



# SEP 12.1 Advanced Features

**Anthony Flaviani**

Director, Technical Field Enablement



# Agenda

1 Changes in the Threat Landscape

2 Symantec Endpoint Protection 12

3 Unrivaed Security

4 Blazing Performance

5 Built For Virtual Environments

# Malware Authors Have Switched Tactics



75% of malware infect less than 50 machines

From:

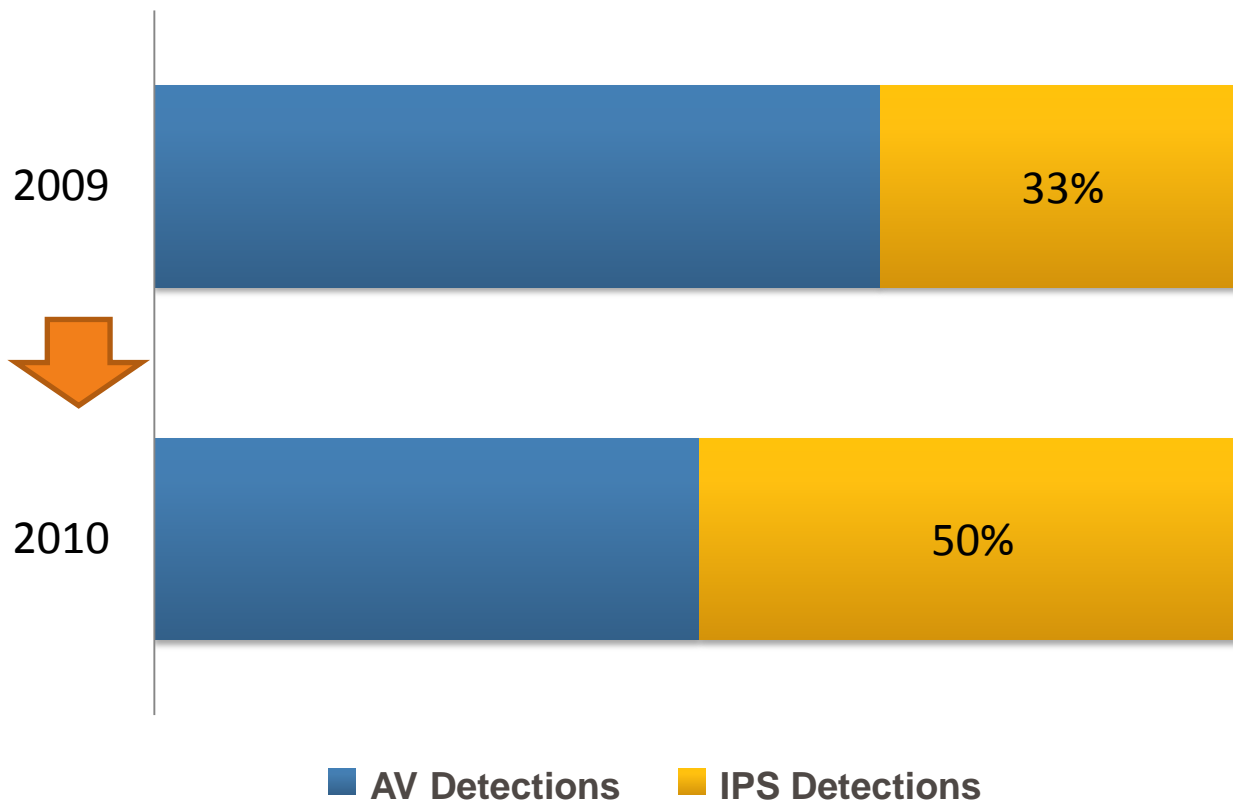
A mass distribution – one worm hits millions of PCs

- Storm made its way onto millions of machines across the globe

To:

A micro distribution model.

- Hacked web site builds a trojan for each visitor
- The average **Harakit** variant is distributed to 1.6 users!



## The Problem

# Millions of file variants (good and bad)

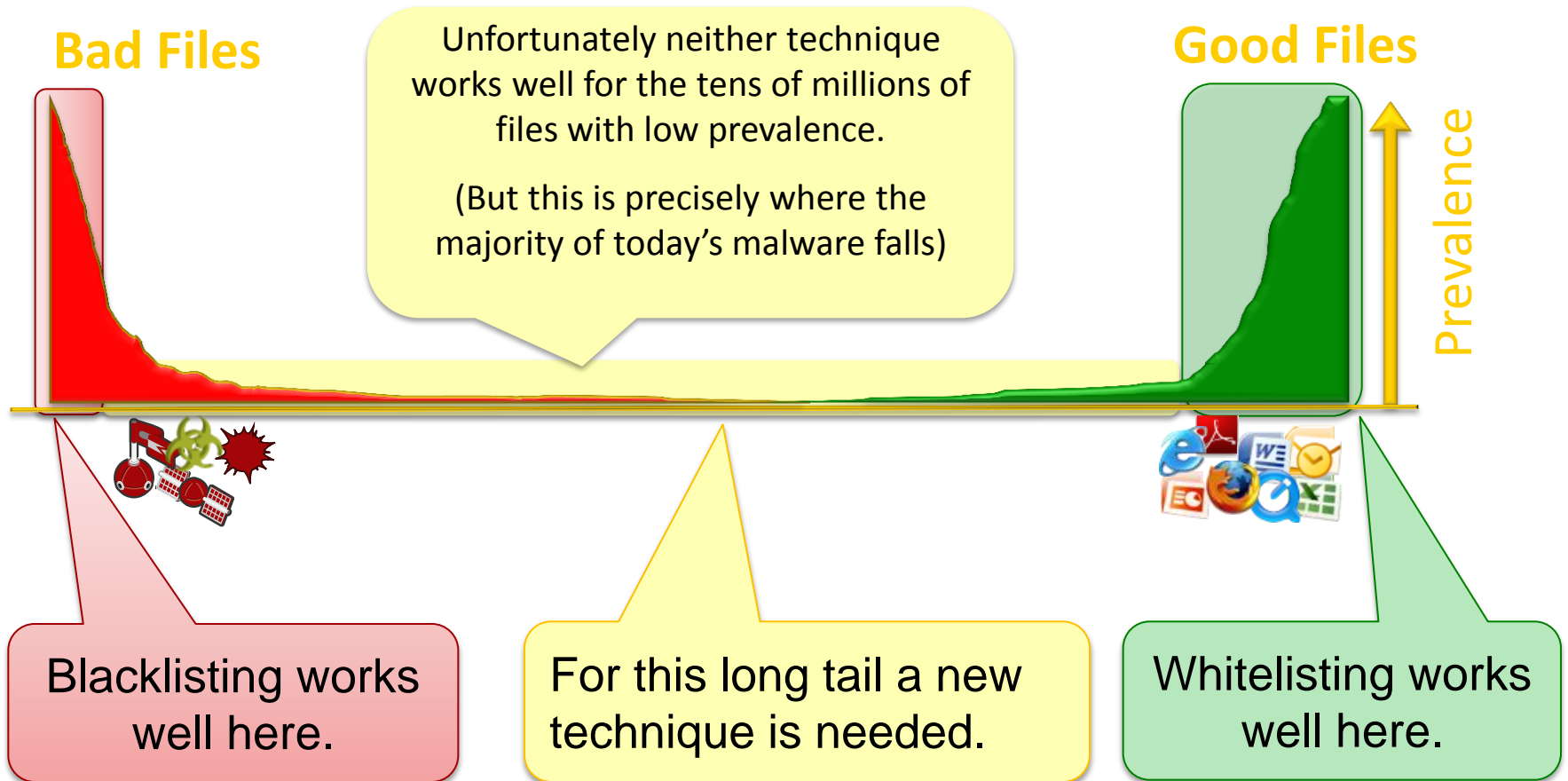
- So imagine that we know:



- about every file in the world today...
- and how many copies of each exist
- and which files are good and which are bad
- Now let's order them by prevalence with
  - **Bad** on left
  - **Good** on the right

## The Problem

# No Existing Protection Addresses the “Long Tail”





# **Symantec Endpoint Protection 12.1**



# What's New in SEP 12



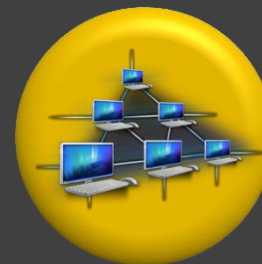
## Unrivalled Security

- Powered by Insight
- Real Time Behavior Monitoring with SONAR



## Blazing Performance

- Up to 70% reduction in scan overhead
- Smarter Updates
- Faster Management



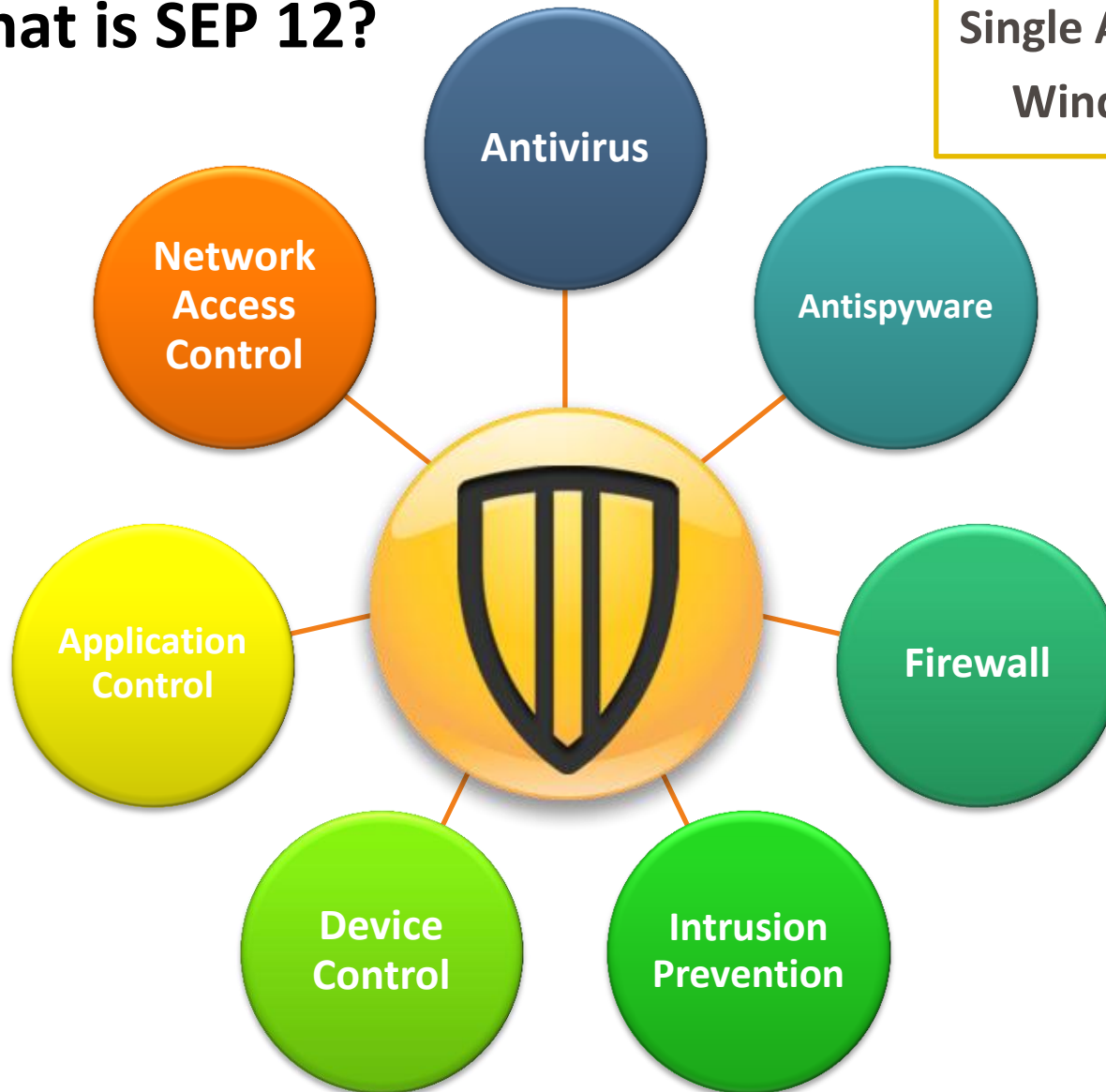
## Built for Virtual Environments

- Tested and optimized for virtual environments
- Higher VM densities



# What is SEP 12?

Single Agent, Single Console  
Windows, Mac & Linux



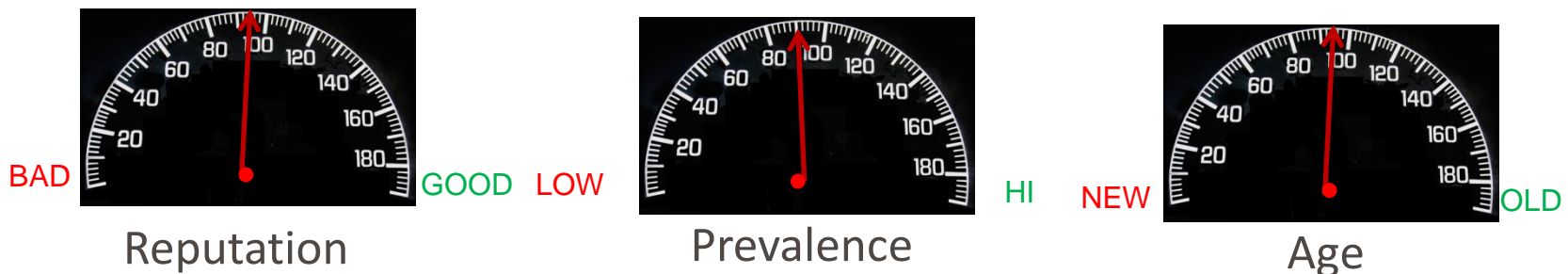


# Powered by Insight



Proactive protection against new, mutating threats

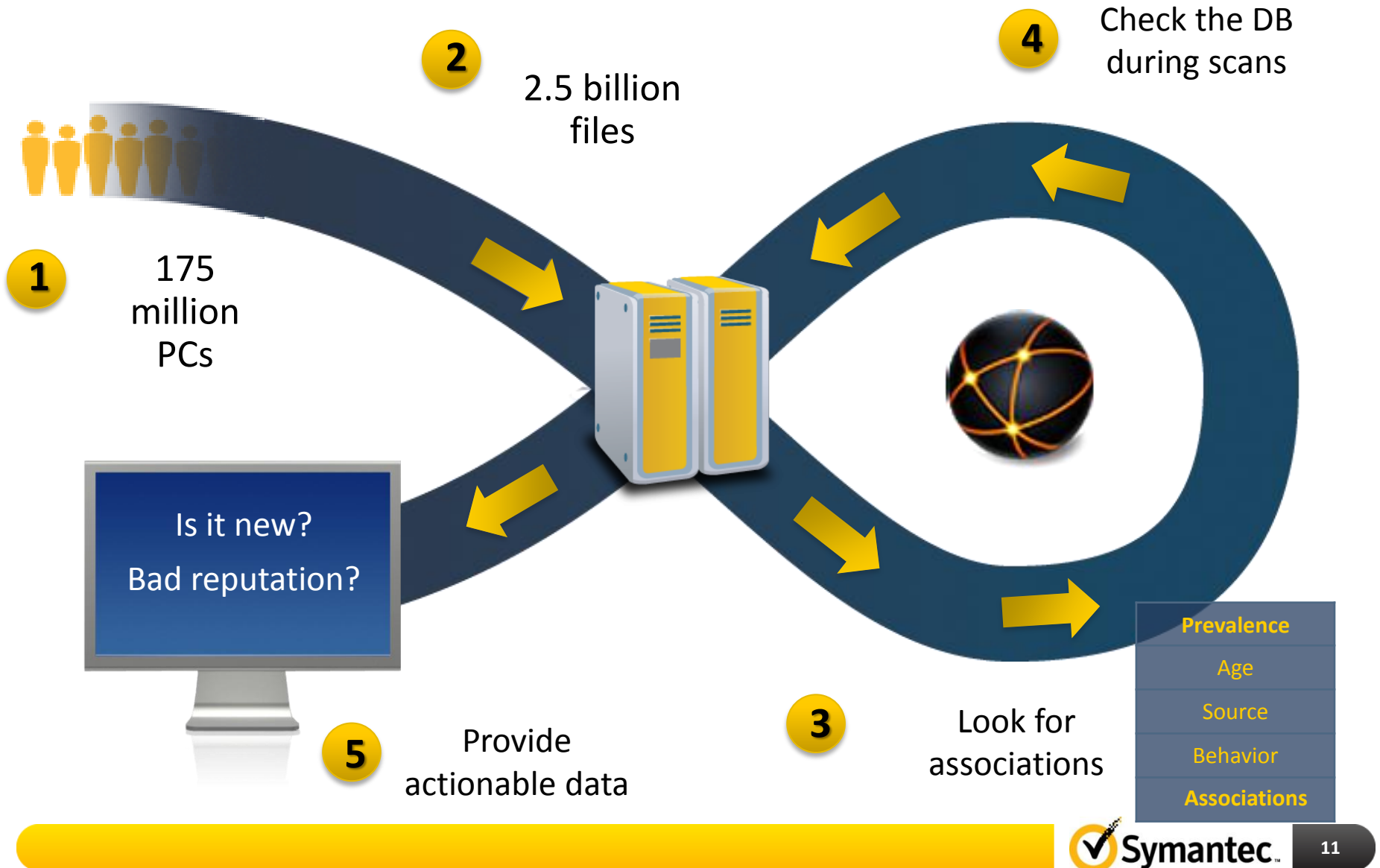
- Puts files in context, using their age, frequency, location and more to expose threats otherwise missed
- Using community-based security ratings
- Derived from Symantec's more than 175 million endpoints





Unrivaled  
Security

# How Insight Works



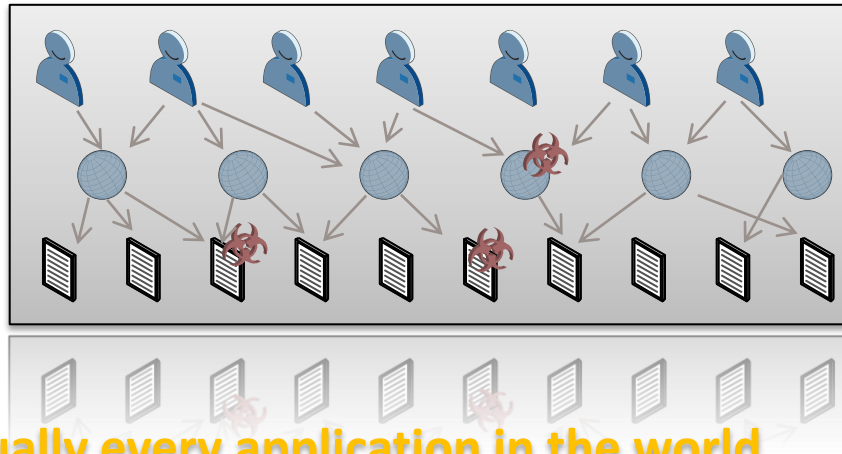
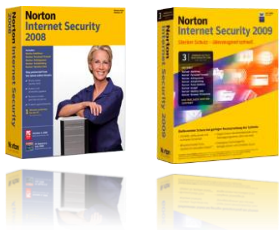
# Reputation

## Our Implementation

We then built a massively-parallel analysis algorithm

### Norton Community Watch

Opt in program to collect anonymous data



### Symantec Reputation Engine

Uses the collected data to determine safety reputation



**Symantec  
File Safety  
Reputations**

**Our system tracks virtually every application in the world**

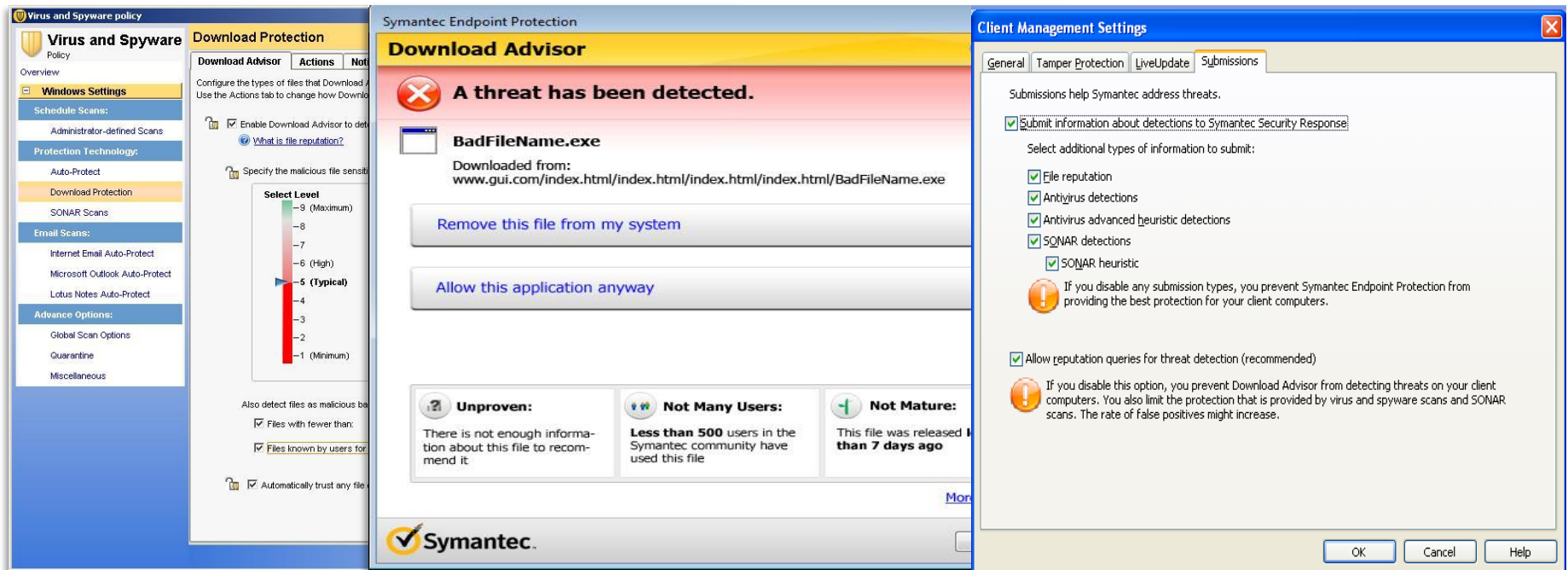
- 2.5B unique app files across all versions and languages
- It has data on all files: EXEs, drivers, DLLs, plug-ins
- Provides reputation, prevalence, discovery date of every file
- Leveraged in Download Insight, SONAR, and ScanLess



Unrivaled  
Security

# Download Insight

- Download Insight is a technology that checks the reputation of binaries being downloaded and blocks them if they are “Bad”.
- Download Insight scans files when they are downloaded using what we term a portal application (IE, Firefox, IE)



# A Weapon Against False Positives

Reputation reduces false positives in two important ways:



- 1 Our back-end systems check the reputation of every file sent to our labs

**Filters legitimate files so that analysts don't inadvertently fingerprint these**



- 2 Our endpoint products consult with reputation before removing suspicious software

**Greatly reduces the risk of a high prevalence FP**



# Behaviour Analysis and System Heuristics

- Symantec Online Network for Advanced Response (SONAR)
  - Suspicious Behavior Detection
  - System Change detections
    - Hosts file and DNS change detections.
  - Tamper Protection (SymProtect)
- It's the next generation heuristics engine
- Unlike SEP 11, SONAR Provides real time protection
- Able to convict on process launch.
  - Behaviors of applications are assessed as they happen, in real time.
- Improved with new support for File and Registry protection.
- Updateable through LiveUpdate





Unrivaled  
Security

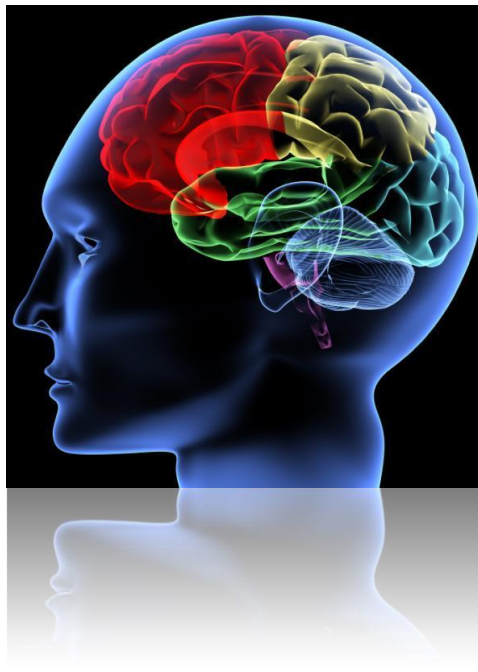
## SONAR Features

This information enables three new features

Artificial Intelligence Based  
Classification engine



Human-authored  
Behavioral Signatures

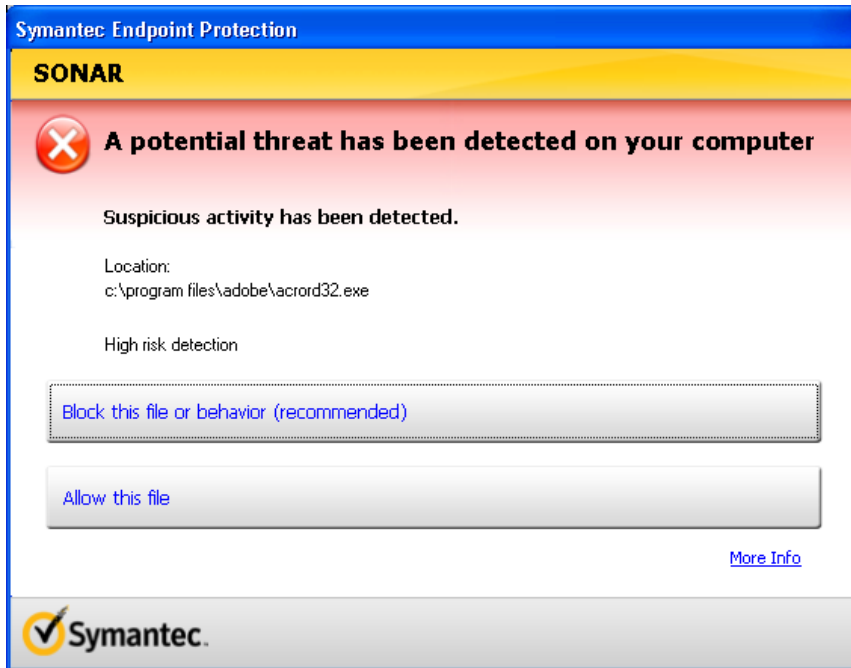


Behavioral Policy  
Lockdown

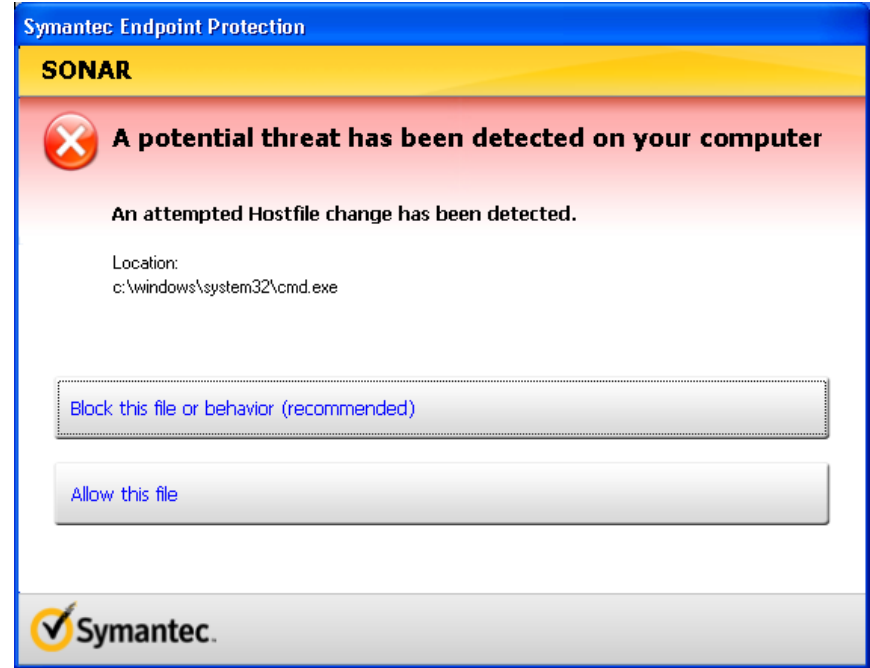




# SONAR



Detect:  
**Suspicious Behavior**



Detect:  
**System Changes**

## Results in the Field



	Blocked June 2010	Blocked Since Launch
Standalone Reputation	1.17M	6.7M
Heuristics + Reputation	192,000	2.2M
Behavior + Reputation	1.29M	14.6M
Reputation Behavior +	2.65M	23.5M

**And this is just the beginning!**



Unrivaled  
Security

# SymProtect

- SymProtect (Tamper Protection) has been changed from Log-only by default to Block and Log.
- SEP 12.1 also made the addition of file and registry protection.
- Process protection – only processes backed by files in the SEP silo
  - Migrations will keep legacy settings.
  - May affect custom tools that try to modify SEP resources:
    - Registry
    - Files
    - Named objects
    - Processes (Only processes backed by files in the SEP silo are protected).
- By default, only Symantec signed applications are not affected by Tamper Protection
  - Administrators may create authorizations within SEPM



# Updated Firewall/IDS/Browser Heuristics

The screenshot displays the Symantec Firewall Policy console. The 'Rules' tab is active, showing a list of firewall rules. Below it, the 'Windows Integration' tab is also visible, showing options to disable the Windows Firewall and a message to suppress notification at startup. A context menu is open over the 'Disable Windows Firewall' section, showing options: 'Disable Once Only', 'No Action', 'Disable Once Only', 'Disable Always', and 'Restore If Disabled'. The 'Detailed Network Threat Protection Event Information' window is also open, showing event details for a blocked Remote BinLogin BO 2 attack.

No	En...	Name	Action	Application	Host	S
1	<input type="checkbox"/>	Block IPv6	Block	Any	Any	
2	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (Teredo)	Block	Any	Any	
3	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (ISATAP)	Block	Any	Any	
4	<input checked="" type="checkbox"/>	Allow fragmented packets	Allow	Any	Any	
5	<input checked="" type="checkbox"/>	Allow wireless EAPOL	Allow	Any	Any	
6	<input checked="" type="checkbox"/>	Allow Local File Sharing to local computers	Allow	Any	Any	

**Windows Integration**

**Disable Windows Firewall:**

At startup, disable the Windows Firewall. Firewall will be re-enabled when Symantec Firewall is installed.

**Windows Firewall Disabled Message:**

Suppress notification message at startup if Windows Firewall is disabled.

**Detailed Network Threat Protection Event Information**

**Symantec**

**Client Affected:** [SID: 20038] Remote BinLogin BO 2 attack blocked. Traffic has been blocked for this application: 'DEVICE\HARDISK\VOLUME1\PORTLISTENER\PORTLISTENER.EXE'

**Event Description:** Intrusion Prevention

**Attack Type:** Remote BinLogin BO 2

**Event Time:** 01/07/2011 13:57:35

**Remote Host IP:** 192.168.191.1

**Occurrence:** 1

**Alert:** 1

**Begin Time:** 01/07/2011 13:17:48

**End Time:** 01/07/2011 13:17:48

**Location Name:** Default

**Severity:** Critical

**Local MAC:** 903CFB87669E19A8AEE01977E5E2F70

**Remote MAC:** 903CFB87669E19A8AEE01977E5E2F70

**Network Protocol:** TCP

**Traffic Direction:** Inbound

**Send SNMP trap:** 1

**Remote Host Name:** N/A

**Hack Type:** 0

**Application Name:** /DEVICE\HARDISK\VOLUME1\PORTLISTENER\PORTLISTENER.EXE

**Risk Detected:** Default

**Domain Name:** My Site

**Site Name:** My Site

**Server Name:** hercules

**Group Name:** My Company\Default Group

**Signature ID:** 20038

**Signature Name:** Remote BinLogin BO 2

**Signature Sub ID:** 69975

**Intrusion URL:** N/A

**Intrusion Payload URL:** N/A

**Local Port:** 513

**Remote Port:** 59166

**Computer Name:** alototskXP3v1

**Current:** alototskXP3v1

**When event occurred:** alototskXP3v1

**IP Address:** 192.168.191.128

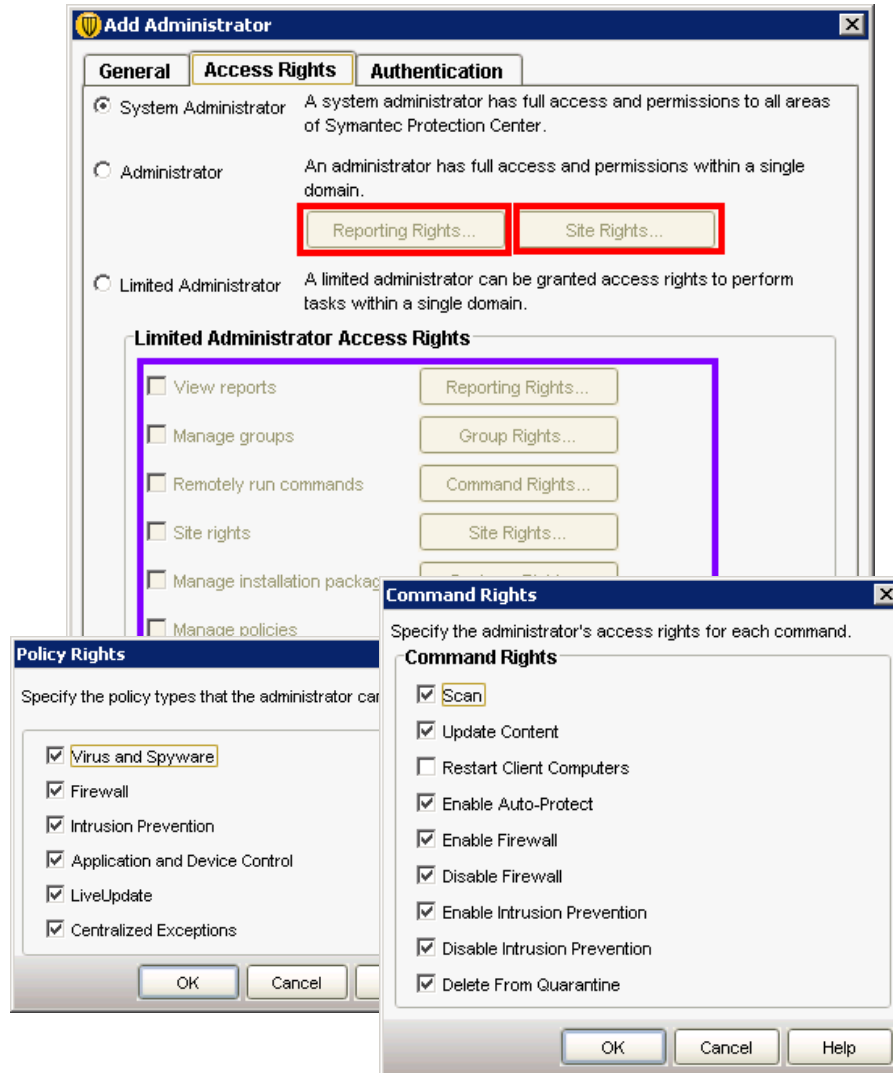
**Current:** 192.168.191.128

**When event occurred:** 192.168.191.128

- NDIS5/NDIS6 Support
- Firewall Rules can be applied to IPv6 Traffic
- Decoupled FW Dependencies with AV/DC/IDS
- Improved Windows Firewall Integration
- Improved IDS Reporting and Error Handling
- Browser Heuristics



# Role-based Access Control



- Limit the rights of administrators based on administrative role
- Allow administrators to view policies by assigning them read-only access
- Restrict what commands admins can do based on their need
- Assign policy rights based on admin expertise



# Advanced Security Policies

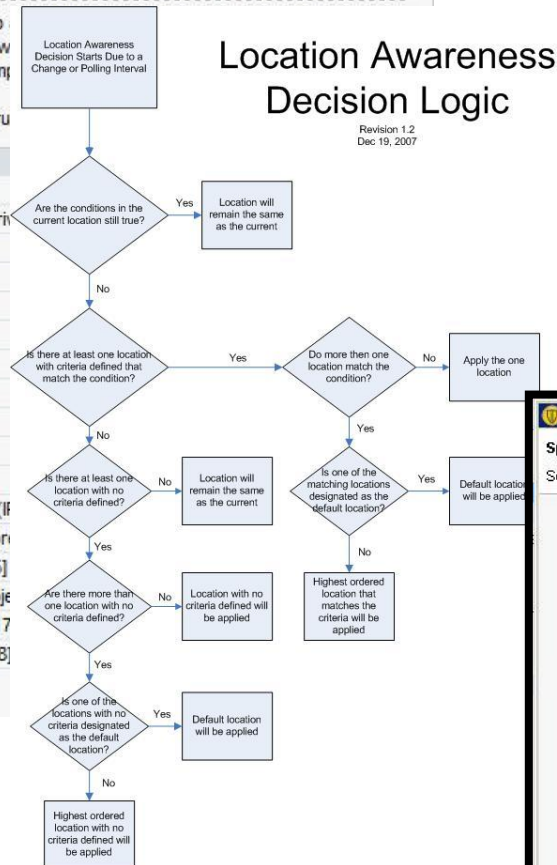
## Application Control

### Application Control Rule Sets

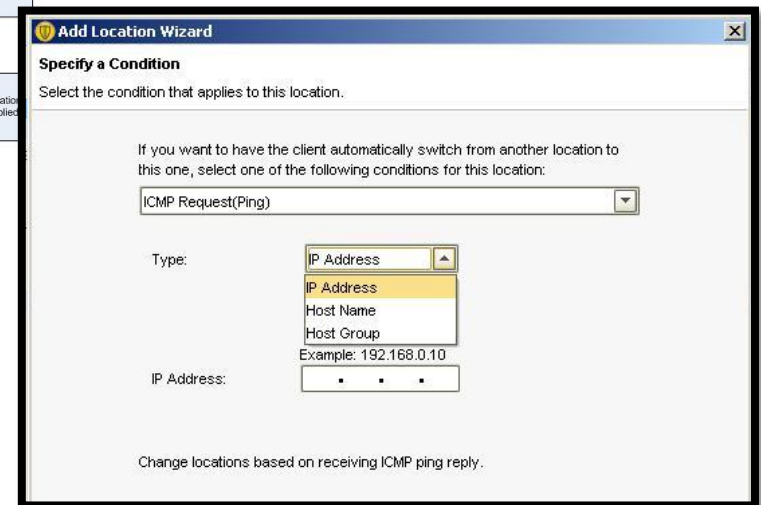
Application Control restricts what an application is permitted to do. Application Control has many purposes, including preventing malware and confidential data from inadvertently being removed from your computer.

Only advanced administrators should create Application Control rule sets.

Enabled	Rule Sets
<input type="checkbox"/>	Block applications from running [AC2]
<input checked="" type="checkbox"/>	Block programs from running from removable drives [AC3]
<input type="checkbox"/>	Make all removable drives read-only [AC4]
<input type="checkbox"/>	Block writing to USB drives [AC5]
<input type="checkbox"/>	Log files written to USB drives [AC6]
<input type="checkbox"/>	Block modifications to hosts file [AC7]
<input type="checkbox"/>	Block access to scripts [AC8]
<input type="checkbox"/>	Stop software installers [AC9]
<input type="checkbox"/>	Block access to Autorun.inf [AC10]
<input type="checkbox"/>	Block Password Rest Tool [AC11]
<input type="checkbox"/>	Block File Shares [AC12]
<input type="checkbox"/>	Prevent changes to Windows shell load points (Hijack) [AC13]
<input type="checkbox"/>	Prevent changes to system using Internet Explorer [AC14]
<input type="checkbox"/>	Prevent modification of system files (IPS) [AC15]
<input type="checkbox"/>	Prevent registration of new Browser Helper Objects [AC16]
<input type="checkbox"/>	Prevent registration of new Toolbars (IPS) [AC17]
<input type="checkbox"/>	Prevent SEP services from being stopped [AC18]



- Upgraded Default Policies Tuned for Today's Threat Landscape
- New ICMP Trigger for Location Awareness

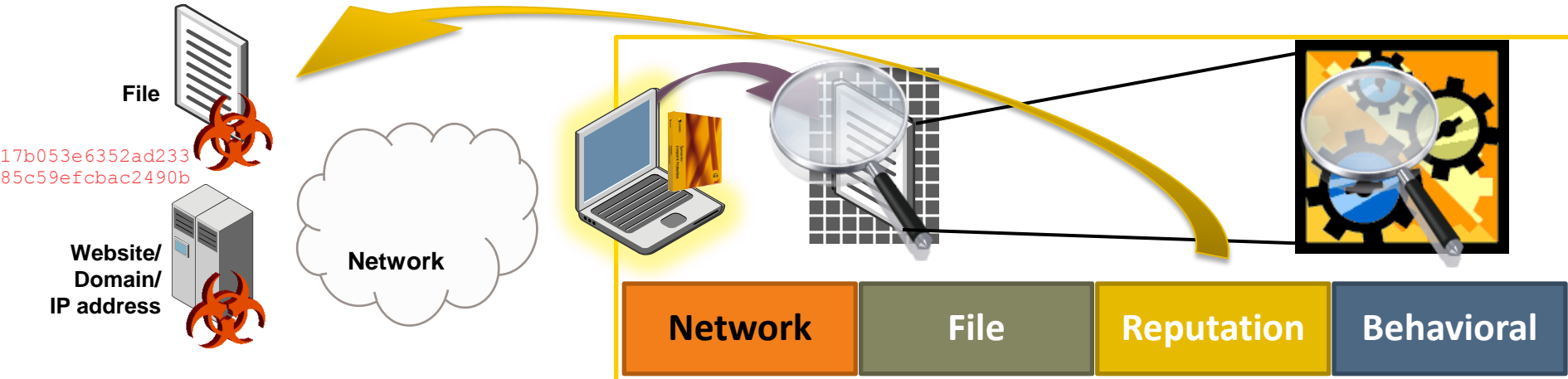




Unrivaled  
Security

# Symantec Endpoint Protection Model

## Defense in Depth



### 1 Network-based Protection

Stops malware as it travels over the network and tries to take up residence on a system

- Protocol aware IPS
- Browser Protection

### 2 File-based Protection

Looks for and eradicates malware that has already taken up residence on a system

- Antivirus Engine
- Auto Protect
- Malheur

### 3 Reputation-based Protection

Establishes information about entities e.g. websites, files, IP addresses to be used in effective security

- Insight
- Domain Reputation
- File Reputation

### 4 Behavioral-based Protection

Looks at processes as they execute and uses malicious behaviors to indicate the presence of malware

- SONAR
- Behavioral Signatures

## Results in the Field

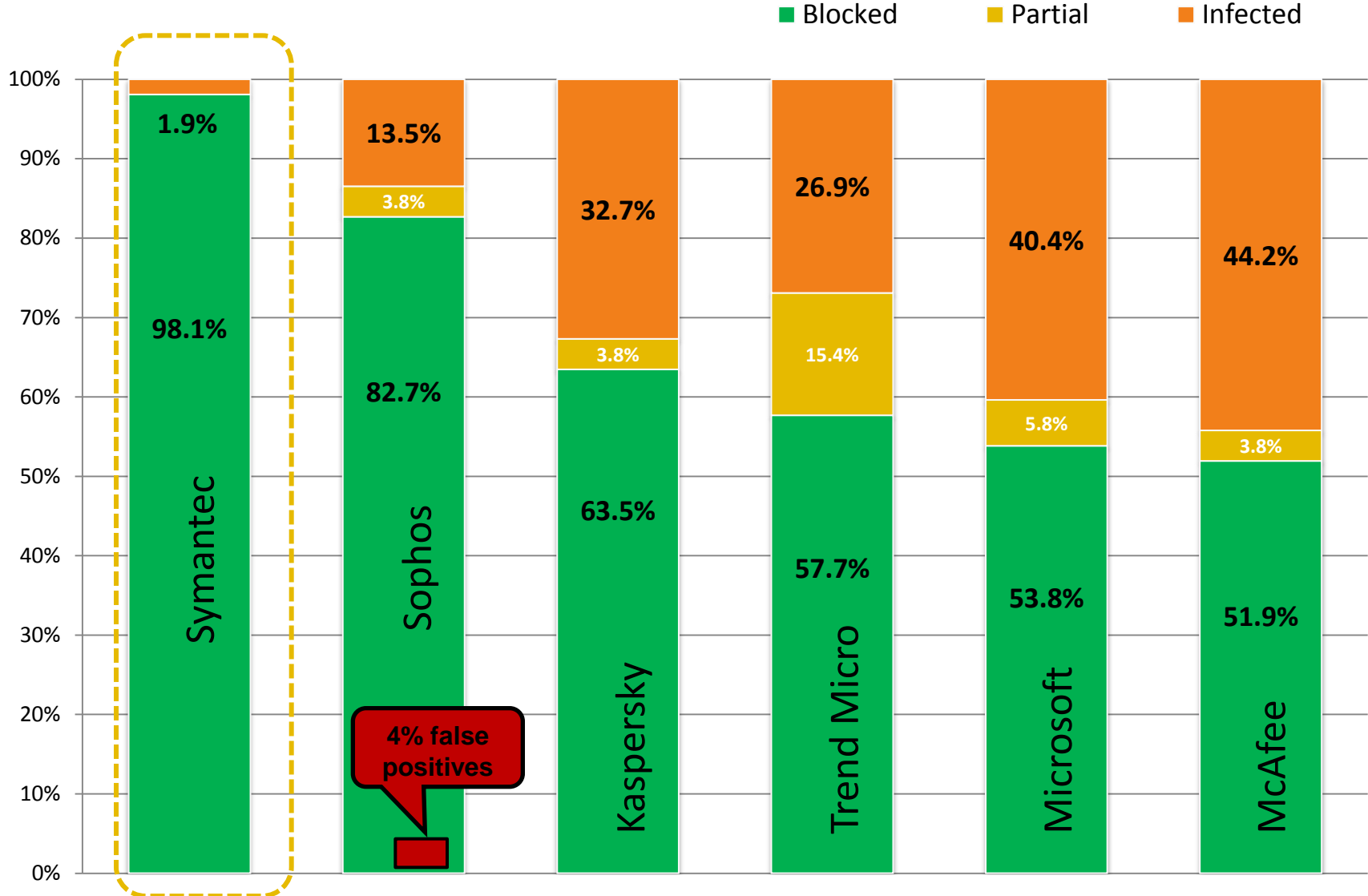


	Blocked June 2010	Blocked Since Launch
Standalone Reputation	1.17M	6.7M
Heuristics + Reputation	192,000	2.2M
Behavior + Reputation	1.29M	14.6M
Reputation Behavior +	2.65M	23.5M

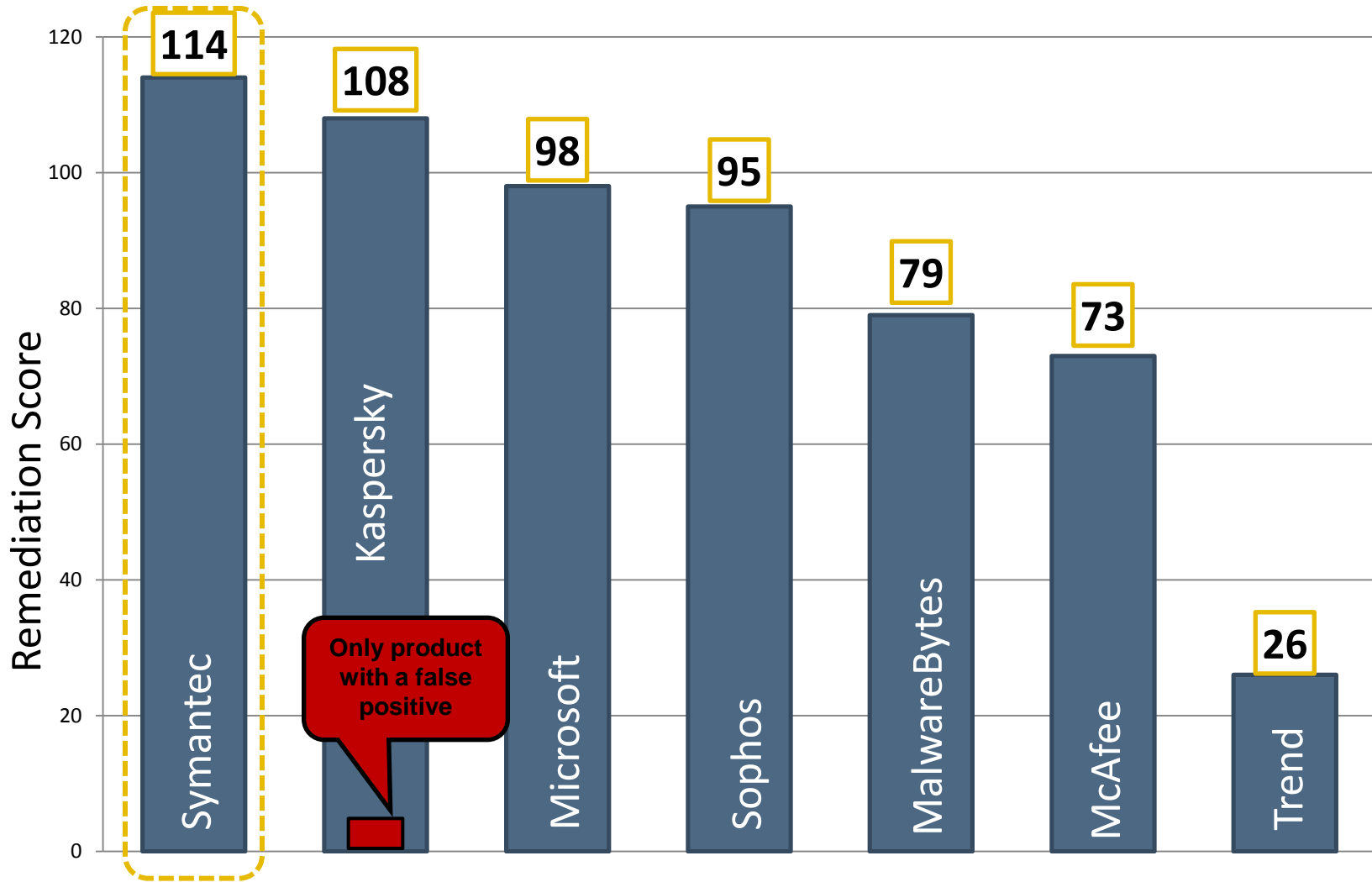
**And this is just the beginning!**



# More Effective in Real World Test



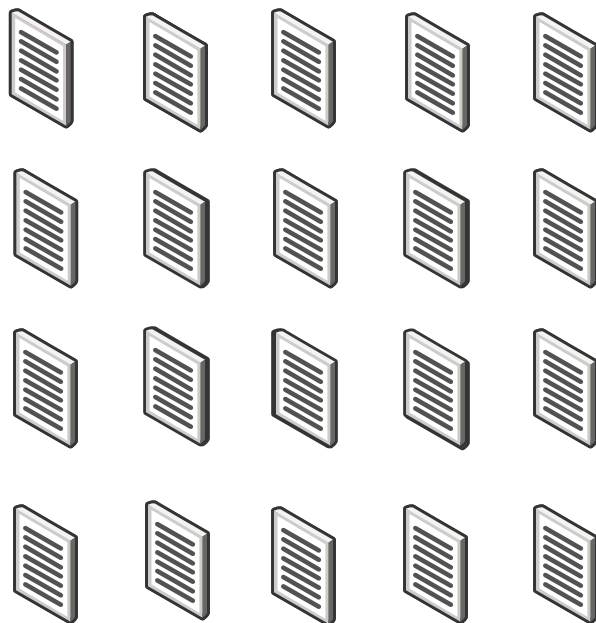
# More Effective in Remediation



# Blazing Performance with Reputation Optimized Scanning



Blazing  
Performance



## Traditional Scanning

Has to scan every file



On a typical system, 80% of active  
applications can be skipped!



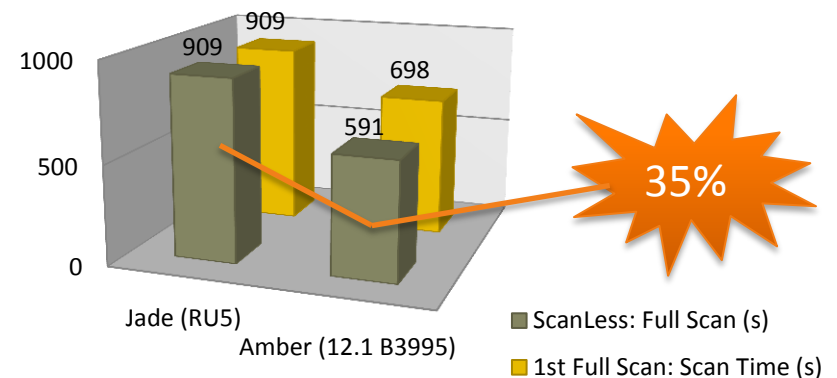
## Reputation- Optimized Scanning

Skips any file we are sure is good,  
leading to much faster scan times

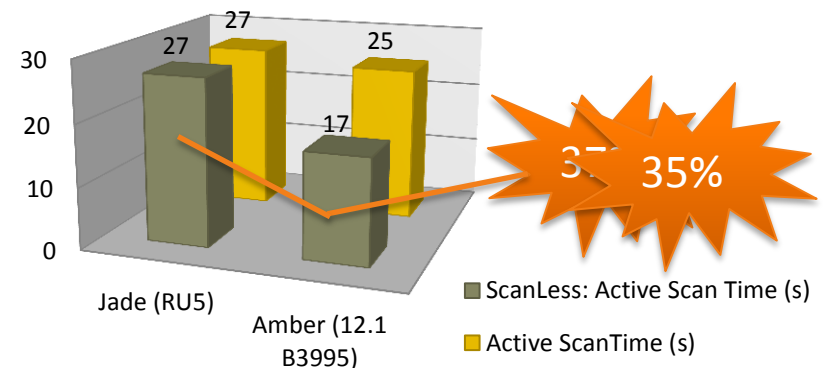
# Benefits of ScanLess

- Faster: SEP 12.1 1<sup>st</sup> scans are 15% faster than that of SEP 11.0 RU5
- Faster: Subsequent scans shows amazing improvement with ScanLess enabled

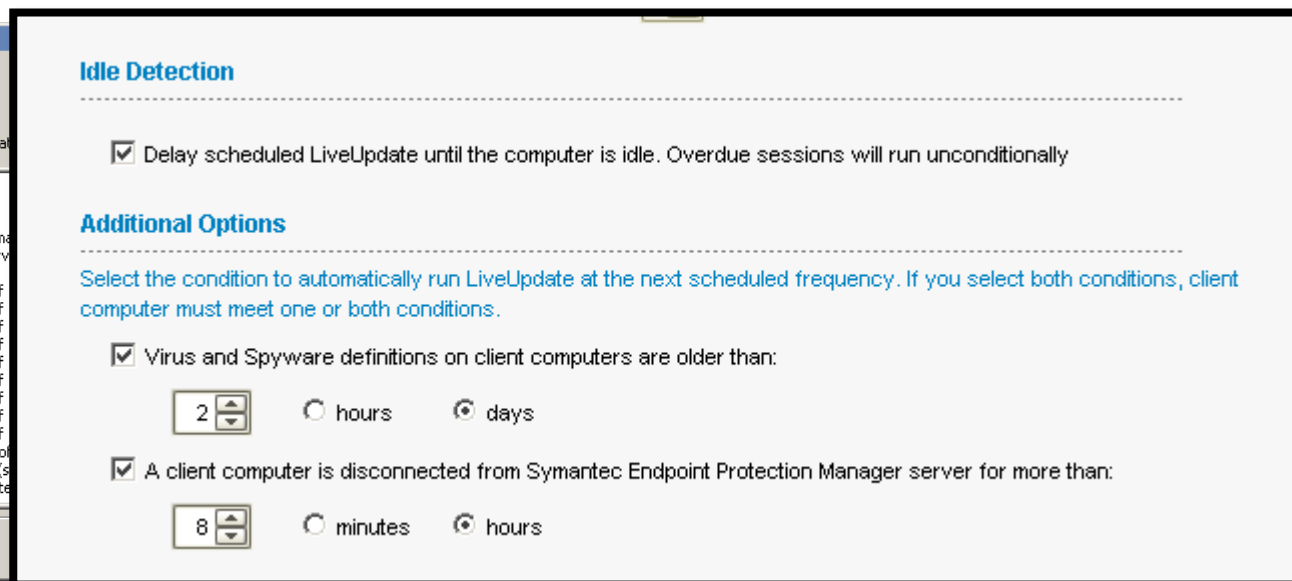
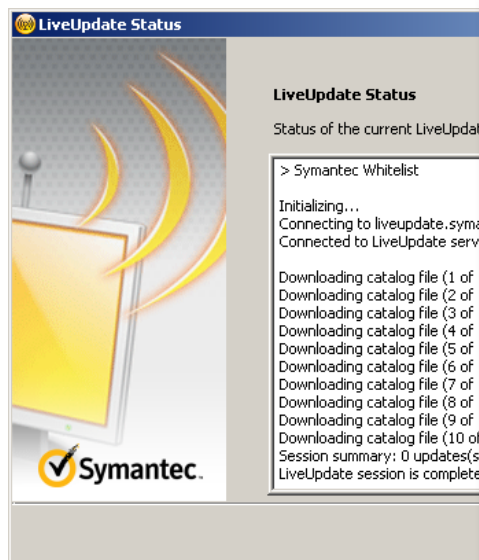
## Full Scan of SEP 12.1 vs 11.0 RU5



## ActiveScan SEP 12.1 vs 11.0 RU5



# Improved LiveUpdate



	Size (MB)	Time (s)	CPU (%)	Write Count
12.1 b3860	1	29	40	28
11.0 RU5	1	82	43	538

12.1 content was the same size  
 12.1 update time was 65% faster  
 12.1 CPU usage was 7% lower  
 12.1 disk writes were 95% less

# Results:

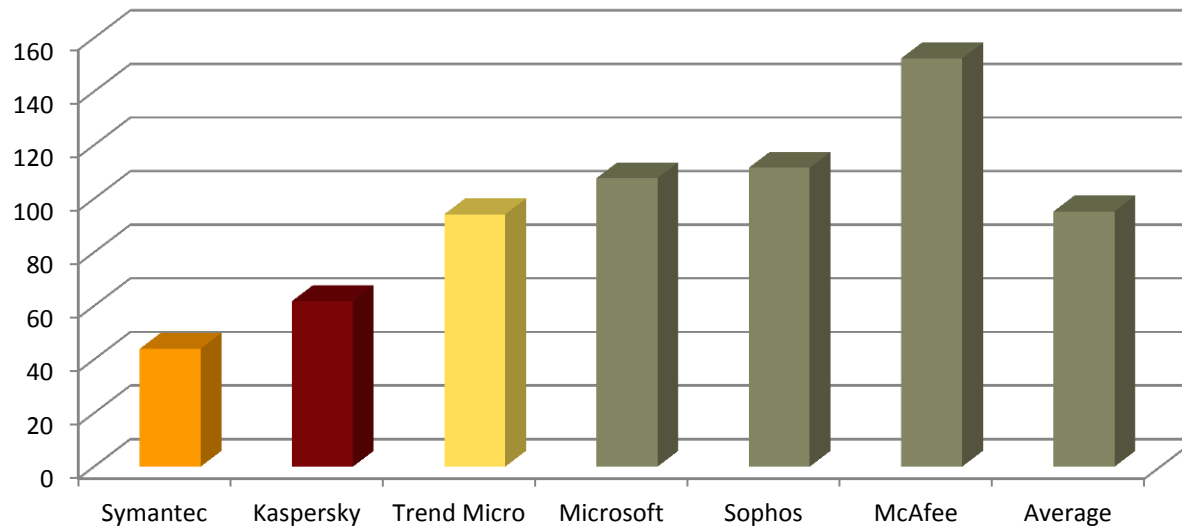
Symantec Endpoint Protection Scans:

3.5X faster than McAfee

2X faster than Microsoft



**Ranked 1<sup>st</sup> in overall Performance!**

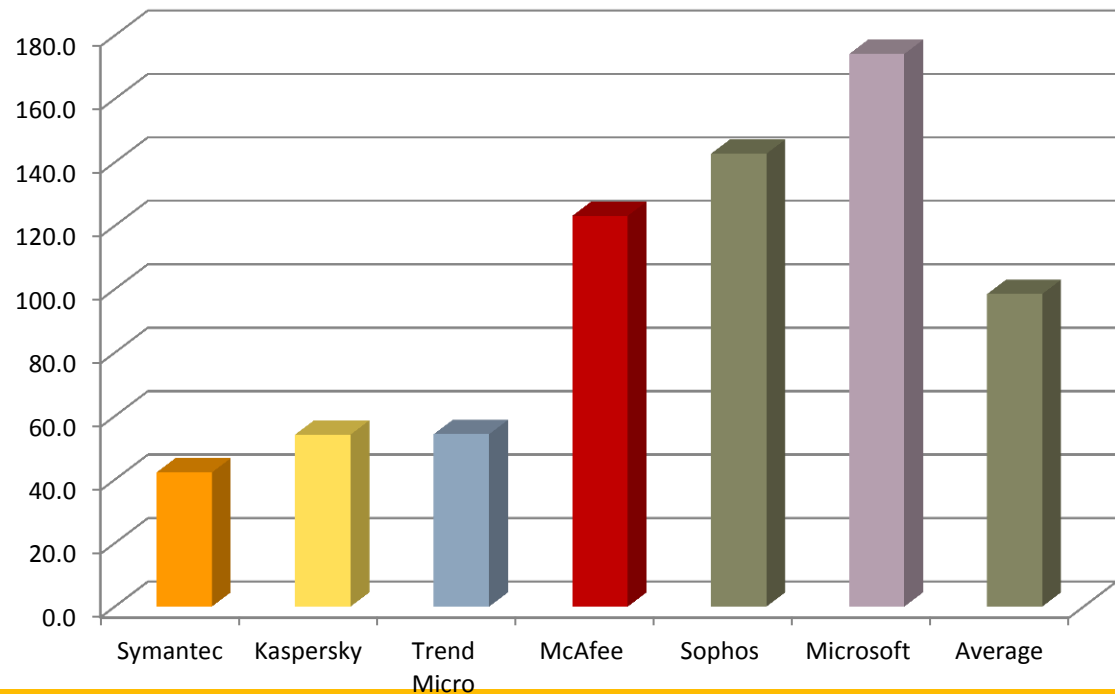


PassMark™ Software, Feb., 2011 - <http://www.passmark.com/AVReport>

# Results:



**Memory Usage**



PassMark™ Software, Feb., 2011 - <http://www.passmark.com/AVReport>

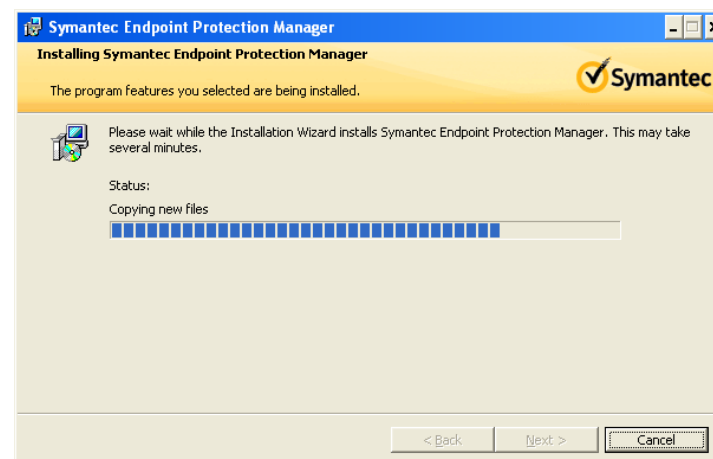
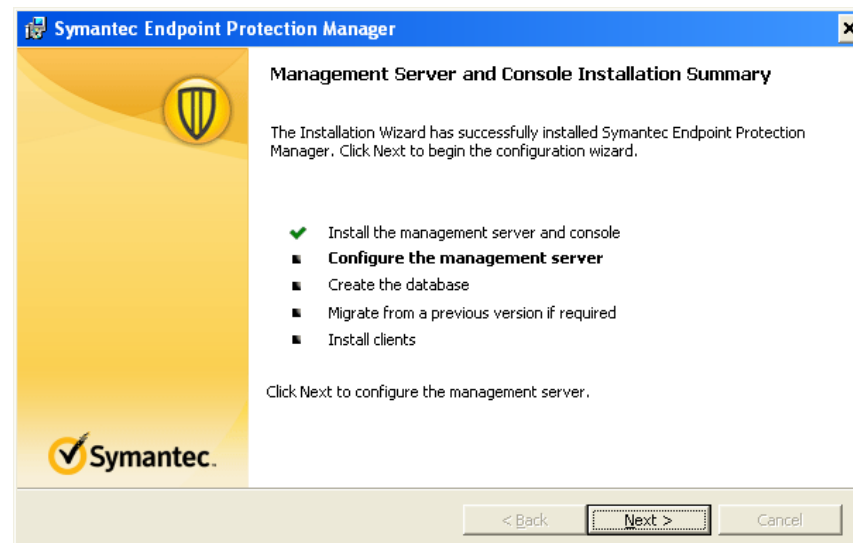
Symantec Endpoint Protection uses:  
66% less memory than McAfee  
76% less memory than Microsoft



Blazing  
Performance

# Simple Management Server Installation

- Limited user input required
- Installs in minutes
- Reduced product dependencies for streamlined installation
  - No dependencies on IIS
  - Built-in or remote database
  - Built-in web server
  - Built-in Java runtime
- Increased platform support for better compatibility
  - Windows XP, 2003, 2008, 7







Blazing  
Performance

# Client Deployment Wizard

The screenshot shows two overlapping windows from the Symantec Client Deployment Wizard. The top window, titled 'Client Deployment Wizard', is in the 'Remote Push' step. It shows a sidebar with options: 'Web Link and Email', 'Remote Push' (selected), 'Preparing for...', and 'Save Package'. The main area is titled 'Select Group and Protection Types' and shows 'Available Packages' with a dropdown menu set to 'Windows - Symantec Endpoint Protection version 12.1.204.3950'. Below this, it lists 'This selection includes: WIN64BIT: Windows - Symantec Endpoint Protection version 12.1.204.3950 (2011-01-06)' and 'WIN32BIT: Windows - Symantec Endpoint Protection version 12.1.204.3950 (2011-01-06)'. The 'Group' is set to 'My Company\Default Group'. The bottom window, titled 'Reporting - Deployment Report', shows a 'Symantec Endpoint Protection' report generated on 01/14/2011 13:05:36. It includes a 'Deployment Report' section with a table showing installation status and a 'Deployment Details' section with a table showing deployment status for a specific computer.

Deployment Report	
Installed, restart needed (0)	
Successfully installed (1)	
Rollbacks (0)	
Incompatible operating system (0)	
Errors (0)	

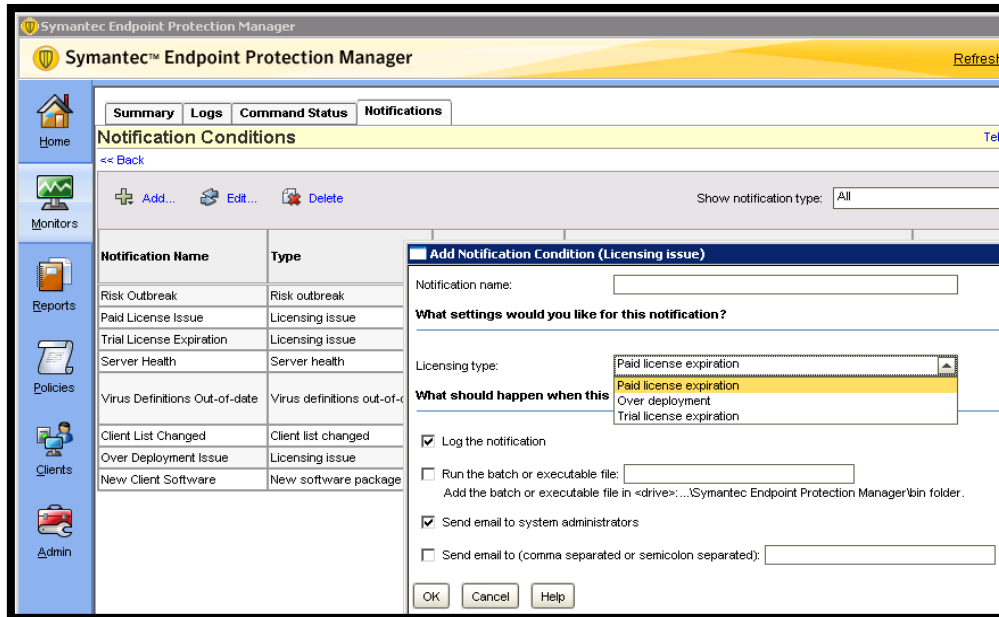
Deployment Details	
<input checked="" type="checkbox"/> Installed, restart needed	
<input checked="" type="checkbox"/> Successfully installed	
<input type="checkbox"/> Rollbacks	
<input type="checkbox"/> Incompatible operating system	
<input type="checkbox"/> Errors	

Computer Name	IP Address	User Name	Deployment Status
STZ-VXPS3PRF86	10.180.245.110	Administrator	Install successful.

- Less package management by auto detecting 32bit/64bit clients
- Immediate protection by including latest policies and content into the packages
- Flexible deployment options to meet different requirements of customers:
  - Remote Push
  - Web Link or Email
  - Export for 3rd Party Distribution
- Visibility into deployment status via the client deployment report

# Product Notifications

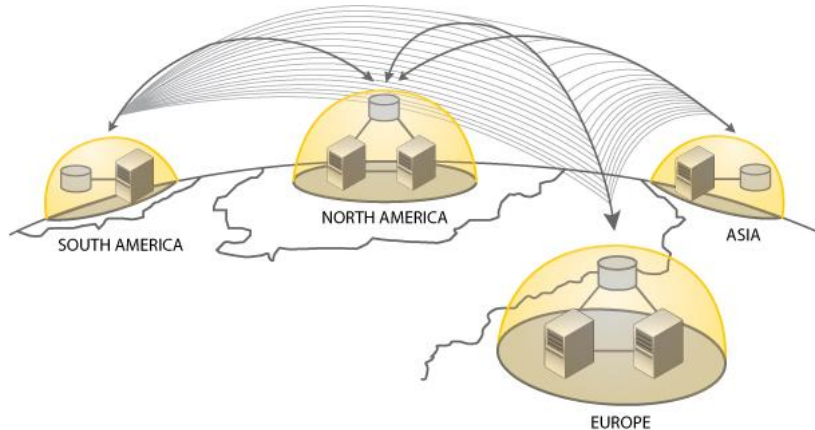


- Mobile friendly notifications
- Built-in notifications:
  - Virus outbreak
  - Clients with out-of-date definitions
  - Licensing
  - Client changes
  - Server Health
  - New software updates
- Automated actions via the execute of scripts for notifications

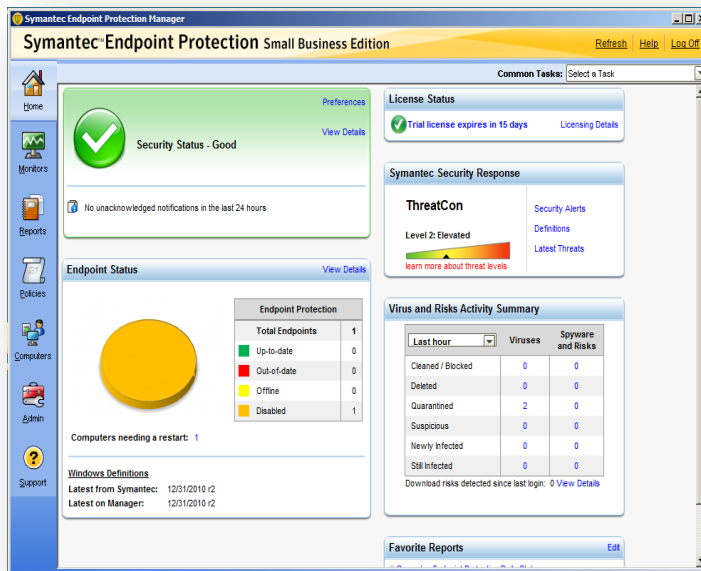


Blazing  
Performance

# Scalable Server Architecture



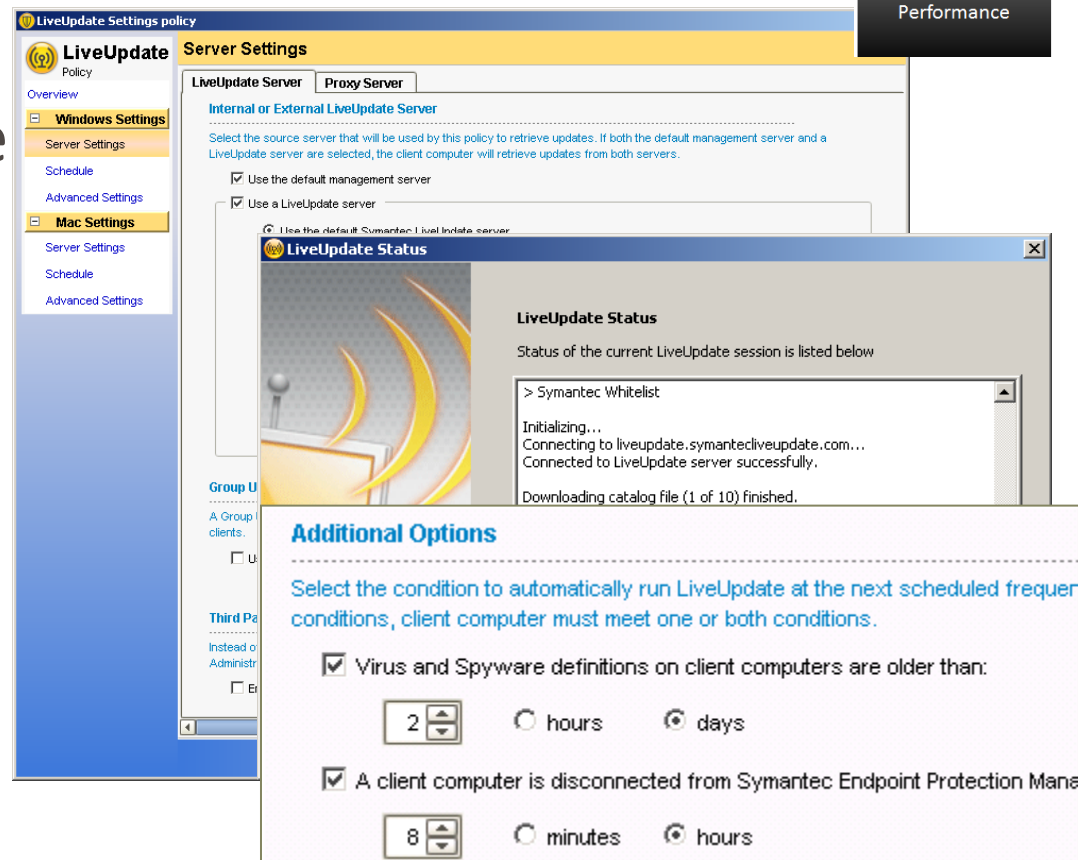
- 80,000 clients per server
- Multi-server architecture for larger client support
- Multi-site architecture to reduced bandwidth by clients
- Fast user interface through efficient database management:
  - Automatic database maintenance
  - Smart database memory caching
- Content distribution via 'delta' files for reduced network traffic





# Improved LiveUpdate

- Improved Performance
- Idle Time Update
- Centrally Configure Proxy Settings
- Separate Mac and Windows LiveUpdate Settings in a Single Policy



Internal Testing

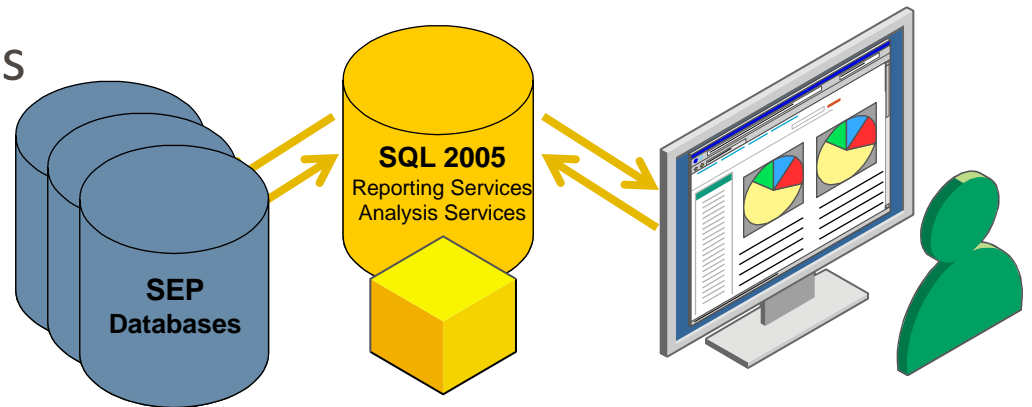
	Size (MB)	Time (s)	CPU (%)	Write Count
12.1 b3860	1	29	40	28
11.0 RU5	1	82	43	538

12.1 content was the same size  
12.1 update time was 65% faster  
12.1 CPU usage was 7% lower  
12.1 disk writes were 95% less

# Powerful Reporting

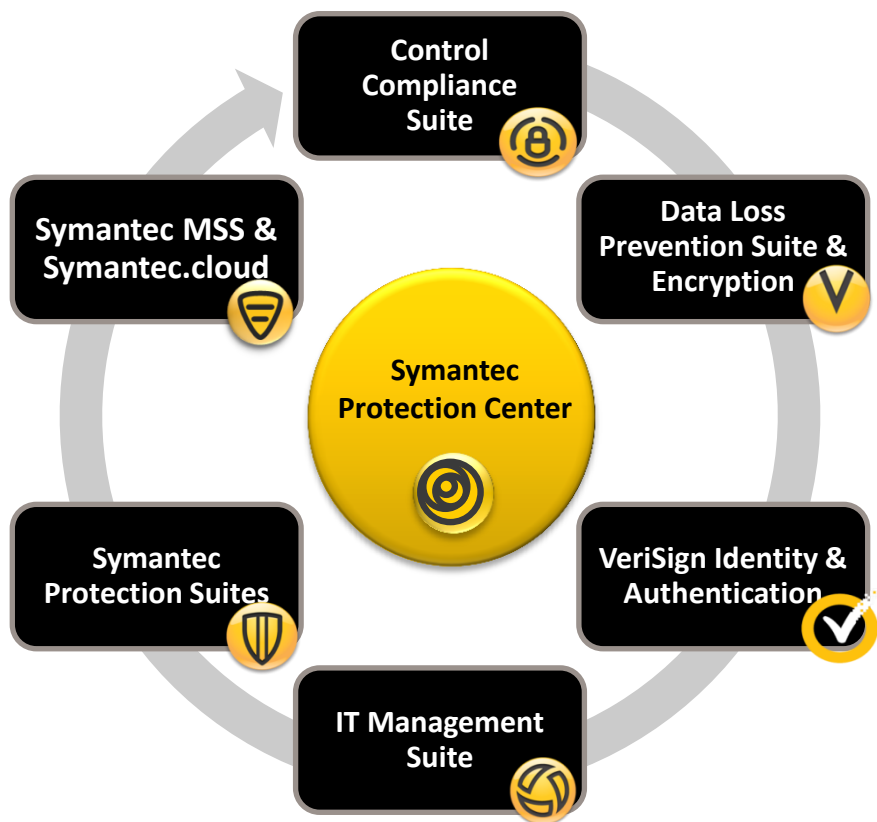
## Advanced Reporting & Analysis with IT Analytics™

- Advanced ad-hoc data-mining
- Graphical dashboards and easy reporting
- Leverages OLAP Cubes for reporting & multi-dimensional data exploration
- User friendly custom reports
- Export to multiple formats
- Pivot tables and charts



# Integration into Symantec Protection Center

## Central Management Console



### Intelligence

Identify emerging threats across local and global environments

### Priority

Prioritize tasks based on role, context and severity

### Action

Accelerate time to protection with relevant, actionable intelligence

VMITAVISION Symantec Management Console - Windows Internet Explorer

http://localhost/Altiris/Console/

Favorites VMITAVISION Symantec Ma... Suggested Sites Get More Add-ons

VMITAVISION Symantec Management Console

Symantec Management Console Home Manage Actions Reports Settings Help

Symantec

Open Save Delete New KPI Table Chart

### Symantec Endpoint Protection Exception Policies Cube

Drop Filter Fields Here

Drop Column Fields Here

Drop Row Fields Here

Drop Totals or Detail Fields Here

This cube was last processed: 4/27/2011 9:49 PM

- Software License Compliance Cube
- Software Purchases Cube
- SQL Servers Cube
- Symantec Endpoint Protection Access Rights Cube
- Symantec Endpoint Protection Agent Behavior Events Cube
- Symantec Endpoint Protection Agent Security Events Cube
- Symantec Endpoint Protection Agent System Events Cube
- Symantec Endpoint Protection Agent Traffic Events Cube
- Symantec Endpoint Protection Alerts Cube
- Symantec Endpoint Protection AntiVirus Policies Cube
- Symantec Endpoint Protection Application and Device Control
- Symantec Endpoint Protection Clients Cube
- Symantec Endpoint Protection Exception Policies Cube**
- Symantec Endpoint Protection Firewall Policies Cube
- Symantec Endpoint Protection Host Integrity Events Cube
- Symantec Endpoint Protection Host Integrity Policies Cube
- Symantec Endpoint Protection Insight Detections Cube
- Symantec Endpoint Protection Intrusion Prevention Policies C
- Symantec Endpoint Protection LiveUpdate Policies Cube
- Symantec Endpoint Protection Policies Cube
- Symantec Endpoint Protection Scans Cube
- Symantec Endpoint Protection Server Admin Events Cube
- Symantec Endpoint Protection Server System Events Cube
- Symantec Endpoint Protection SONAR Detections Cube
- Tasks Cube






















Dashboards

Done
























Local intranet | Protected Mode: Off 100%

# ITA – Reports and Dashboards

## Dashboards

-  Altiris Agent Dashboard
-  Asset Control Dashboard
-  Computer Inventory Dashboard
-  DLP Incident Dashboard
-  Event Console Alerts Dashboard
-  IT Analytics Usage Dashboard
-  Monitor Alerts Dashboard
-  Patch Management Dashboard
-  ServiceDesk Change Trend Dashboard
-  ServiceDesk Incident Trend Dashboard
-  ServiceDesk Problem Trend Dashboard
-  Software Compliance Dashboard
-  Software Delivery Dashboard
-  Software Installs Dashboard
-  Symantec Endpoint Protection Client Dashboard
-  Symantec Endpoint Protection Host Integrity Event Dashboard
-  Symantec Endpoint Protection Insight Detection Dashboard
-  Symantec Endpoint Protection Risk Dashboard
-  Symantec Endpoint Protection SONAR Detection Dashboard
-  Vista Readiness Dashboard
-  Windows 7 Readiness Dashboard

## Reports

-  Add Remove Programs
-  Application Metering
-  Asset
-  Computer
-  Data Loss Prevention
-  Event Console
-  Installed Files
-  IT Analytics Events
-  Monitor
-  Patch Management
-  ServiceDesk
-  Software Delivery
-  Software License
-  Symantec Endpoint Protection
  -  Client Version Details
  -  Host Integrity Event Details
  -  Insight Detection Details
  -  Intrusion Prevention Signature Details
  -  Scan Trend
  -  SONAR Detection Details
  -  Virus Alert Details
  -  Virus Alert Trend
  -  Virus Definition Distribution Details



# The Problem

## Virtualization brings new challenges

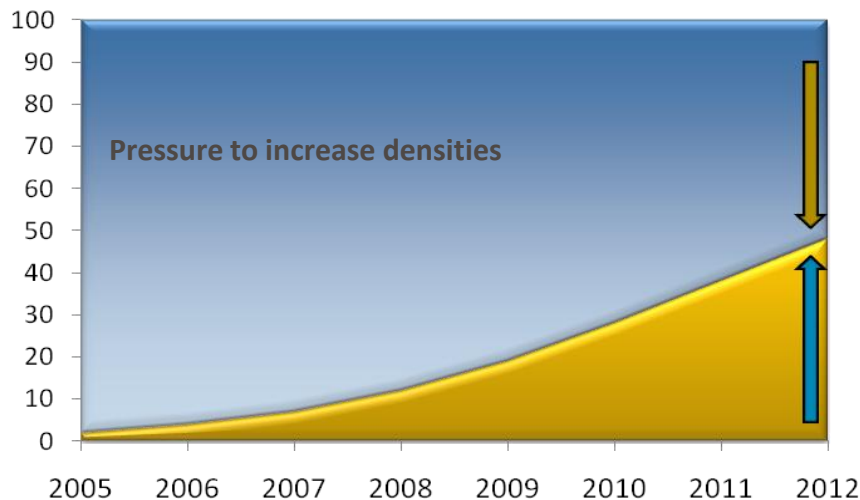
2009: 7m physical servers  
7m+ virtual servers



Gartner:

60% of production VM's will be  
less secure than their physical  
counterparts

The Scan Storm



### • Virtualization solves problems

- Flexibility
- Deployment of new systems
- Energy
- Space
- Improved Management

# Virtualization Features

Virtual Client  
Tagging

Virtual Image  
Exception

Shared Insight  
Cache

Offline Image  
Scanning

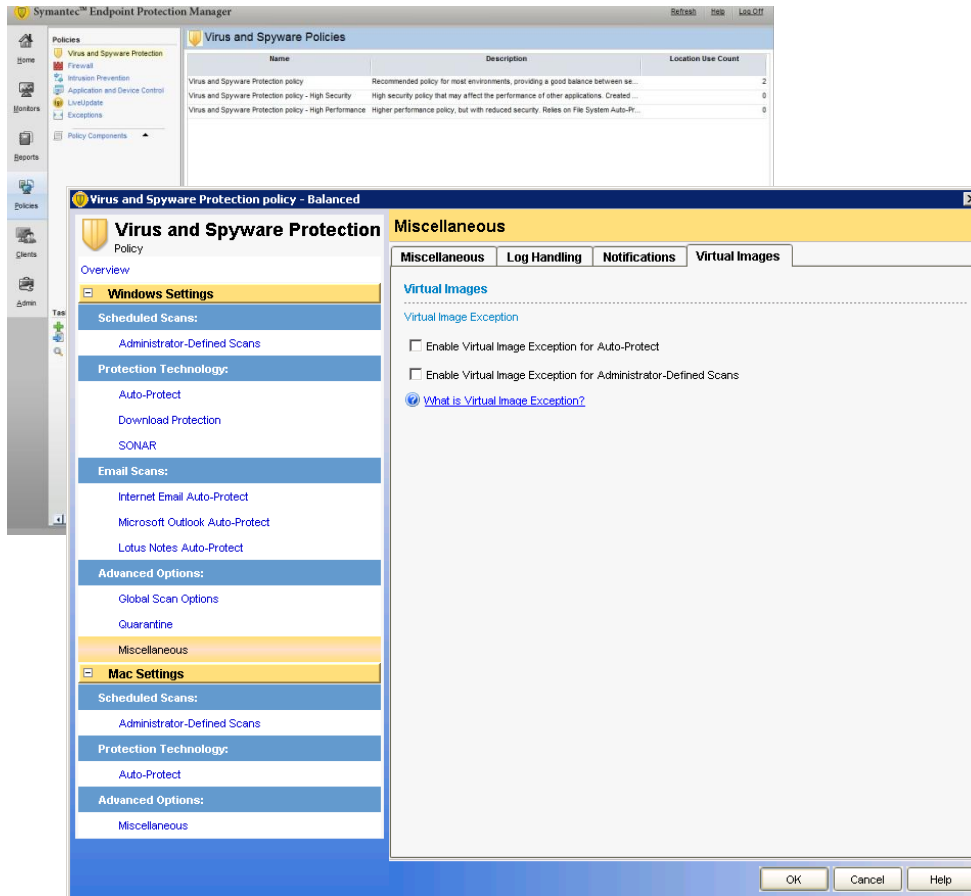
Resource  
Leveling

**Together – up to 90% reduction in disk IO**

# Virtual Image Exception – Avoids Unnecessary Scanning

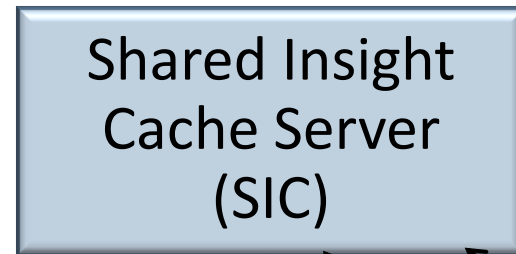


Built for Virtual  
Environments



- Set exclusions for files in virtual environments
- Ability to turn on and off Image Exceptions
- Options for silent and automated operation

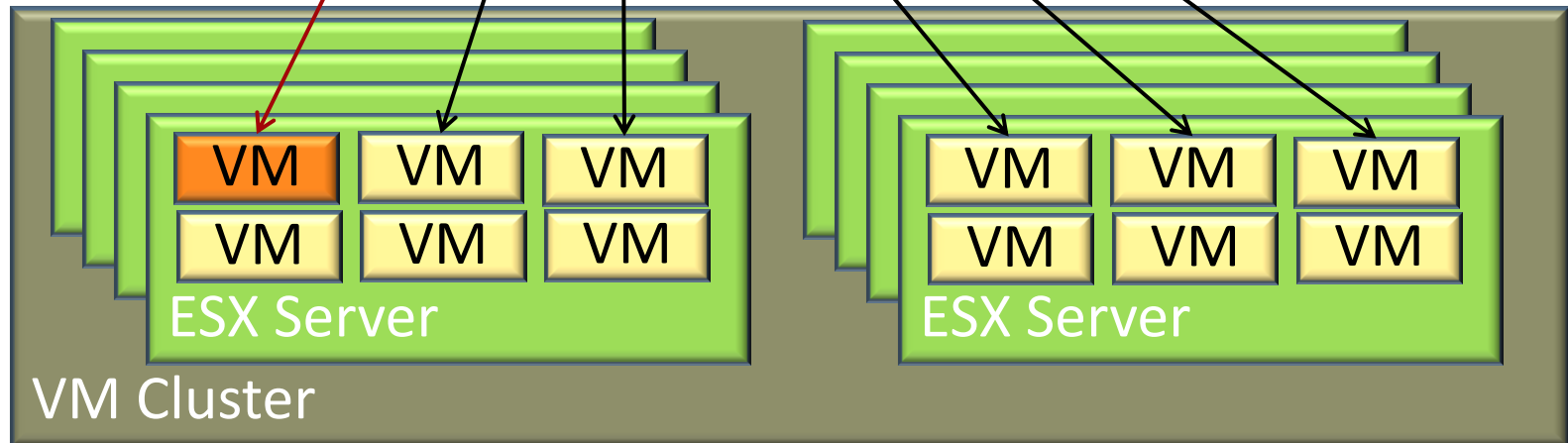
# Shared Insight Cache - High Level



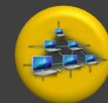
File Hash	Def Ver	Result
AE32D...	2011.1...	Clean
B923E...	2011.1...	Clean
F9123...	2011.1...	Clean
C3FDA...	2010.2...	Clean

First SEP client needs to scan a file.  
Queries SIC and finds no record.  
SEP scans the file and sends the  
results to the SIC.

Subsequent SEP clients need to scan the same file. They  
query the cache server and find the file has already been  
scanned with the same version of defs and the file is clean.  
SEP client skips scanning the file.



# Virtual Client Tagging – Simplifies Endpoint Management



Built for Virtual  
Environments

The screenshot shows the 'Edit Properties for rz-win7-test' window with the 'Search Clients' tab active. The 'Query' section has 'Find' set to 'Computers' and 'In Group' set to 'My Company\Default Group'. The 'Search Criteria' table is as follows:

Search Field	Comparison Operator	Value
Virtualization Platform		N/A
		N/A
		VMware
		Microsoft
		Citrix

The 'Query Results' section shows a table with the following data:

Name	Operating System	Domain	Description

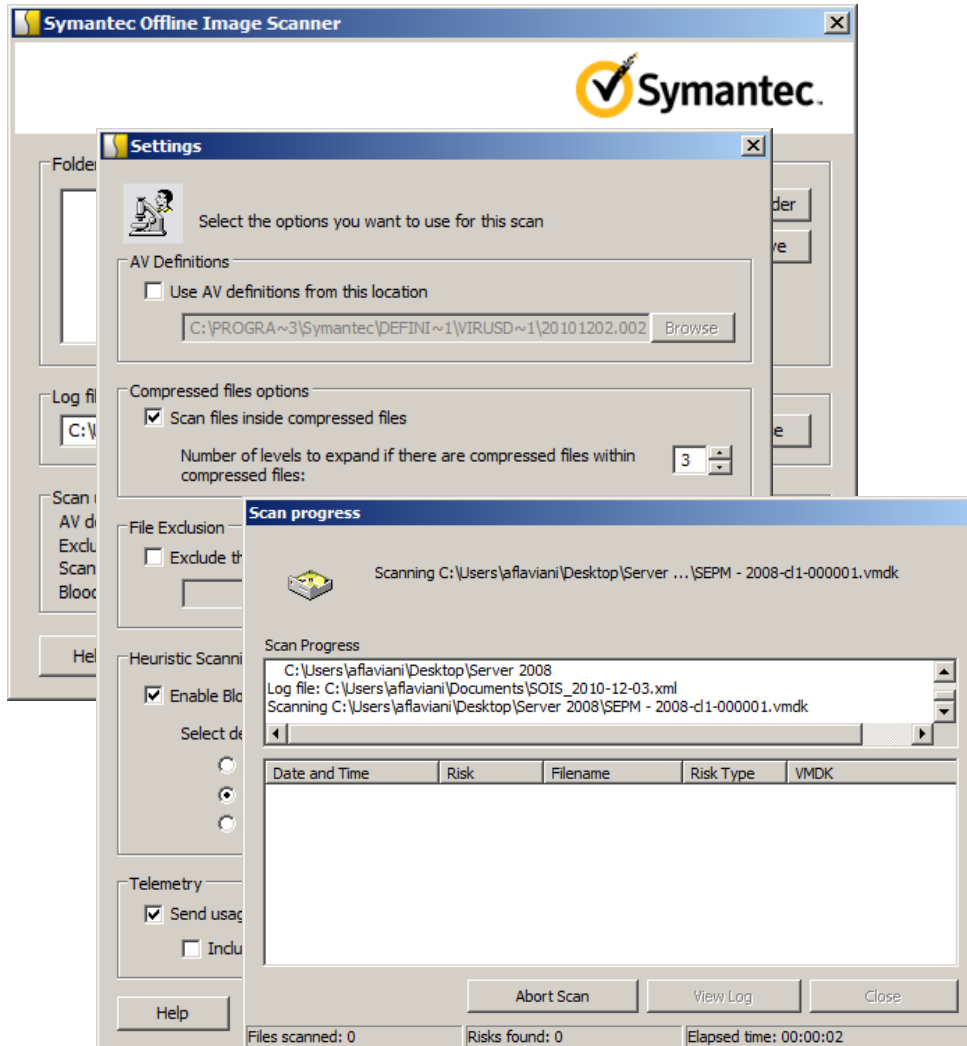
The 'Virtualization Platform' field in the 'Deployment status' section is set to 'VMware'.

- Ability to determine if the client is running in a Virtual Environment
- The tagging is built into the SEP client
- Works with VMware ESX/i, Microsoft Hyper-V, Citrix Xen
- Client runs the check and reports the information back to the manager
- Virtual Environment Status is in reports, client properties and is searchable

# Offline Image Scanner – Detects Malware in VM Images



Built for Virtual  
Environments



- Avoids spinning up virtual machines with latent infections
- No dependency on other Symantec solutions (beyond AV definitions)
- Doesn't require a traditional install
- Able to scan FAT32 and NTFS file-systems in the guest OS
- Options for silent and automated operation
- Detailed logging/reporting capabilities



Built for Virtual  
Environments

# Scan Randomization - Prevents AV Storms

- Choose when scheduled scans will run:
  - Daily – up to 23 hours
  - Weekly – up to 167 hours
  - Monthly – up to 671 Hours
- Minimizes concurrent scans across entire pools of virtual machines

**Edit Scheduled Scan**

**Scan Details** | **Schedule** | **Actions** | **Notifications**

**Scanning Schedule**

Specify how often the scan should run.

Scan: ☐ Daily ☐ Weekly ☒ Monthly

At: 02 : 00 PM

On day: 1

**Scan Duration**

☐ Scan until finished (recommended to optimize scan performance)

☒ Scan for up to: 671 hours

☒ Randomize scan start time within this period (recommended in VMs)

**Retry Scheduled Scans**

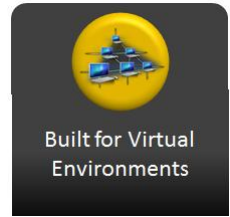
Specify the retry interval in case the computer is off or unable to start the scan at the scheduled time.

☐ Retry the scan within: 11 days

OK Cancel Help

# The Result:

## SEP 12.1 Performance Expectations



	Full Scan IO performance improvement
12.1 vs. 11	60% reduction in total disk IO
12.1 Shared Insight Cache vs. 12.1 without	50-80% reduction in total disk IO*
12.1 with Virtual Image Exception vs. 12.1 without	50-80% reduction in total disk IO*

\* Expected results, final numbers are still pending

The total benefit to a customer running SEP 12.1 with the virtualization features is an estimated 80%-90% reduction in disk IO for full scans as compared to 11.x.

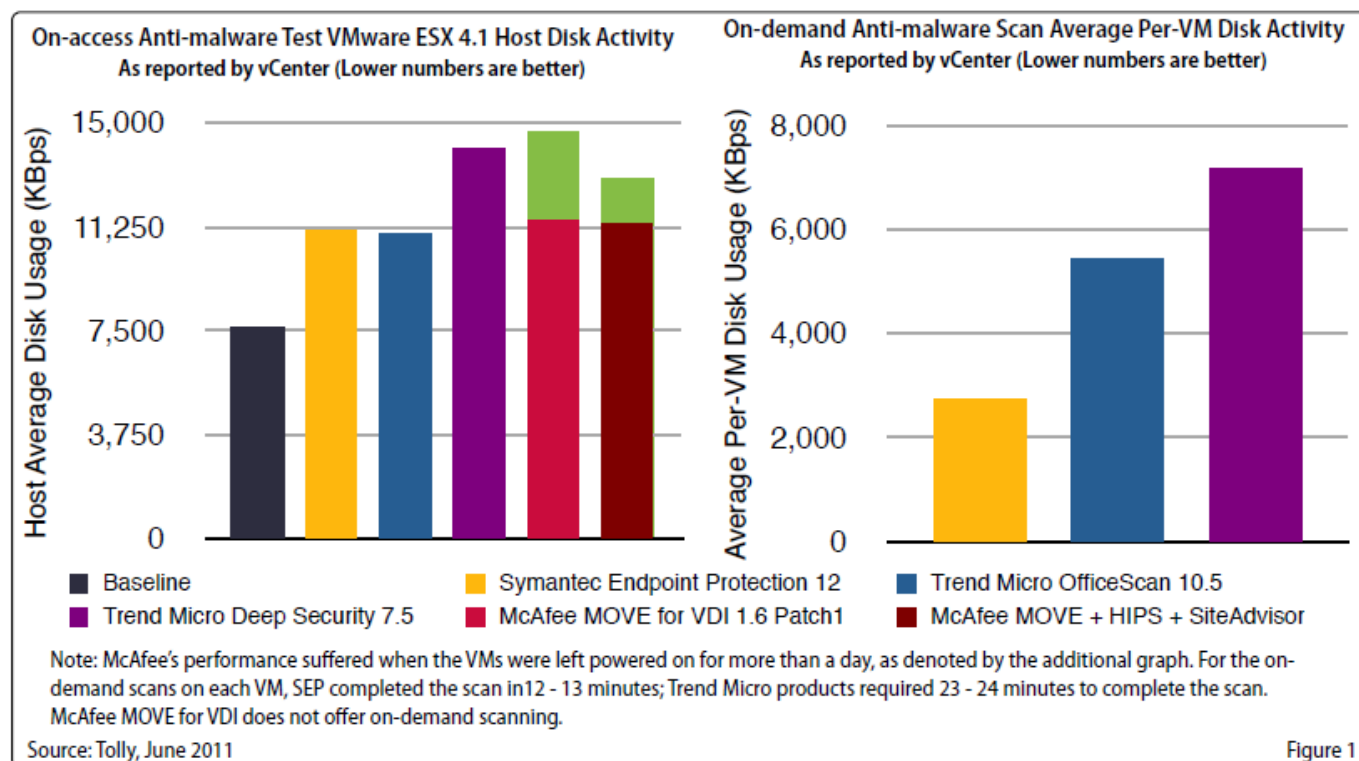


# SEP 12 Performance in Virtual Environments



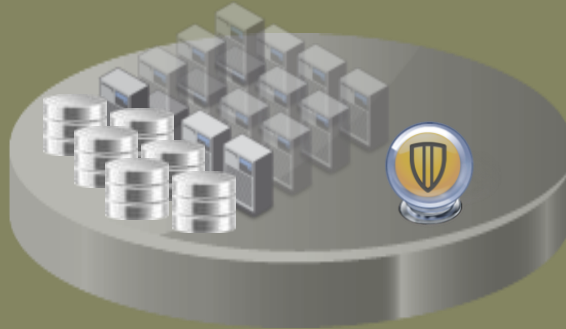
## Results:

- ✓ On-access scan: 20% less disk bandwidth compared to Trend Micro's agentless DeepSecurity
- ✓ On-demand scan: 50% less time, 49% less disk bandwidth



# Virtualization Summary:

## SEP 12 Delivers What Matters



- Full Security
- Higher Density
- Avoid “AV-Storms”
- Easier Management
- No Additional Cost
- Hypervisor Agnostic

