

# Should You Install Messaging Security Software on Your Exchange Server?

**An Osterman Research White Paper**

*Updated August 2009*

**SPONSORED BY**



**Sunbelt Software**



## Executive Summary

---

Security is the most single critical task for any email administrator. Starting with a foundation of anti-spam and anti-virus capabilities, organizations should focus on other capabilities, as well, including policy management and a variety of other tasks designed to protect the network and the company from external and internal threats.

There are a number of ways to deploy messaging security, including appliances, software installed on dedicated servers, hosted or managed services and installation of software directly on the email server itself. While there are proponents and opponents of these approaches, there seems to be relatively strong opposition to the last approach on the part of many email administrators.

Osterman Research conducted a survey for Sunbelt Software to determine attitudes toward installing security software directly on servers that run Microsoft Exchange Server. Because many IT decision makers have an aversion to installing any third-party software directly on the hardware that runs Exchange Server, we wanted to determine how strong this aversion might be, as well as the potential for addressing the concerns that lead to many decision makers' reluctance to install any third-party on Exchange Server.

### **SURVEY BACKGROUND AND METHODOLOGY**

Osterman Research completed 102 Web-based surveys during June 2008 with individuals who are involved in managing Microsoft Exchange for their organizations. The organizations surveyed had a median of 1,250 employees and a median of 630 email users. Organizations across a range of industries were surveyed. Seventy-one percent of users in the organizations surveyed are on Exchange 2003, 25% are on Exchange 2007 and the balance are on earlier versions of Exchange.

What we found was interesting. While many administrators are opposed to the notion of installing software directly on Exchange Server, many are actually open to the idea of doing so if someone can demonstrate that it will not negatively impact the performance of Exchange.

This white paper discusses the detailed results of the survey, our conclusions about administrators' attitudes about installing third-party software on the Exchange Server, and it provides information on Sunbelt Software's VIPRE® Email Security for Exchange, a robust and comprehensive email security solution that can be installed directly on the Exchange Server with no adverse effects on system performance.

## Survey Findings

---

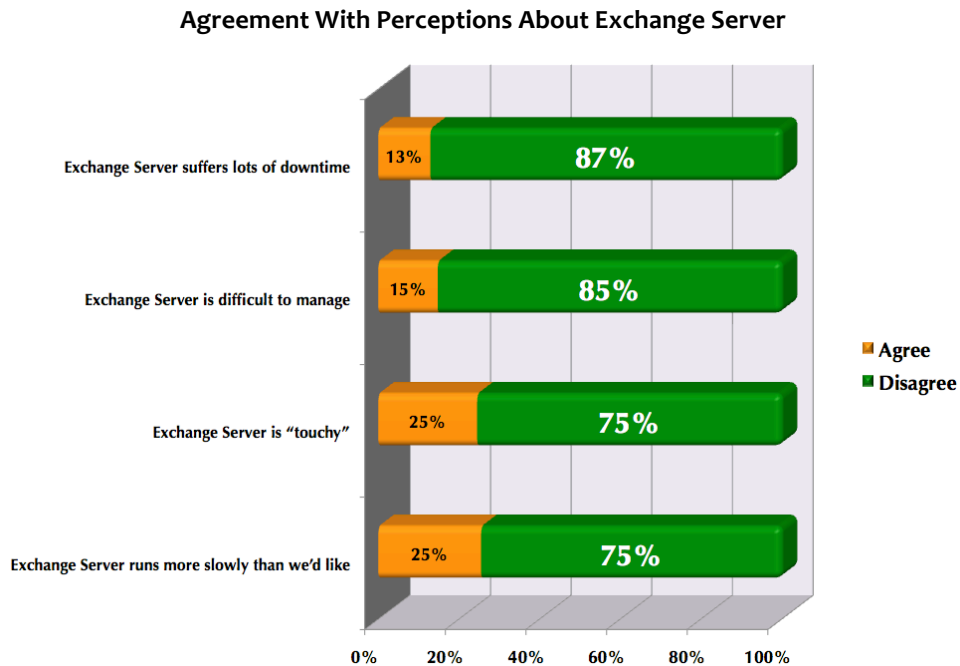
### **IS EXCHANGE "TOUCHY"?**

One of the issues that we wanted to explore in this survey was the extent to which Exchange might be considered "temperamental", and so might cause administrators to feel uneasy about installing any third-party software on the server along with Exchange. We asked a

series of questions to determine just how temperamental Exchange might be. Here is what we found:

- Only 25% of Exchange administrators largely or completely agree that Exchange Server is “touchy”.
- Only 25% of Exchange administrators largely or completely agree that Exchange Server runs more slowly than administrators consider to be acceptable.
- Only 15% largely or completely agree that Exchange Server is difficult to manage.
- Only 13% largely or completely agree that Exchange Server suffers “lots” of downtime.
- Fifty-nine percent of Exchange administrators largely or completely agree that Exchange is a great email system, while 72% have no plans to migrate away from Exchange during the next five years.

In short, then, our findings demonstrated that the vast majority of Exchange administrators consider Exchange to be a fairly solid messaging platform that suffers acceptable levels of downtime and is simply not difficult to manage, as shown in the following figure.



### STILL THE RELUCTANCE

However, two-thirds of Exchange administrators “don’t like” running third-party software on the same platform as Exchange Server. Further, 60% would rather install appliances or additional servers for security than install software on Exchange Server. This is likely due to perceptions that third-party software running on the same platform as Exchange Server can

somehow bring down the server more often than if the third-party software runs on separate hardware. About one-half of survey respondents reported that they have experienced or heard of situations in which a colleague, peer or someone else installed messaging security software on their Exchange Server and experienced adverse results.

## CONVINCING DECISION MAKERS

Our research revealed something of a mismatch between perceptions about Exchange Server and attitudes about installing software on the same hardware as Exchange Server: administrators largely believe that Exchange Server is a solid, reliable platform, but they don't want to install any third-party software on the same hardware anyway.

However, our research also found that administrators are open to change based on four questions we asked in the survey:

- If it could be demonstrated to you that installing messaging security software on your Exchange Server would have no adverse impact on system downtime, would you be willing to install this software on your Exchange Server? **65% of decision makers responded Yes.**
- If it could be demonstrated to you that installing messaging security software on your Exchange Server would have no adverse impact on message delivery time, would you be willing to install this software on your Exchange Server? **67% of decision makers responded Yes.**
- If it could be demonstrated to you that installing messaging security software on your Exchange Server would make server and security management easier and less time-consuming, would you be willing to install this software on your Exchange Server? **76% of decision makers responded Yes.**
- If it could be demonstrated to you that installing messaging security software on your Exchange Server would make server and security management less expensive than managing separate servers or appliances, would you be willing to install this software on your Exchange Server? **78% of decision makers responded Yes.**

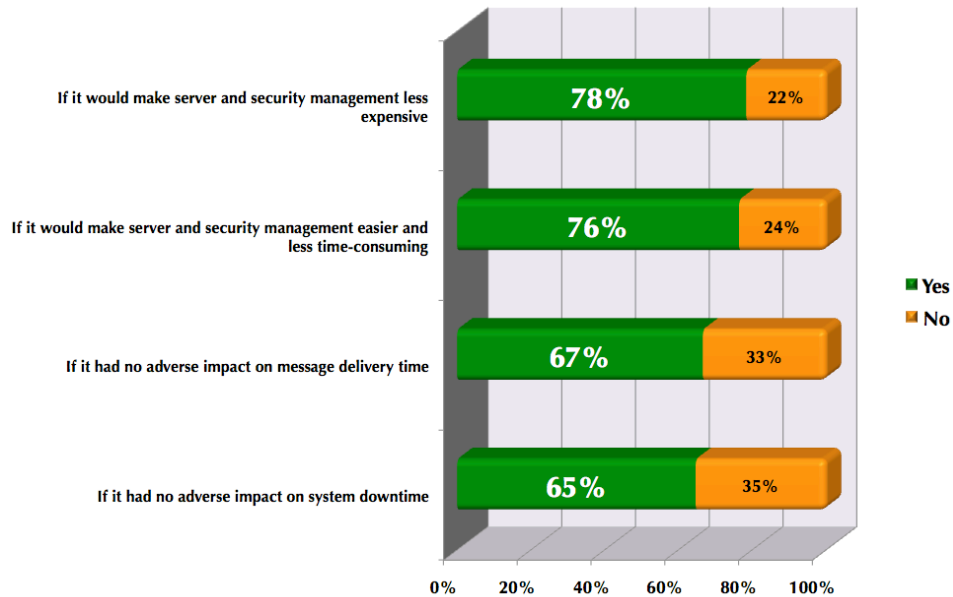
### **Roberts Wesleyan College**

*This College, located in Rochester, New York, offers both graduate and undergraduate programs for its 2,500 email users. Both faculty and staff complained of too much spam reaching them, while the IT department was spending far too much time filtering and blocking unwanted emails for them. IT staff was spending time reviewing headers, blocking unwanted IP addresses and performing other tasks that consumed significant staff resources.*

*The College installed VIPRE for Exchange in under 30 minutes on its Exchange Server and experienced a dramatic decrease in the amount of time spent filtering and blocking spam and now had one product to handle both anti-virus and anti-spam capabilities. Further, by putting quarantine control in the hands of end users, IT staff was able to save additional resources in managing messaging security.*

The bottom line is that while Exchange administrators are largely reluctant to install any third-party software on the same platform as Exchange Server, the vast majority of them are open to considering the potential for doing so if their concerns can be adequately addressed as shown in the following figure.

**If It Could Be Demonstrated That Installing Security Software Directly on the Exchange Server Would Have No Adverse Impacts, Would You Be Willing To Do So?**



## Why Install Security Software Directly on the Exchange Server?

There are two primary benefits associated with installed messaging security software on the same hardware as Exchange Server:

- **Lower labor costs**  
Labor costs are typically lower when installing because additional servers or appliances do not have to be sourced, deployed, configured and maintained. This is particularly advantageous for smaller organizations that typically pay more per seat for their messaging systems than larger organizations and often do not have dedicated IT staff that have the time to evaluate, configure or deploy additional hardware. Installing robust messaging security software directly on the server can allow a smaller organization to achieve a high level of protection with minimal IT resources.
- **Lower hardware costs**  
By installing software directly on the server, organizations can avoid the additional hardware and support costs that result from deploying additional appliances or servers in

the messaging infrastructure. This can result in substantial savings over the typical three-year lifespan of the system.

- **Better protection**

Installing security software on the Exchange Server in combination with appliances or servers at the gateway, or in combination with a hosted security solution, will create a layered security solution that will often result in improved capture rates for spam and viruses. This provides additional security, allowing a layered defense that maximizes protection for email users.

In short, organizations that choose to install the right messaging security software directly on an Exchange Server can reduce the cost and complexity of the messaging environment while providing robust defenses against a variety of threats.

## INDEPENDENT CORROBORATION

The efficacy of installing security software directly on Exchange Servers has been corroborated by an independent analysis from Hewlett Packard<sup>1</sup>. That analysis concluded:

*Based on the results of this extensive lab testing, HP recommends including antivirus protection in every Microsoft Exchange Server 2007 messaging solution to prevent potential damage from virus attacks. With antivirus protection, the CPU cycles did increase, but not enough to impact the user experience. The benefits far outweigh the risks.*

### PCN Consulting

*PCN is a solution provider with offices in Manhattan, Westchester and Connecticut. Their clients were complaining of receiving hundreds of spam messages per day along with the lost productivity resulting from this level of spam. While PCN considered both hardware- and software-based solutions, many of their clients preferred a software-only approach. PCN evaluated several server-based solutions and found VIPRE for Exchange on the recommendation of a new client. The quarantine feature of VIPRE for Exchange resonated well with their clients' needs, allowing users to see their captured messages rather than waiting to find out if an important message was flagged as spam.*

*PCN experienced a 95% to 98% reduction in spam reaching users' inboxes and experienced no system interference with their clients' existing networks. PCN technical staff found the VIPRE for Exchange installation to be simple – they were able to use just the default settings during the initial installation, speeding the entire installation process.*

---

<sup>1</sup> *Impact of implementing antivirus protection in a Microsoft Exchange Server 2007 environment*  
<http://h71028.www7.hp.com/ERC/downloads/4AA1-5525ENW.pdf>

## About VIPRE Email Security for Exchange

---

### OVERVIEW

VIPRE Email Security for Exchange is an integrated package of messaging security capabilities that can be installed directly on the Exchange Server. Its advanced framework integrates smoothly and perfectly with Exchange and will not drain resources. The code is highly optimized for low CPU and disk access resources. Having just one product that 'does it all' on your exchange server improves reliability.

VIPRE for Exchange gives you several security layers for message inspection, cleansing and management. By using multiple scanning engines for both spam and viruses, while integrating other messaging security rules, all treatment of messages occurs at the server, not at your end-user's workstation – no client software needed, and all modules play nice together. VIPRE for Exchange is the powerful combination of 'best-of-breed' and 'all-in-one'.

### POLICY-BASED PLUG-IN MANAGEMENT

VIPRE's plug-in architecture was designed with flexibility and extendibility in mind. That way you get a robust product that enables you to manage your entire email security. You can create customizable policies utilizing the integrated plug-in management. VIPRE for Exchange includes plug-ins for antispam, antivirus, attachment filtering, and disclaimers.

With extensive policy creation capabilities, you can create custom policies for groups of users or a single user using Active Directory. You can set parameters based on user and/or organizational requirements. If you wish, you can simply associate all users with filters attachments at the Exchange server, before they reach your users and as they are sent between users.

The default plug-in policies enable you to have a powerful email security protection solution in place in just a few minutes. You can also create separate policy templates for different groups or individuals. And, you don't have to set up and maintain lists of blocked IP addresses and constantly create all sorts of custom rules. You have the flexibility to fine-tune the aggressiveness of detection for all messaging plug-ins.

### FAST DEPLOY IN EXCHANGE 2000-2007 ENVIRONMENTS

VIPRE's management console enables you to install, configure and manage your full messaging security from one central location. Designed as an MMC snap-in, deployment is simple with a minimum of configuration effort needed. VIPRE for Exchange seamlessly integrates with Microsoft Exchange and provides world-class spam, virus, file attachment protection, and disclaimers. Additionally, VIPRE for Exchange makes it easy to create policies across multiple messaging plug-ins.

### MULTIPLE SCANNING ENGINES FOR BETTER DETECTION AND PROTECTION

VIPRE for Exchange is designed to meet both the spam and virus protection needs of your organization. With multiple spam and virus scanning engines, you automatically receive higher detection rates and a more accurate response to the messaging threats that attempt

to enter your network. As an integrated email content inspection, antispam and antivirus solution, VIPRE for Exchange not only scans and eliminates viruses and other dangerous message content, but also filters attachments at the Exchange server, before they reach your users and as they are sent between users.

### **EMAIL CONTENT INSPECTION AND ATTACHMENT FILTERING**

Using powerful policy-based attachment filtering capabilities, you can configure inspection and filtering on a per-policy basis. VIPRE's intelligent Suspicious Mail Attachment Removal Technology (S.M.A.R.T) filter scans the header of a file to verify that an attachment is what it says it is and has not just been renamed. No more renaming .exe files to get around the filters. You can set rules based on users and file types that enable you to quarantine potentially harmful content or attachments by file extension including .doc, .exe, .dll, .pdf, visual basic scripts and more. For example, you could allow certain users to send .exe files internally while blocking them from being sent externally.

### **GLOBAL AND POLICY-BASED DISCLAIMERS**

VIPRE for Exchange allows you to configure global disclaimers for all outbound email. With global disclaimers, disclaimers can be added to every email. Or if you prefer, configure policy-based disclaimers that are only added to emails from specific users, groups, domains or public folders. VIPRE for Exchange also prevents multiple disclaimers when replying or forwarding and gives you the ability to allow users to bypass the disclaimer on a per email basis. Additionally, disclaimer templates are included that allow you to easily set up disclaimers using HTML or plain text. Template samples include legal disclaimers, virus warning disclaimers, copyright disclaimers, and more.

## **Summary**

---

Should you install messaging security software on an Exchange Server, or is it better to use separate servers, appliances or services to provide these capabilities? Osterman Research believes that while these external solutions provide excellent performance, installing the right messaging security software directly on the Exchange Server also provides excellent performance without compromising Exchange Server stability, reliability, performance or maintainability.

VIPRE Email Security for Exchange from Sunbelt Software provides an integrated and robust set of messaging security capabilities that is easy to install on the Exchange Server, is easy to maintain, and will not compromise any of the capabilities offered by Exchange.

***Should You Install Messaging Security Software on Your Exchange Server?***

© 2009 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

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, statute, 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.