

Richi Jennings Associates

Email: reports@richij.com • Web: richij.com/contact • Tel: +44.7789.200701

TCO of Lotus Domino Threat Protection

Total Cost of Ownership of server-based security software, protecting against malware and other email-borne threats in a Notes/Domino environment

July 2009



*This document was independently researched and prepared
by Richi Jennings Associates for Trend Micro, Inc.*

Executive Summary

Email continues to be a key vector for threats, such as viruses, Trojan horses, and links to malicious Web sites. Users are being exposed to increasingly sophisticated, often socially engineered attacks. It's essential for Notes/Domino administrators to protect their users.

Unfortunately, threat protection does not come cost-free: the total cost of ownership can be surprisingly high. However, after independent research and analysis, we have identified *substantial* savings in typical organizations.

In this short report, we show how a typical 10,000-user organization could save at least \$50,000 per year, while also boosting end-users' productivity.





Richi Jennings Associates independently conducted all analysis for this document and retained full editorial control. Trend Micro commissioned this white paper with full distribution rights.

Richi Jennings Associates acknowledges all trademarks.



This document is licensed using a Creative Commons Public License, specifically: *Attribution-Non-Commercial-Share Alike 2.0 UK: England & Wales*. For full details, see <http://creativecommons.org/licenses/by-nc-nd/2.0/uk/legalcode>

A summary deed with no legal value appears below:

-  You are free to copy, distribute, display, and perform the work under the following conditions:
-  *Attribution*. You must give the original author credit.
-  *Non-Commercial*. You may not use this work for commercial purposes.
-  *No Derivative Works*. You may not alter, transform, or build upon this work.

For any reuse or distribution, you must make clear to others the license terms of this work.

Any of these conditions can be waived if you get permission from the copyright holder.

Nothing in this license impairs or restricts the author's moral rights.

Your fair dealing and other rights are in no way affected by the above.

Contents

Executive Summary	2
1. Introduction	4
Background	4
Purpose of this Report	4
2. TCO Results; How to Save Money	5
How to Optimize your TCO.....	5
3. Conclusion.....	8
Reduce your TCO through Operational Improvements.....	8
Reduce your TCO through Product Choice	8

1. Introduction

Background

Email continues to be a key vector for malware, such as viruses and Trojan horses. Not only should we be concerned about infected attachments, but criminals also send email that links to malicious Web sites.

It's essential for Notes/Domino administrators to protect their users against malware and other email-borne threats. An important part of that protection is server-based protection software. Such software is designed to block threats that arrive or that have previously been stored in users' mailboxes.

Such software typically runs on the Domino servers, scanning incoming messages from other users and from the Internet, as well as periodically scanning users' mailbox contents. The scans are designed to identify threats and remove them. The aim is to prevent users from inadvertently infecting their own computers and other parts of the organization's IT infrastructure.

However, such threat protection does not come without cost. Read on to understand the "elephant in the room," and to see how a typical 10,000 user organization could save at least \$50,000 per year, while also boosting end-users' productivity.

Purpose of this Report

We have designed this report to help you understand the total cost of ownership (TCO) of server-based threat protection in a Notes/Domino environment. The report is based on informed analysis work with large organizations, IBM, and our extensive experience of enterprise messaging/collaboration.

It will help you understand:

- The typical TCO of a Domino threat protection system
- How each cost component affects the TCO
- How to optimize your own TCO

We have built a simple yet powerful mathematical model that captures the major individual costs and calculates the TCO. There's an accompanying TCO Tool, which consists of a spreadsheet to implement the model, and an appendix which describes it. You'll be able to customize this spreadsheet to describe your own environment, if you wish.

After reading this report, you will be able to find money-saving opportunities and justify any investments required to seize those opportunities.

The next section outlines typical costs based on our TCO model and describes how to realize substantial cost savings...

2. TCO Results; How to Save Money

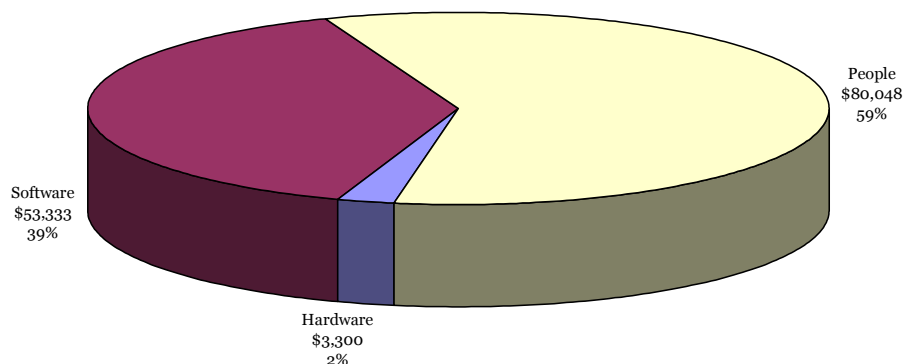
We simulated a typical large organization of 10,000 users, and calculated the total cost of ownership of Notes/Domino threat protection as **US\$140,000** per year, or \$14 per user per year.

The simulation is based on a typical—or “median”—organization of this size. In our experience, such organizations’ threat protection environments are not well optimized. There’s usually scope for improvement, to make substantial cost savings.

We made all our cost assumptions conservatively, so your actual TCO may be higher and your potential cost savings may also be larger. Due to economies of scale, smaller organizations will experience higher per-user TCO figures; and larger organizations will see lower figures.

It’s usual in TCO calculations such as this to find that “people costs” make up a large proportion of the total. Using our conservative assumptions, more than half of the costs are due to IT staff, helpdesk staff, and end-user productivity losses.

The chart below shows the typical annual TCO split into three major cost components: hardware, software, and people.



*Typical annual TCO, showing three major cost components
(source: Richi Jennings)*

How to Optimize your TCO

Our analysis shows that **reducing the administrative overhead** offers the most opportunity for cost reduction. Another opportunity is to make the threat protection **more accurate**.

The TCO model shows that it’s possible to make **substantial savings**. Even with conservative assumptions, we predict an optimized TCO of \$9 per user per year, saving 35%. This can translate to a \$50,000 saving per year for our typical 10,000 user organization.

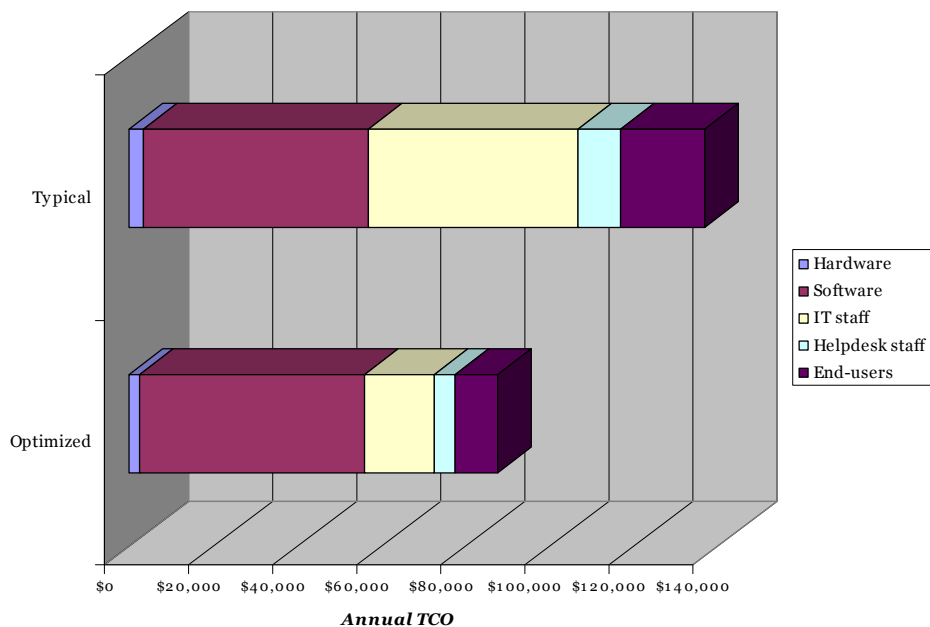
In our research with large organizations that use Notes/Domino, we identified five ways in which they typically wasted money related to threat protection. They

typically experience one or more of the following issues, each of which have a TCO impact:

1. **Signature updates frequently fail**, requiring manual intervention and causing delay: resulting in malware infections by emergent threats.
2. **Signature updates available “too late”** from the vendor: also resulting in infections from emergent threats.
3. **Patches and version updates are time-consuming**, requiring configuration settings to be reinstated by hand: resulting in wasted time for IT administrators.
4. **Vendor support organization lacks expertise** in Domino environments (despite competence with Exchange): resulting in wasted time for IT administrators, helpdesk staff, and end-users.
5. **Impractical to consolidate** the Domino servers,¹ because 32-bit threat protection software does not take advantage of 64-bit performance improvements, constraining the ability to consolidate onto fewer, larger servers: resulting in unnecessary work for IT administrators and higher hardware costs.

If we were to solve these five problems, it would allow us to optimize the TCO and save substantial amounts of money.

The chart below compares our baseline, typical TCO scenario with one that is optimized to resolve the five issues and save at least \$50,000. In this chart, we’ve further divided the “people” cost component into its three component parts.



TCO comparison, showing conservative estimate of possible savings (source: Richi Jennings)

¹ this issue mainly experienced on the Windows Server platform

There are full details in the TCO Tool appendix describing how solving these issues saves money, but in summary, it's mainly due to these factors:

- **Lower administrative overhead required:** a 25% saving from a combination of reduced manual intervention by IT staff, better vendor support, and a more efficient, consolidated server environment (problems 1, 3, 4, 5).
- **Fewer infections from emergent threats:** a 10% saving in helpdesk overhead and improved end-user productivity, because signature updates are available and deployed in a timely manner, which improves accuracy (problems 1, 2, 4).

Indirect Savings from Consolidation

These TCO calculations deliberately ignore the additional savings made indirectly by consolidating the network into fewer, larger servers. If 32-bit threat protection software is preventing consolidation, you might argue that solving this issue saves all of the money saved by consolidation—not just the cost savings directly allocated to threat protection alone.

The indirect cost saving would be in reducing the number of administrative staff and the cost of the hardware. These savings might be of the order of an *additional* \$50,000, so you might argue that the total cost savings are \$100,000.

Visibly Benefitting your Organization

To look at it another way: by optimizing your TCO, you'll be able to focus more IT staff and helpdesk attention on projects that have a **visible benefit** to the organization. That's in contrast to threat protection, which is normally only visible when things go wrong.

In addition, you'll be boosting end-users' productivity and will be able to use the TCO model to measure the value to the organization of the optimizations you've made.

The next section outlines the optimizations you should consider making...

3. Conclusion

It's obvious that there are substantial cost savings to be made by reducing wasted staff time. Of course, it's important to understand the size of this cost saving, and to assess how worthwhile the changes required are. There are two ways of approaching these cost savings.

Reduce your TCO through Operational Improvements

Organizations should carefully examine their operational practices for cost-saving opportunities. Are there, for example, ways of automating repetitive tasks? Similarly, ask yourself if there's scope to decrease the number of malware incidents by investing in better end-user training.

However, your threat protection software may be thwarting your efforts. You may be limited by the inflexibility of the product you currently use, or by recurring problems with it, or simply by its inadequate accuracy.

Reduce your TCO through Product Choice

There's anecdotal evidence that some threat protection products require far more administrative overhead than others; and that real-world accuracy varies significantly. Preliminary user interviews indicate that certain vendors' products for Notes/Domino seriously limit administrative efficiency; and that, as we outlined earlier, users are too often put at risk by delayed signature updates. Emergent threats are far more likely to cause infection if the vendor delivers threat signatures late, or if deployment of signatures is delayed due to a failure of the automatic update process.

This requires further, quantitative research and analysis: a project we are hoping to work on in the near future. However, it does appear that some major vendors are failing the Notes/Domino user community.

To summarize the issues described earlier:

1. Signature updates frequently fail
2. Signature updates arrive "late"
3. Patches are time-consuming
4. Vendor's lacks Domino support expertise
5. Software not 64-bit-ready

If your experience matches one, some, or all of these issues, the potential TCO benefits of a switch to a competitive product could *easily* justify the return on investment of such a switch.

Next, discover how to calculate your own TCO using the companion TCO Tool.