2010 TREND MICRO ENTERPRISE SUMMIT

Securing the Virtualized Enterprise – Preparing for the Cloud

Produced by:

TREND MICRO™

CSO
BUSINESS RISK LEADERSHIP

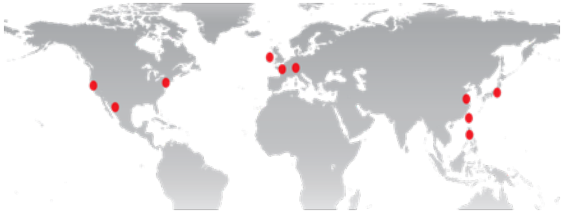
Trend Micro Update

Founded	United States in 1988
Headquarters	Tokyo, Japan
Employees	4,800
2009 Financials	Sales $1 Billion
	Income $300 Million
	Total Cash $1.7 Billion
Leadership	Largest independent security-only software company
	“Global 100 Most Sustainable Corporations”
	Top 3 in Messaging, Web and Endpoint security
	Leader in virtualization & cloud computing security

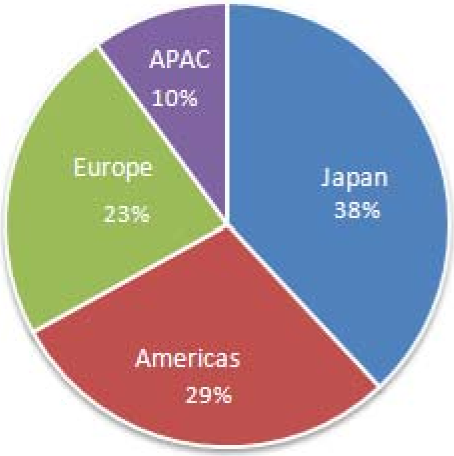
TrendLabs
Global Technical Support & R&D Center of TREND MICRO

New malware every 1.5 seconds

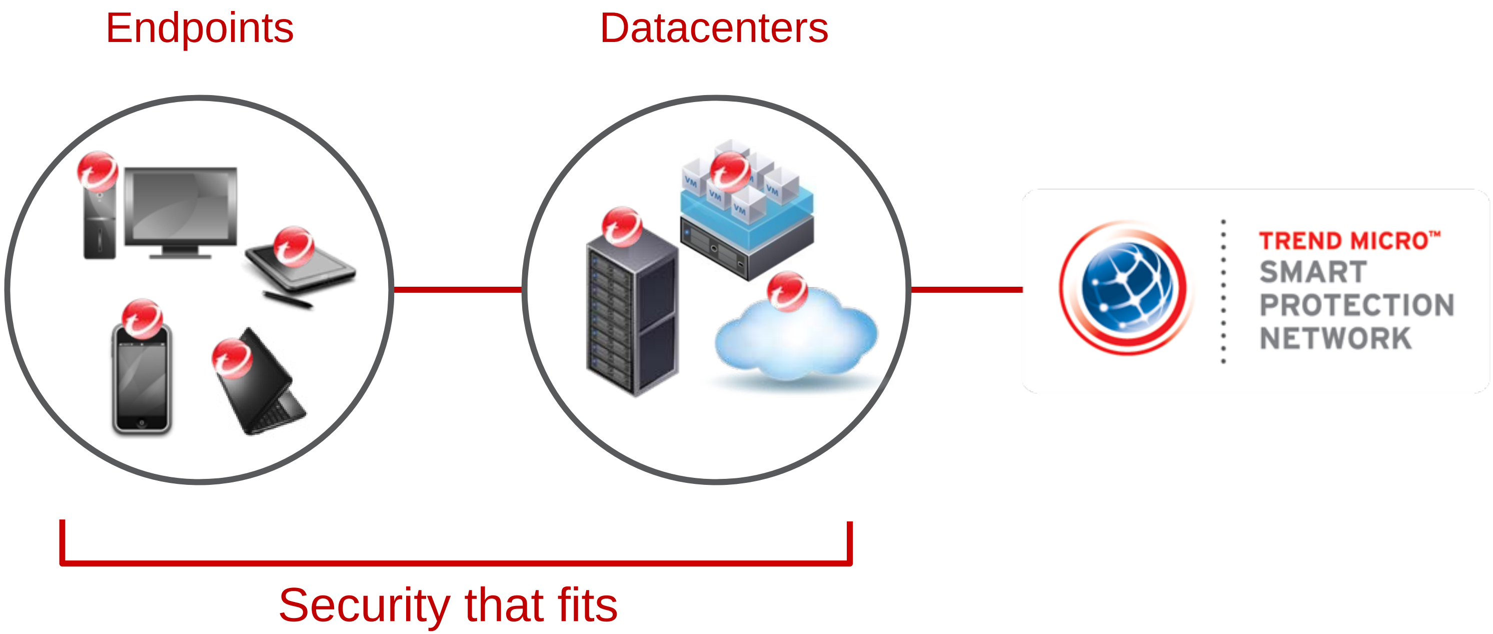
- Real-time alerts for new threats
- 1,000+ researchers
- 10 labs & 24x7 ops



Sales by Region



Product Strategy



Consumers

Titanium
- Strong
- Fast
- Easy-to-use
- Light

SMB

Worry-Free
- Safer
- Smarter
- Simpler

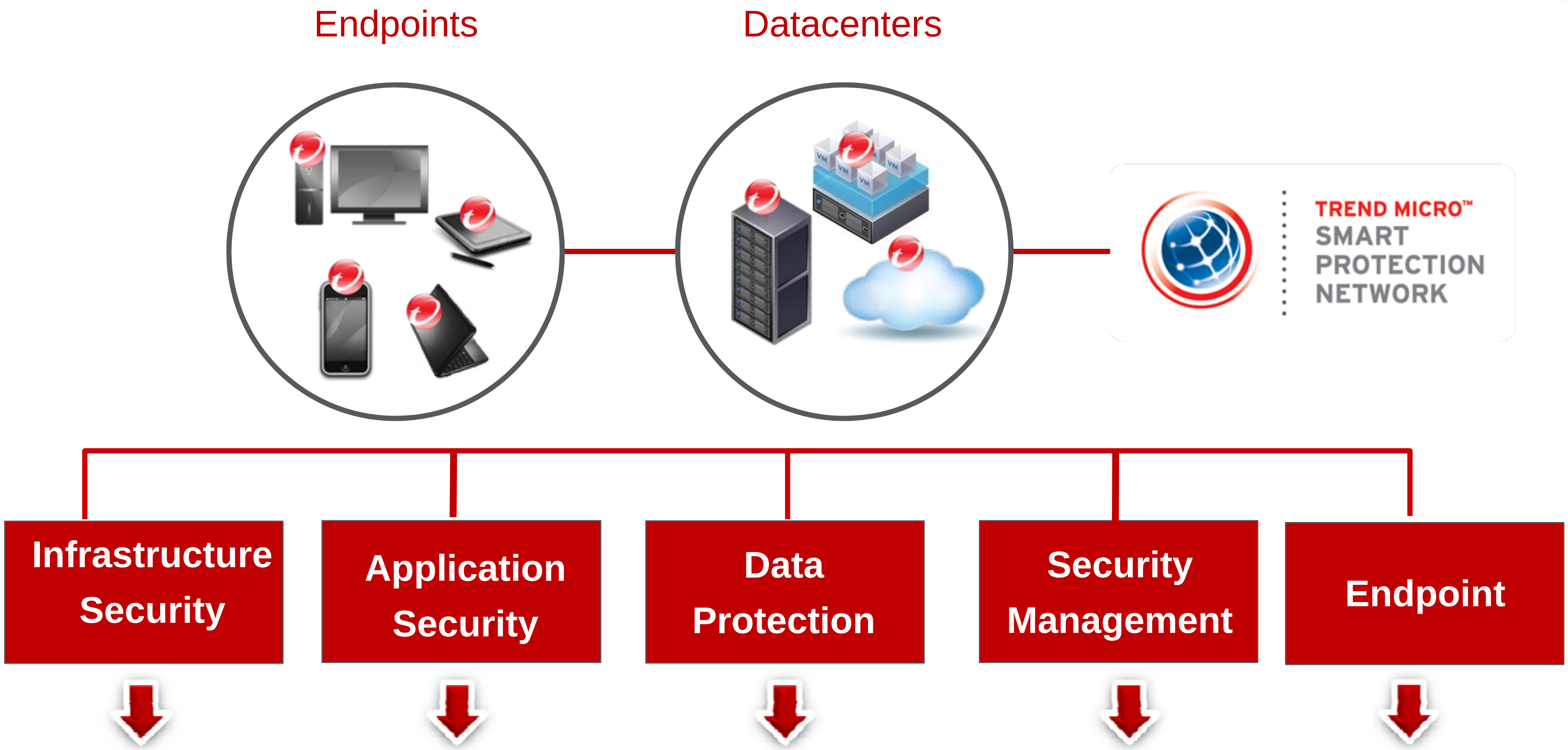
Enterprises

OfficeScan
DeepSecurity
SecureCloud
Other…

- More comprehensive protection
- Broader platform coverage
- Greater operational efficiency
- Tighter integration

Enterprise Strategy:

Trend Micro Enterprise Security - TMES



Infrastructure Security

- Physical
- Virtual
- Cloud

Application Security

- WWW
- HTTP
- SMTP

Data Protection

- End Point
- Network
- Cloud

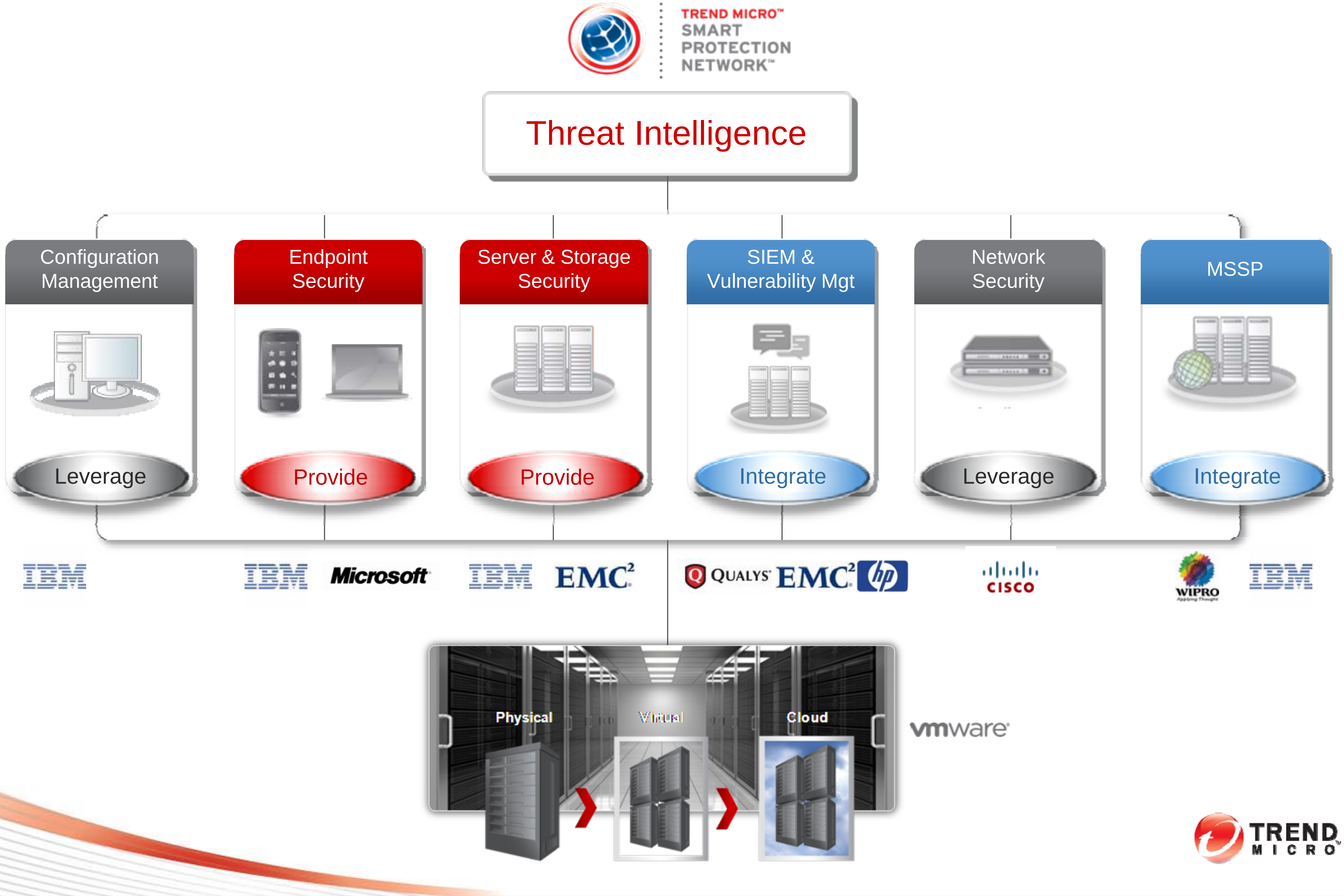
Security Management

- Products
- Compliance
- Event

Endpoint

- Fat Client
- Mobile
- VDI

Security That Fits: Partner Ecosystem



TREND MICRO™

Cloud Impact to IT Industry

Virtualization

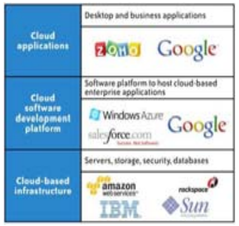
Dynamic Datacenter with
Shared System , share storage

3G Network
Net Devices

Ubiquitous, Borderless
Data Access, data everywhere

Security Innovation: Security that Fits

Public Cloud



Cloud applications	Desktop and business applications
	ZOHO Google
Cloud software development platform	Software platform to host cloud-based enterprise applications
	Windows Azure salesforce.com Google
Cloud-based infrastructure	Servers, storage, security, databases
	amazon web services rackspace IBM Sun

Ownership of Data vs. Computing
Confidentiality & Access Control

Cloud Application

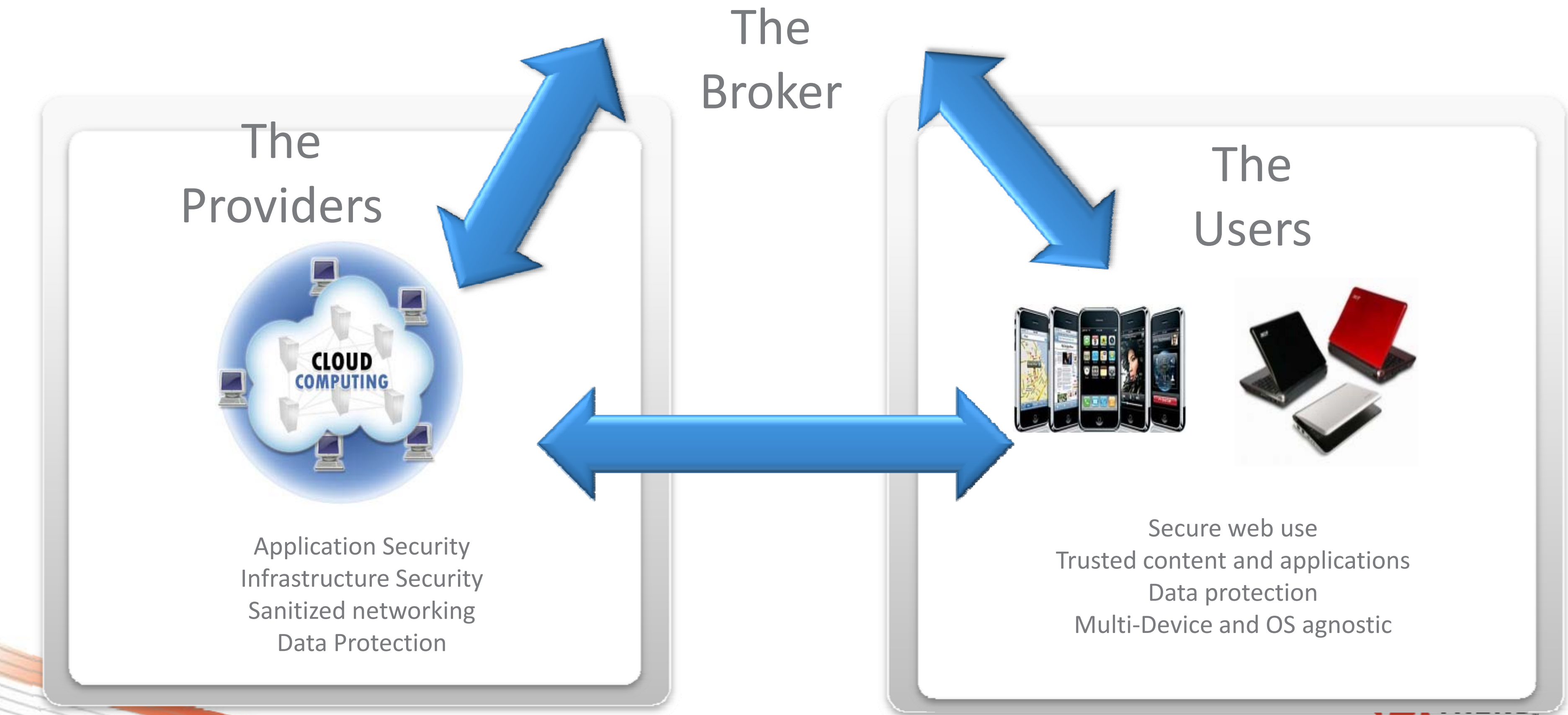
New Platform for New Apps. Example,
Web defacing, SQL injection

Long Term Product Strategy Vision
3 components in the new ecosystem

- Threat Trends
- Reputation Services
- Global Watch

TREND MICRO™
SMART
PROTECTION
NETWORK™

- Off-network/On-network
- Customized Response
- Event and Incident Management
- Remediation Services



The Broker

The Providers

Application Security
Infrastructure Security
Sanitized networking
Data Protection

The Users

Secure web use
Trusted content and applications
Data protection
Multi-Device and OS agnostic

Why is the security broker so important ?

- Attacks are targeted…or not
  - Response needs to be real-time, usage-specific, AND customizable
  - Prevention, compliance, and remediation need to be traffic-aware
- Users are mobile…. or not
  - Enforcement and knowledge need to be on/off network
  - Data protection is becoming critical
- Vulnerabilities are known but not patched…or not
  - Prevention needs to be environment-specific
- The cloud is everything….or not
  - Network, physical, virtual, and cloud

Securing Your Web World

The Broker
Trend Micro Smart Protection Network

Security That Fits: The Threat Landscape

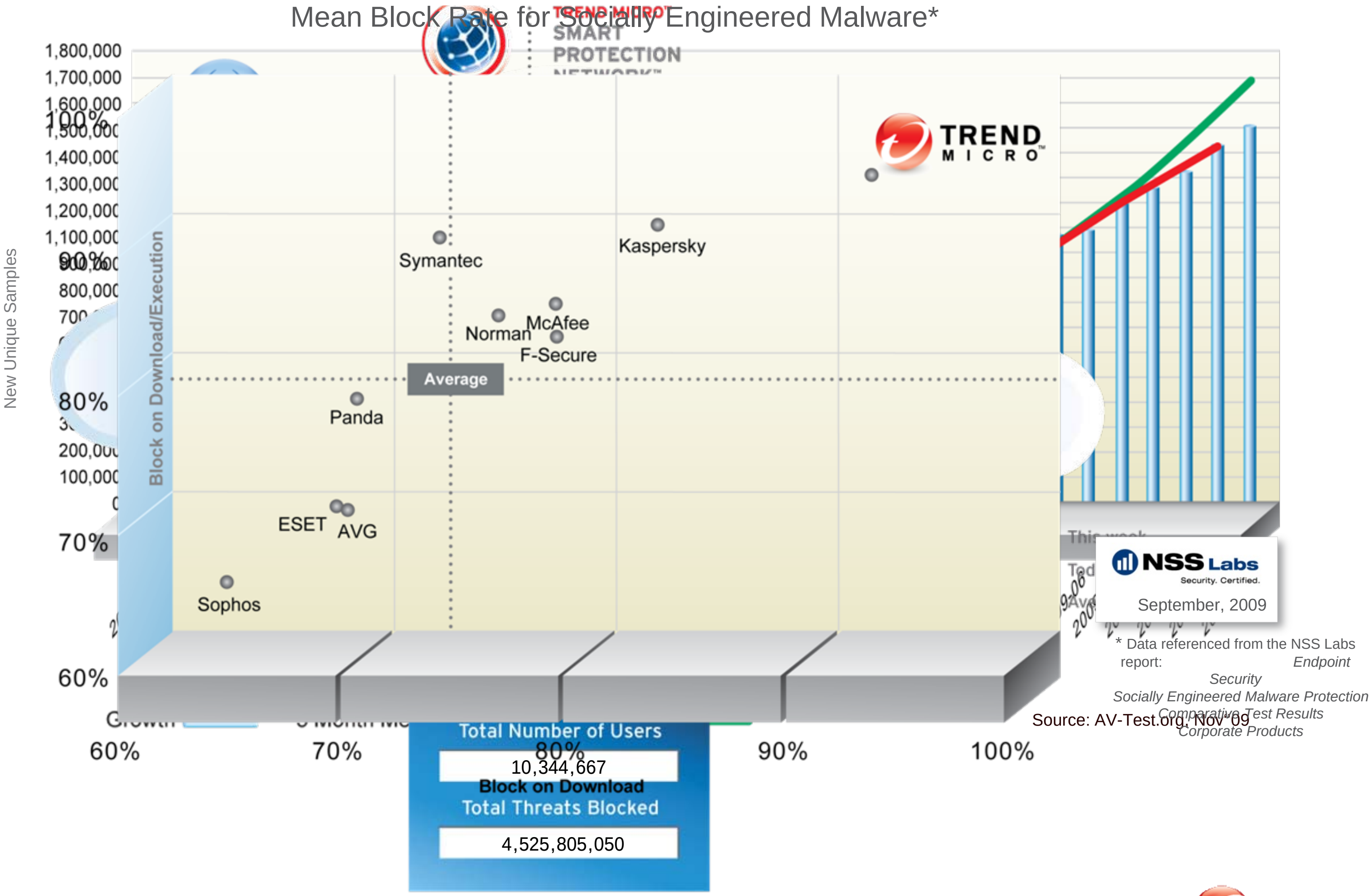
Trend Micro provides industry-proven real-world protection

NEW
Threat Every
1.5
Seconds

Blocking Billions of Threats Daily

#1
Real-world Online Testing

Mean Block Rate for Socially Engineered Malware*

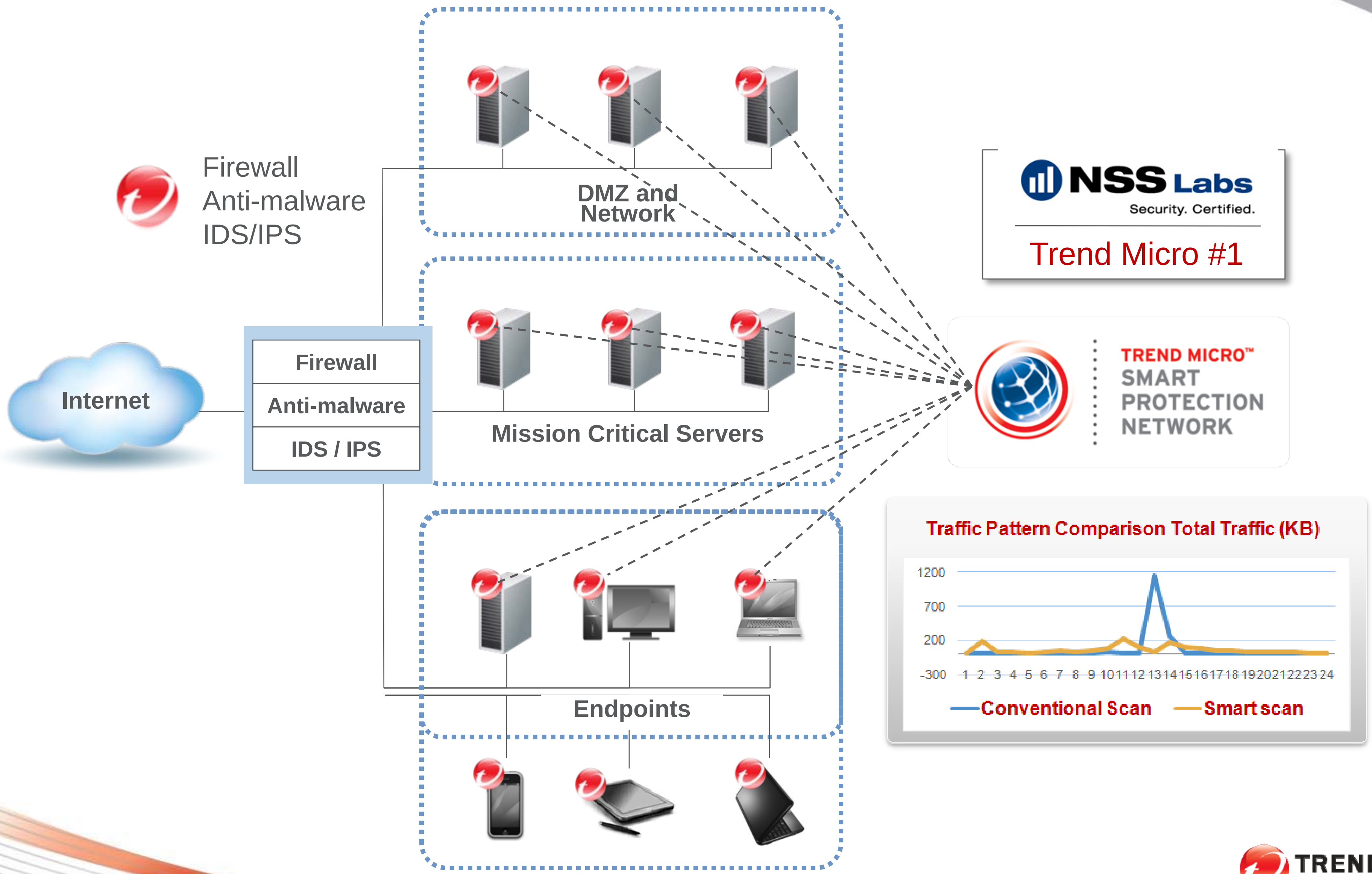


September, 2009

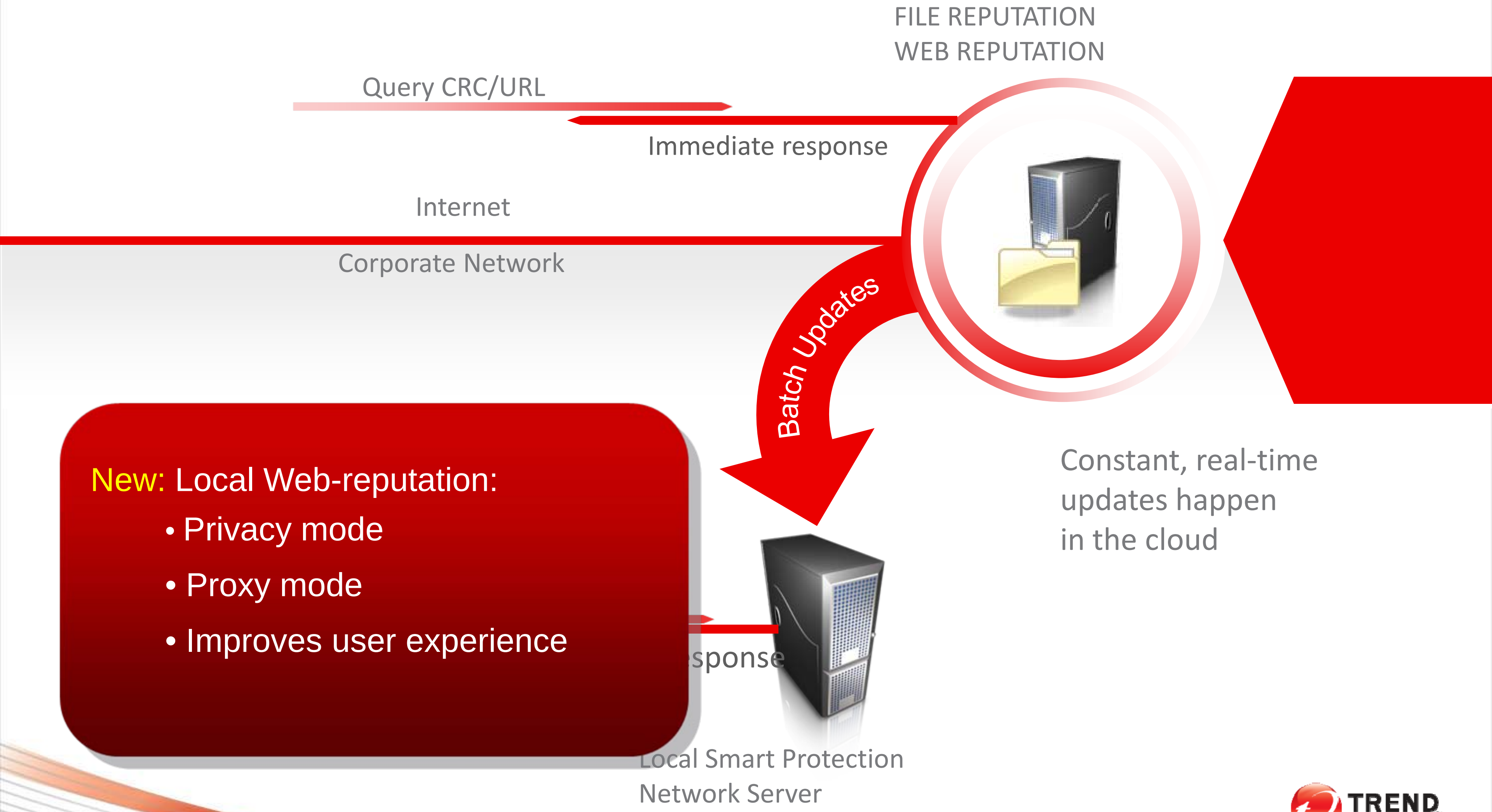
Source: AV-Test.org, Nov '09

* Data referenced from the NSS Labs report: *Endpoint Security Socially Engineered Malware Protection Comparative Test Results Corporate Products*

Smart Protection Network



Released in 2010: Enteprise-scale Local Cloud Option for File Reputation AND Web Reputation

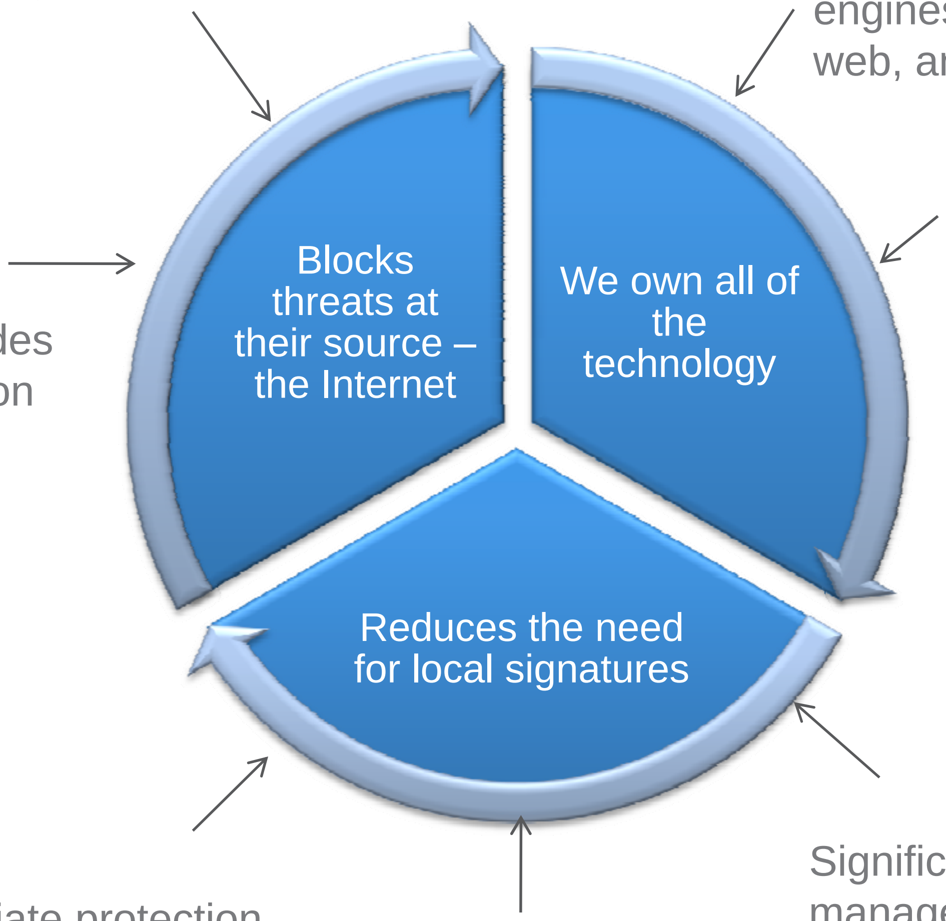


Constant, real-time updates happen in the cloud

New: Local Web-reputation:

- Privacy mode
- Proxy mode
- Improves user experience

Smart Protection Network Key Benefits



Blocks threats at their source – the Internet

We own all of the technology

Reduces the need for local signatures

Threats blocked before they reach you network

Patented correlation engines across email, web, and file

Available across all solutions

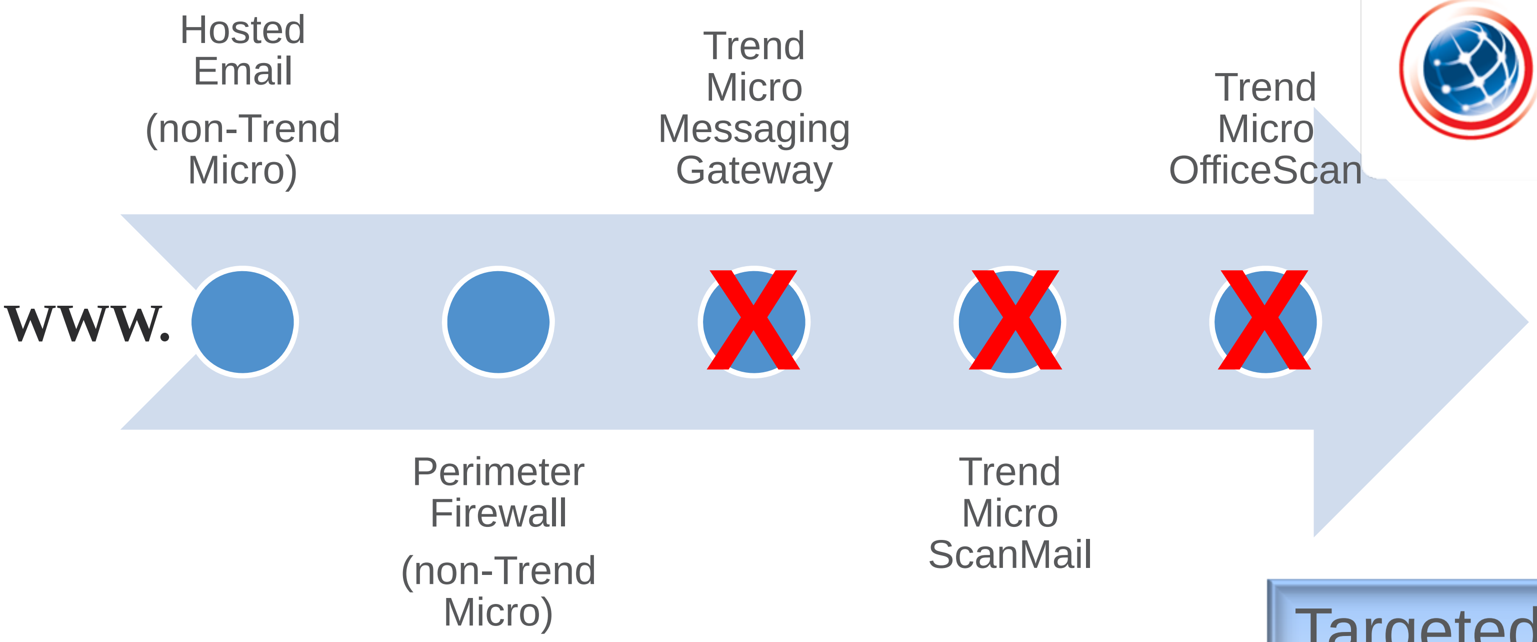
Feedback loop provides customized protection

Significantly reduced management burden

Immediate protection

Reduced bandwidth consumption

Flow and targeted attack pitch



www.

Hosted Email

(non-Trend Micro)

Perimeter Firewall

(non-Trend Micro)

Trend Micro Messaging Gateway

Trend Micro ScanMail

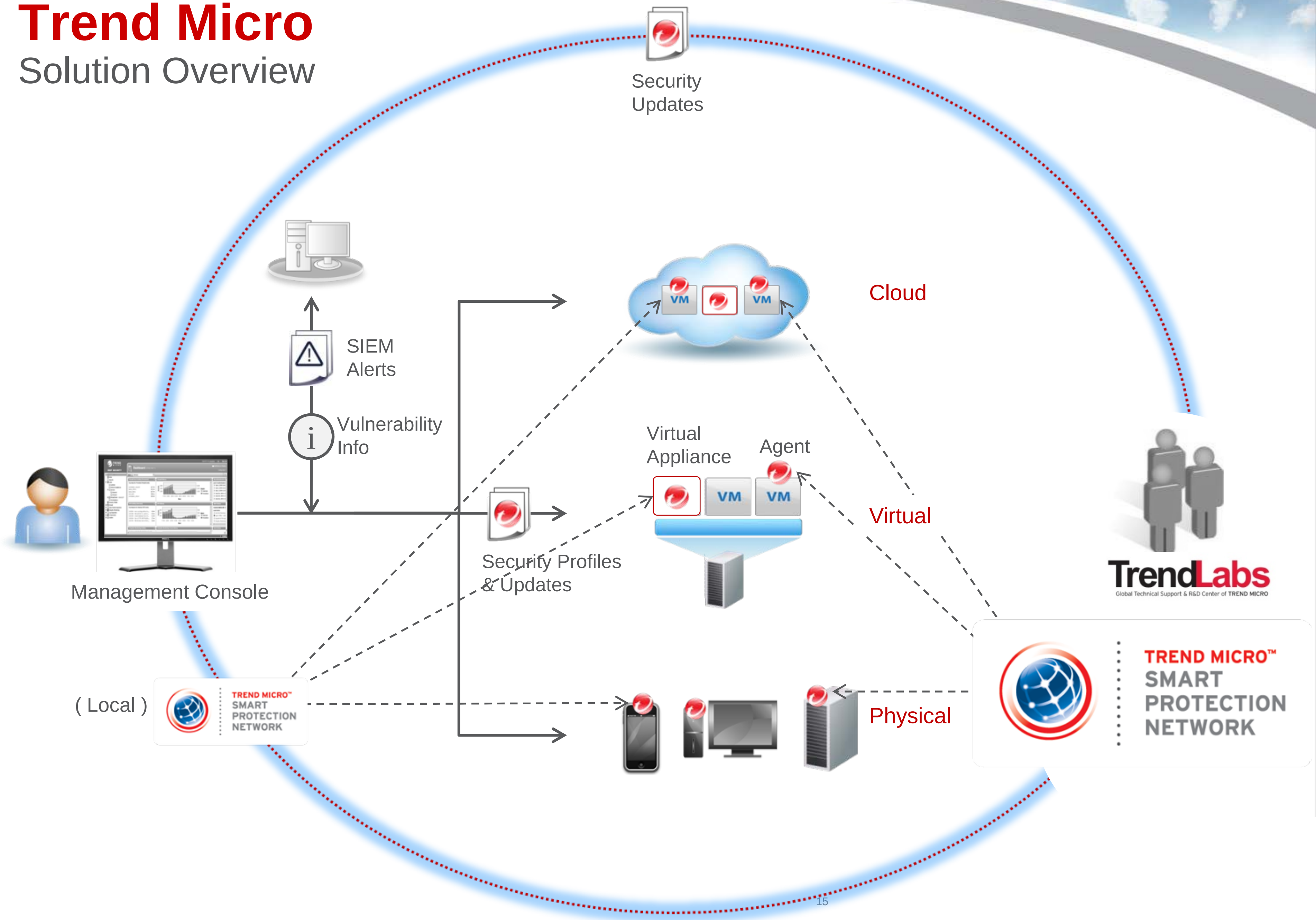
Trend Micro OfficeScan

TREND MICRO™ SMART PROTECTION NETWORK

Targeted Attacks Need Custom Protection

Trend Micro

Solution Overview



Security Updates
SIEM Alerts
Vulnerability Info
Cloud
VM
VM
Virtual Appliance
Agent
VM
VM
Virtual
Management Console
Security Profiles & Updates
TrendLabs
Global Technical Support & R&D Center of TREND MICRO
TREND MICRO™ SMART PROTECTION NETWORK
(Local)
TREND MICRO™ SMART PROTECTION NETWORK
Physical

Securing Your Web World

The Users
Multi-Device Mobile Computing Protection

The user conundrum

RFI Process

I need..

Zero-day/HIPs

Mobile

Encryption

Data Leakage

PO Process

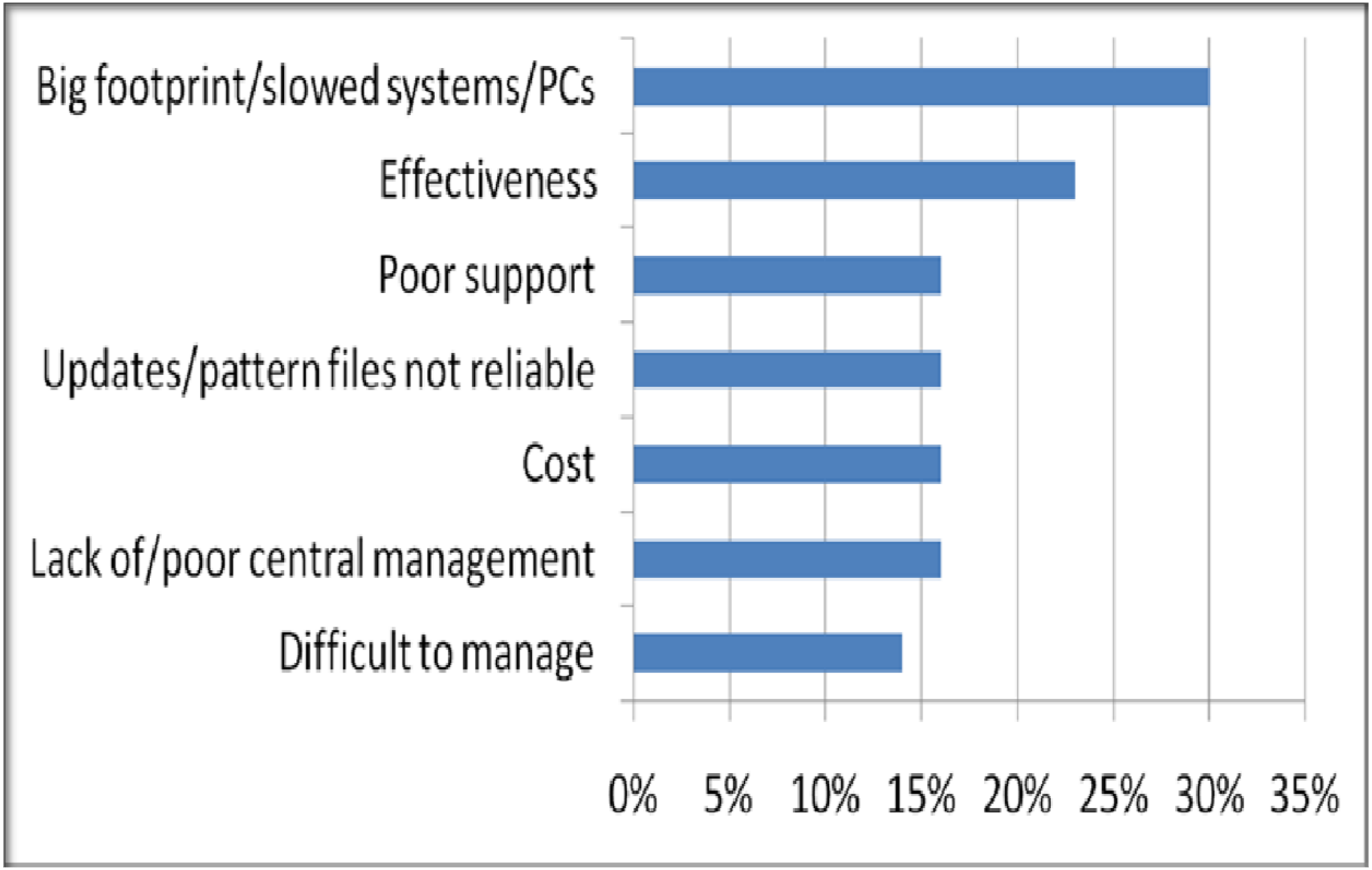
I'll buy..

Performance

1, 2, 3

Ease of management

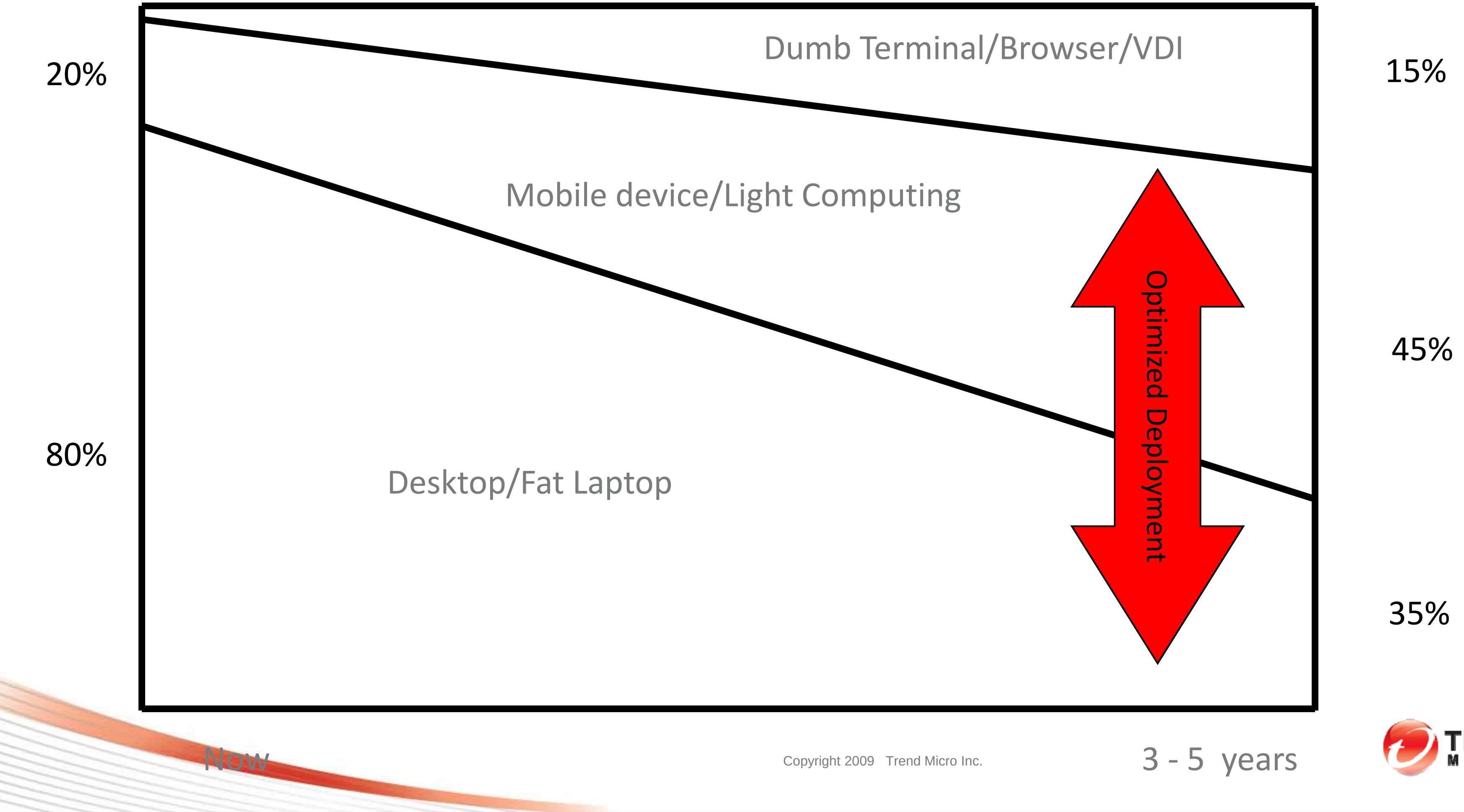
Why are you switching endpoints ?



Our view of market evolution

End Point Revolution

Increase End Point Coverage and market share and upsell data protection modules.



Endpoint Roadmap Priorities for 2011

Client and network performance

Plug-in architecture for flexible add-on security

Intelligent multi-device computing security

Off and on-network policy enforcement

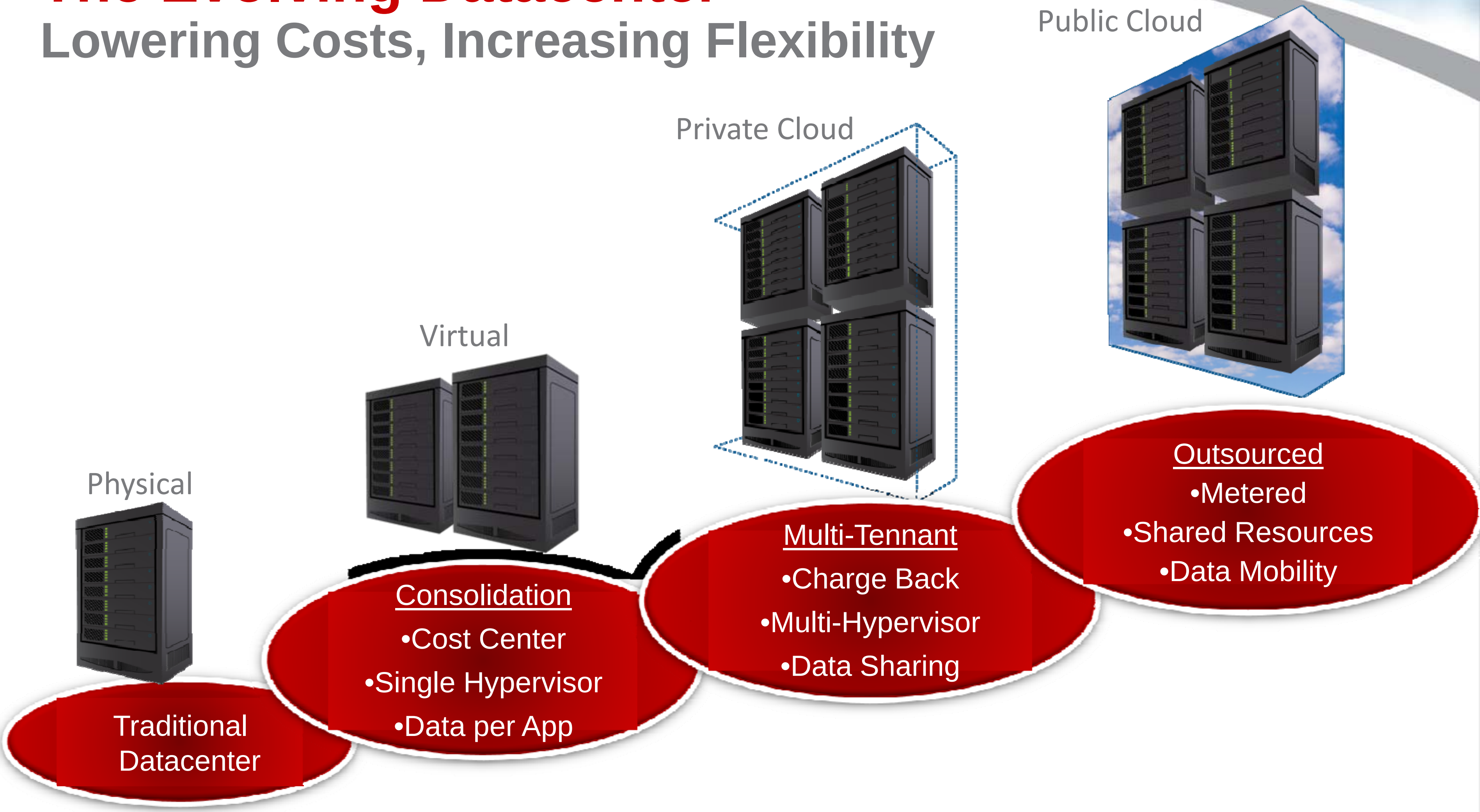
Command center and SIEM integration

Securing Your Web World

The Providers
Physical, Virtual, Private, Public, and Hybrid

The Evolving Datacenter

Lowering Costs, Increasing Flexibility



Physical

Traditional Datacenter

Virtual

Consolidation

- Cost Center
- Single Hypervisor
- Data per App

Private Cloud

Multi-Tennant

- Charge Back
- Multi-Hypervisor
- Data Sharing

Public Cloud

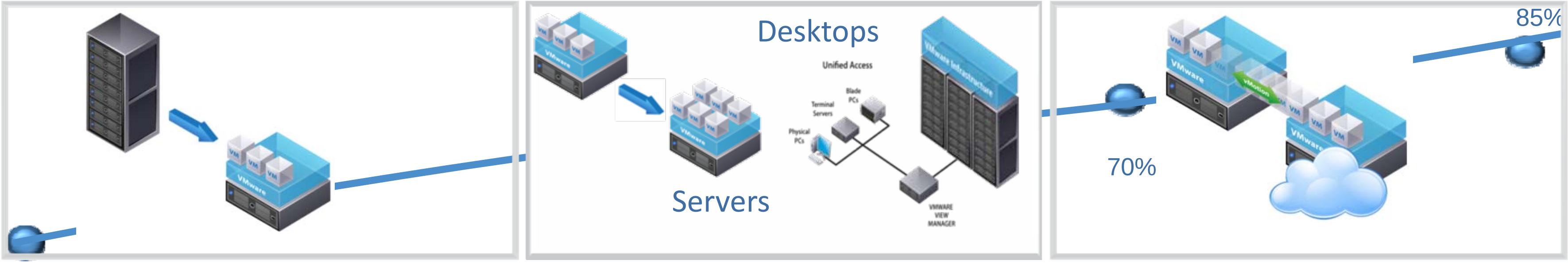
Outsourced

- Metered
- Shared Resources
- Data Mobility

Network & Infrastructure Security Need To Evolve

“Typical” Customer Virtualization Evolution

Stage 1 Consolidation	Stage 2 Expansion & Desktop	Stage 3 Private > Public Cloud



DC Consolidation	Mission critical applications & Endpoint Control	Public and private cloud
- Non-mission critical base applications - Standardized hypervisor - VM Management	- Performance becomes critical -API and advanced management use VDI sampling -Enhanced Compliance controls	- Multi-hypervisor -Virtualized storage -Multi-tenancy -Workload Management -Dedicate or Burst to public

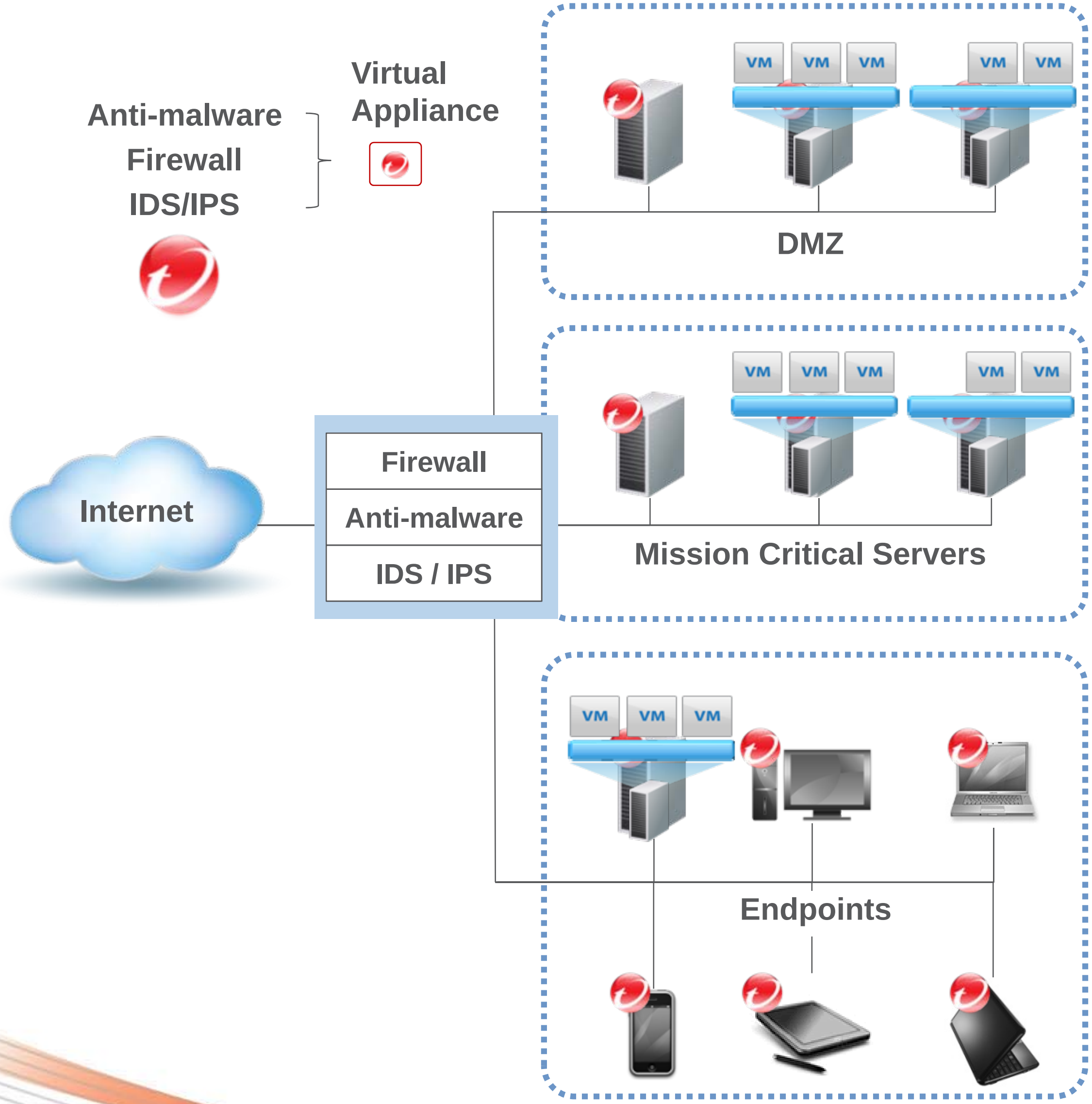
Phase 1 Security Challenge

Perimeter-only (“Outside-in”) approach together with rapid virtualization have created less secure application environments

Through 2012, 60% of virtualized servers will be less secure than the physical servers they replace.

“Addressing the Most Common Security Risks in Data Center Virtualization Projects” Gartner, 25 January 2010

Virtualization

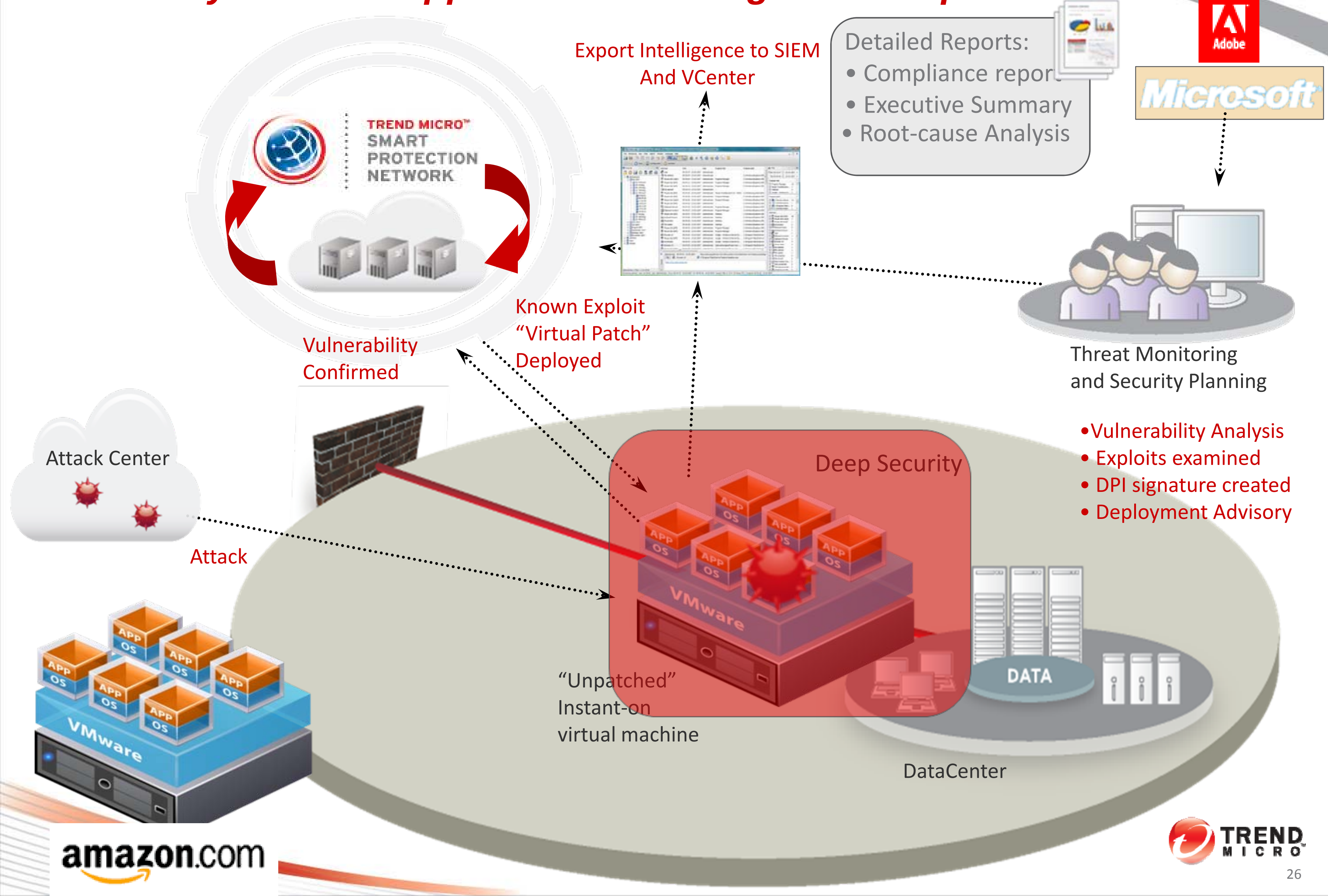


VM
VM
VM
Virtualization

TREND MICRO™ SMART PROTECTION NETWORK

Tying it all together:

Case Study – Virtual Application Patching and Compliance



Export Intelligence to SIEM And VCenter

Detailed Reports:

- Compliance report
- Executive Summary
- Root-cause Analysis

Known Exploit "Virtual Patch" Deployed

Vulnerability Confirmed

Threat Monitoring and Security Planning

- Vulnerability Analysis
- Exploits examined
- DPI signature created
- Deployment Advisory

Attack Center

Attack

Deep Security

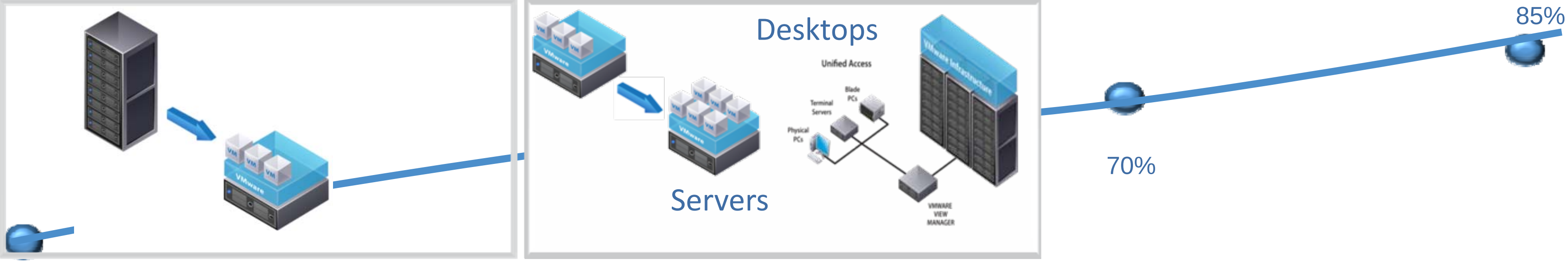
"Unpatched" Instant-on virtual machine

DataCenter

“Typical” Customer Virtualization Evolution

Stage 1
Consolidation

Stage 2
Expansion & Desktop



DC Consolidation

- Non-mission critical base applications
- Standardized hypervisor
-VM Management

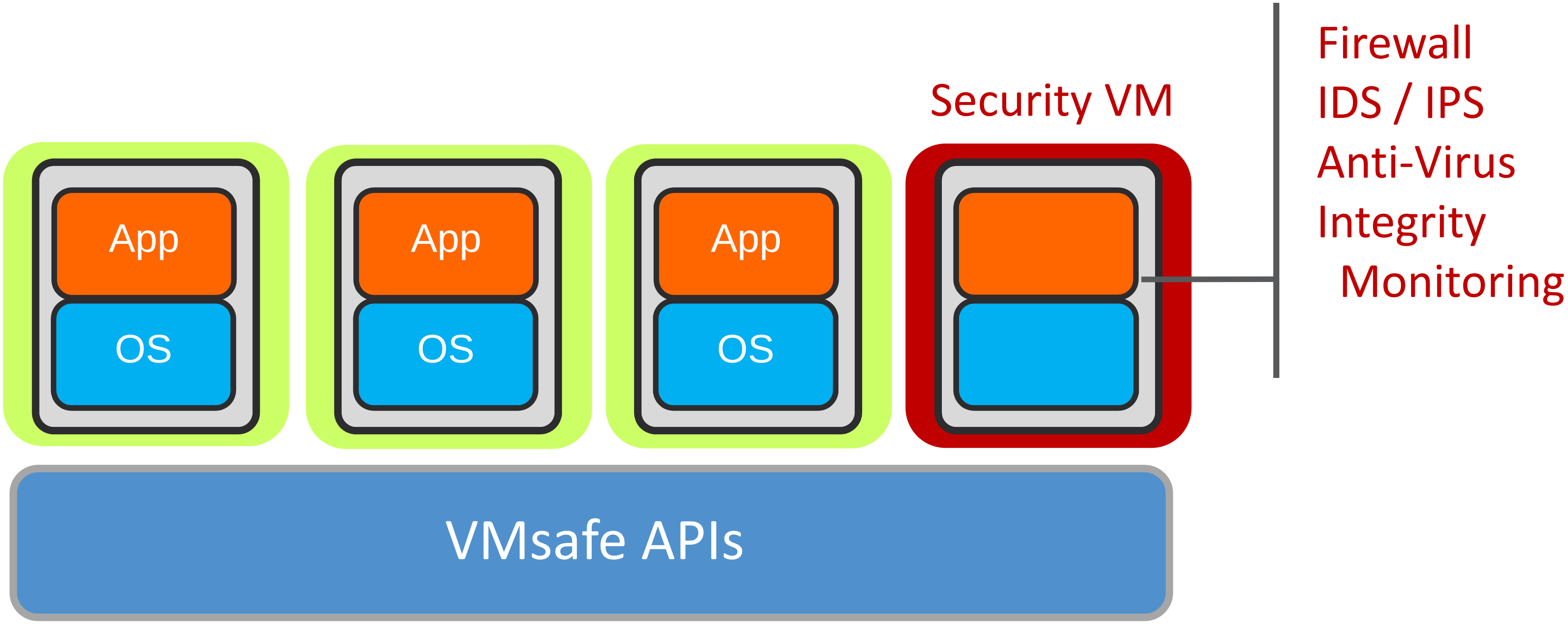
Mission critical applications & Endpoint Control

- Performance becomes critical
-API and advanced management use
VDI sampling
-Enhanced Compliance controls

Phase 2: Security Challenge

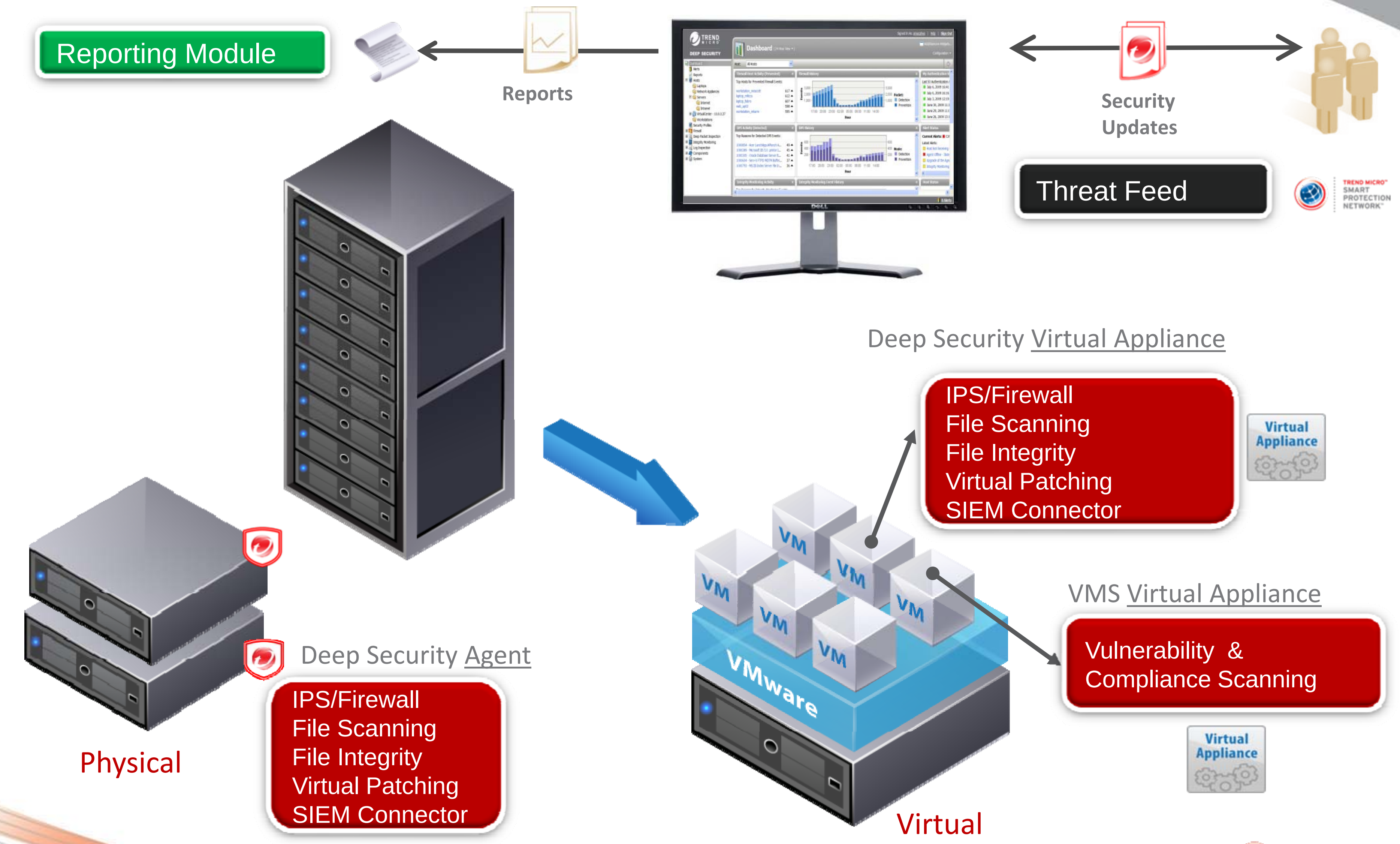
”Virtually unaware” traditional security architectures eliminate the benefits of VDI and virtualized mission-critical applications

Phase II: Concern
Server Performance



- Protect the VM by inspection of virtual components
- Unprecedented security for the app & data inside the VM
- Complete integration with, and awareness of, vMotion, Storage VMotion, HA, etc.

Deep Security Platform



Reporting Module

Reports

Security Updates

Threat Feed

Deep Security Virtual Appliance

- IPS/Firewall
- File Scanning
- File Integrity
- Virtual Patching
- SIEM Connector

VMS Virtual Appliance

Vulnerability & Compliance Scanning

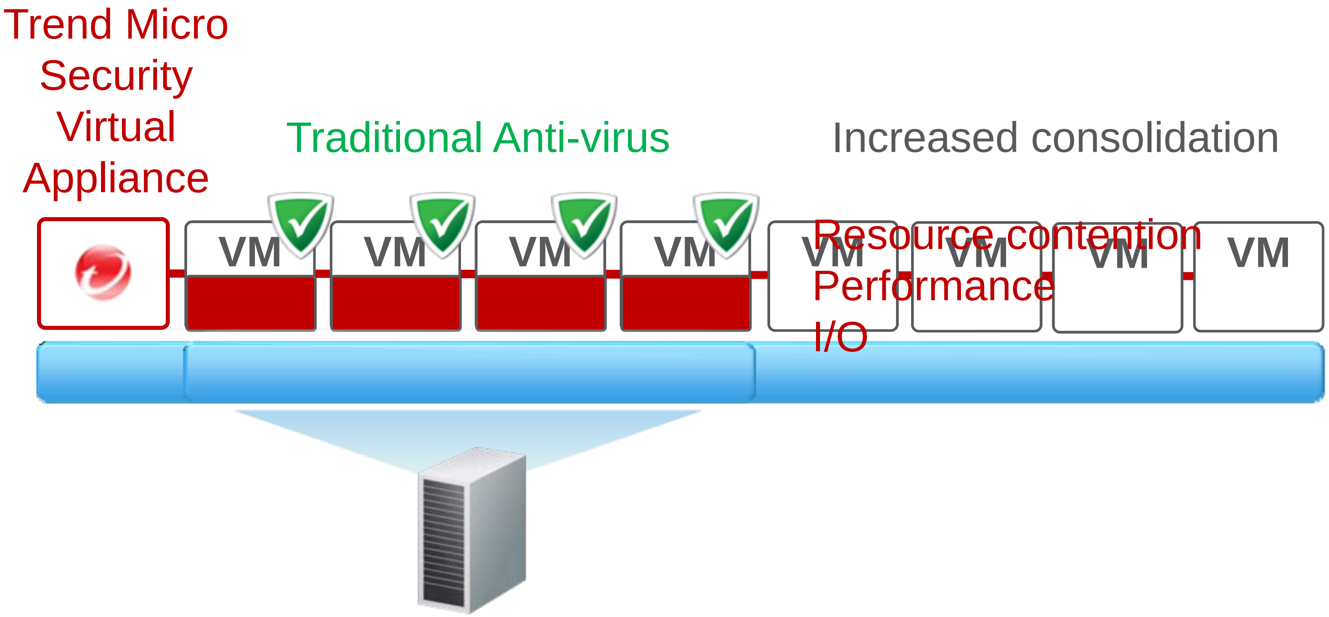
Deep Security Agent

- IPS/Firewall
- File Scanning
- File Integrity
- Virtual Patching
- SIEM Connector

Physical

Virtual

Security Spotlight #1:
Resource contention



Trend Micro VDI solutions more than double the hosts per server

Summary of Phase II Solutions

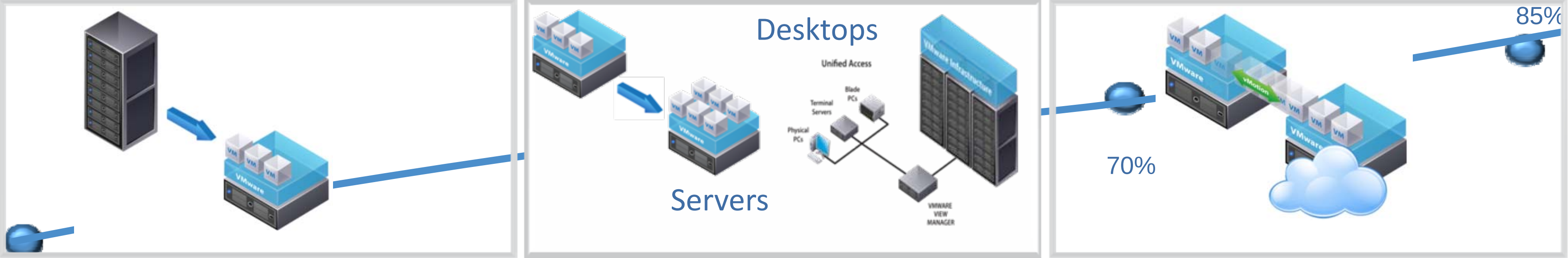
- Physical, virtual and cloud in one platform
- Light and lean agents when deep visibility is required
  - Using cloud-client architecture
- Hybrid application security
  - Cloud-based for scale, on-premise for protection
- Agent-less option for application & server performance
  - Using virtualization APIs
- Architecture optimizes performance across entire infrastructure
  - Processes are “virtually-aware” across CPU, network, and storage

“Typical” Customer Virtualization Evolution

Stage 1
Consolidation

Stage 2
Expansion & Desktop

Stage 3
Private > Public Cloud



DC Consolidation

- Non-mission critical base applications
- Standardized hypervisor
- VM Management

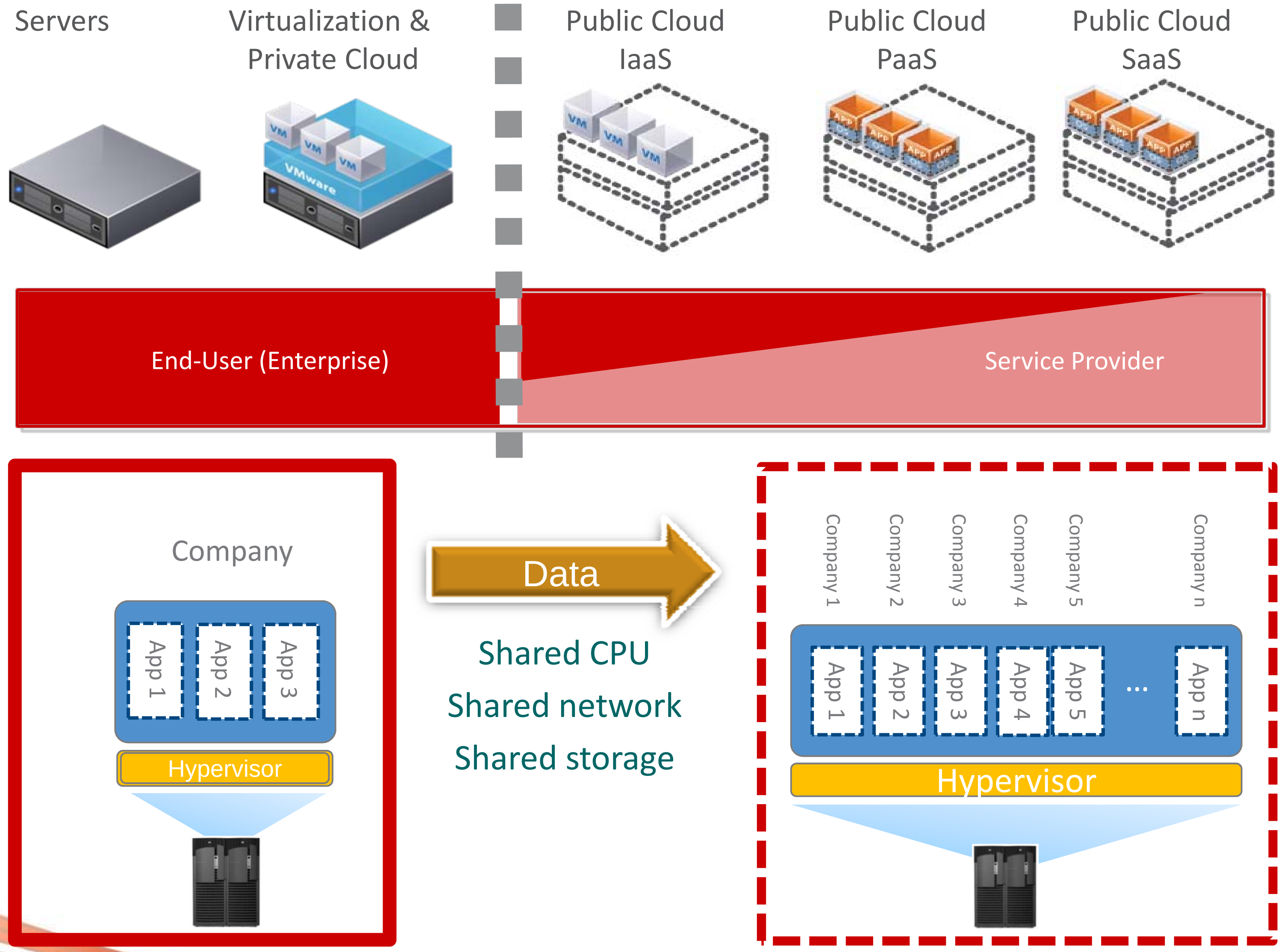
Mission critical applications & Endpoint Control

- Performance becomes critical
-API and advanced management use
VDI sampling
-Enhanced Compliance controls

Hybrid and selected public cloud

- Multi-hypervisor
-Virtualized storage
-Workload Management
-Burst to public

The Public Cloud:
Who Has Control? How Secure is the Data?



Servers

Virtualization & Private Cloud

Public Cloud IaaS

Public Cloud PaaS

Public Cloud SaaS

End-User (Enterprise)

Service Provider

Company

App 1 App 2 App 3

Hypervisor

Data

Shared CPU

Shared network

Shared storage

Company 1 Company 2 Company 3 Company 4 Company 5 Company n

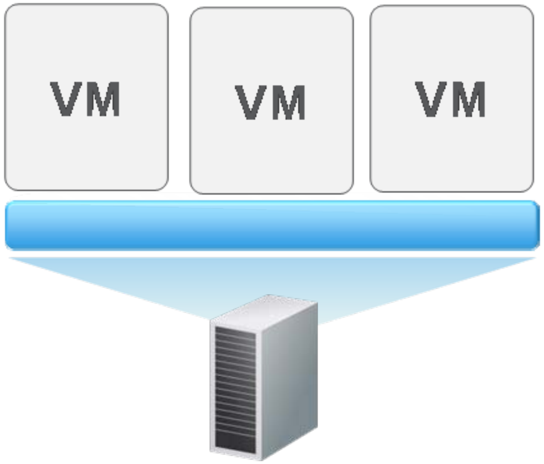
App 1 App 2 App 3 App 4 App 5 … App n

Hypervisor

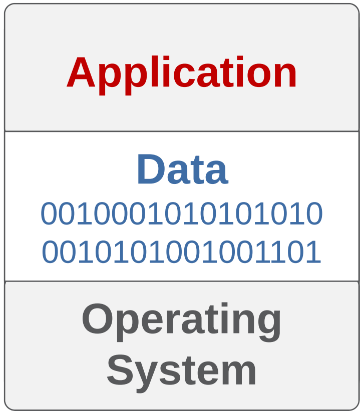
Phase 3: Security Challenge

How do I protect data in a virtualized and multi-tenant storage environment (private, hybrid, or public cloud) ?

Security Spotlight #2:



Virtual Machine Workload



Application

Data
0010001010101010
0010101001001101

Operating System

Key Issues

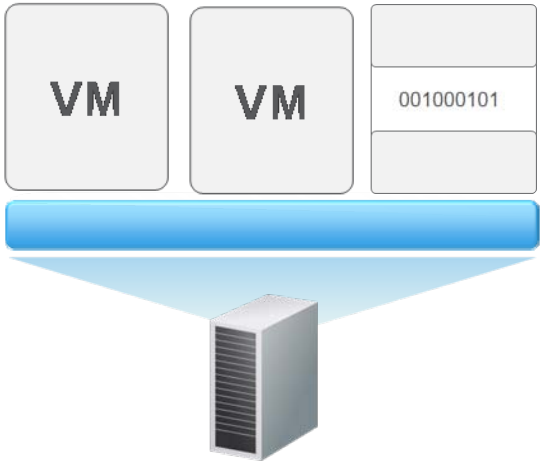
→ Availability

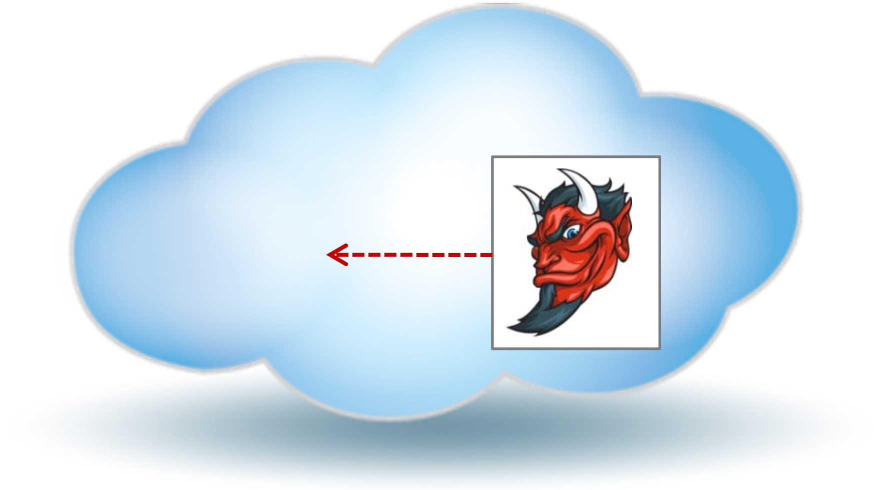
→ Integrity / Privacy

→ Availability

Security Spotlight #2:
Full Workload Encryption

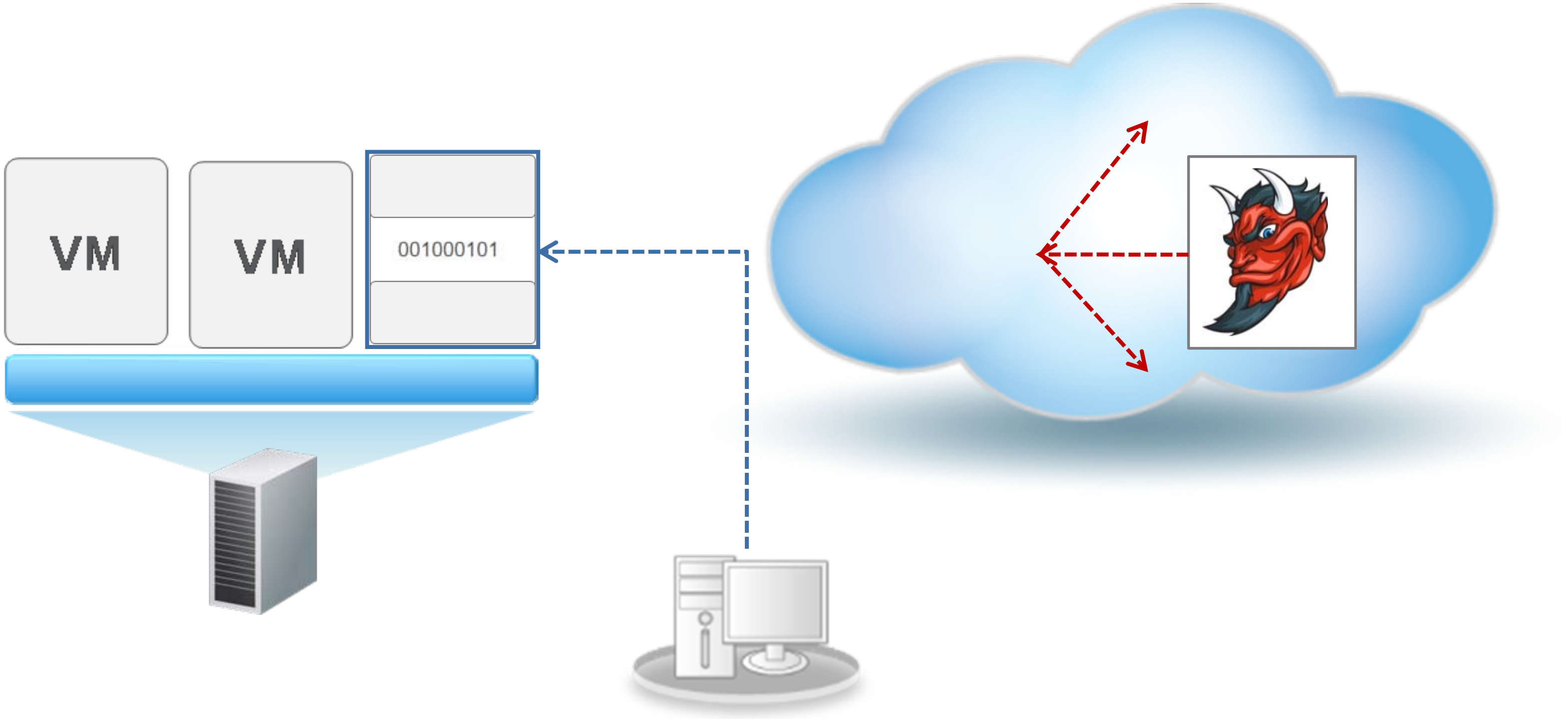
Data Theft





Security Spotlight #2:
Full Workload Encryption

Data is Protected

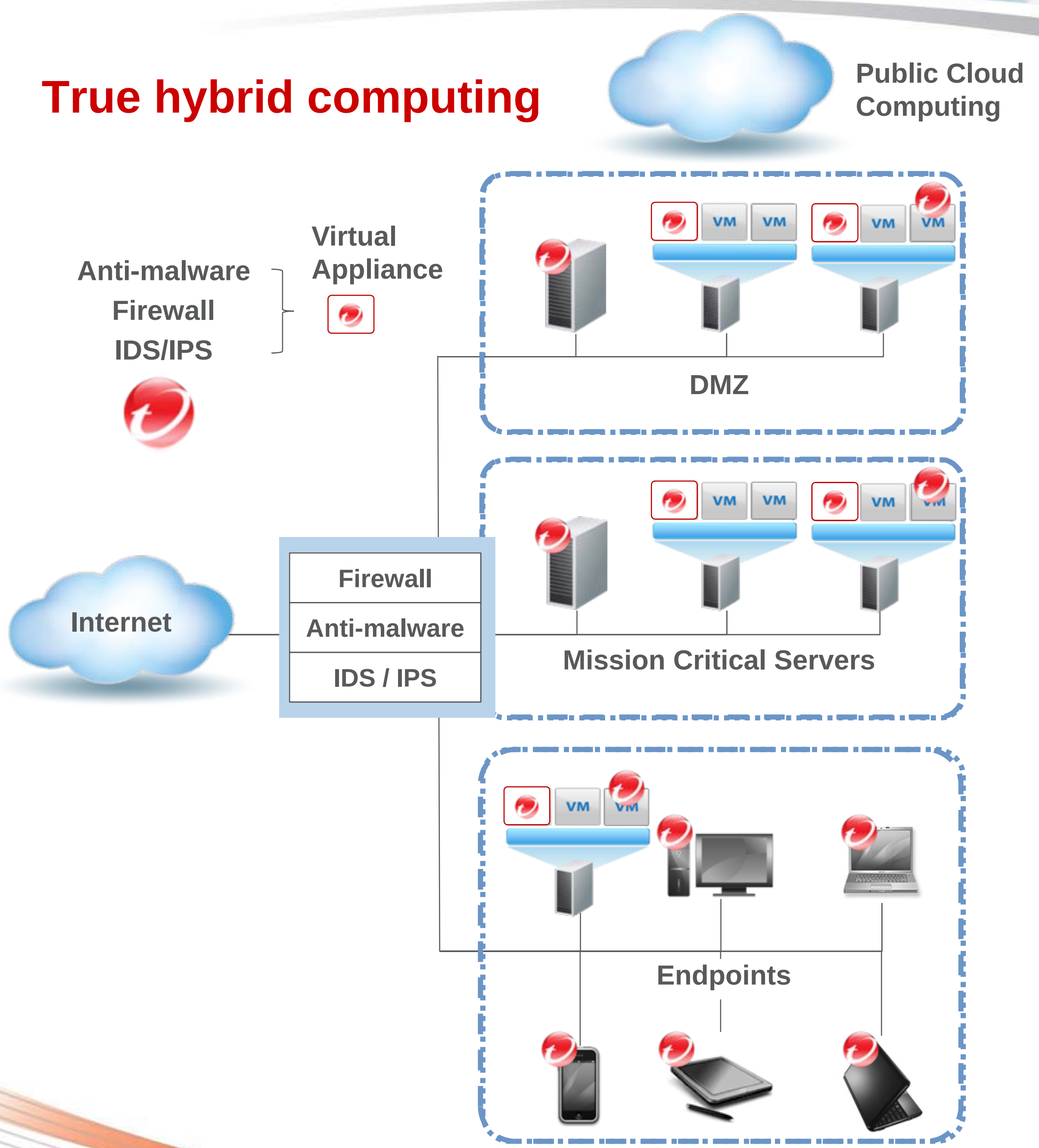


Full Workload Encryption

All Phases: Architecture Security Challenge

How do I bring it all together in a manageable way across virtualized, private and public cloud environments?

True hybrid computing

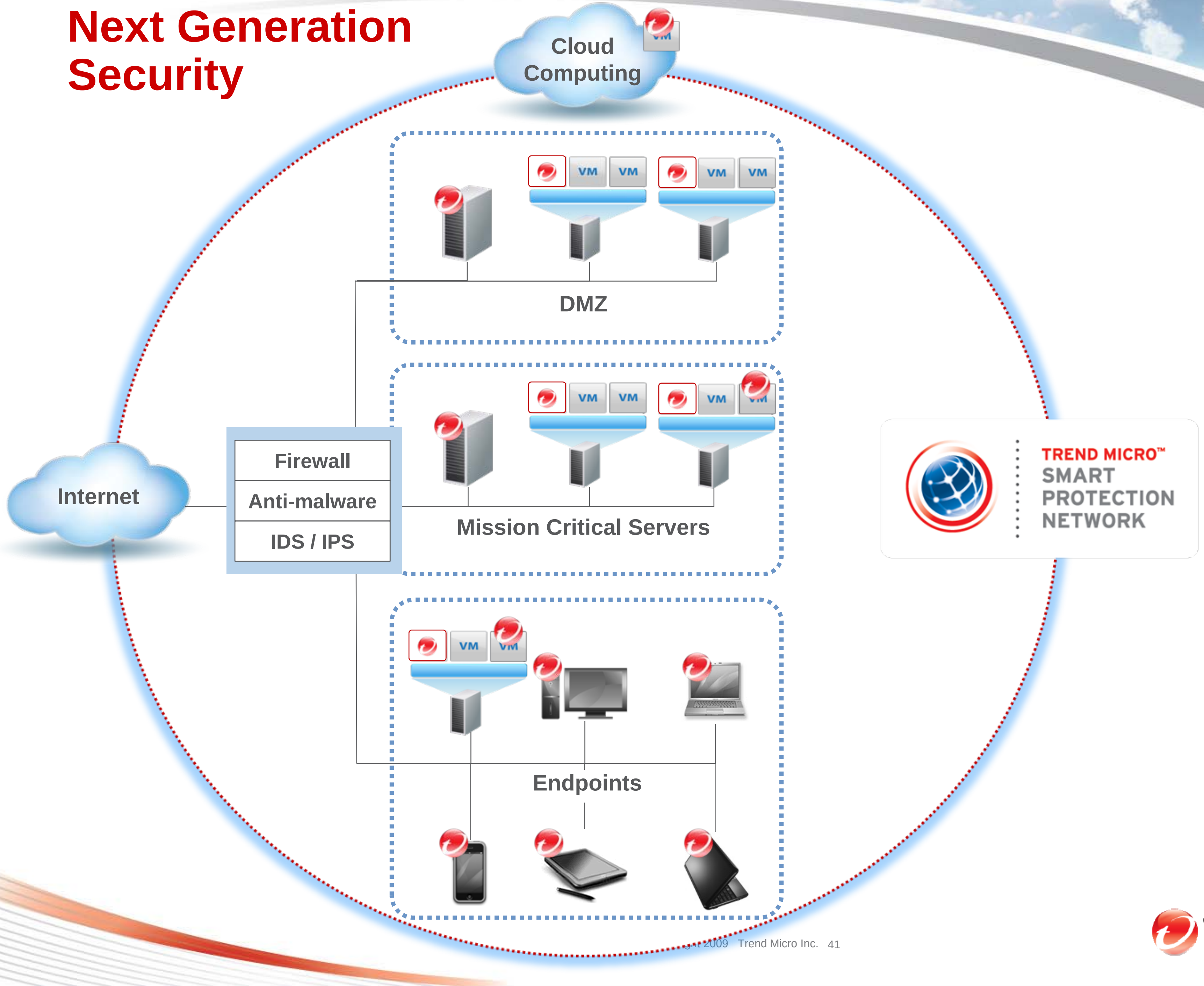


Agent-based protection

- Anti-malware
- Firewall
- IDS/IPS
- Integrity Monitoring
- Encryption

TREND MICRO™ SMART PROTECTION NETWORK

Next Generation Security



“Typical” Customer Virtualization Evolution

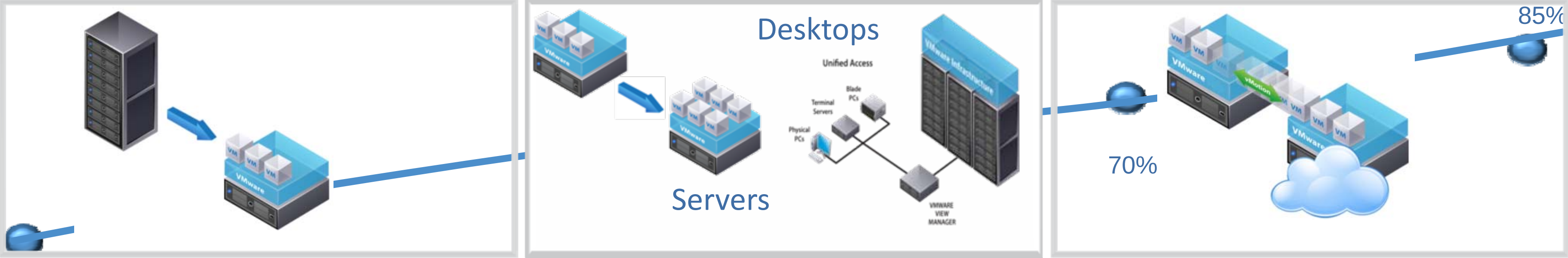
Stage 1
Consolidation

→

Stage 2
Expansion & Desktop

→

Stage 3
Private > Public Cloud



Secure the workload

Deep Security

Architected for performance

OfficeScan 10.5

Deep Security

Data secured prior to mobility

SecureCloud

Optimized Cloud Security Architecture

Smart Protection Network

GET TECHIE

Virtualization needs virtualization security

Massive Cost Reduction

Speed and Business Impact

Expertise and Performance

NEEDS A “BETTER-THAN-PHYSICAL” CLOUD SECURITY ARCHITECTURE

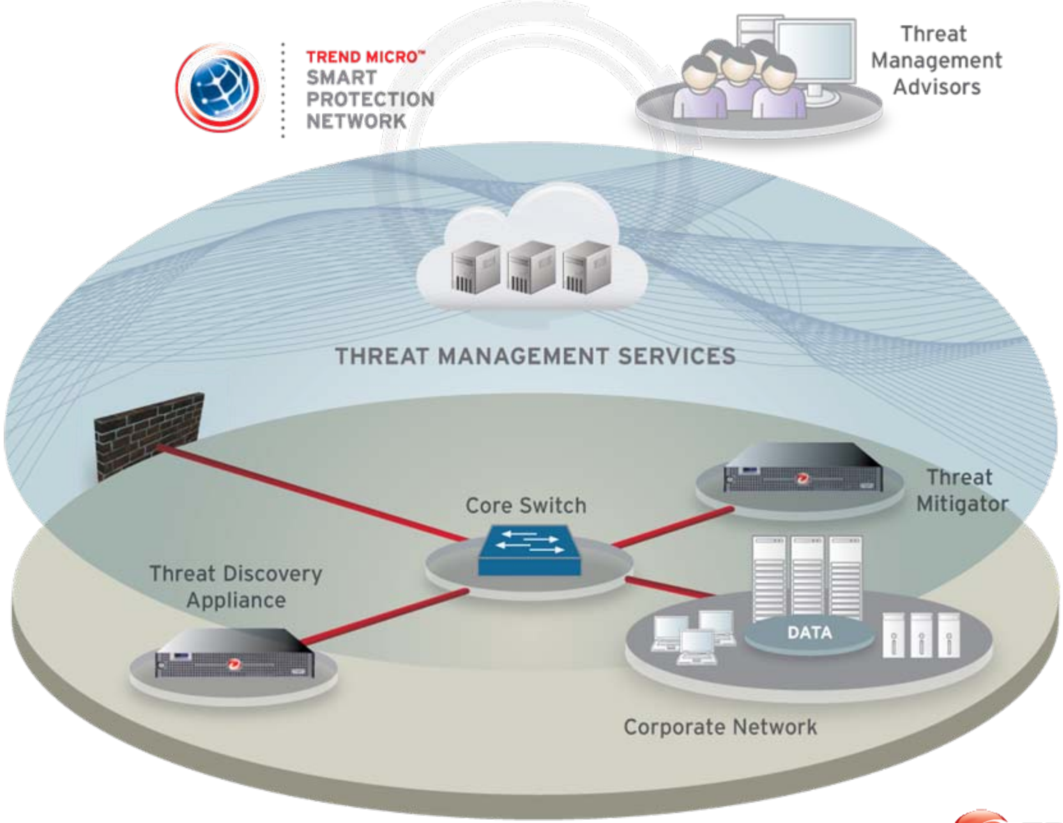
Securing Your Web World

Tying it All Together with Management and Services

Components of Trend Micro Services

Security services that strengthens an organization’s ability to deal with incidents:

- Threat Discovery
- Threat Containment
- Threat Remediation
- Incident Command Center
- Integration with SIEM

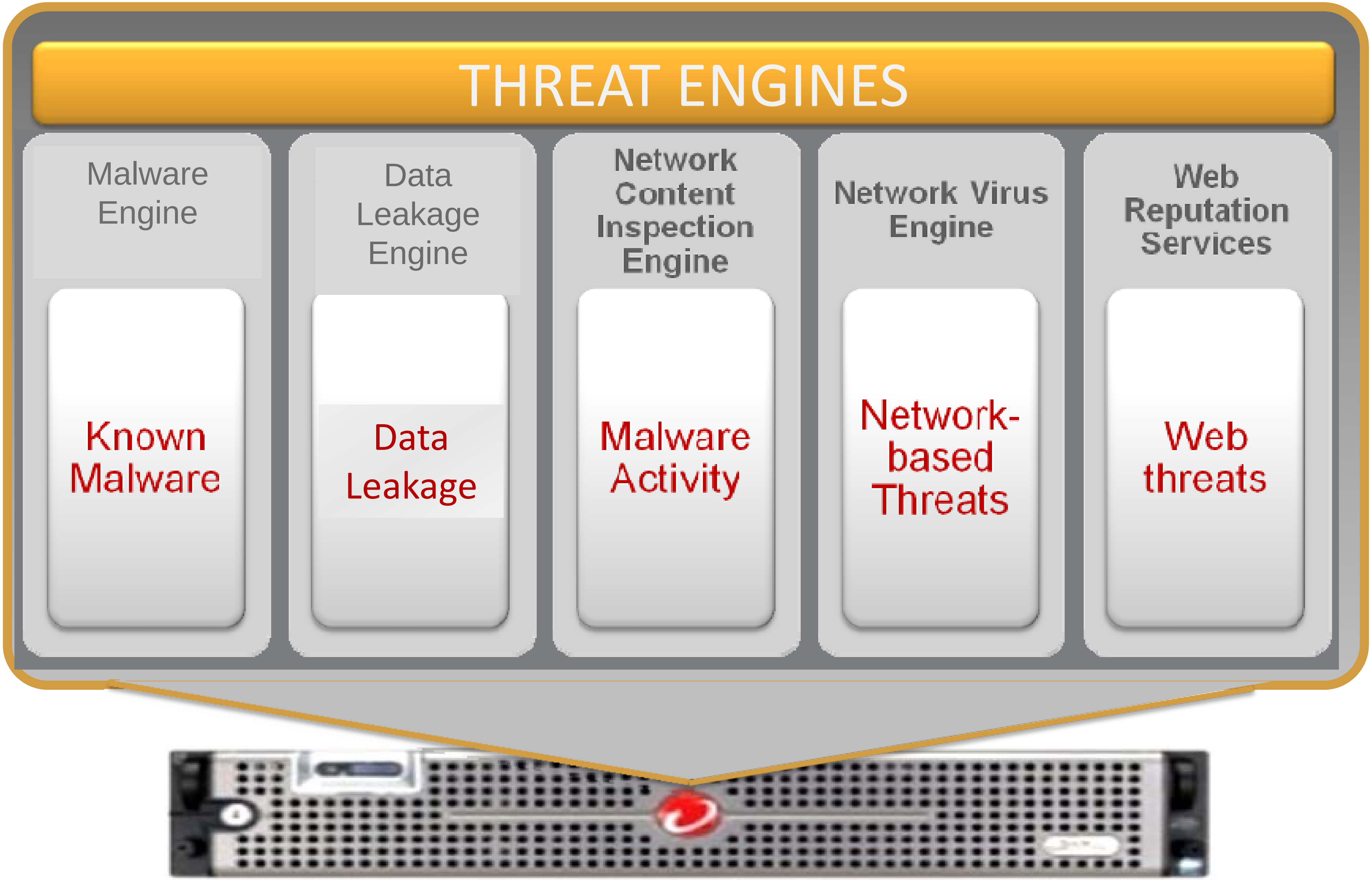

TREND MICRO™ SMART PROTECTION NETWORK
Threat Management Advisors
THREAT MANAGEMENT SERVICES
Core Switch
Threat Mitigator
Threat Discovery Appliance
DATA
Corporate Network

CIO Insight Vendor Value Survey

... Delivering Required Support

1. Cisco
2. NetApp
3. Trend Micro

Threat Discovery Technology



THREAT ENGINES

Malware Engine

Known Malware

Data Leakage Engine

Data Leakage

Network Content Inspection Engine

Malware Activity

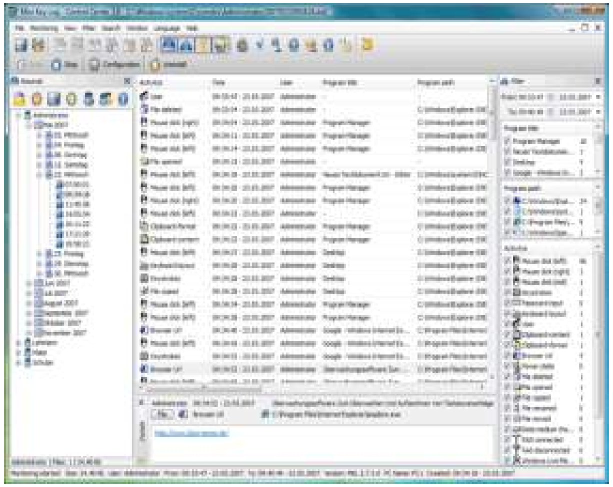
Network Virus Engine

Network-based Threats

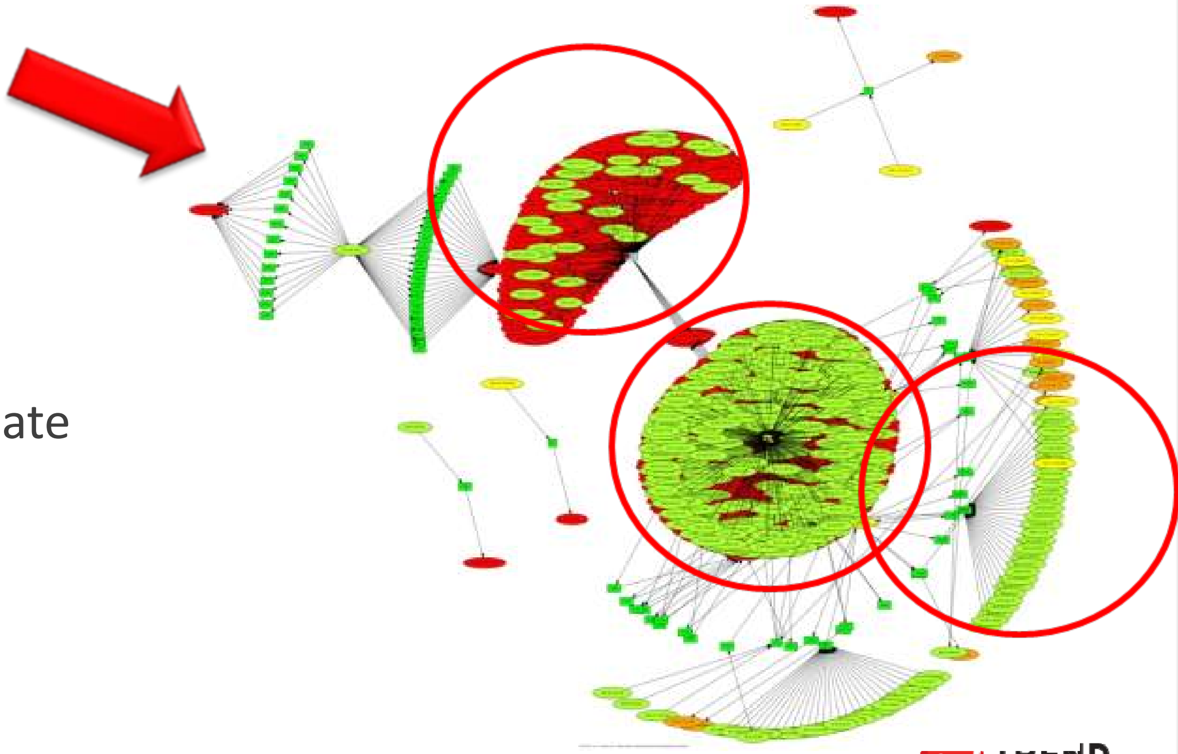
Web Reputation Services

Web threats

Next Generation Management

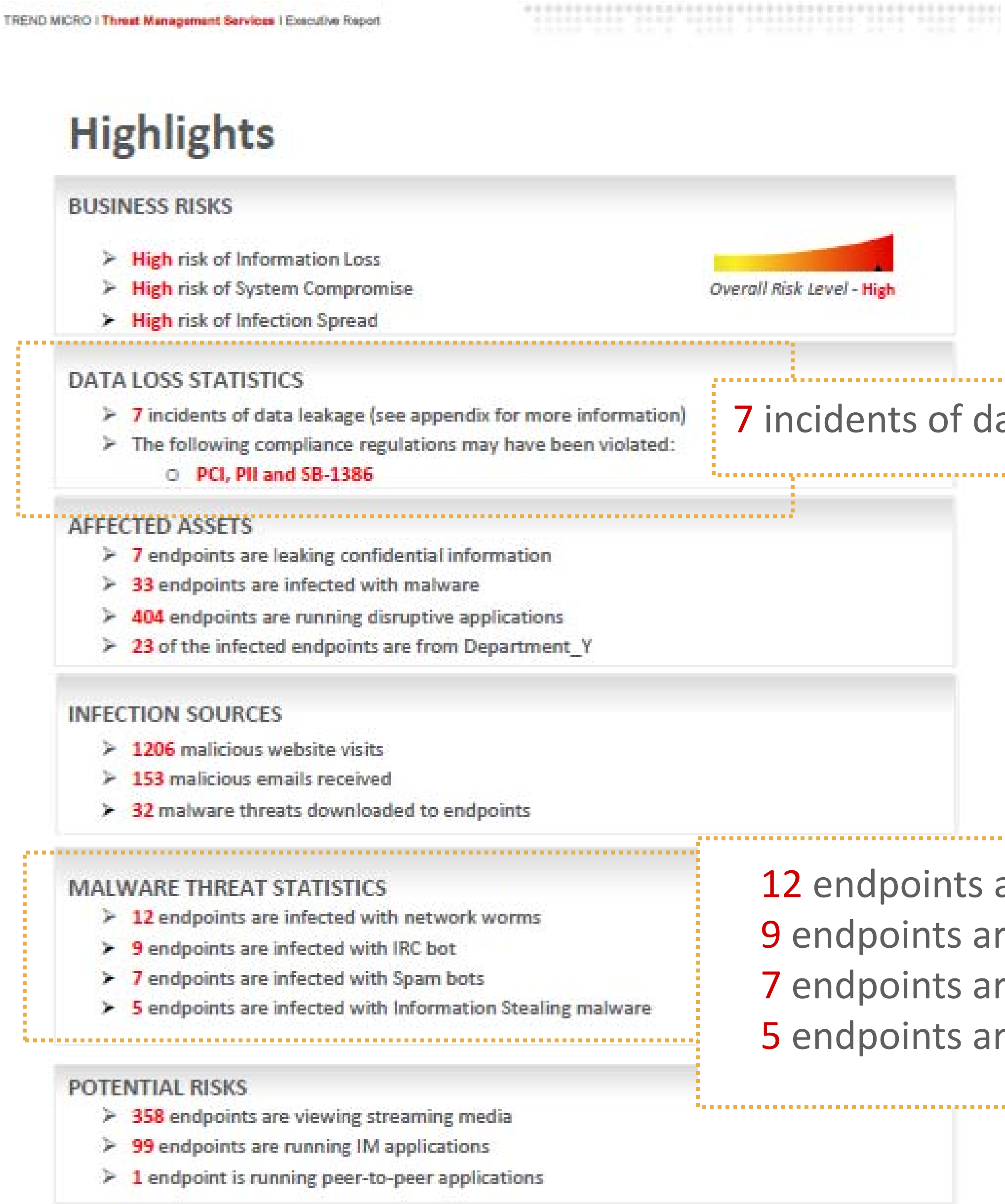


A picture is worth a thousand words



- Track the attack in action
- Identify the attack
- Understand the source
- Determine steps to remediate
- Understand root cause
- What was exploited
- Implement prevention

Incident Command Center Report Details



TREND MICRO | Threat Management Services | Executive Report

Highlights

BUSINESS RISKS

- High risk of Information Loss
- High risk of System Compromise
- High risk of Infection Spread

Overall Risk Level - High

DATA LOSS STATISTICS

- 7 incidents of data leakage (see appendix for more information)
- The following compliance regulations may have been violated:
  - PCI, PII and SB-1386

AFFECTED ASSETS

- 7 endpoints are leaking confidential information
- 33 endpoints are infected with malware
- 404 endpoints are running disruptive applications
- 23 of the infected endpoints are from Department_Y

INFECTION SOURCES

- 1206 malicious website visits
- 153 malicious emails received
- 32 malware threats downloaded to endpoints

MALWARE THREAT STATISTICS

- 12 endpoints are infected with network worms
- 9 endpoints are infected with IRC bot
- 7 endpoints are infected with Spam bots
- 5 endpoints are infected with Information Stealing malware

POTENTIAL RISKS

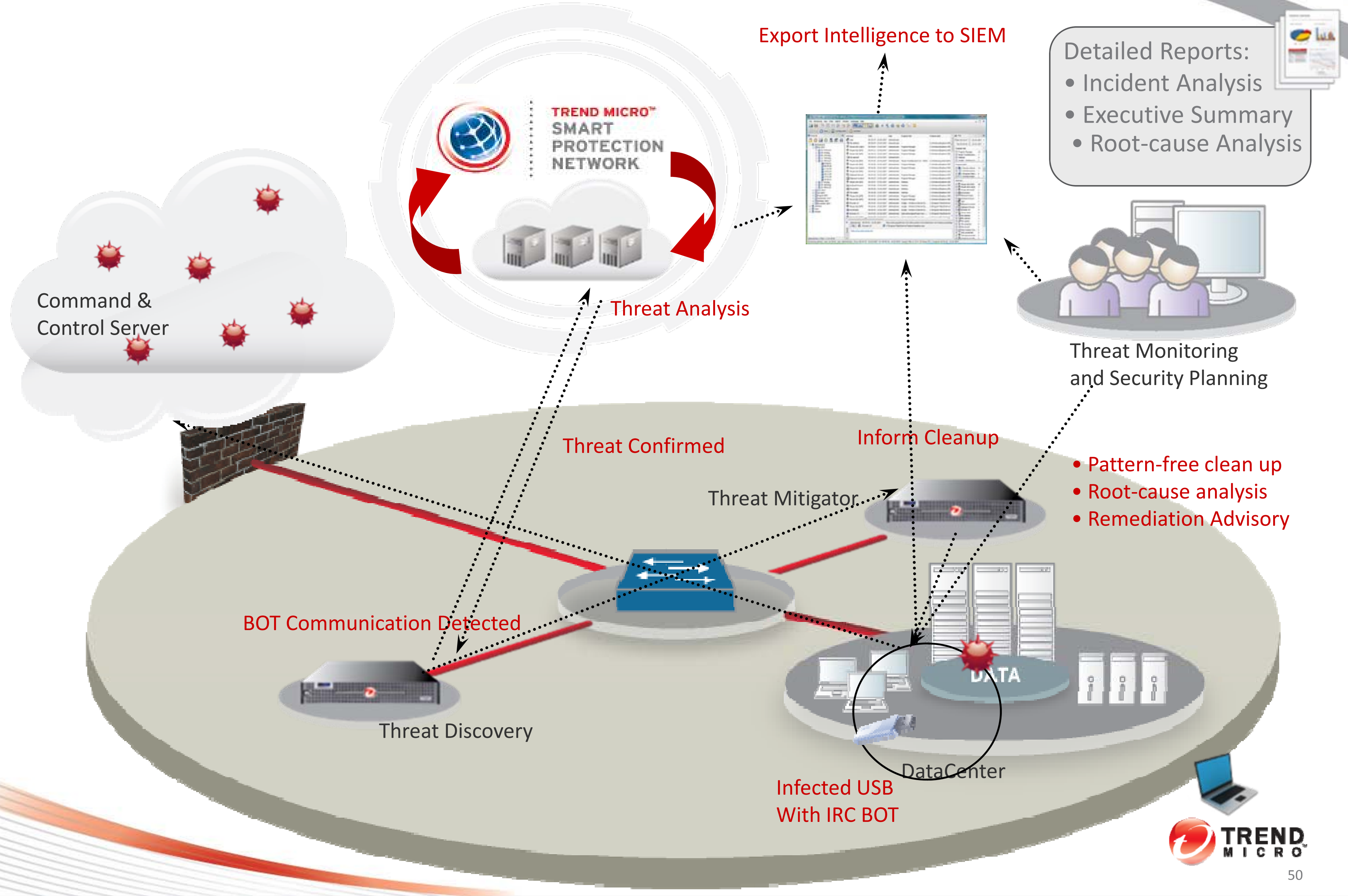
- 358 endpoints are viewing streaming media
- 99 endpoints are running IM applications
- 1 endpoint is running peer-to-peer applications

7 incidents of data leakage

12 endpoints are infected with network worms
9 endpoints are infected with IRC bots
7 endpoints are infected with Spam bots
5 endpoints are infected with info stealing malware

Tying the model together – Threat Management

Case Study -- IRC Bots



Export Intelligence to SIEM

Detailed Reports:

- Incident Analysis
- Executive Summary
- Root-cause Analysis

Command & Control Server

Threat Analysis

Threat Monitoring and Security Planning

Threat Confirmed

Inform Cleanup

- Pattern-free clean up
- Root-cause analysis
- Remediation Advisory

Threat Mitigator

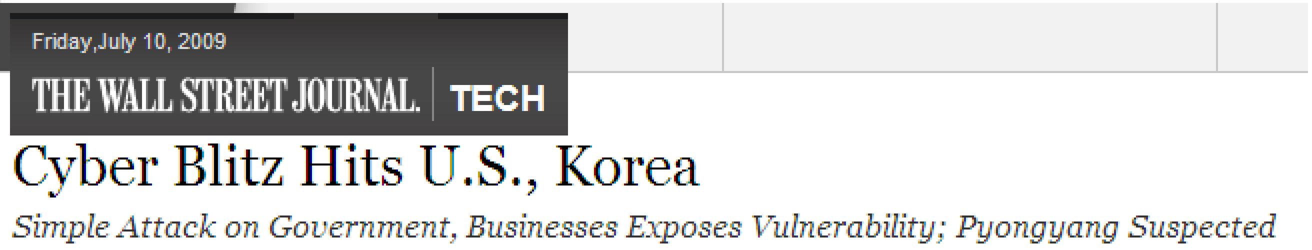
BOT Communication Detected

Threat Discovery

DataCenter

Infected USB
With IRC BOT

South Korean Botnet Attack – July 4th 2009

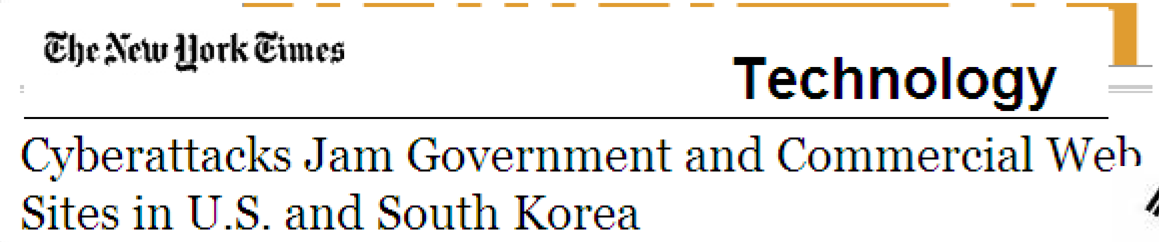


Friday,July 10, 2009

THE WALL STREET JOURNAL. | TECH

Cyber Blitz Hits U.S., Korea

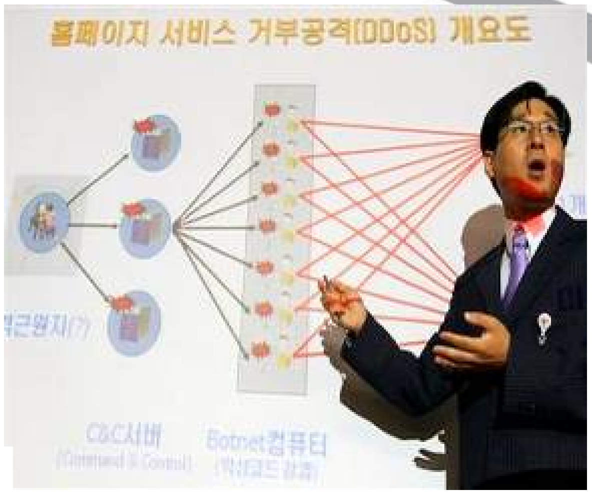
Simple Attack on Government, Businesses Exposes Vulnerability; Pyongyang Suspected



The New York Times

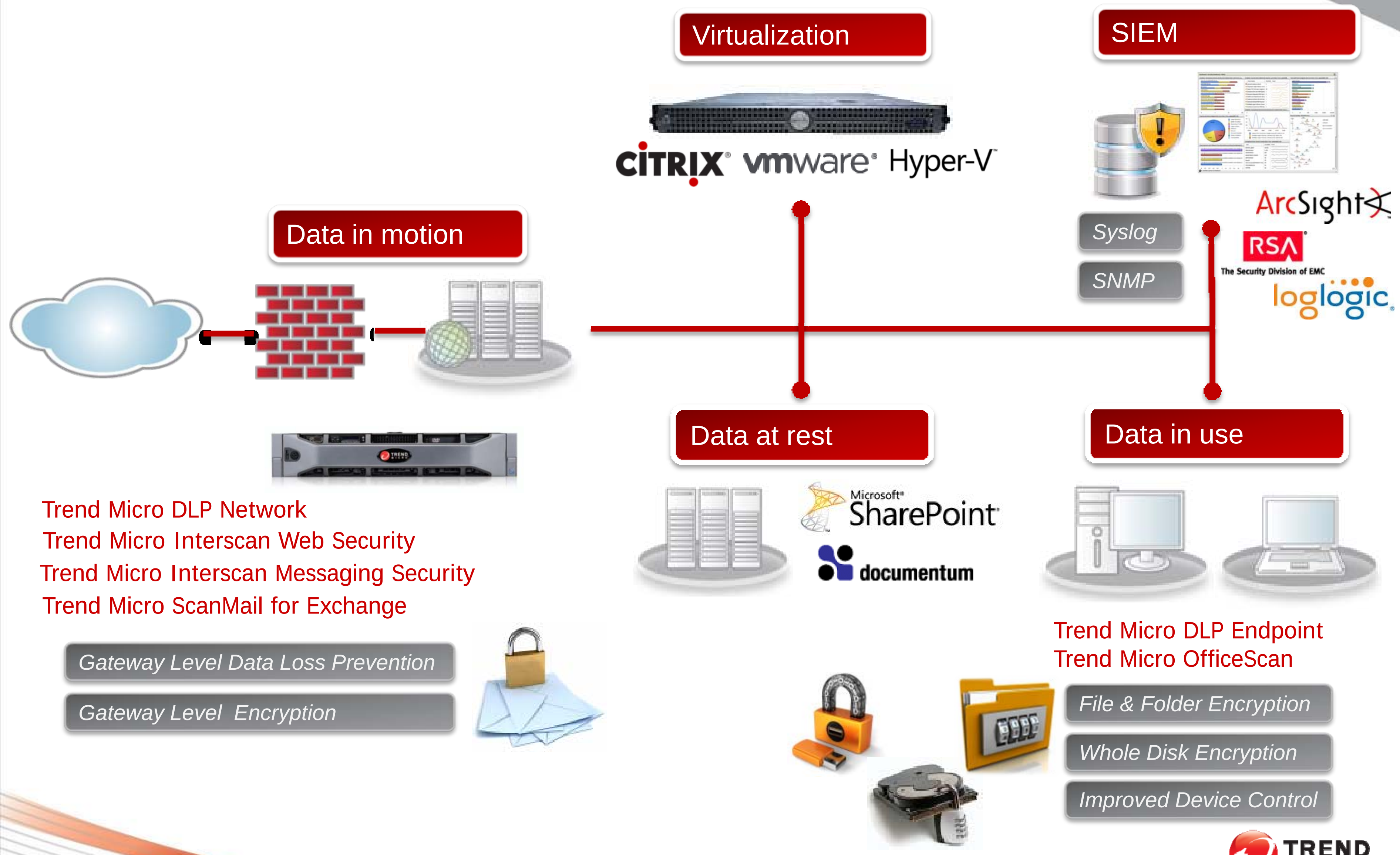
Technology

Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea



- Korean eBay Auction site shut down for 72 hours
- Hackers tried to shut down entire South Korean National Infra.
- Several Government sites shut down or compromised. Data destroyed.
- Cabinet Ministerial Level task force setup. Annual budget 25 M dollars.
- 6 Government Ministries set up to adopt anti-botnet initiative.
- Trend Micro chosen by Ministry of Education & Ministry of Public Administration

Trend Micro Data Loss Prevention Solution Vision



Trend Micro DLP Network
Trend Micro Interscan Web Security
Trend Micro Interscan Messaging Security
Trend Micro ScanMail for Exchange

Gateway Level Data Loss Prevention

Gateway Level Encryption

Trend Micro DLP Endpoint
Trend Micro OfficeScan

File & Folder Encryption

Whole Disk Encryption

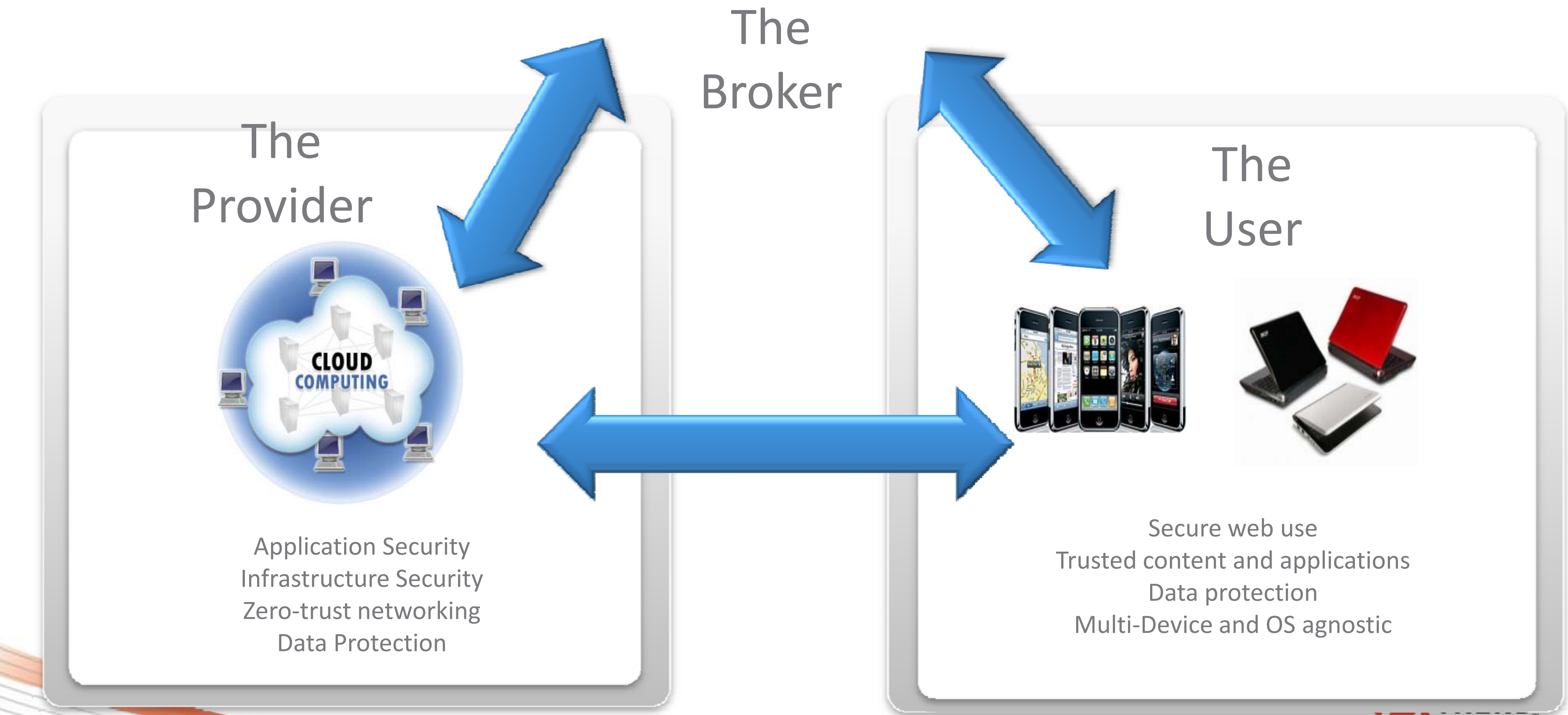
Improved Device Control

Long Term Product Strategy Vision
3 components in the cloud ecosystem

- Threat Trends
- Reputation Services
- Global Watch

TREND MICRO™ SMART PROTECTION NETWORK™

- Off-network/On-network
- Event Correlation
- Event and Incident Management
- Remediation Services



The Broker

The Provider

Application Security
Infrastructure Security
Zero-trust networking
Data Protection

The User

Secure web use
Trusted content and applications
Data protection
Multi-Device and OS agnostic

Q&A

Why we think we offer the best security

- Security is what we do and ALL that we do
- The platform change is here…..or not
- We have a significant lead in the new platform protecting the **provider for the cloud and from the cloud**
- We have the best architecture to secure the multi-device mobile computing **user**
- We are the only real-time, custom, environment-specific security **broker** -- with services to match
- Our model can deploy anywhere – public, private, or hybrid
- It can scale to any size
- It is built for speed
- It is the security model of the future