



## **Comparative Efficacy Assessment of Emmunize**

### **March 2011**

#### **Contents:**

<b>Introduction</b>	<b>2</b>
<b>Versions of the Applications Tested</b>	<b>2</b>
<b>Penetration Test Tools and Malware Samples used</b>	<b>2</b>
<b>Methodology used</b>	<b>2</b>
<b>Test results</b>	<b>3</b>
<b>Analysis of results and their implications</b>	<b>4</b>
<b>Conclusion</b>	<b>5</b>

## Introduction:

This report has been commissioned with the objective of providing an independent efficacy assessment of a cohort of Antimalware / Antivirus applications, including Emmunize.

This comparative assessment will measure each products efficacy against a range of real and theoretical threats.

## Versions of the Applications Tested:

- Emmunize (1.0.0.19)
- Coranti Anti-Virus & Anti-Spyware (1.3.1)
- G Data Antivirus 2011 (21.1.2.2)
- Avira AntiVir Premium (10.0.0.667)
- Immunet Protect Plus (3.0.18)
- BitDefender Antivirus AntiVirus Pro 2011 (14.0.28.351)
- F-Secure Antivirus 2011 (10.51 Build 106)
- McAfee Antivirus Plus 2011
- Sunbelt VIPRE Antivirus Premium 2011 (4.0.3904)
- Avast Antivirus Professional (6.0.1000)
- Panda Antivirus Pro 2011 (10.00.00)
- Eset Nod32 Antivirus (4.2.71.2)
- Kaspersky Antivirus 2011 (11.0.2.556)
- Norton Antivirus 2011 (18.5.0.125)
- AVG Antivirus 2011 (0.0.1204 Build 3403)
- Prevx 3 (3.0.5.220)
- Microsoft Security Essentials (2.0.657.0)

## Penetration Test Tools and Malware Samples used:

In order to assess efficacy against real threats currently prevalent in the wild, 50,000 malware samples were used, all aged between 1 – 14 days.

In order to assess efficacy against potential targeted attacks and true zero day threats, the following malware samples and simulators were used:

- Custom, zero day Zeus build X 5
- Custom Zero day SpyeEye build X 5
- MRG Financial Malware Simulator Versions 2.0, 2.0.s, 2.0.s.1\*

\* = The MRG Financial Malware Simulator is a tool developed by MRG Effitas to properly simulate a new or zero day piece of financial malware. The simulator is used to accurately model how real financial malware behaves on a system in the real world.

## Methodology used:

Testing was conducted using VMWare

1. Windows 7 Ultimate 32 system is crated, with internet access and all updates are applied.
2. A folder containing the malware samples is copied to the desktop.
3. The system is cloned seventeen times, thus making a copy for each of the products being tested.
4. Each of the applications is installed on to one of their respective clones.
5. Where applicable, all product and signature updates are applied.
6. A snapshot of each VM is created.
7. Testing is conducted as follows:

- a. A static scan is conducted of the malware samples via a context menu option and the full scan / remediate cycle is completed.
- b. A snapshot of the system is created.
- c. If any samples remain, each is executed to determine if the security application can detect them dynamically.
- d. If any sample is able to execute, undetected by the security application, the snapshot in 7b is restored and testing continues using the next sample after the one which executed.

**Test results:**

The table below shows the percentage of the 50,000 malware samples detected by each security application:

Security Product	Infections Prevented %
Emmunize	100
Coranti Anti-Virus & Anti-Spyware	99.384
G Data Antivirus 2011	99.096
Avira AntiVir Premium	98.904
Immunet Protect Plus	98.788
BitDefender Antivirus AntiVirus Pro 2011	98.696
F-Secure Antivirus 2011	98.684
McAfee Antivirus Plus 2011	98.658
Sunbelt VIPRE Antivirus Premium 2011	98.464
Avast Antivirus Professional	98.25
Panda Antivirus Pro 2011	97.296
Eset Nod32 Antivirus	96.536
Kaspersky Antivirus 2011	96.438
Norton Antivirus 2011	96.172
AVG Antivirus 2011	93.518
Prevx	92.56
Microsoft Security Essentials	91.75

To put these results in context, the table below shows the actual number of malware samples missed, which would equate to the number of systems infected, if each sample was executed on an individual system:

Security Product	Number of Malware Infections
Emmunize	0
Coranti Anti-Virus & Anti-Spyware	308
G Data Antivirus 2011	452
Avira AntiVir Premium	548
Immunet Protect Plus	606
BitDefender Antivirus AntiVirus Pro 2011	652
F-Secure Antivirus 2011	658
McAfee Antivirus Plus 2011	671
Sunbelt VIPRE Antivirus Premium 2011	768
Avast Antivirus Professional	875
Panda Antivirus Pro 2011	1352
Eset Nod32 Antivirus	1732
Kaspersky Antivirus 2011	1781
Norton Antivirus 2011	1914
AVG Antivirus 2011	3241
Prevx	3720
Microsoft Security Essentials	4125

The table below shows the percentage of the zero day and custom malware samples detected by each security application:

Security Product	Zero Day and Custom Malware Infections Prevented %
Emmunize	100
Prevx	23.076
Sunbelt VIPRE Antivirus Premium 2011	7.692
Coranti Anti-Virus & Anti-Spyware	0
G Data Antivirus 2011	0
Avira AntiVir Premium	0
Immunet Protect Plus	0
BitDefender Antivirus AntiVirus Pro 2011	0
F-Secure Antivirus 2011	0
McAfee Antivirus Plus 2011	0
Avast Antivirus Professional	0
Panda Antivirus Pro 2011	0
Eset Nod32 Antivirus	0
Kaspersky Antivirus 2011	0
Norton Antivirus 2011	0
AVG Antivirus 2011	0
Microsoft Security Essentials	0

#### Analysis of results and their implications:

All MRG Effitas tests are designed to closely match real world scenarios and so provide an efficacy assessment which should map to an application when used for real in the enterprise or by a home user.

The tests and operating system in this report were selected to represent the systems currently in use and the threats faced under different circumstances and use environments.

We selected the mix of tests to assess efficacy against two threat categories:

- In the wild malware – such as Trojans, Backdoors, Worms, Rootkits, Macro Viruses, Exploits KeyLoggers & Rogues
- Targeted attacks – focused attacks against a business or user

The volume of malware in the wild has exploded in the last eighteen months. Currently MRG Effitas processes approximately 200,000 unique samples every day – which equates to 72,000,000 / year. Users are facing an unprecedented numbers of threats whilst conducting their online activities and with amount of malware being so high, even security products which offer very high detection rates are inevitably going to fail the user.

Out of the 50,000 early life samples, only Emmunize was able to properly protect the system and block every single sample. Whilst in the normal sense, products such as Coranti and G Data performed well with scores above 99%, it should be put in context by noting that these equate to 308 and 452 malware infections respectively, compared to the outstanding zero infections allowed by Emmunize.

Looking at the zero day and custom malware test results gives us a more dramatic example of the effectiveness of Emmunize and its ability to protect against these threats. As with the in the wild test, Emmunize protected the system against 100% of the samples used, with the next best result being from Prevx, with 23%, then VIPRE with 7.7%. The remaining fifteen security products failed to detect a single sample in this category.

## **Conclusion:**

MRG Effitas has never conducted an efficacy assessment using a large number of samples where a product has detected 100% - until now.

We all regularly see various product assessments and are accustomed to seeing the top performers return results in the low to high 99% range and so have come to regard such results as being “good” – and indeed, given the constraints of the technology used, such a result is a remarkable achievement. This said however, we need to consider the results in the context of the current threat landscape, which is characterised by unparalleled types and volumes of threats.

The second table, showing the actual numbers of malware samples the security applications allowed to infect the system brings meaning to the results and highlights the world of difference between a 99.3% and 100% score. Whilst allowing 308 infections may seem good in comparison to the 4125 allowed by the worst performer, it should be remembered that with modern malware, which invariably tries to steal your identity or money, just one single infection, allowed just once is all that is required for the cybercriminals to have achieved their objective.

In using white listing technology, Emmunize is able to offer 100% protection from all malware, including zero day and early life threats and outperform any product which relies on signatures, heuristics or HIPS.