TREND MICRO™

Securing Your Journey to the Cloud

Deep Security

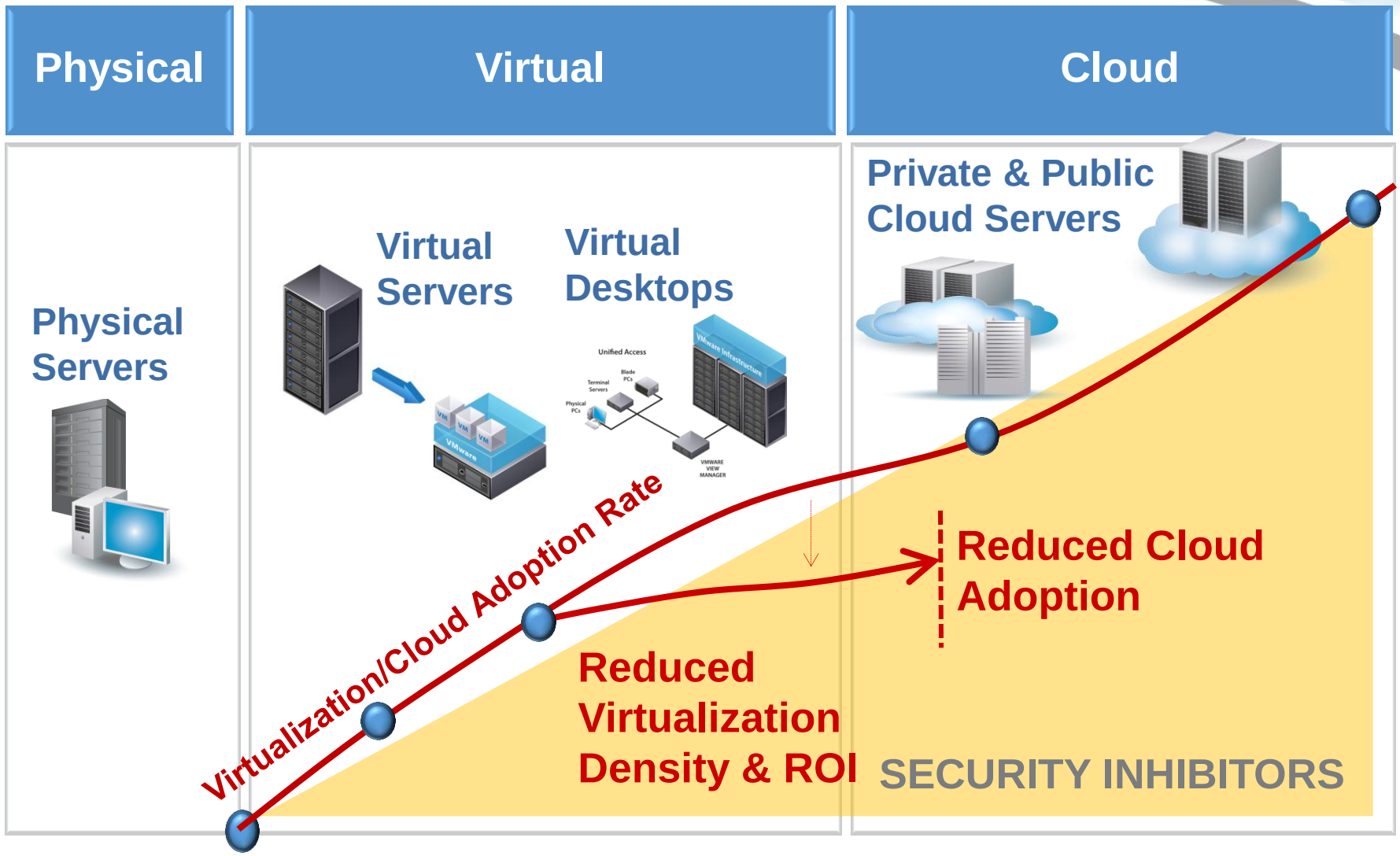
Προστατεύοντας Server Farm

Σωτήρης Δ. Σαράντος

Σύμβουλος Δικτυακών Λύσεων

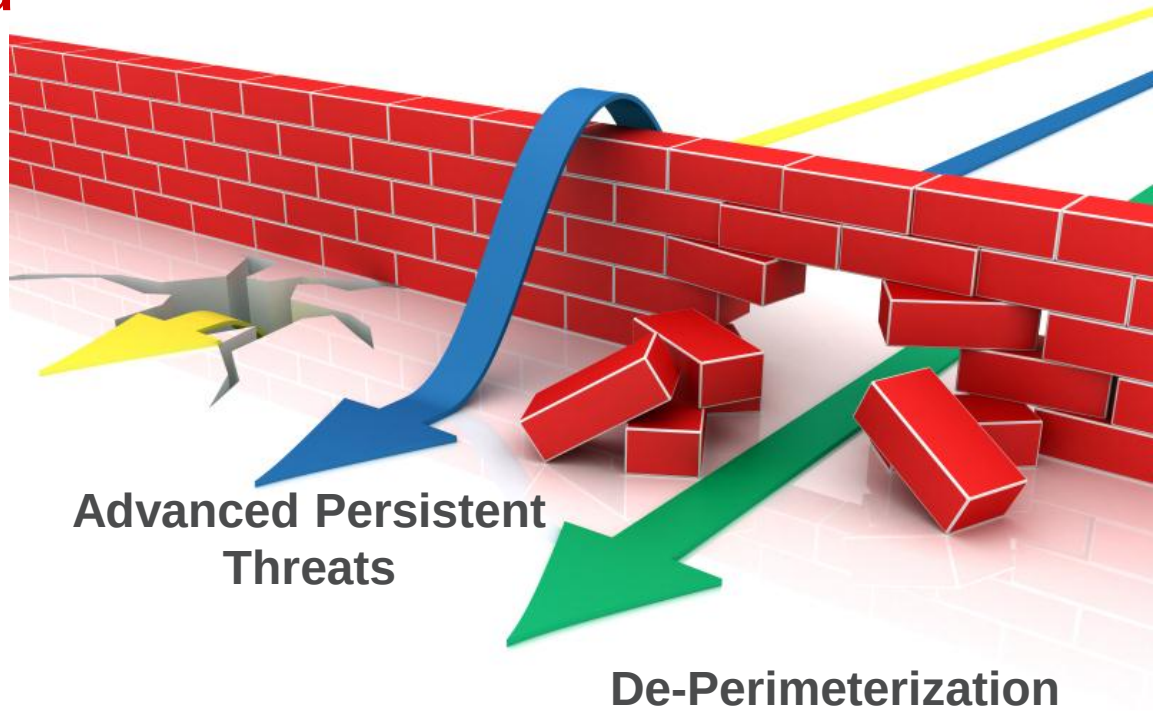
DIGITAL SIMA

Legacy Security Hinders Datacenter Consolidation



Advanced threats are breaching existing defenses

- More Sophisticated
- More Targeted
- More Frequent
- More Profitable



Basic perimeter and host defenses not adequate anymore

Organizations Struggle With Keeping Servers Patched

National Vulnerability Database
nvd.nist.gov

2095 Critical "Software Flaw" Vulnerabilities in 2010

- Common Vulnerabilities & Exposures ("CVE"): Score 7-10

2095 per year =

8 critical alerts everyday!

NVD Statistical Data

Year	# Vulns	% Total
1997	145	57.54
1998	134	54.47
1999	424	47.43
2000	452	44.31
2001	773	46.09
2002	1,004	46.57
2003	678	44.40
2004	969	39.53
2005	2,038	41.32
2006	2,760	41.77
2007	3,159	48.50
2008	2,841	50.44
2009	2,722	47.48
2010	2,095	45.16
2011*	1,658	43.87

Compliance Mandates Driving Costs Up

Solutions Need to Achieve Broader Coverage with Lower TCO

More standards:

- PCI, SAS70, HIPAA, ISO 27001, FISMA / NIST 800-53, MITS…

More specific security requirements

- Virtualization, Web applications, EHR, PII…

More penalties & fines

- HITECH, Breach notifications, civil litigation

> "DMZ consolidation using virtualization will be a "hot spot" for auditors, given the greater risk of mis-configuration and lower visibility of DMZ policy violation. Through year-end 2011, auditors will challenge virtualized deployments in the DMZ more than non-virtualized DMZ solutions."
>
> *-- Neil MacDonald, Gartner*

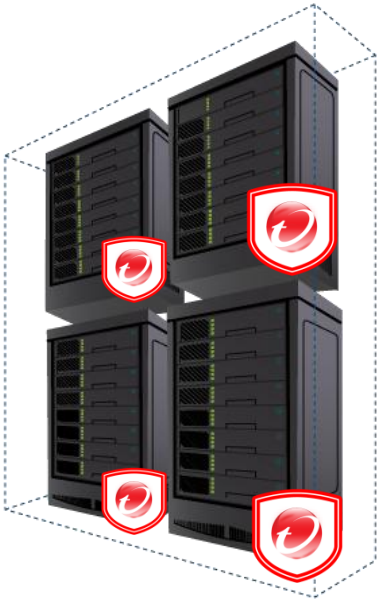
Trend Micro Deep Security

A server security platform for:

Microsoft
solaris
Linux
vmware
AIX
hp HP-ux
CITRIX

PHYSICAL

VIRTUAL



CLOUD

- Intrusion Prevention
- Firewall
- Anti – Malware
- Web Reputation
- Integrity Monitoring
- Log Inspection

VMware vShield enabled Agent-less

TREND MICRO

DIGITAL SIMA

Deep Security Agent/Virtual Appliance

System, application and data security for servers

6 protection modules

Reduces attack surface. Prevents DoS & detects reconnaissance scans

Firewall

Intrusion Prevention

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

Tracks credibility of websites and safeguards users from malicious urls

Web Reputation

Anti-Virus

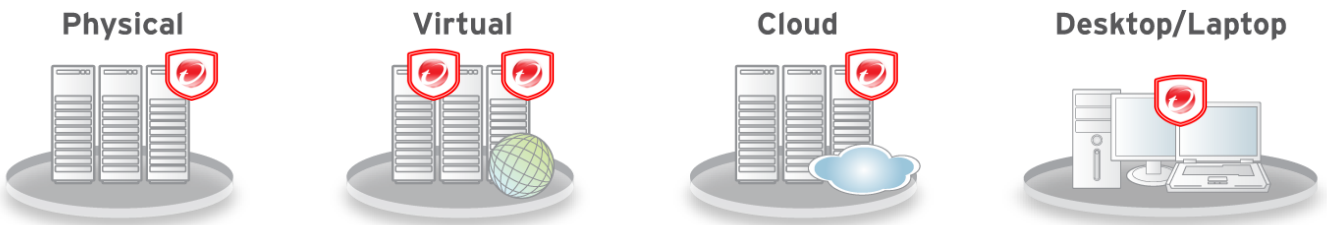
Detects and blocks malware (web threats, viruses & worms, Trojans)

Optimizes the identification of important security events buried in log entries

Log Inspection

Integrity Monitoring

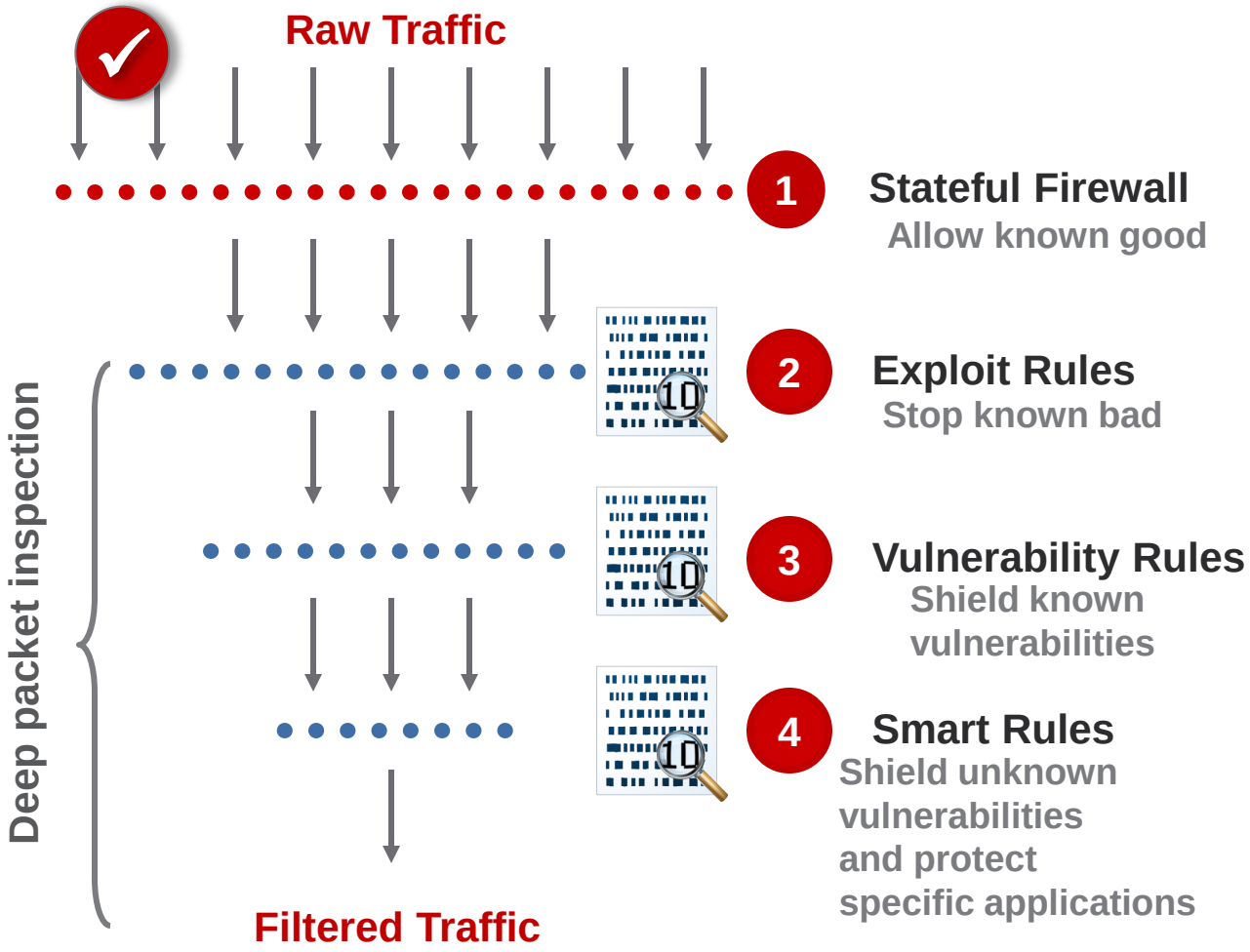
Detects malicious and unauthorized changes to directories, files, registry keys…



Protection is delivered via Agent and/or Virtual Appliance

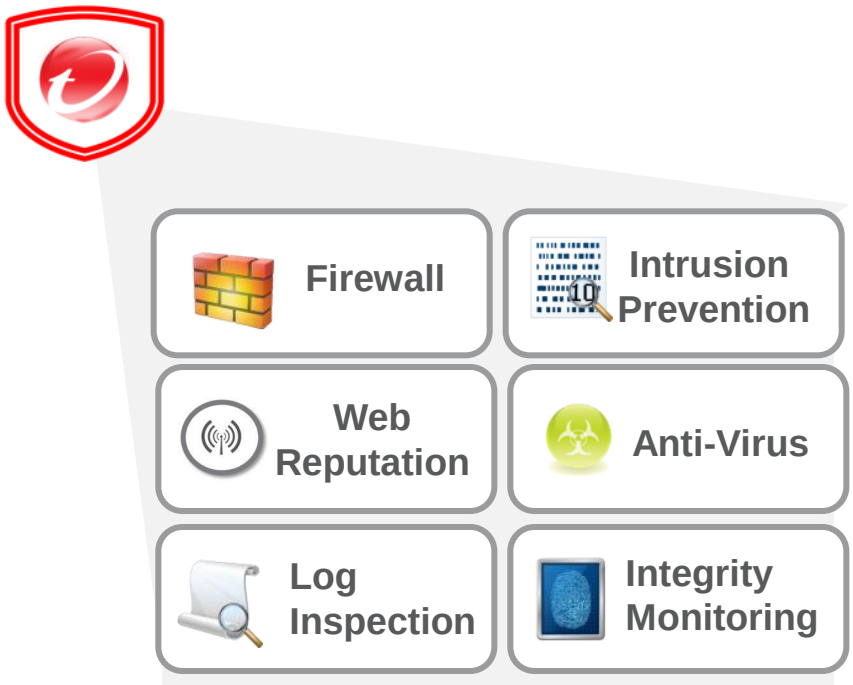
*** Log Inspection is only available in agent form today**

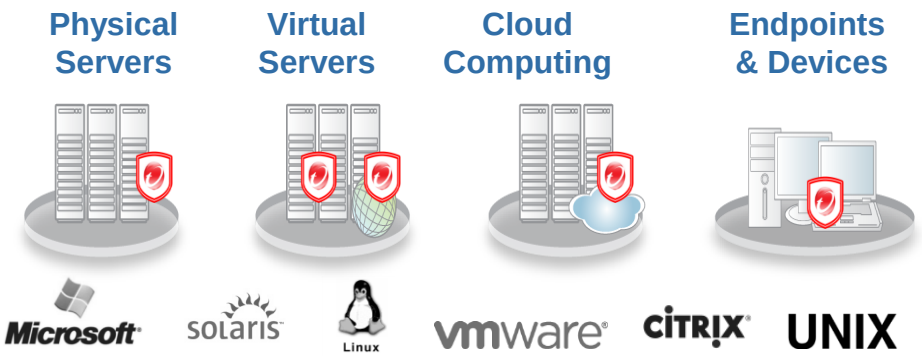
Virtual Patching with Deep Security



Over 100 applications shielded including:
Operating Systems
Database servers
Web app servers
Mail servers
FTP servers
Backup servers
Storage mgt servers
DHCP servers
Desktop applications
Mail clients
Web browsers
Anti-virus
Other applications

Deep Security for Defense-in-Depth & Compliance



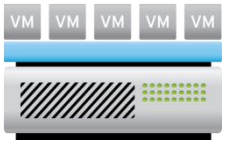


Addressing 7 PCI Regulations and 20+ Sub-Controls Including:	
☑(1.)	Network Segmentation
☑(1.x)	Firewall
☑(5.x)	Anti-virus
☑(6.1)	Virtual Patching*
☑(6.6)	Web App. Protection
☑(10.6)	Daily Log Review
☑(11.4)	IDS / IPS
☑(11.5)	File Integrity Monitoring

*** Compensating Control**

Virtualization Security with Deep Security

Agentless Security Platform for Virtual Environments



Deep Security Virtual Appliance

- Intrusion prevention
- Firewall
- Anti-malware
- Web reputation
- Integrity monitoring

The Old Way

With Deep Security

Higher Density

Fewer Resources

Easier Manageability

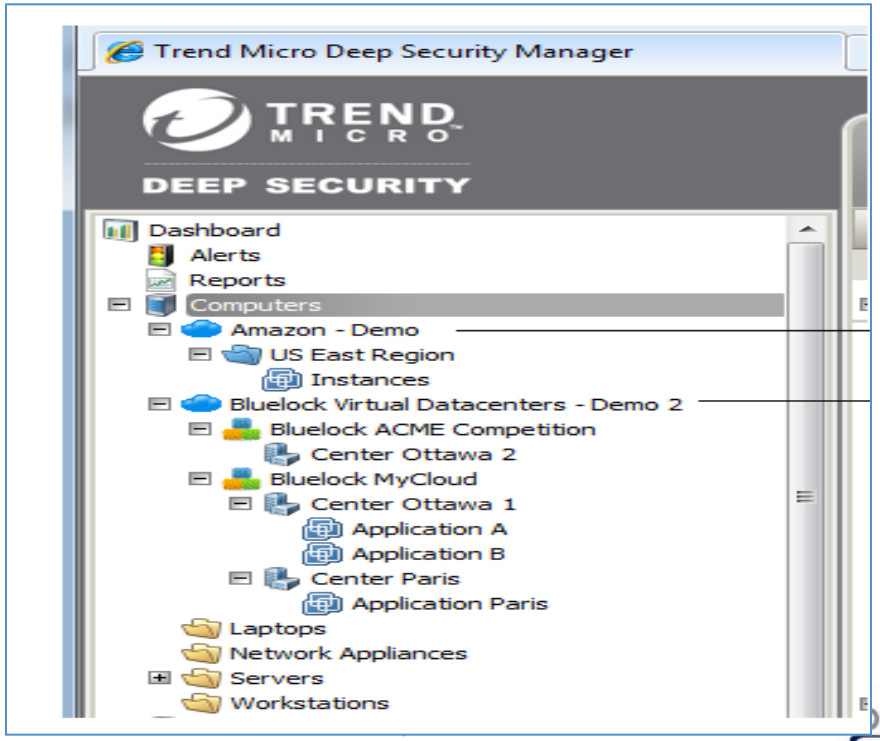
Stronger Security

TREND MICRO

DIGITAL SIMA

Extending Datacenter Security to Hybrid Cloud

- AWS and vCloud API integration
  - Single management pane-of-glass between VM's in internal VMware datacenters, VPC's, and public clouds
- Hierarchical policy management
  - Inheritance enables customized policies for different VM's or datacenters, while central IT can mandate compliant baseline settings



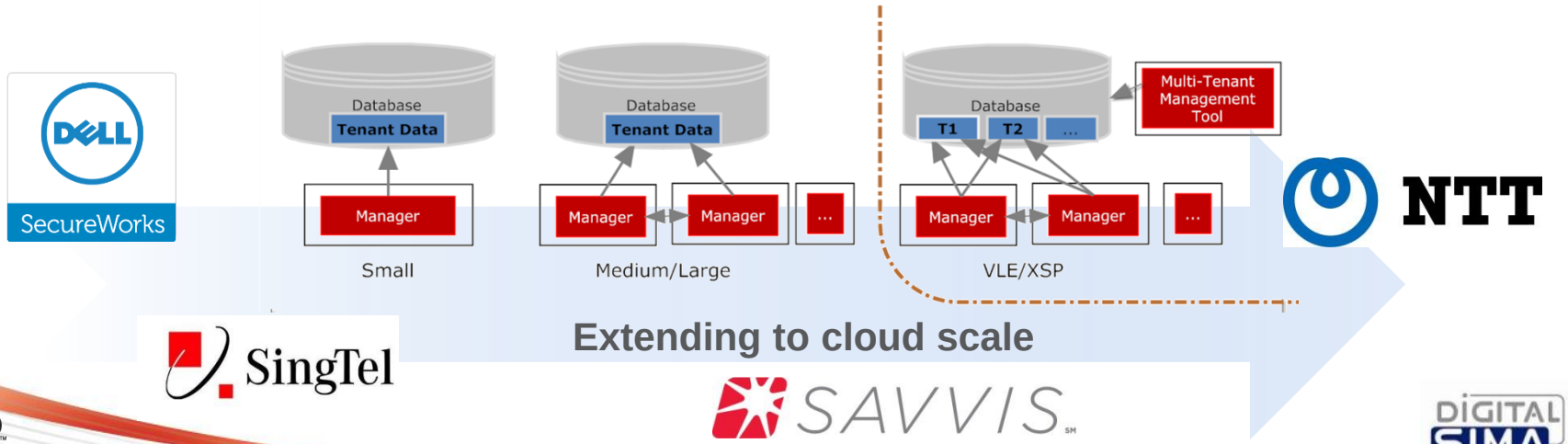
Agile Security Management for the Cloud

Multi-tenant Deep Security Manager architected for key attributes of cloud computing*:

- *Resource-pooling* – independent tenant policies/data for shared, multi-tenant clouds
- *Elasticity* - Automated deployment of components to cloud scale
- *Self-service* – Policies can be delegated by cloud admin to tenants through self-service GUI
- *Broad network access* – Web-based console built on RESTful APIs for extensibility and integration with broader cloud management frameworks

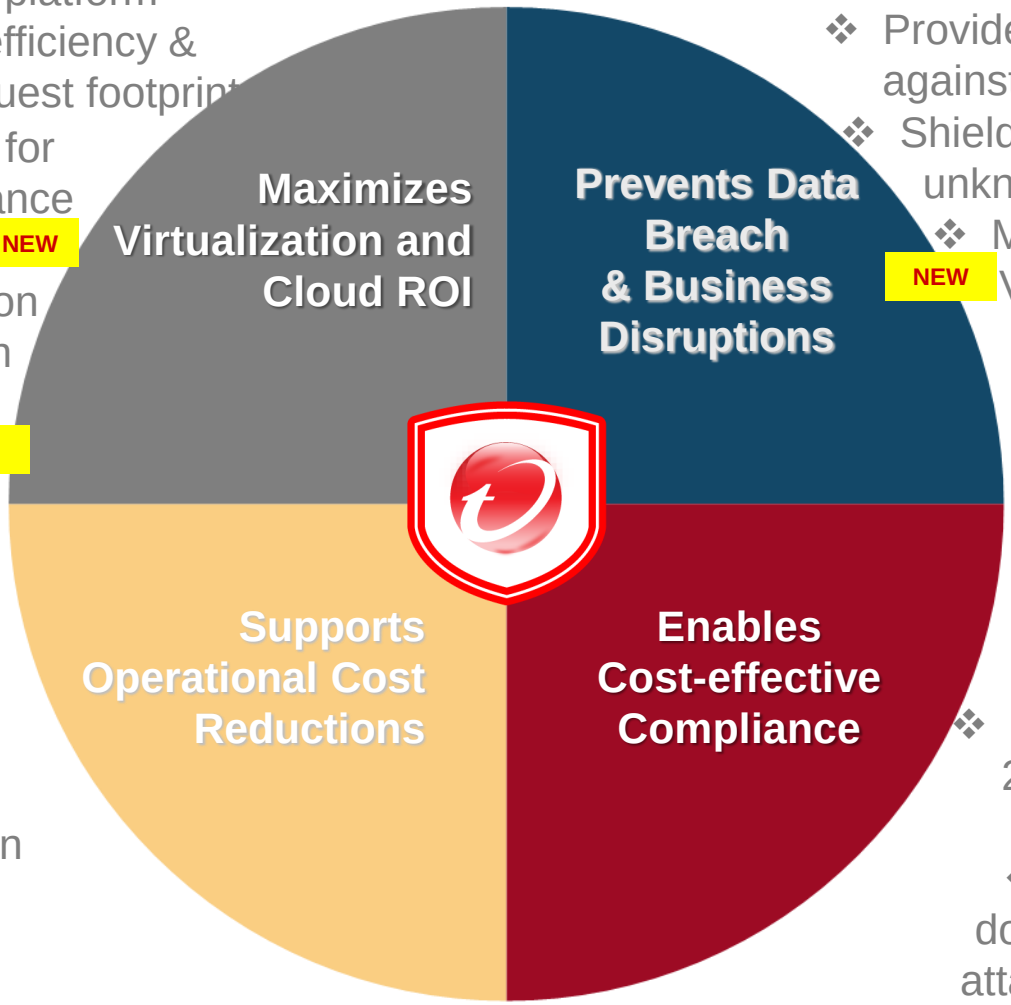
Same architecture can be deployed as security-as-a-service by IaaS public cloud providers, or within enterprise ITaaS for private clouds

*e.g. NIST definition of Cloud Computing



Deep Security: Overall benefits

- Agentless security platform increases resource efficiency & VM density with zero guest footprint
- Scanning de-duplication for increases scan performance and resource efficiency NEW
- vCloud Director & Amazon Web Services integration automatically secures public/hybrid clouds NEW
- Multi-tenancy support enables providers to offer secure clouds NEW



- Provides layered defense against advanced attacks
- Shields against known & unknown vulnerabilities
- Monitors integrity of VMware hypervisor NEW
- Web reputation prevents malicious website access

- Integrated security managed by single pane of glass
- Supports task automation with recommendation scans, trusted sources and event whitelisting
- Virtual patching reduces need for emergency patching enables prioritization of secure coding efforts

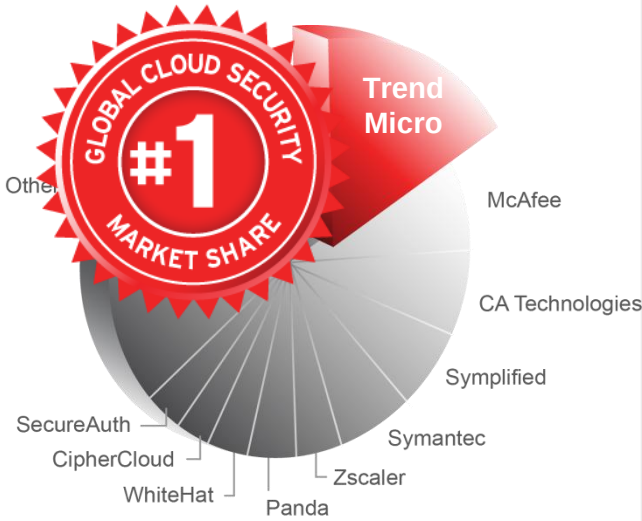
- Supports PCI DSS 2.0, NIST, HIPAA & other regulations
- Detailed reports document prevented attacks & compliance status

TREND MICRO

DIGITAL SIMA

Deep Security
Summary of highlights

- A fully integrated server security platform
- Only solution to offer specialized protection for physical virtual and cloud
- First and only agentless security platform (anti-malware, web reputation, firewall, intrusion prevention, VM & hypervisor integrity monitoring) for VMware environment
- First and only datacenter security solution that extends to public/hybrid cloud
- Only solution in its category to be certified EAL 4+



TREND MICRO

DIGITAL SIMA

DIGITAL SIMA

1988

Ίδρυση της Digital SIMA

1990

Προώθηση κι εξειδίκευση σε λύσεις δικτύωσης WAN / LAN / Voice Data

2000

Νέο τμήμα Ασφάλειας Δικτύων

2010

Διανομή και μεταπώληση προϊόντων LAN / WAN και Ασφάλειας Δικτύων

Τεχνογνωσία και Υποστήριξη

Ποιοτική Επιλογή Προϊόντων

Εξειδίκευση

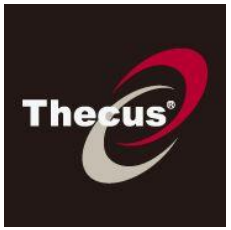
TREND MICRO

DIGITAL SIMA

Networking

Security

Storage



TREND MICRO
Securing Your Journey to the Cloud

Σας Ευχαριστώ !