RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

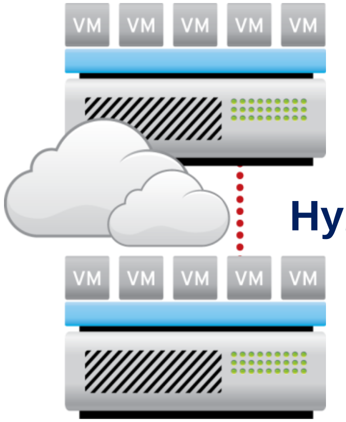
Defense Against Threats in the Cloud

Dave Asprey

VP Cloud Security

Trend Micro
@daveasprey
Blog : cloudsecurity.trendmicro.com

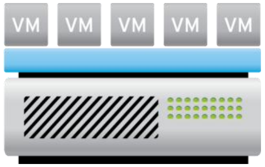
What’s Not a Cloud Anyway?



Hybrid Cloud

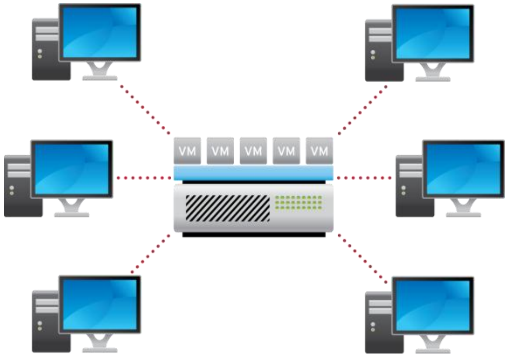
IaaS

Physical Desktops & Servers



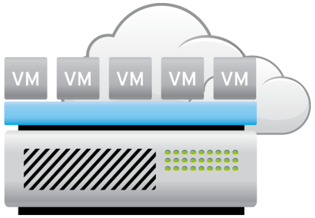
Server Virtualization

BYOPC



Desktop Virtualization

Mobile

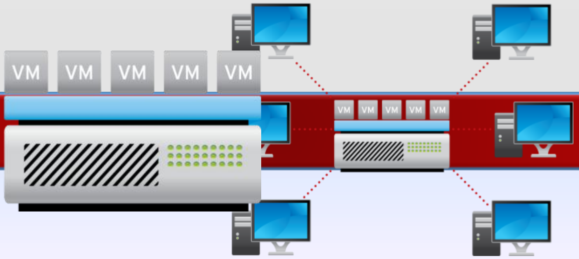


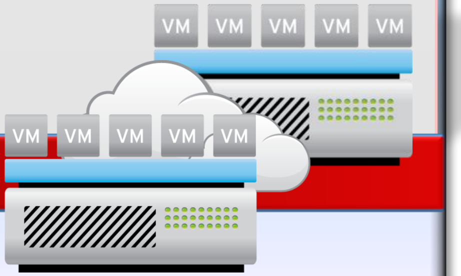
Private Cloud

Cross-platform Security

Physical | **Virtual** | **Cloud**

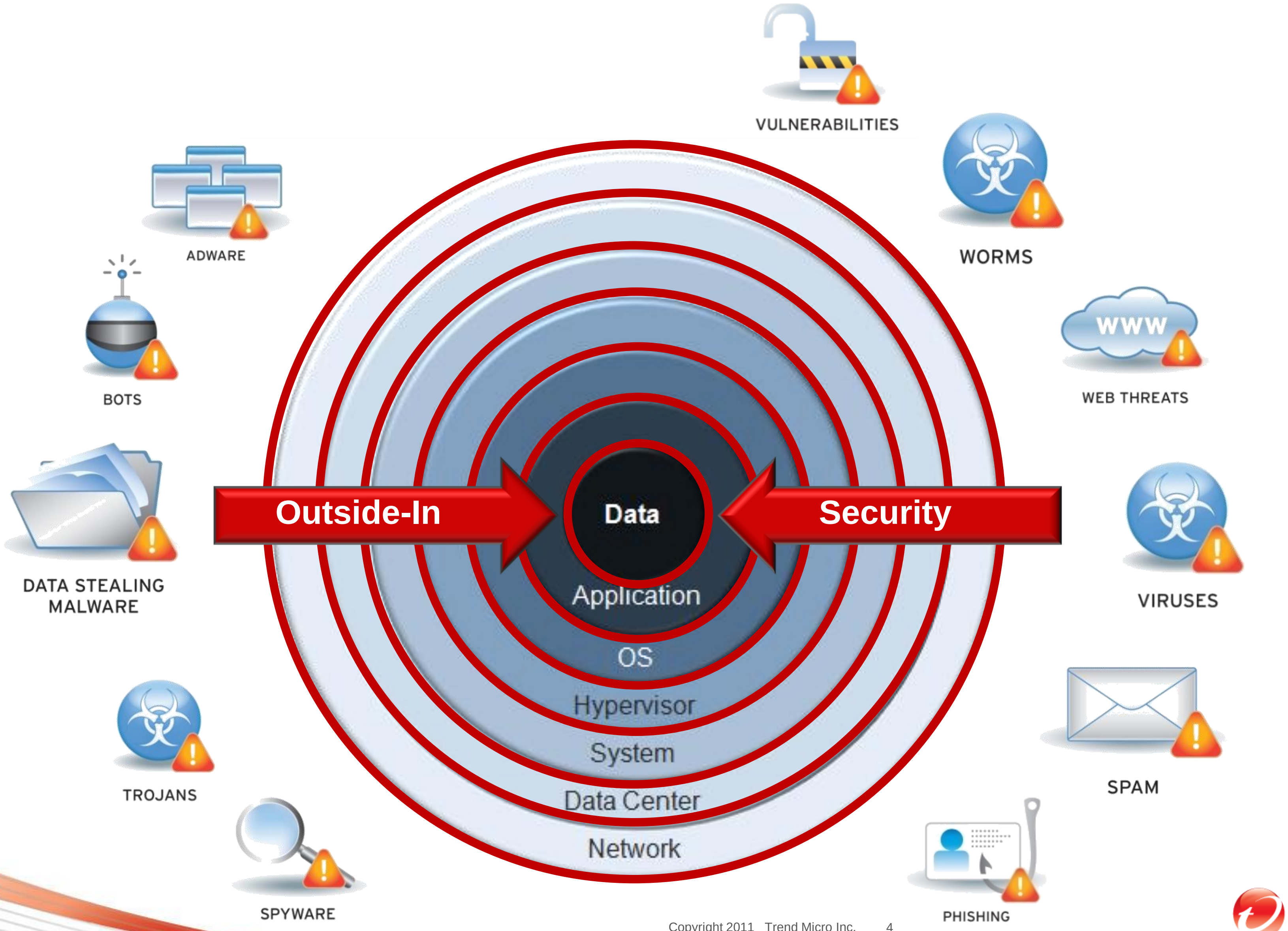
- New platforms don't change the threat landscape
- Integrated security is needed across all platforms
- Each platform has unique security risks





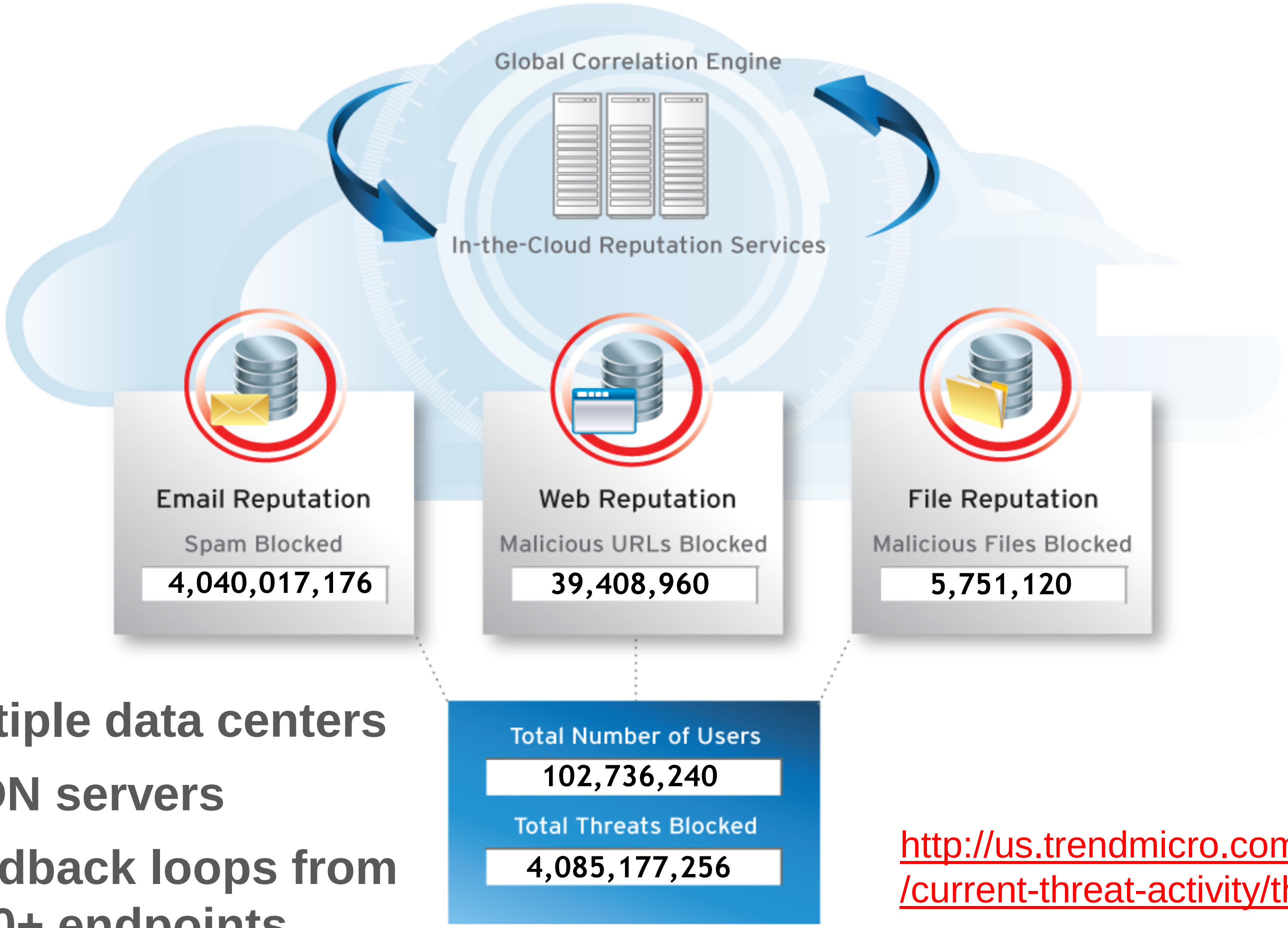
Single Management Console

Outside-in Model of Perimeter Defense



Outside-in Model of Perimeter Defense

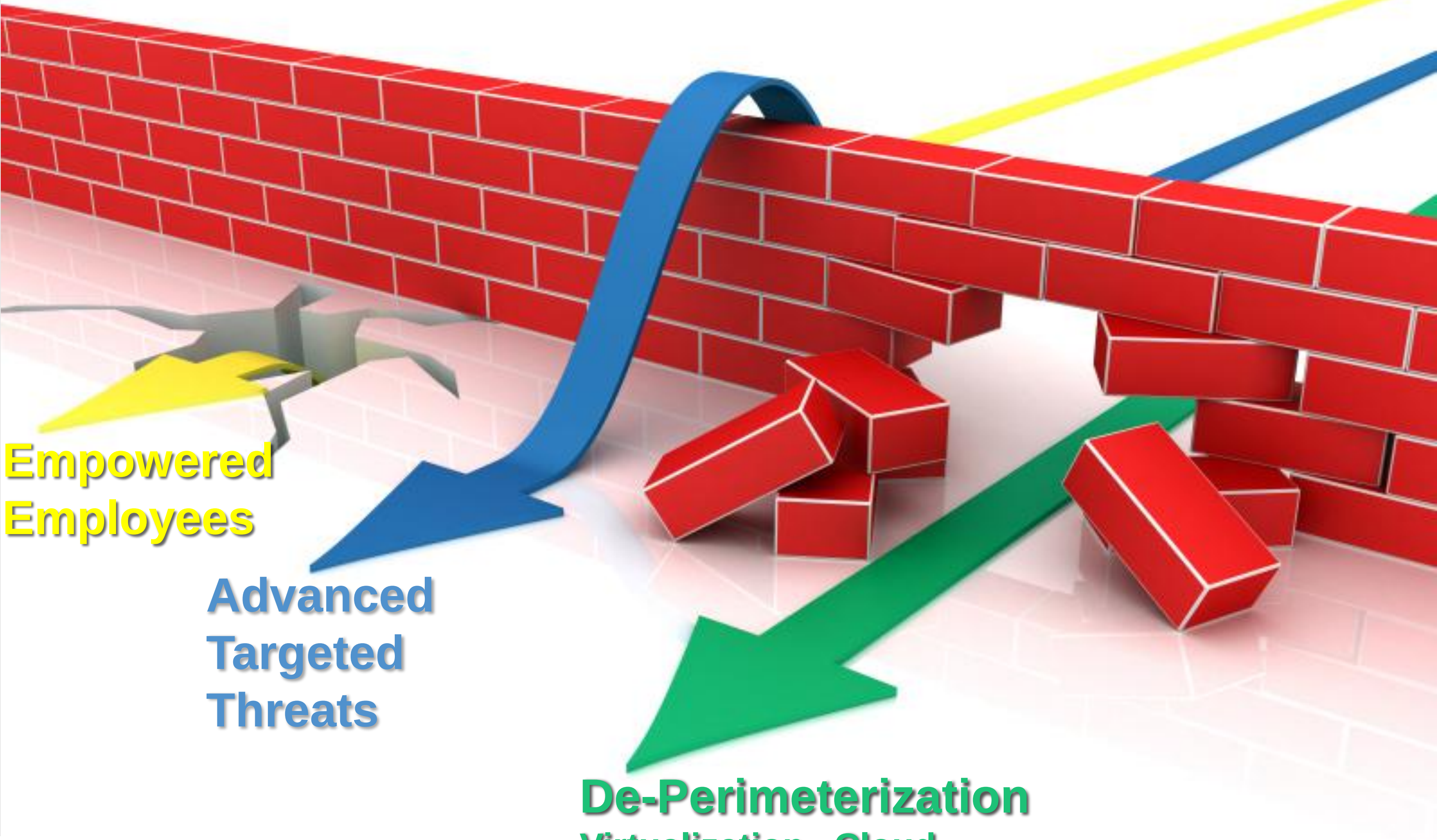
Correlated, reputation-based security
Stops threats before they enter your network



- Spans multiple data centers
- 50,000+ CDN servers
- Built-in feedback loops from 100,000,000+ endpoints

http://us.trendmicro.com/us/trendwatch/current-threat-activity/threat-tracker/

Outside-in Perimeter Defense Isn't Enough…



Empowered Employees

Advanced Targeted Threats

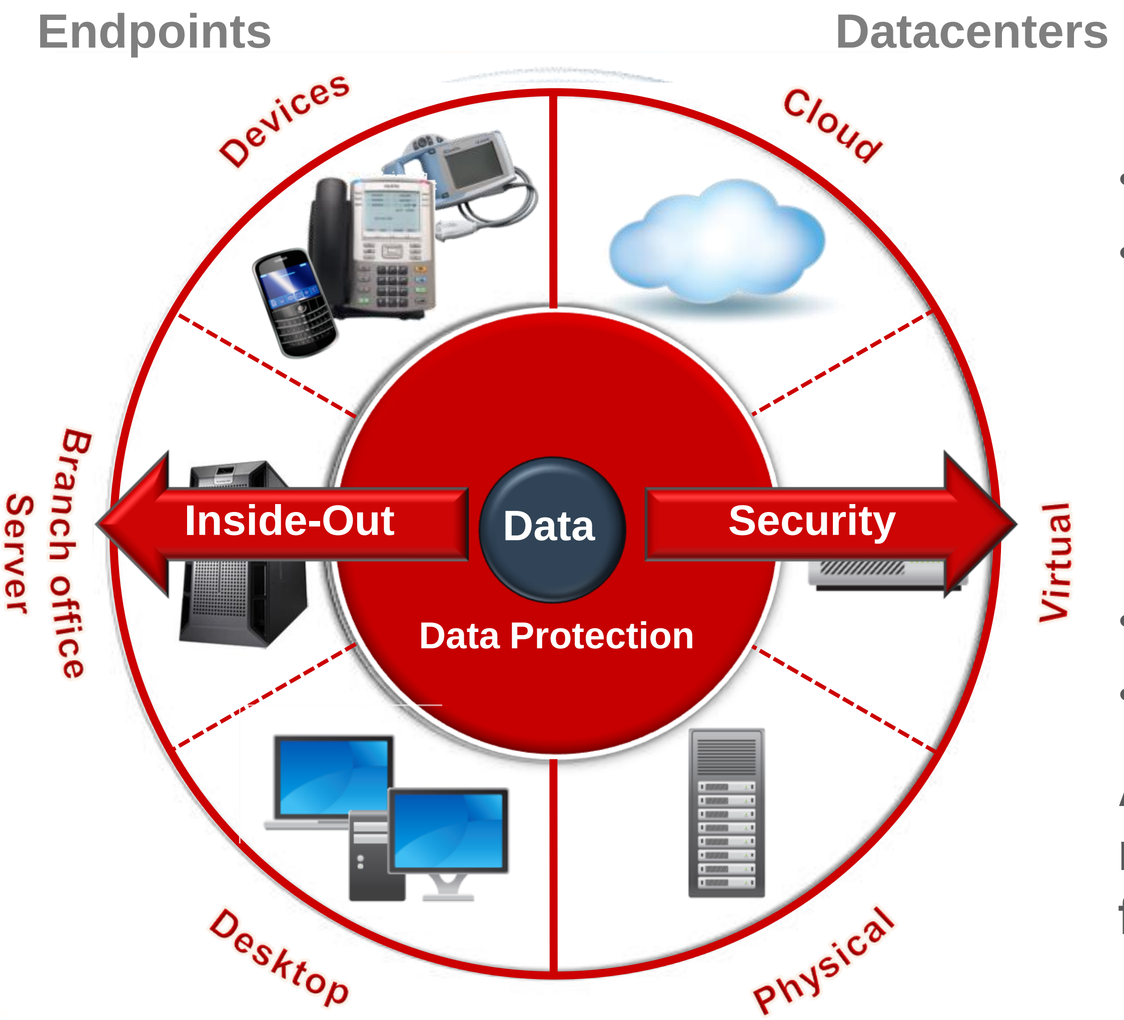
De-Perimeterization

Virtualization, Cloud Consumerization & Mobility

Source: Forrester

Integrated Security Across Platforms

Inside-out Security



- Self-Secured Workload
- Local Threat Intelligence
  - **When**-Timeline Aware
  - **Who**-Identity Aware
  - **Where**-Location Aware
  - **What**-Content Aware
- User-defined Access Policies
- Encryption

All **network-connected data** must be able to **defend** itself from attacks

Platform-specific Security Risks

Physical

Manageability

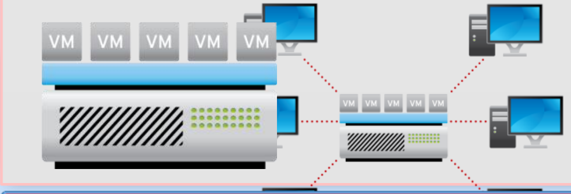
- Glut of security products
- Less security
- Higher TCO

Reduce Complexity

Virtual

Performance & Threats

- Security degrades performance
- New VM-based threats

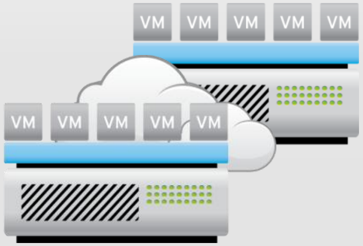


Increase Efficiency

Cloud

Visibility & Threats

- Less visibility
- More external risks



Deliver Agility

Integrated Security
Single Management Console

Reduce Complexity

Consolidate Security Vendors

Physical

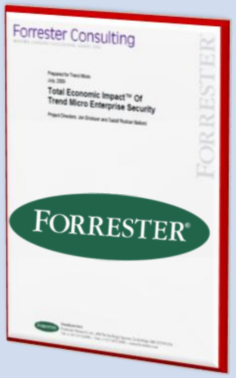
Windows, Linux, Solaris, etc

Vendor Management Savings:

30% Less Time

Improved Security and Availability:

73% Fewer Security Incidents



Forrester Consulting

Prepared for Trend Micro

[illegible]

Total Economic Impact™ Of Trend Micro Enterprise Security

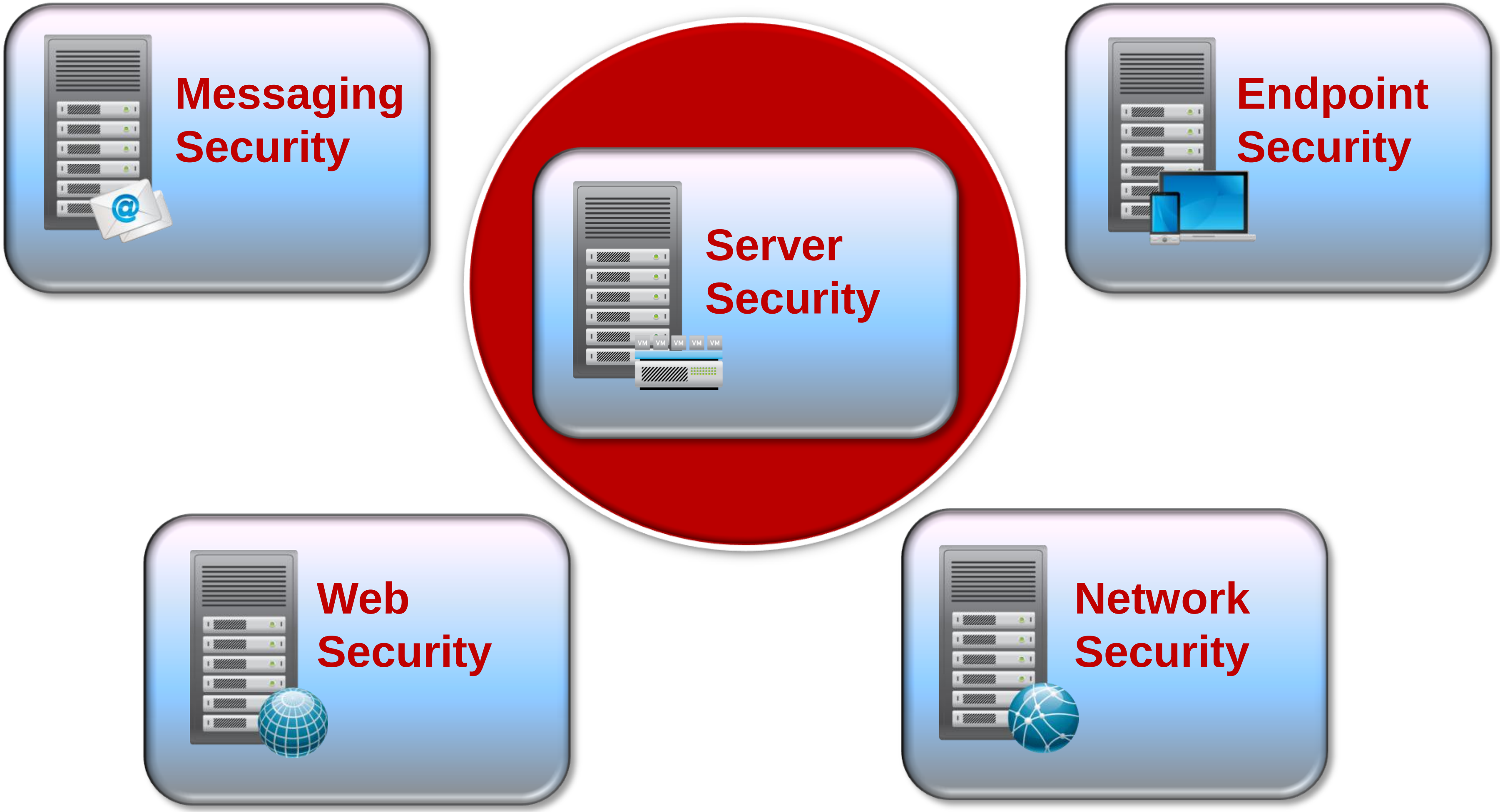
Project Directors: [illegible]

FORRESTER

FORRESTER®

Source: Forrester. The Total Economic Impact of Trend Micro Enterprise Security. 6/11.

Integrated Security Across Your Clouds



Messaging Security

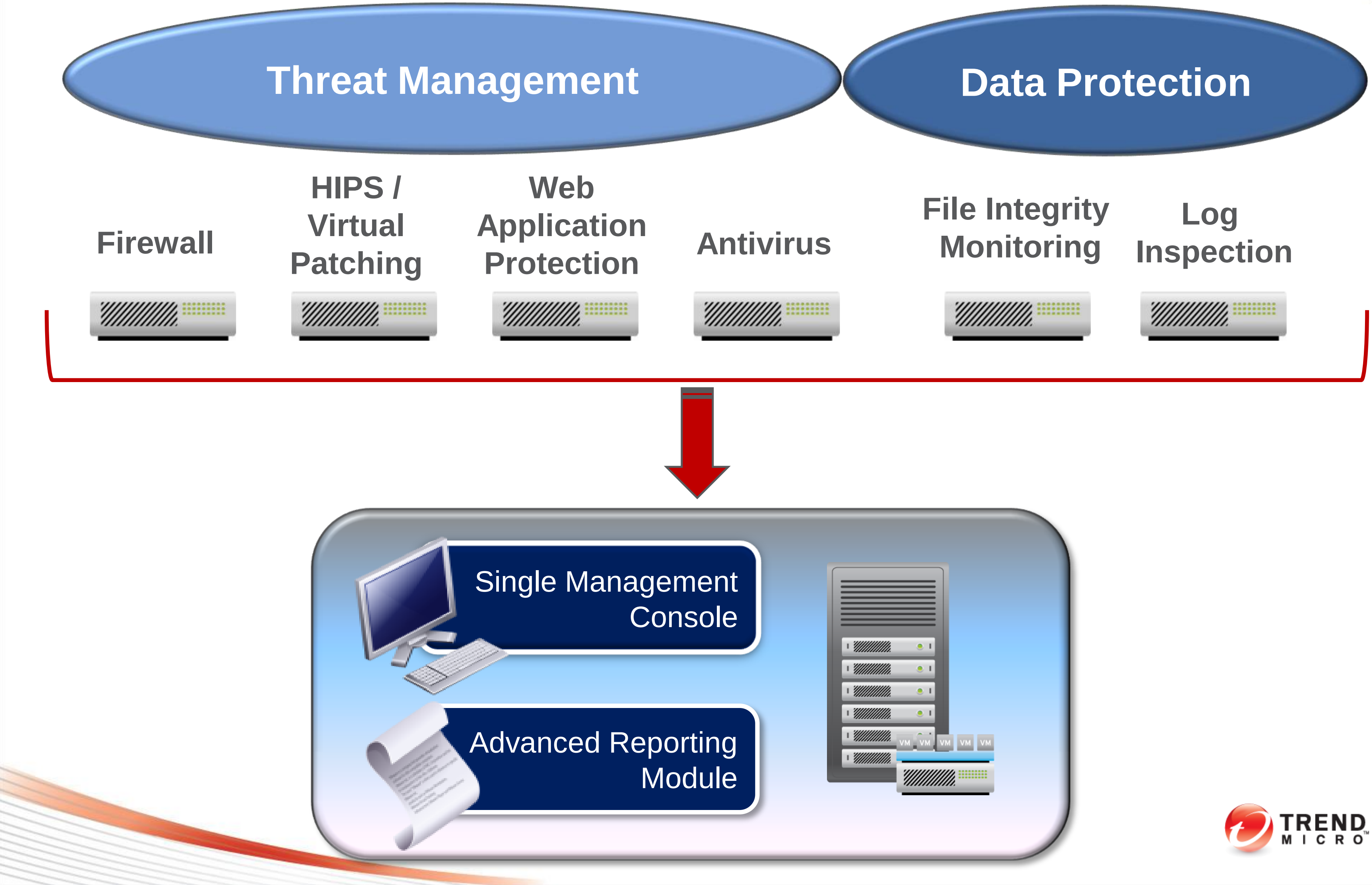
Server Security

Endpoint Security

Web Security

Network Security

Benefits of Integrated Server Security



Threat Management

Data Protection

Firewall

HIPS / Virtual Patching

Web Application Protection

Antivirus

File Integrity Monitoring

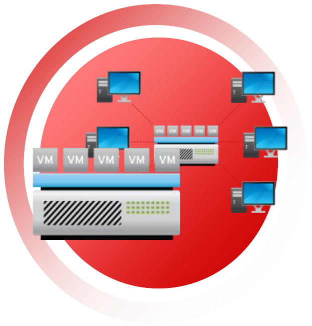
Log Inspection

Single Management Console

Advanced Reporting Module

Server and Desktop Virtualization Security

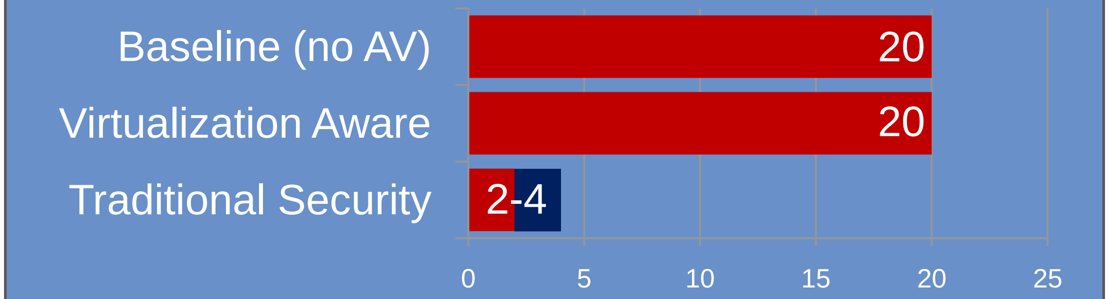
Virtualization



Deployment

- Server Virtualization in production / trial = 59%
- Desktop virtualization in production / trial = 52%

Consolidation Ratios



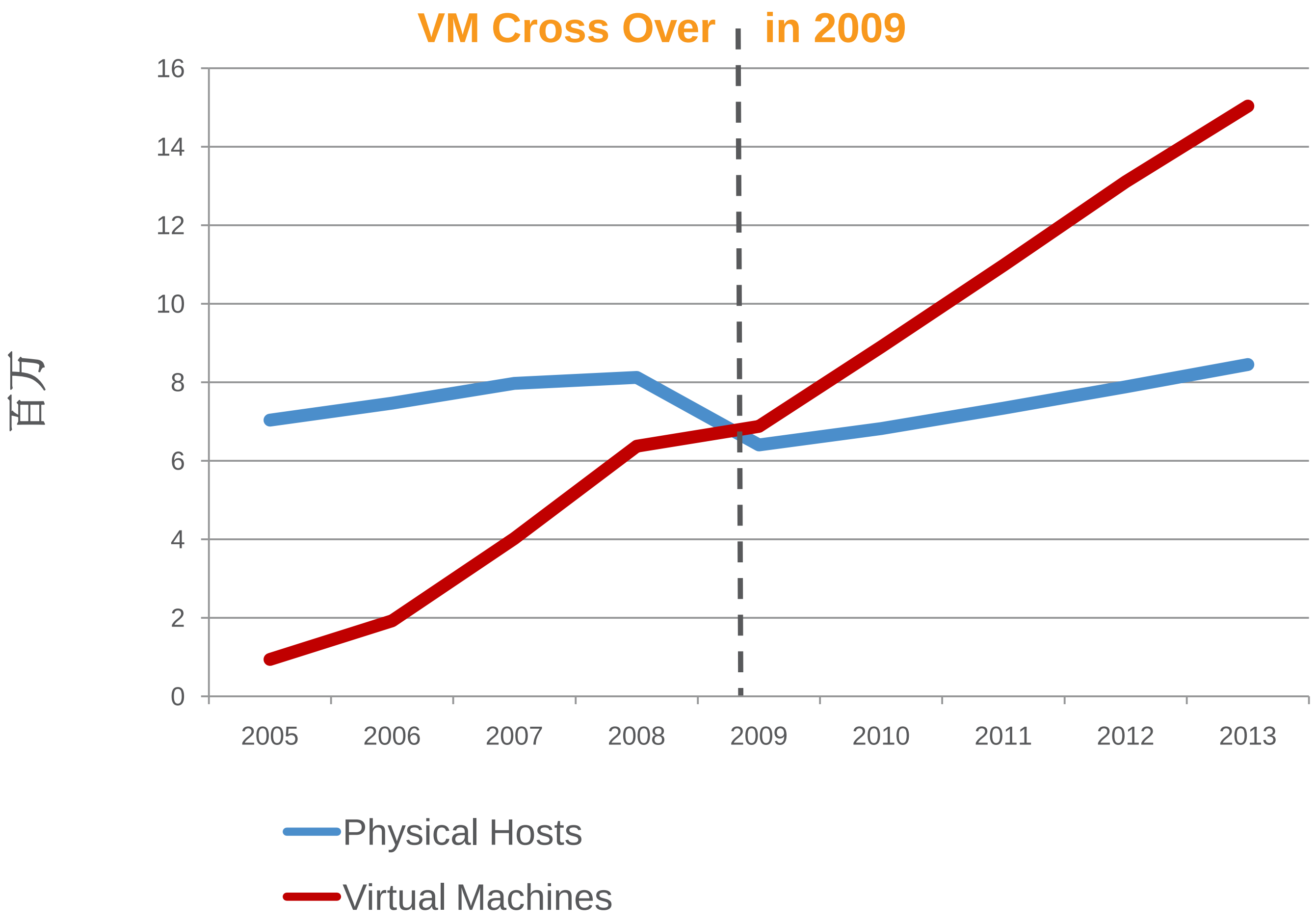
Source: Indusface June 2010

Cloud Foundation

If server virtualization is deployed then

- 62% have also deployed a private cloud
- 60% have also deployed a public cloud

More Virtual Machines than Physical Hosts

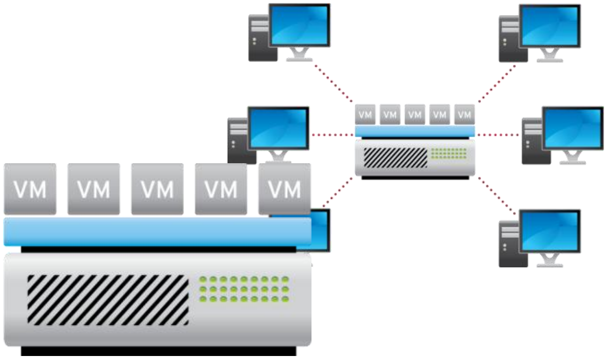


Server and Desktop Virtualization Security

Security for Virtualization

Virtualization-aware security

- For virtual servers
- For virtual desktops



Security Using Virtualization

Security virtual appliances and hybrids

- Virtualize security in the DMZ
- Pair virtual appliance & SaaS

Hardware vs Virtual Appliance

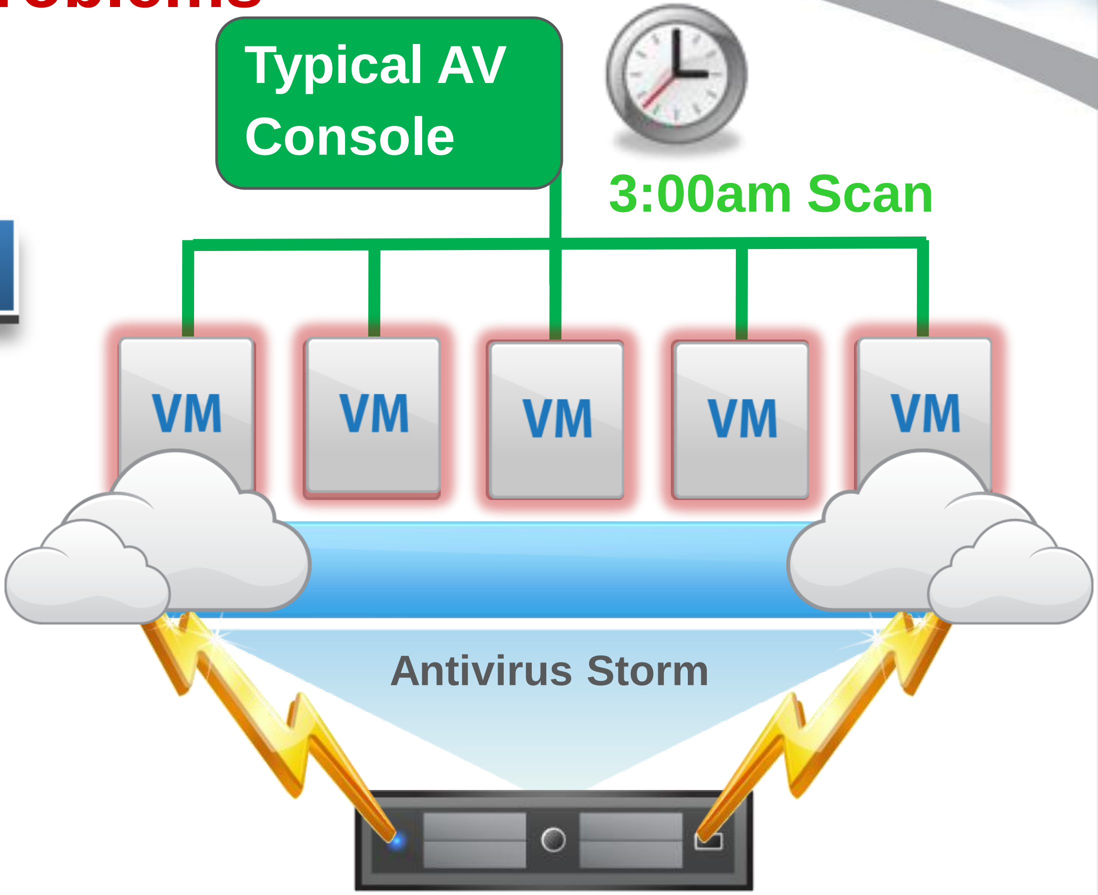
(3000 users, 3 years)	Hardware	Software	Cost/ user
Security Appliance	$25,879	$142,992	**$47.67**
Virtual Appliance	$2,700	$69,024	**$23.91**

47% Savings

Source: Osterman Research

Virtualization Security Problems

1 Resource Contention

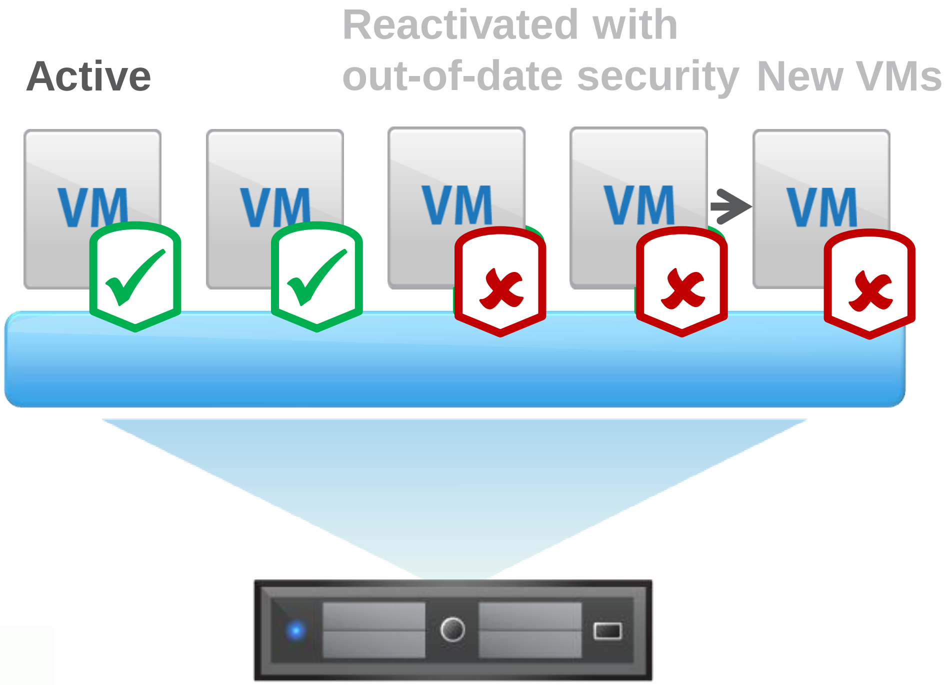


Automatic antivirus scans overburden the system

Virtualization Security Problems

1 Resource Contention

2 Instant-on Gaps



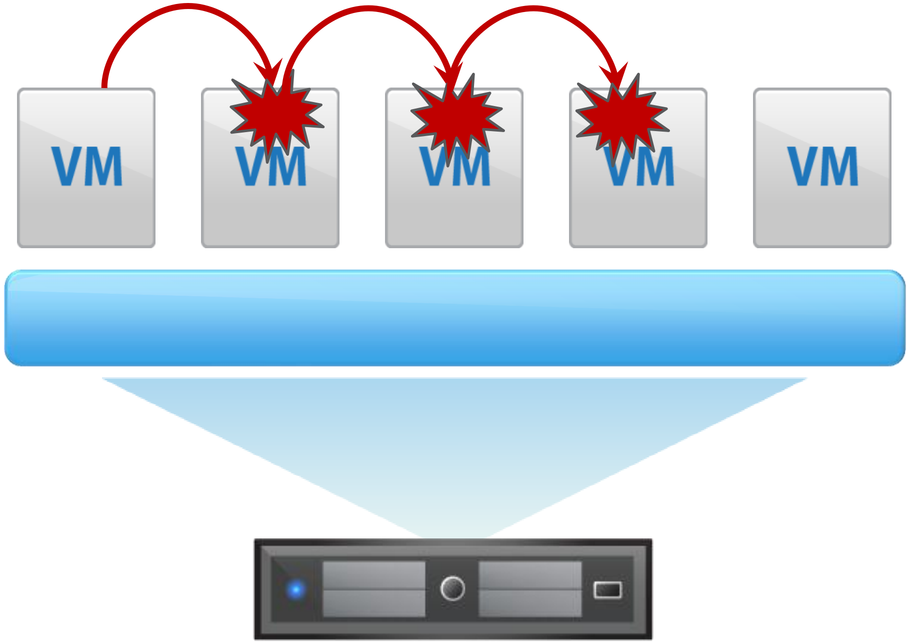
Cloned VMs must have a configured agent and updated pattern files

Virtualization Security Problems

1 Resource Contention

2 Instant-on Gaps

3 Inter-VM Attacks / Blind Spots



Attacks can spread across VMs

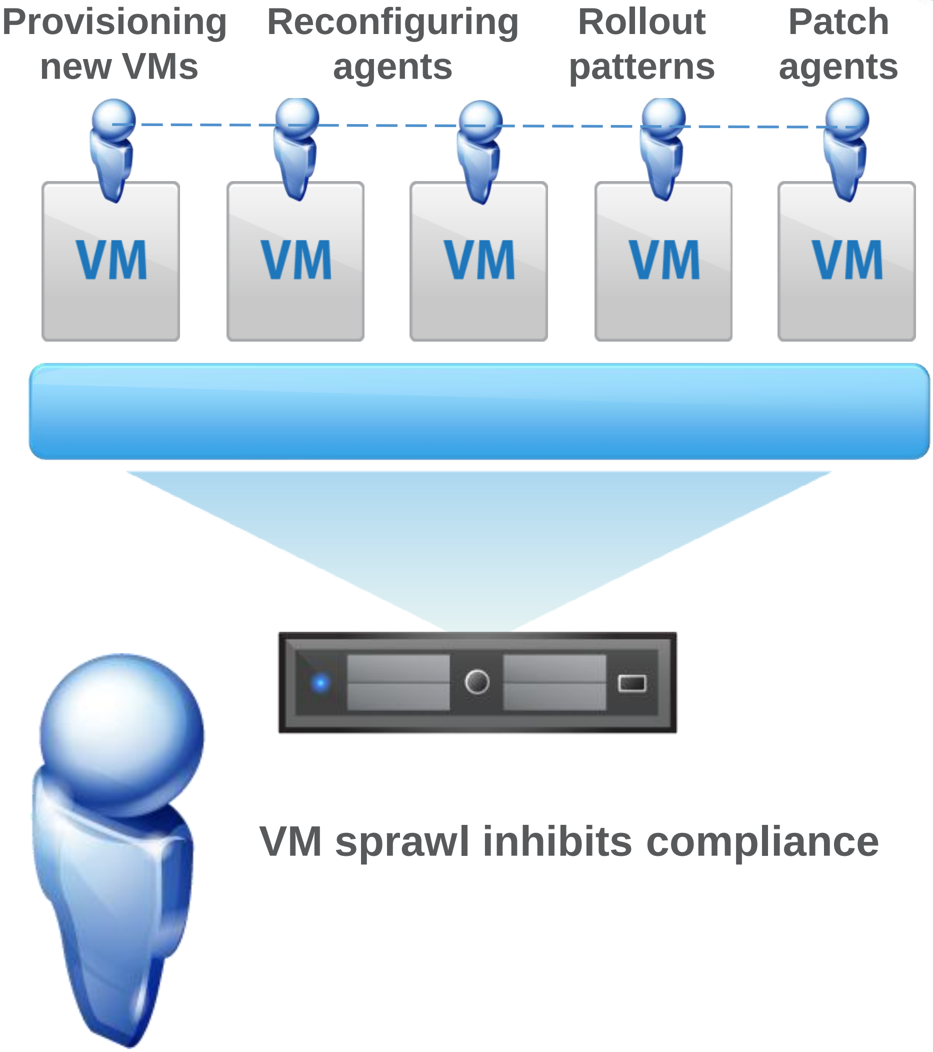
Virtualization Security Problems

1 Resource Contention

2 Instant-on Gaps

3 Inter-VM Attacks / Blind Spots

4 Complexity of Management



VM sprawl inhibits compliance

Addressing Security Problems

1 Resource Contention

Solution: Agentless AV with staggered scans from a separate scanning VM

2 Instant-on Gaps

Solution: Dedicated scanning VMs with layered protection

3 Inter-VM Attacks / Blind Spots

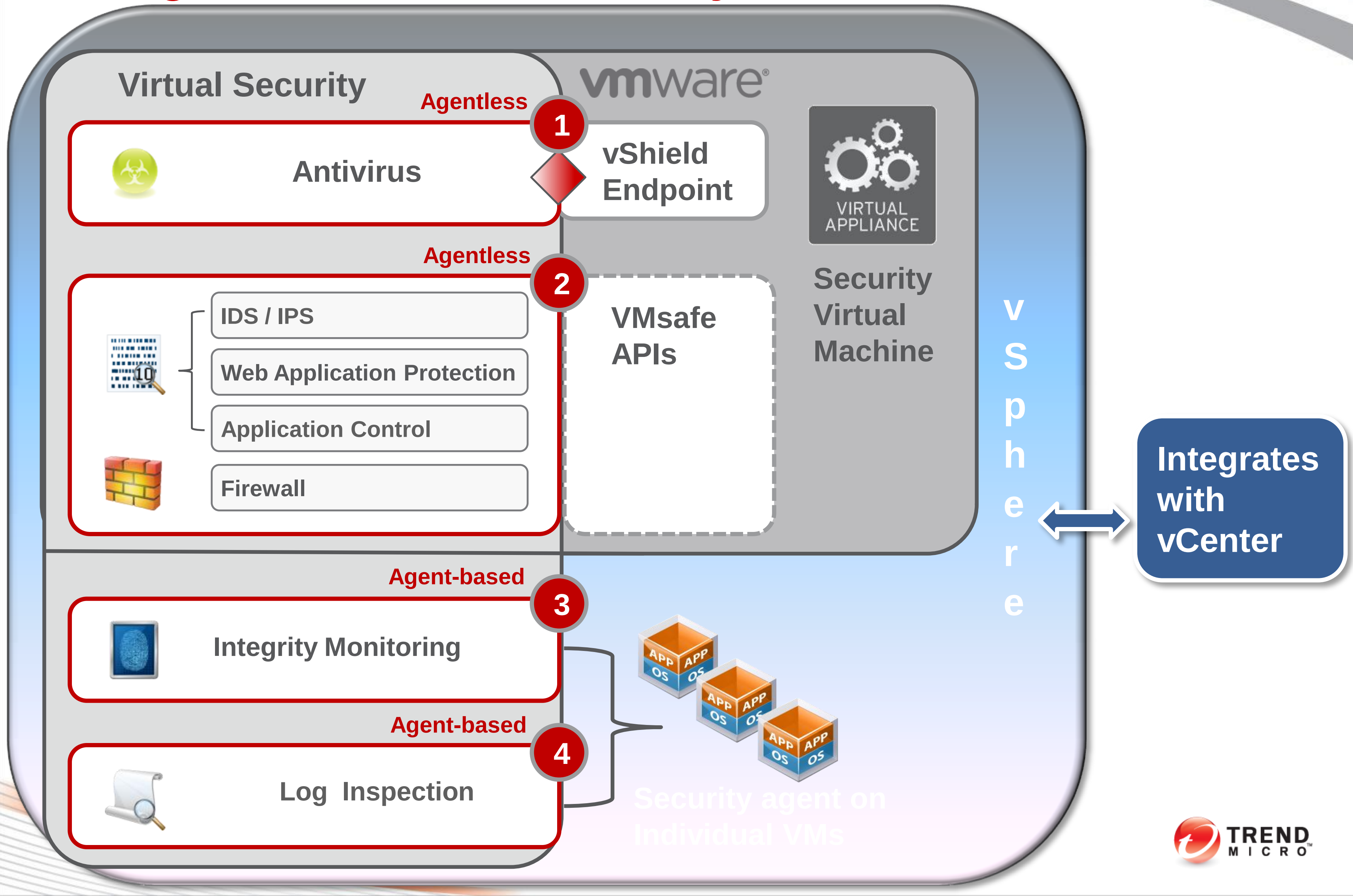
Solution: VM-aware security with virtualization platform integration

4 Complexity of Management

Solution: Integration with virtualization management consoles such as VMware vCenter

Virtualization

Fitting into the VMware Ecosystem



Virtual Security

Agentless

1

Antivirus

vShield Endpoint

Agentless

2

IDS / IPS

Web Application Protection

Application Control

Firewall

VMsafe APIs

Security Virtual Machine

Agent-based

3

Integrity Monitoring

Agent-based

4

Log Inspection

Security agent on Individual VMs

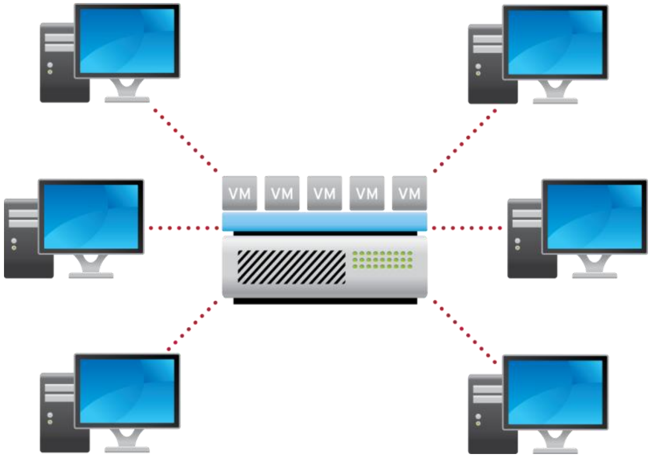
vSphere

Integrates with vCenter

TREND MICRO

Virtualization
Virtual Desktop Security

- **Integrates tightly with leading VDI vendors**
  - VMware vCenter
  - VMware View
  - Citrix XenServer
  - Citrix XenDesktop
- **Uses hypervisor API integration**
  - Optimizes scanning operations
  - Enables intelligent per-host scheduling to prevent resource contention
  - Provides agentless AV option
- **Offers off-network protection with agent-based security**



Deliver Agility

Cloud Deployments and Security

Cloud Computing

Cloud Deployment:

• Private:	pre-production = 43%;	production = 13%
• Public:	pre-production = 43%;	production = 13%
• Hybrid:	pre-production = 45%;	production = 10%

Public Cloud Security:

43% experienced a security issue in the last 12 months

Encryption is Key to Cloud Security:

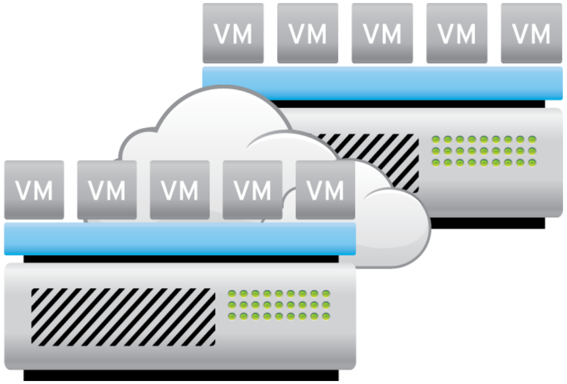
- 85% encrypt data in the public cloud
- 85% keep a 1:1 copy of data in the public cloud

Deliver Agility

Cloud Deployments and Security

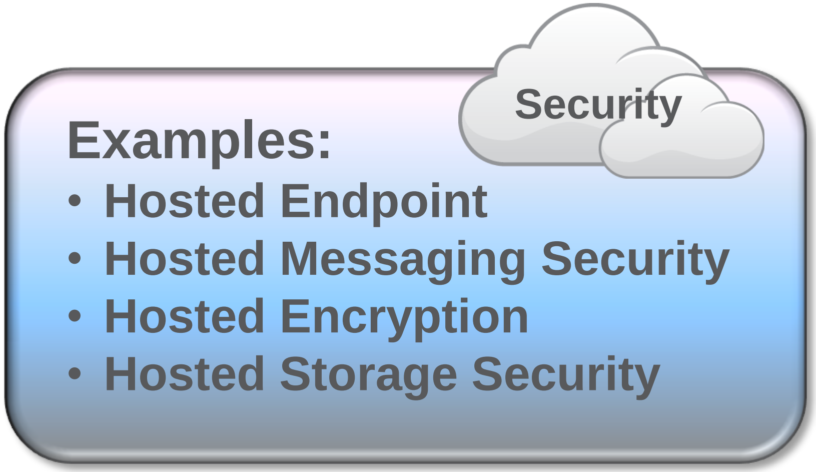
Security for the Cloud

- For private clouds
- For public cloud
- For hybrid clouds



Security from the Cloud

- Hosted security
- Hybrid SaaS
- Reputation services
- Security updates



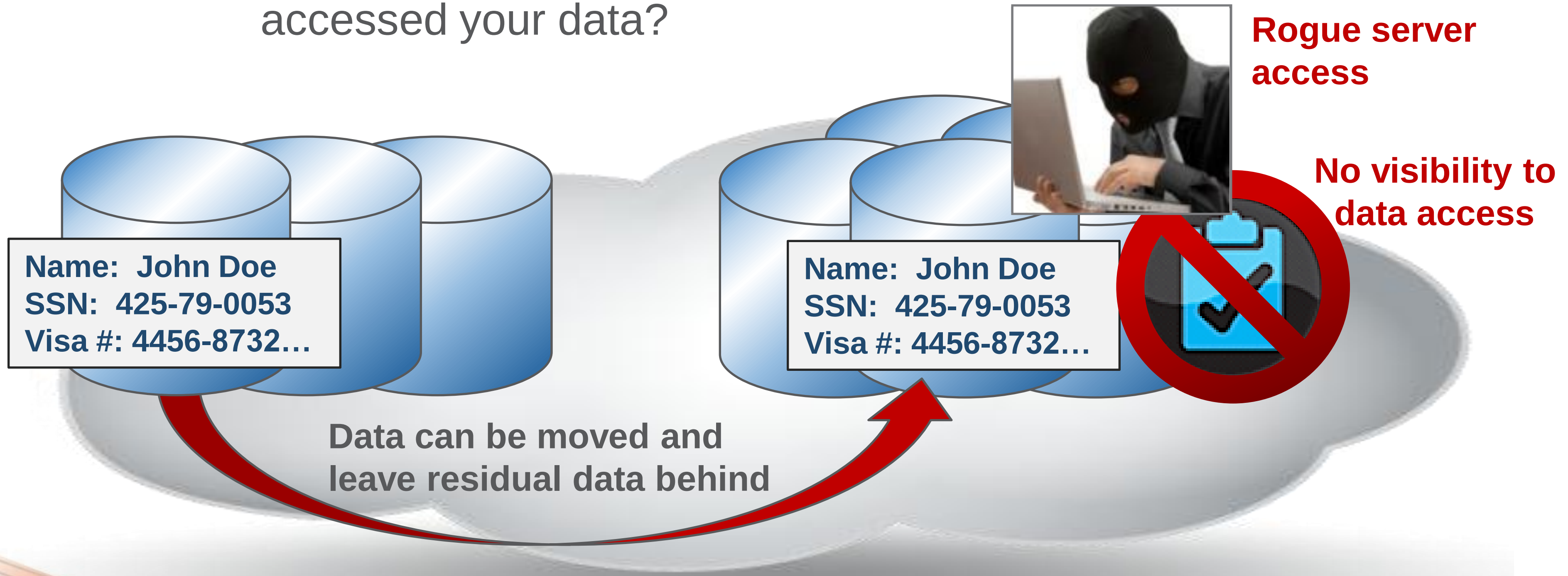
Examples:

- **Hosted Endpoint**
- **Hosted Messaging Security**
- **Hosted Encryption**
- **Hosted Storage Security**

Public IaaS Clouds

Security and Privacy are #1 Concerns

- Your data is mobile — has it moved?
- Who can see your information?
- Who is attaching to your volumes?
- Do you have visibility into who has accessed your data?



Rogue server access

No visibility to data access

Name: John Doe
SSN: 425-79-0053
Visa #: 4456-8732…

Name: John Doe
SSN: 425-79-0053
Visa #: 4456-8732…

Data can be moved and leave residual data behind

What is the Solution?

Data Protection in the Cloud

Encryption with Policy-based Key Management

AES Encryption 128, 192, & 256 bits

- Unreadable to outsiders
- Obscured data on recycled devices

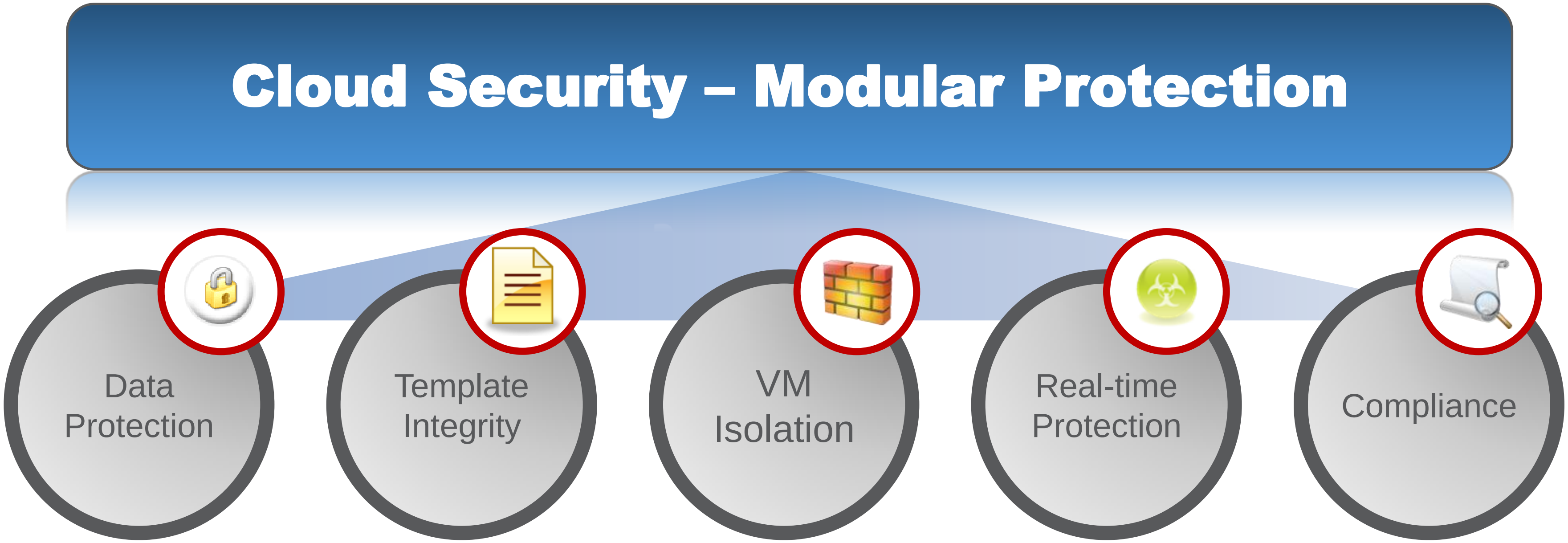
Policy-based Key Management

- Trusted server access
- Control for when and where data is accessed

Auditing, Reporting, & Mobility

- Compliance support
- Custody of keys—SaaS or virtual appliance
- No vendor lock-in

Security that Travels with the VM



Self-Defending VM Security in the Cloud

- Agent on VM allows travel between cloud solutions
- One management portal for all modules
- SaaS security deployment option

amazon web services™ vmware®

Securing the Cloud is about Protection…

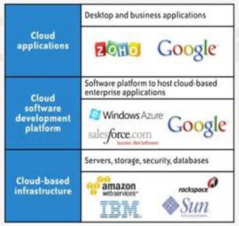
Virtualization & Network

Mobile & Endpoint

Hybrid Cloud Management

- Physical
- Virtual
- Cloud

Mobile Data, Cloud Storage

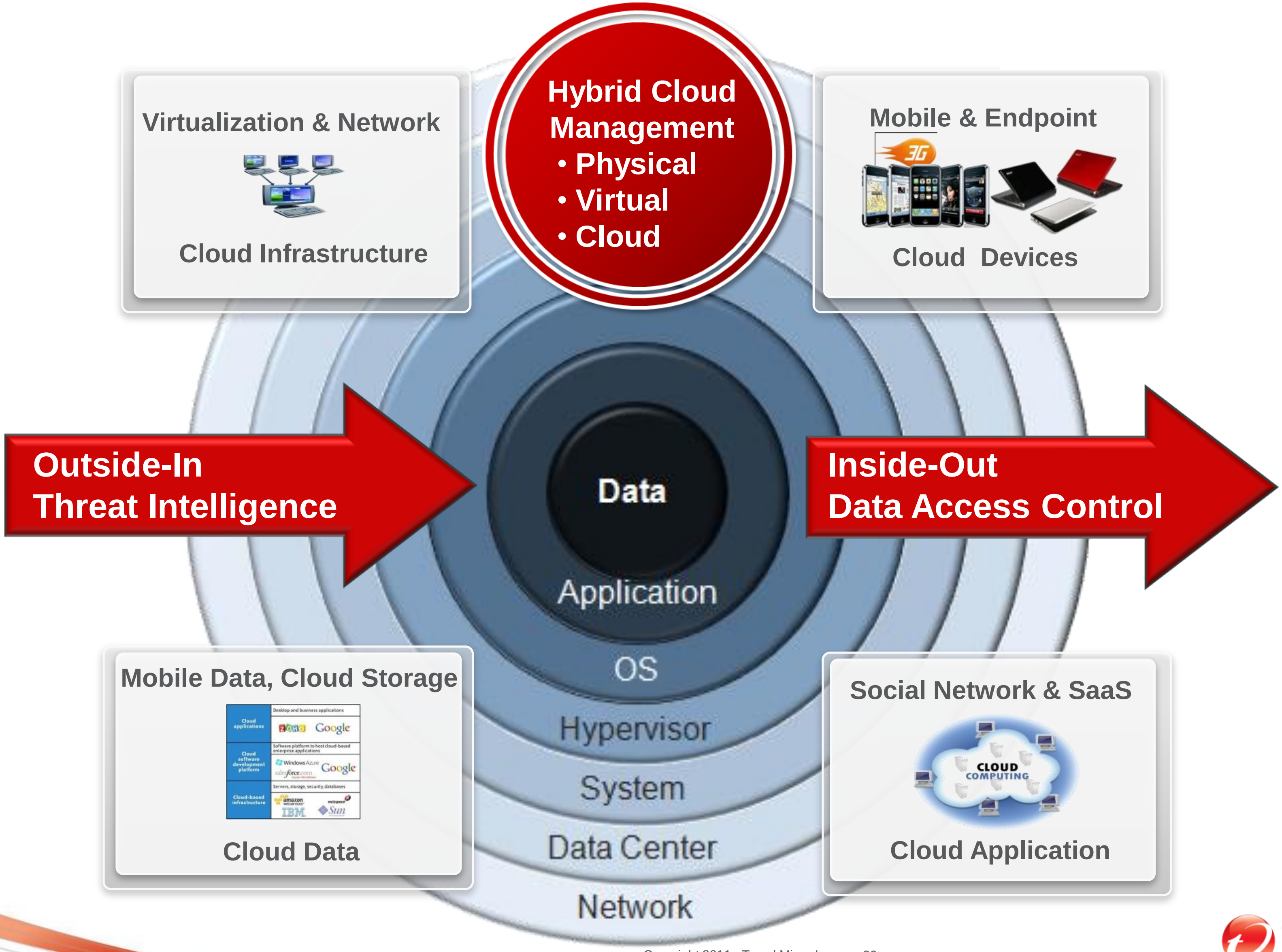


Cloud applications	Desktop and business applications
	zoho Google
Cloud software development platform	Software platform to host cloud-based enterprise applications
	Windows Azure salesforce.com Google
Cloud-based infrastructure	Servers, storage, security, databases
	amazon webservices rackspace IBM Sun

Social Network & SaaS

What is the Solution?

Securing Your Journey to the Cloud



Hybrid Cloud Management
- Physical
- Virtual
- Cloud

Virtualization & Network

Cloud Infrastructure

Mobile & Endpoint

Cloud Devices

Outside-In
Threat Intelligence

Inside-Out
Data Access Control

Data

Application

OS

Hypervisor

System

Data Center

Network

Mobile Data, Cloud Storage

Cloud Data

Social Network & SaaS

Cloud Application

3G
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
CLOUD COMPUTING

Securing Your Journey to the Cloud

Software

Reduce Complexity

- Integrate security—server, web, email, endpoint, network
- Improve security and availability

Virtual

Increase Efficiency

- Apply VM-aware security
- Ensure higher VM densities
- Get better performance *and* better protection

Cloud

Deliver Agility

- Encrypt with policy-based key management
- Deploy self-defending VMs in the cloud
- Use security that travels with your data