

Richi Jennings Associates

Email: richi@richi.co.uk • AIM and Skype: richij • Tel: +44.7789.200701

Blocking Malware in the Cloud: Does It Work?

*An independent analysis of Trend Micro's cloud-based Web Reputation
technology—part of the Trend Micro Smart Protection Network*

January 9, 2009



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

Executive Summary

As malware becomes ever more sophisticated and resistant to our defenses, the anti-malware industry is faced with the challenges of “signature bloat”—or *threat of volume*, as Trend Micro™ describes it.

After independent analysis, we’re convinced by Trend Micro’s main claims for its Web Reputation technology—part of its cloud-based *Smart Protection Network*. It offers better protection and better performance.

In this short report, we outline the increasing challenges raised by the classic way of detecting malware, describe Trend Micro’s approach, examine the probable benefits, and discover whether real customers are experiencing these benefits.





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
How Web Reputation Works	4
2. Theoretical Benefits	5
Fewer Malware Infections.....	5
Reduced Overhead	5
Improved Performance	5
Reduced Network Usage	5
3. Actual Results	6
Conclusion: Web Reputation Delivers on its Promise	6

1. Introduction

Background

Trend Micro was an early innovator in what we now think of as “traditional” anti-malware technologies. These traditional methods for detecting malware are heavily based around pattern files, which contain unique characteristics or “signatures” of known malware samples. These signatures are researched, extracted, and published by *TrendLabs*SM—Trend Micro’s anti-malware research team.

As malware becomes ever more sophisticated and resistant to our defenses, the whole anti-malware industry is faced with several difficult problems; two of which are:

Too Many Unique Malware Samples

Anti-malware engines need to search through tens of millions of signatures in order to verify that a suspect file is uninfected. However, many of the signatures may never be used—they remain in the pattern files because the risk of removing them is too great.

This of course means that typical pattern files have grown large and unwieldy. This has a very real performance impact, both on the act of scanning and when periodically updating the signatures.

Malware Aggressively Spreading

Users need a way to get a definitive judgment when presented with an unknown file—*is this malware or not?*

The time between malware being released into the wild to the first infections is far shorter today than it has ever been. This means that signatures are typically too slow to update. The inevitable delay between publication and deployment offers a window of time for undetected malware to infect PCs.

How Web Reputation Works

Web downloads are now the primary vector for malware infection. For example, a Trojan downloaded by clicking on links in “e-card spam” or downloading malware from a hacked Web site that’s otherwise legitimate.

Trend Micro’s Web Reputation technology sets out to prevent users from accidentally downloading malware by blocking access to malicious sites. It does this by checking the reputation of the target Web page in real time—the in-the-cloud reputation database effectively blocks the connection to the site.

The next section outlines the potential benefits in more detail...

2. Theoretical Benefits

Naturally, Web Reputation means that fewer files need to be scanned and that users are less vulnerable to delays in deploying signatures.

Below are the top four *theoretical* reasons why cloud-based malware download blocking might be better than a traditional, signature-based approach.

Fewer Malware Infections

Job#1 is to protect against malware infection. Web Reputation eliminates the typical delay before signatures for known malware are deployed. Because of the cloud-based approach, download sources are always validated against the latest published reputation.

This should greatly improve accuracy against newly-emergent malware.

Reduced Overhead

Because there's less scanning required, memory footprints and disk I/O usage should be significantly improved. These resources can now be used for *real* work, rather than for protection.

Improved Performance

Overall performance should improve as a result of using Web Reputation. A major end-user complaint is that real-time malware scanning slows down their PCs, reducing productivity and adding to stress levels. The mere fact that this processing is reduced will improve perceived performance, leading to happier users.

Assuming that Trend Micro's data centers are appropriately sized, there should be little or no *significant* perceived delay in checking the reputation of legitimate downloads.

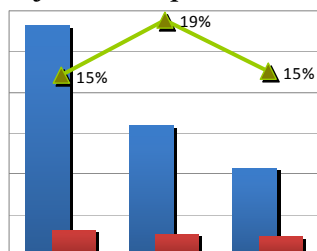
Reduced Network Usage

The traditional approach requires that the user download the malware before it is scanned. This can waste a surprising amount of network bandwidth. This shared resource can now be used for *real* work, rather than transferring malware.

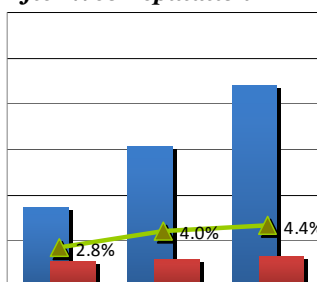
These are the most significant and believable benefits, in our opinion. In the next section, we'll discuss how these theories match reality...

3. Actual Results

Before Web Reputation

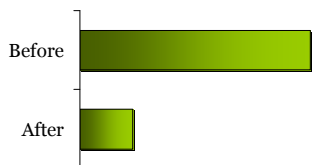


After Web Reputation



■ # of Customers
 ■ # of Calls
 ▲ % Malware

Proportion of Malware-Related calls
 (Before/After Web Reputation)



Trend Micro offered its own data, based on product support call volumes before and after users migrated to Web Reputation versions of Trend Micro products.

Customers choosing to migrate have an improved experience, as measured by this support data. The data were collected over a three month period and measure the numbers of support incidents. The data were also segmented by whether or not each support call was related to a malware infection.

The first two figures on the left show the relative number of customers, the number of calls, and the proportion of calls that were related to a malware infection. The third figure compares the two groups of customers by the number of malware-related calls. (We chose to omit scales, for confidentiality reasons.)

The average Web Reputation customer makes far fewer support calls related to malware infections. The data show a **75% improvement** in the number of calls, versus customers using the older, signature-based products. When the data are normalized, just 4% of support calls were related to malware infections with Web Reputation, versus 16% of calls with the older products.

However, the total number of other support calls increased by 50%. When the data are normalized, 21% of Web Reputation customers called support with non-malware incidents, versus 14% of those using the older products. This increase is roughly what would be expected for customers in mid-migration.

We have not audited the support data, but we have no reason to suspect that they are unrepresentative. However, we did want to test the data and investigate the other benefits, by conducting our own research...

Independently of Trend Micro, we surveyed and/or interviewed several customers who have migrated to Web Reputation. The customers represented organizations of all sizes—from fewer than 50 users to more than 15,000. The respondents were situated in North America and Europe.

Generally, these IT managers are happy they made the switch. All respondents reported **fewer malware infections**—some reported “far” fewer infections. The performance experienced is good. Migration was relatively simple; without unreasonable support issues.

Although the sample size wasn’t large, it’s clear that the switch to Web Reputation has been a positive one for these customers. These *qualitative* reports clearly support the list of benefits presented in the previous section.

Conclusion: Web Reputation Delivers on its Promise

In brief, we’re convinced by Trend Micro’s main claims for its Web Reputation technique. After independent analysis, we are persuaded that it offers better protection and better performance—making the migration effort worthwhile.