TREND MICRO™ | Securing Your Web World

Deep Security

Total Protection for Datacenter and e-commerce

Khoi Ngo

Country Sales Manager, Vietnam & Cambodia

vmware PARTNER TECHNOLOGY ALLIANCE

About Trend Micro

A global cloud security leader that creates a world safe for businesses and consumers exchanging digital information, through content security and threat management

EVA CHEN
CEO and Co-Founder

1000+ Threat Experts

TrendLabs

VISION

A world safe for exchanging digital information

MISSION

Innovate to provide the best content security that fits into the IT infrastructure

Founded
United States in 1988

Headquarters
Tokyo, Japan

Employees
5,000

Market
Content Security and Threat Management

Locations
28 Offices Worldwide

$1 Billion Annual Revenue / $1.7 Billion Total Assets

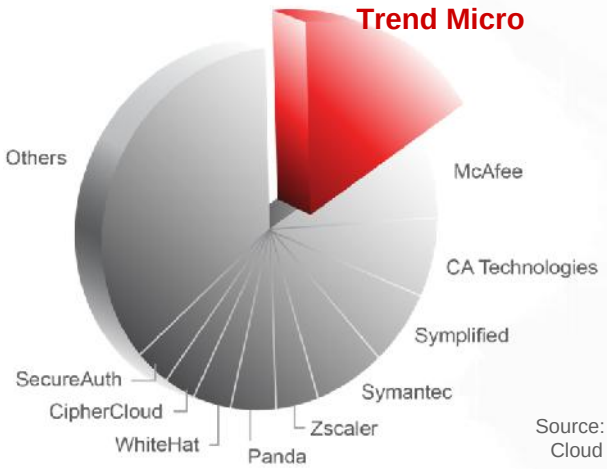
#1 in Virtualization & Corporate Server Security

Top 3 in Messaging, Web and Endpoint Security

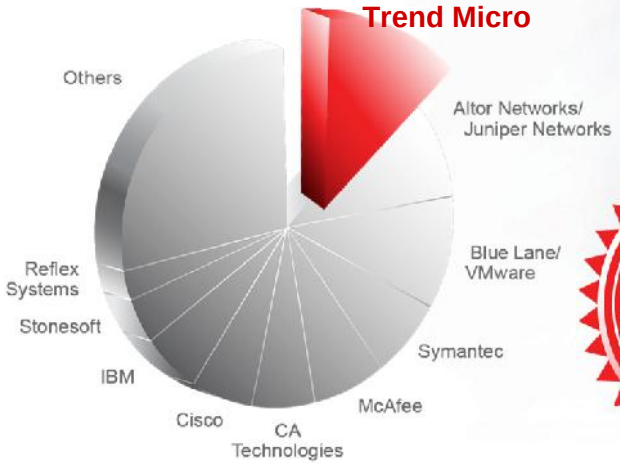
A Leader in Cloud Security

TREND MICRO

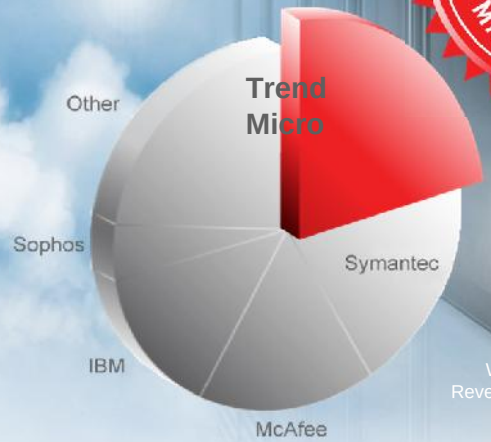
Trend Micro - #1 Market Leader in Securing Your Journey to the Cloud



Source: 2012 Technavio – Global Cloud Security Software Market



Source: 2011 Technavio – Global Virtualization Security Management Solutions



Worldwide Endpoint Security Revenue Share by Vendor, 2010
Source: IDC, 2011

TREND MICRO

Trend Micro Foundation: TrendLabs

TrendLabs helps provide a worldwide platform for delivering timely threat intelligence, service, and support anytime, anywhere.

- More than 1000 threat research and service and support experts at 15 locations
- Collaborative account management
- Automated alerts for new threats
- ISO 9001 2000, BS7799 certifications
- COPC-2000 Standards Certification

➢ Protection requires more than a product…

➢ It requires service—timely and expert service.

TrendLabs
Global Antivirus Research & Support Center

TREND MICRO

Securing Your Journey to the Cloud

Trend Micro and VMware Alliance

History of Security Innovation with VMware

Improves Security

by providing the most secure virtualization infrastructure, with APIs, and certification programs

Improves Virtualization

by providing security solutions architected to fully exploit the VMware platform

2008

- Feb: Join VMsafe program
- RSA: Trend Micro announces Coordinated approach & Virtual pricing And shows Vmsafe demo
- VMworld: Trend Micro virtsec customer

2009

- May: Trend acquires Third Brigade
- RSA: Trend Micro announces virtual appliance
- July: CPVM GA
- Nov: Deep Security 7 with virtual appliance
- Q4: Joined EPSEC vShield Program

2010

- RSA: Trend Micro Demos Agentless
- VMworld: Announce Deep Security 7.5
- Sale of DS 7.5 Before GA
- Dec: Deep Security 7.5 w/ Agentless AntiVirus
- 2010: >100 customers >$1M revenue

2011

- RSA: Other vendors "announce" Agentless
- Q1: VMware buys Deep Security for Internal VDI Use
- Vmworld: Announce Deep Security 8 w/ Agentless FIM

Trend Micro Momentum with vSphere Customers

- VMware-integrated agentless antivirus released in Nov. 2010
  - 1000 agentless security customers in the first year
  - Over 250,000 VMs are licensed for agentless antivirus
- Full agentless Deep Security suite available for vSphere 5
- Latest Agentless File Integrity Monitoring released in 2012
- Largest customer purchase is 8,000 VMs
- Most dense deployment is 300 VMs/host

"Deep Security provides a **robust** set of tools to add to your toolbox.
The perceived **performance** improvement is **visible** to the naked eye."
- Ed Haletky, Virtualization Practice (www.virtualizationpractice.com)

Trusted by Global 500 Companies

- **48 of the top 50 Global Corporations**
- 10 of the top 10 Automotive companies
- 10 of the top 10 Telecom companies
- 8 of the top 10 Banks
- 9 of the top 10 Oil companies

Trust Trend Micro security solutions*

Trend Micro protects **96%** of the top 50 global corporations.

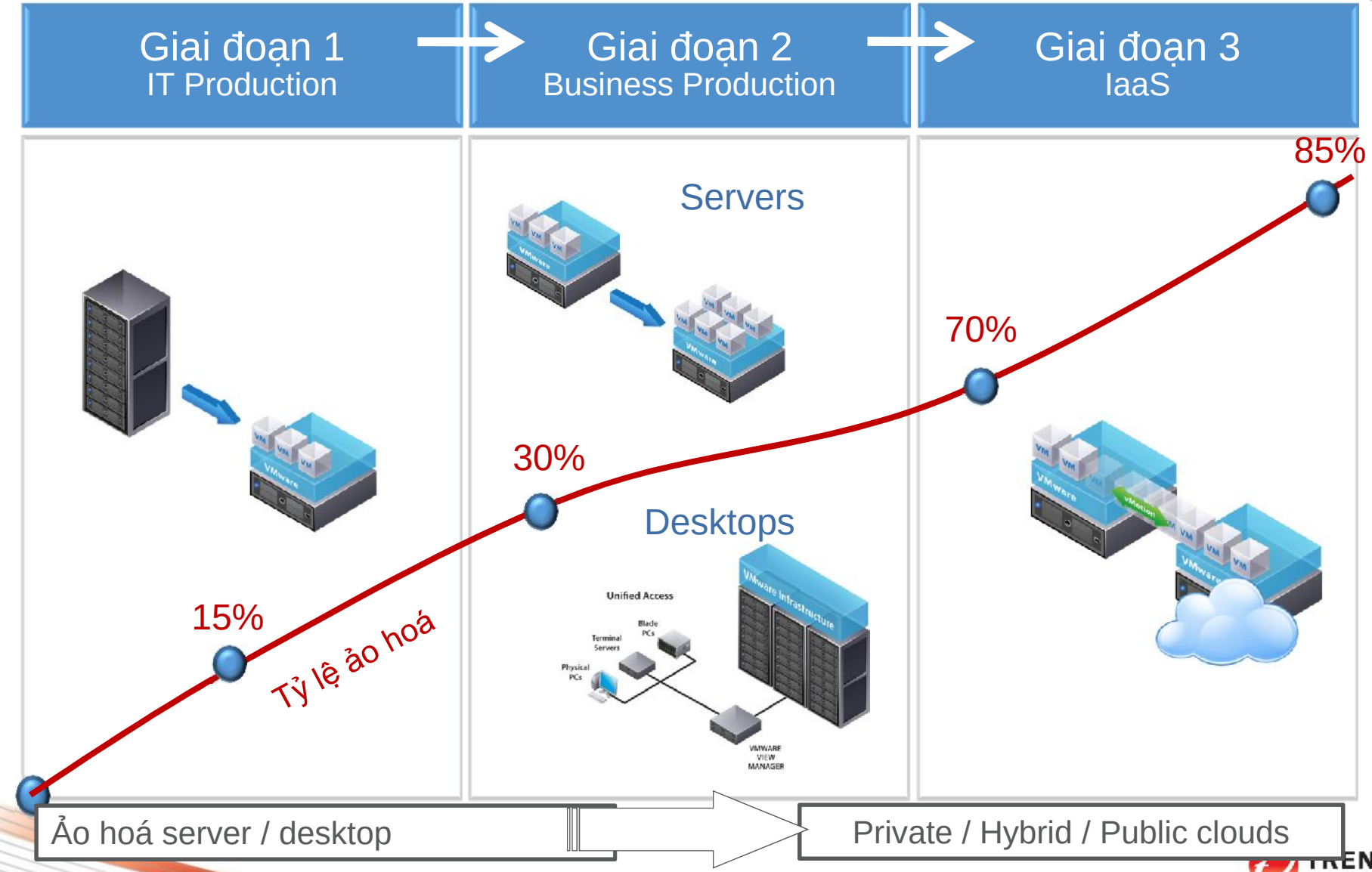
Trend Micro protects **100%** of the top 10 automotive companies.

Trend Micro protects **100%** of the top 10 telecom companies.

Trend Micro protects **80%** of the top 10 banks.

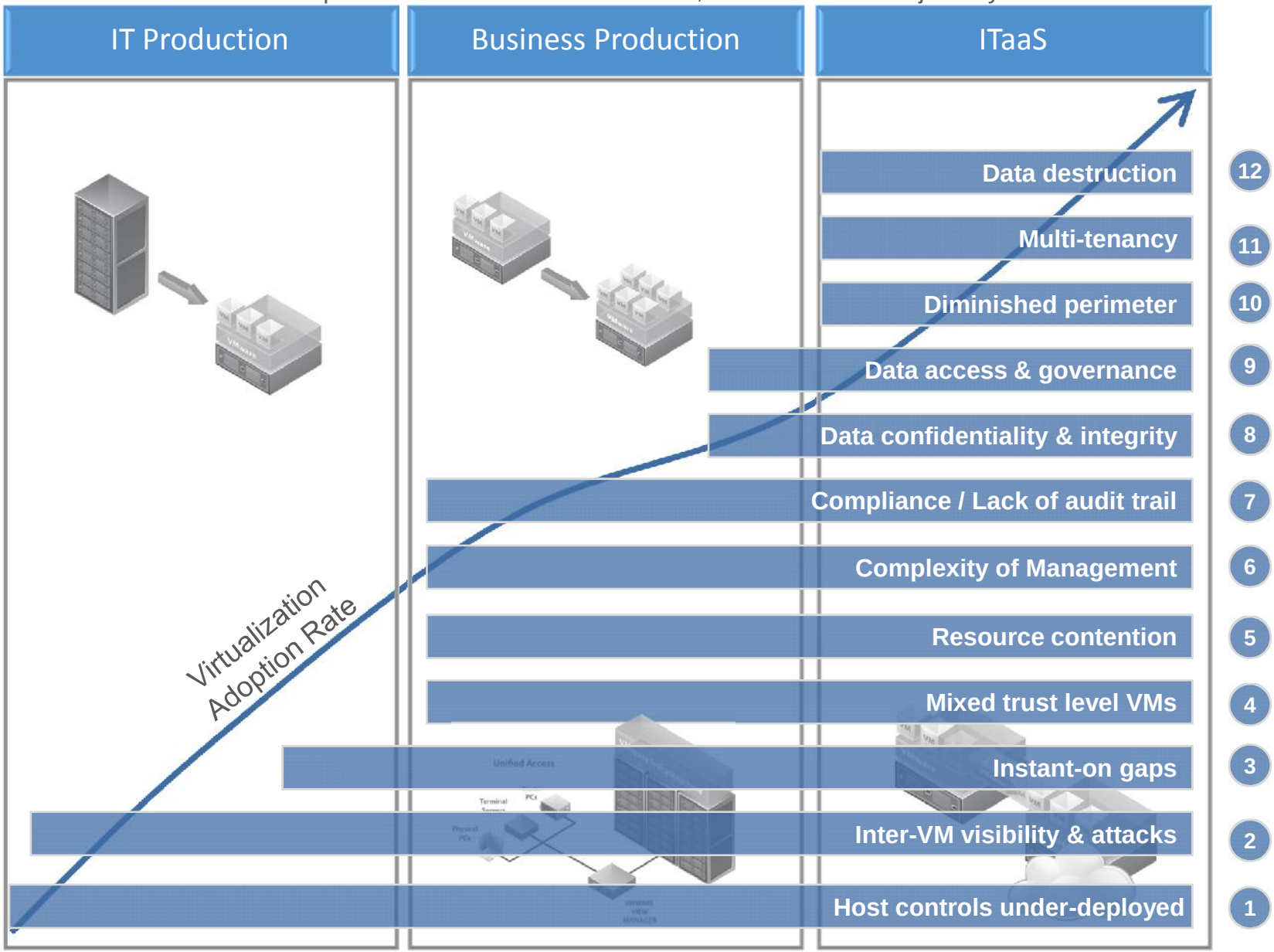
Trend Micro protects **90%** of the top 10 oil companies.

Những giai đoạn của lộ trình ảo hoá lên ĐTĐM



Security challenges in virtualization

VMware and Trend Micro help customers address these issues, and accelerate the journey



Security challenges in virtualization journey

(Explains the security and compliance challenges previously outlined)

1. **Host-based controls under-deployed**
File Integrity Monitoring, host IDS/IPS and anti-malware are often under-deployed, because of cost, complexity or performance.

2. **Inter-VM visibility & attacks**
Traditional network security devices cannot detect or contain malicious inter-VM traffic.

3. **Instant-on gaps**
It's all but impossible to consistently provision security to "instant-on" VMs, and keep it up-to-date. Dormant VMs can eventually deviate so far from the baseline that merely powering them on introduces a massive security hole.

4. **Mixed trust level VMs**
Workloads of different trust levels are likely being consolidated onto a single physical server without sufficient separation..

5. **Resource contention**
Resource-intensive operations (AV storms & pattern-file updates) can quickly result in an extreme load on the system.

6. **Complexity of Management**
Virtualization has led to the proliferation of more virtual machines (VM sprawl) than their physical predecessors, leading to increased complexity in provisioning security agents to each VM, and constantly reconfiguring, patch and rolling out patterns to each VM.

7. **Compliance/Lack of audit trail**
Higher levels of consolidation put greater stress on the ability to ensure compliance, particularly amongst mission critical / Tier 1 applications. As well, virtualization makes it more difficult to maintain audit trails, and understand what, or by whom, changes were made.

8. **Data confidentiality & integrity**
Unencrypted information in cloud environments is subjected to various risks including theft, unauthorized exposure and malicious manipulation

9. **Data access & governance**
RESTful-authentication* in the cloud can be susceptible to brute force and hijacking, attacks allowing unauthorized data access. Breakdown in the separation of duties might allow unauthorized vendor access to data. (* Representational State Transfer)

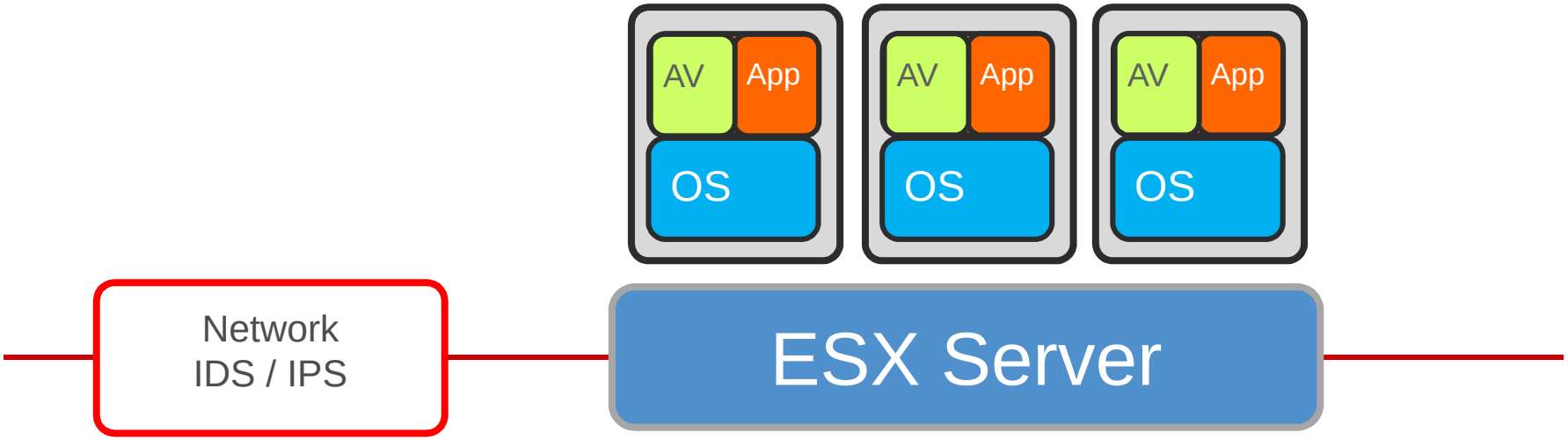
10. **Diminished perimeter**
Security mechanisms are under the cloud service provider's control and perimeter security mechanisms are significantly diminished.

11. **Multi-tenancy**
In cloud environments, your VMs exist with other unfamiliar, potentially hostile VMs with unknown security.

12. **Data destruction**
Some cloud providers do not overwrite storage before recycling it to another tenant; in some cases where the storage is overwritten, data may be vulnerable after a system crash or unexpected termination.

TREND MICRO

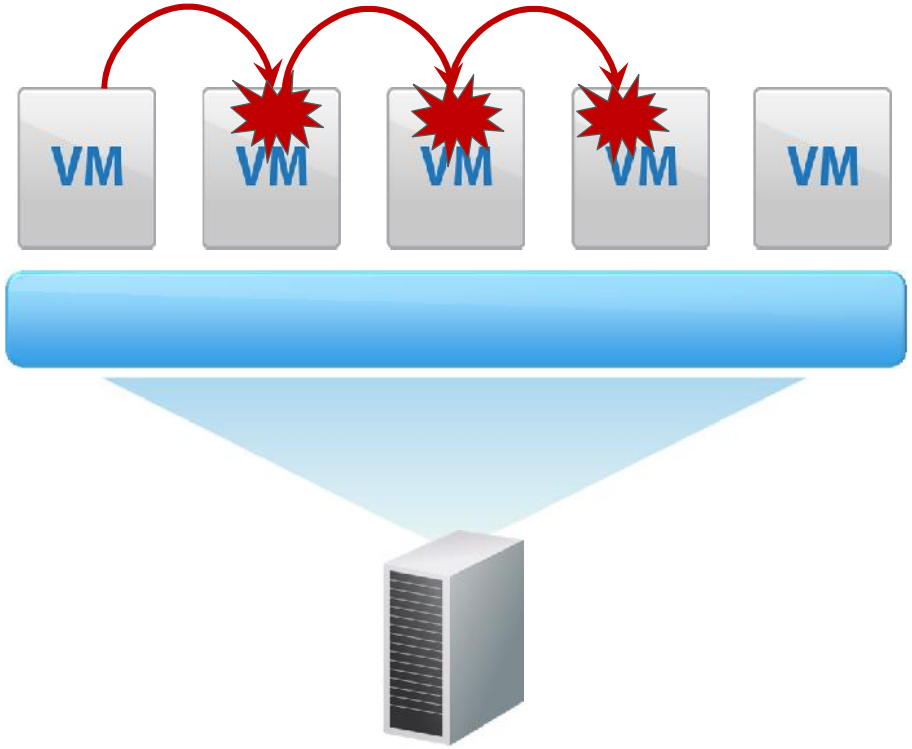
Các bảo mật truyền thống cho server



- Anti-virus: bảo vệ kiểu cài agent-based cho từng VM, trực tiếp trên server. Định kỳ download signature file và quét toàn bộ HDD.
- IDS/IPS: Sử dụng thiết bị hoặc software trên lớp mạng

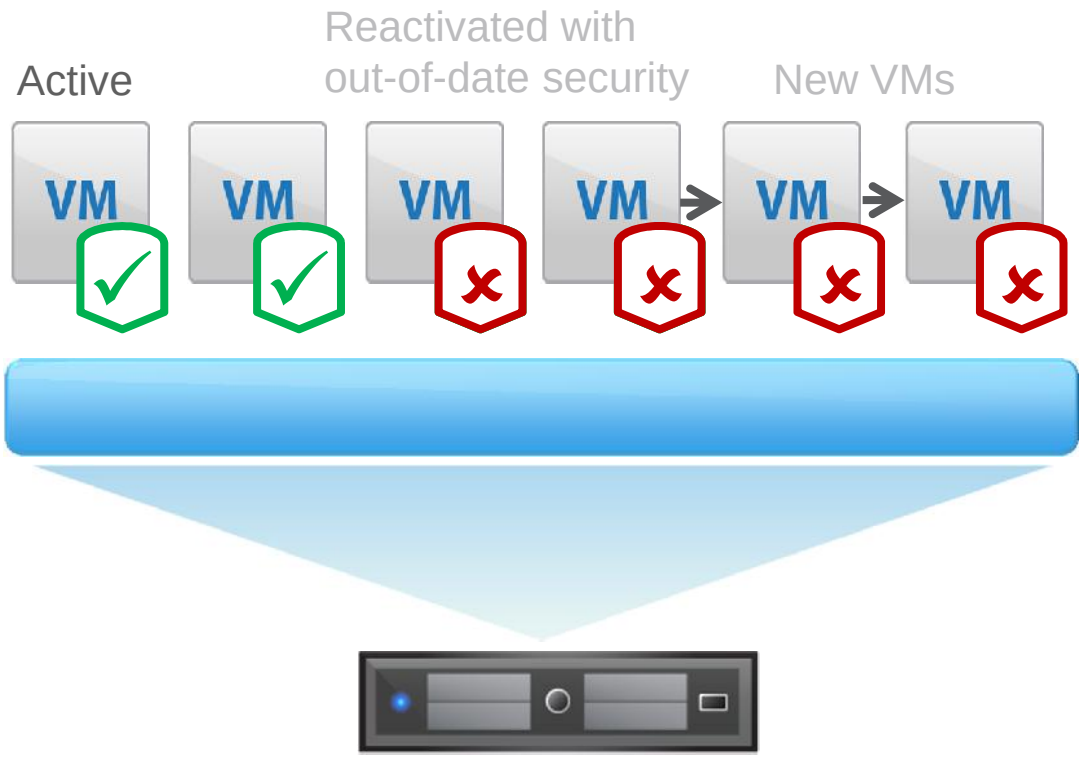
2 Inter-VM attacks

Vẫn xảy ra tấn công giữa các VM cùng server vật lý do sử dụng chung CPU, RAM, Disk



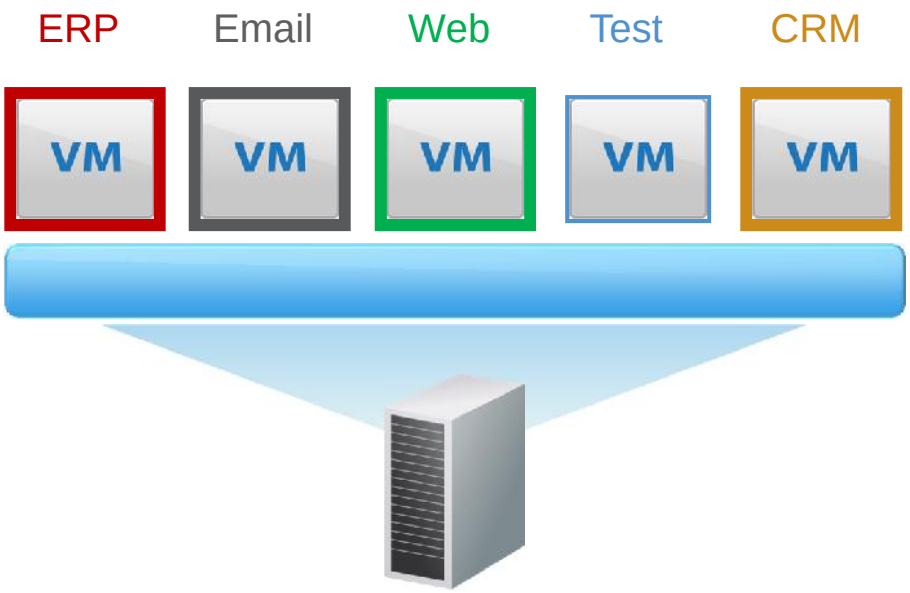
3 Instant-on gaps

Lỗ hổng an ninh của các VM activate/inactivate/ dormant/newly added… phát sinh trong quá trình vận hành và không thể patch & restart server mọi lúc



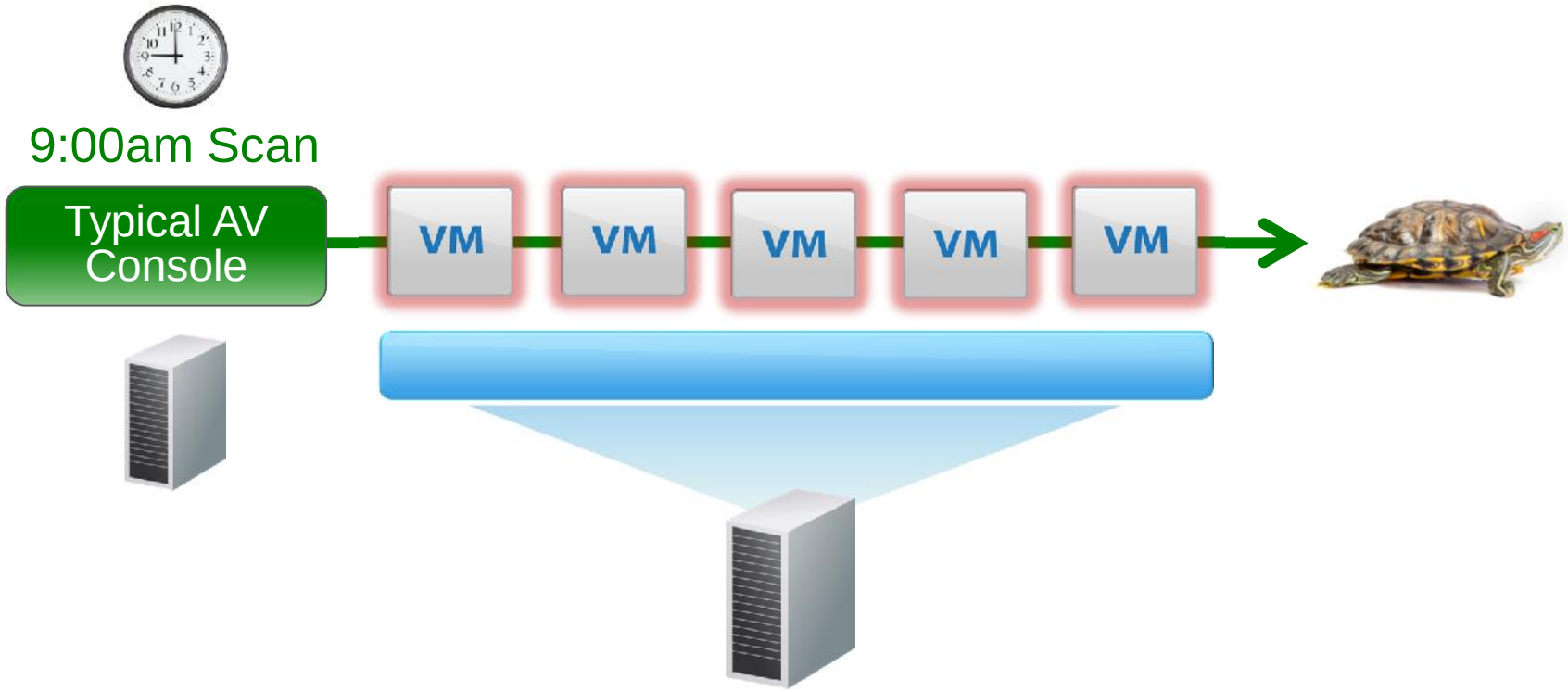
4 Mixed trust level VMs

Chênh lệch ngày càng tăng về độ tin cậy và độ ưu tiên giữa các VM cùng server vật lý. Trong quá trình vận hành liên tục của ứng dụng, rất khó cách ly các VM này.



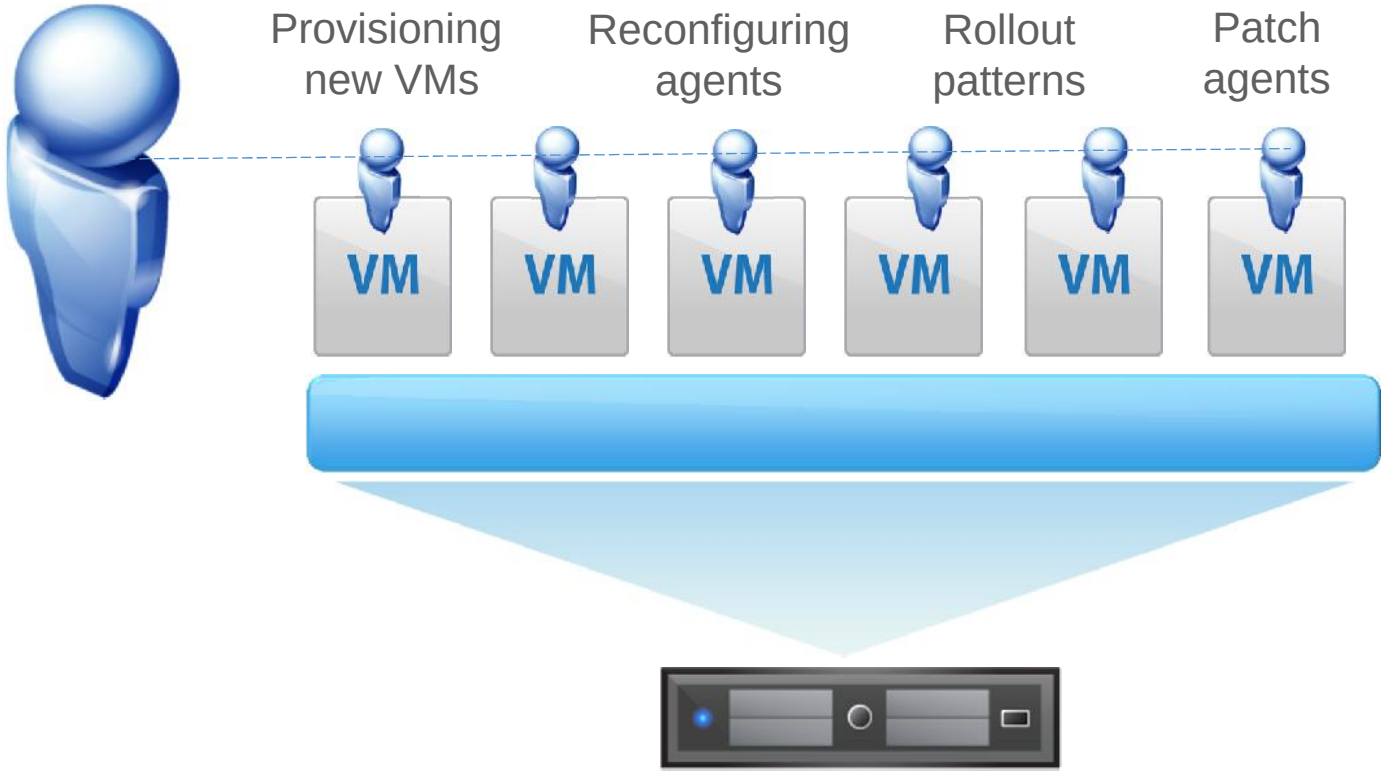
5 Resource contention

Tiêu thụ đáng kể nguồn lực của server đặc biệt khi VM đồng loạt quét virus hoặc cập nhật signature file



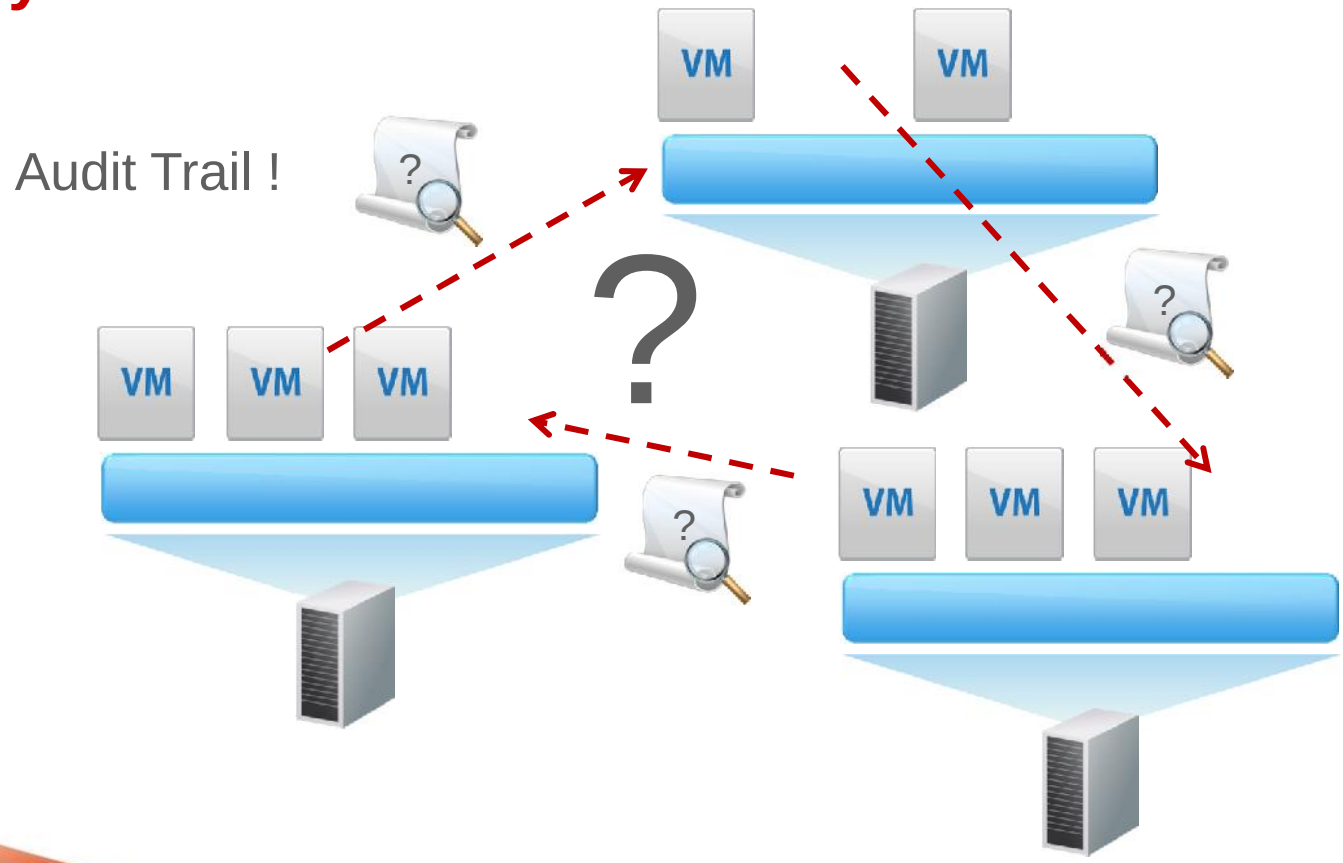
6 Complexity of Management

Các VM thuộc quyền quản lý của các chủ thể có nhiều mức độ an toàn khác nhau và không chia xẻ quyền quản lý cho IDC admin trong khi lại đòi hỏi admin phải đảm bảo security mức cao nhất.



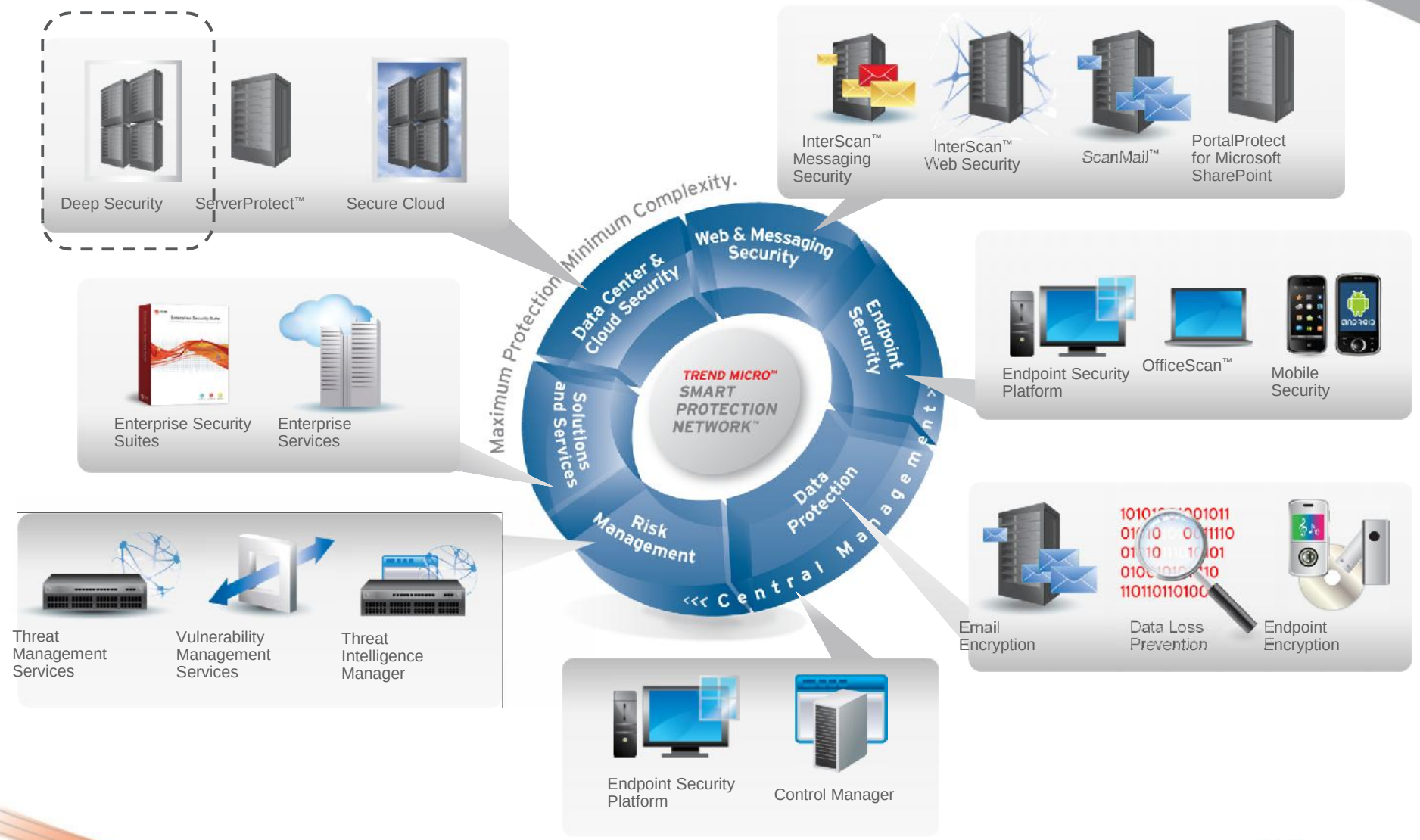
7 Compliance/Lack of audit trail

Rất khó theo kịp yêu cầu đảm bảo tuân thủ các chuẩn PCI cho server trong một trường ảo luôn co dãn và thay đổi



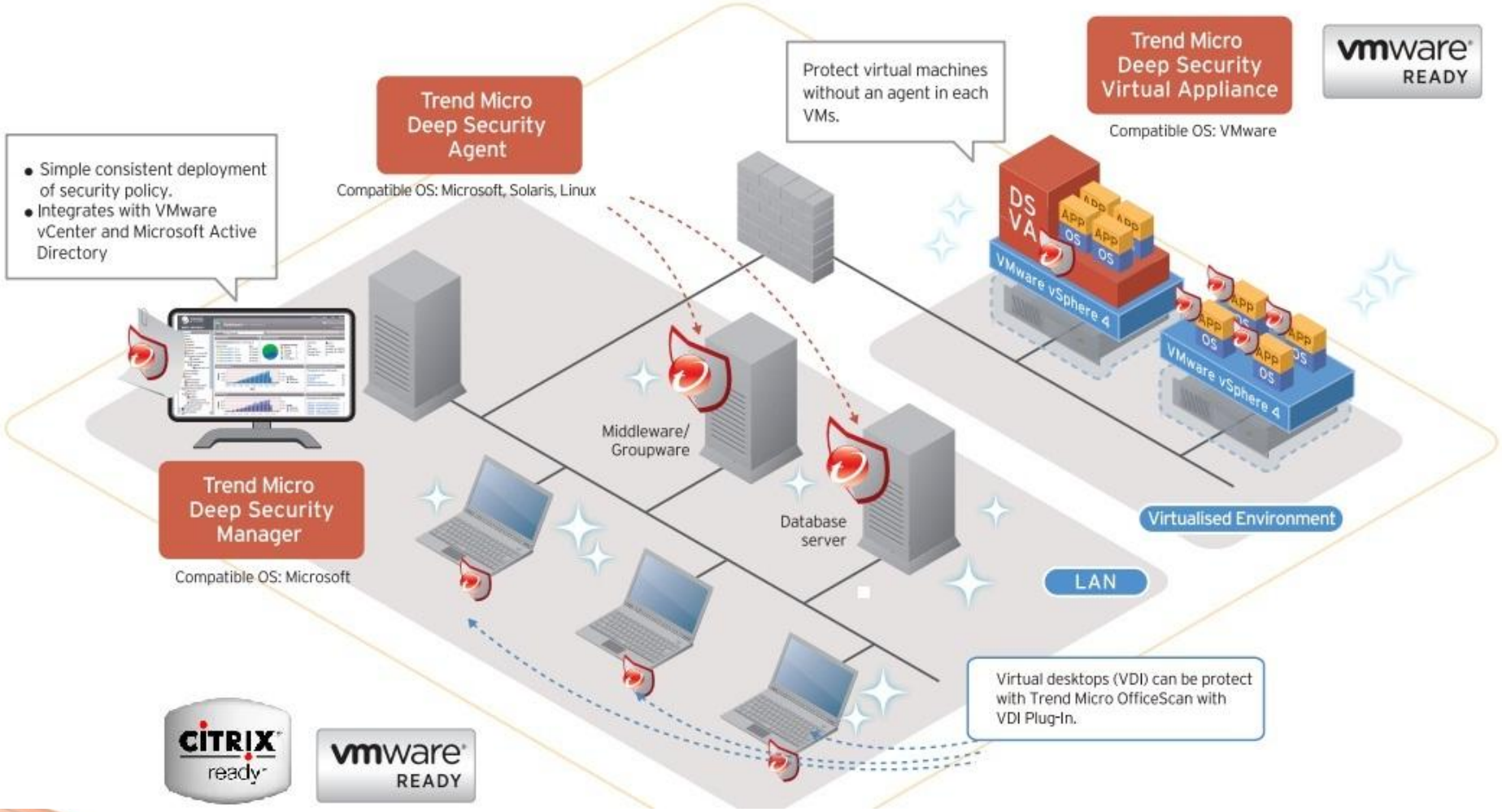
TREND MICRO

Trend Micro – Enterprise Products



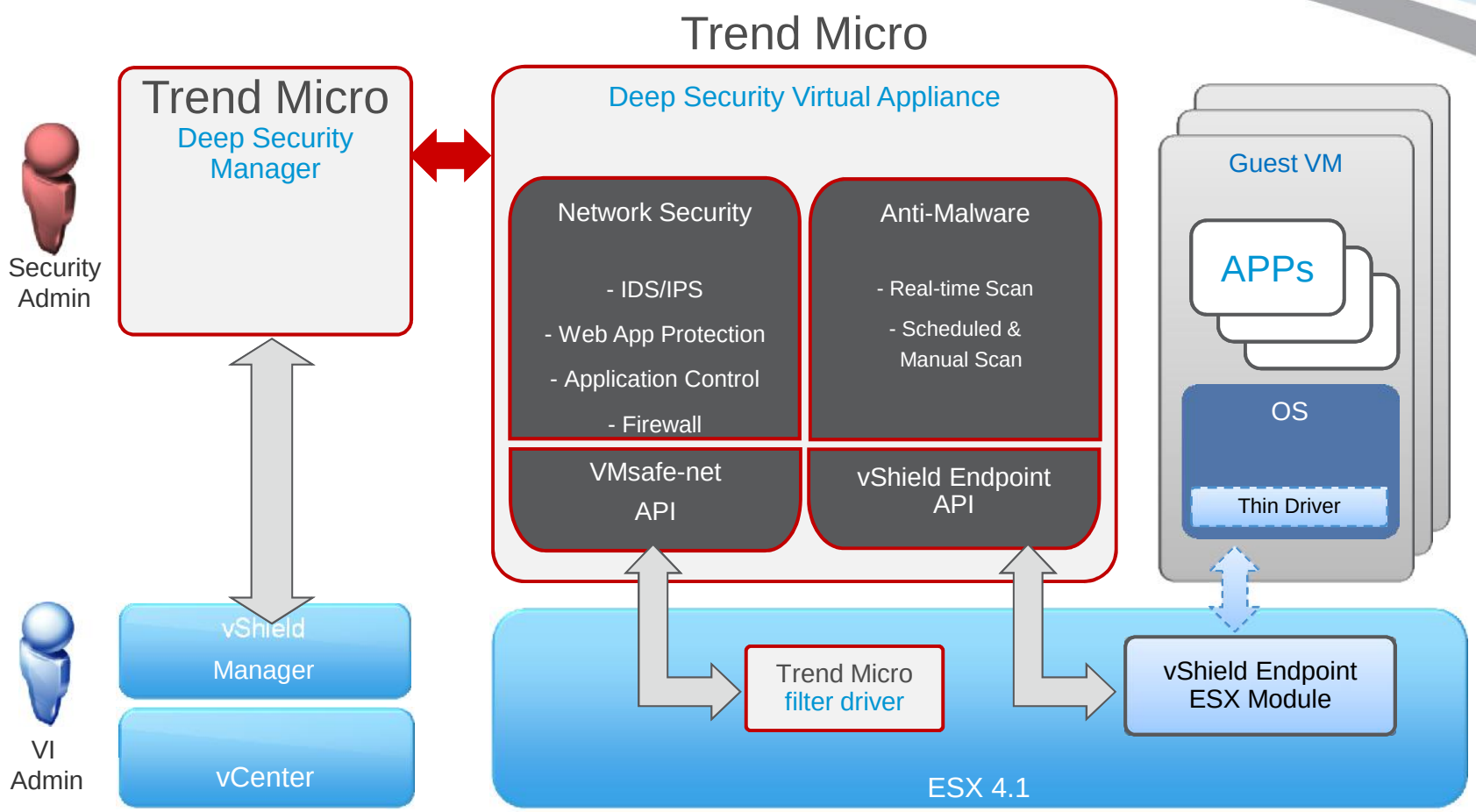
Trend Micro
Deep Security

Deep Security diagram – agent & agentless



TREND MICRO

Agent-less Security Architecture



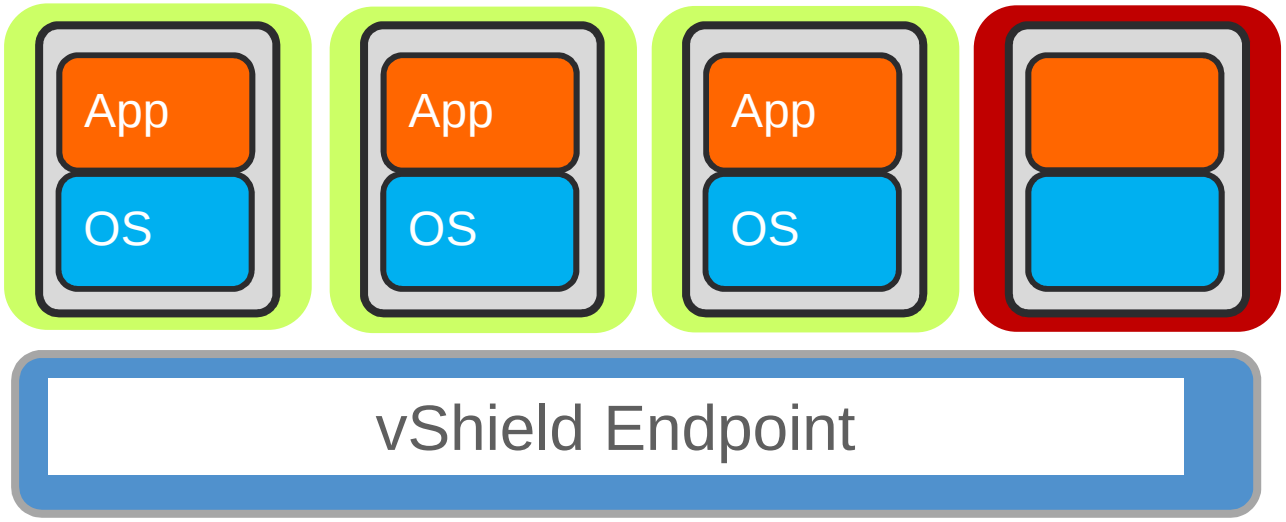
Legend →

Trend Micro product components

VMware Platform

vShield Endpoint Components

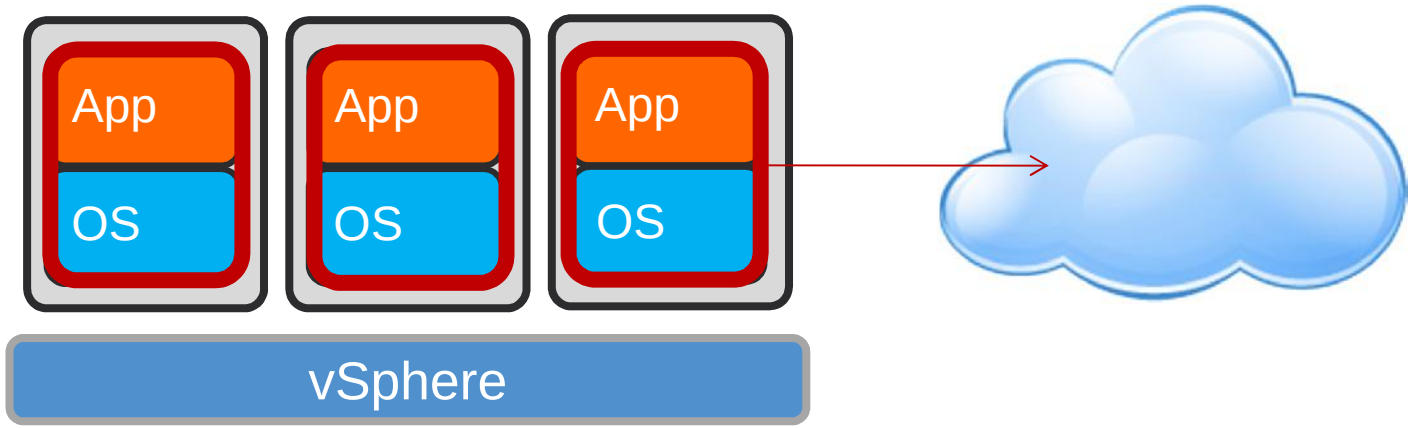
True style of security for virtualization: Hypervisor vs Agentless and Virtual Appliance



Anti-virus
Virtual Appliance

- Secures VMs from the outside using vShield Endpoint APIs
- More manageable: No agents to configure, update, patch
- Faster performance: Freedom from AV Storms
- Stronger security: Instant ON protection + tamper-proofing
- Higher consolidation: Inefficient operations removed

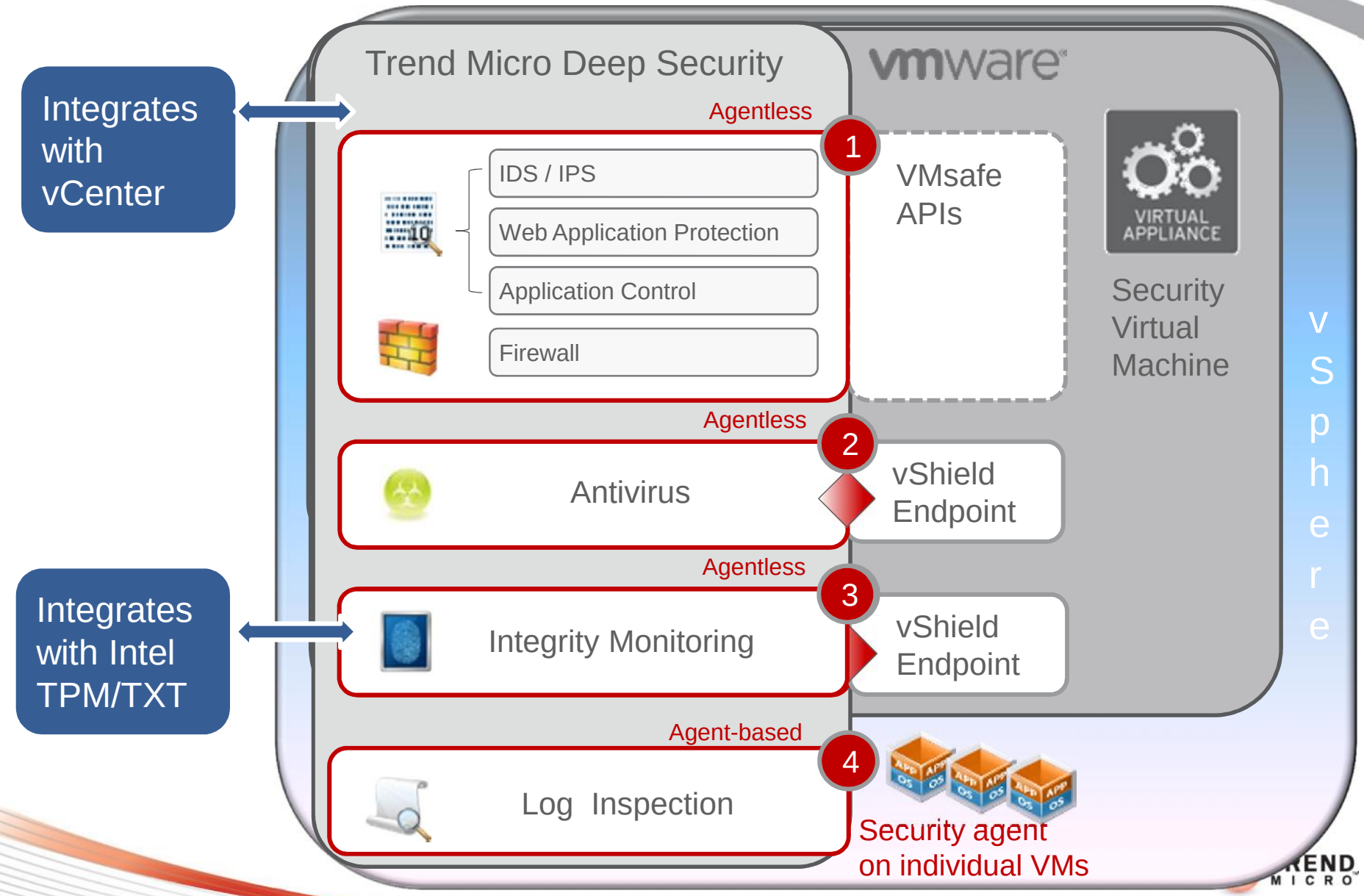
Security that is Cloud-Ready



- Security for datacenter VMs moves to the cloud with application and data
- Advanced security modules (IDS/IPS, Integrity monitoring) protect server in multi-tenant environment

Deep Security 8

Agentless Security for VMware



Deep Security 8.0 Summary

vmware TREND MICRO DEEP SECURITY

Agentless

VMsafe APIs

- IDS / IPS
- Web Application Protection
- Application Control
- Firewall

1

Detects and blocks known and zero-day attacks that target vulnerabilities *(PCI*)*

Shields web application vulnerabilities *(PCI*)*

Provides increased visibility into, or control over, applications accessing the network

Reduces attack surface. Prevents DoS & detects reconnaissance scans *(PCI*)*

Agentless

vShield Endpoint

- Antivirus
- Integrity Monitoring

2

Detects and blocks malware (web threats, viruses & worms, Trojans). *(PCI*)*

3

Detects malicious and unauthorized changes to directories, files, registry keys. *(PCI*)*

Integrates with vCenter

Agent-based

- Log Inspection

4

Optimizes the identification of important security events buried in log entries. *(PCI*)*

(PCI*): Help

TREND MICRO

Trend Micro Deep Security

5 protection modules

Deep Packet Inspection

- IDS / IPS
- Web Application Protection
- Application Control

Firewall

Integrity Monitoring

Log Inspection

Anti-Virus

Shields web application vulnerabilities

Detects and blocks known and zero-day attacks that target vulnerabilities

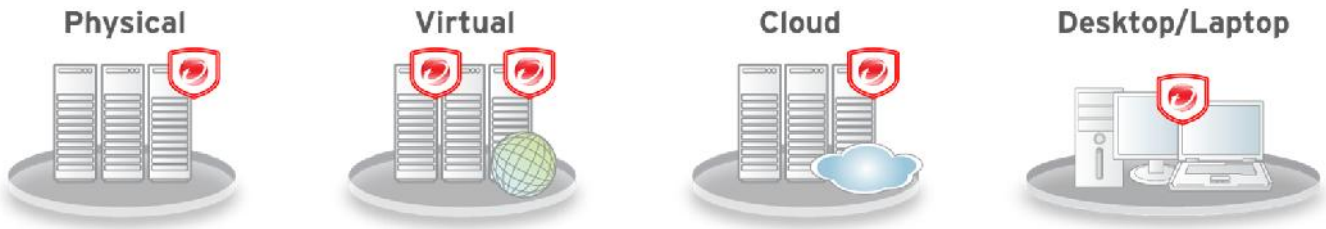
Provides increased visibility into, or control over, applications accessing the network

Reduces attack surface. Prevents DoS & detects reconnaissance scans

Detects malicious and unauthorized changes to directories, files, registry keys…

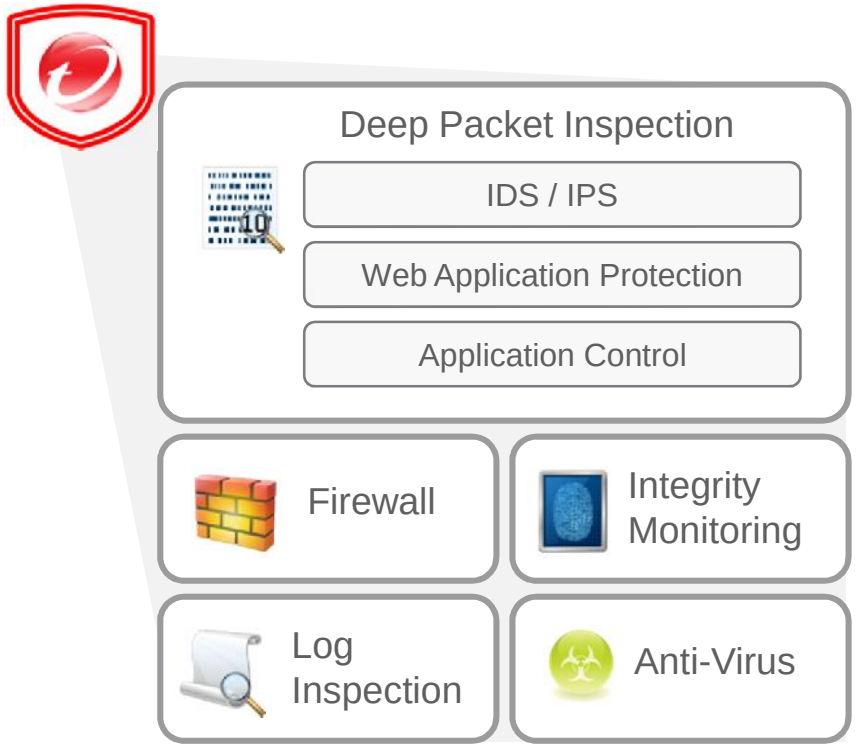
Optimizes identification of important security events across multiple log files

Detects and blocks malware (viruses & worms, Trojans)



Protection is delivered via Agent and/or Virtual Appliance

Deep Security for PCI compliance



Addressing 7 PCI Regulations and 20+ Sub-Controls Including:	
☑ (1.)	Network Segmentation
☑ (1.x)	Firewall
☑ (5.x)	Anti-virus*
☑ (6.1)	Virtual Patching**
☑ (6.6)	Web App. Protection
☑ (10.6)	Daily Log Review
☑ (11.4)	IDS / IPS
☑ (11.5)	File Integrity Monitoring

* Available for VMware only Q3 2010
** Compensating Control

Addresses distributed environment challenges

Firewall

Full function centrally managed network and application firewall

Reduces PCI scope without the cost and complexity of network firewalls

Deep Packet Inspection

Provides IDS / IPS, Web App Protection, Application Control

Eliminates ad-hoc/emergency patching

Protects “un-patchable” systems and applications

Integrity Monitoring

Full System Monitoring in real-time; Scheduled & on-demand scanning

Detects remote malicious activities

Provides audit trail of system changes

Log Inspection

Collects & analyzes OS and application logs for security events

Automates event collection & analysis

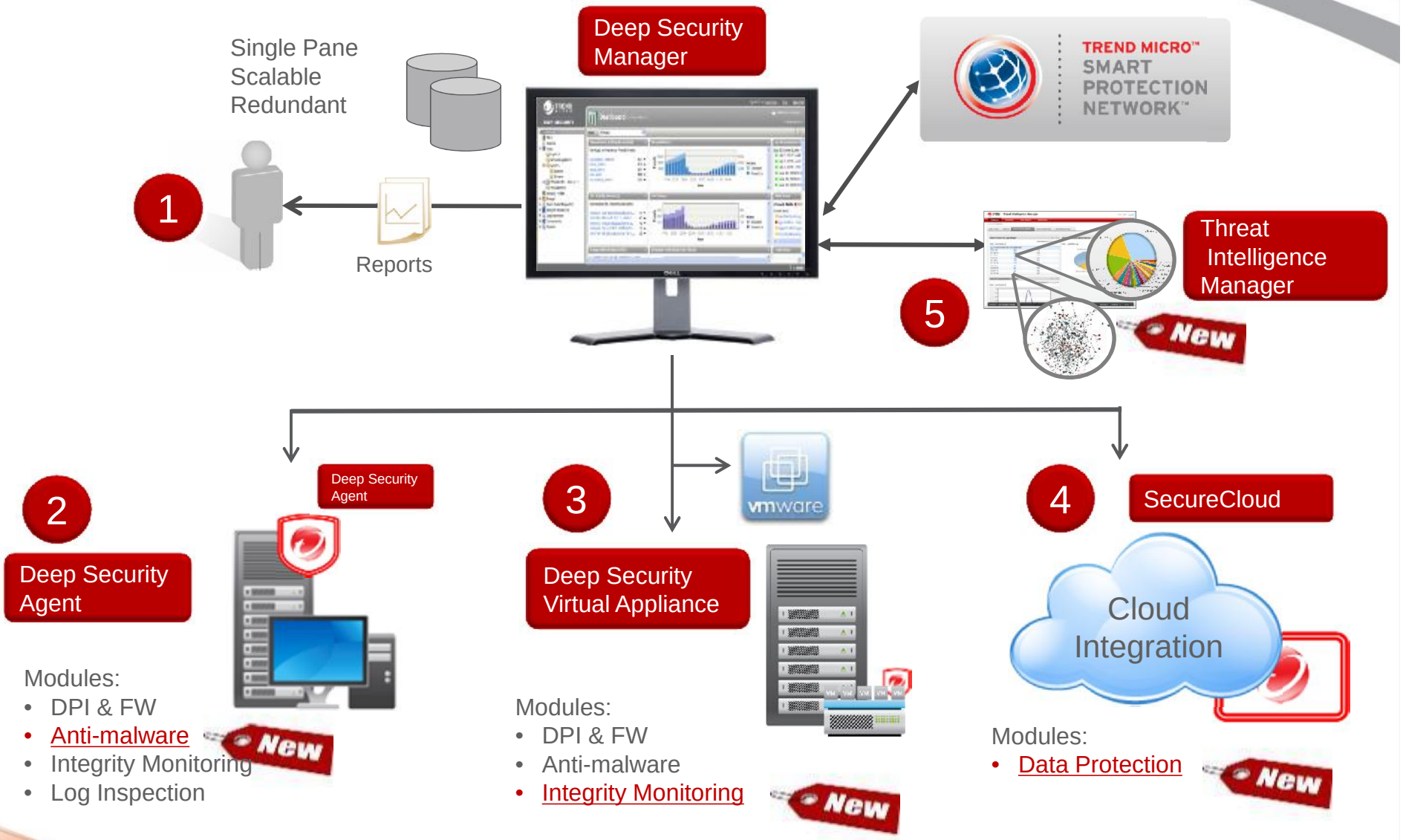
Prioritized alerting focuses management and minimizes overhead

Antivirus

Malware protection for virtual servers

Optimized performance and flexibility in a single solution

Deep Security Architecture



TREND MICRO

Platforms protected

Microsoft

Windows 2000
Windows 2003 (32 & 64 bit)
Windows XP
Vista (32 & 64 bit)
Windows Server 2008 (32 & 64 bit)
Windows 7
HyperV (Guest VM)

solaris

8, 9, 10 on SPARC
10 on x86 (64 bit)

Linux

Red Hat 4, 5 (32 & 64 bit)
SuSE 10, 11

vmware

VMware ESX Server (guest OS)
VMware Server (host & guest OS)

CITRIX

XenServer (Guest VM)

UNIX

HP-UX 11i (11.23 & 11.31)
AIX 5.3, 6.1

Integrity Monitoring
& Log Inspection modules

TREND MICRO

Virtual Patching

Challenge 2

Consistent patch management and deployment to protect against vulnerability exploits

- Attacks on system and application vulnerabilities.
- Unable to keep up with various patches for mixture of server operating systems and applications.
- Certain applications and servers cannot be stopped for patch application.
- Patches are no longer provided for legacy applications and operating systems.

Solution 2

Virtual Patching - Automatically detect vulnerabilities in operating system and application, and protect them from exploits.

- Automatically take an inventory of applications and OS on the server and identify relevant Common Vulnerabilities and Exposures (CVE)
- Automatically apply IDS/IPS rules to shield affected applications and OS.
- Look for out-of-box protection against 100+ applications, including database, web, email and FTP servers.

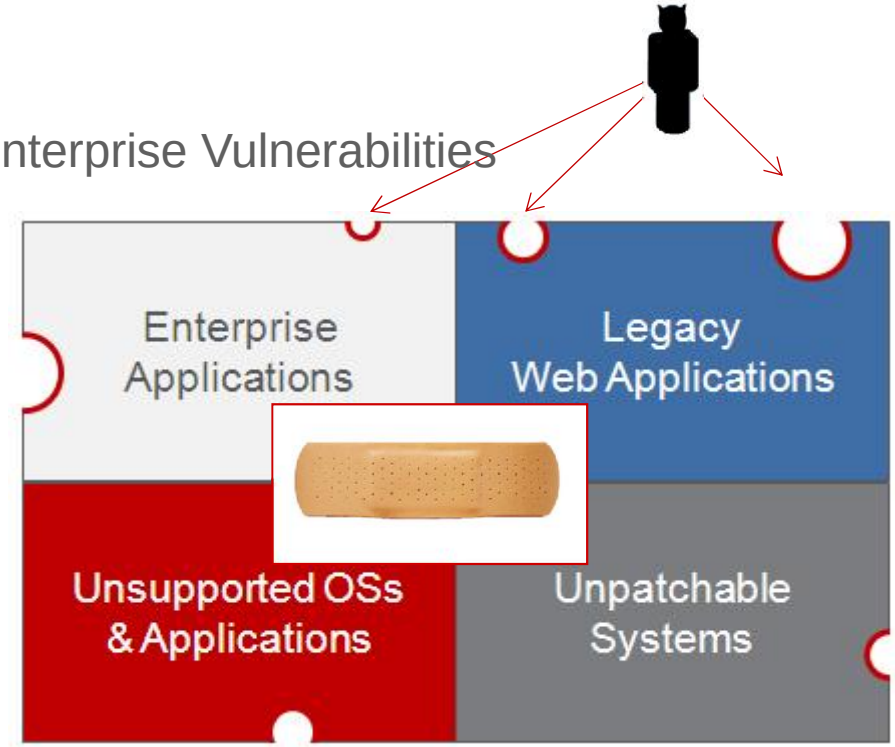
TREND MICRO

The Patching Conundrum

Takes days to months until patches are available and can be tested & deployed

Enterprise Vulnerabilities

Developers not available to fix vulnerabilities



Patches are no longer being developed

Can't be patched because of cost, regulations, SLA reasons

- Enterprises spend a third of their time on patching
- But ¾ of enterprises say their patching is not effective

Source: InformationWeek, Analytics Report: 2010 Strategy Security Survey

TREND MICRO

Over 100 applications protected

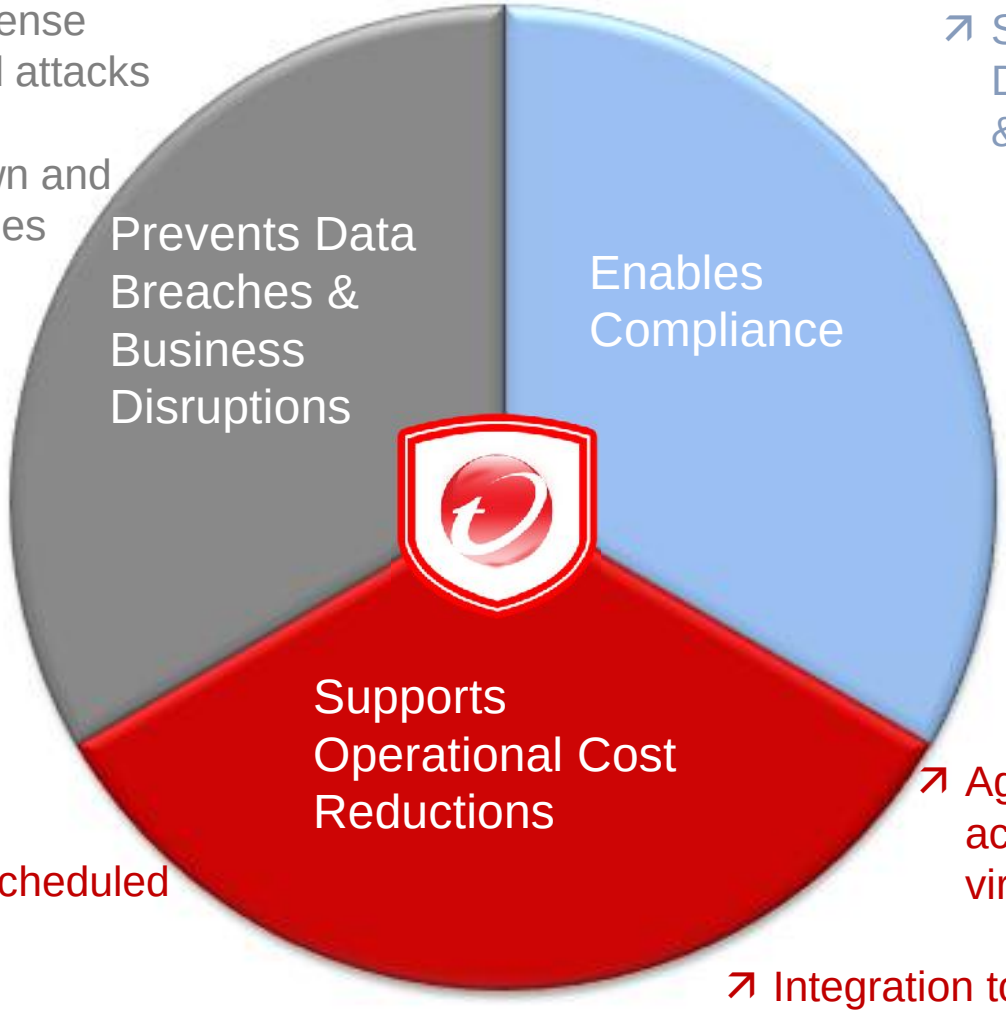
Deep Security rules shield vulnerabilities in these common applications

Operating Systems	Windows (2000, XP, 2003, Vista, 2008, 7), Sun Solaris (8, 9, 10), Red Hat EL (4, 5), SuSE Linux (10,11)
Database servers	Oracle, MySQL, Microsoft SQL Server, Ingres
Web app servers	Microsoft IIS, Apache, Apache Tomcat, Microsoft Sharepoint
Mail servers	Microsoft Exchange Server, Merak, IBM Lotus Domino, Mdaemon, Ipswitch, IMail,, MailEnable Professional,
FTP servers	Ipswitch, War FTP Daemon, Allied Telesis
Backup servers	Computer Associates, Symantec, EMC
Storage mgt servers	Symantec, Veritas
DHCP servers	ISC DHCPD
Desktop applications	Microsoft (Office, Visual Studio, Visual Basic, Access, Visio, Publisher, Excel Viewer, Windows Media Player), Kodak Image Viewer, Adobe Acrobat Reader, Apple Quicktime, RealNetworks RealPlayer
Mail clients	Outlook Express, MS Outlook, Windows Vista Mail, IBM Lotus Notes, Ipswitch IMail Client
Web browsers	Internet Explorer, Mozilla Firefox
Anti-virus	Clam AV, CA, Symantec, Norton, Trend Micro, Microsoft
Other applications	Samba, IBM Websphere, IBM Lotus Domino Web Access, X.Org, X Font Server prior, Rsync, OpenSSL, Novell Client

TREND MICRO

Deep Security 8: Key benefits

- Provides layered defense against sophisticated attacks
- Shields against known and unknown vulnerabilities
- Monitors system and hypervisor integrity
- Web reputation prevents malicious website access



- Supports more PCI DSS 2.0, NIST, HIPAA & other regulations
- Detailed reports document prevented attacks & compliance status

- Prioritize secure coding efforts
- Manage unscheduled patching
- Cloud-based event whitelisting & Trusted events simplify FIM mgmt

- Agentless architecture accelerates realize virtualization savings
- Integration to enterprise platforms & apps lowers costs

TREND MICRO

TEST REPORT

Tolly.

#211101
February 2011
Commissioned by Trend Micro, Inc.

Trend Micro Deep Security 7.5 vs. McAfee and Symantec

Anti-virus Performance in VMware ESX Virtual Environments

Executive Summary

Server and desktop virtualization are essential elements of any IT strategy that seeks to decrease capital and operational expenditures. In the rush to implement virtualization technologies, many organizations simply deploy the same anti-virus solution that is in use on their physical server and desktop systems. Because these traditional anti-virus solutions are not designed specifically for virtual environments, they can create significant operational issues such as anti-virus (AV) storms, resource wastage and administrative overhead, and hamper the organization's objective of maximizing VM densities.

Trend Micro, Inc. commissioned Tolly to benchmark the performance within virtual environments of the Trend Micro Deep Security solution vs. McAfee Total Protection for Endpoint and Symantec Endpoint Protection 11.0. Specifically, this testing evaluated the impact each solution had on host system (physical server) resources especially as guest machine density increased to up to 100 virtual machines simultaneously running in a VMware ESX 4.1 environment.

TEST HIGHLIGHTS

The Trend Micro Deep Security Virtual Appliance:

1. Demonstrated consistently lower demand for system CPU, memory and disk I/O over traditional agent-based solutions even during periods when the workload was designed not to stress AV
2. Successfully avoided AV storm issues with scheduled scans and pattern updates that prevented other solutions from testing beyond 25 VMs
3. Demonstrated density improvements of 29% to 275% over McAfee and Symantec running test workloads

Tests showed that Trend Micro Deep Security, which provides an agentless virtual appliance-based approach to anti-virus protection optimized for virtualization, consistently consumed less CPU, RAM and disk I/O resources than the non VM-aware implementations where anti-virus agents and processing resided in each and every Windows 7 virtual machine.

TREND MICRO

Tolly Group – Test report

http://us.trendmicro.com/us/home/enterprise/tolly-report/index.html

Hoặc

http://trendmicro.mediaroom.com/index.php?s=43&type=current&news_item=862&WT.mc_id=2008HP_News

VMware Performance Host Testbed Components

Component	Version/Build
VMware ESX	4.1.0
VMware vCenter Server	4.1.0 build 258902
VMware View Composer Server	2.1 build 277387
VMware View Connection Server	4.5.0
VMware vShield Manager	4.1 build 310451
Server Hardware	2x Xeon x5680 (Hexacore) running at 3.33GHz with 192 GB of DDR 3 RAM (Total of 24 logical cores)
Storage Area Network	HP StorageWorks MSA connected via 4GB FibreChannel
Guest VM Resources	1GB RAM and 1 vCPU
Guest Operating System	Microsoft Windows 7 Enterprise

2010 Table 3

Systems Under Test

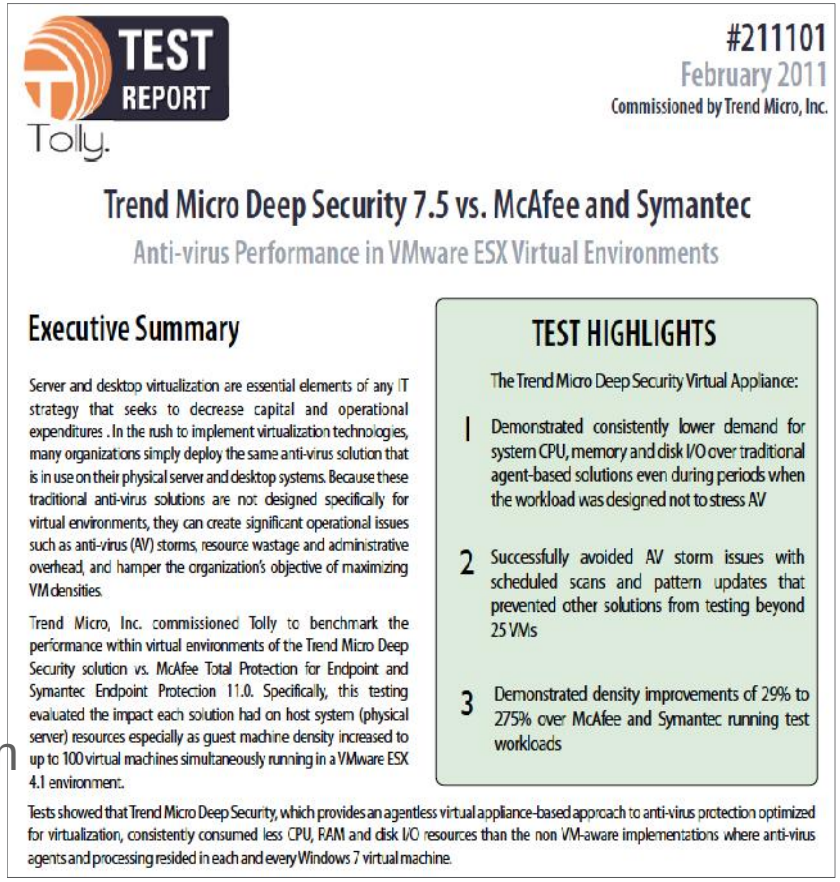
Vendor	Product	Components	Virtual Machine Aware	Implementation
Trend Micro, Inc.	Deep Security 7.5	Trend Micro Deep Security Manager version 7.5.1378; Trend Micro Deep Security Virtual Appliance 7.5.0.1600; Filter Driver 7.0.0.894; Default configuration. Assigned the pre-configured Windows Anti-Malware Protection security profile.	Yes	Automatic, single virtual appliance. Agentless client communicates via VMware vShield API
McAfee	Total Protection for Endpoint	McAfee ePolicy Orchestrator 4.5; McAfee Agent for Windows 4.5.0 Minor Version 1270; McAfee VirusScan(R) Enterprise 8.7.0 Minor version 570 with Hot Fix 2; McAfee AntiSpyware Enterprise 8.7 Minor version 129; McAfee Host Intrusion Prevention 7.0.0 minor Version 1070; McAfee SiteAdvisor(R) Enterprise Plus 3.0.0 Minor version 476 All with default policies. Cancelled pre-configured Full Scan and Update client tasks.	No	Traditional endpoint client
Symantec	Endpoint Protection 11.0	Version 11.0.6100.645	No	Traditional endpoint client

Source: Tolly, October 2010 Table 2

TREND MICRO

Tolly Report

- Third party lab test of DS Agentless AV with traditional AV
- Symantec Endpoint Protection 11.0 and McAfee VirusScan Enterprise 8.7 were tested
- Symantec/McAfee consumed more virtual system resources (CPU, Memory, Disk) in both idle and storm conditions
- Symantec/McAfee could not scale to support over 25 desktop VMs/host
- Tolly Group report projects that Trend can support 2-3 times desktop VM density as these other solutions.
- Report is hosted on www.trendmicro.com/virtualization as well as on Tolly.com



TEST REPORT

Tolly.

#211101
February 2011
Commissioned by Trend Micro, Inc.

Trend Micro Deep Security 7.5 vs. McAfee and Symantec

Anti-virus Performance in VMware ESX Virtual Environments

Executive Summary

Server and desktop virtualization are essential elements of any IT strategy that seeks to decrease capital and operational expenditures . In the rush to implement virtualization technologies, many organizations simply deploy the same anti-virus solution that is in use on their physical server and desktop systems. Because these traditional anti-virus solutions are not designed specifically for virtual environments, they can create significant operational issues such as anti-virus (AV) storms, resource wastage and administrative overhead, and hamper the organization's objective of maximizing VM densities.

Trend Micro, Inc. commissioned Tolly to benchmark the performance within virtual environments of the Trend Micro Deep Security solution vs. McAfee Total Protection for Endpoint and Symantec Endpoint Protection 11.0. Specifically, this testing evaluated the impact each solution had on host system (physical server) resources especially as guest machine density increased to up to 100 virtual machines simultaneously running in a VMware ESX 4.1 environment.

TEST HIGHLIGHTS

The Trend Micro Deep Security Virtual Appliance:

1. Demonstrated consistently lower demand for system CPU, memory and disk I/O over traditional agent-based solutions even during periods when the workload was designed not to stress AV
2. Successfully avoided AV storm issues with scheduled scans and pattern updates that prevented other solutions from testing beyond 25 VMs
3. Demonstrated density improvements of 29% to 275% over McAfee and Symantec running test workloads

Tests showed that Trend Micro Deep Security, which provides an agentless virtual appliance-based approach to anti-virus protection optimized for virtualization, consistently consumed less CPU, RAM and disk I/O resources than the non VM-aware implementations where anti-virus agents and processing resided in each and every Windows 7 virtual machine.

TREND MICRO

Tolly Report
Test Environment

VMware Performance Host Testbed Components

Component	Version/Build
VMware ESX	4.1.0
VMware vCenter Server	4.1.0 build 258902
VMware View Composer Server	2.1 build 277387
VMware View Connection Server	4.5.0
VMware vShield Manager	4.1 build 310451
Server Hardware	2x Xeon x5680 (Hexacore) running at 3.33GHz with 192 GB of DDR 3 RAM (Total of 24 logical cores)
Storage Area Network	HP StorageWorks MSA connected via 4GB FibreChannel
Guest VM Resources	1GB RAM and 1 vCPU
Guest Operating System	Microsoft Windows 7 Enterprise

2010 Table 3

Systems Under Test

Vendor	Product	Components	Virtual Machine Aware	Implementation
Trend Micro, Inc.	Deep Security 7.5	Trend Micro Deep Security Manager version 7.5.1378; Trend Micro Deep Security Virtual Appliance 7.5.0.1600; Filter Driver 7.0.0.894; Default configuration. Assigned the pre-configured Windows Anti-Malware Protection security profile.	Yes	Automatic, single virtual appliance. Agentless client communicates via VMware vShield API
McAfee	Total Protection for Endpoint	McAfee ePolicy Orchestrator 4.5; McAfee Agent for Windows 4.5.0 Minor Version 1270; McAfee VirusScan(R) Enterprise 8.7.0 Minor version 570 with Hot Fix 2; McAfee AntiSpyware Enterprise 8.7 Minor version 129; McAfee Host Intrusion Prevention 7.0.0 minor Version 1070; McAfee SiteAdvisor(R) Enterprise Plus 3.0.0 Minor version 476 All with default policies. Cancelled pre-configured Full Scan and Update client tasks.	No	Traditional endpoint client
Symantec	Endpoint Protection 11.0	Version 11.0.6100.645	No	Traditional endpoint client

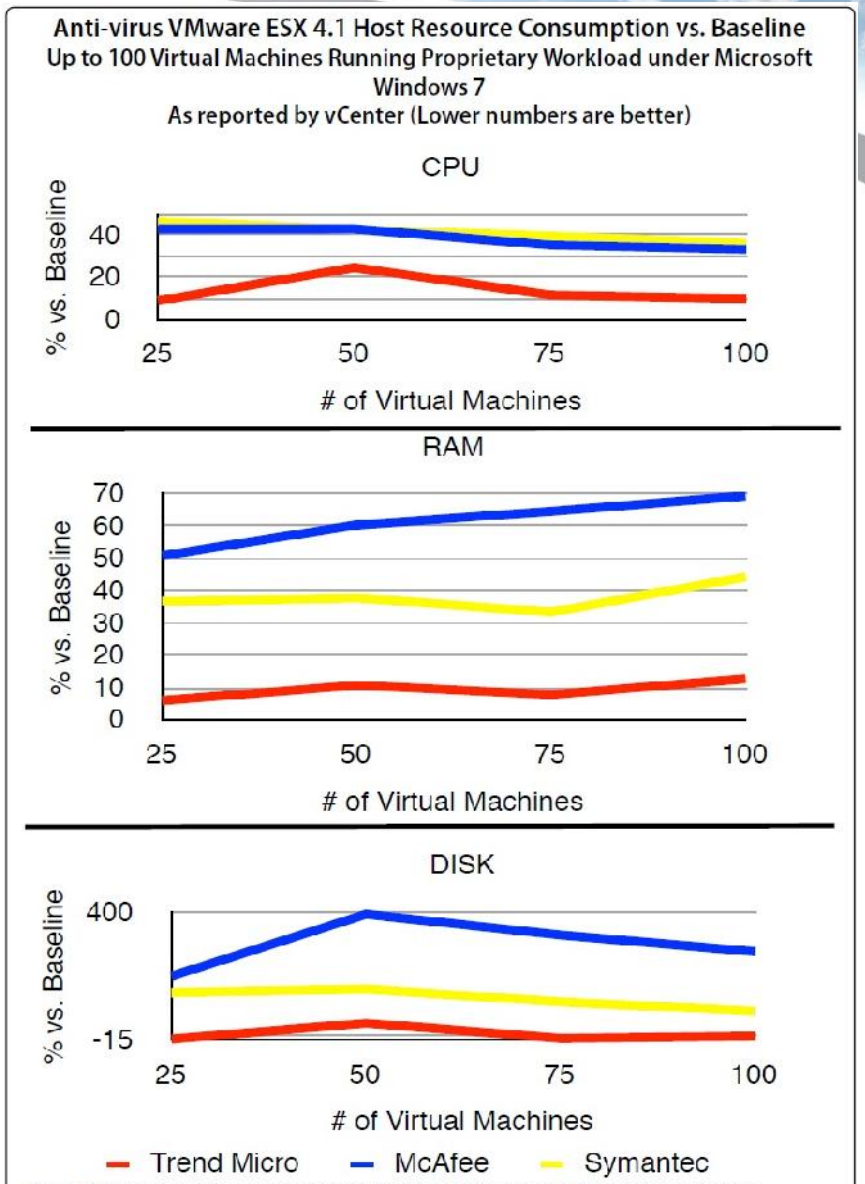
Source: Tolly, October 2010 Table 2

TREND MICRO

Tolly Report
"Idle Load" Results

- All tests observed % consumption over baseline for each resource at 25, 50, 75 and 100 desktop VMs

- On average: Symantec and McAfee consumed 1.7 to 8.5 times the Trend Micro resource overhead – even when idle



Note: All systems running proprietary workload in addition to scan. Baseline is proprietary workload running with no endpoint security solution installed. See report body for baseline values and detailed results. Utilization over baseline is calculated by subtracting baseline from result, dividing by baseline and multiplying by 100. As McAfee was unable to complete the 100 VM test, results for 100 were extrapolated from the 25, 50 and 75 VM tests. Average of 30 minute run. Disk usage results vary up to 30% and are include for reference purposes only.

Source: Tolly, October 2010

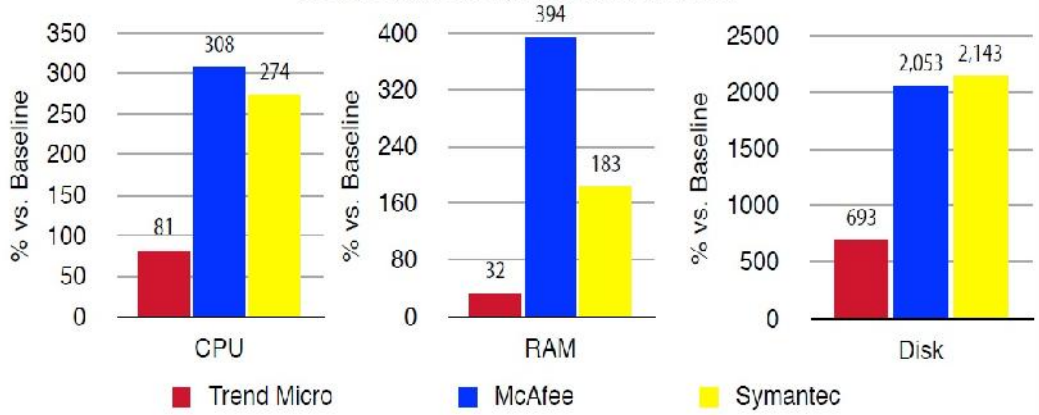
Figure 1

Tolly Report
"Full Scan Storm" Load

- At 25 VMs: Symantec and McAfee depicted 'storm' symptoms with resource usage from 3.4 times to 12 times as DS AV.

- Symantec & McAfee could not be tested beyond 25 desktop VMs
- DS AV was endorsed as being able to support 100 VMs per host

Anti-virus VMware ESX 4.1 Host Resource Consumption Overhead vs. Baseline
Request On-Demand Scan of 25 Virtual Machines Running Microsoft Windows 7
As reported by vCenter (Lower numbers are better)



Note: All systems running proprietary workload in addition to scan. Baseline is proprietary workload running with no endpoint security solution installed. Baseline values: Average CPU – 4,109.76 MHz, Average RAM – 7,893.28 MB, Average Disk – 1,741.23 KBps. Trend automatically runs only a single scan at one time. Other vendors triggered 25 simultaneous scans. Each vendor recommends various methods such as randomization for load-leveling on-demand scans. See report body for details. Utilization over baseline is calculated by subtracting baseline from result, dividing by baseline and multiplying by 100. Average of 30 minute run.

Source: Tolly, October 2010

Figure 2

Anti-virus Solution Scalability Under VMware ESX 4.1
On-Demand Scan Scenarios of Virtual Machines Running Microsoft Windows 7

Vendor	Product	Number of Virtual Machines Targeted for On-Demand Scan			
		25	50	75	100
Trend Micro, Inc.	Deep Security 7.5	Yes, completely stable	Yes, completely stable	Yes (projected, not tested)	Yes (projected, not tested)
McAfee	Total Protection for Endpoint	Yes, but with stability problems	Because of instability problems with 25 simultaneous scans, Tolly engineers did not attempt greater numbers. McAfee offers a randomization option in its client task that could provide load distribution for such both scheduled and manually triggered tasks.		
Symantec	Endpoint Protection 11.0	Yes, but with stability problems	Because of instability problems with 25 simultaneous scans, Tolly engineers did not attempt greater numbers. Symantec recommends configuring scheduled tasks for randomization. This would spread the on-demand scan requests for 100 virtual machines to approximately 160 hours by default. Manually triggered tasks cannot have randomized start times.		

Note: Trend Micro is the only virtualization-aware solution tested and automatically staggers on-demand scans so that scans are performed serially.

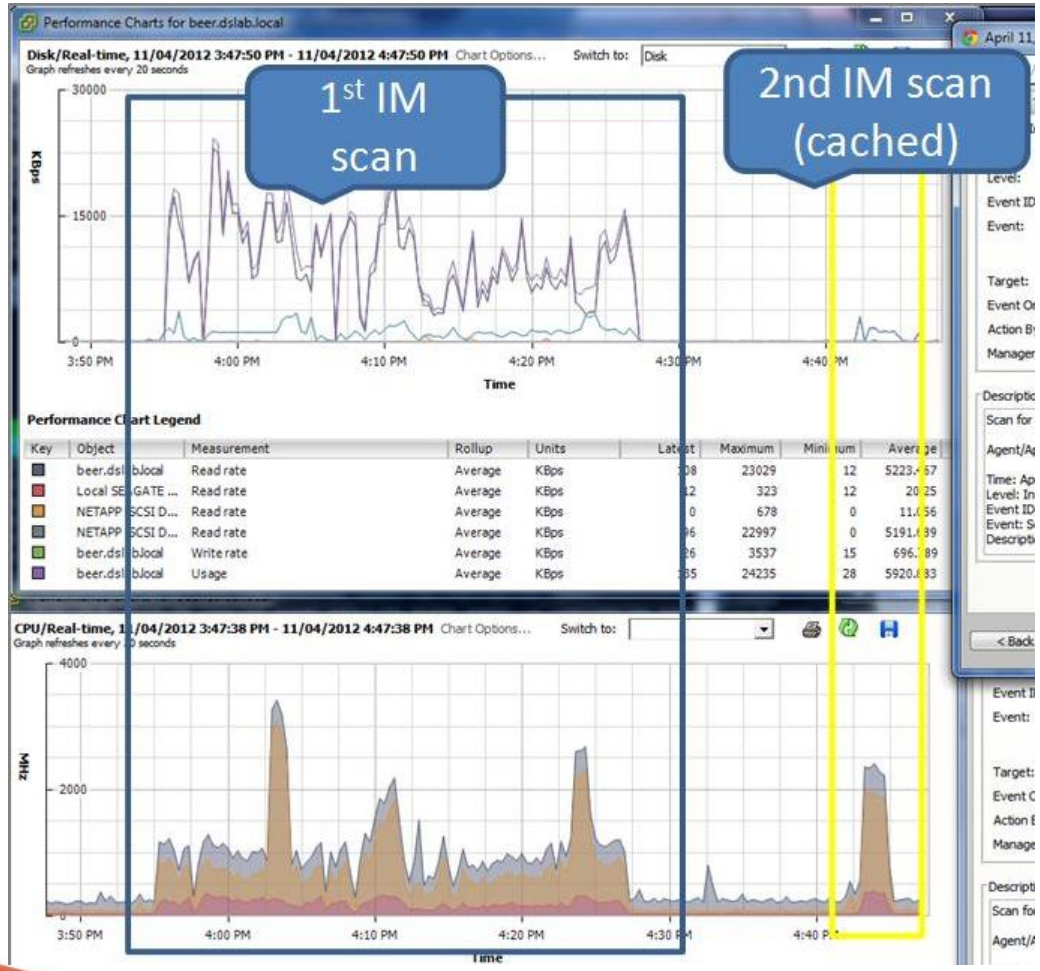
Source: Tolly, October 2010

Table 1

Further Reductions in IOPS and CPU utilization

Additional efficiency from coming vShield and Deep Security capabilities

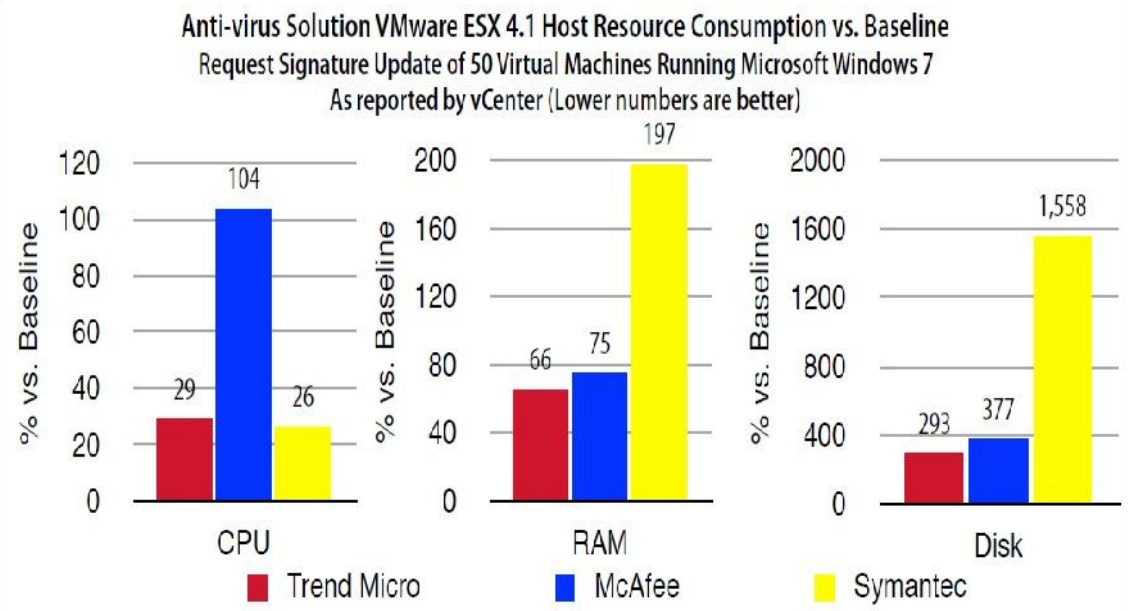
- Caching in security virtual appliances reduces utilization on subsequent scans
- Reduced IOPS will further enhance VDI consolidation



Tolly Report
"Pattern Update Storm" Load

- Like full scans, pattern updates also led to AV storms with Symantec and McAfee

- Again, McAfee consumed about 3.6 times the CPU and Symantec consumed 3 times the RAM of DS AV.



Note: All systems running proprietary workload in addition to test task. Baseline is proprietary workload running with no endpoint security solution installed. Baseline values: Average CPU = 8,434.91 MHz, Average RAM = 14,119.62 MB, Average Disk = 2,341.41 KBps. Trend only needs to download the signature file to its single virtual security appliance. Other vendors triggered 25 simultaneous updates. Each vendor recommends various methods for load-leveling updates. See report body for details. Utilization over baseline is calculated by subtracting baseline from result, dividing by baseline and multiplying by 100. Average of 15 minute run.

Source: Tolly, October 2010

Figure 3

Tolly Report
VM Density Comparisons

Nominal VM Density
(Assuming Idle load)

Trend density = 29-43% higher

True VM Density
(Factoring AV storm avoidance)

Trend density = 106-274% higher
= 2 times to 3.75 times

(On server VMs, same level of resource efficiency = 40-60% improvement in true density.)

VM Density Improvement - Proprietary Workload: Trend vs. Competitor
(Nominal Density)

	CPU	RAM	DISK
McAfee	31.4%	42.4%	236%
Symantec	34.6%	29%	174%

VM Density Improvement - On-Demand Scan: Trend vs. Competitor
(True Density)

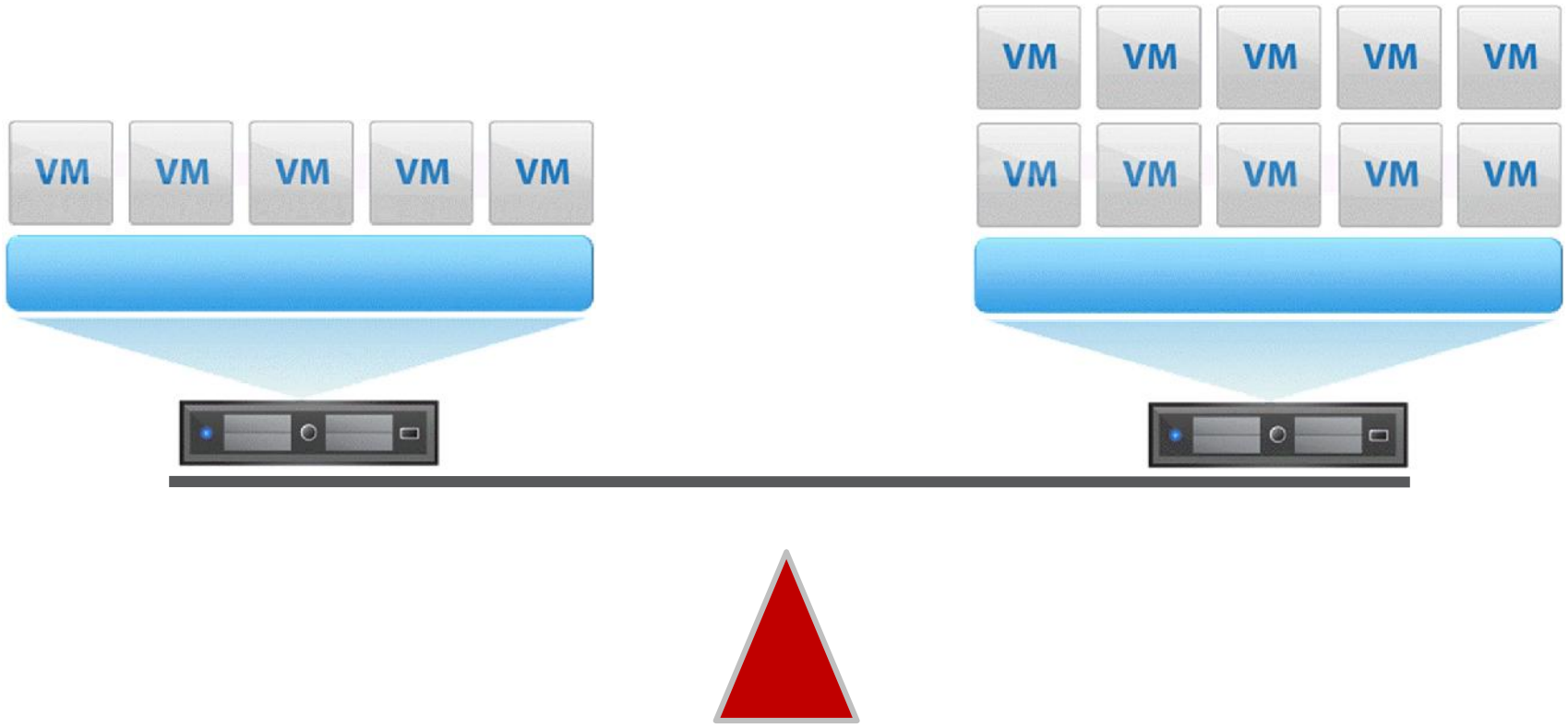
	CPU	RAM	DISK
McAfee	124.9%	273.5%	171.6%
Symantec	106.0%	114.1%	183%

Note: Based on resource consumption, figures in table represent the scaling/density improvement potential of Trend Micro vs. each competitor.
Nominal density refers to systems running a load that does not stress the AV.
True density refers to a load that drives the AV solution.

Source: Tolly, October 2010

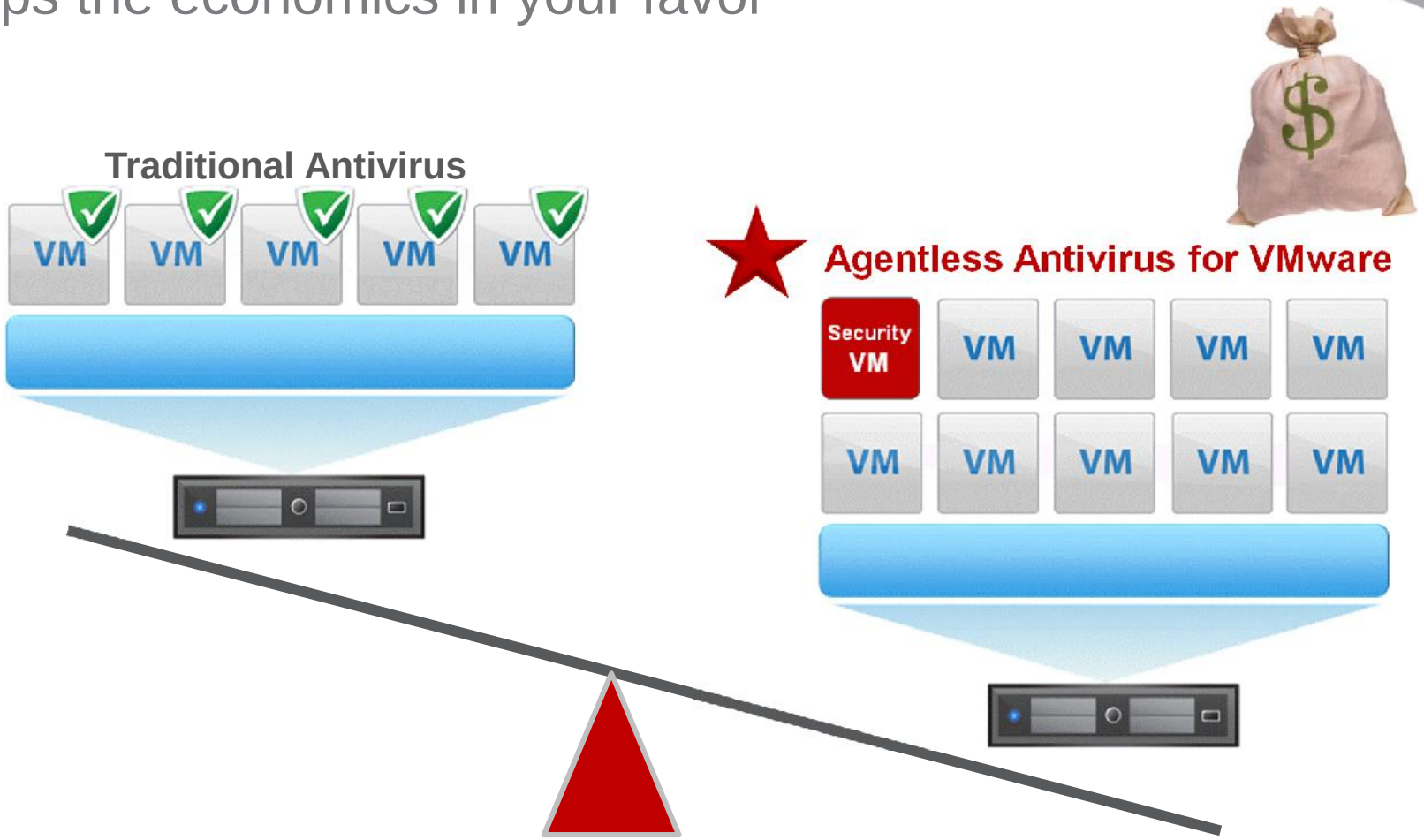
Table 5

Consolidation: Which one is better?



Agentless Security for VMware

Tips the economics in your favor



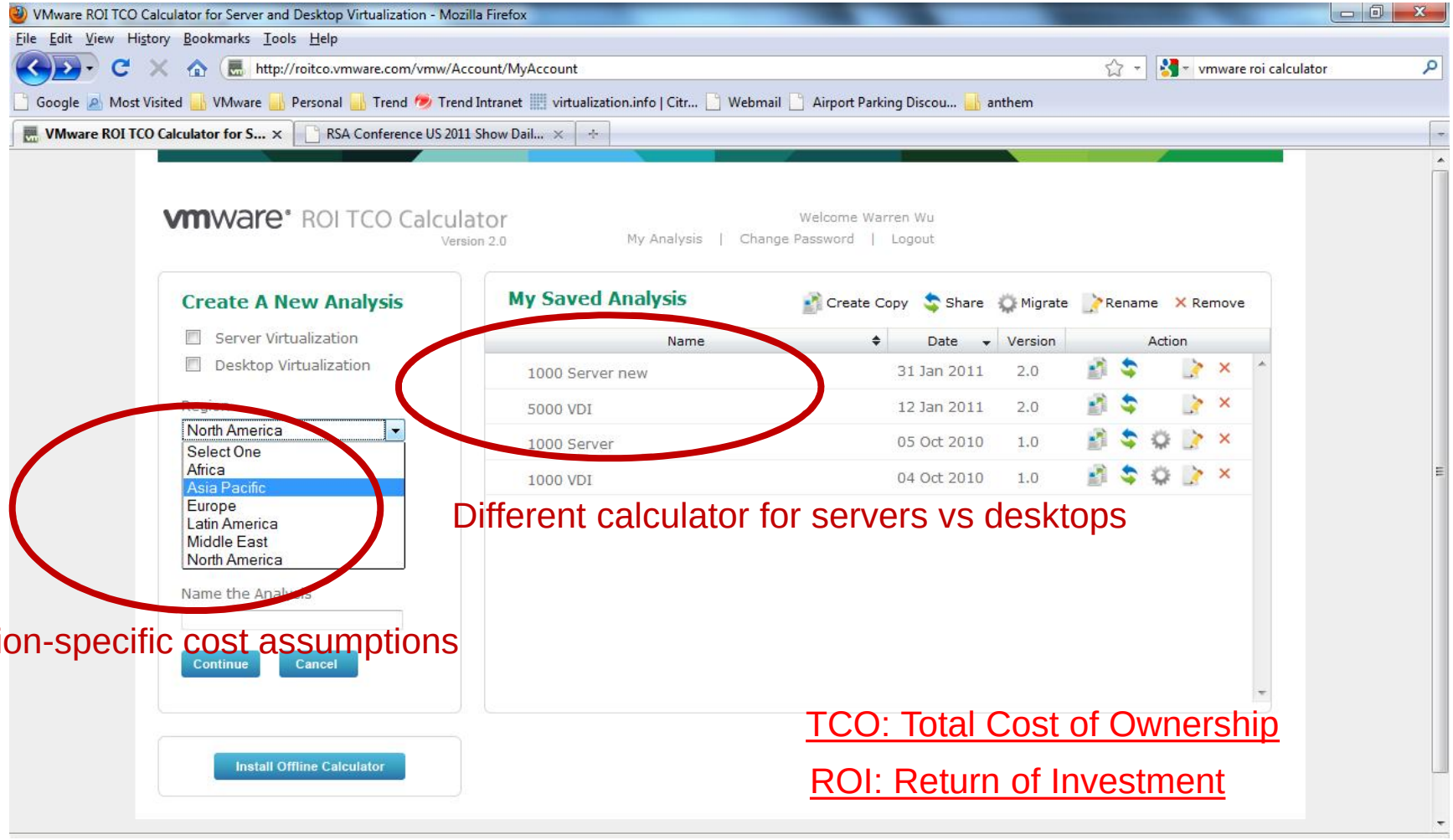
Improved Density means $$$ Saved

Desktop Virtualization TCO 1000 Virtual Desktops	With Trend Micro	With Traditional Antivirus
VDI Images per server	75	25
Servers Required to Host 1000 Virtual Desktops	14	40
Capex Savings for 1 server	$5900 (from VMware TCO Calculator)	
Power, Cooling & Rackspace Savings for 1 server over 3 years	$3600 (from VMware TCO Calculator)	
3-year savings for 1000 virtual desktops running Trend Micro	**$(5900+3600) X 26 fewer servers = $247,000**	

Similar savings accrue for server VM as well.
3-year savings for 600 server VMs running Trend Micro = $200,000

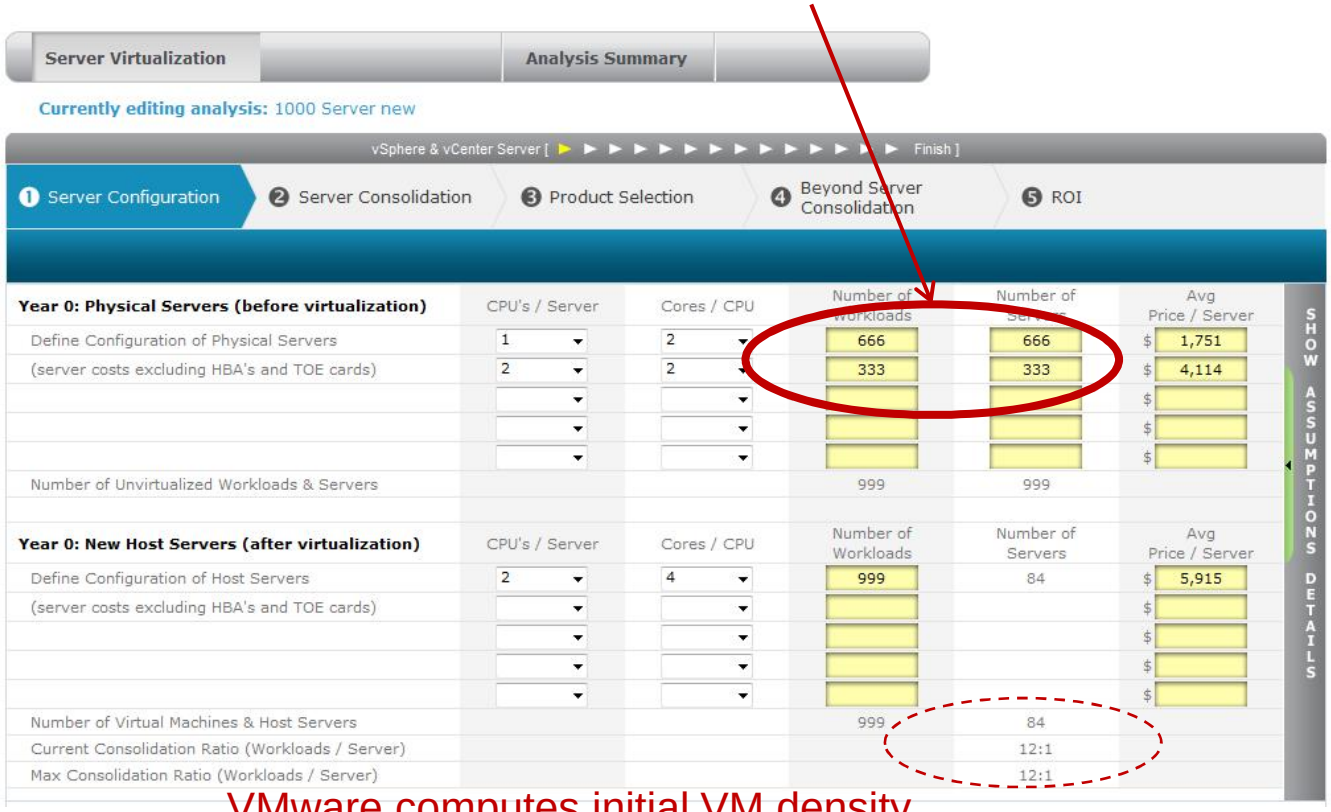
VMware Online ROI TCO Calculator

http://roitco.vmware.com - Transparent cost assumptions



VMware Consolidation Calculation

Only one input needed - # of servers or desktops to virtualize



Server Virtualization | Analysis Summary

Currently editing analysis: 1000 Server new

vSphere & vCenter Server [▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ Finish]

1 Server Configuration | 2 Server Consolidation | 3 Product Selection | 4 Beyond Server Consolidation | 5 ROI

Year 0: Physical Servers (before virtualization)	CPU's / Server	Cores / CPU	Number of Workloads	Number of Servers	Avg Price / Server
Define Configuration of Physical Servers	1	2	666	666	$ 1,751
(server costs excluding HBA's and TOE cards)	2	2	333	333	$ 4,114
					$
					$
					$
Number of Unvirtualized Workloads & Servers			999	999	

Year 0: New Host Servers (after virtualization)	CPU's / Server	Cores / CPU	Number of Workloads	Number of Servers	Avg Price / Server
Define Configuration of Host Servers	2	4	999	84	$ 5,915
(server costs excluding HBA's and TOE cards)					$
					$
					$
					$
Number of Virtual Machines & Host Servers			999	84	
Current Consolidation Ratio (Workloads / Server)				12:1	
Max Consolidation Ratio (Workloads / Server)				12:1	

SHOW ASSUMPTIONS DETAILS

VMware computes initial VM density

- VMware model (~1.5 VM's per core) may be higher than typical customer VM density – varies widely on age of hardware, type of workload
- 6:1, 12:1, 24:1, 80:1 server ratios all can be good, depends on # of HW sockets, cores
- Deep Security % savings valid at any starting consolidation ratio!

Dashboard Visibility

TREND MICRO DEEP SECURITY

Signed In As: admin | Help | Sign Out

vCenter - 10.0.1.24 and sub-groups (By Group)

Search

Advanced Search

New | Discover... | Export... | Preview

- Dashboard
- Alerts
- Reports
- Hosts
  - Laptops
  - Network Appliances
  - Servers
  - vCenter - 10.0.1.24
  - Workstations
- Security Profiles
- Firewall
  - Firewall Events
  - Firewall Rules
  - Stateful Configuratio
- Deep Packet Inspection
  - DPI Events
  - DPI Rules
  - Application Types
- Integrity Monitoring
  - Integrity Monitoring I
  - Integrity Monitoring I
- Log Inspection
  - Log Inspection Event
  - Log Inspection Rules
  - Log Inspection Deco
- Components
- System
  - System Events
  - System Settings
  - System Information
  - Tags
  - Scheduled Tasks
  - Roles
  - Users

Name	Platform	Security Profile	Status	Last Successful Update
Hosts > vCenter - 10.0.1.24 > Hosts and Clusters > Esxi-dev (4)				
10.10.1.107	VMware ESX 4.0.0 b	None	Unprepared	N/A
10.10.100.50	VMware ESXi 4.0.0 b	None	Prepared	N/A
10.10.100.60	VMware ESXi 4.0.0 b	None	Prepared	N/A
10.10.100.61	VMware ESXi 4.0.0 b	None	Prepared	N/A
Hosts > vCenter - 10.0.1.24 > Virtual Machines > Esxi-dev (17)				
asdf (710)	Suse Linux Enterpris	None	Unmanaged (VM Stopped)	N/A
dsva (10.10.1.150)	Debian 2.6	None	Multiple Errors	August 14, 2009 14:58
dsva (dsva50)	Suse Linux Enterpris	None	Unmanaged (VM Paused)	N/A
dsva (flygon)	Suse Linux Enterpris	None	Unmanaged (VM Paused)	N/A
gg_rc_xp32	Microsoft Windows 7	None	Unmanaged (VM Stopped)	N/A
j-k8-13	Microsoft Windows S	None	Unmanaged (VM Paused)	N/A
j-k8-21	Microsoft Windows S	None	Unmanaged (VM Stopped)	N/A
j-k8-7	Microsoft Windows S	None	Unmanaged (VM Stopped)	N/A
justin2k3	Microsoft Windows S	TESTTTTT	Update Pending (Offline)	August 14, 2009 17:02
justin2k3_2	Microsoft Windows S	None	Unmanaged (VM Stopped)	N/A
kb_sol10u7		None	Unmanaged (VM Stopped)	N/A
kbxu64_89		None	Unmanaged (VM Stopped)	N/A

	Appliance	Agent
Status:	Update Pending (Offline)	Update Pending (Offline)
Firewall:	**On, 1 rule**	**On, 1 rule**
DPI:	**Prevent, 2 rules**	**Prevent, 2 rules**
Integrity Monitoring:	Not Capable	On, 1 rule
Log Inspection:	Not Capable	On, 2 rules

ESX Server: 10.10.100.61

Appliance: dsva (10.10.1.150)

19 Alerts

TREND MICRO

Lợi ích của việc sử dụng Agentless và Virtual Appliance

- Tiết kiệm chi phí đầu tư cơ bản (ít server vật lý hơn → đầu tư ít hơn, nguồn và hạ tầng ít hơn), hệ số đầu tư ROI cao hơn (xem các trang về ROI TCO calculation sau đây hoặc vào http://roitco.vmware.com)
- Quản lý dễ dàng hơn (1 Deep Security manager có thể quản lý tới 100 Virtual Appliance), chi phí quản lý (ít đầu thiết bị hơn) sẽ dễ dàng hơn.
- Hệ thống được bảo vệ theo thời gian thực với tác dụng của Smart Protection Network
- Không cần config security cho VM khi di chuyển VM giữa các server (policy bám dính theo VM)
- Tiết kiệm chi phí nâng cấp software nếu sử dụng tính năng Virtual Patching, không cần restart server.
- Tiết kiệm chi phí do nâng cao hiệu suất khi không còn hiện tượng AV Storm

TREND MICRO

TREND MICRO
Securing Your Journey to the Cloud

SECURING YOUR JOURNEY TO THE CLOUD

physical. virtual. cloud.

TREND MICRO™ | Securing Your Journey to the Cloud

Ask Security? Ask Trend Micro!

Khôi Ngô, Country Manager

☎ **+84 913 225 486**

khoi_ngo@trendmicro.com

NETWORKWORLD® Reprint

Maximize your return on IT ■ www.networkworld.com March 7, 2011 ■ Volume 28, Number 5

CLEAR CHOICE TEST: VIRTUALIZATION SECURITY

New tools emerge to protect VMs

Testing reveals that no one product can do it all when it comes to VM security

BY DAVID STROM

As enterprises move toward virtualizing more of their servers and data center infrastructure, the security technologies that are plentiful and commonplace in the physical world become few and far between.

While few direct attacks on virtual machines

incorporated Blue Lane's software into its vShield

capabilities, they are not directly comparable. We developed a scorecard that indicates which vendors do a better job in various categories, but we're not naming an overall winner. In fact, a few of these vendors have teamed up to provide combined solutions. This coupled with the active mergers mentioned above means that this is a very dynamic category and you should expect further consolidations and changes.

TREND MICRO

NETRESULTS

Product name	Power Broker	vSecurity	HyTrust Appliance	Virtual Management Center	Deep Security
Company	BeyondTrust Software	Catbird Networks	HyTrust	Reflex Systems	Trend Micro
Price	Starts at $1,600 per server (plus maintenance).	$1,995/socket.	$1,000/host.	Each protective module is $600/socket.	$200/VM for anti-malware, $1,100/ VM for all protective modules.
Pros	Root password protection of hosts.	Complex network protective features based on industry	Solid access controls and simple setup.	Comprehensive set of security solutions across a wide feature set.	Reports that are clear and actionable and suitable for management.
Cons	Command line interfa requires custom script			e a	Compliance is skimpy.
Total score	3.375				4.25

SCORECARD

Product	Deep Security	HyTrust Appliance	Virtual Mgmt. Center	Power Broker	vSecurity
Reporting (25%)	4.5	3.5	3	3	3
Host management (25%)	4	4	4.5	3	3
Policy Controls (25%)	4	4	4	3.5	4
User Management (25%)	4.5	4.5	4.5	4	2
Total	4.25	3.875	4.0	3.375	3.0

SCORING KEY: 5: EXCEPTIONAL; 4: VERY GOOD; 3: AVERAGE; 2: BELOW AVERAGE; 1: SUBPAR OR NOT AVAILABLE

FEATURESSUMMA

Product, Version	URL, Pric				Notable Features
BeyondTrust PowerBroker v6.2	Beyondtrus $1,600/ser				Root ESX password protection
Catbird vSecurity 3.5	Catbird.com $1,995/per socket	Yes	ESX/ESXi all v3.5 and v4.; Citrix Xen	Compliance, Firewall/IDS	Deep inspection rules
HyTrust Appliance v2.1.2	Hytrust.com $1,000/host	No	ESX/ESXi all v3.5 and v4.	Access control, compliance	Root ESX password protection
Reflex Systems v2.9	Reflexsystems.com $1,800/per socket	Yes	ESX only, all v3.5 and v4.	Access, Compliance, Firewall/IDS	Topo map, network zones, change tracking
Trend Micro Deep Security v7.5	Trendmicro.com $1,100/VM	Either	ESX/ESXi all v3.5 and v4; and VMsafe	Antivirus, Firewall/ IDS, Compliance	Deep inspection rules, reports

Back up slides for PCI DSS 2.0

PCI DSS 2.0 Virtualization Guidelines

PCI DSS 2.0 Virtualization Guideline	Required Controls
1. Hypervisor environment is in scope - Hypervisor and supporting components must be hardened - Security patches applied ASAP - Logging/monitoring of hypervisor events	**Deep Security DPI and FIM** - Virtual Patching Prevents VMs from being compromised to attack hypervisor - FIM checks the integrity of vSphere utilizing Intel TPM/TXT
2. One function per server - Physical servers had the same requirement, no change in behavior	**Deep Security Firewall** - Firewall ensures only requires ports and protocols are accessible
3. Separation of duty - Consider multi-factor authentication - Access controls for both local and remote should be accessed - Review and monitor RBAC controls - Enforce least privilege where possible	**Deep Security Manager** - Support for RBAC enables separation of duty of security policies
4. Mixing VM's of different trust levels - In order for in-scope and out-of-scope VMs to co-exist on the same hypervisor the VMs must be isolated from each other	**Deep Security Firewall and IDS/IPS** - A combination of VLAN and per VM firewall and IDS/IPS provides the isolation and visibility into inter-VM traffic required

TREND MICRO

PCI DSS 2.0 Virtualization Guidelines

PCI DSS 2.0 Virtualization Guideline	Required Controls
5. Dormant VMs and VM snapshots - Access should be restricted - Ensure that only authorized VMs are added and removed - Recognize that VMs are dynamic and state cannot be assumed	**Deep Security Agentless DPI & AV** - Automated VM discovery via real-time integration w/ vCenter - Dormant VMs are protected by the Virtual Appliance when first powered on eliminating 'stale' protection policies
6. Immaturity of monitoring solutions - Traditional tools do not monitor inter-VM traffic - Virtualization tools are still immature compared to their physical counterparts	**Deep Security IDS/IPS, FIM & LI** - Deep Security IDS/IPS provides visibility into inter-VM traffic - Integrity Monitoring provides visibility into unauthorized changes to guest-VMs and the hypervisor - Log Inspection provides visibility into security events occurring to guest-VMs
7. Information leakage - Increased risk of information leakage between logical network segments & between logical components	**Deep Security (all modules)** - IDS/IPS, FIM and Log Inspection provides visibility as shown in #6 above - Firewall reduces the VMs attack surface

PCI DSS 2.0 Virtualization Guidelines

PCI DSS 2.0 Virtualization Guideline	Required Controls
8. Defense in depth - Traditional security appliances cannot protect virtual - Traditional agent-based security products can impact performance	**Deep Security (all modules)** - Automated VM discovery via real-time integration w/ vCenter & new VMs are auto-protected w/ a default security profile - Protection for physical, server VMs, VDI, hybrid cloud, and public cloud
9. VM Hardening - Harden VMs (OS & Apps) by disabling unnecessary services, ports, interfaces, and devices - Send logs off-board in near real-time - Establish limits on VM resource usage	**Deep Security and VMware** - IDS/IPS & firewall hardens VMs - Integrity Monitoring provides visibility into unauthorized changes to guest-VMs - Log Inspection provides visibility into security events occurring to guest-VMs & forwards in real-time
10. Cloud Computing - Cloud service provider must provide sufficient assurance that the scope of PCI compliance is sufficient - Customer is required to provide additional necessary controls	**Deep Security and SecureCloud** - Deep Security protects VMs in enterprise, hybrid cloud and public cloud environments - SecureCloud provides encryption services independent of cloud provider ensuring only authorized personnel can access the data