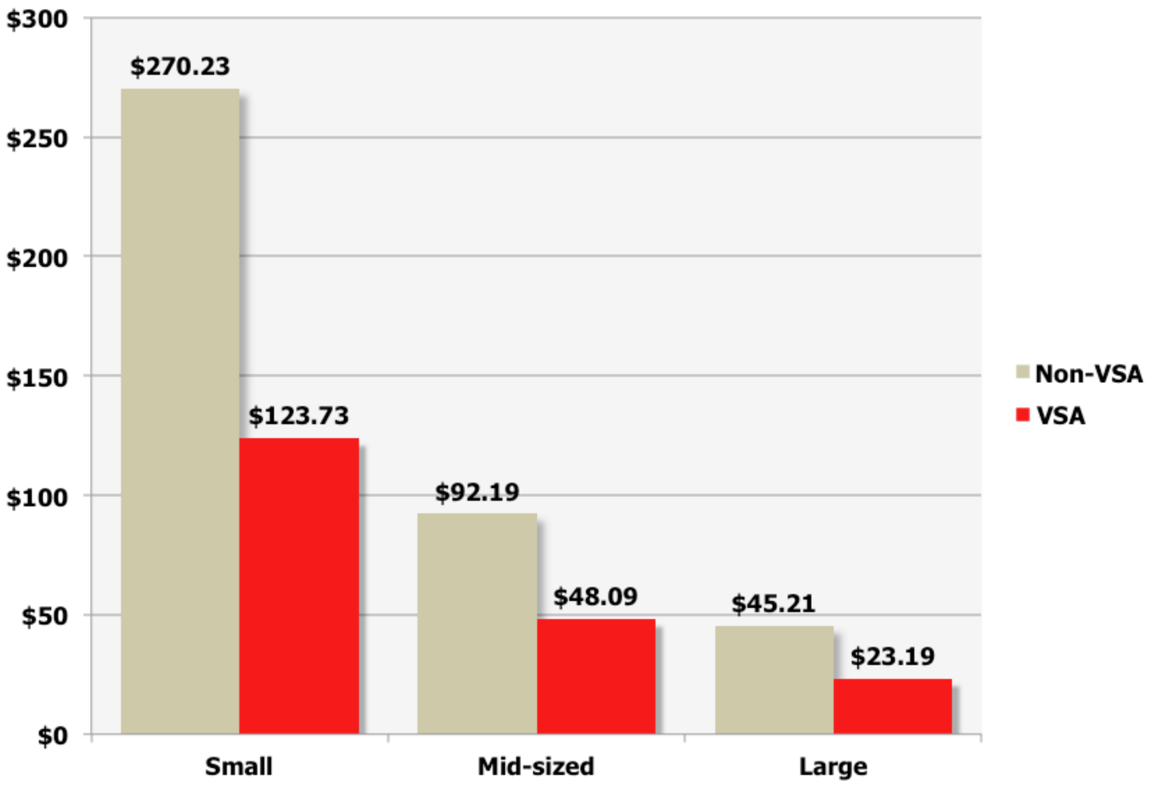
Executive Summary

The deployment model for gateway security software is evolving from software installed on servers to security appliances to hosted security solutions. However, while more security is migrating to the cloud, the majority of security solutions will remain as on-premise solutions for the foreseeable future.

Consequently, a key issue for decision makers today is the use of virtual security appliances (VSAs) – pre-built OS and software security applications that are packaged, deployed updated, maintained and managed as a single unit. Unlike a traditional hardware appliance, these virtual appliances let customers easily acquire, deploy and manage, pre-integrated solution stacks on general-purpose hardware. A VSA can be deployed either as a dedicated hardened appliance or on a virtual server, allowing the deployment of multiple VSAs on one physical server.

The allure of the VSA is that it couples the flexibility of the software paradigm with the operational and economic merits associated with a turnkey appliance. In addition, it can share in the benefits of virtual infrastructure. The primary benefit is reduced cost of ownership for any size of organization. As shown in the following figure, organizations that have made the switch to VSAs have cut their gateway security costs on average 48% to 54% (depending on the size of the organization).

Three-Year Cost of Ownership per User
Non-VSA and VSA Architectures



ABOUT THIS WHITE PAPER

This white paper focuses on the cost benefits of VSAs, presenting the results of a survey conducted specifically for this paper. It also provides a brief overview of Trend Micro and its virtual security appliance offerings.

The Benefits of Virtual Security Appliances

The benefits of VSAs, as most will recognize from virtualizing other areas of the data center, include:

- **Reduced IT costs**
  Security services focused on threat detection and remediation are simply a necessary – albeit a critical – cost of doing business. Consequently, IT organizations, CIOs, CFOs and others are seeking ways of reducing their overall IT costs. This is particularly important as new requirements are added to the mix of necessary IT expenditures, including archiving, data loss prevention, policy-based encryption, Web threat protection and the like. Reducing both IT hard (actual cash outlays for servers, etc.) and soft (downtime and opportunity) costs through virtualization and other means make more funds available for these other initiatives.

SURVEY FINDING
Organizations that deployed VSAs were able to increase the number of users per server by an average of 50%.

- **A greater number of users per server**
  Our research found that the number of users per server increased significantly when using VSAs. For example, when comparing the median number of users per server across traditional and VSA environments, the number of users per server was from 7% to 31% higher for VSA deployments depending on the server function.

- **Consolidation of servers**
  There is a strong push by many IT organizations to consolidate servers in order to ease IT staffing burdens, recover facility space, optimize assets, and reduce costs. Server consolidation offers a number of important benefits, including the ability to reassign IT staff to other initiatives and to reduce overall IT costs.

- **Increased IT department efficiency**
  As new burdens are placed on IT staff to deploy new capabilities, either in response to new threats or increasing need to advance IT services, the growth of IT staff resources does not typically keep pace with the new requirements because of budget issues, especially in a slow economy. If IT organizations do not become more efficient, they will simply not be able to keep pace with the demands placed upon them by senior managers, regulators and others.

- **Reduced Operational Costs**
  Another key benefit of virtualization is its ability to lower the costs of operating an IT infrastructure, including data center hard and soft costs.

Fewer distinct servers and proprietary appliances result in less hardware to purchase. With less hardware, IT requires less rack and floor space to support these servers and staff, which supports more compact data centers, less power consumption, and reduced overall heat load and cooling requirements. Beyond the dramatic procurement savings in servers illustrated in the example that results, the potential facilities cost savings can also be significant.

Further, less IT staff time is dedicated to managing multiple servers with various operating environments and interfaces, or proprietary appliances outside the corporate standard, thus lowering data center labor costs or shifting existing resources to more strategic projects in support of new business objectives. The use of standardized hardware can also reduce an organization's operational costs in several other ways, such as easier parts sourcing or replacement, a single vendor for support, standard change management processes, etc.

SURVEY FINDING
The use of a VSA security infrastructure has reduced IT labor requirements during a 'typical' week by 39%; labor requirements during 'bad' weeks were reduced by 50%.

Regardless of whether organizations were previously using traditional security software or appliances, the move to VSAs helped them reduce administration and associated costs 49% (in the case of organizations with more than 5,000 users) to 54% (for organizations with fewer than 1,000 users).

- **The "greening" of IT**
  While "green IT" is a relatively low priority for most organizations, a key component of green IT – reducing power consumption – is a top-of-mind priority for many. For example, between 2000 and 2005, electricity consumption by servers in the United States increased from 12 billion to 23 billion kilowatt-hours, in part because the average power consumption per server has increased dramatically[1]. Virtualization allows companies to reduce the amount of energy consumed for running servers and cooling data centers. Not only will this reduce costs, but also it will allow utilities to postpone or eliminate the construction of new energy production resources.

SURVEY FINDINGS

In order to assess the real world, quantifiable benefits of security virtual appliances in these areas, we surveyed organizations that made the transition from traditional security software and appliances to virtual appliances and combined that with market information on prevailing unit costs. Here's what we found.

- **Lower capital expenditures**
  One of the more important benefits of virtualization is the positive impact that it can have on capital expenditures for hardware and software. Most server hardware runs at just a small fraction of its total computing capacity, in large part due to the increasing use of multi-core processors. Because a number of virtualized servers can run on a single physical server, the number of servers purchased and maintained

[1] http://www.infoq.com/articles/power-consumption-servers

can be reduced. Further, underused assets, such as spares, can be more effectively integrated into a pool of available resources to address capacity management or rapid replacement of failed servers. Finally, because VSAs run on general purpose, rather than proprietary hardware, acquisition costs are substantially lower.

Fewer physical servers translate into fewer copies of operating systems, less management software and other software tools required to maintain the infrastructure, resulting in lower acquisition and maintenance costs. Virtual appliances can provide an optimized operating system for a particular application (aka JeOS – Just Enough Operating System). Further, our research found that the per user price of virtual appliance offerings was roughly 20% lower than the average from leading security software vendors. In the case of traditional appliance customers, we found that virtual appliances could also reduce the per user costs (of antispam, antivirus, URL filtering and other subscriptions) by roughly 30% above and beyond the per unit cost savings for hardware noted above.

- **Uptime and employee productivity**
  Virtualization makes it much easier to quickly provision key infrastructure elements to meet changing demand requirements without the expense of bringing additional, physical servers into a data center. In particular, improved failover, faster disaster recovery and enhanced business continuity become much more achievable and affordable. All of this translates to improved uptime and employee productivity.

SURVEY FINDING
Respondents reported that their pre-VSA security infrastructure experienced an average of 69 minutes of unplanned downtime during a typical month; with their VSA infrastructure, unplanned downtime has dropped to an average of 37 minutes.

What This Means To Your Bottom Line

As discussed, virtualization and virtual security appliances can offer a number of tangible benefits for organizations of all sizes. Providing security at the gateway into any organizations' network should address several key layers of content control which support compliance to acceptable use policies, limit legal liability, protect intellectual property, and further optimize both employee and infrastructure productivity. For example, Web capabilities should include URL filtering and customizable content control for granular web use policies, Web reputation based filtering to block zero-day threats, malware content scanning to stop viruses, etc. before threats reach the network, and proxy and caching services to optimize content delivery. Email capabilities should include anti-spam and customizable content control for granular email filtering, anti-spam and email reputation based filtering, including in-the-cloud inbound email protection to pre-filter known spam before hitting the gateway, Web reputation and malware content scanning to stop viruses and links to infected web sites before threats reach the network.

RESULTS OF THE SURVEY

Osterman Research's in-depth survey of organizations that had deployed virtualization technology for their security infrastructure helped us create a "before" and "after" picture for managing security. The goal of the survey was to determine how three-year costs of ownership compares in a non-virtualized and virtualized Trend Micro environment for the infrastructure elements and for the IT labor required to manage both environments.

We developed two different cost models: one based on differences between security software servers and a virtual security architecture and another that compared VSAs with traditional appliances. The results of the cost model found relatively little bottom line difference between the savings from software to VSA and the savings from appliance to VSA (although software customers save relatively more staff time and cost, whereas traditional appliance customers save more on hardware/license cost), and so for the sake of clarity in comparing pre- and post-virtual environments we opted to compare only VSAs and appliance-based environments.

SURVEY FINDING
Respondents estimated that their overall data center costs dropped by an average of 28% because they implemented a virtual security infrastructure.

We segmented the data into three groups: small organizations (mean of 313 users based on the survey findings), mid-sized organizations (2,275 users), and large organizations (21,050 users). We then compared the pre-virtualization and current virtualization environment in order to build a cost model comparing both environments.

Assumptions used in this analysis included a fully burdened annual salary per IT staff member of $80,000, a fully burdened annual salary per non-IT staff member of $65,000, and non-virtual appliances based on average prices of industry-leading email- and Web-security appliances obtained through secondary sources. Our findings are summarized below.

Three-Year Cost of Ownership, Traditional Security Appliances

Cost Element	Small	Mid-Sized	Large
Number of users	313	2,275	21,050
Three-year cost of IT labor	$180,506	$292,874	$611,897
Total cost of hardware	$19,070	$41,115	$148,769
Total cost of software	$42,435	$224,146	$1,304,683
Productivity impact of downtime on end users	$11,738	$71,094	$789,375
Total cost of ownership, three years	**$253,748**	**$629,229**	**$2,854,723**
Total cost of ownership per user, three years	**$810.70**	**$276.58**	**$135.62**
Total cost of ownership per user, annual	**$270.23**	**$92.19**	**$45.21**

Three-Year Cost of Ownership, Virtual Security Appliances

Cost Element	Small	Mid-Sized	Large
Number of users	313	2,275	21,050
Three-year cost of IT labor	$80,690	$147,931	$336,506
Total cost of hardware	$5,940	$18,000	$32,000
Total cost of software	$26,615	$133,825	$701,344
Productivity impact of downtime on end users	$2,934	$28,438	$394,688
Total cost of ownership, three years	**$116,179**	**$328,193**	**$1,464,537**
Total cost of ownership per user, three years	**$371.18**	**$144.26**	**$69.57**
Total cost of ownership per user, annual	**$123.73**	**$48.09**	**$23.19**

Summary

Most messaging, Web, network and other security capabilities will continue to be deployed using on-premise hardware and software, notwithstanding significant growth in both the hosted and hybrid delivery models. An increasing proportion of on-premise deployments will be "appliances" because the self-contained nature of these devices makes them easy to deploy, configure and manage.

While virtualization has been in use for decades, it has become a hot topic of conversation in IT departments because of increasing requirements to reduce IT costs, improve the availability of the IT infrastructure, to reduce power requirements, and to make IT departments and staff more efficient. Our work with organizations that have made the transition to virtual security appliances shows that the average organization saves a significant 45-55% of their previous security spend on hardware, software, administrative and downtime costs.

BOTTOM LINE
The average organization that deploys VSAs saves a significant 48-54% of their previous security spend on hardware, software, administrative and downtime costs.

Trend Micro is a leading vendor that offers a growing array of virtual security appliances, allowing organizations of all sizes to realize the benefits that virtualization can provide while maintaining their security posture.

About Trend Micro's Virtual Appliance Offerings

Today, Trend Micro gateway security solutions defend organizations against Internet content security threats including spam, unwanted web content, spyware, phishing, viruses, Trojans, and other malware as well as protecting sensitive information with content filtering and encryption.

Trend Micro's software virtual appliances, InterScan Web Security Virtual Appliance and InterScan Messaging Security Virtual Appliance, support both VMware ESX/vSphere virtual machine environments (virtual appliances), as well as "bare metal" installations for non-virtualized environments (software appliances). Customers have a choice to deploy Trend Micro software virtual appliance security solutions as either a virtual appliance in a VMware virtual machine environment, or a software appliance on a dedicated server platform – whichever is the best fit for their IT needs.

TREND MICRO VMWARE READY VIRTUAL SECURITY APPLIANCES

The following Trend Micro gateway security products are VMware Ready validated virtual appliances, rigorously tested and supported in environments when minimum system requirements are fulfilled. VMware has tested and certified the Trend Micro VSAs including support for the Trend Micro VSA guest operating system. More information is available at www.vmware.com/appliances.

TREND MICRO ENTERPRISE SECURITY FOR GATEWAYS

- InterScan Web Security Virtual Appliance
- InterScan Messaging Security Virtual Appliance
- Advanced Reporting and Management
- Email Encryption Gateway

Certified by Trend Micro

A key feature of Trend Micro's software appliances is the Certified by Trend Micro program. This program ensures that certified software appliances have been properly integrated with Trend Micro software, tested for compatibility and validated to Trend Micro's performance standards.

The advantage of the Certified by Trend Micro certification process is that it ensures customers that their software appliance will run seamlessly with Trend Micro security solutions, that configuration of the systems will be kept to a minimum, and that the cost of deployment is as low as possible. It also ensures that hardware solutions have been completely vetted and meet Trend Micro's standards for compatibility and performance.

About Trend Micro

Trend Micro Incorporated, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks, and the newest Web threats. Its flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe.

ABOUT THIS WHITE PAPER

This white paper, sponsored by Trend Micro, discusses the benefits of deploying security applications as virtual appliances for organizations that want to improve the efficiency of their IT infrastructure and to lower its cost. This white paper offers some information on Trend Micro's virtual security appliances and their Enterprise Security for Gateways solution suite.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statue, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.