Virtualizing Email Gateway Security

Flexible, Cost-Effective Protection at the Email Gateway

August 2009

VIRTUALIZING EMAIL GATEWAY SECURITY

I. COST AND COMPLEXITY DRIVE VIRTUALIZATION EFFORTS

Virtualization initiatives have gained momentum as businesses seek ways to reduce operations costs and complexity in the face of a weak economy and rising power costs. Green IT initiatives are being launched in many organizations to help reduce the impact of rising costs on the overall enterprise bottom line. At the same time, increasingly complex IT infrastructures are demanding more management time and resources, which are already in short supply. Virtualization offers one way to help organizations address these demands.

RISING ENERGY COSTS

Today, datacenters consume almost one percent of the global electricity supply and by 2020, consumption is expected to quadruple. Electricity represents at least 25 percent of a large organization's IT costs today (Revolutionizing Datacenter Efficiency, McKinsey & Company Uptime Institute Symposium), and with the need to maintain always-on service levels for critical business applications, that percentage will likely increase. Even if datacenters maintain current electricity usage levels, costs will escalate, as demand skyrockets around the world and prices for fuel, such as coal and natural gas, rise in response.

HARDWARE FATIGUE

As infrastructure has become more complex over the past few years, many IT organizations have addressed each new challenge with a new solution. They have become inundated with a proliferation of small hardware appliances dedicated to solving single problems. Deploying and managing new servers or dedicated hardware appliances for each of these applications adds to the increasing costs and complexity of maintaining the datacenter. In addition to the increased need for more rack space, IT organizations find the myriad of servers and hardware appliances with differing management interfaces complex to manage.

COMPLEX SERVER ENVIRONMENTS

Traditional server deployments typically require a lengthy procurement, installation, configuration, testing, and deployment cycle, which slows an organization's ability to deploy critical applications. At the same time, few servers are fully utilized, which increases total cost of ownership. Virtual machines are more efficient and easier to deploy than physical servers and traditional software.

II. EXTENDING VIRTUALIZATION TO MORE DATACENTER FUNCTIONS

With significantly lower initial and operational costs, the move to virtualizing infrastructure is compelling. Adopting a simple virtualized infrastructure can reduce annual server costs per user by up to 35 percent, when compared with a physical static x86 server configuration. Infrastructures with more than 25-percent virtualization, storage virtualization, and systems management tools can reduce costs by up to 52% per user per year (IDC, Business Value of Virtualization: Realizing the Benefits of Integrated Solutions, July 2008).

For this reason, the concept of virtualization is being extended beyond simply virtualizing servers that host business and web applications, to virtualizing other datacenter functions such as network gateway security applications.

WHAT ARE VIRTUAL APPLIANCES?

A virtual appliance includes a pre-installed, pre-configured operating system and an application stack that is packaged, deployed and maintained, updated and managed as a unit that operates on a virtualized platform. As pre-packaged units, they simplify deployment and administration because automated patching and updates come from a single vendor. With no need to provision extra power, cooling capacity or hardware, virtual appliances can provide additional functionality with little, or no, added environmental impact. Organizations are implementing virtual appliances for capabilities that range from business intelligence and document management to backup, network monitoring, application development and security.

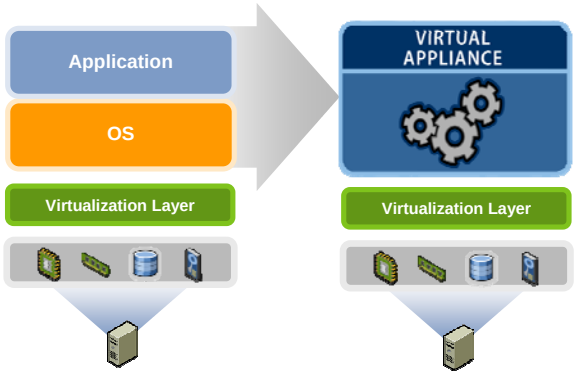

Figure 1: A virtual appliance packages an application and an operating system together as a cohesive unit

WHY VIRTUAL APPLIANCES FOR GATEWAY EMAIL SECURITY APPLICATIONS?

Email security is especially well suited for the cost savings and increased efficiency of a virtual appliance deployment. Email is critical to conducting daily business, which is why even in tough economic times, nearly 60 percent of enterprises plan to increase spending on email security, according to IDC. Spam continues to proliferate, which quickly burdens physical servers and taxes management resources, and with extreme fluctuations in spam volumes, server capacity needs are unpredictable. Organizations must face difficult choices between unplanned spending on additional capacity to minimize the impact of high spam volumes on the business, or putting up with decreased performance and user dissatisfaction.

Many organizations plan to use virtual appliances to achieve their email gateway security goals. Osterman Research estimates that up to 39 percent of antivirus and antispam servers will be virtualized by 2010 (Why You Need to Consider Virtualization, September 2008). In addition, IDC found that 34 percent of organizations are planning to adopt virtual security appliances for email security over the next 12 months, and large organizations (10,000+ employees) will be the most aggressive adopters at 48 percent (IDC Messaging Security Survey: The Good, Bad, and Ugly, February 2009). Virtual Security Appliances will also be the fastest growing segment of the Messaging Security market, growing from $17M in 2008 to $525M in 2013, representing a 98-percent compound annual growth rate (IDC Worldwide Messaging Security 2008 Vendor Shares and 2009-2013 Forecast).

BENEFITS OF DEPLOYING A VIRTUAL APPLIANCE ON VMWARE

Messaging security virtual appliances in a VMware environment deliver the same cost benefits at the gateway as virtualized solutions deliver for other datacenter needs, namely lower costs, a smaller footprint, simplified management, and ease of deployment. They also have the additional benefits of significantly reduced initial start-up costs and lower maintenance and management costs, which deliver a lower total cost of ownership over traditional email gateway protection solutions.

Simplified Deployment and Management Saves Time

With a virtual appliance, configuration, installation, patching and testing time is reduced, which lowers overall administrative and management costs. Patching of the entire virtual appliance (both the application and the operating system) is automatically delivered by one vendor, further reducing the amount of management time needed. VMware vCenter Server provides monitoring and health checks on the virtual appliances in the VMware environment, simplifying management.

Business Continuity for Email Gateway Protection

Building on the high availability and scalability features of VMware, messaging security virtual appliances can also play a key role in supporting business continuity strategies. VMware Data Recovery further provides fast, simple, data backup and recovery for virtual machines.

Highly Available Email Gateway Protection

Messaging security virtual appliances are also designed for large-scale enterprise deployment. The VMware Infrastructure and VMware vSphere environments provide resiliency for all components of a virtual appliance, enabling enterprises to deliver on the enterprise IT objectives of reliability, scalability, redundancy, and availability. Messaging security virtual appliances also take advantage of VMware features for distributed enterprises, including:

- **VMware VMotion:** Eliminates the need to schedule application downtime due to planned server maintenance through live migration of virtual machines and virtual appliances across servers, with no disruption to users or loss of service.
- **VMware Fault Tolerance:** Provides continuous availability, without any data loss or downtime, to virtual appliances and applications.
- **VMware High Availability:** Provides cost effective, automated restart within minutes for all applications in the event of hardware or operating system failures.

SCALABILITY FOR CLUSTERED ENVIRONMENTS

VMware Infrastructure and VMware vSphere also support infinite email gateway protection scalability for clustered environments. Datacenter managers can support more users with less effort while helping ensure high performance. The VMware Distributed Resource Scheduler continuously monitors utilization across resource pools and dynamically load-balances server resources to deliver the right resources to virtual messaging security appliances, maximizing protection based on business priority.

III. VIRTUAL APPLIANCES AND VAPPS FOR CLOUD COMPUTING

The vCloud Initiative of VMware delivers enterprise-class cloud computing, by federating compute capacity on demand between virtual datacenters and cloud service providers to support existing and new applications. The VMware vCloud Initiative is aimed at helping companies, both large and small, safely tap compute capacity inside and outside their firewalls—how they want, when they want, and as much as they want—to ensure quality of service for any application they want to run, internally or as a service.

In addition, the VMware vCloud Initiative can leverage the large range of applications supported by software vendors running on VMware, as well as the growing ecosystem of VMware Ready Virtual Appliances. With VMware Ready Virtual Appliances, deploying new applications to the cloud or on-premise becomes very simple. VMware partners such as Trend Micro are leveraging VMware Ready Virtual Appliances to enable easy patching, management, and migration of applications in and out of cloud services.

In order to enable a smooth transition to cloud strategies, VMware has introduced vApps— the next generation of virtual appliances. A vApp is a pre-built software solution, consisting of multiple virtual machines, packaged and maintained as a single entity in the industry standard Open Virtualization Format (OVF). vApps typically encapsulate all components of a complex, multi-tier application as well as the operational policies and service levels associated with it. Best defined as self-managing and self-describing entities, vApps comprise any applications running on any OS, and provide a mechanism for customers to move their applications between internal clouds or external clouds while retaining the same service levels. This makes them ideal containers for cloud computing. vApps can be created with and managed through VMware vSphere 4.0

IV. TREND MICRO MESSAGING SECURITY VIRTUAL APPLIANCE, VMWARE READY

Trend Micro and VMware are helping customers achieve datacenter transformation by maximizing their virtualization initiatives with flexible, secure solutions. The Trend Micro™ InterScan™ Messaging Security Virtual Appliance is VMware Ready validated to complement virtualized environments with comprehensive email protection at the gateway. VMware Ready solutions ensure baseline interoperability and higher levels of integration with VMware products. With the VMware Ready logo, customers know that the Trend Micro appliance has passed VMware-specified criteria and is optimized for VMware's Virtual Datacenter operating system.

The Trend Micro InterScan Messaging Security Virtual Appliance can be deployed as a dedicated virtual appliance on industry-standard, bare-metal hardware or as a VMware Ready virtual appliance for deployment in VMware ESX/Infrastructure environments.

V. COMPREHENSIVE VIRTUAL GATEWAY EMAIL SECURITY

MULTI-TIERED SPAM, PHISHING DEFENSE, AND OPTIONAL ENCRYPTION

Trend Micro Smart Protection Network™ uses a combination of in-the-cloud reputation services to block a large portion of malicious email before it can hit the premises-based gateway. Defenses built into the virtual appliance provide in-depth email analysis using a variety of leading-edge techniques, such as patent-pending image spam detection, identifying malicious embedded URLs and other up-to-the-minute defenses to counter new spamming techniques. Organizations can apply automatic profiling and reputation services to stop spam and viruses, creating a firewall against DHA and bounced mail attacks. InterScan Messaging Security Virtual Appliance also uses signatures, heuristics, and reputation services to stop phishing—including corporate spear-phishing attacks.

AWARD-WINNING ANTIVIRUS AND ANTISPYWARE

Trend Micro stops virus and spyware hidden in email attachments. Powered by Smart Protection Network™, InterScan Messaging Security Virtual Appliance provides immediate protection that functions like a virtual neighborhood watch. Trend Micro's unique web reputation database captures threat intelligence from a worldwide network of customers, from consumers to large enterprises. Each attack on an individual PC adds to the database—fine-tuning Trend Micro's knowledge of a website's reputation, malware behavior, and spam sources—and enabling near-zero-hour protection.

FLEXIBLE CONTENT FILTERING

Inbound and outbound emails and attachments are scanned for inappropriate content and loss of sensitive data, based on attachment characteristics, lexicons, identifiers, and customized data rules. InterScan Messaging Security Virtual Appliance provides flexible remediation options, including company-specific legal disclaimers, quarantine emails and issue alerts; it enables policies to target senders or recipients by company, group or individual; and it supports data loss prevention, regulatory compliance and corporate governance initiatives.

VI. CUSTOMERS MOVE TO TREND MICRO VIRTUAL APPLIANCE

Trend Micro customers are extending their virtualization strategies to include virtualizing email gateway protection using Trend Micro InterScan Messaging Security Virtual Appliance.

OCHSNER HEALTH SYSTEM

Ochsner Health System is a non-profit, academic, multi-specialty healthcare delivery system in Southeast Louisiana. To manage costs as the company grows, IT has embarked on several cost-saving initiatives including consolidation of its email servers. The company's hardware-based email gateway security solution did not scale effectively, and as IT reviewed alternatives, it wanted its new solution to work well within its VMware virtualized environment. Ochsner chose Trend Micro InterScan Messaging Security Virtual Appliance because it was VMware Ready and delivered high availability and disaster recovery capabilities for email communication.

"It was very important that Trend Micro InterScan Messaging Security was validated as VMware Ready. Within our organization's virtualization initiatives, deploying a virtual appliance provided lower total cost of ownership and ease of management compared to our previous hardware appliance solution."

—Mark L. Smith, Network Administrator, Ochsner Health System

VII. VIRTUAL EMAIL GATEWAY PROTECTION IN VMWARE ENVIRONMENTS

In a tight economy it makes more sense than ever to deploy virtualized solutions for email gateway security. Trend Micro InterScan Messaging Security Virtual Appliance makes it fast and easy to gain award-winning protection and take advantage of the high-availability, scalability, business continuity, and cost-saving benefits inherent in a VMware virtualized environment.

For more information, visit the VMware Virtual Appliance Marketplace at http://www.vmware.com/appliances to learn more about virtual appliances and download a trial copy. Also, visit Trend Micro at www.trendmicro.com.

ABOUT VMWARE

VMware is the global leader in virtualization solutions, from the desktop, through the datacenter, to the cloud. VMware provides the foundation for more datacenter consolidation and virtualization initiatives than any other company. Its customers include 130,000+ organizations of all sizes across all industries including all of the Fortune 100, 96% of the Fortune 1,000 and small and medium businesses.

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. Visit TrendWatch at www.trendmicro.com/go/trendwatch to learn more about the latest threats. Trend Micro's flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe. Many of these solutions are powered by the Trend Micro Smart Protection Network, a next generation cloud-client content security infrastructure designed to protect customers from Web threats. A transnational company, with headquarters in Tokyo, Trend Micro's trusted security solutions are sold through its business partners worldwide.