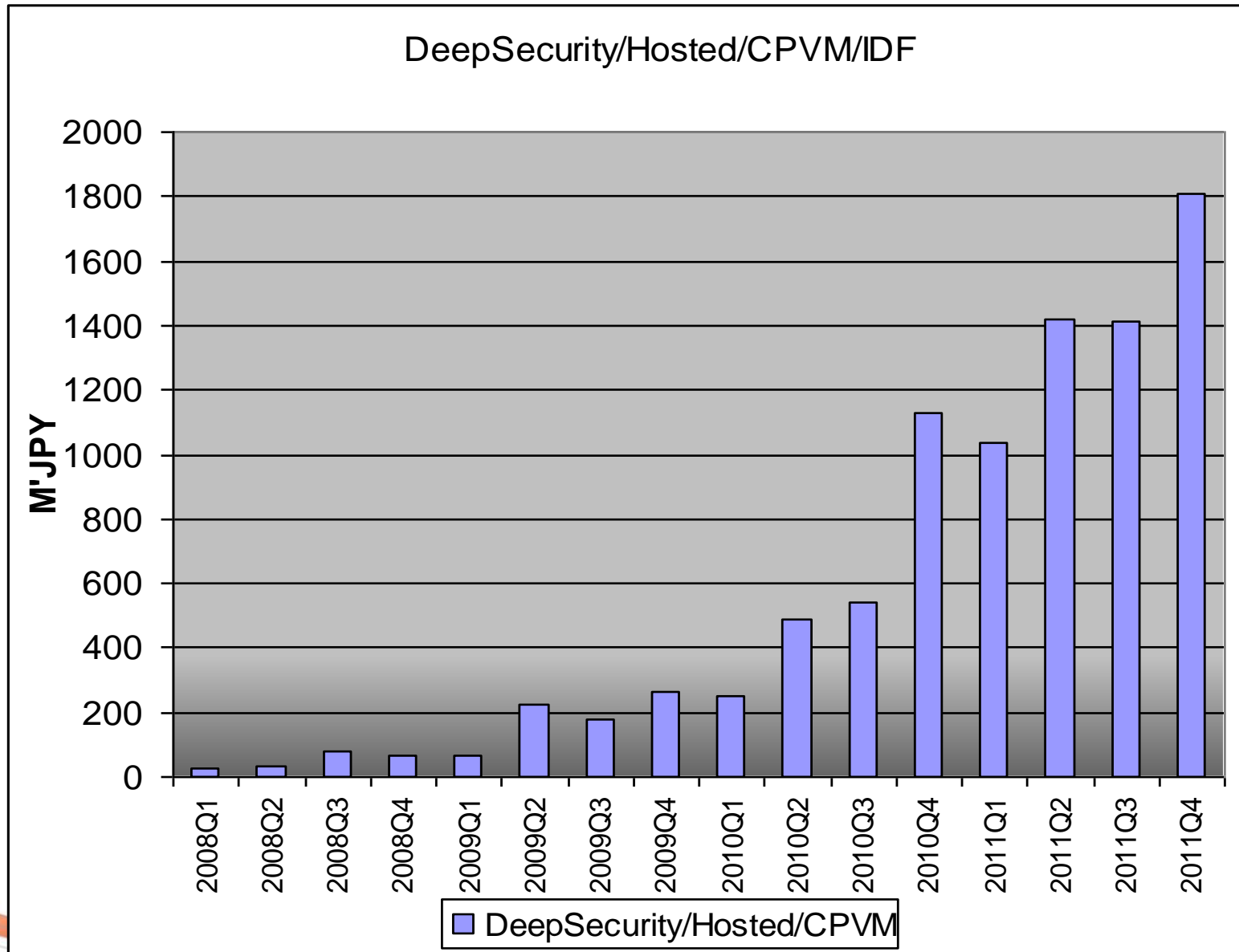


Why Trend Micro is Winning

Eva Chen
02/16/2012

Cloud Security revenue Q to Q Growth



Smart Protection Network 2.0

– Cloud Security Intelligence from Big Data Processing



TREND MICRO™
SMART
PROTECTION
NETWORK™

Cloud Evolution Intelligence

- Auto platform detection
- Virtual Patching
- Workload encryption

Mobility Intelligence

- Geo Location intelligence
- SIM card based identification
- Mobile App Reputation service
- Device control

APT & Target Attack Intelligence

- Real time C&C list
- Application Whitelist
- Document exploit detection
- Data Fingerprint
- Deep content Inspection



Security that Fit – The Vending Machine Approach

Platforms

Endpoint

Data Center

Network

Management

Consumer Home



Endpoint Platform

- Anti-Malware
- Mobile
- Data Loss Prevention
- Encryption
- SafeSync



Data Center Platform

- Anti-Malware
- IPS/IDS
- File Integrity
- Log Inspection
- Data Loss Prevention
- Encryption



Network Platform

- Anti-Malware
- Data Loss Prevention
- Application ID
- Mobile
- Web/DB



Management Platform

- Policy
- Reporting
- Threat Intelligence
- Dashboard
- Configuration
- Update



Consumer Home Platform

- Anti-Malware
- Mobile
- Data Protection
- Encryption
- SafeSync

Cloud Era Security Challenge

Defending against Threats in Physical, Virtual, and Cloud Environments

**Outside-in
Perimeter Defense
Isn't Enough...**

Advanced
Persistent Threats



Mobility



Elastic
Perimeter



5 C's

Cost Reduction

Compliance and DP

Control Over Risk

Consumerization

Cloud

5 C's

Cost Reduction

Compliance

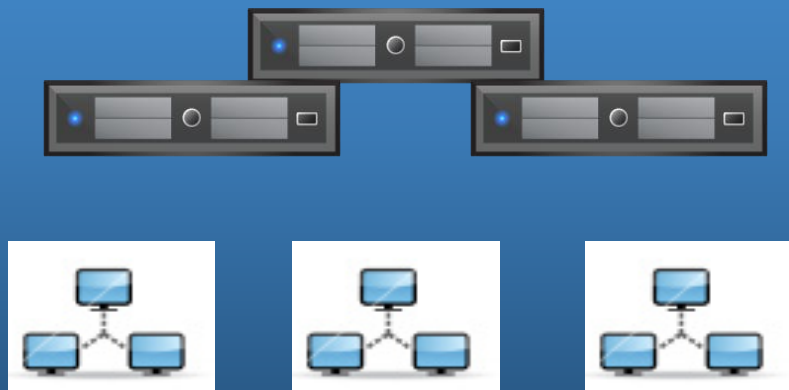
Control Over Risk

Consumerization

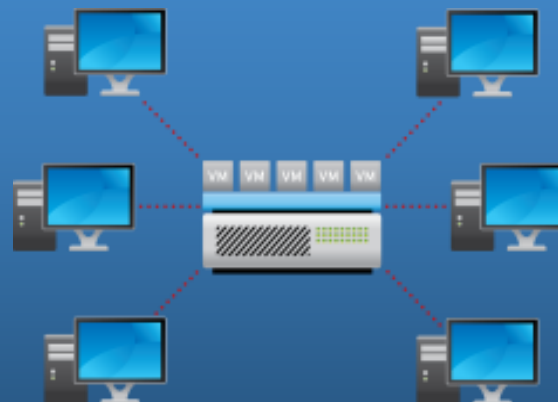
Cloud

Virtual Appliances Gateway

The Old Way



With Virtual Appliances Gateway



Solution - IWSVA

4 in 1 Web Gateway Virtual Appliance

Business Benefit – One Vendor, No Hardware and Better Web Security

Solution - IMSVA

5 in 1 Hybrid Messaging Gateway Virtual Appliance

Business Benefit – One Vendor, Less Traffic Load On Network, No Hardware Cycle and Better Email Security

Physical – Virtual - Cloud

Agentless AntiVirus

The Old Way

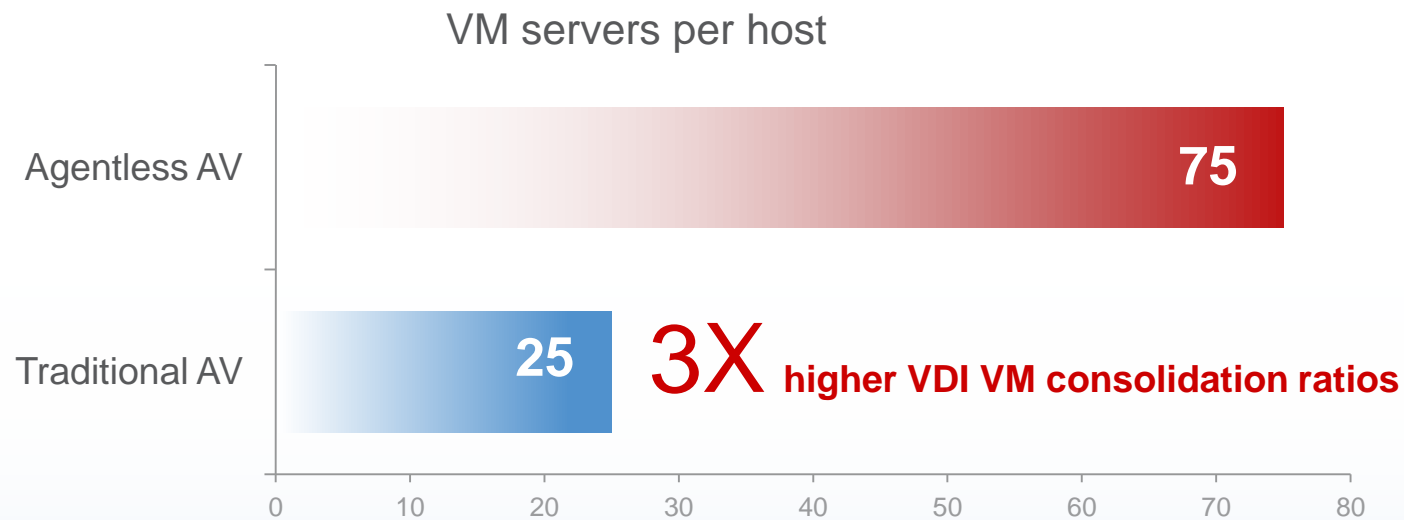


With Agent-less Security



Cost Reduction & Consolidation

Agentless Security on Virtual Desktop VMs



3-year Savings on 1000 VDI VMs = \$539,600

Sources: Tolly Enterprises Test Report, Trend Micro Deep Security vs. McAfee and Symantec, February 2011; Saving estimate based on VMware ROI calculations

Channel Opportunity – Public Cloud Service Providers Savvis, Dell, Singtel, GoDaddy, Swisscom

- Global Private and Public Cloud Providers
 - Using internally or Reselling Trend Micro as-a-service (TMaaS)
- Density needs are very demanding
 - Building virtualization-aware security into their cloud platforms
- Most are extending into shared storage data protection with SecureCloud
- Ease of management and integration with private infrastructure are top customer requirements
 - One security model for private and public cloud
 - Add-on service or self-service – IPS, AV, FIM
 - Burst with consistency of security management model

Channel Opportunity – Public Cloud Service Providers Savvis, Dell, Singtel, GoDaddy, Swisscom

- Global
 - Us
- Dense
 - Bu
- Most with
- Ease of infra
 - Or
 - Ac
 - Bu

**We are winning
where scale
and cost matter
the most**

5 C's of Cloud

Cost Reduction

Compliance and DP

Control Over Risk

Consumerization

Cloud

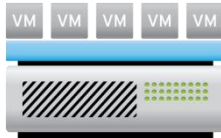
Compliance and Data Privacy

- Compliance
 - Virtual Patching
 - File Integrity Monitoring
- Data Privacy
 - Data Encryption
 - Data Leakage Prevention

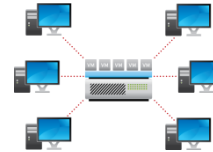
Compliance

Agent-based and Agentless FIM

Agentless FIM for VMware



Protection for virtualized desktops and data centers



The Old Way



With Agent-less Security



Customer Case Study

- SaaS Provider for Sales Automation

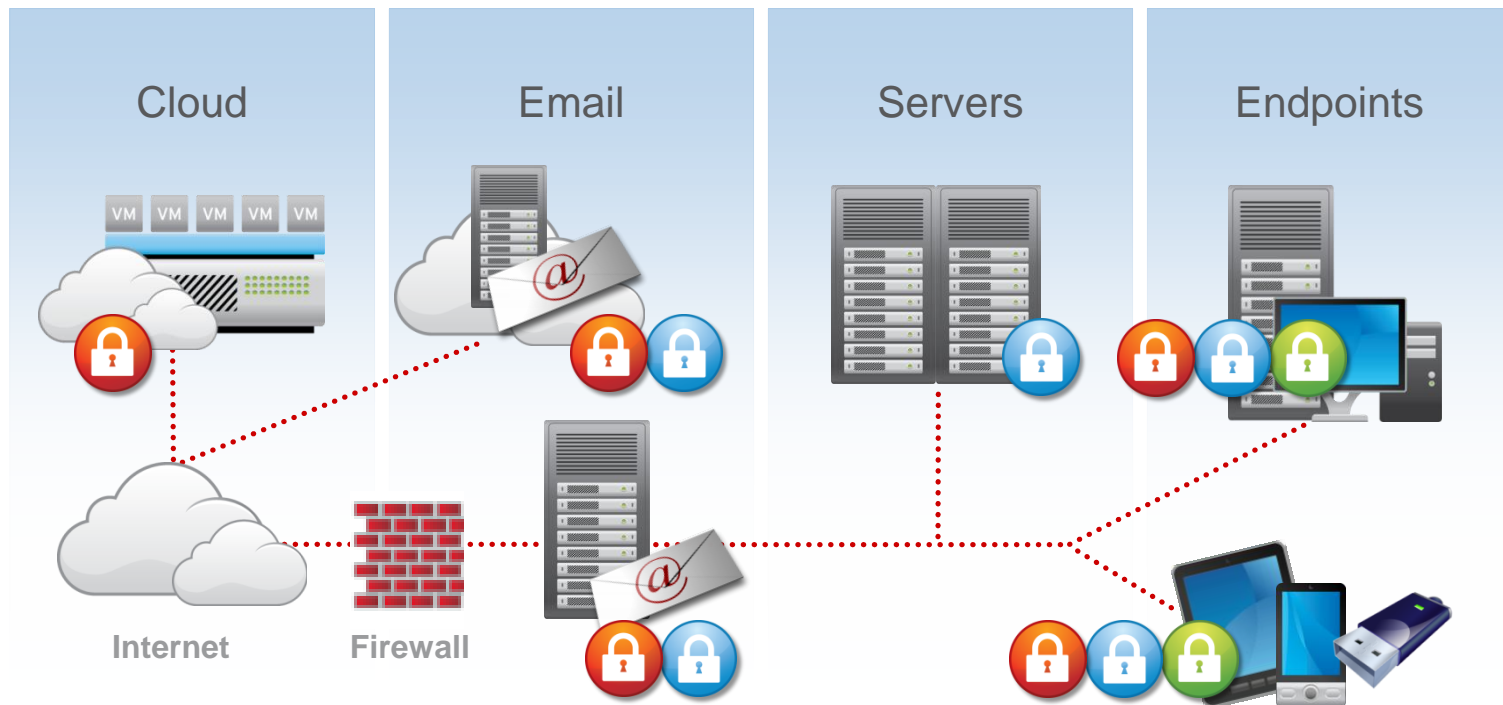
- Significant Compliance Needs
 - Needed to monitor application integrity
 - Reviewed several options
- Chose Trend Micro File Integrity Monitoring
 - On the Deep Security Server platform
 - Across 1000s of Servers

Compliance and Data Privacy

- Compliance
 - Virtual Patching
 - File Integrity Monitoring
- Data Privacy
 - Smart Data Protection
 - Integrated DLP

Data Protection across Your Network

 Encryption  Data Loss Prevention  Device Control



Customer Case Study - SecureCloud American Airlines



- Mostly virtualized global private infrastructure
- Needed to move some applications to public cloud
 - Distributed public-facing customer applications
- Significant security and compliance requirements
 - A data protection model where AA held the keys
 - Flexibility to switch cloud providers without long audit process
- Extended AA security architecture to include workload and data encryption model in cloud
 - Compliance and data protection needs met

**We are
winning where
Compliance
and data
protection
most needed**

5 C's of Cloud

Cost Reduction

Compliance

Control Over Risk

Consumerization

Cloud

The APT Phenomena

RSA, Sony, Mitsubishi,
CitiGroup ... show power
of targeted attacks

Stuxnet, DUQU, and
100's of attacks on
company IP around
the globe...

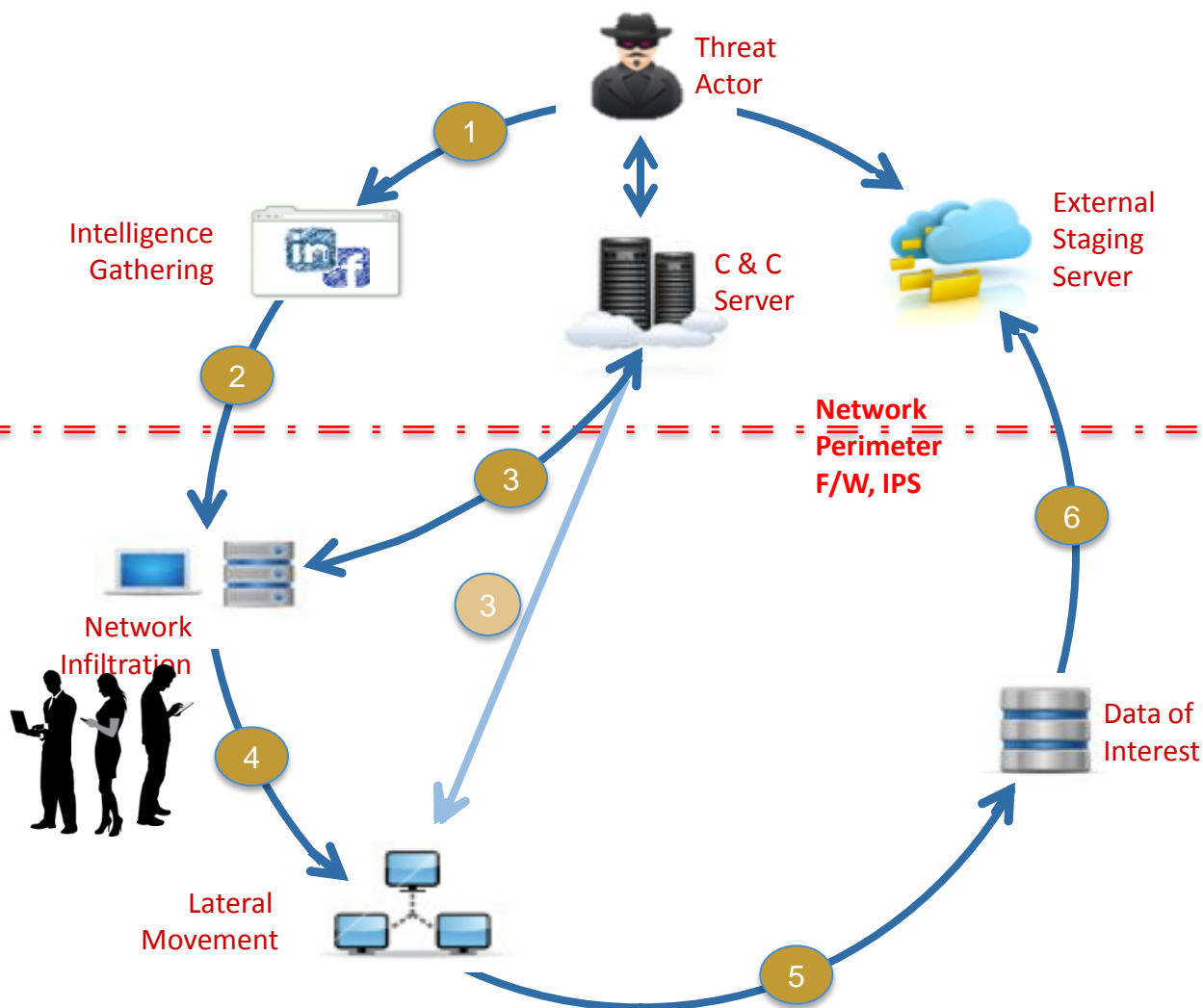
GhostClick controls over 4 Million

The New Norm
according to IDC

A Cyber Intrusion
Every 5 Minutes...
according to US-CERT

Trend Micro finds
over 90% of
enterprise networks
contain active malicious
malware

APT and Targeted Attack slip through perimeter security



Social

- People are the weakest link
- Spear Phishing
- Drive-by Downloads

Sophisticated

- Exploits vulnerabilities
- Remote control and backdoor
- Uses credentials & privileges

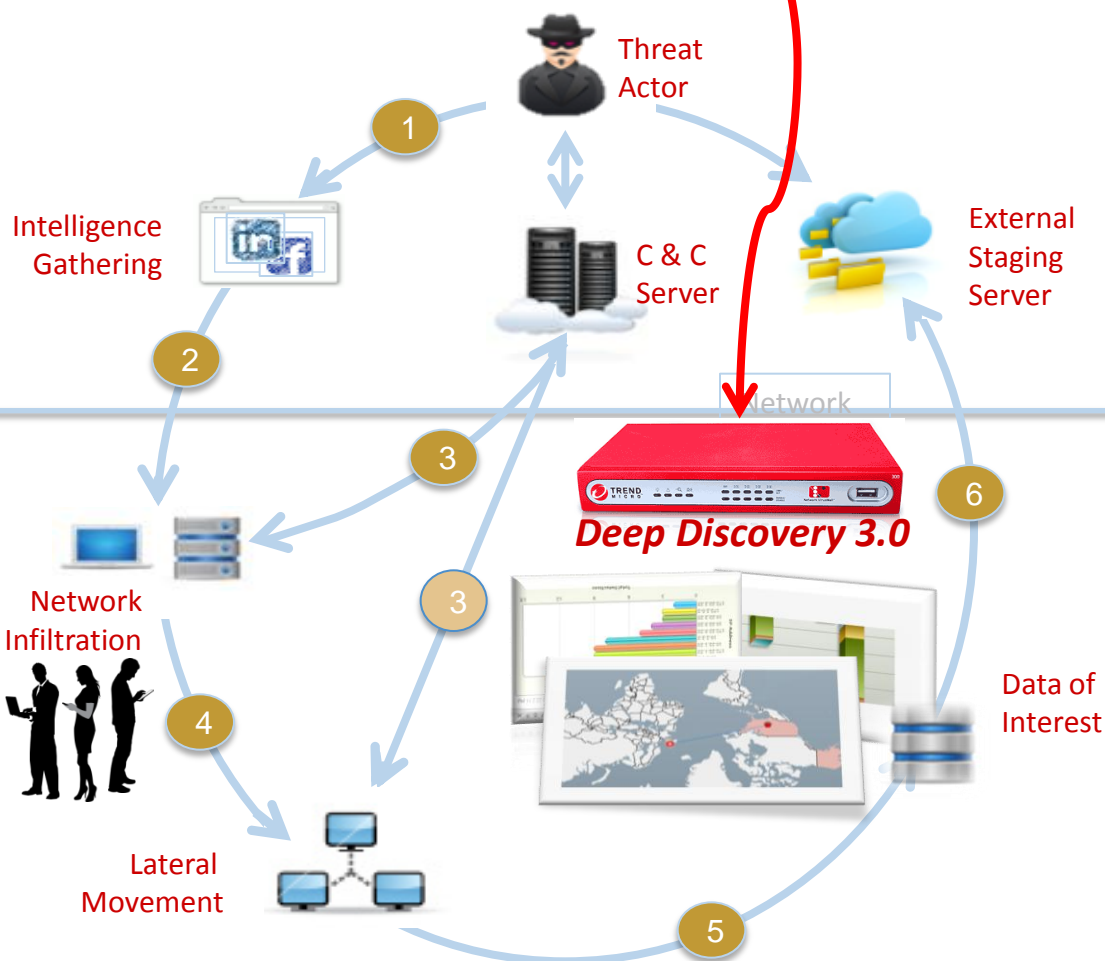
Stealthy

- Low profile
- Masked activities
- Difficult to detect

Connect Threat Intelligence with Inside Network Visibility



TREND MICRO™
SMART
PROTECTION
NETWORK™



Specialized Threat Detection Across the Attack Sequence

Malicious Content

- Emails containing embedded document exploits
- Drive-by downloads
- Zero-day & known malware

Suspect Communication

- C&C communication for any type of malware & bots
- Backdoor activity by attacker

Attack Behavior

- Malware activity: propagation, downloading, spamming ...
- Attacker activity: scan, brute force, service exploitation ...
- Data exfiltration

Deep Discovery (TDA 3.0) ---- Discover APT and Target Attack with actionable items

Deep Discovery User: admin Log out

Dashboard Detections Logs Reports Administration Help

You are here: Detections

Detections

Search hostname or IP address

Range: Past 24 hours

IP Address	Hostname	Group	Total Detections	File Pattern	Malicious Behavior	Suspicious Behavior	Exploit	Grayware	Web Reputation	Dis
10.2.0.2	10.2.0.2	Default	11	1	3	0	0	1	0	
10.2.1.2	10.2.1.2	Default	8	1	2	0	0	1	0	
10.2.2.2	10.2.2.2	Default	2	0	1	0	0	0	0	

Top Hosts with Events Detected

Period: Past 24 Hours Last refreshed at 2012-01-22 2:11 PM

Top 10 Total Events Detected

IP Address	Total Events
10.2.0.2	11
10.2.1.2	8
172.22.1.22	9
10.22.1.22	9
10.2.2.2	2
172.22.0.22	1
10.22.0.22	1
10.22.2.22	1
172.2.0.2	1
172.22.3.22	1



Visualization Analysis Alarms Reporting

Specialized Threat Detection

Sandbox Analysis

Smart Threat Tracking

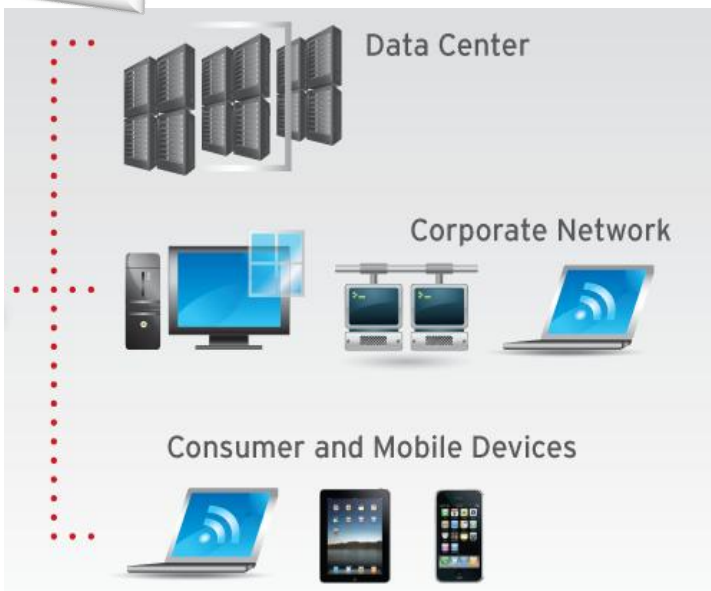
Threat Connect Intelligence

SIEM Connect

Network Inspection Platform

Deep Discovery

Network Visibility, Insight & Control



**We are winning
because
firewall/IDS/IPS
can not defend
against APT**

5 C's of Cloud

Cost Reduction

Compliance

Control Over Risk

Consumerization

Cloud

CONSUMERIZATION is Causing a Shift

Corporate
Devices

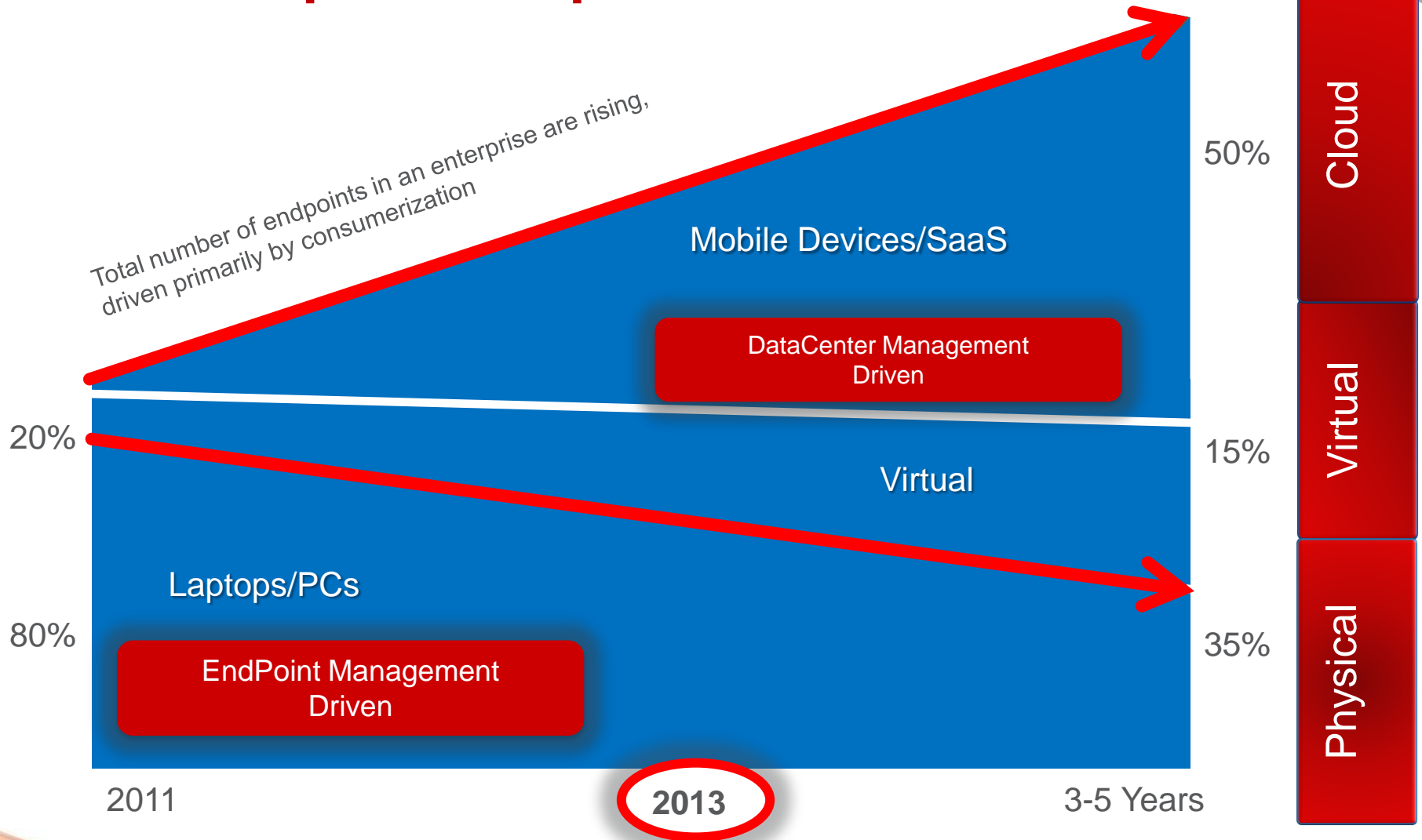


Bring your
Own devices



CONSUMERIZATION

The Enterprise Endpoint Evolution

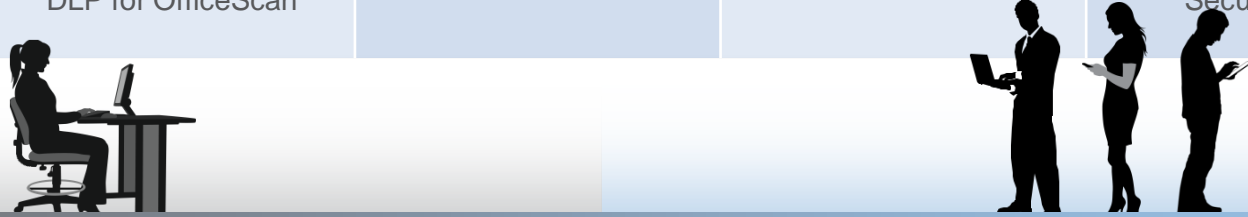


Cross-over year 29

Consumerization

Solutions to Fit *YOUR* Balance of Control and Freedom

Regain visibility & control	Mobile Security 7 OfficeScan	Deep Security	Titanium Titanium for Android	Hosted MDM (2H)
Share data with confidence	DLP for OfficeScan	OfficeScan VDI Deep Security		SafeSync for Business SecureCloud
Protect data anywhere	Endpoint Encryption DLP for OfficeScan			SafeSync for Business SecureCloud



CONTROL

Company-owned,
fully managed

Employee-owned,
full "BYOIT"



The Future of Endpoint Customer Case Study – VMWare – VDI

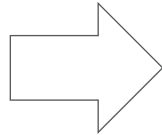
- Significant VDI deployment where security was required
- Investigated many options to include hypervisor-based VDI security
 - Density was THE critical requirement
- Chose hypervisor-based security for performance and management reasons
 - Striving for 348 desktops per server
 - Managed 16 virtual appliances vs. 2500 VMs

vmware®

How we win in Consumerization

Customer Type

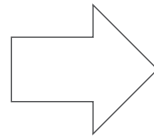
“Control or Denial”



How We Win

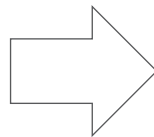
- Performance
 - Ease of management
 - Support

“Add Mobile Devices”



- One Vendor for Endpoint
 - 80/20 MDM

“Rethink, New Infrastructure”



- Best VDI
- Server-centric

5 C's of Cloud

Cost Reduction

Compliance

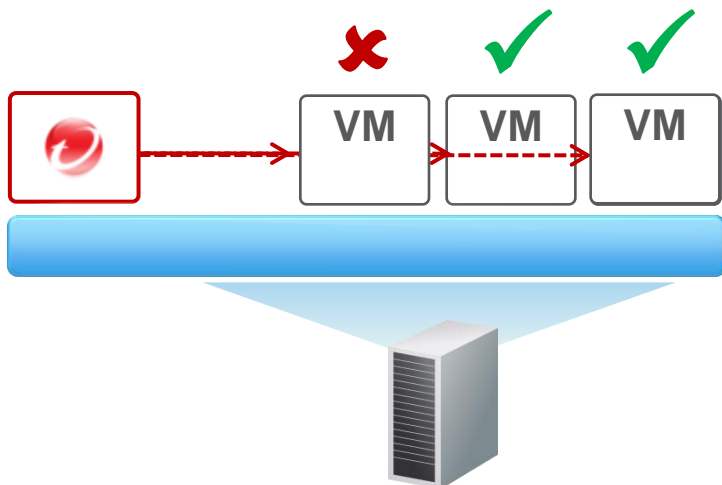
Control Over Risk

Consumerization

Cloud

Physical – Virtual – Public Security Management and Compliance Policy Assurance and Visibility

Deep Security
(Virtual Appliance)



Internal Virtual DC

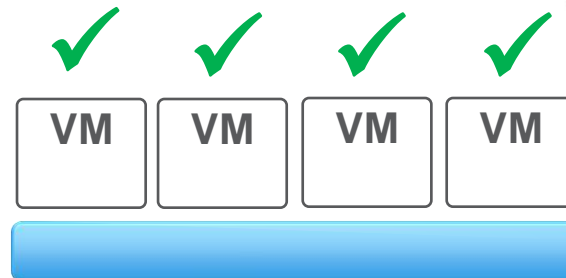
Standard Policy Profile

Vulnerability shielding

Hypervisor –based:

IPS

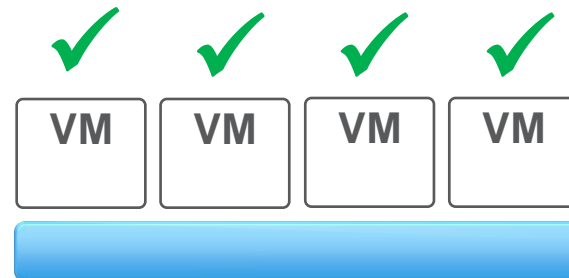
AV



Customer facing
Private Cloud

PCI-DSS = FIM

Data encryption



Public Cloud

Agent-based

All VMs = FIM

Workload encryption



Copyright 2011 Trend Micro, Inc.

Business Benefits of Trend Micro Cloud Security

- Reduced Cost of Operations
- Increased Application Stability and Performance
- Higher Virtualization ROI
- Secure Use of Public Cloud
- Reduced Investment in Management

Case Study – Australian Bureau of Statistics

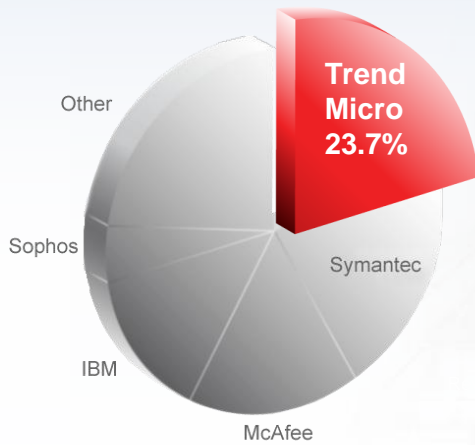
- Large Australian Government Organization
- 99% virtualized across multiple DCs
- Moved to host-based security model for 3 reasons:
 - VMotion – wanted security profile to follow host
 - Vulnerability shielding and compliance
 - Consistency of management – one platform across all environments = Physical, Virtual, Cloud

Trend is No.1 in Server and Virtualization Security

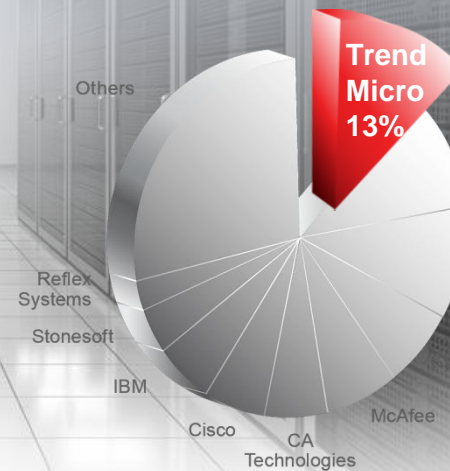
Physical

Virtual

Cloud



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



Source: 2011 Technavio – Global
Virtualization Security Management
Solutions

Why Trend Micro is Winning?

- **Winning where the future is – Cloud Security**
- **Winning with sustainable, expandable, cloud security architecture --- SPN**
- **Winning what matter for customers --- 5 Cs**
 - **Cost, Compliance, Control Risk, Consumerization, Cloud**



SECURING
YOUR JOURNEY
TO THE
CLOUD



An Innovative, trustworthy, security focused global organization