TREND MICRO

Securing Your Journey to the Cloud

An toàn thông tin cho môi trường ảo hoá và điện toán đám mây

Khoi Ngo • Country Sales Manager

Trend Micro Vietnam

Nội dung

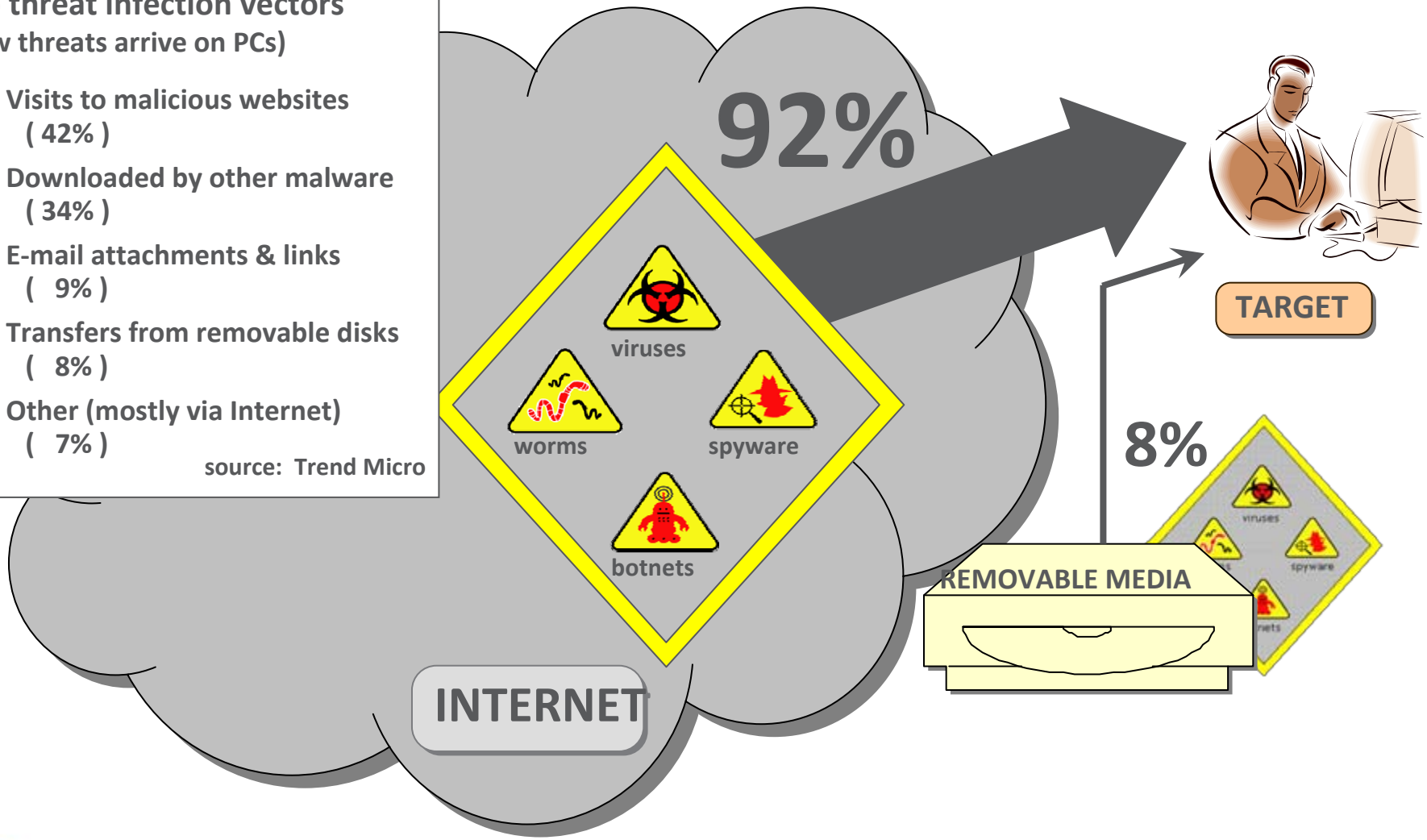
1. **Quan điểm mới về An toàn thông tin với điện toán đám mây: ngăn chặn hiểm hoạ trước khi tới được máy tính với thông tin nhận dạng cập nhật từ đám mây.**
2. An toàn thông tin với môi trường ảo hoá: những vấn đề tiềm ẩn và giải pháp.
3. Chọn giải pháp an toàn thông tin cho các hệ thống ảo hoá để giảm chi phí quản lý và tăng hệ số đầu tư (ROI).

Ngày nay, hầu hết hiểm hoạ đến từ Internet

Top threat infection vectors
(how threats arrive on PCs)

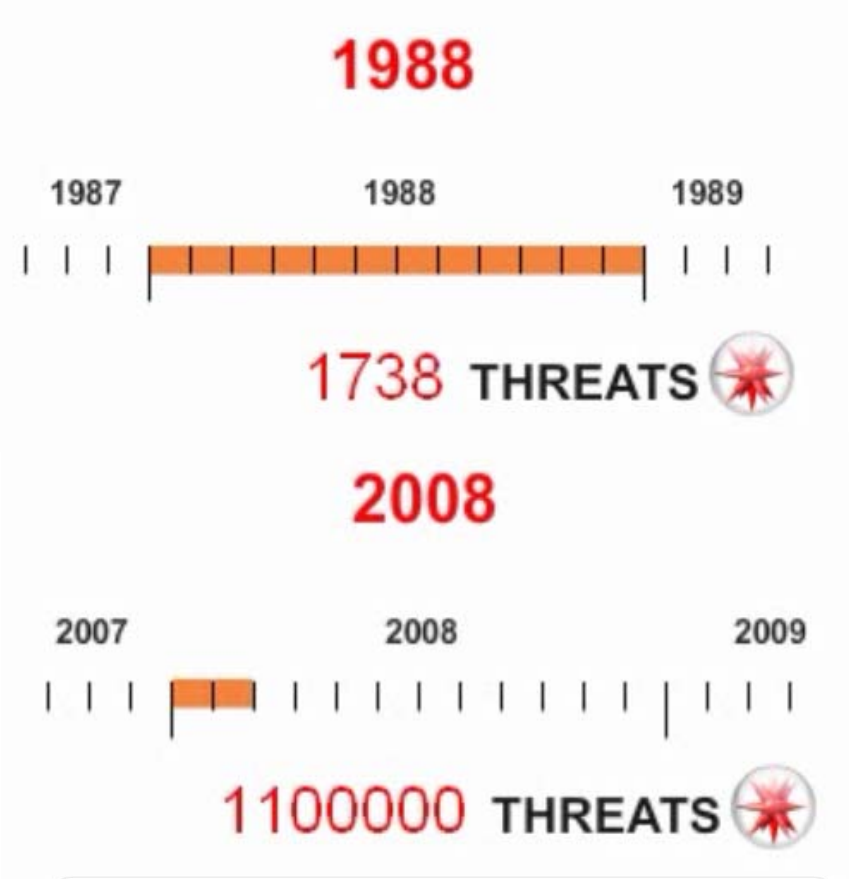
1. Visits to malicious websites (42%)
2. Downloaded by other malware (34%)
3. E-mail attachments & links (9%)
4. Transfers from removable disks (8%)
5. Other (mostly via Internet) (7%)

source: Trend Micro



TREND MICRO

Mã độc, virus, malware, spyware…



Malware chiếm 90% các mã độc ghi nhận được

—2009 Verizon Security Report

TrendLab 2010: 3 biến thể mới/1.5 giây…

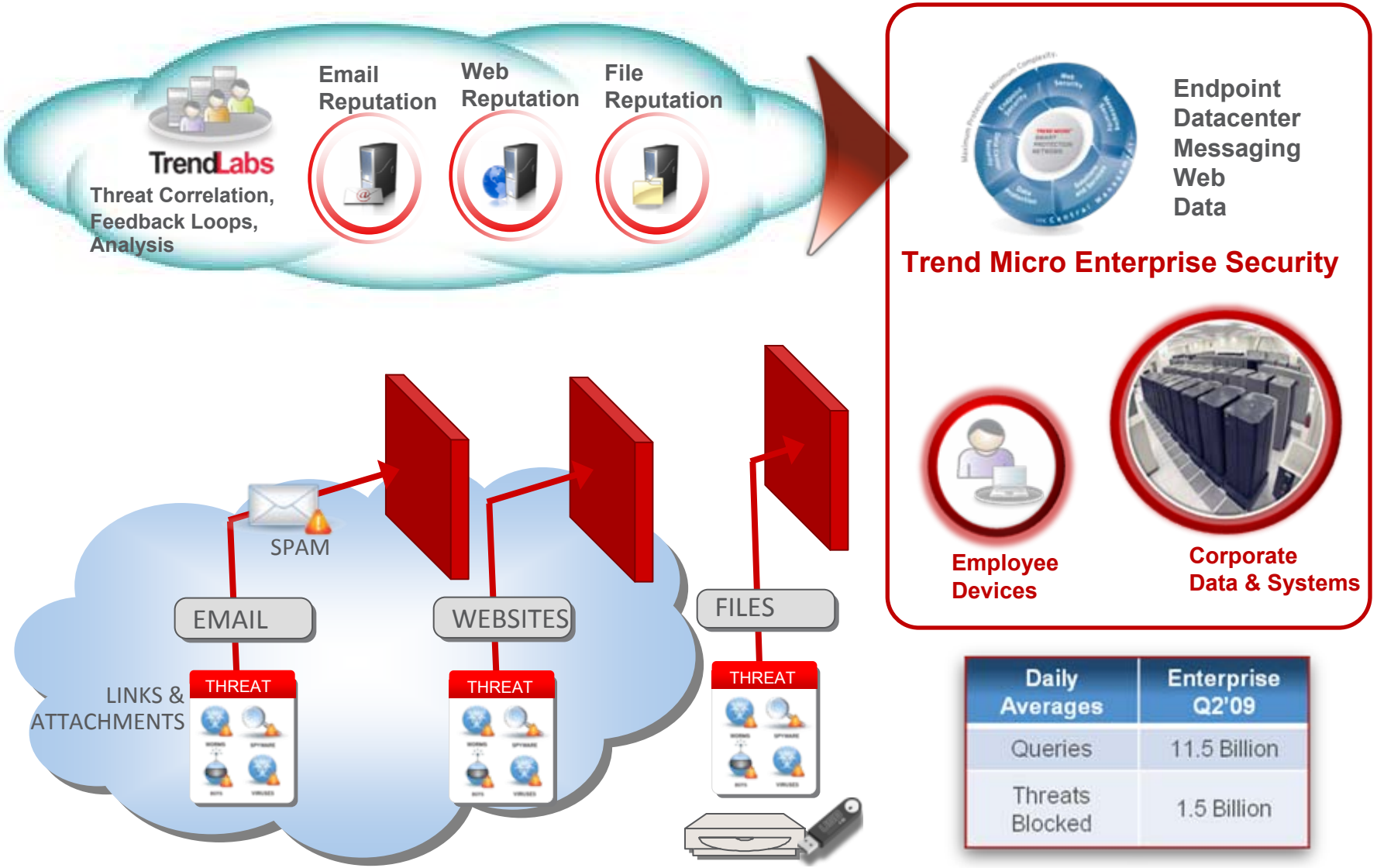
>225,000

malware mới mỗi ngày…

TREND MICRO

TREND MICRO™
SMART
PROTECTION
NETWORK

The Smart Protection Network



Daily Averages	Enterprise Q2'09
Queries	11.5 Billion
Threats Blocked	1.5 Billion

Bảo vệ khách hàng tốt hơn!

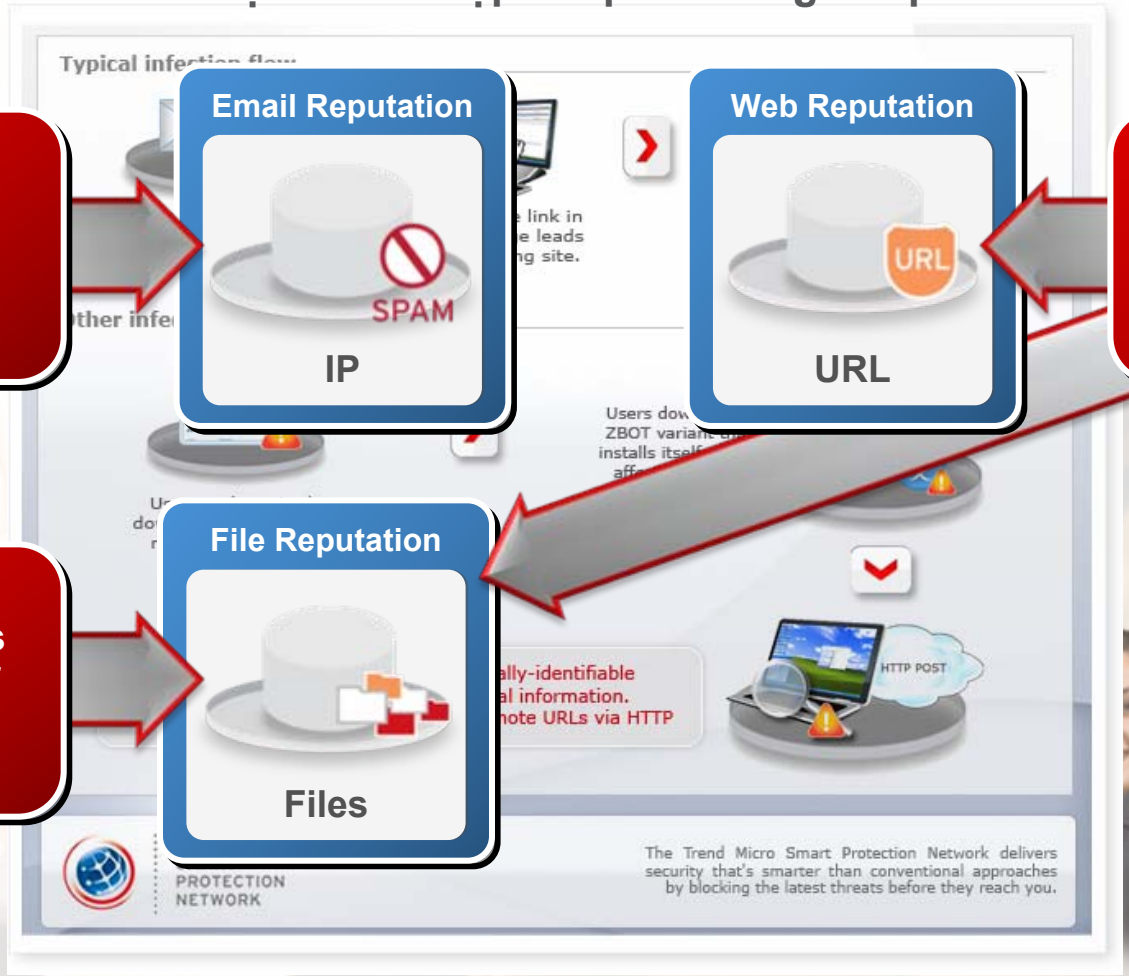
Trend Micro: Mã độc bị nhận dạng ngăn chặn trước khi đến được máy tính của bạn

Quan điểm cũ: cho mã độc thâm nhập và quét chúng với pattern file

ERS blocks spammed emails

FRS detects and prevents download of malicious binary files

WRS prevents access to malicious URLs



TREND MICRO

Trend Micro Enterprise Security

Endpoint Security
PC, Laptop, Mobile Device Security
Extensive Platform/OS Support
Unified Security & Systems Mgt

Web Security
Web Gateway Security
Website Security

Messaging Security
Email Gateway Security
Mail & Collaboration
Server Security

Data Center Security
Business Server Security
Protection, Integrity, Compliance
Physical/Virtual/Cloud Computing

Solutions & Services
Regulatory Compliance
Threat Management Services
Premium Support Service & more

Data Protection
Data Loss Prevention
Email & Endpoint Encryption

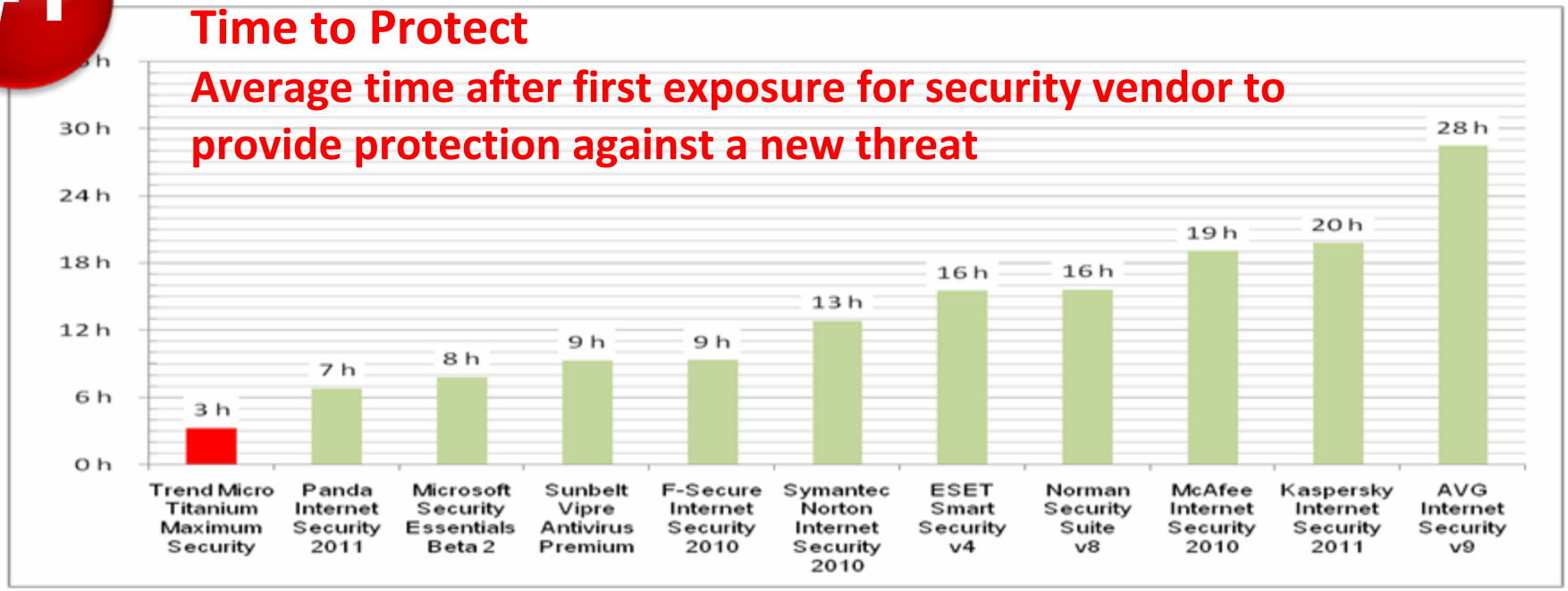
Central Management
Centralized Security Mgt
Unified Security & Systems Mgt

TREND MICRO

Thời gian đưa ra bản vá cho mã độc mới

Titanium is faster than any of its competitors at providing protection against newly identified web threats.

#1



source: NSS Labs Report, "Endpoint Protection Products Test Report for Socially Engineered Malware", September 2010

FAST

Automatically update PC with latest virus definition files, Real-Time Protection in the Cloud

Malware bị phát hiện và ngăn chặn trước khi phát tác

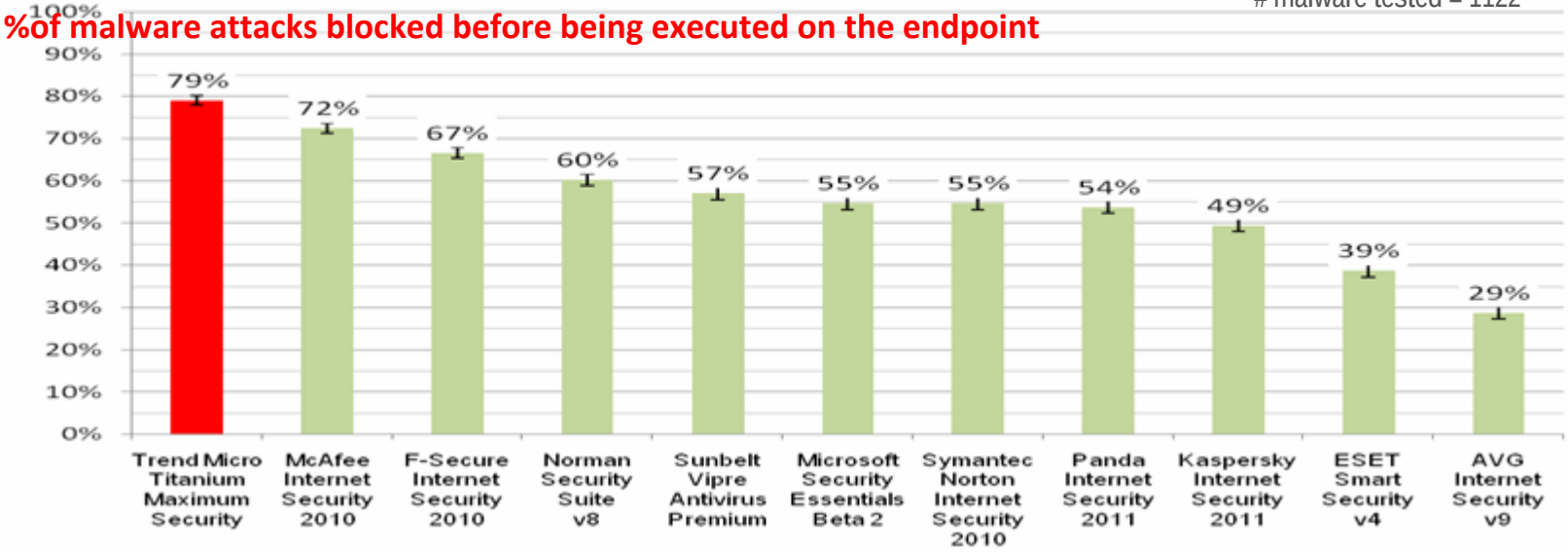
Titanium is the best at catching web threats before they execute on a user's computer

#1

Malware Caught before Execution

error bars are 95% confidence interval for number of malware tested
malware tested = 1122

%of malware attacks blocked before being executed on the endpoint



source: NSS Labs Report, "Endpoint Protection Products Test Report for Socially Engineered Malware", September 2010

SAFE

#1 in detecting and providing Protection against new threats

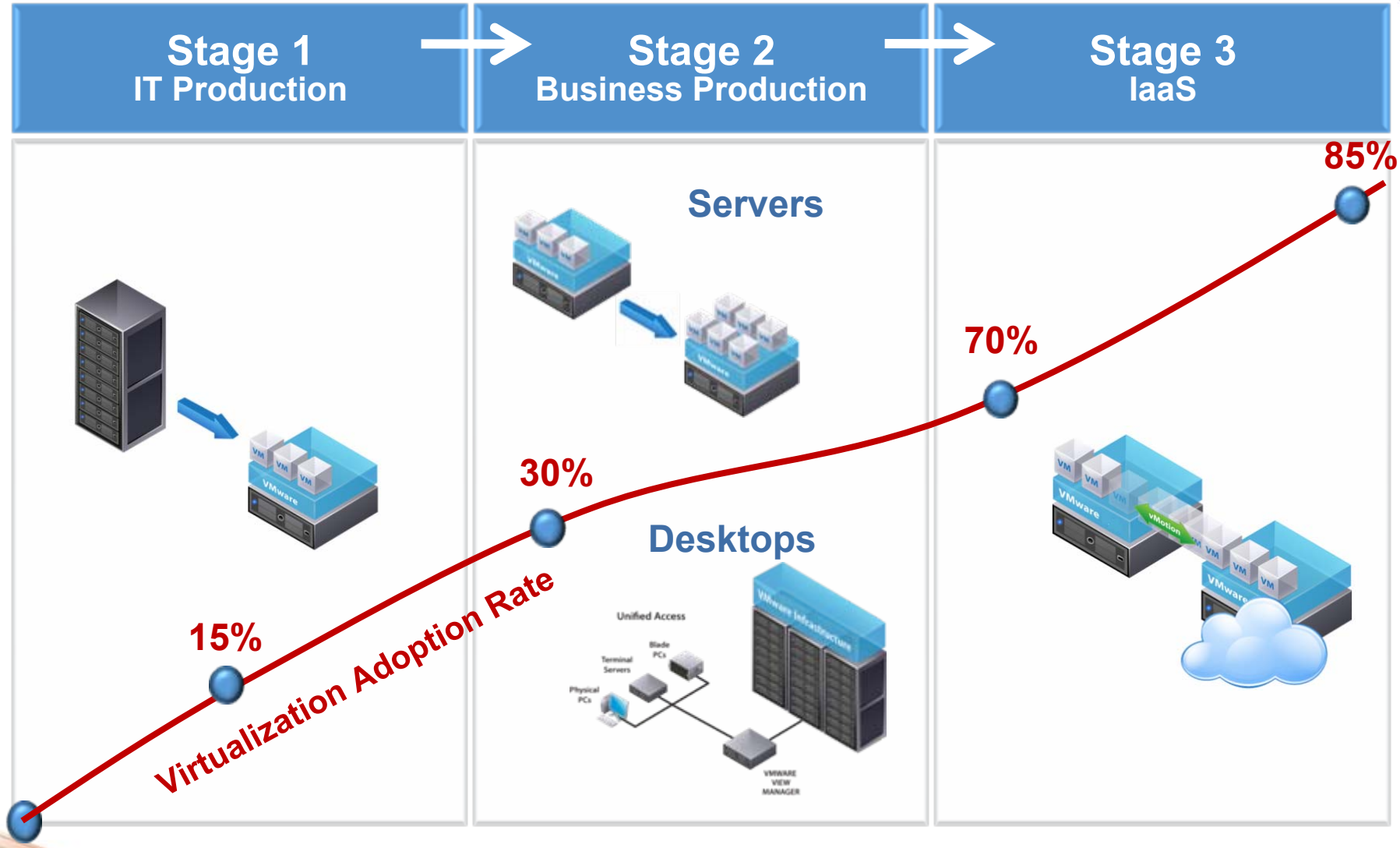
Nội dung

1. Quan điểm mới về An toàn thông tin với điện toán đám mây: ngăn chặn hiểm hoạ trước khi tới được máy tính với thông tin nhận dạng cập nhật từ đám mây.

2. **An toàn thông tin với môi trường ảo hoá: những vấn đề tiềm ẩn và giải pháp.**

3. Chọn giải pháp an toàn thông tin cho các hệ thống ảo hoá để giảm chi phí quản lý và tăng hệ số đầu tư (ROI).

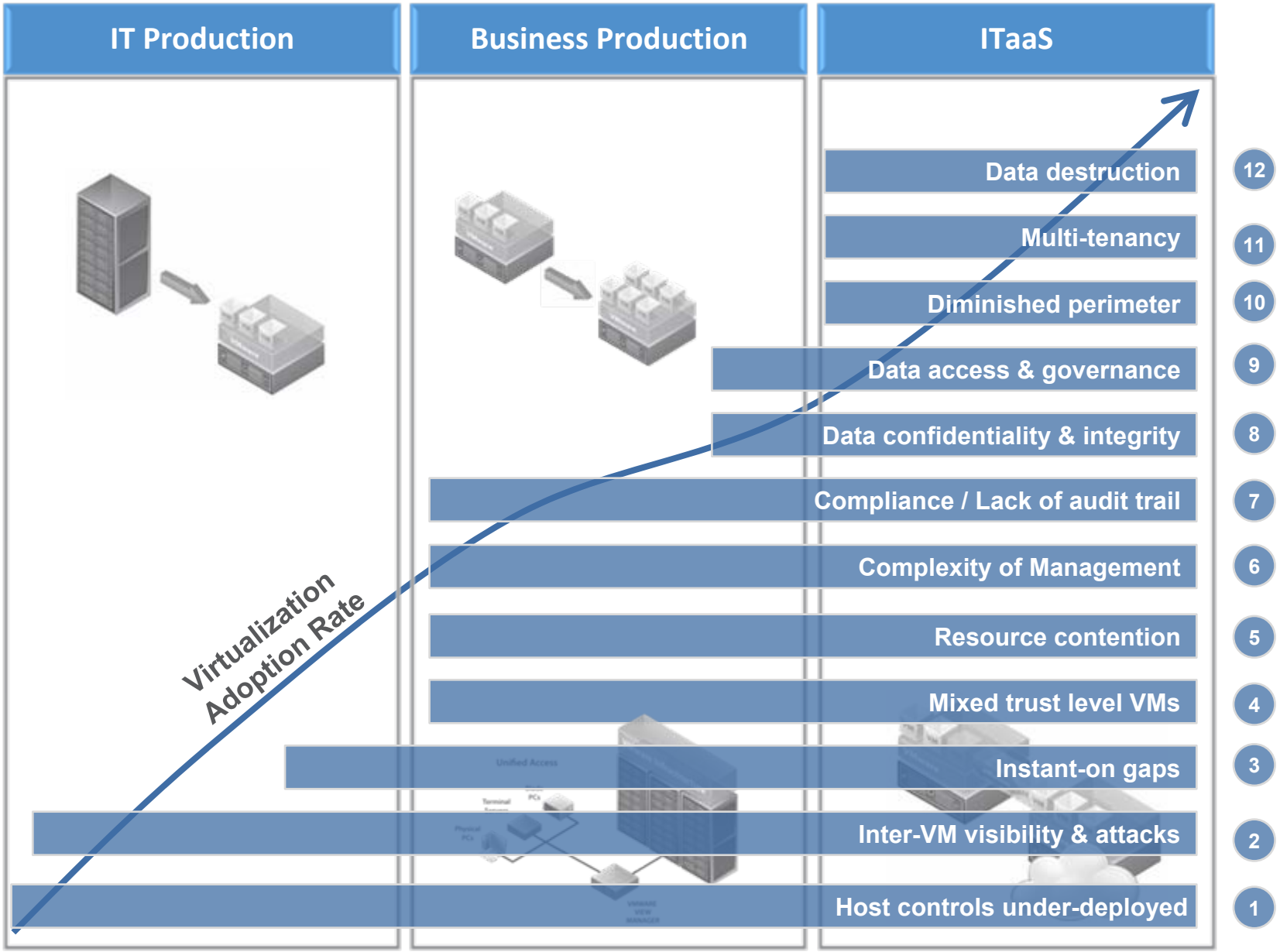
Những giai đoạn của lộ trình ảo hoá



TREND MICRO

Những thách thức về an toàn thông tin trên lộ trình ảo hoá

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



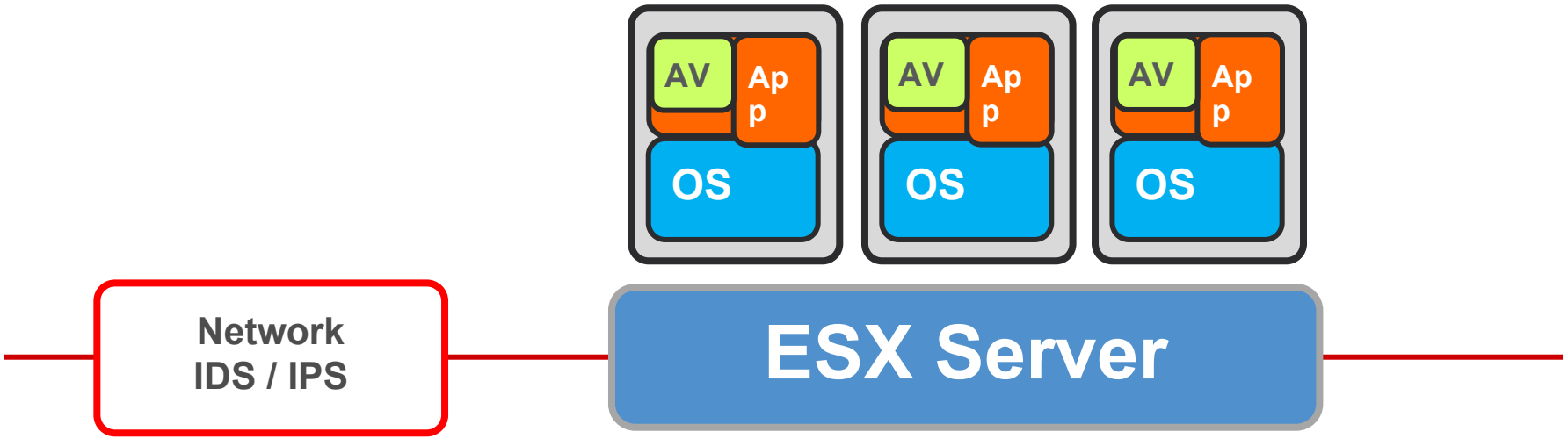
Security Challenges Defined

(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

Securing Servers the Traditional Way

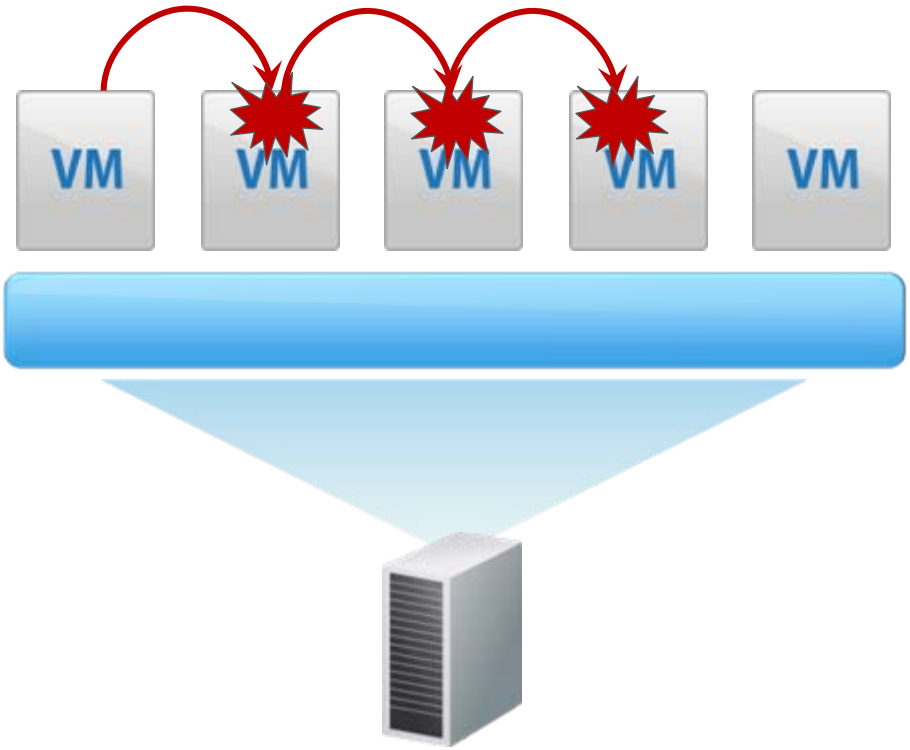


- Anti-virus: Local, agent-based protection in the VM
- IDS / IPS : Network-based device or software solution

TREND MICRO

Tấn công giữa các VM cùng server vật lý

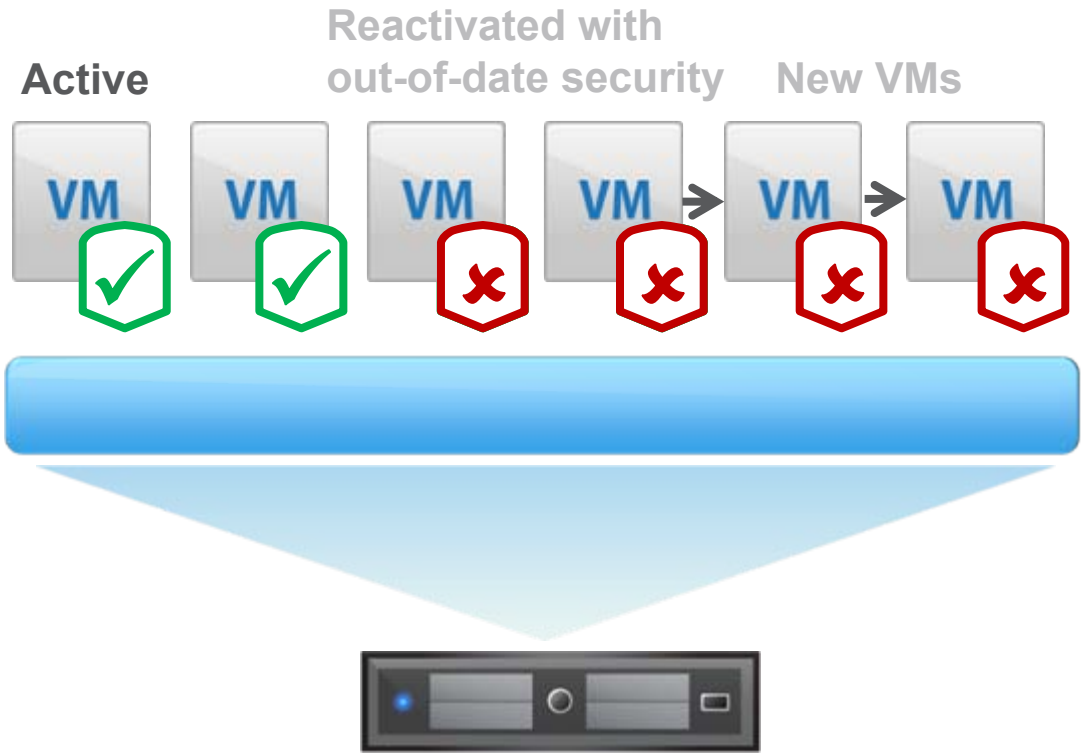
1 Inter-VM attacks



TREND MICRO

Lỗ hổng an ninh của các VM activate/inactivate/ dormant/newly added…

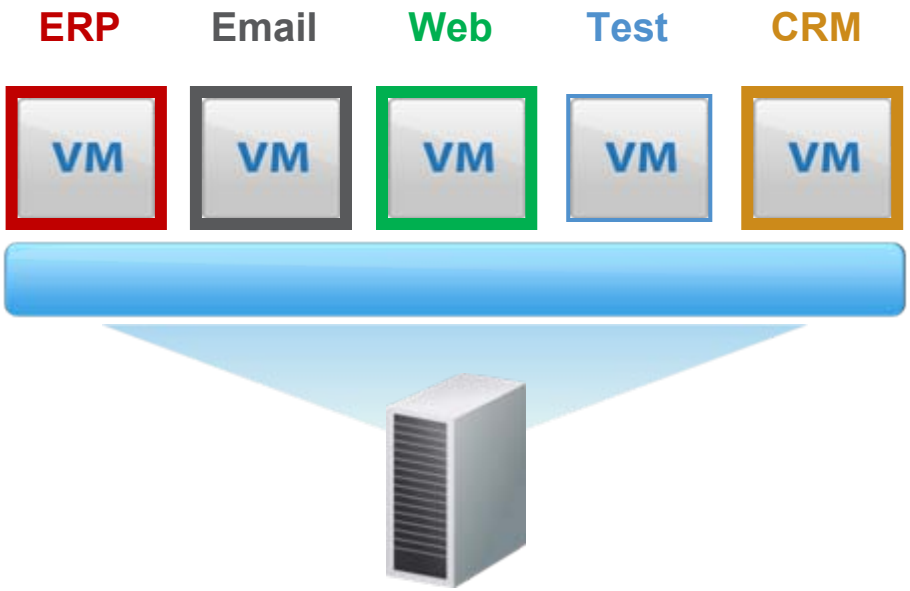
2 Instant-on gaps



TREND MICRO

Chênh lệch về mức độ bảo mật và quản lý giữa các VM cùng server vật lý

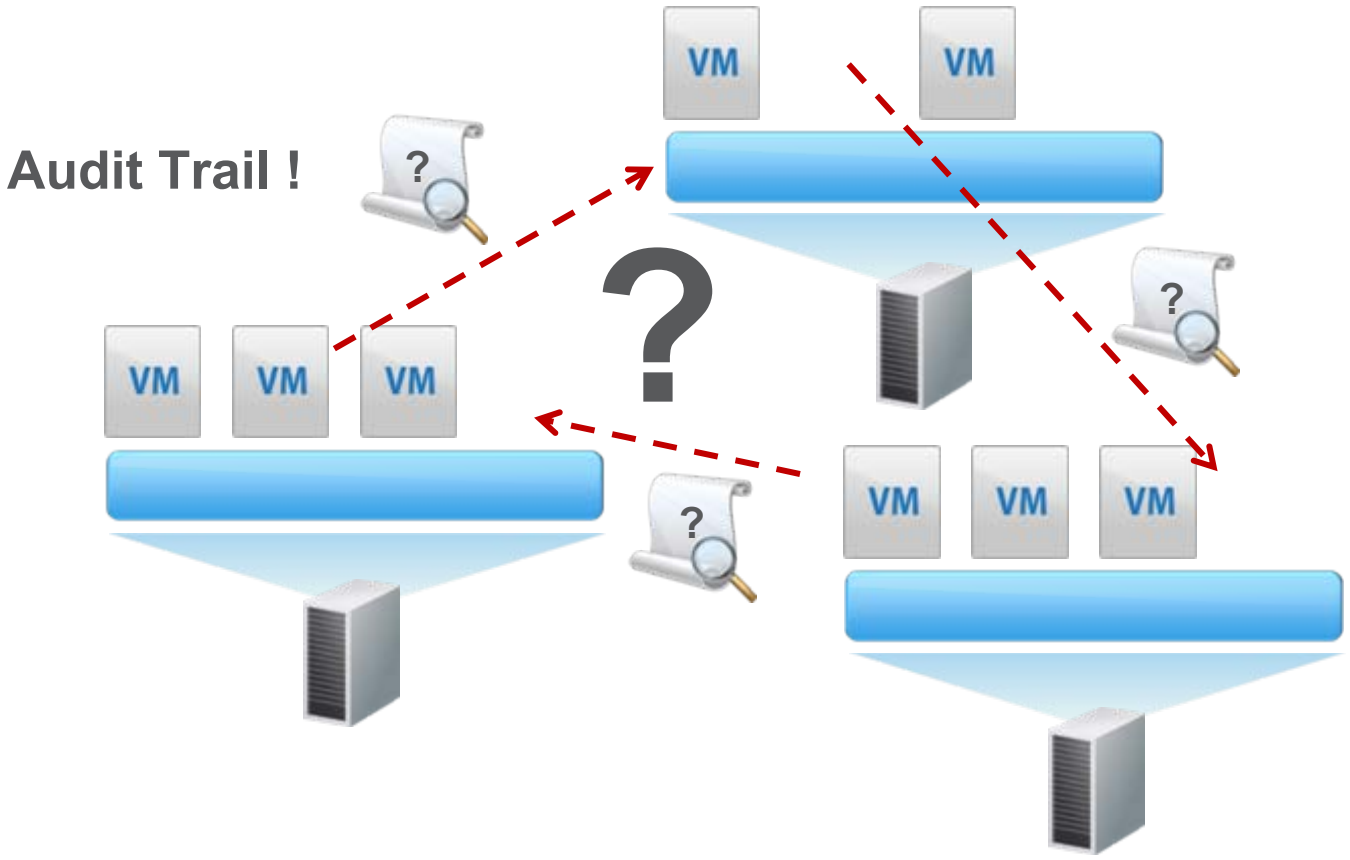
3 Mixed trust level VMs



TREND MICRO

Quá nhiều chuẩn bảo mật cần tuân thủ

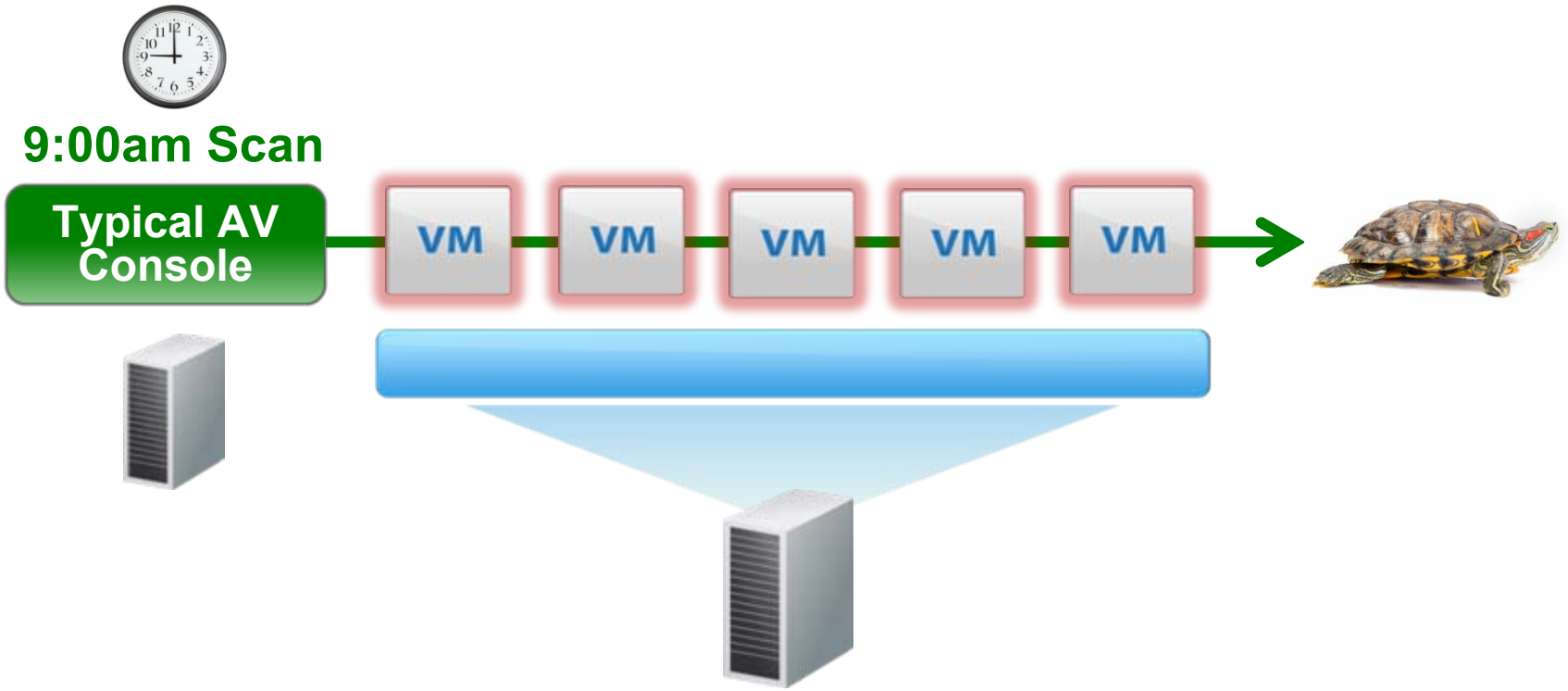
4 Compliance



TREND MICRO

Tiêu thụ đáng kể nguồn lực của server

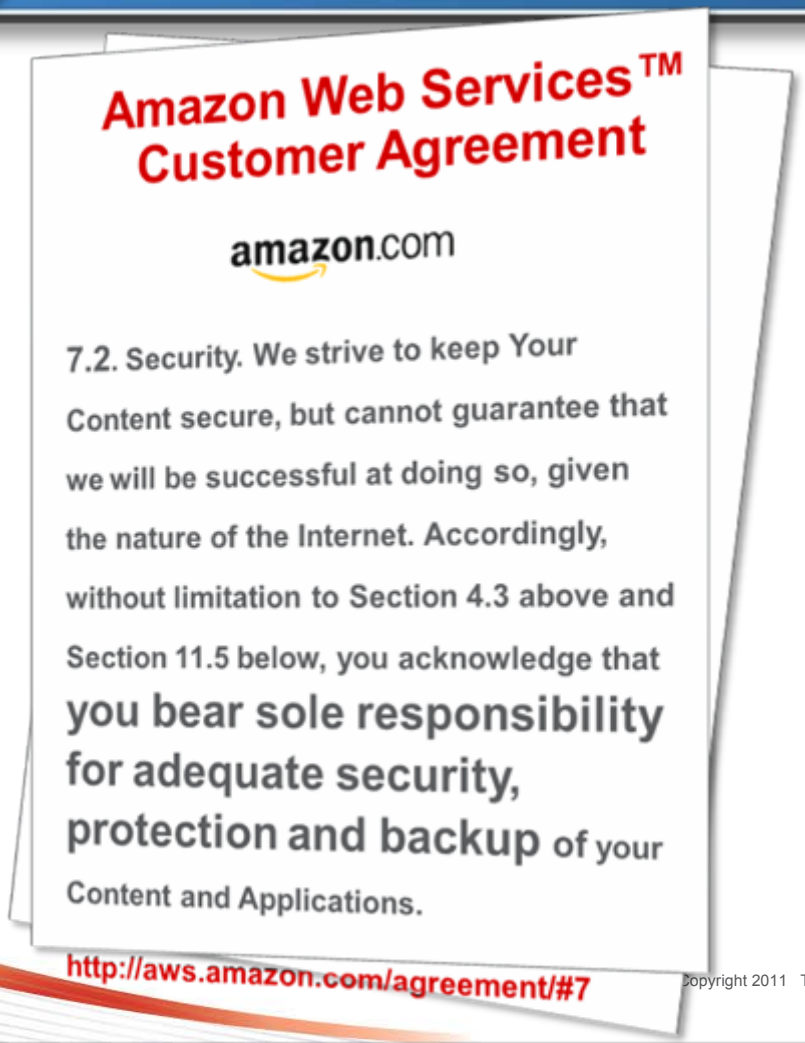
5 Resource contention



TREND MICRO

Rủi ro về an ninh thuộc về khách hàng sử dụng dịch vụ của "đám mây"

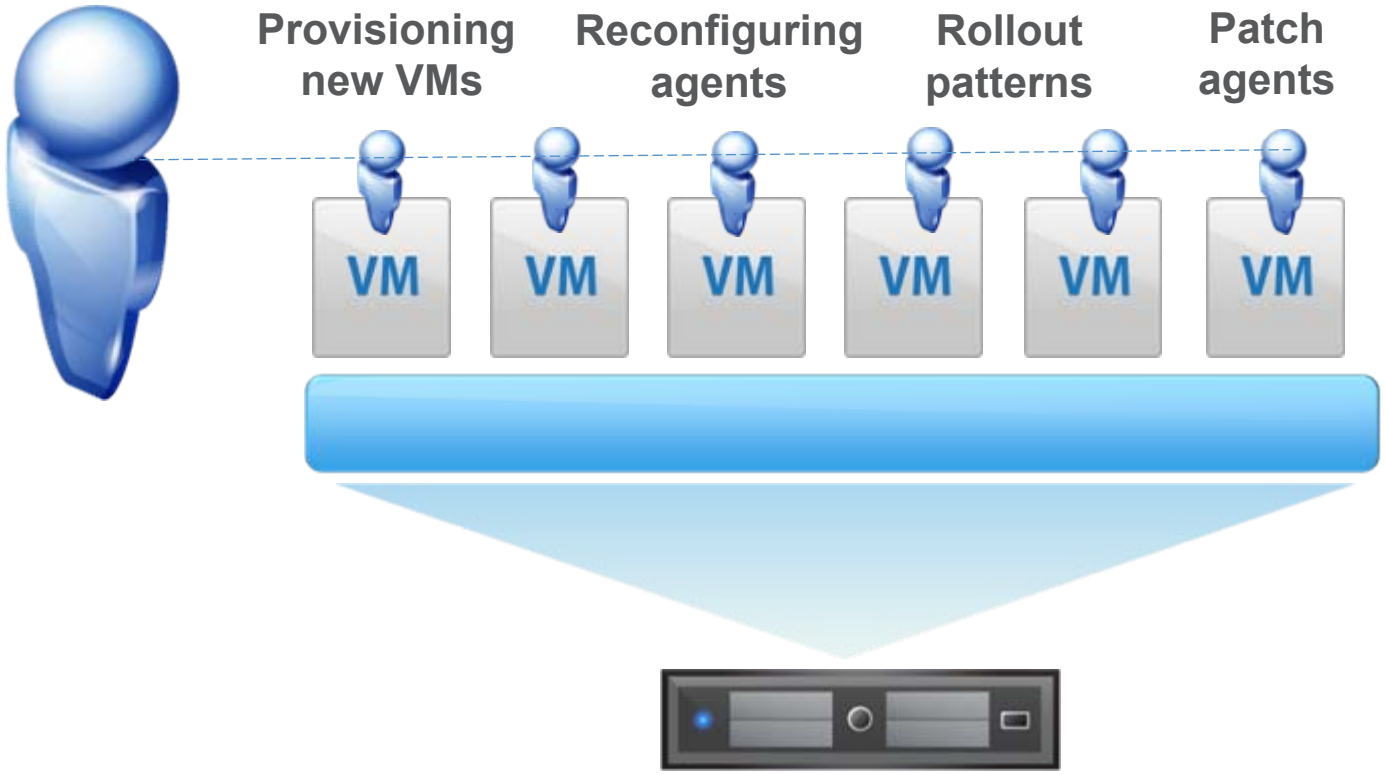
6 Data confidentiality and integrity



The cloud user is responsible for security, and needs to plan accordingly.

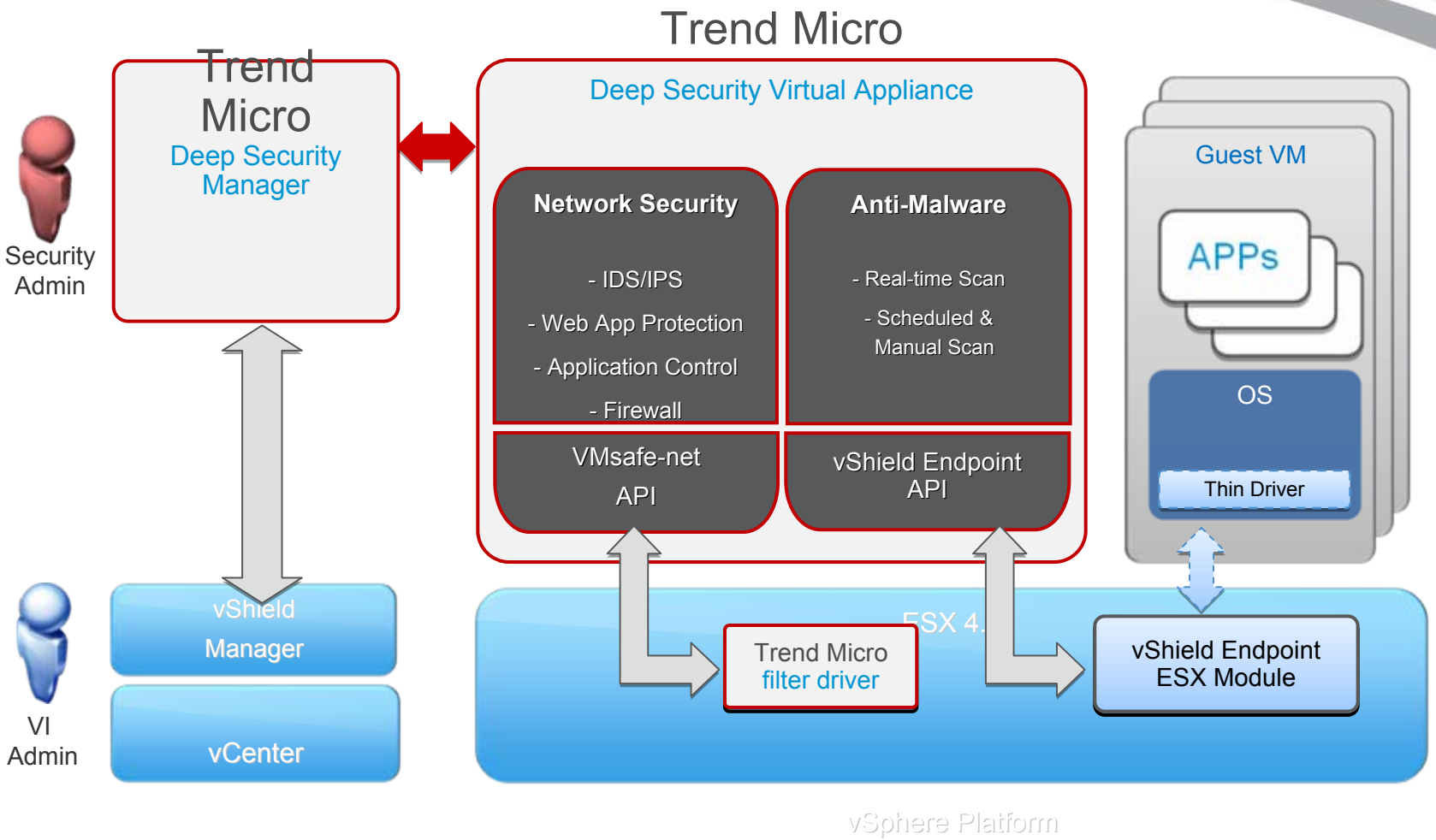
TREND MICRO

7 Complexity of Management



TREND MICRO

Agent-less Security Architecture

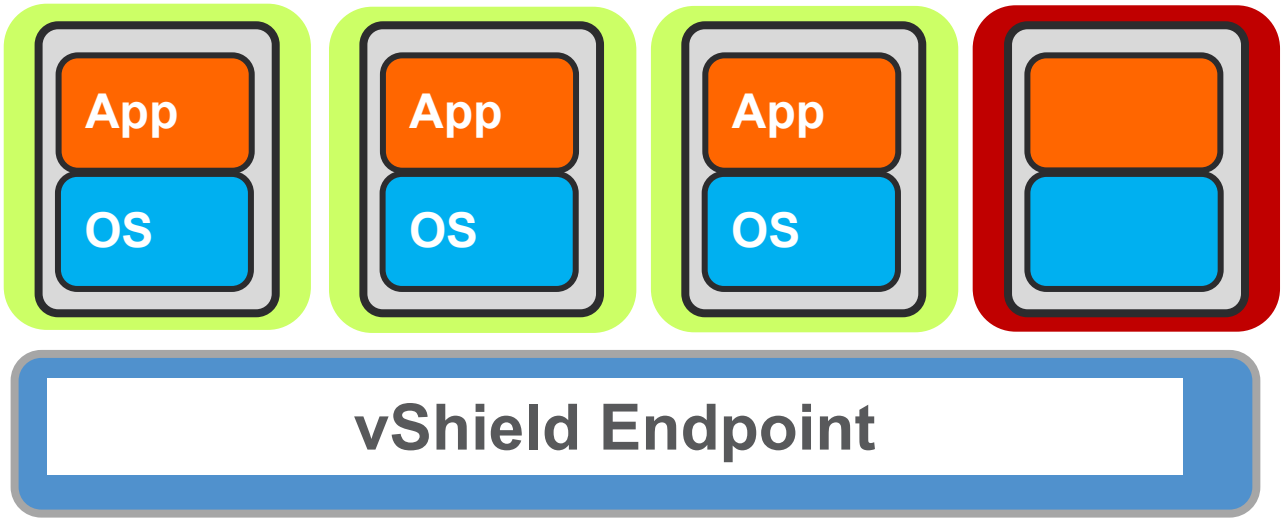


Legend →

Trend Micro product components	VMware Platform	vShield Endpoint Components

TREND MICRO

Hypervisor-Powered Security Architectures

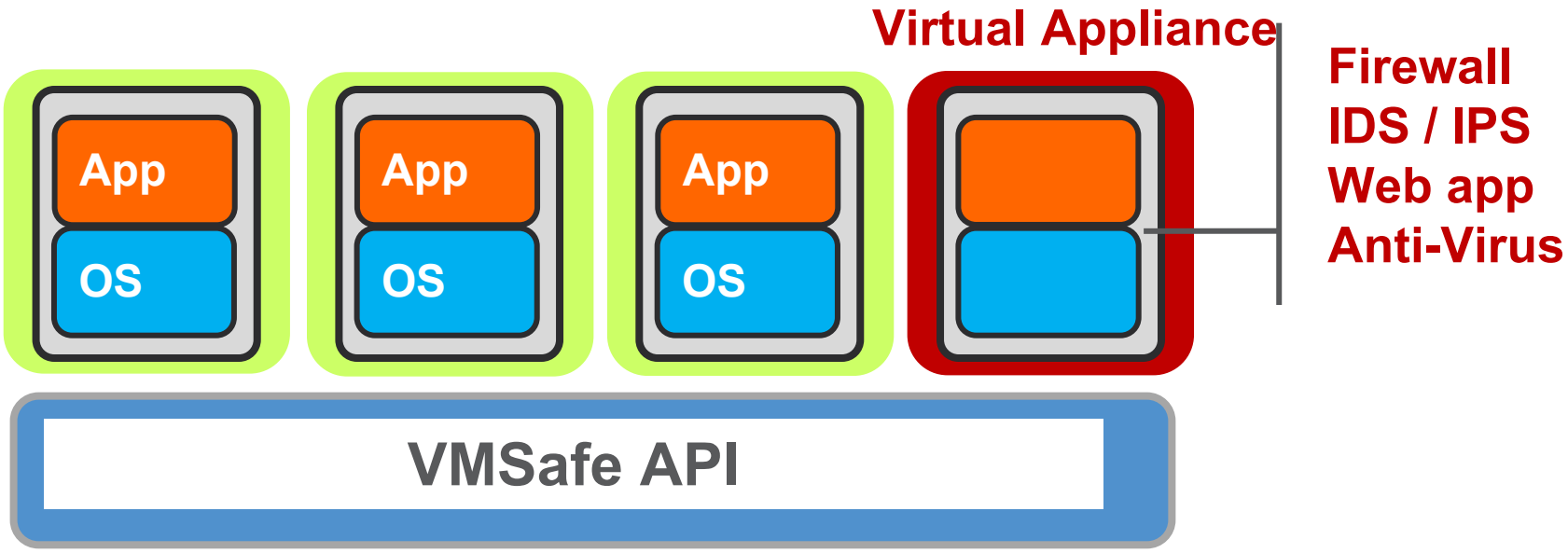


Anti-virus Virtual Appliance

- 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

TREND MICRO

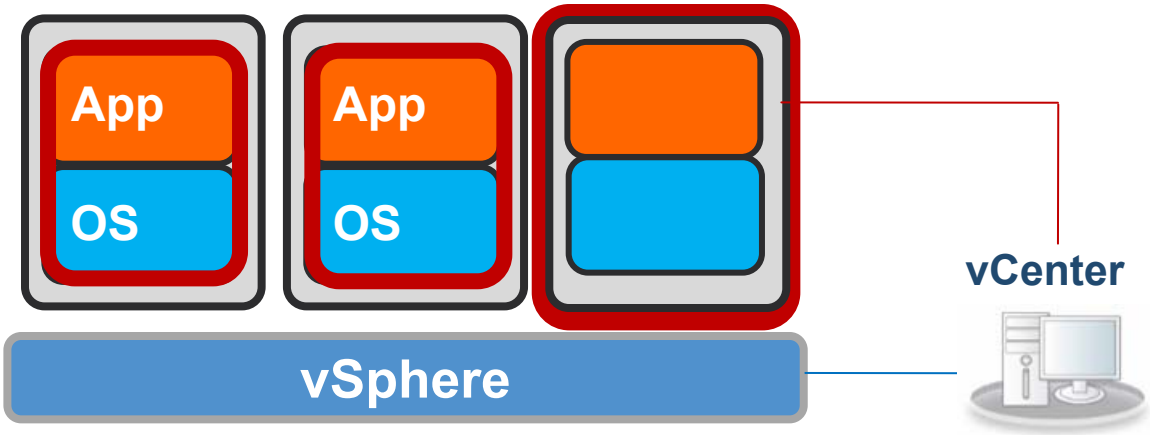
Hypervisor-Powered Security Architectures



- VMsafe enables you to supplement perimeter defense
- Agentless IDS/IPS, Firewall and application protection

TREND MICRO

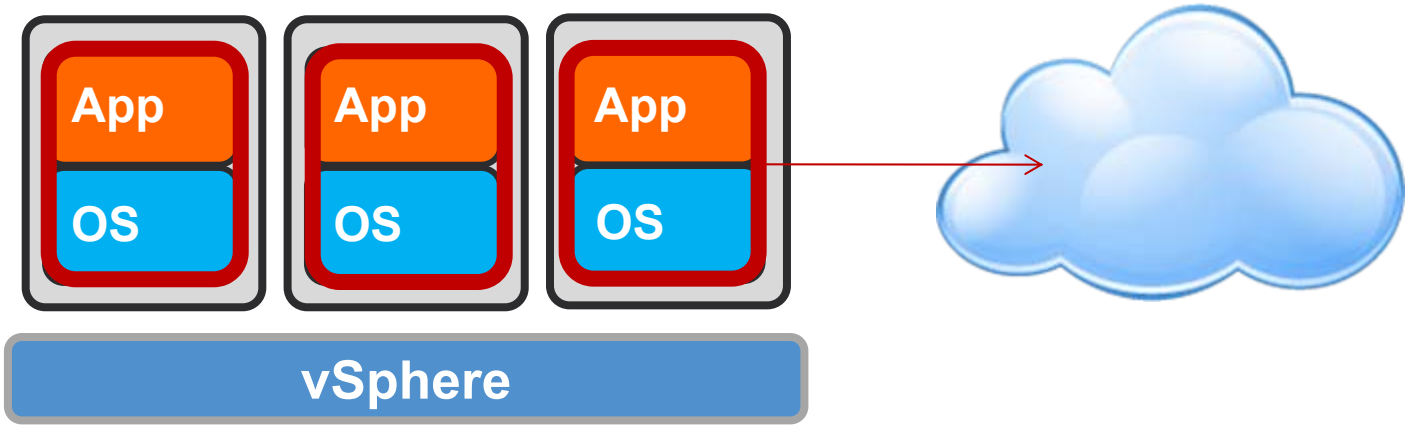
Virtualisation-aware agents



- vCenter integration makes security Virtualisation-aware
- V-aware agents complement virtual appliance
- Use cases: offline desktops, compliance, defense in depth

TREND MICRO

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

TREND MICRO

Deep Security Summary

vmware TREND MICRO DEEP SECURITY

Agentless 1

vShield Endpoint — Antivirus

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

Agentless 2

VMsafe APIs — IDS / IPS; Web Application Protection; Application Control; Firewall

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*)*

Agent-based 3

Integrity Monitoring

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

Agent-based 4

Log Inspection

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

(PCI*): Help

TREND MICRO

Nội dung

1. Quan điểm mới về An toàn thông tin với điện toán đám mây: ngăn chặn hiểm hoạ trước khi tới được máy tính với thông tin nhận dạng cập nhật từ đám mây.

2. An toàn thông tin với môi trường ảo hoá: những vấn đề tiềm ẩn và giải pháp.

3. **Chọn giải pháp an toàn thông tin cho các hệ thống ảo hoá để giảm chi phí quản lý và tăng hệ số đầu tư (ROI).**

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

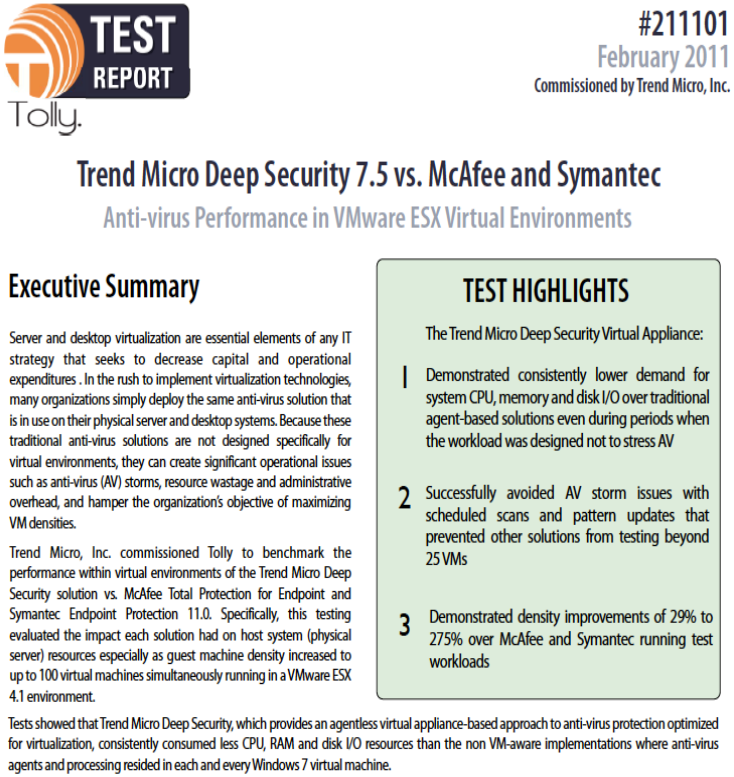
Vendor	Product	Components	Virtual Machine Aware	Implementation
Trend Micro, Inc.	Deep Security 7.5	Trend Micro Deep Security Manager version 7.5.1378; Trend Micro Deep Security Virtual Appliance 7.5.0.1600; Filter Driver 7.0.0.894; Default configuration. Assigned the pre-configured Windows Anti-Malware 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

- 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

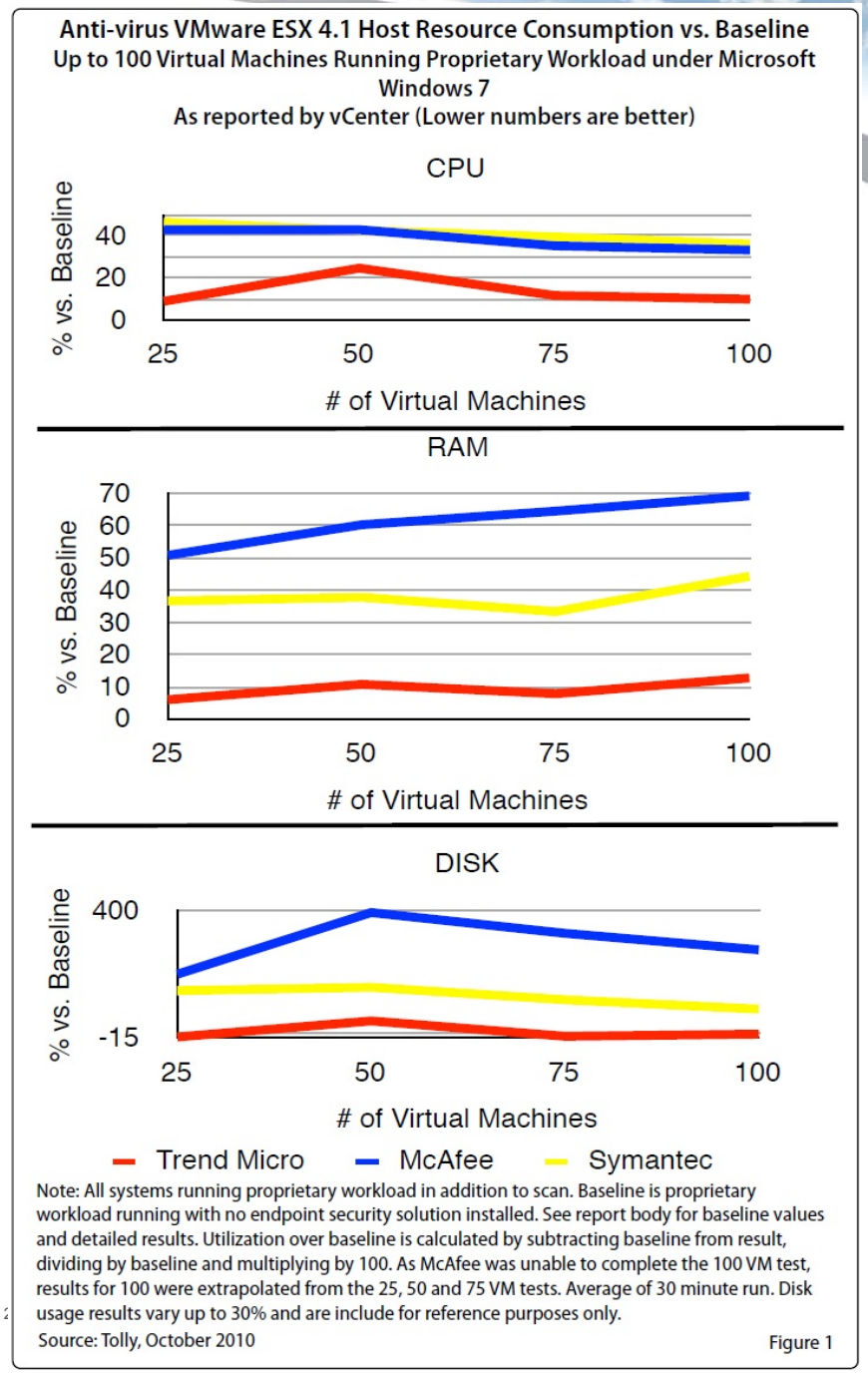
Tests showed that Trend Micro Deep Security, which provides an agentless virtual appliance-based approach to anti-virus protection optimized for virtualization, consistently consumed less CPU, RAM and disk I/O resources than the non VM-aware implementations where anti-virus agents and processing resided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

TREND MICRO

Tolly Report "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



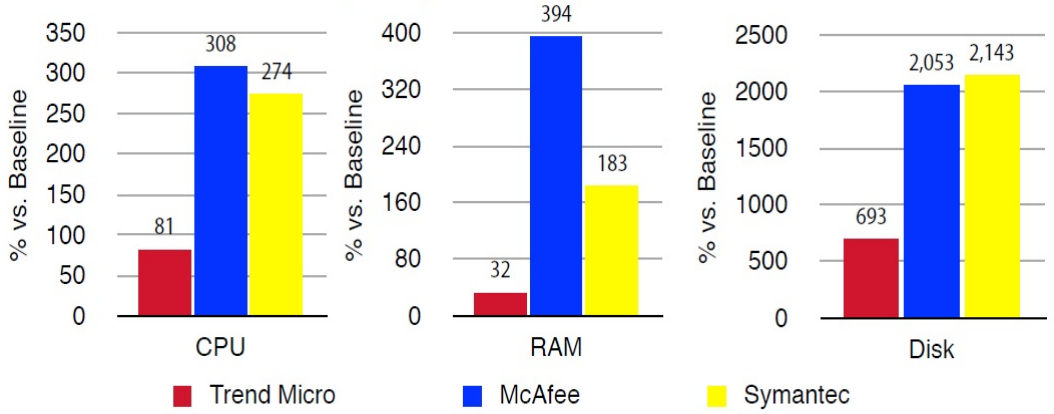
Tolly Report
"Full Scan Storm" Load

- 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.

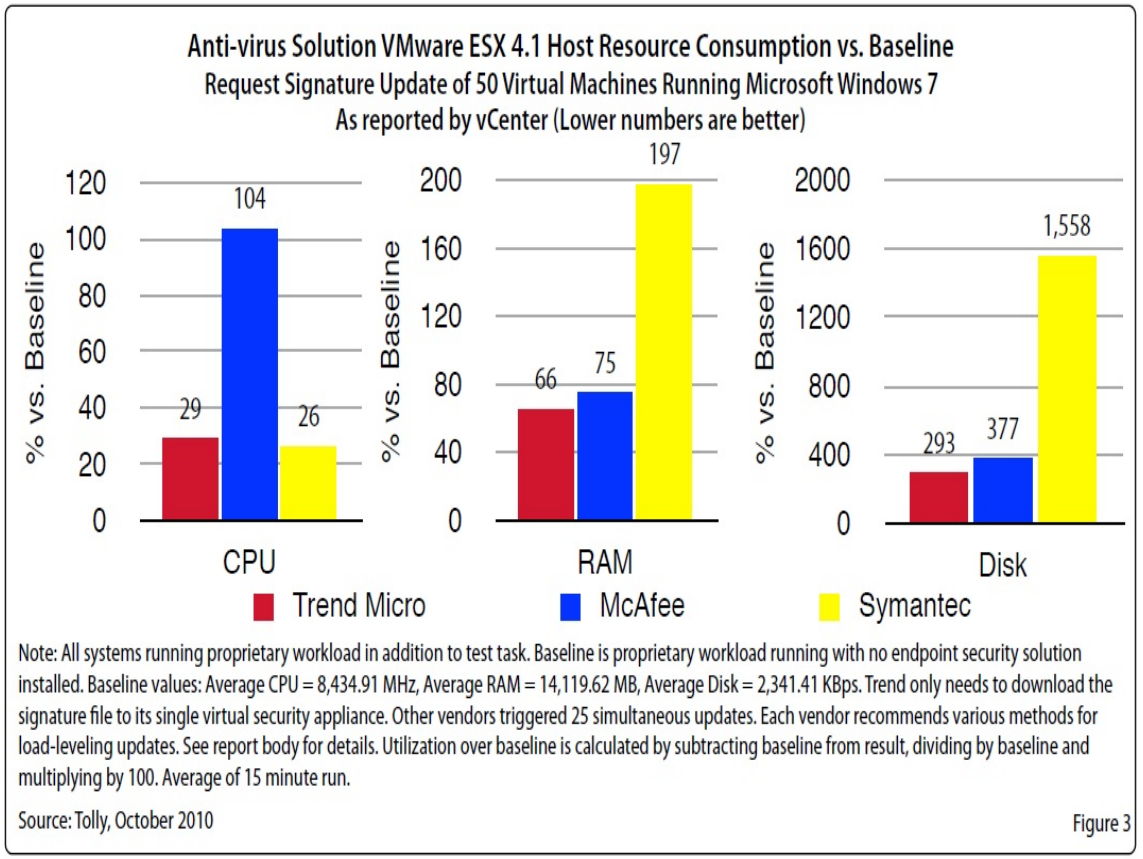
Source: Tolly, October 2010

Table 1

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

State of Enterprise Security Today

External Analysis

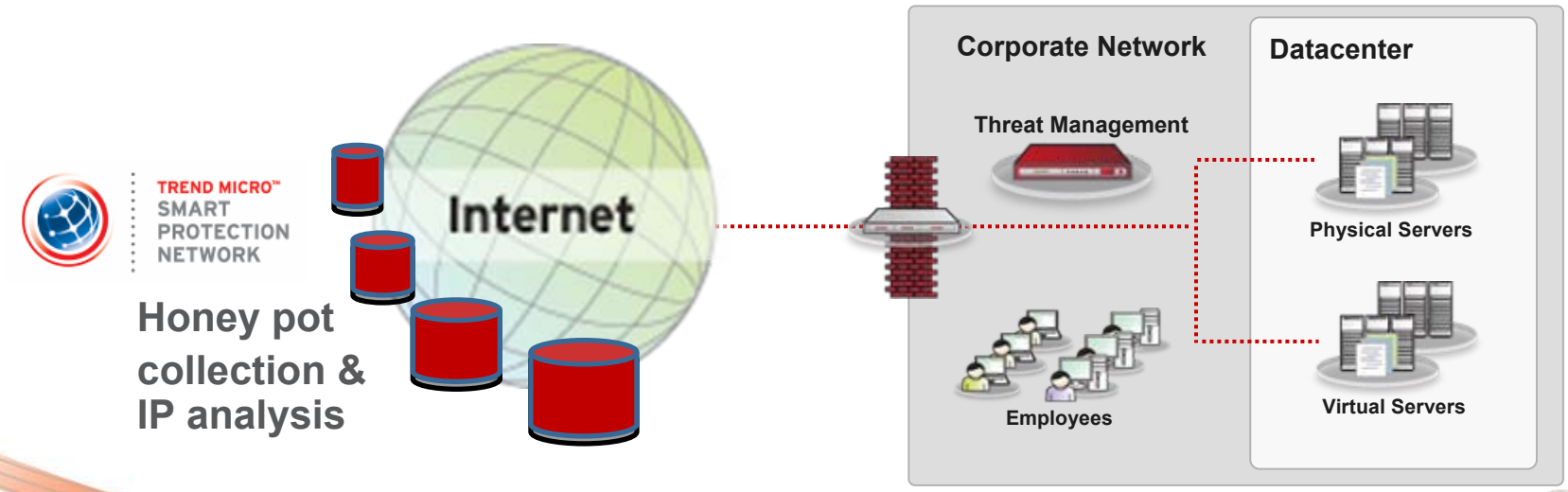
Malicious Traffic Collection

- Using passive techniques
- Found & analyzed 138M+ infected IP's over a 3 year period
- 25% are enterprise endpoints
- 300 day median infection duration

Internal Analysis

Enterprise Threat Assessments

- 100's of enterprises; avg 7000+ users
- 100% have active malware
- 77% have active bots
- 56% have active data stealing malware



Trend Micro – Securing your Journey to the Cloud

--- chúng tôi cung cấp giải pháp an ninh suốt lộ trình doanh nghiệp chuyển đổi lên Điện toán đám mây

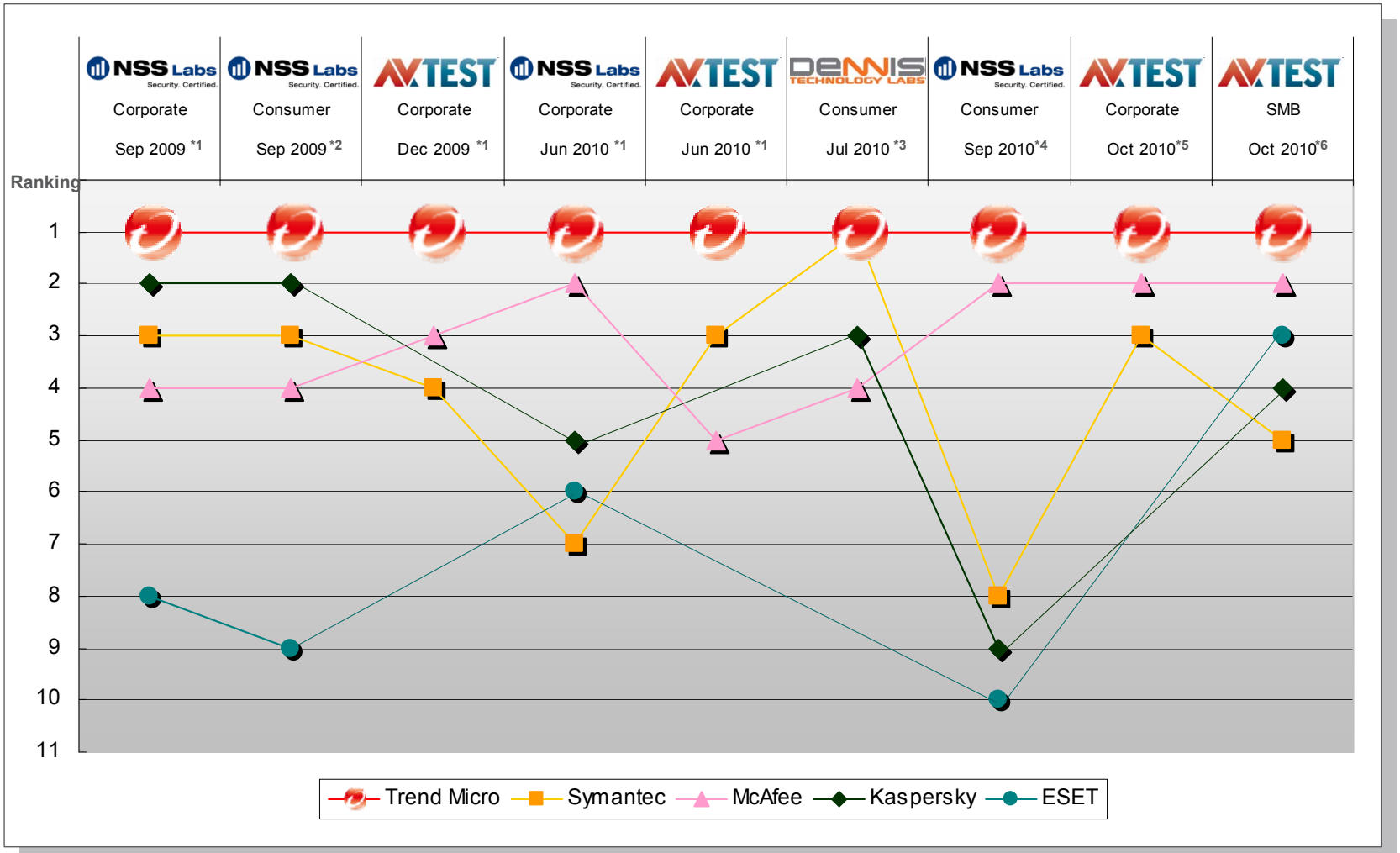
TREND MICRO™

#1 in Server Security*

VISIT US AT RSA 2011
IN SAN FRANCISCO

TRENDMICRO.COM/CLOUD

Trend Micro's real world protection validated by third party test labs



Note: If multiple products from one vendor were evaluated, then vendor's vest performance is listed.

*1: Http://www.trendmicro.co.jp/protection
*2: http://www.nsslabs.com/research/endpoint-security/anti-malware/q3-2009-endpoint-protection-group-test-report-socially-engineered-malware.html
*3: http://www.dennistechnologylabs.com/reports/s/a-m/trendmicro/PCVP2010-TM.pdf
*4: http://www.nsslabs.com/research/endpoint-security/anti-malware/consumer-anti-malware-products:-group-test-report-q3-2010.html
*5: http://us.trendmicro.com/imperia/md/content/us/pdf/trendwatch/av-test_october_2010_enterprise_endpoint_comparative_report_final_11-10-10.pdf
*6: http://us.trendmicro.com/imperia/md/content/us/pdf/trendwatch/av-test_october_2010_smb_endpoint_comparative_report_final_11-5-10.pdf

TREND MICRO

vmware®

Improves Security

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

TREND MICRO™

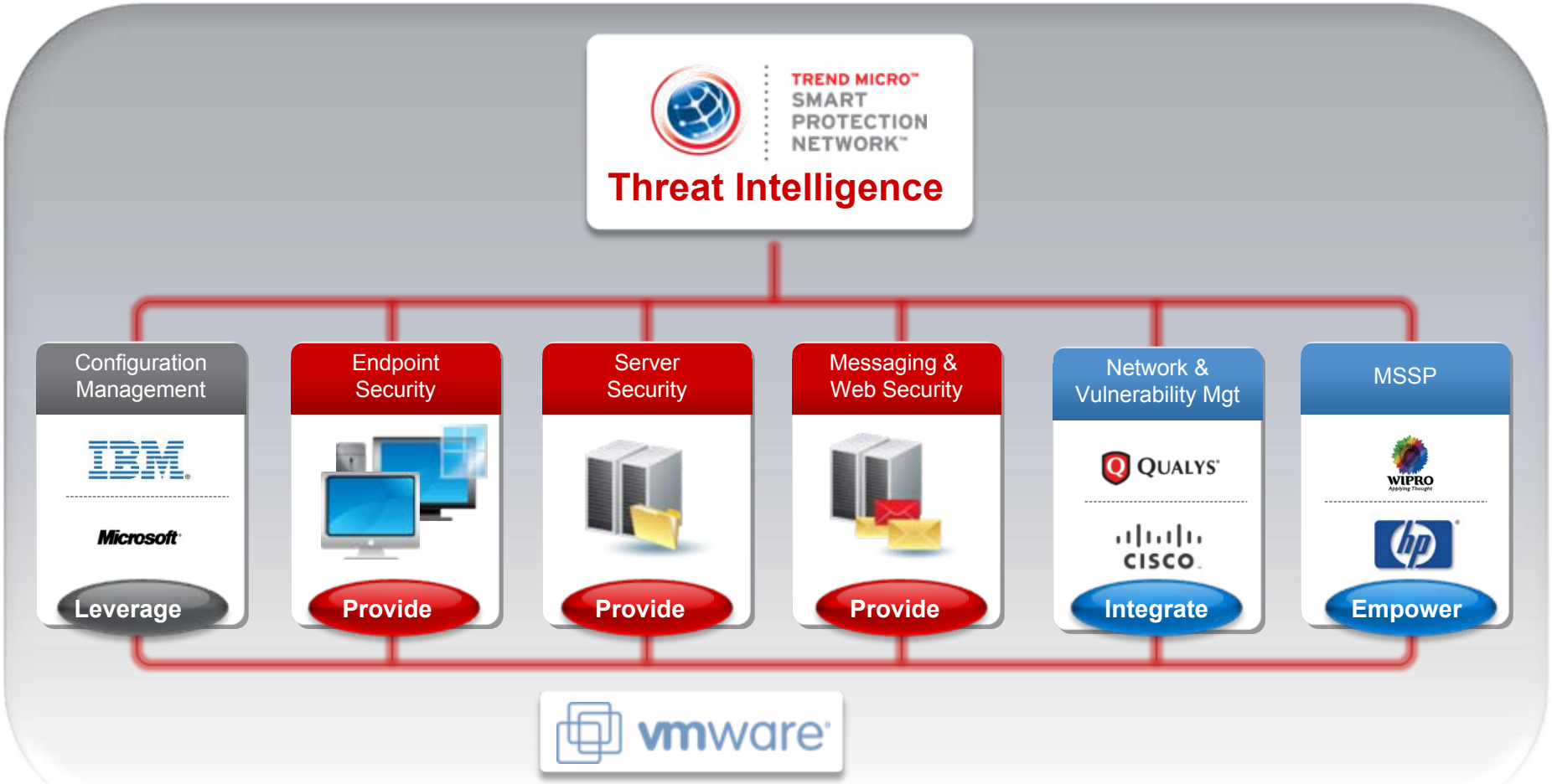
Improves Virtualization

by providing security solutions architected to fully exploit the VMware platform

Better-than-physical security for VMware customers

Security That Fits: Your Partner to the Hybrid Cloud

Trend Micro helps you maximize your current investments, not replace them,



TREND MICRO