
AS Stallion
110311
Security for Virtual Server Environments
Urmas Püss

Trend 1: Threat Evolution & Perimeter Porosity

Trend 2: Challenges of Dynamic Datacenter

Deep Security: Make Servers Self-Defending

Deep Security: Agentless AV and IDS/IPS

TREND 1: Today's threat environment

- **More Profitable**
  - $100 billion: Estimated profits from global cybercrime
    -- *Chicago Tribune, 2008*

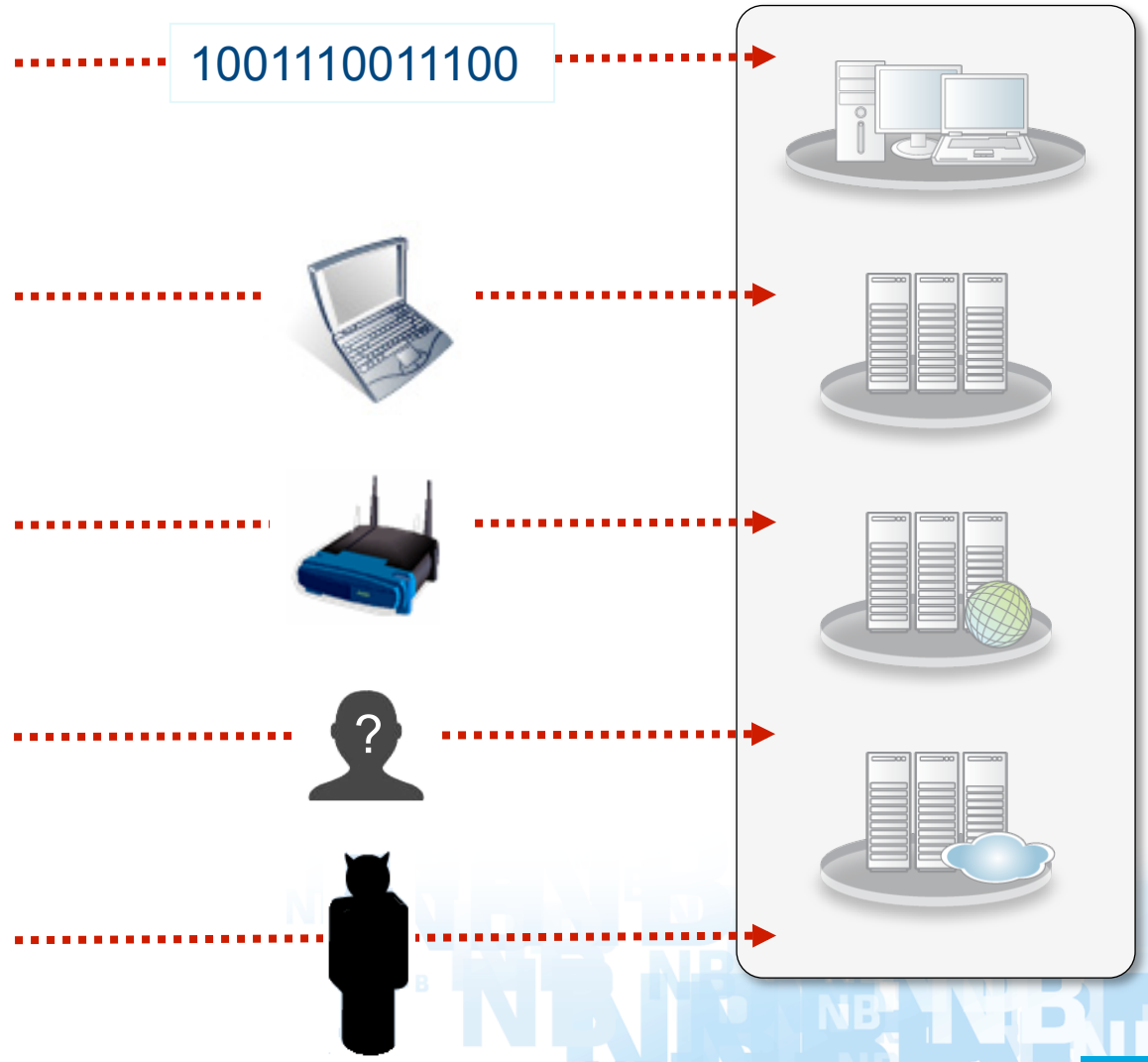
- **More Sophisticated**
  - "Breaches go undiscovered and uncontained for weeks or months in 75% of cases."
    -- *Verizon Breach Report, 2009*

- **More Frequent**
  - "Harvard and Harvard Medical School are attacked every 7 seconds, 24 hours a day, 7 days a week."
    -- *John Halamka, CIO*

- **More Targeted**
  - "27% of respondents had reported targeted attacks".
    -- *2008 CSI Computer Crime & Security Survey*

Perimeter defenses are not enough

1. Encrypted Attacks
2. Mobile Computers
3. Wireless Networks
4. Unsuspecting Users
5. Insider Attacks



© 2005, Third Brigade Inc.

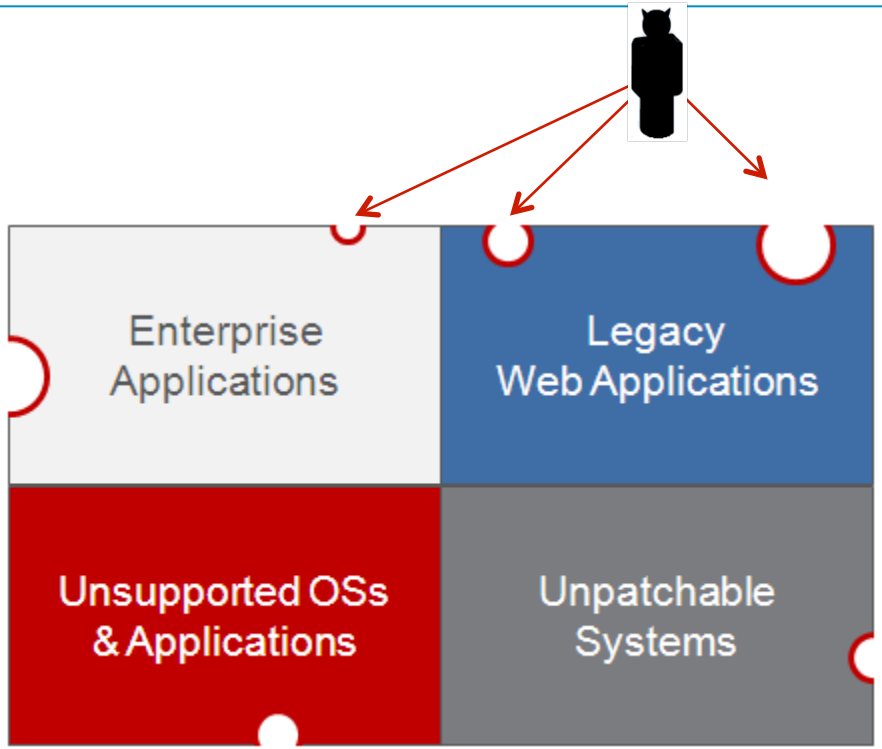
Where are you vulnerable?

Takes days to months until patches are available and can be tested & deployed:

- "Microsoft Tuesday"
- Oracle
- Adobe

Patches are no longer being developed:

- Red Hat 3 -- Oct 2010
- Windows 2000 -- Jul 2010
- Solaris 8 -- Mar 2009
- Oracle 10.1 -- Jan 2009



Developers not available to fix vulnerabilities:

- No longer with company
- Working on other projects

Can't be patched because of cost, regulations, SLA reasons:

- POS
- Kiosks
- Medical Devices

Trend 1: Threat Evolution & Perimeter Porosity

Trend 2: Challenges of Dynamic Datacenter

Deep Security: Make Servers Self-Defending

Deep Security: Agentless AV and IDS/IPS

TREND 2: The Evolving Datacenter
Lowering Costs, Increasing Flexibility

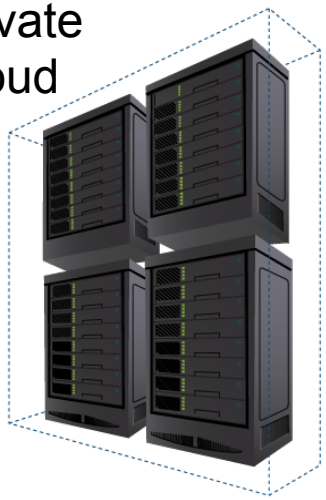
Physical

Traditional datacenter

Virtual

Servers virtualized with minimal changes to datacenter processes

Private Cloud



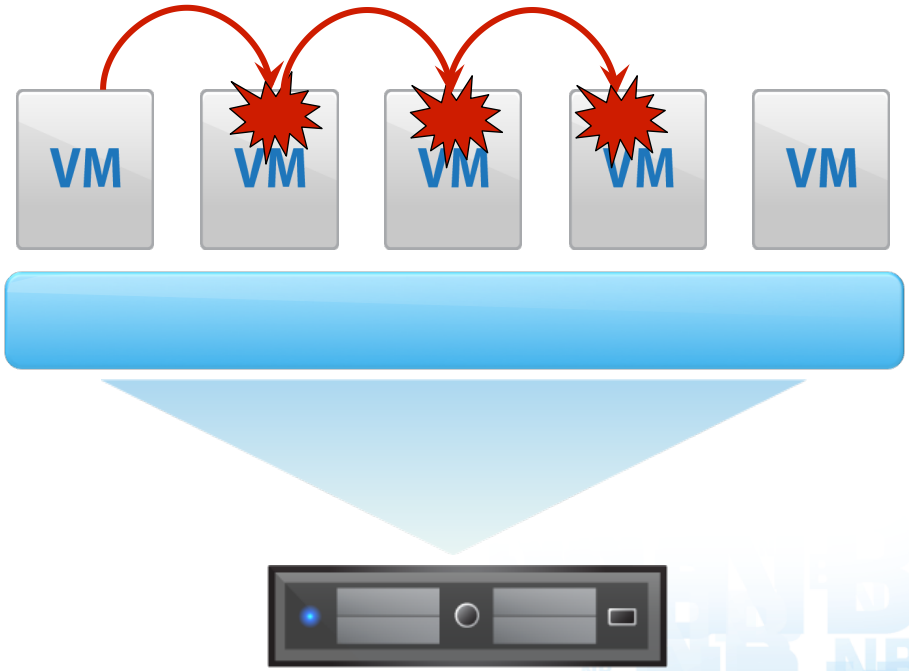
Servers virtualized in scalable, shared, automated & elastic environment

Public Cloud

Select enterprise applications in public cloud

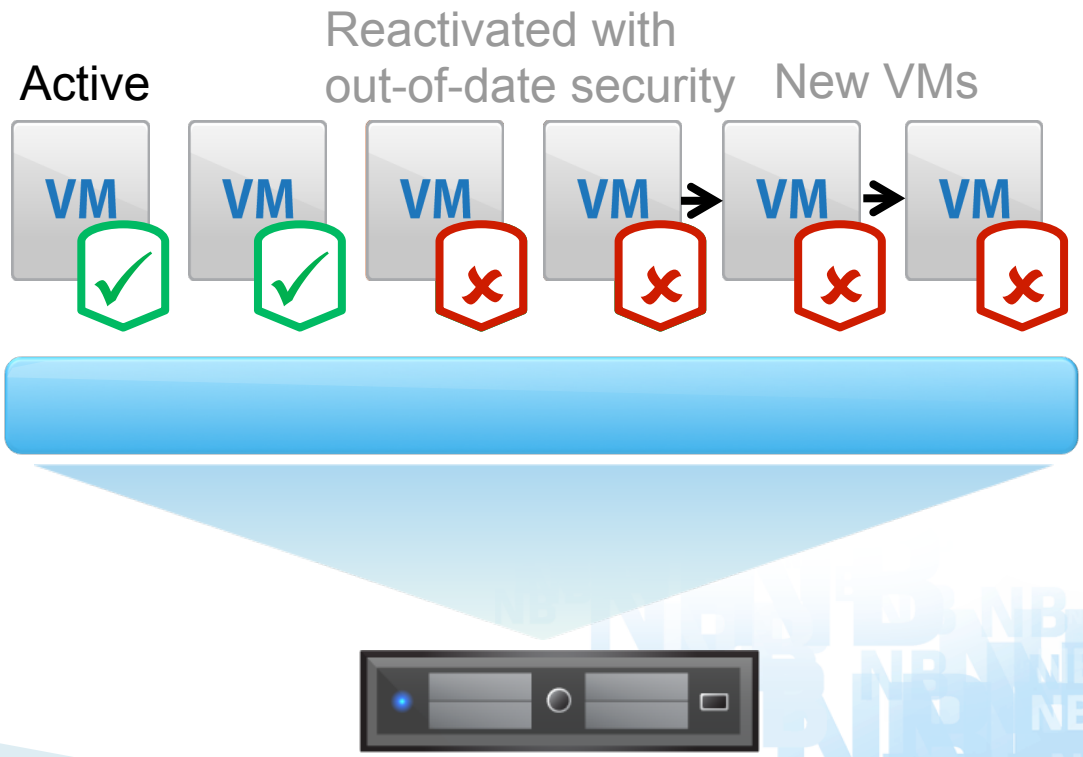
Stage 1 Security Inhibitors

1 Inter-VM attacks/ blind spots



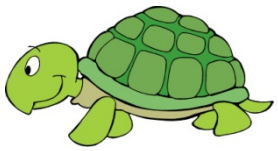
Security Inhibitors to Virtualization

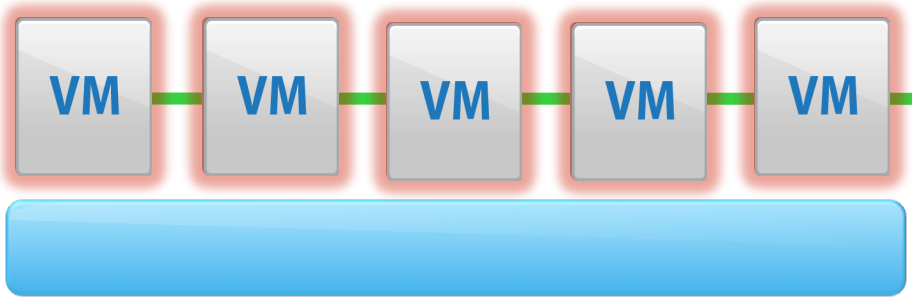
2 Instant-on gaps



Stage 2 Security Inhibitors

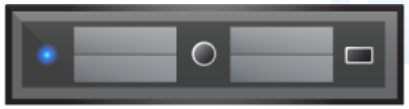
3 Resource contention





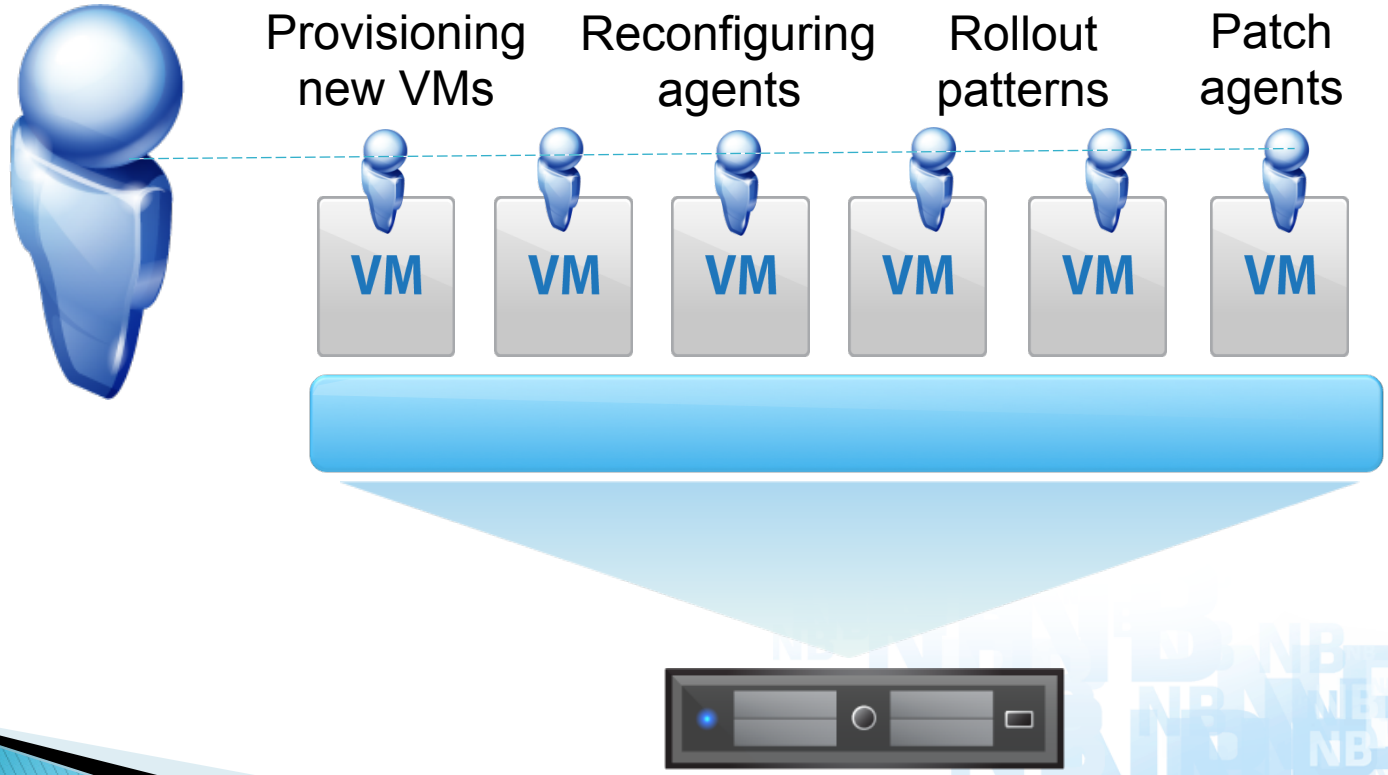
3:00am Scan

Typical AV Console



Security Inhibitors to Virtualization

4 Complexity of Management



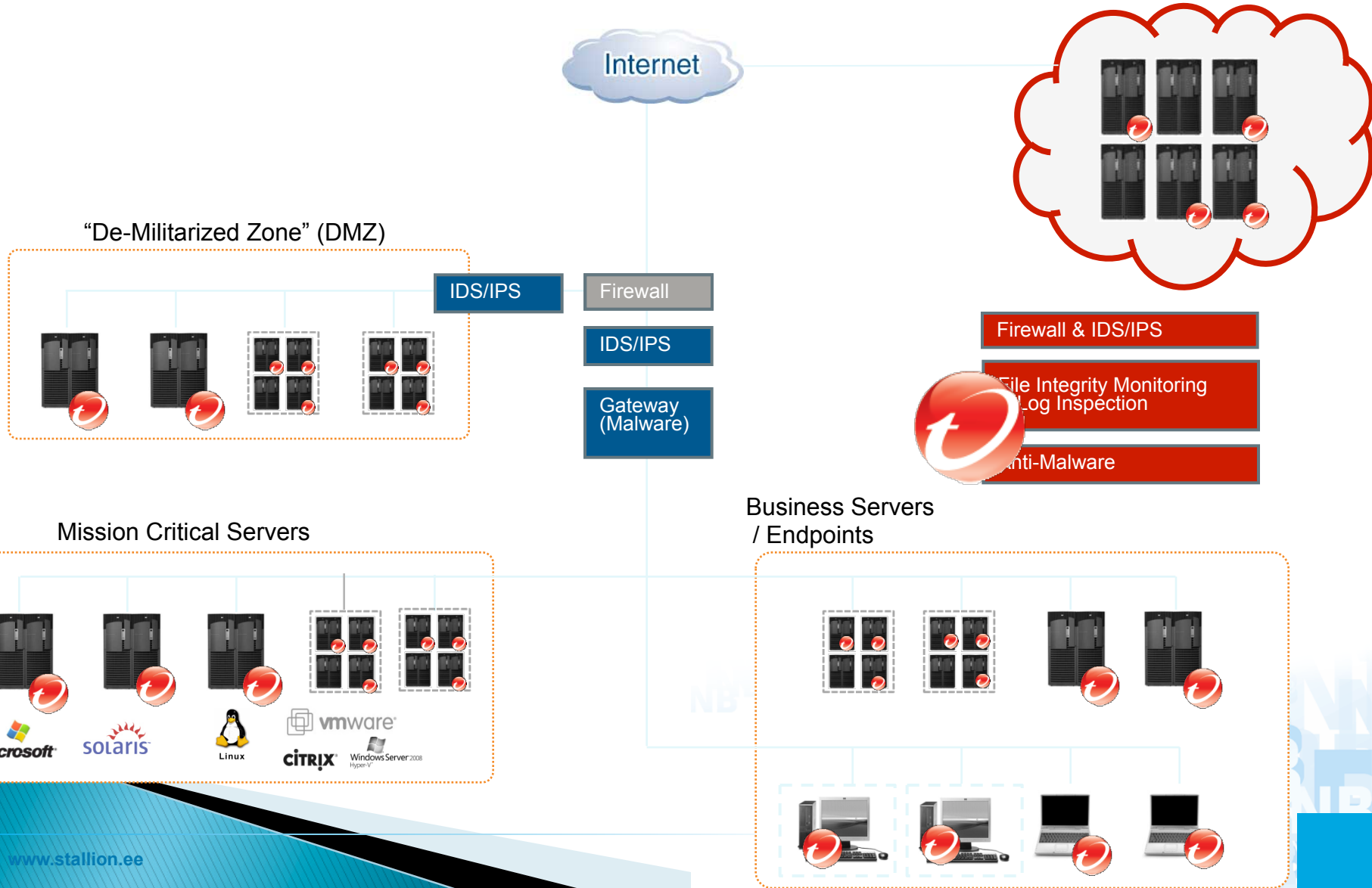
Trend 1: Threat Evolution & Perimeter Porosity

Trend 2: Challenges of Dynamic Datacenter

Deep Security: Make Servers Self-Defending

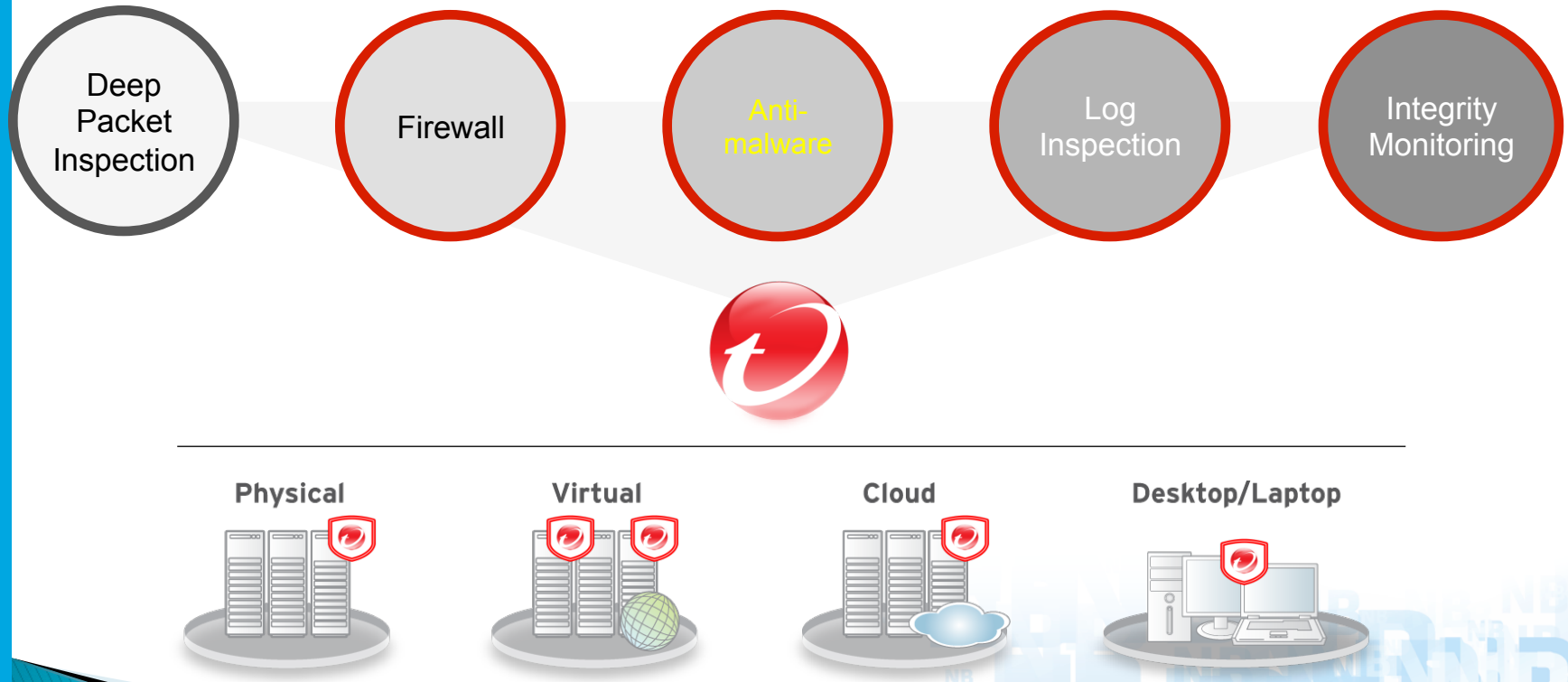
Deep Security: Agentless AV and IDS/IPS

Retreat To The Server!



Trend Micro Deep Security
Server & application protection

- Latest anti-malware module adds to existing set of advanced protection modules



Trend Micro Deep Security
Server & application protection

5 protection modules

Deep Packet Inspection

- IDS / IPS
- Web Application Protection
- Application Control

Shields web application vulnerabilities

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

Provides increased visibility into, or control over, applications accessing the network

Reduces attack surface. Prevents DoS & detects reconnaissance scans

Firewall

Anti-Virus

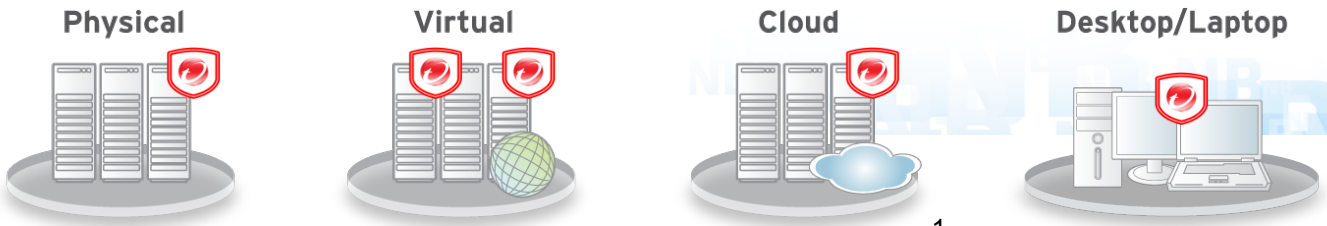
Detects and blocks malware (web threats, viruses & worms, Trojans)

Optimizes the identification of important security events buried in log entries

Log Inspection

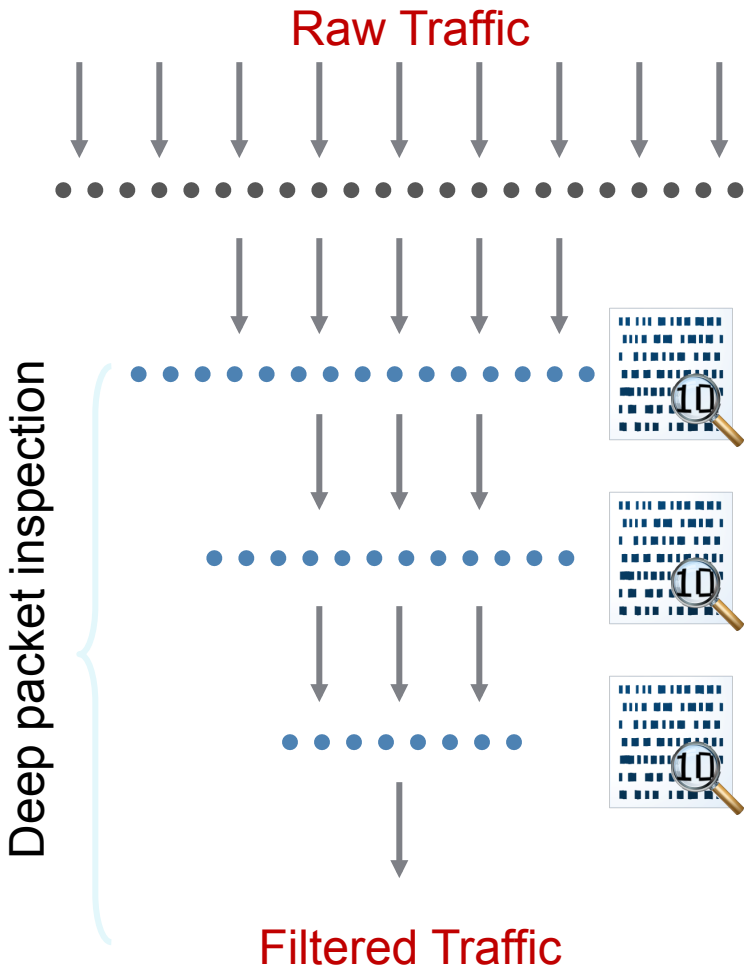
Integrity Monitoring

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



Protection is delivered via Agent and/or Virtual Appliance

Layered approach to shielding vulnerabilities



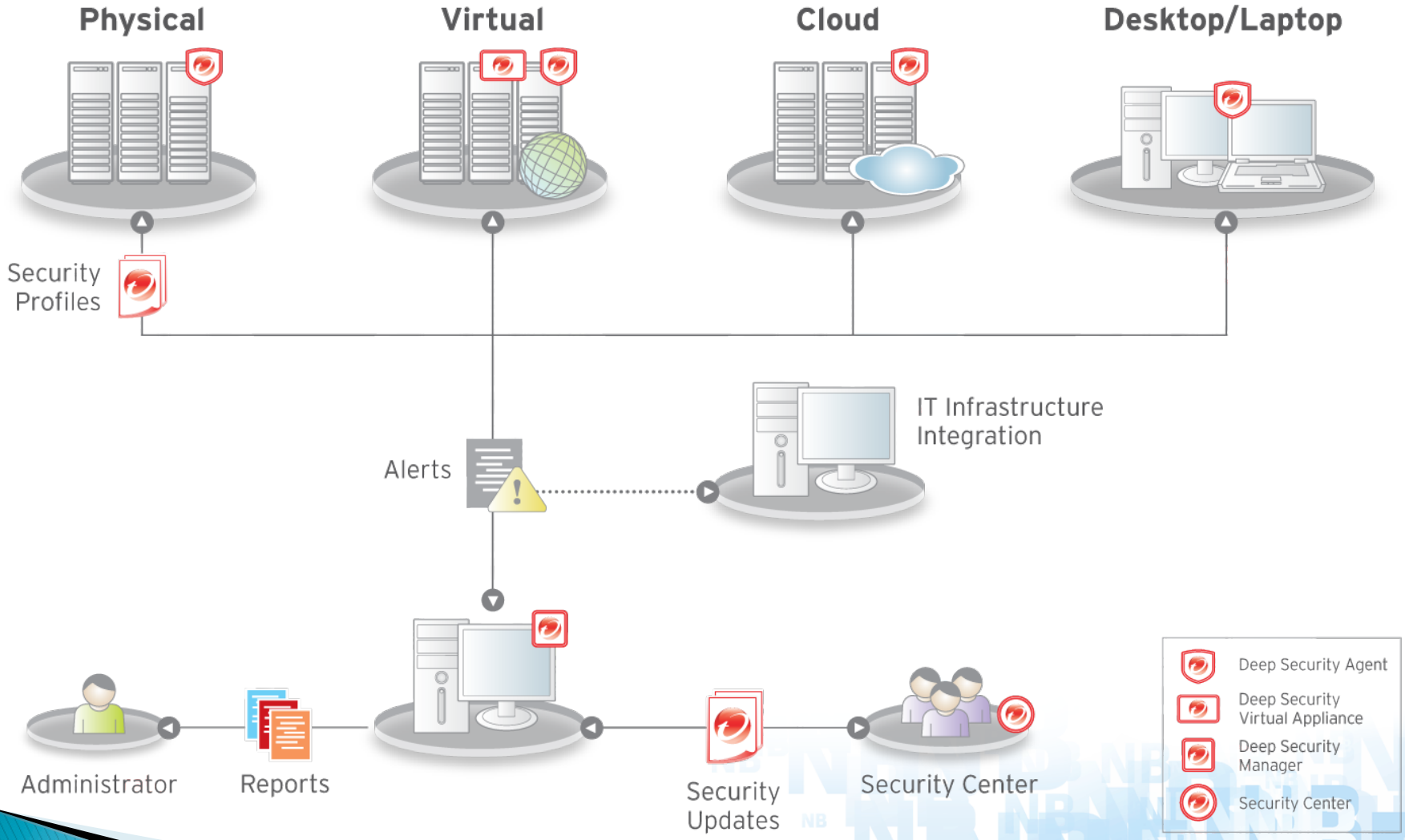
1	Stateful Firewall	Allow known good
2	Exploit Rules	Stop known bad
3	Vulnerability Rules	Shield known vulnerabilities
4	Smart Rules	Shield unknown vulnerabilities (Zero-day) , and protect specific applications

Over 100 applications protected

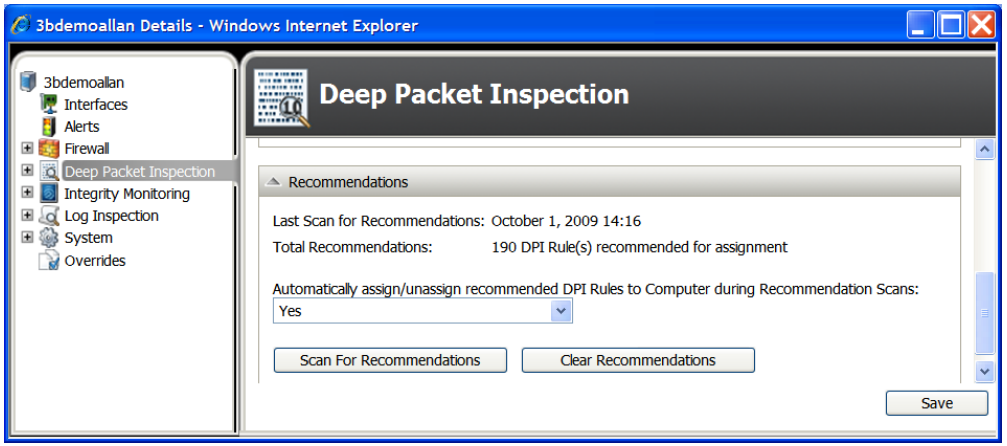
Deep Security rules shield vulnerabilities in these common applications

Operating Systems	Windows (2000, XP, 2003, Vista, 2008, 7), Sun Solaris (8, 9, 10), Red Hat EL (4, 5), SuSE Linux (10,11)
Database servers	Oracle, MySQL, Microsoft SQL Server, Ingres
Web app servers	Microsoft IIS, Apache, Apache Tomcat, Microsoft Sharepoint
Mail servers	Microsoft Exchange Server, Merak, IBM Lotus Domino, Mdaemon, Ipswitch, IMail,, MailEnable Professional,
FTP servers	Ipswitch, War FTP Daemon, Allied Telesis
Backup servers	Computer Associates, Symantec, EMC
Storage mgt servers	Symantec, Veritas
DHCP servers	ISC DHCPD
Desktop applications	Microsoft (Office, Visual Studio, Visual Basic, Access, Visio, Publisher, Excel Viewer, Windows Media Player), Kodak Image Viewer, Adobe Acrobat Reader, Apple Quicktime, RealNetworks RealPlayer
Mail clients	Outlook Express, MS Outlook, Windows Vista Mail, IBM Lotus Notes, Ipswitch IMail Client
Web browsers	Internet Explorer, Mozilla Firefox
Anti-virus	Clam AV, CA, Symantec, Norton, Trend Micro, Microsoft
Other applications	Samba, IBM Websphere, IBM Lotus Domino Web Access, X.Org, X Font Server prior, Rsync, OpenSSL, Novell Client

Deep Security architecture



Recommendation Scans



- The server being protected is analyzed to determine:
  - OS, service pack and patch level
  - Installed applications and version
  - DPI rules are recommended to shield the unpatched vulnerabilities from attacks
  - As patches, hotfixes, and updates are applied over time, the Recommendation Scan will:
    - Recommend new rules for assignment
    - Recommend removal of rules no longer required after system patching
  - Recommendations for DPI, Integrity Monitoring, and Log Inspection rules are supported

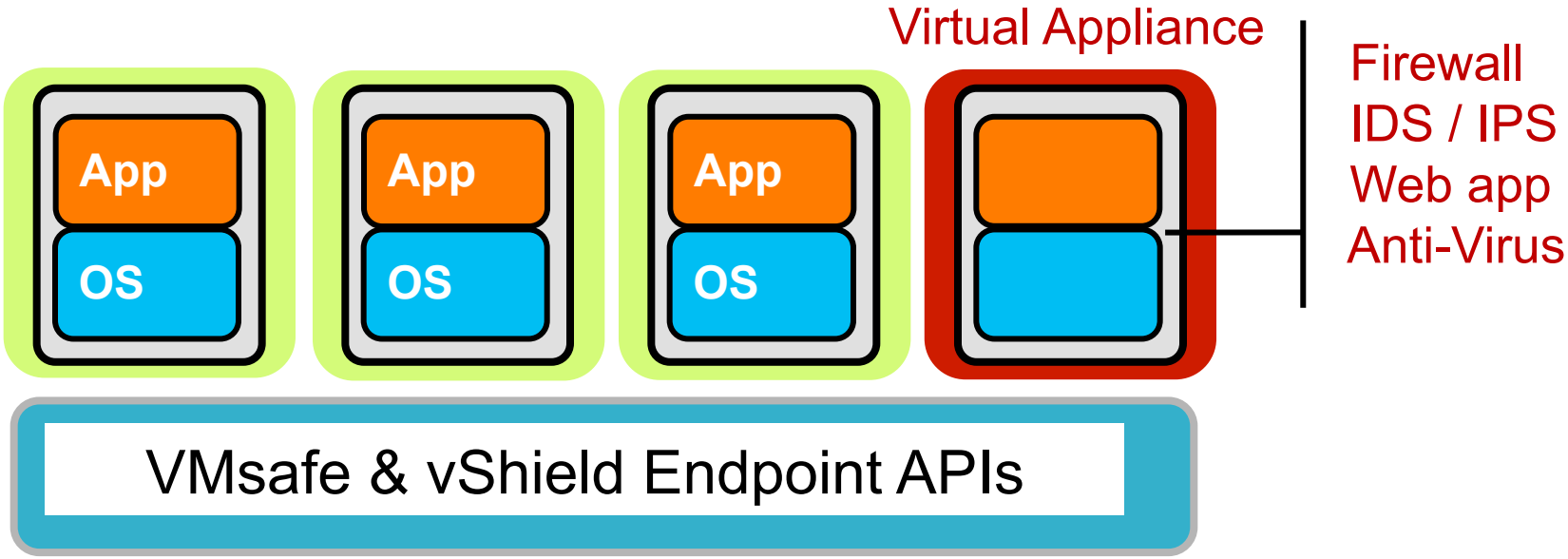
Trend 1: Threat Evolution & Perimeter Porosity

Trend 2: Challenges of Dynamic Datacenter

Deep Security: Make Servers Self-Defending

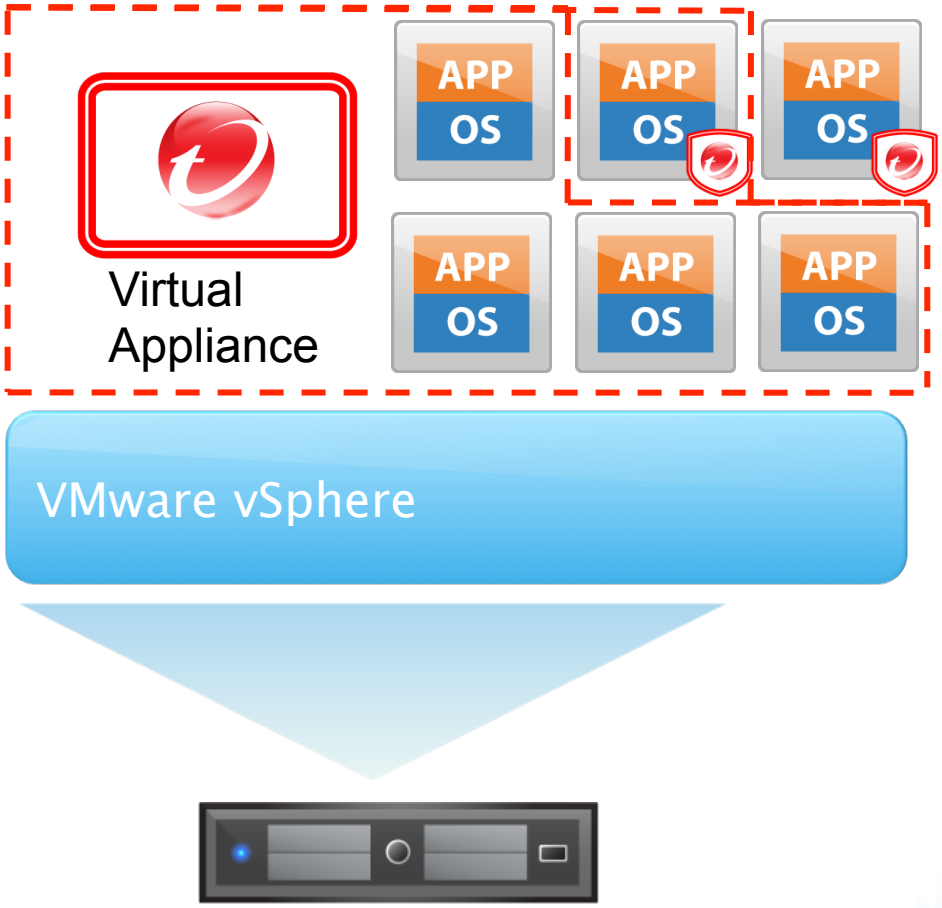
Deep Security: Agentless AV and IDS/IPS

Leveraging New Security Paradigms
VMware hypervisor APIs – VMsafe & vShield Endpoint



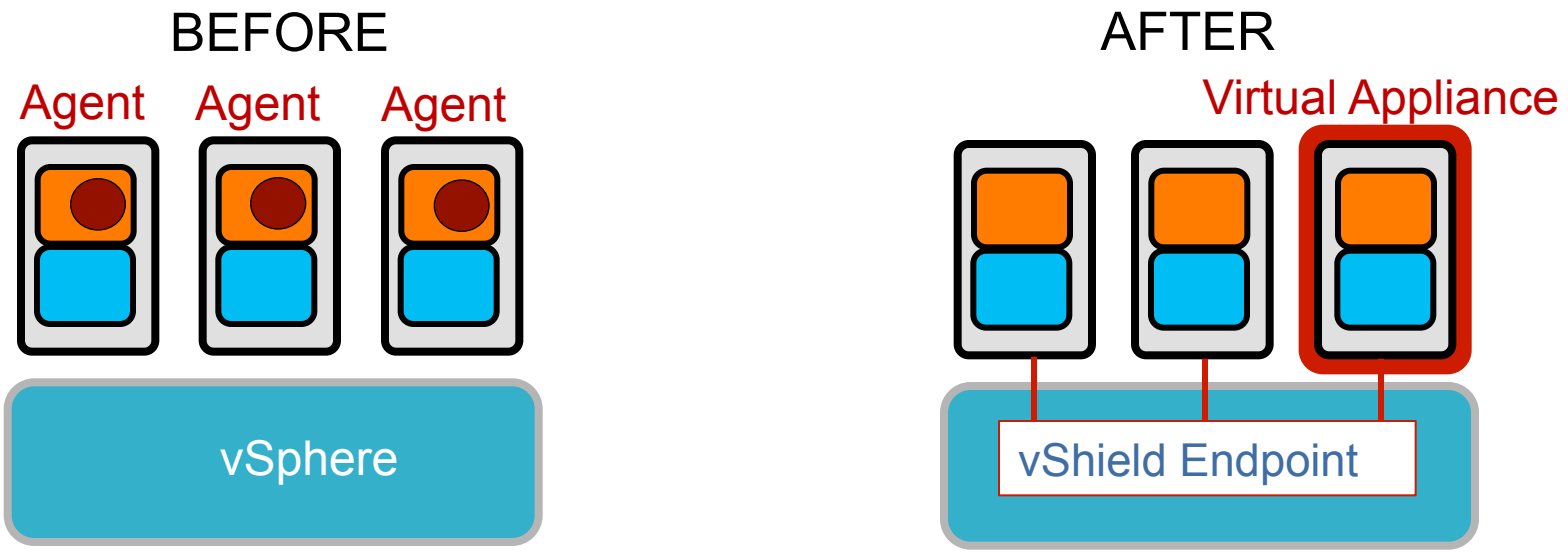
- Secures VMs from the outside, no changes to VM
- VMsafe enables traffic inspection at hypervisor layer
- vShield Endpoint enables agentless AV scanning
- Enables strong tamper-proofing from malware

Coordinated Protection with Agent and Security Virtual Appliance



- Agent adds additional protection not possible over hypervisor today
- vCenter integration makes agents virtualization-aware
- Useful for offline desktops, cloud, defense in depth
- Deep Security Virtual appliance kicks in if agent were to disappear/roll back

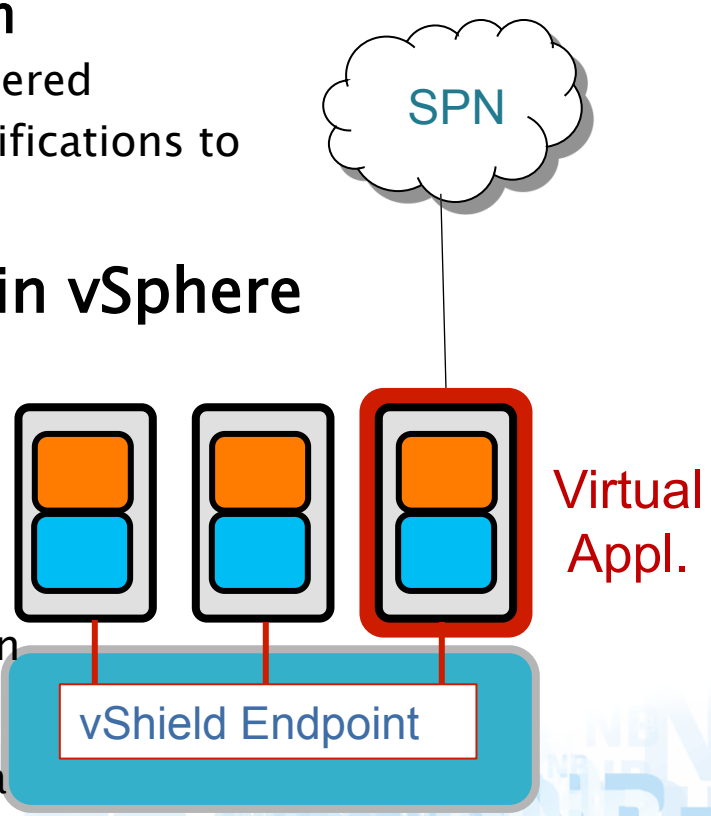
The Promise of Agentless Anti-malware



- Significantly improved manageability - no agents to configure, update and patch
- Faster performance – Freedom from AV Storms
- Stronger security – Instant ON protection + tamper-proofing
- Higher consolidation levels – Inefficient operations removed

Deep Security 7.5 Key New Features

- **Agent-Less Real Time Scan**
  - Triggers notifications to AV engine on file open/close
  - Provides access to file data for scanning
- **Agent-Less Manual and Schedule Scan**
  - On demand scans are coordinated and staggered
  - Traverses guest file-system and triggers notifications to the AV engine
- **Integrates with vShield Endpoint (in vSphere 4.1)**
- **Zero Day Protection**
  - Trend Micro SPN Integration
- **Agent-Less Remediation**
  - Active Action, Delete, Pass, Quarantine, Clean
- **API Level Caching**
  - Caching of data and results to minimize data traffic and optimize performance



TÄNAN.