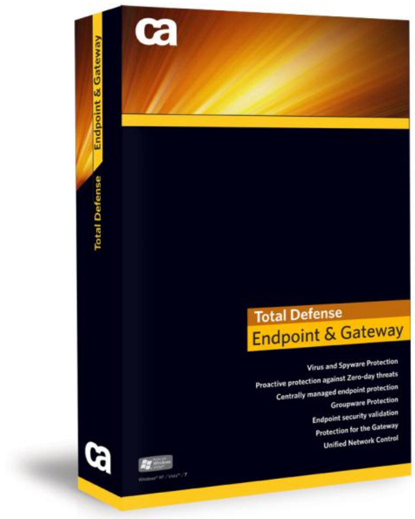

ca
Total Defense
Endpoint & Gateway
Virus and Spyware Protection
Proactive protection against Zero-day threats
Centrally managed endpoint protection
Groupware Protection
Endpoint security validation
Protection for the Gateway
Unified Network Control

Total Defense for Endpoint and Gateway r12 Independent Product Review

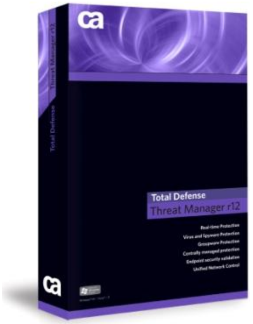
Gold Master Release

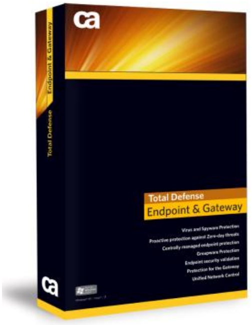
August 2010

Document:	CA Total Defense r12 – Gold Master Release –Product Review
Authors:	K. Lai, D. Wren
Company:	PassMark Software
Date:	23 August 2010
Edition:	Edition 2
File:	CA_R12_GoldMaster_review Ed2.docx

Table of Contents

Total Defense Feature Comparison





	Anti-virus r12	Threat Manager r12	Total Defense for Endpoint r12	Total Defense for Endpoint Premium Edition r12	Total Defense for Endpoint and Gateway r12
Anti-Malware	✓	✓	✓	✓	✓
HIPS - Endpoint Firewall			✓	✓	✓
HIPS – Intrusion Prevention			✓	✓	✓
HIPS – Operating System Security			✓	✓	✓
HIPS – Application Controls			✓	✓	✓
GROUPWARE – Microsoft Exchange		✓		✓	✓
GROUPWARE – Lotus Notes		✓		✓	✓
GROUPWARE – Microsoft Sharepoint		✓		✓	✓
GROUPWARE – NetApp		✓		✓	✓
Vulnerability Assessment	✓	✓	✓	✓	✓
Network Access Protection		✓		✓	✓
Gateway Security					✓

Introduction

In August 2010, PassMark Software conducted a standalone product review of the Gold Master release of Total Defense for Endpoint and Gateway r12.

This review presents our insight into the features available in r12, as well as our subjective opinions on our experiences configuring and operating CA Total Defense for Endpoint and Gateway r12.

We have also examined the system performance impact of Total Defense for Endpoint and Gateway r12 in comparison to three competing enterprise suites.

Installation

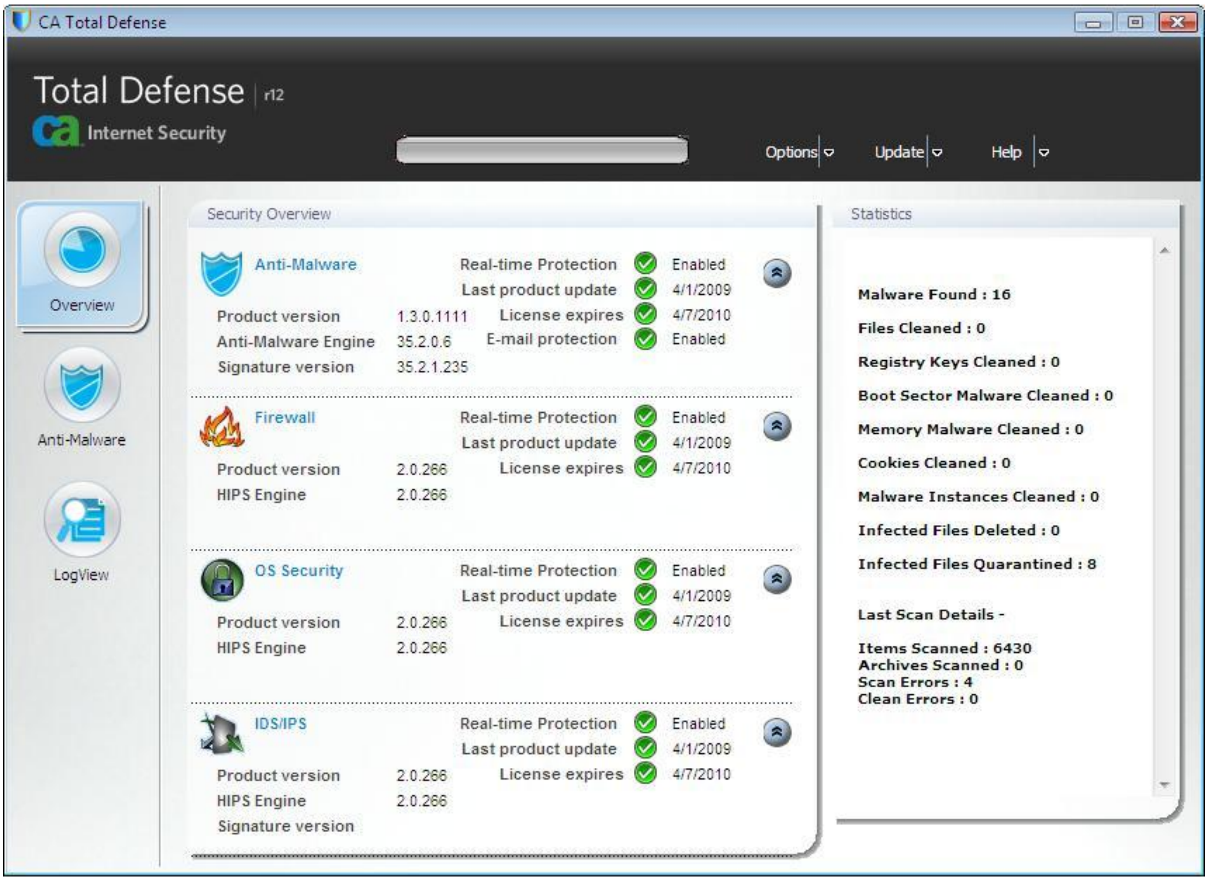
Total Defense r12 comes with a large amount of installation options for a single product. The installer has options for multiple languages; standalone or distributed installation types; Gateway Security software; Groupware installation; Unified Network Control installation and options to use an internal or external SQL database.

Pre-requisites include IIS6 or higher, .NET 3.5, the Adobe Flash Player and Microsoft NAP. Groupware supports the following servers, Exchange, Domino and Sharepoint.

The same product can scale from a small business installation to installations with thousands of end points. For large installations, above 1000 endpoints, CA is recommending a distributed install, with different management functions spread across multiple machines.

The number of options available means there are over 30 steps to the installation. Depending on the options selected and hardware in use, a first-time user can expect the basic, standalone installation of the Total Defense Management Server and Console to take roughly one to two hours.

Discovering Endpoints



Anti-Malware

Real-time Protection: Enabled
Last product update: 4/1/2009
License expires: 4/7/2010
E-mail protection: Enabled
Product version: 1.3.0.1111
Anti-Malware Engine: 35.2.0.6
Signature version: 35.2.1.235

Firewall

Real-time Protection: Enabled
Last product update: 4/1/2009
License expires: 4/7/2010
Product version: 2.0.266
HIPS Engine: 2.0.266

OS Security

Real-time Protection: Enabled
Last product update: 4/1/2009
License expires: 4/7/2010
Product version: 2.0.266
HIPS Engine: 2.0.266

IDS/IPS

Real-time Protection: Enabled
Last product update: 4/1/2009
License expires: 4/7/2010
Product version: 2.0.266
HIPS Engine: 2.0.266
Signature version

Malware Found : 16
Files Cleaned : 0
Registry Keys Cleaned : 0
Boot Sector Malware Cleaned : 0
Memory Malware Cleaned : 0
Cookies Cleaned : 0
Malware Instances Cleaned : 0
Infected Files Deleted : 0
Infected Files Quarantined : 8

Last Scan Details -

Items Scanned : 6430
Archives Scanned : 0
Scan Errors : 4
Clean Errors : 0

There are several ways to discover endpoints from the Total Defense Management Server and Console. The simplest method is through the Endpoint Discovery feature, which lets administrators choose from up to four levels of Discovery (DNS Scan, ICMP Sweep, TCP Sweep and Port Scanning) based on the size and complexity of the deployment.

Total Defense also detects the operating system running on endpoints using up to three methods, Windows Management Instrumentation (WMI), WinRM or Active Fingerprinting.

Administrators initially perform a “Full Discovery” of the network. Using the default DNS and ICMP options gives a quick scan, which is effective in most cases, but using the TCP sweep option can result in scans that take much longer to complete. PassMark Software conducted a “Full Discovery” on a network of nine endpoints using DNS Scan, ICMP Sweep and TCP Sweep as discovery methods. The discovery process was lengthy, taking roughly two hours to complete, and provided little real-time feedback about discovery status. Despite this, the Full Discovery correctly detected all endpoints and operating systems.

After a Full Discovery is performed, administrators can conduct an “Incremental Discovery” to find new endpoints on the network. In our testing, this took slightly less time than a “Full Discovery” but still took roughly one and a half hours to conduct a sweep using DNS Scan, ICMP Sweep and TCP Sweep on a network of nine endpoints which had already been discovered.

It should be noted that the CA documentation recommends that TCP Sweep should not be run unless required.

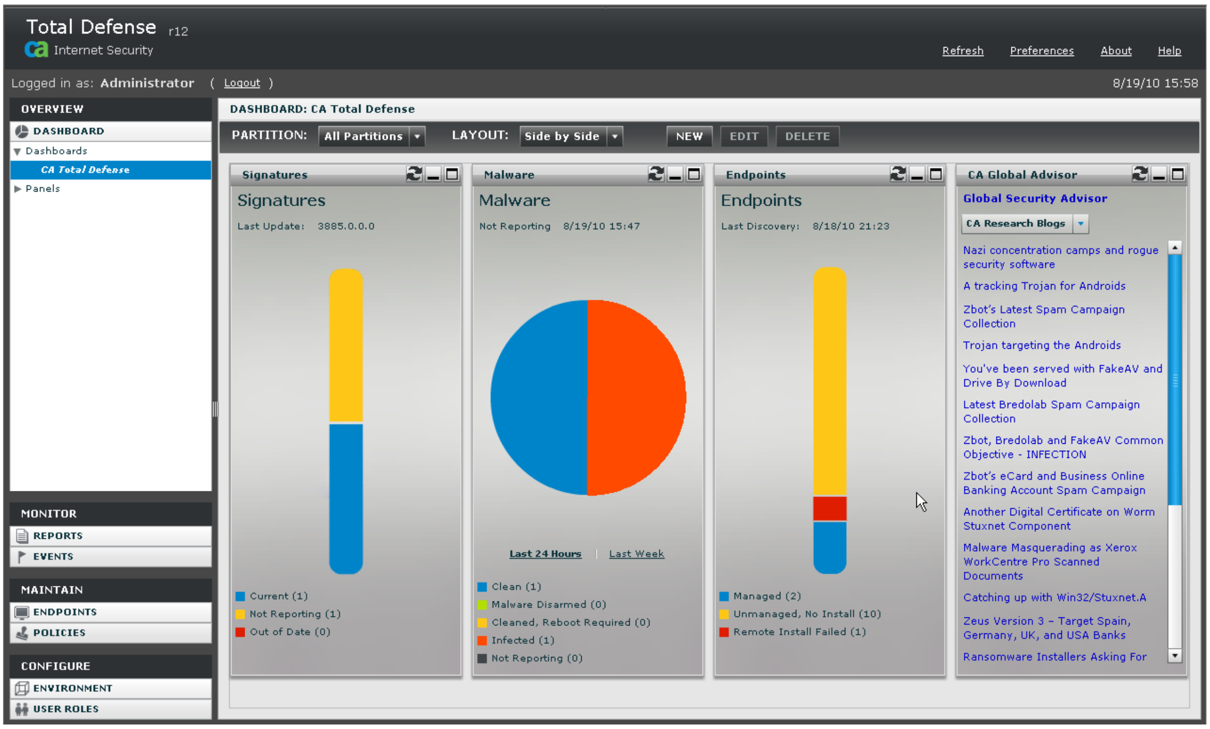
Deploying to Endpoints

From the Centralized Deployment page, administrators can create and assign deployment packages to unmanaged or managed endpoints. Administrators can specify the different components to be included in each deployment package.

There is also an option to remove security products from other vendors prior to the deployment of the Total Defense client. In our testing, we found that the competitive uninstaller successfully removed Symantec Endpoint Protection from the endpoint machine. CA is planning to document the products which are compatible with this competitive uninstaller, but no list is currently available.

Deploying the Total Defense endpoint module to a 'clean' endpoint via the network was fast and easy. In our testing, network deployment to an endpoint with a Windows Vista operating system took approximately four minutes.

Interface Design



Nazi concentration camps and rogue security software

A tracking Trojan for Androids

Zbot's Latest Spam Campaign Collection

Trojan targeting the Androids

You've been served with FakeAV and Drive By Download

Latest Bredolab Spam Campaign Collection

Zbot, Bredolab and FakeAV Common Objective - INFECTION

Zbot's eCard and Business Online Banking Account Spam Campaign

Another Digital Certificate on Worm Stuxnet Component

Malware Masquerading as Xerox WorkCentre Pro Scanned Documents

Catching up with Win32/Stuxnet.A

Zeus Version 3 – Target Spain, Germany, UK, and USA Banks

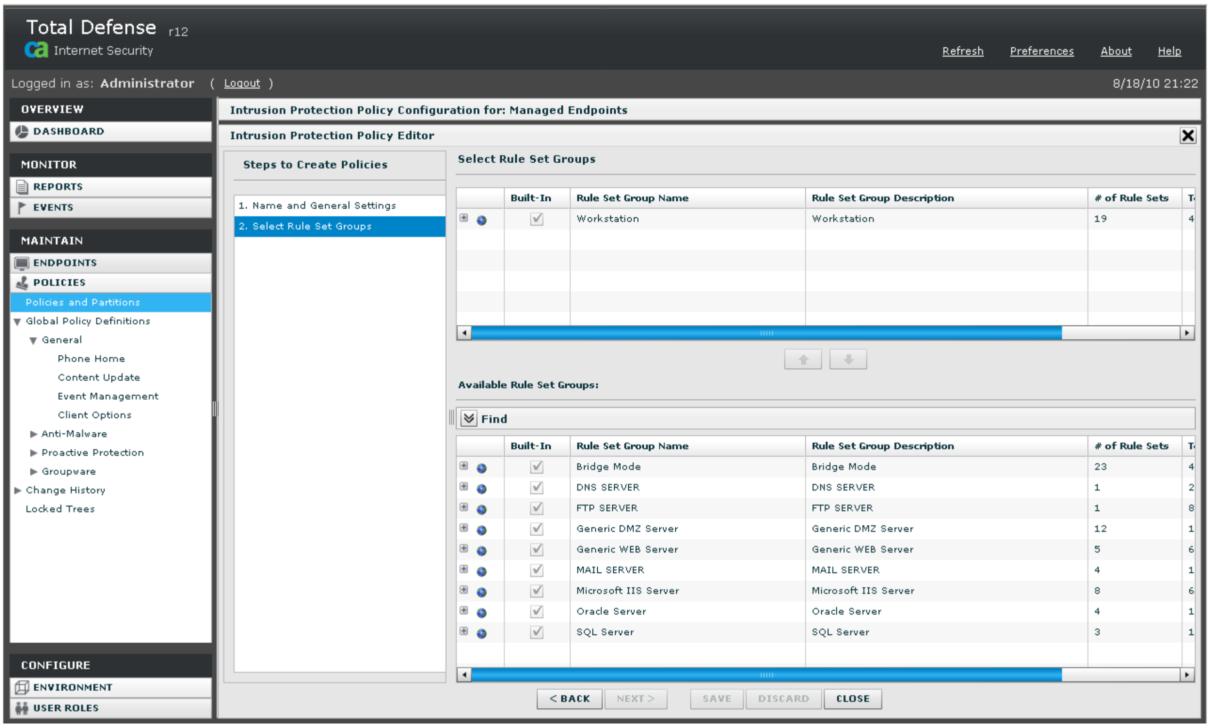
Ransomware Installers Asking For

The Enterprise Management Console (EMS) interface in Total Defense for Endpoint and Gateway is a significant improvement on previous versions, with a well organized and consistent appearance. The basic layout will be familiar to anyone with experience with enterprise security products.

The initial view after an administrator has logged in is a dashboard which shows graphical information about the security status of the network, including the status of virus signatures, malware, endpoints and the CA Global Advisor. The dashboard layout flexible and allows administrators to choose between tiled or side-by-side views. Each administrator can also customize the information displayed by the dashboard and save their personalized dashboard for future viewing.

On the client side the interface functions are organised into three tab categories: Overview, Anti-Malware and LogView. Although simple, everything that was required was available and it was easy to locate specific functions from the user interface. The interface will look familiar to anyone upgrading from the previous r8 release, or CA’s consumer products.

Policy Management



Intrusion Protection Policy Configuration for: Managed Endpoints

Intrusion Protection Policy Editor

Steps to Create Policies

1. Name and General Settings
2. Select Rule Set Groups

Select Rule Set Groups

	Built-In	Rule Set Group Name	Rule Set Group Description	# of Rule Sets	T
⊞ ●	✓	Workstation	Workstation	19	4

Available Rule Set Groups:

	Built-In	Rule Set Group Name	Rule Set Group Description	# of Rule Sets	T
⊞ ●	✓	Bridge Mode	Bridge Mode	23	4
⊞ ●	✓	DNS SERVER	DNS SERVER	1	2
⊞ ●	✓	FTP SERVER	FTP SERVER	1	8
⊞ ●	✓	Generic DMZ Server	Generic DMZ Server	12	1
⊞ ●	✓	Generic WEB Server	Generic WEB Server	5	6
⊞ ●	✓	MAIL SERVER	MAIL SERVER	4	1
⊞ ●	✓	Microsoft IIS Server	Microsoft IIS Server	8	6
⊞ ●	✓	Oracle Server	Oracle Server	4	1
⊞ ●	✓	SQL Server	SQL Server	3	1

Total Defense for Endpoint and Gateway r12 has two layers of Policy Management: partition assignment and policy trees.

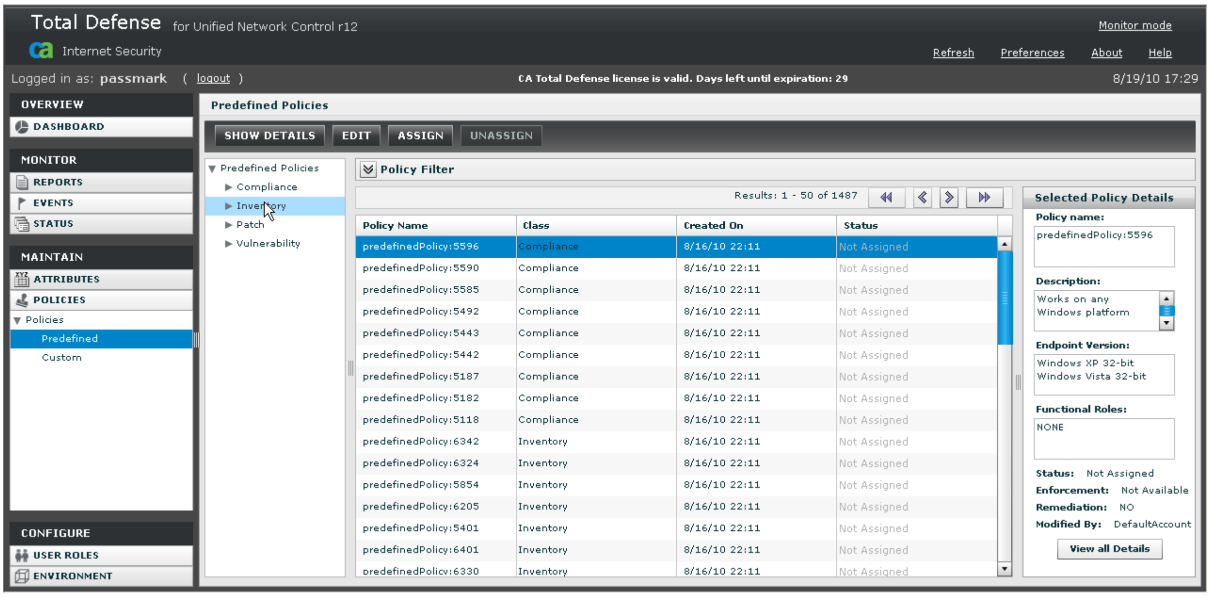
Endpoint machines are arranged into partition assignments for user access and management by different groups of administrators based on IP Address, Endpoint Name, Platform, Active Directory Tree or custom variables. For example, one group of administrators may manage policy for endpoint machines running a specific operating system only, while another group manages all systems in a specified IP Range.

Endpoints within partitions can then be further sub-divided into policy groups known as ‘branches’ based on similar criteria to partition assignment. As endpoints are discovered through Full or Incremental Discovery, they are automatically placed into the appropriate partition and branch with all associated security policies in effect.

Administrators have access to several categories of policy for each Branch. Policy control is relatively flexible, with dozens of configuration options available under each Policy category. In addition, Administrators with access to Global Policy Definitions can set policies which affect all endpoints across all partitions.

By default, all endpoints are assigned CA-recommended policies. The default policies provide a reasonable amount of protection for a new deployment ‘out of the box’ without interrupting business operations.

Unified Network Control (UNC)



Logged in as: passmark (logout)

CA Total Defense license is valid. Days left until expiration: 29

8/19/10 17:29

Predefined Policies

Results: 1 - 50 of 1487

Policy Name	Class	Created On	Status
predefinedPolicy:5596	Compliance	8/16/10 22:11	Not Assigned
predefinedPolicy:5590	Compliance	8/16/10 22:11	Not Assigned
predefinedPolicy:5585	Compliance	8/16/10 22:11	Not Assigned
predefinedPolicy:5492	Compliance	8/16/10 22:11	Not Assigned
predefinedPolicy:5443	Compliance	8/16/10 22:11	Not Assigned
predefinedPolicy:5442	Compliance	8/16/10 22:11	Not Assigned
predefinedPolicy:5187	Compliance	8/16/10 22:11	Not Assigned
predefinedPolicy:5182	Compliance	8/16/10 22:11	Not Assigned
predefinedPolicy:5118	Compliance	8/16/10 22:11	Not Assigned
predefinedPolicy:6342	Inventory	8/16/10 22:11	Not Assigned
predefinedPolicy:6324	Inventory	8/16/10 22:11	Not Assigned
predefinedPolicy:5854	Inventory	8/16/10 22:11	Not Assigned
predefinedPolicy:6205	Inventory	8/16/10 22:11	Not Assigned
predefinedPolicy:5401	Inventory	8/16/10 22:11	Not Assigned
predefinedPolicy:6401	Inventory	8/16/10 22:11	Not Assigned
predefinedPolicy:6330	Inventory	8/16/10 22:11	Not Assigned

Selected Policy Details

Policy name: predefinedPolicy:5596

Description: Works on any Windows platform

Endpoint Version: Windows XP 32-bit
Windows Vista 32-bit

Functional Roles: NONE

Status: Not Assigned

Enforcement: Not Available

Remediation: NO

Modified By: DefaultAccount

The Unified Network Control (UNC) is included as part of Total Defense for Endpoint and Gateway package, and can be optionally installed. UNC allows administrators enforce compliance standards for systems connecting to the business network. The UNC works as a policy layer on top of Microsoft's Network Access Protection (NAP), using NAP to enforce compliance with policies set by the administrator in the UNC console.

The UNC is not integrated with the Total Defense management console, but is rather accessed through a separate console which is installed on the server machine. If users are familiar with Total Defense management console, they will have no trouble using the UNC module console as it shares a consistent look and feel.

At the time of writing, the client component cannot be deployed through the network to endpoints from the UNC Console, but can be installed locally or deployed via Active Directory. During the course of our testing, we discovered that installing the Total Defense client prior to the UNC client would cause a conflict resulting in the unsuccessful installation of the UNC client. To work around this issue, administrators should install the UNC client prior to installing the Total Defense client.

We also discovered that, as this is a separate management console, user-created partition assignments (for user access control) and policy branches in the Management Server are unfortunately not shared with UNC.

An interesting feature of UNC is monitor mode, which lets administrators monitor the current environment without taking action on non-compliance. This feature can be useful in evaluating the correct configuration and policy settings for network access control prior to implementation.

In addition, CA's development team[1] has advised that UNC also has the following features:

- ***Role Based Policy Assessment:*** *Unified Network Control allows administrator to conduct role based policy assessment. Admin can make decision based on user identity and endpoint state.*

- ***Generic Detection:*** *Unified Network control has factory supplied attributes / objects that can be used to define policies to conduct configuration check of Total Defense EPP client installed on endpoint. Unified Network Control also provides generic detection capabilities that allows administrators to write custom attributes / objects to conduct similar assessment for non CA products.*

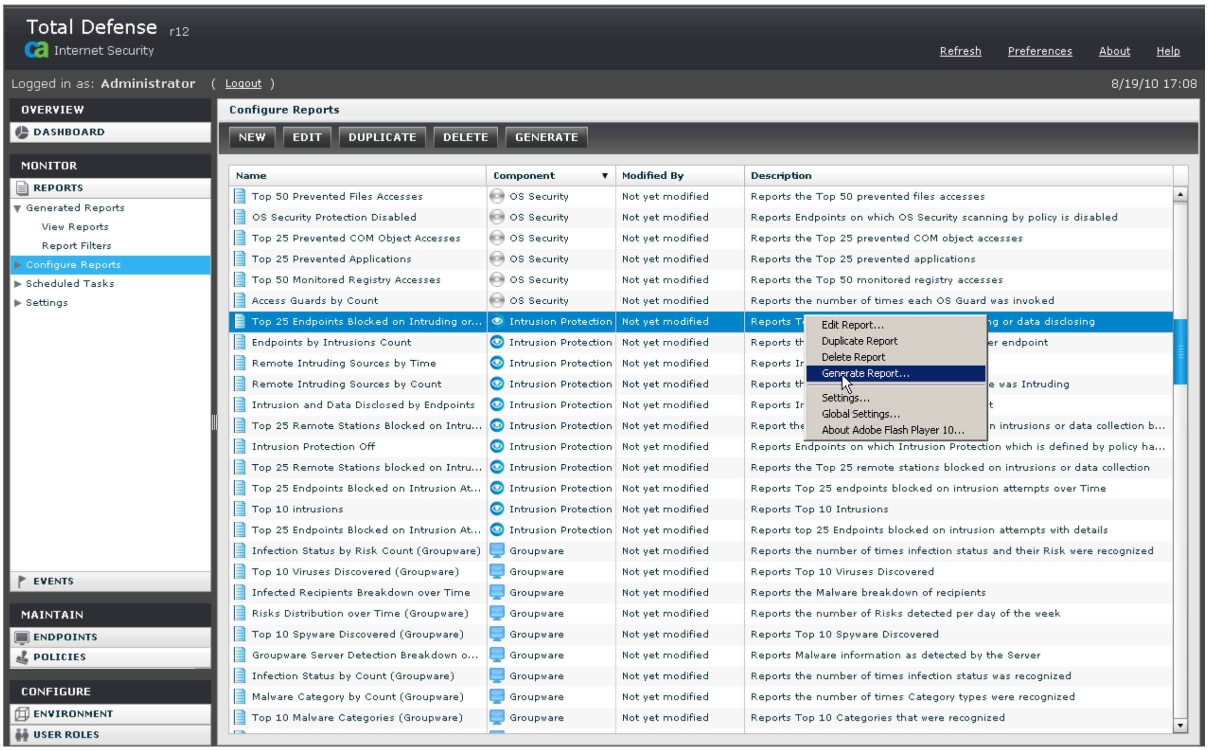
- ***Generic Remediation:*** *Unified Network Control offers generic remediation capability. Administrator can define custom remediation actions for every active policy. Remediation can be done by the mean of executing local process or making call to external system for executing pre-defined actions e.g. calling patch management system to push patches to the endpoint.*

Total Defense for Gateway

The Gateway component in Total Defense has remained unchanged from r8.1, with the exception of a new module allowing integration with the improved reporting functionality in r12.

[1] While we haven't had a chance to verify this functionality due to time limitations, the CA Development Team gave us this information about the unique features in UNC.

Report Generation



Name	Component	Modified By	Description
Top 50 Prevented Files Accesses	OS Security	Not yet modified	Reports the Top 50 prevented files accesses
OS Security Protection Disabled	OS Security	Not yet modified	Reports Endpoints on which OS Security scanning by policy is disabled
Top 25 Prevented COM Object Accesses	OS Security	Not yet modified	Reports the Top 25 prevented COM object accesses
Top 25 Prevented Applications	OS Security	Not yet modified	Reports the Top 25 prevented applications
Top 50 Monitored Registry Accesses	OS Security	Not yet modified	Reports the Top 50 monitored registry accesses
Access Guards by Count	OS Security	Not yet modified	Reports the number of times each OS Guard was invoked
Top 25 Endpoints Blocked on Intruding or…	Intrusion Protection	Not yet modified	Reports T ng or data disclosing
Endpoints by Intrusions Count	Intrusion Protection	Not yet modified	Reports th er endpoint
Remote Intruding Sources by Time	Intrusion Protection	Not yet modified	Reports Ir
Remote Intruding Sources by Count	Intrusion Protection	Not yet modified	Reports th e was Intruding
Intrusion and Data Disclosed by Endpoints	Intrusion Protection	Not yet modified	Reports Ir t
Top 25 Remote Stations Blocked on Intru…	Intrusion Protection	Not yet modified	Report the n intrusions or data collection b…
Intrusion Protection Off	Intrusion Protection	Not yet modified	Reports Endpoints on which Intrusion Protection which is defined by policy ha…
Top 25 Remote Stations blocked on Intru…	Intrusion Protection	Not yet modified	Reports the Top 25 remote stations blocked on intrusions or data collection
Top 25 Endpoints Blocked on Intrusion At…	Intrusion Protection	Not yet modified	Reports Top 25 endpoints blocked on intrusion attempts over Time
Top 10 intrusions	Intrusion Protection	Not yet modified	Reports Top 10 Intrusions
Top 25 Endpoints Blocked on Intrusion At…	Intrusion Protection	Not yet modified	Reports top 25 Endpoints blocked on intrusion attempts with details
Infection Status by Risk Count (Groupware)	Groupware	Not yet modified	Reports the number of times infection status and their Risk were recognized
Top 10 Viruses Discovered (Groupware)	Groupware	Not yet modified	Reports Top 10 Viruses Discovered
Infected Recipients Breakdown over Time	Groupware	Not yet modified	Reports the Malware breakdown of recipients
Risks Distribution over Time (Groupware)	Groupware	Not yet modified	Reports the number of Risks detected per day of the week
Top 10 Spyware Discovered (Groupware)	Groupware	Not yet modified	Reports Top 10 Spyware Discovered
Groupware Server Detection Breakdown o…	Groupware	Not yet modified	Reports Malware information as detected by the Server
Infection Status by Count (Groupware)	Groupware	Not yet modified	Reports the number of times infection status was recognized
Malware Category by Count (Groupware)	Groupware	Not yet modified	Reports the number of times Category types were recognized
Top 10 Malware Categories (Groupware)	Groupware	Not yet modified	Reports Top 10 Categories that were recognized

Total Defense for Endpoint and Gateway provides users with a huge number of reports ‘out-of-the-box’. These reports cover all product components and come with easy-to-use templates for creating custom reports. User access permissions are also enforced when viewing or generating reports.

Report generation is highly configurable and is one of the highlights of the product; users can create their own custom report, or edit one of the many preset reports provided to suit their needs. Users can also schedule periodic reports using “Schedule Tasks”, and configure generated reports to be e-mailed to an account, printed locally or have the generation event submitted to an RSS feed.

Once generated, reports can be filtered on different categories including event severity, output count, time frame, IP address, endpoint name, and more. Reports can be generated as pie charts, bar graphs or tables in one of four file formats: PDF, CSV, HTML and Word.

However, we found that generating reports on-demand would place the requested report in a queue for execution. There was very little feedback while reports were in the queue, which became an issue when we attempted to generate multiple reports at the same time. We ended up clicking on “Refresh” button repeatedly to check for updates on the status of report generation.

Report filters also allow narrowing down of the reports displayed in the View Reports page to suit user needs. Report filters are highly customizable to retrieve the exact information required by the user and can be based on time, status, component, partition, name, task and more.

Remote Deployment Service & Support

CA are currently offering a free Remote Deployment Service to assist CA customers with installing and configuring Total Defense for Endpoint and Gateway r12, migrating from legacy versions of Total Defense, as well as assisting with the removal of third party security suites.

Remote deployment assistance is available between 6:30am and 9:00pm CST from Mondays to Fridays (and 9am to 4pm GMT for European users). The service is available worldwide, but is currently limited to English-speaking customers only.

CA also offers all their customers free, 24/7 phone-based technical support at no extra charge.

License Management

CA provides the Product Subscription Management (PSM) web site, which is accessible from the management console. This website lets administrators actively manage their CA Total Defense licenses. CA have referred to this feature as “licensing in the cloud”.

If the user decides to expand their deployment or add additional components after initial purchase of CA Total Defense r12, they can use the PSM to request a migration to a product with additional features. In our testing, however, we didn’t see any option to downgrade to one of the simpler, presumably cheaper, product editions. If a user purchases additional components, CA sends a new license key for the additional products. The same is true for upgrading product to a higher version. If user is renewing, upgrading or migrating existing product and not adding new components, they can simply enter the new license key using the Link Order tab in the Product Subscription Management tool. The PSM application lets user easily manage the assignment, removal and reassignment of endpoints to and from license pool.

The PSM also includes a link for the CA resellers and can provide reports to the reseller about the number of licenses actually deployed. Making a request for a renewal or migration from PSM will route the request back to the reseller who initially sold you the software, which should make CA’s resellers happy as it maintains their business relationship with the customer. From an end user’s point of view this can also be beneficial, but it might have been nice to allow the option to instantly purchase additional licenses from CA, rather than waiting for the reseller to get back to them.

CA has advised us that Total Defense customers can also deploy an unlimited number of additional end points beyond the licensed amount with a grace period of 30 days. This is beneficial for customers who have expanded their deployment and require immediate protection from malware, but may still be involved in the purchasing process. This will also help customers that experience a temporary spike in their endpoint numbers, and allow purchases to be consolidated into a larger block.

Customers only need to purchase Groupware licenses for server nodes where it is required. For example, if a deployment has 500 endpoint systems but only one system (the e-mail server) requires the Groupware component, only one license is required. The ‘base’ CA Total Defense Management Console can additionally be installed as much as required, without incurring additional costs or license use.

Value

The recommended retail price of CA Total Defense places it on par with similar products from other vendors. However unlike other vendors CA includes a Remote Deployment Service and 24/7 phone-based technical support as part of the deal.

As a bundle, CA Total Defense for Endpoint and Gateway r12 provides a massive amount of functionality in a single box. The Total Defense package is multi-layered and comprehensive, providing protection for gateways, network access control and compliance, host intrusion protection as well as groupware features.

As a package these bundled features and services, combined with the flexible licensing, make the package great value.

Of particular interest is the substantial discount CA is offering customers who are switching from a competing product. In many cases it is cheaper to purchase new CA Total Defense endpoint licenses than to renew licenses with an existing enterprise security vendor.

Endpoint Performance

PassMark Software has conducted benchmark tests for system impact and resource usage for endpoint components of CA Total Defense and three leading enterprise suites. To increase chart readability, we have abbreviated the names of competing suites in the graphs in the following section.

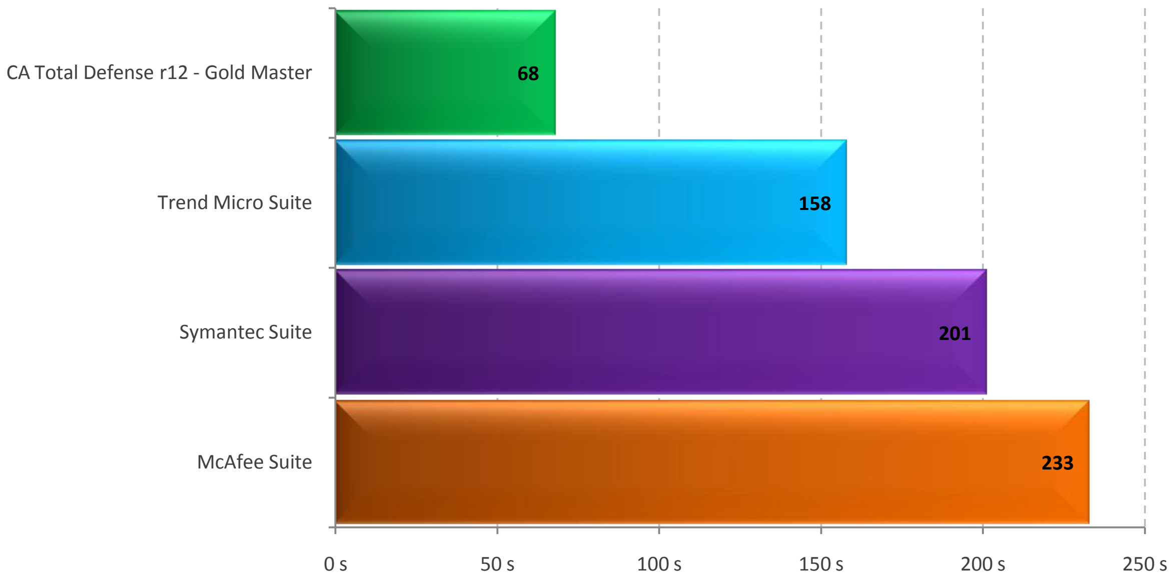
The full names of product variants and versions we have tested can be found in the table below:

Product Name in Graph	Products Tested	Product Version
CA Total Defense r12	Server: CA Total Defense Management Server Client: CA Total Defense	12.0
Symantec Suite	Server: Symantec Endpoint Protection Manager Client: Symantec Endpoint Protection	11.0
McAfee Suite	Server: McAfee ePolicy Orchestrator Client: McAfee VirusScan Enterprise Client: McAfee Host Intrusion Prevention	4.7
Trend Micro Suite	Server: Trend Micro OfficeScan Server Client: Trend Micro OfficeScan Client	10.0

For all products, we have tested only the basic product and have not installed any optional Network Access Control add-ons as part of testing. For example, we have not included the Unified Network Control (UNC) module as part of our tests for CA Total Defense for Endpoint and Gateway.

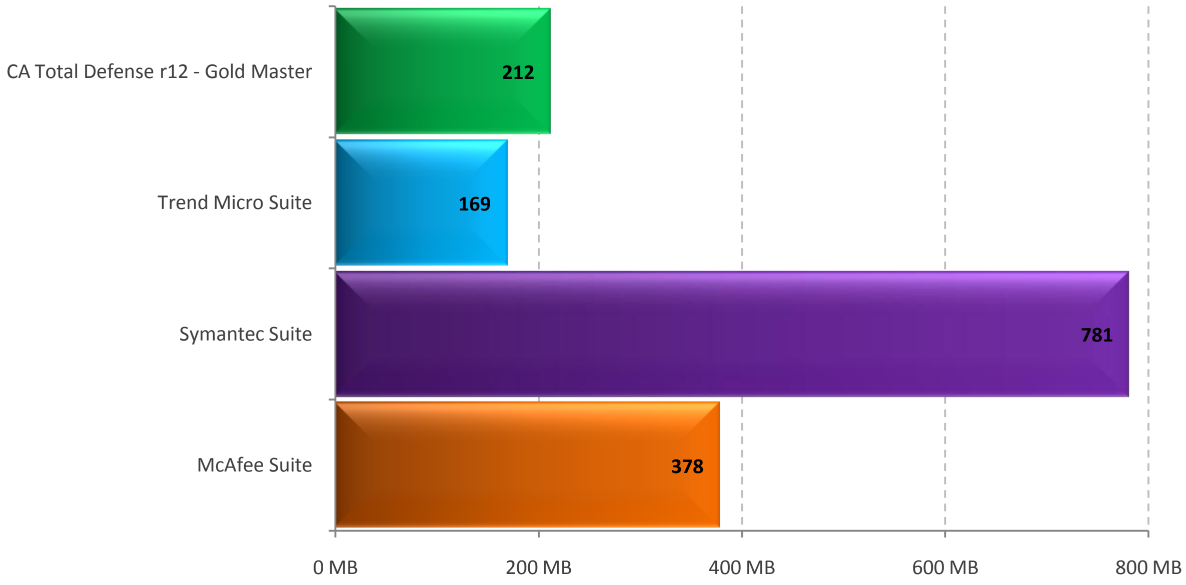
Scan time

This metric measures the time taken to scan a sample set of files. Our final result is measured in seconds and calculated from an average of five samples.



Client Installation Size

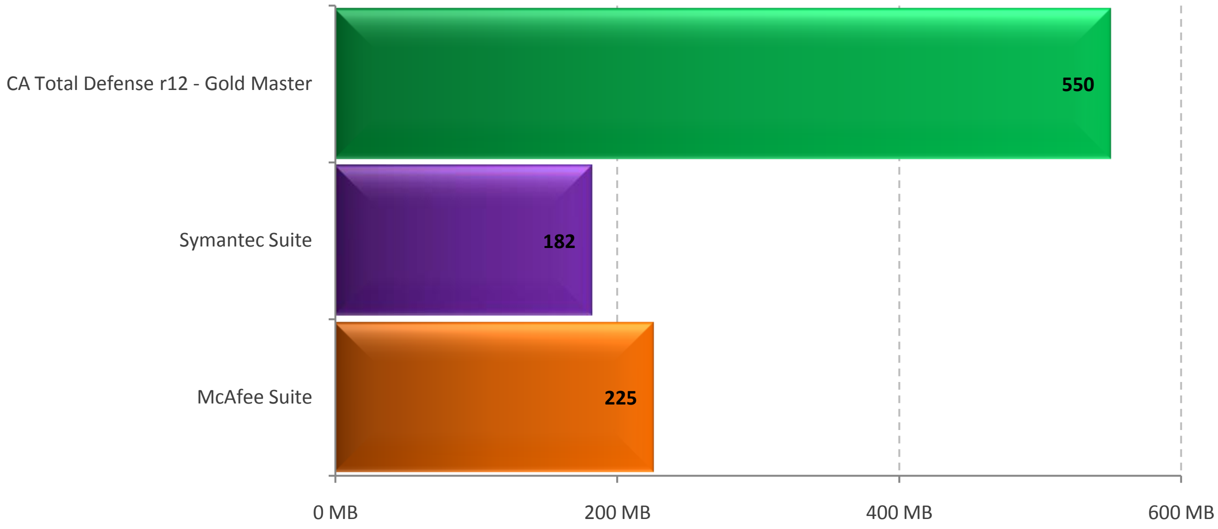
This metric measures the total additional disk space consumed by the installation of the endpoint client. The result is measured in megabytes (MB).



Memory Usage Commit Charge

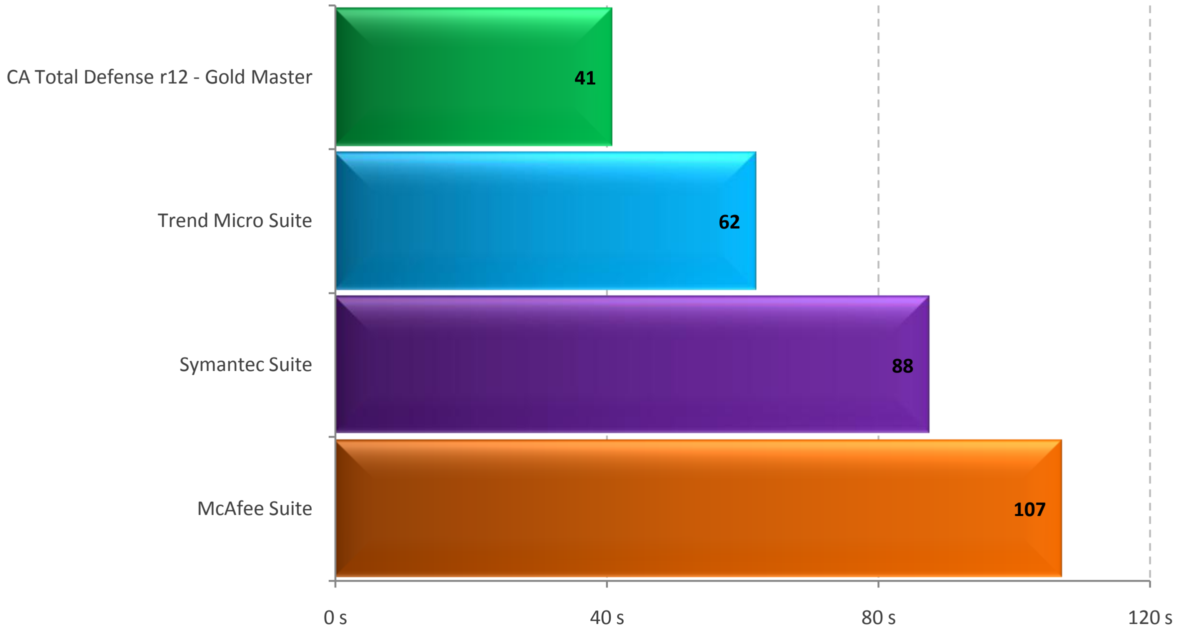
This metric measures the total additional memory use consumed by the endpoint machine during a period of system idle where an endpoint security product has been installed. Our final result is measured in megabytes (MB), and calculated from an average of 40 samples.

This test was conducted on the **Windows 7 Ultimate (64-bit)** platform. Due to time constraints, test results for the Trend Micro Suite are unavailable.



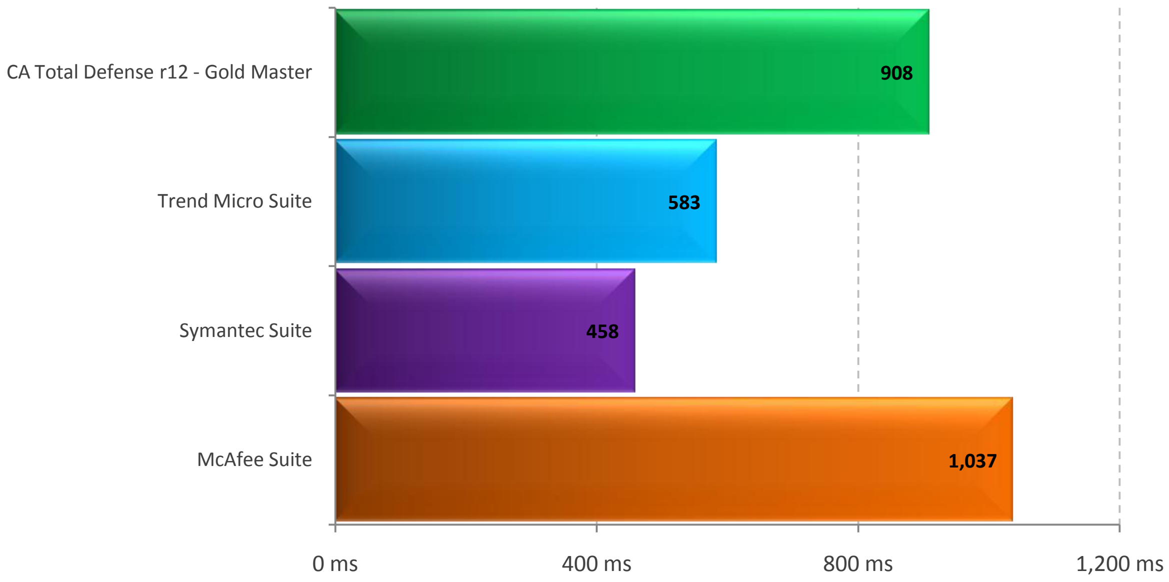
Boot time

This metric measures the time taken to boot the machine where an endpoint security product has been installed. Our final result is measured in seconds (s) and calculated from an average of fifteen (15) reboots.



Internet Explorer launch time

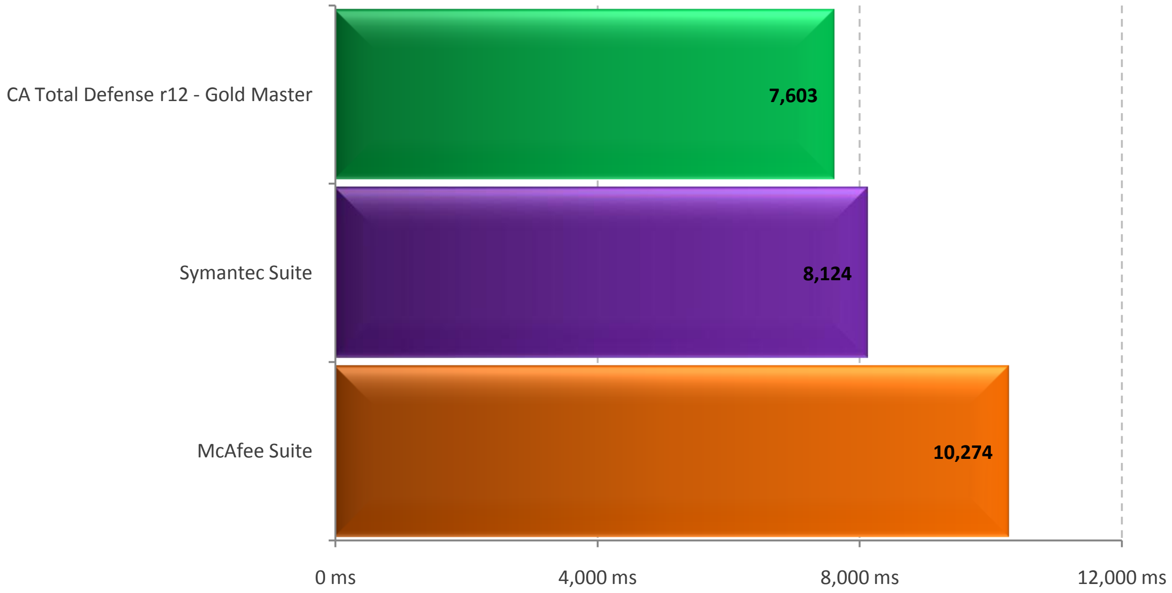
This metric measures the total time taken to launch Internet Explorer. Our final result is measured in milliseconds (ms), and calculated from an average of five (5) samples.



Word Document Launch Time

The metric measures the total time taken to launch a moderately sized Microsoft Word 2007 document with a system restart prior to application launch. Our final result is measured in milliseconds (ms), and calculated from an average of five (5) samples.

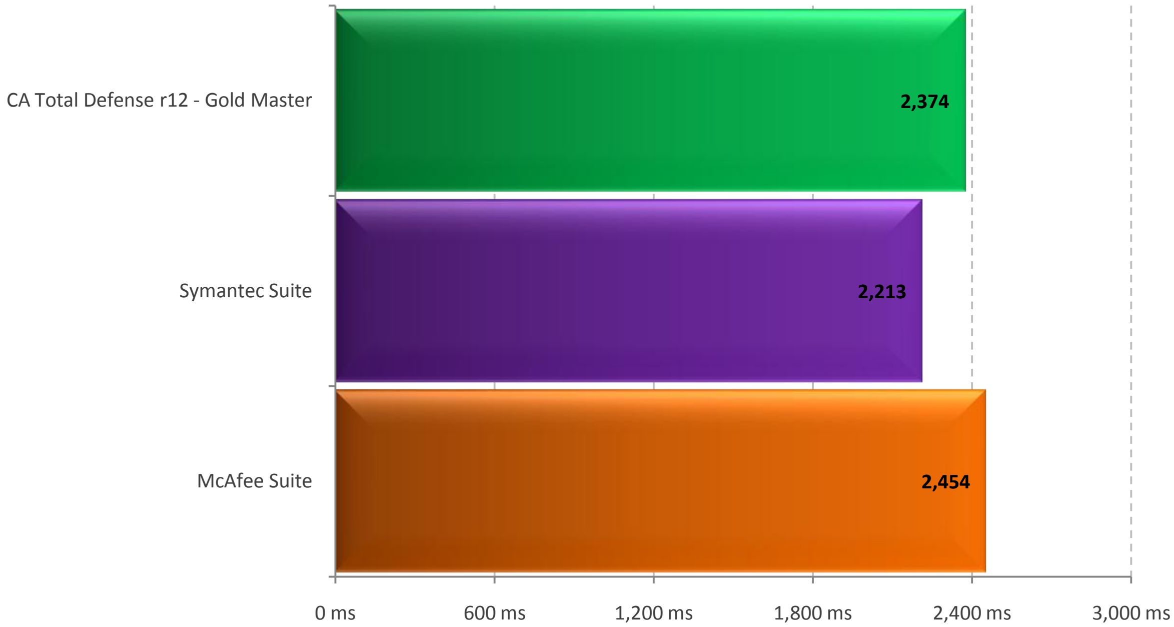
This test was conducted on the **Windows 7 Ultimate (64-bit)** platform. Due to time constraints, test results for the Trend Micro Suite are unavailable.



Word Document Restart Time

The metric measures the total time taken to launch a moderately sized Microsoft Word 2007 document without a system restart prior to application launch. Our final result is measured in milliseconds (ms), and calculated from an average of ten (10) samples.

This test was conducted on the **Windows 7 Ultimate (64-bit)** platform. Due to time constraints, test results for the Trend Micro Suite are unavailable.



Disclaimer and Disclosure

This report is intended to be a standalone review of the benefits and flaws of CA Total Defense r12 – Gold Master Release. This review makes no attempt to compare CA Total Defense r12 with competing enterprise products, with the exception of the performance test results which are quantitative measures.

All other views herein represent PassMark Software's subjective opinions and experiences in installing, configuring or operating CA Total Defense for Endpoint and Gateway r12.

Disclaimer of Liability

While every effort has been made to ensure that the information presented in this report is accurate, PassMark Software Pty Ltd assumes no responsibility for errors, omissions, or out-of-date information and shall not be liable in any manner whatsoever for direct, indirect, incidental, consequential, or punitive damages resulting from the availability of, use of, access of, or inability to use this information.

Disclosure

The production of this report was funded by CA, Inc.

Trademarks

All trademarks are the property of their respective owners.

Contact Details

PassMark Software Pty Ltd
Suite 202, Level 2
35 Buckingham St.
Surry Hills, 2010
Sydney, Australia

Phone	+ 61 (2) 9690 0444
Fax	+ 61 (2) 9690 0445
Web	www.passmark.com

Appendix 1 – Test Environment

Windows Vista – Client Machine Specification

Except for the tests noted below the client performance tests were conducted on an endpoint machine running *Windows Vista Ultimate SP2 (32-bit)* with the following technical specifications:

Model:	IBM/Lenovo A55 ThinkCentre Desktop
CPU:	Core2 Duo 6300 @ 1.86GHz
Video Card:	Intel(r)Broadwater-G Graphics Chip Accelerated VGA BIOS
RAM:	2037 MB RAM
Main HDD:	233GB WDC WD2500JS-08NCB1
Network	Gigabit (1GB/s) Ethernet

Windows 7 – Client Machine Specification

The performance tests **Memory Usage Commit Charge** and **Word Document Launch Time** were conducted on an endpoint machine running *Windows 7 Ultimate (64-bit)* with the following technical specifications:

CPU:	Intel Core i7 920 Quad Core @ 2.67GHz
Video Card:	nVidia GeForce 8800 GT
Motherboard:	Intel x58 Motherboard
RAM:	6GB DDR3 RAM
HDD:	Western Digital 500GB 7200RPM