Virtual Security Appliances: A Business Case to Move Off Gateway Hardware Appliances

An Osterman Research White Paper

Published May 2010

SPONSORED BY

TREND MICRO™

Why Should You Read This White Paper?

TRENDS IN THE IT INDUSTRY

There are a variety of important trends developing in the IT industry as organizations of all sizes look to reduce costs, improve employee productivity and gain competitive advantage from the large and growing number of infrastructure elements they have deployed and plan to deploy over the next few years. These trends are driven by a variety of factors, not least of which are the continuing challenges in the economy and the growing sophistication of Web-based and more traditional threats. Among these trends are:

- **Faster software innovation**
  The pace of software innovation, particularly with regard to security, is proceeding faster than the financial lifecycle of the infrastructure that most organizations will deploy. Much of this innovation is being driven by the increasingly sophisticated threats coming from the Internet, growing use of Web 2.0 applications and the increasing risk associated with data loss.

- **A desire for an integrated solution**
  The vast majority of organizations want an integrated, gateway solution to security because of the growing number of blended threats (e.g., spam containing links to malware-laden Web sites) and because they can achieve efficiencies in the IT staff time devoted to managing security and other capabilities.

- **Greater availability of multi-core processors**
  The growing base of multi-core processors is dramatically increasing the level of computing performance available, but at decreasing costs on both an absolute level and on a price-per-performance basis.

- **A desire for non-proprietary solutions**
  Decision makers are increasingly interested in non-proprietary hardware options because of their desire for standardizing computer assets and the growing requirement to be more agile – these trends are particularly important in a challenging economy.

Why You Should Focus on Virtual Appliances

While virtualization has been in use for more than 30 years, starting first in mainframe environments, it has found renewed interest in recent years as virtualization technologies focus on cost effective server hardware. And because of the convergence of excess computing capacity, adoption of Web applications and private/public cloud computing, and the need to stretch IT resources to the extent practically possible, adoption of platforms such as VMware vSphere have exploded. The result has been growth in the number of offerings that can take advantage of virtualization technologies and decision makers' willingness to embrace them.

VIRTUALIZATION OFFERS MANY IMPORTANT BENEFITS

So, why should organizations of any size be interested in virtualization for their content security functionality (and market research shows that most mid-sized and large organizations have already done so[1])? There are a variety of reasons:

- Virtualization can reduce hardware and related costs by allowing multiple servers to run on the same hardware platform. For example, an email or unified communications server, a Web security server and/or a mobile messaging server could all run on the same physical server, significantly reducing hardware requirements, IT labor requirements and power consumption.

- Virtualization can make it much easier to add additional capacity to the existing infrastructure.

- Disaster recovery and business continuity can be improved because virtualization makes it easier and more affordable to add redundant capacity to the infrastructure.

- Maintenance tasks can be made significantly easier.

- Virtual Appliances are pre-built software solutions, comprised of one or more Virtual Machines that are packaged, updated, maintained and managed as a unit. Unlike a traditional hardware appliance, these virtual appliances let customers easily acquire, deploy and manage, pre-integrated solution stacks.

LONG-TERM GROWTH OF VIRTUALIZATION

In some ways, the drivers for virtualization are not dissimilar to the drivers for SaaS (software as a service): reducing on-premise hardware under management, reducing IT labor required for managing an IT infrastructure, and reducing power requirements are driving virtualization as they are driving demand for SaaS services.

As shown in the following figure, decision makers anticipate that their use of virtualization will increase significantly over the next couple of years for infrastructure elements like email servers, email security servers and Web security servers.

---

[1] *Channel Insider*, January 10, 2010 (http://is.gd/82afy)

Distribution of Virtualized Servers by Type
2009-2011
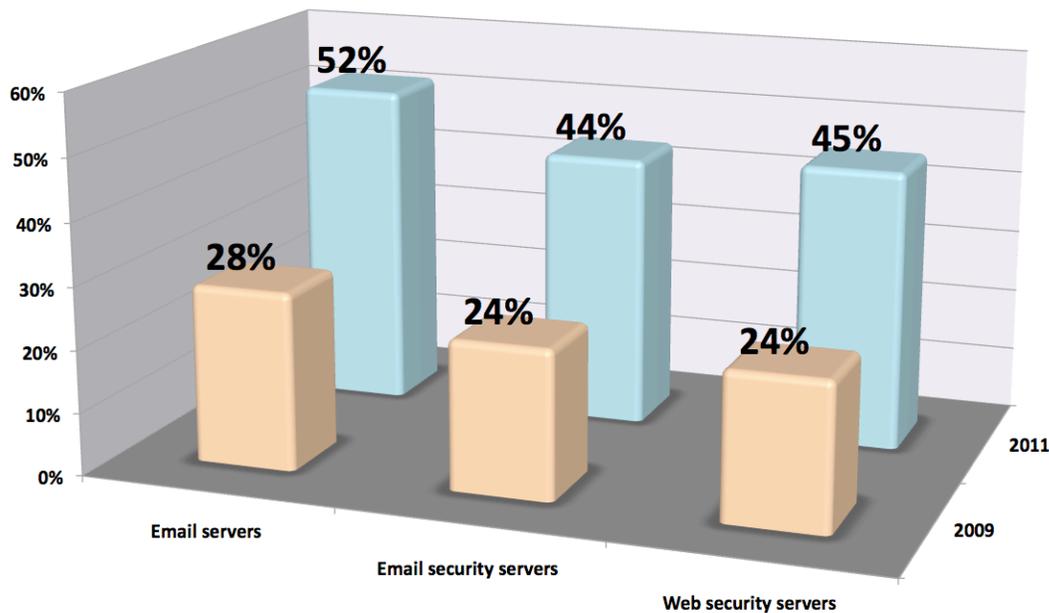
In short, the virtual appliance couples the flexibility of the software paradigm with the operational and economic merits associated with a turnkey appliance that can share in the virtual infrastructure.

Comparing Virtual Appliances With Traditional Models

WHAT MAKES VIRTUALIZATION INTERESTING?

Virtualization, at its most basic level, is focused on disengaging an application or service from the physical infrastructure required to make that service available. The goal in virtualization is any or all of several things, including lowering the cost of managing the infrastructure, improving its flexibility and using excess computing capacity to its best advantage.

Because virtualization permits the separation of applications and services from the physical hardware on which they run, there are a number of important advantages that organizations can realize as they move toward a virtualized model in addition to those noted above:

•   Rapid provisioning to meet capacity requirements. For example, a virtualized security server can be brought much more quickly in response to a spam storm or other external threat than would be the case with physical servers.
•   Greater flexibility in resource allocation, allowing services to be deployed wherever they are needed.

- Allowing a common management framework for optimizing IT services.

- Greater efficiency in managing the IT infrastructure, including more efficient load balancing, improved failover, faster disaster recovery and enhanced business continuity.

KEY DRIVERS FOR VIRTUALIZATION

There are a number of important "macro" drivers that are motivating organizations of all sizes to consider the use of virtualization for at least some of the functions in their infrastructure, including:

- **Cost reduction**
  For most organizations, IT is simply an expense. 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.

- **Making IT departments more efficient**
  Similarly, IT departments must become more efficient. 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.

- **Improving disaster recovery and business continuity**
  Messaging, Web systems and collaboration applications are mission-critical for most organizations and are becoming more so as information exchange via the Internet becomes more prevalent. As a result, capabilities must be deployed that can ensure the availability of these systems as close to 24x7 as possible. 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.

- **The need to maximize investments and resources**
  Virtualization allows organizations to consolidate servers, optimize their underused hardware and staff resources, reduce their capital expenditures and reduce the costs associated with managing security and other parts of the IT infrastructure.

- **Requirements to optimize the IT infrastructure**
  Growth in the number and variety of external threats, the risks associated with inadvertent data loss, government requirements to protect the integrity of sensitive

data, and other factors are necessitating the addition of new capabilities on a regular basis. As a result, the overall IT infrastructure must be optimized in order to accommodate these ever-increasing obligations.

• **Server consolidation**
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. For example, a 2009 survey by Osterman Research found that 58% of organizations have consolidated their email servers in a single data center; a 2006 survey found that only 34% of organizations had done this.

Server consolidation offers a number of important benefits, including the ability to reassign IT staff to other initiatives and to reduce overall IT costs.

• **The "greening" of IT**
Between 2000 and 2005, the electrical power consumed by servers doubled, a trend that continues today because of two factors: a) increasing numbers of servers in data centers and b) greater power consumption per server (from 50 watts per server before 2000 to 250 watts per server in 2008)[2].

By reducing the amount of energy consumed for running servers and cooling data centers, organizations can dramatically reduce their costs, not to mention the positive impact this will have on postponing or eliminating the construction of new energy production resources.

LOWER CAPITAL EXPENDITURES
One of the more important benefits of virtualization is the positive impact that it can have on capital expenditures in a number of areas:

• **Hardware**
Because a number of virtualized servers can run on a single physical server, hardware acquisition and maintenance costs can be dramatically reduced. Underused assets, such as servers that are treated as spares, can be more effectively integrated into a pool of available resources to address capacity management or rapid replacement of failed servers.

• **Software**
Similarly, because fewer physical servers are required, fewer copies of operating systems, management software and other software tools are 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).

• **Use of excess computing capacity**
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. The result is that

---

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

virtualization can result in significantly improved utilization of existing or new hardware resources by taking advantage of these spare CPU cycles.

REDUCED OPERATIONAL COSTS

Another key benefit of virtualization is its ability to lower the costs of operating an IT infrastructure, including:

- **Data center costs**
  Hard costs: Fewer distinct servers and proprietary appliances result in simply 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 follows, the potential facilities cost savings can be dramatic.

  Soft costs: Less IT staff time is dedicated to managing multiple servers with various operating environments and interfaces, thus lowering data center labor costs or shifting existing resources to more strategic projects in support of new business objectives. Through one VMware management console IT professionals can manage multiple physical and virtual servers in a number of locations.

- **IT lifecycle management costs**
  In addition to reduced capital expenditures and lower operational costs, virtualization offers a number of other benefits. For example, because an organization can operate fewer physical servers and less software in a virtualized environment, generally fewer IT staff members will be required to operate the infrastructure. This results in the ability to redeploy these staff members to other projects that offer greater value to the organization.

The use of standardized hardware can also reduce an organization's operational costs in several other ways:

- When upgrades or expansion are required for the on-premise infrastructure, pre-specified, pre-sourced components can simply be pulled off the shelf to rapidly execute these upgrades or new capabilities instead of specifying new appliances or servers.

- Support is easier, since only a single platform needs to be supported instead of multiple appliances from (potentially) multiple vendors.

- Change management practices can be optimized because of the use of a limited number of hardware elements.

- Using standardized hardware from a single vendor provides an organization with a single point of contact for problem resolution, technical support, etc.

In short, the use of software virtual appliances built from industry-standard hardware can result in significantly reduced operational costs compared to hardware appliances.

This is because of a reduction in managing multiple vendors, multiple contracts and multiple configurations that help to minimize complexity and increase IT flexibility.

OTHER BENEFITS FROM THE VIRTUAL APPLIANCE APPROACH

In addition to the reduced capital and operational costs provided by the use of virtual appliances, other benefits of this approach include:

- The ability to add new features and capabilities without having to "rip-and-replace" parts of the existing appliance infrastructure. This reduces the overall cost of an on-premise infrastructure.

- Because the use of virtual appliances can reduce the overall operational costs and IT time investments necessary to manage a security infrastructure, IT staff time can be freed and used for projects that offer greater value to an organization

- Using virtual appliances allows IT staff to respond more quickly to needed changes in the infrastructure, such as when new capabilities must be redeployed quickly.

WHAT IS DRIVING THE ADOPTION OF VIRTUAL APPLIANCES?

One of the chief benefits of the virtual appliance model is that it can reduce the overall costs of managing an IT infrastructure in three ways:

1. By reducing IT staff time required to specify, deploy, configure and maintain different infrastructure elements.

2. By lowering the overall cost of software and hardware.

3. By deploying standardized virtual appliances that can be used for a variety of applications within the data center, costs can be reduced still further while increasing the operational flexibility of the infrastructure.

OTHER BENEFITS

IT organizations that are managing a virtualized infrastructure can respond more quickly to needed changes in the infrastructure. For example, if a rapid increase in spammer activity drives up spam volumes by 20% during a very short period of time, an IT organization can more easily, more quickly and less expensively add additional security servers in a virtualized environment than they could in a conventional IT environment. This allows IT organizations to be far more nimble and responsive than would otherwise be possible.

Further, because there are fewer physical servers in the infrastructure, setting up redundant servers for disaster recovery and business continuity purposes is made easier and less expensive.

An Example of Virtualization's Hard Cost Savings

- Virtualization and Virtual security appliances can offer a number of tangible benefits for organizations of all sizes, although many of the benefits are most profound for larger organizations. 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 employ and infrastructure productivity.

  Web:
  - 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
  - Proxy and caching services to optimize content delivery

  Email:
  - 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
  - Malware content scanning to stop viruses, etc before threats reach the network

Review of a 3,000-Seat Organization

The following table demonstrates the cost savings for a Trend Micro virtual security appliance solution compared to the average of three leading messaging and web content security appliances. For purposes of this comparison, we chose three robust, market-leading systems offered by Blue Coat (ProxySG 810, ProxyAV 810 and Proofpoint P845), McAfee (Web Gateway WG-5000 [Webwasher] and Email Gateway EG-5000 [IronMail]) and Cisco (IronPort S660, M660 and C660). It is important to note that:

- We have used list prices for this analysis.

- The analysis does not take into account other "total" costs.

- The analysis does not take into account the associated savings of consolidating key security layers, including premise and cloud-based components.

**Selected Gateway Web and Messaging Content Security Appliance
Prices to Support 3,000 Users**

Vendor	Web Gateway Security	Messaging Gateway Security	Hardware Appliance Cost (Total) [1]	Software Cost per User	Total Cost	3-Year Cost per User
MEAN ACROSS THREE SYSTEMS			$102,729	Year 1: $53.17 Year 2: $34.68 Year 3: $34.68 Avg $40.85/year	$470,319	$156.77
Trend Micro	Enterprise Security for Gateways (InterScan Gateway Virtual Security Appliances)		$11,033[2]	Year 1: $27.09 Year 2: $10.84 Year 3: $10.84[3] Avg $16.26/year	$151,961	$50.65

Notes
1. *Assumes one cold standby appliance for each platform for redundancy*
2. *Assumes 33% contribution cost of shared VMware Infrastructure consisting of 3 servers.*
3. *A perpetual license and annual renewal model.*

SUMMARY OF COSTS

The average per user cost savings for Trend Micro Enterprise Security for Gateways virtual appliance solution over a three-year period, including hardware and software, is an astounding 68% less than traditional hardware appliance solutions for Web and messaging gateway security. The average per user/year cost savings for the Trend Micro Enterprise Security for Gateways virtual appliance solution, including hardware and software, is an astounding 68% less than traditional hardware appliance solutions for web and messaging gateway security.

Using the assumptions shown above, virtual security appliances will save an organization a substantial amount compared to traditional appliances, although cost savings will vary based on a number of factors, including the number of appliances in the environment, the number of vendors whose appliances are deployed in the data center, and so forth. The virtual appliance model can provide additional savings, such as volume discount purchases, greater reliability, and streamlined operations/maintenance, as discussed above.

About Trend Micro's Virtual Security Appliance Offerings

Today, Trend Micro gateway security solutions support VMware environments to defend organizations against Internet content security threats including spam, unwanted web content, spyware, phishing, viruses, Trojans, and other malware. Customers have a choice to deploy Trend Micro security solutions as software virtual appliances- as either a virtual appliance in a VMware virtual machine environment addressed here, or a software appliance on a dedicated server platform – whichever is the best fit for their IT needs.

TREND MICRO PRODUCTS THAT SUPPORT VIRTUAL SECURITY APPLIANCES

The following Trend Micro gateway security products are supported in VMware environments when minimum system requirements are fulfilled and VMware supports the guest operating system required for the Trend Micro product:

Trend Micro Enterprise Security for Gateways
- InterScan Web Security Virtual Appliance
- InterScan Messaging Security Virtual Appliance
- Advanced Reporting and Management
- Encryption for Email Gateway

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 and make IT departments and staff more efficient. With the growing adoption of virtual appliances which leverage the virtualized infrastructure organizations can realize lower total costs through the ability to use existing spare computing capacity that exists in most organizations, lower IT lifecycle management costs, reduced data center costs, and the ability for IT departments to more quickly respond to changes in the threat landscape.

Trend Micro offers a growing array of virtual appliances allowing organizations of all sizes to realize the benefits that virtualization can provide.

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.

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).

VMWARE READY BY VMWARE

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 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.