TREND MICRO™ Securing Your Web World

Next Generation Datacenters & the Realities of Virtualisation Security

Simon Young • General Manager, Server Security EMEA

Agenda

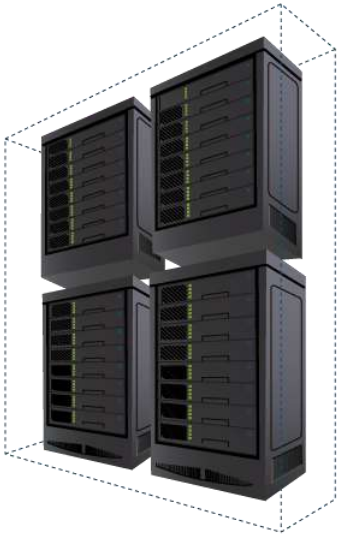
- The Dynamic Data Center & New Security Challenges
- Leveraging Virtualised Infrastructure for improved Security
- Deep Security 7: Overview
- Key Benefits
- Questions

The Dynamic Datacenter

Physical

8 million servers shipped in 2008, ~ 50 million servers deployed
- *IDC*

Virtualised



"30-40% of datacenters are now running critical applications on VMs." - *VMware*
"1 in 4 workloads deployed in 2008 to X86 server was to a VM"
- *Gartner*

Cloud computing

"By 2012, 40% of hardware Infrastructure spending will be as a service."
- *Gartner*

TREND MICRO

Software Vulnerabilities are being Targeted

Gas refineries at Defcon 1 as SCADA exploit goes wild

September 8, 2008: Gasoline refineries, manufacturing plants and other critical facilities that rely on computerized control systems just became more vulnerable to tampering or sabotage with the release of attack code that exploits a security flaw in a widely used piece of software.

Critical Windows vulnerability under attack, Microsoft warns

May 28, 2009 Microsoft has warned of a critical security bug in older versions of its Windows operating system that is already being exploited in the wild to remotely execute malware on vulnerable machines.

Next-gen SQL injection opens server door: 1 in 10 sites naked

April 2, 2009 A vulnerability estimated to affect more than 1 in 10 websites could go lethal with the finding that it can be used to reliably take complete control of the site's underlying server.

TREND MICRO

High profile breaches

Heartland Payment Systems

May-2008: Security breach cost $12.6 million so far, including legal costs and fines from MasterCard and Visa. More >>

fiserv.

Dec-2008: DNS hijacking puts 5,000,000 check processing accounts at risk. More >>

RBS WorldPay

Dec-2008: PII of 1.5M customers & 1.1M Social Security Numbers. More >>

Federal Aviation Administration

Mar-2009: Hackers hijack PII for 45,000 employees & retirees. More >>

TJX

Aug-2007: Hackers placed software on the company's network, and steal 45 M credit card #'s. Costs soar to $256 M. More >>

Cal University of California Berkeley

May-2009: Hackers broke into 2 databases over a 6 month period, and exposed the data of 160,000+ students. More >>

TREND MICRO

Threat Environment

VULNERABILITIES

WEB THREATS

DATA STEALING MALWARE

BOTS

- **More profitable**
  - **$100 billion: Estimated profits from global cybercrime**
    -- *Chicago Tribune, 2008*
- **More sophisticated, malicious & stealthy**
  - **"95% of 285 million records stolen in 2008, were the result of highly skillful attacks"**
  - **"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

TREND MICRO

Compliance Imperative

More standards:

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

More specific security requirements

- Virtualization, Web applications, EHR, PII…

More penalties & fines

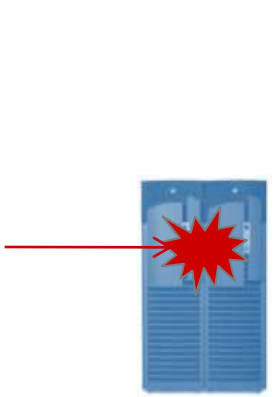
- HITECH, Breach notifications, civil litigation

> "DMZ consolidation using virtualization will be a "hot spot" for auditors, given the greater risk of misconfiguration and lower visibility of DMZ policy violation. Through year-end 2011, auditors will challenge virtualized deployments in the DMZ more than nonvirtualized DMZ solutions.
>
> Neil MacDonald, Gartner, June 2009"

TREND MICRO

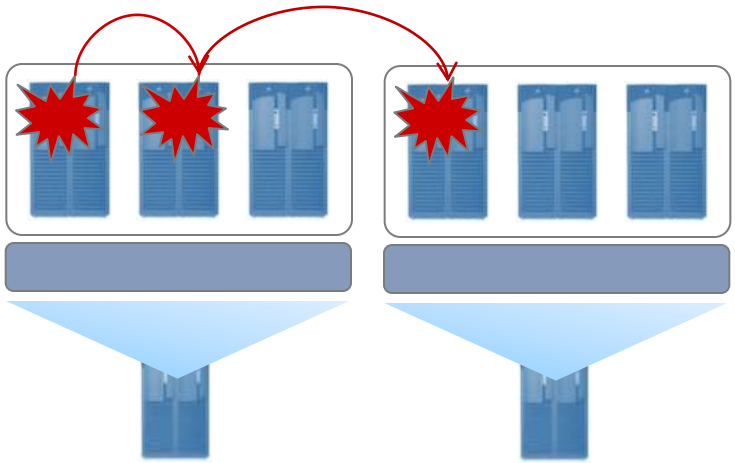
Perimeter defences alone are no longer sufficient

Physical Servers



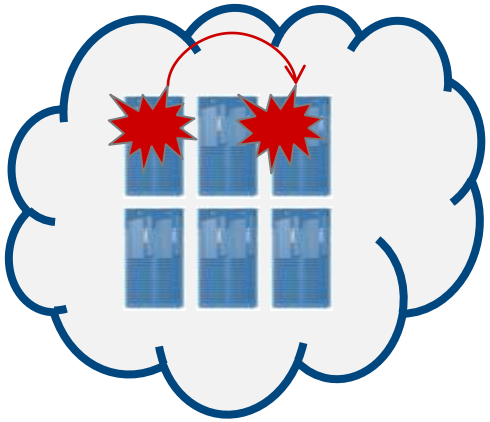
Servers under pressure
- Encrypted attacks
- Wireless networks
- Insider attacks
- Web app attacks

Virtualized Servers



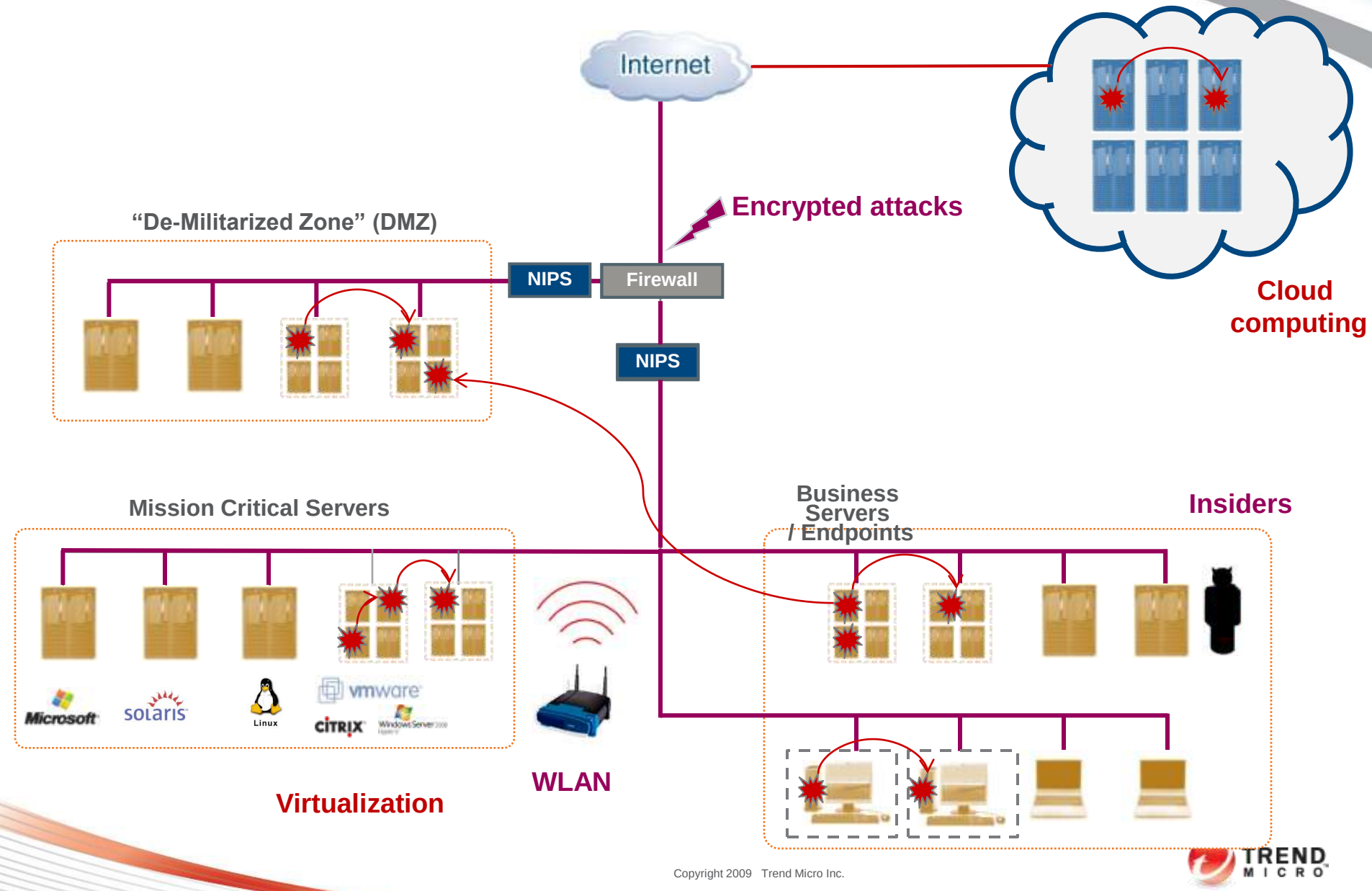
Servers in motion
- Hosting workloads of different sensitivities
- vMotion challenges
- VMs introduced quickly

Cloud Computing



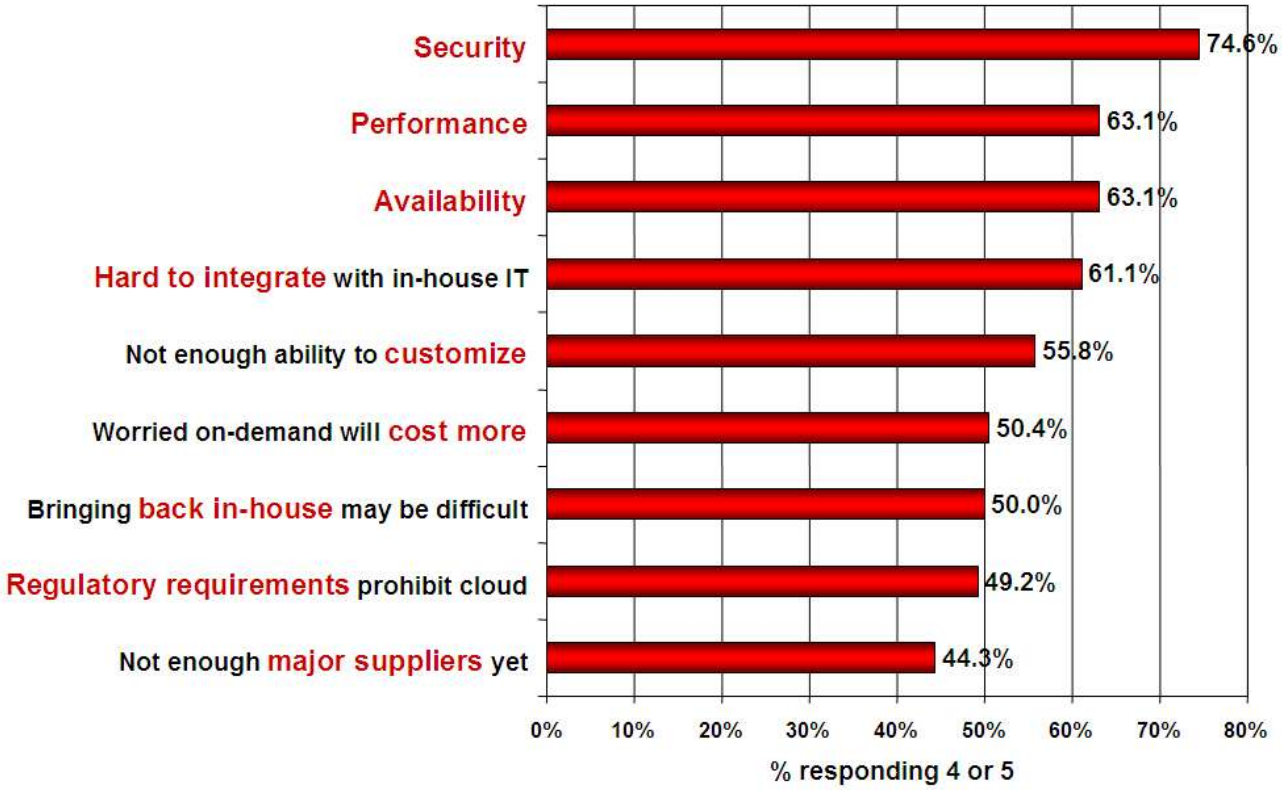
Servers in the open
- Your perimeter provides no protection.
- Cloud computing vendors provide basic, “lowest common denominator” security, which undermines your compliance

Perimeter is cracking



Cloud security is a recognised concern

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

New approaches will be needed to secure cloud-based IT services."

Gartner
***"Cloud-Based Computing Will Enable New Security Services and Endanger Old Ones,"* June 2008**

TREND MICRO

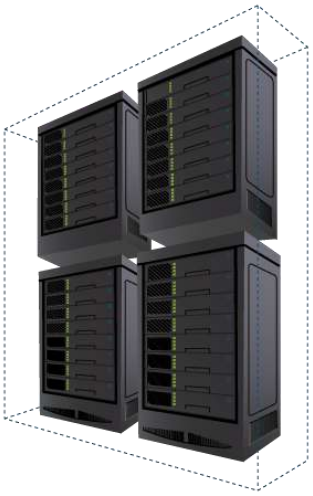
Security Challenges

Challenges	Virtualisation	In Cloud
Dynamic virtual machines: VM Sprawl	✓	
Vulnerability exploits & patch management	✓	✓
Web application threats	✓	✓
System & data integrity: compromise via co-location	✓	✓
Policy & compliance	✓	✓
Rogue corporate resources		✓
Service provider security		✓

TREND MICRO

Dynamic Virtual Machines

Dynamic:



→ Reverted

→ Paused

→ Restarted

→ Cloned

→ Moved

Security challenges

- Achieve and maintain consistent security
  - Propagation of vulnerabilities and configuration errors
  - Maintaining an auditable record of the security state

Vulnerability Exploits & Patch Management

"90% of known *"vulnerabilities that were exploited had patches available for at least six months prior to the breach"*

Verizon, 2008

- Cloud-based perimeter control only provides lowest common denominator
- Client perimeter does not protect virtual machines deployed in an external cloud
- Firewall and IDS/IPS functionality can be deployed to protect each VM instance

TREND MICRO

Web Application Threats

- SQL injections flaws are the most widespread web application vulnerability type
- Affects commercial and custom web apps
- Web app protection can be deployed in software to protect web apps deployed in cloud

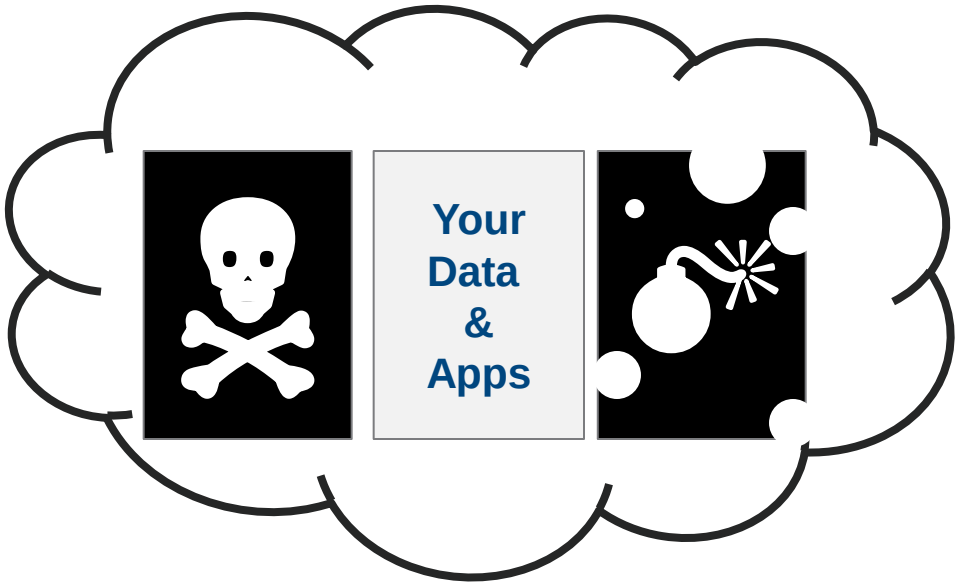
"74% of Web Applications vulnerabilities disclosed had no patch available by end of year"

IBM, 2008

TREND MICRO

System & Data Integrity

"59% of data breaches resulted from hacking and intrusions"
Verizon, 2008



Security Issues:

- Shared physical infrastructure
- Malicious or unauthorised changes

TREND MICRO

Policy & Compliance

- Compliance pressures:
  - PCI, HIPAA, SAS70, ISO, FISMA, COBIT/ COSO…

Challenge:

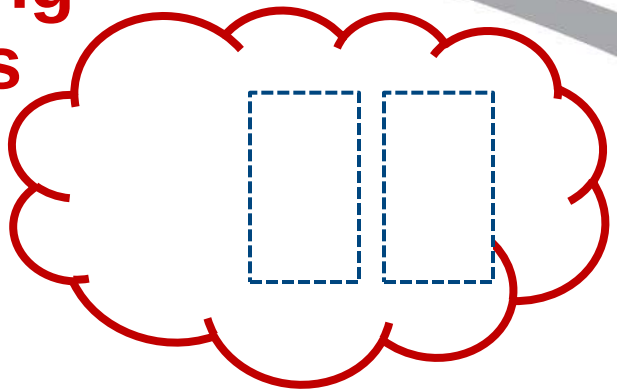
How do you prove compliance when your servers are in the cloud?

TREND MICRO

Leveraging Virtualisation Infrastructure for improved security

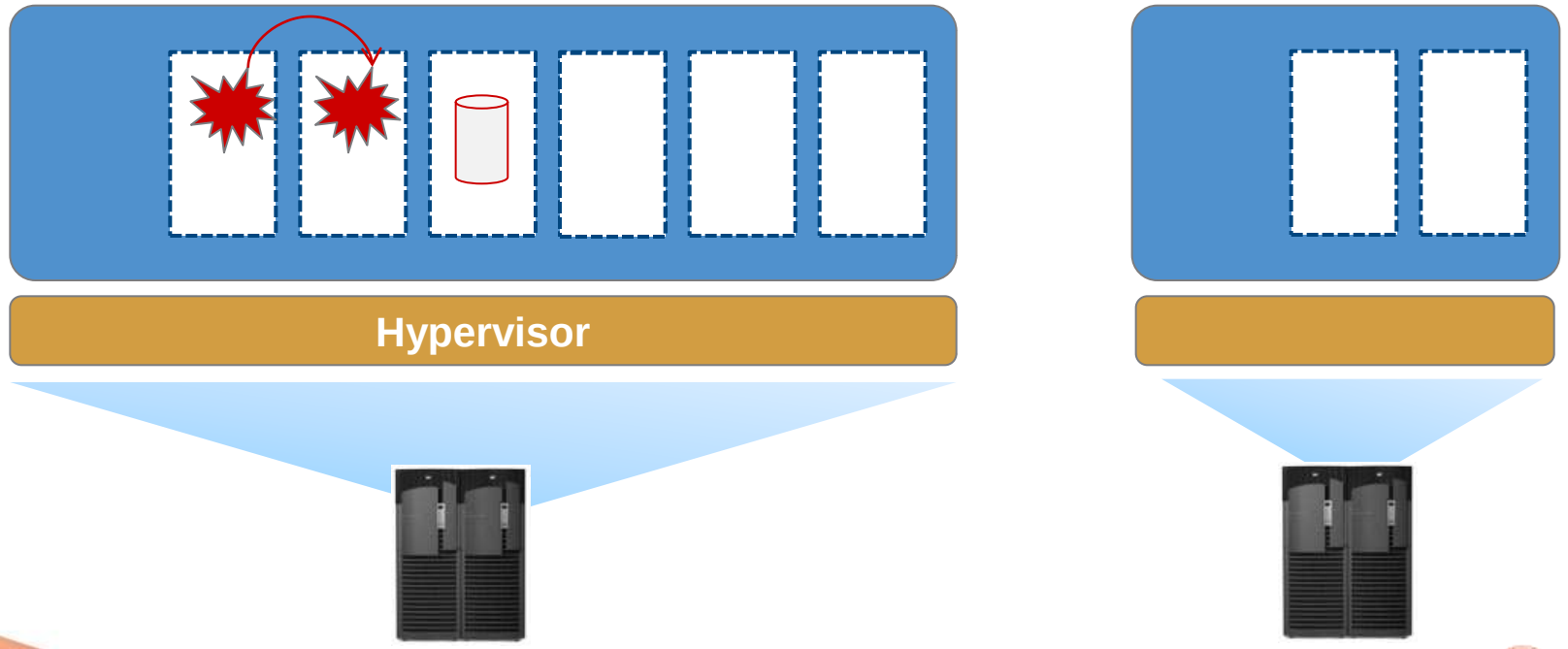
TREND MICRO

Virtualisation & Cloud Computing Create New Security Challenges



Inter-VM attacks

PCI Mobility Cloud Computing

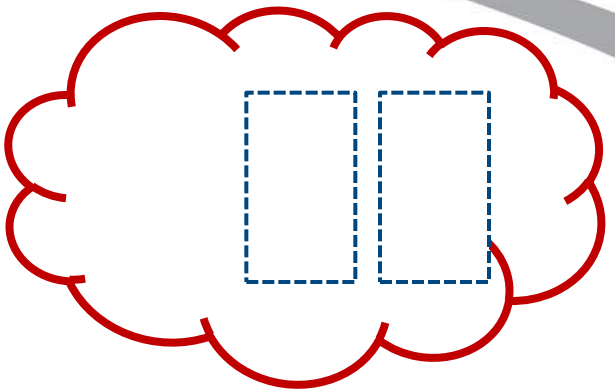


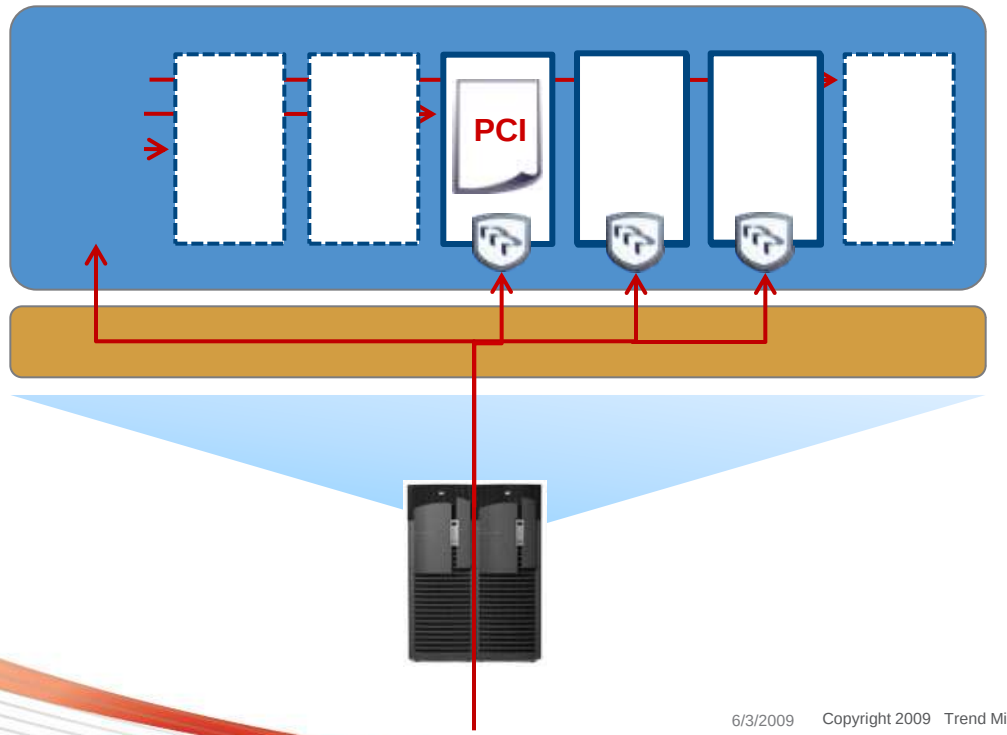
TREND MICRO

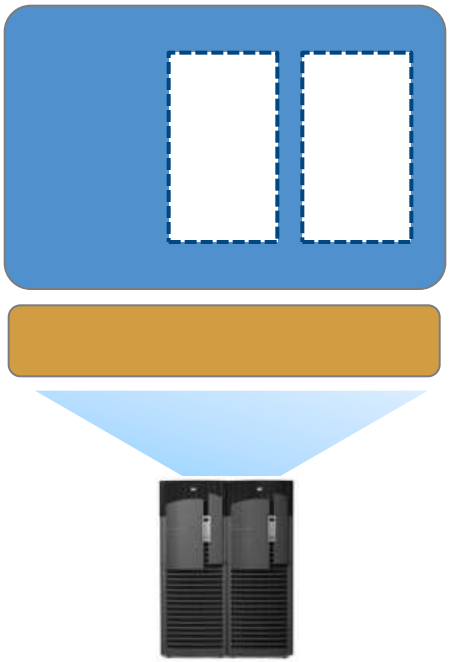
Coordinated Approach

Firewall

IDS / IPS

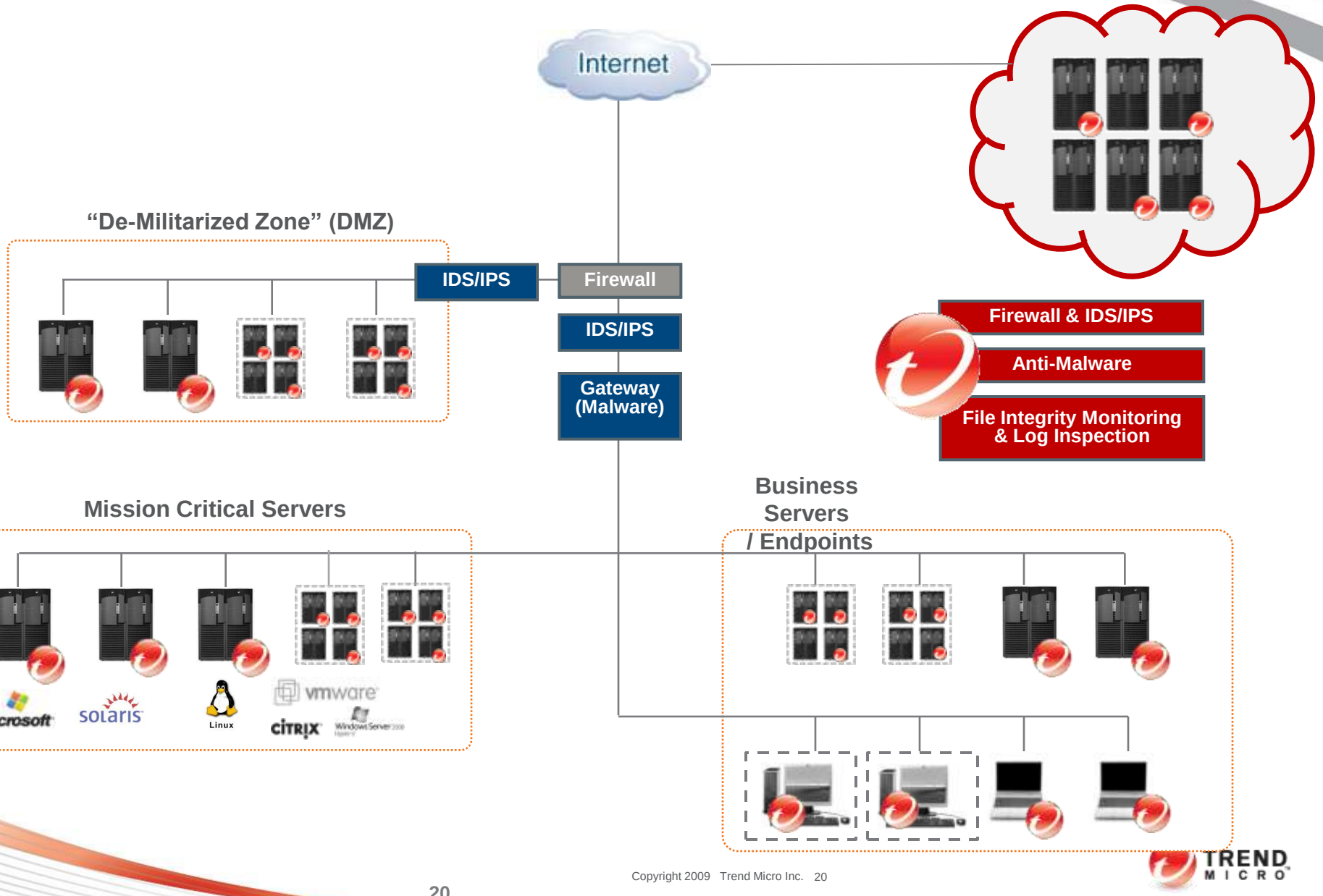






TREND MICRO

Retreat To The Server (VM)!



20

TREND MICRO™ Securing Your Web World

Deep Security 7 Overview

What is Deep Security?

PHYSICAL

VIRTUAL

CLOUD

Deep Packet Inspection

- IDS / IPS
- Web App. Protection
- Application Control

Firewall

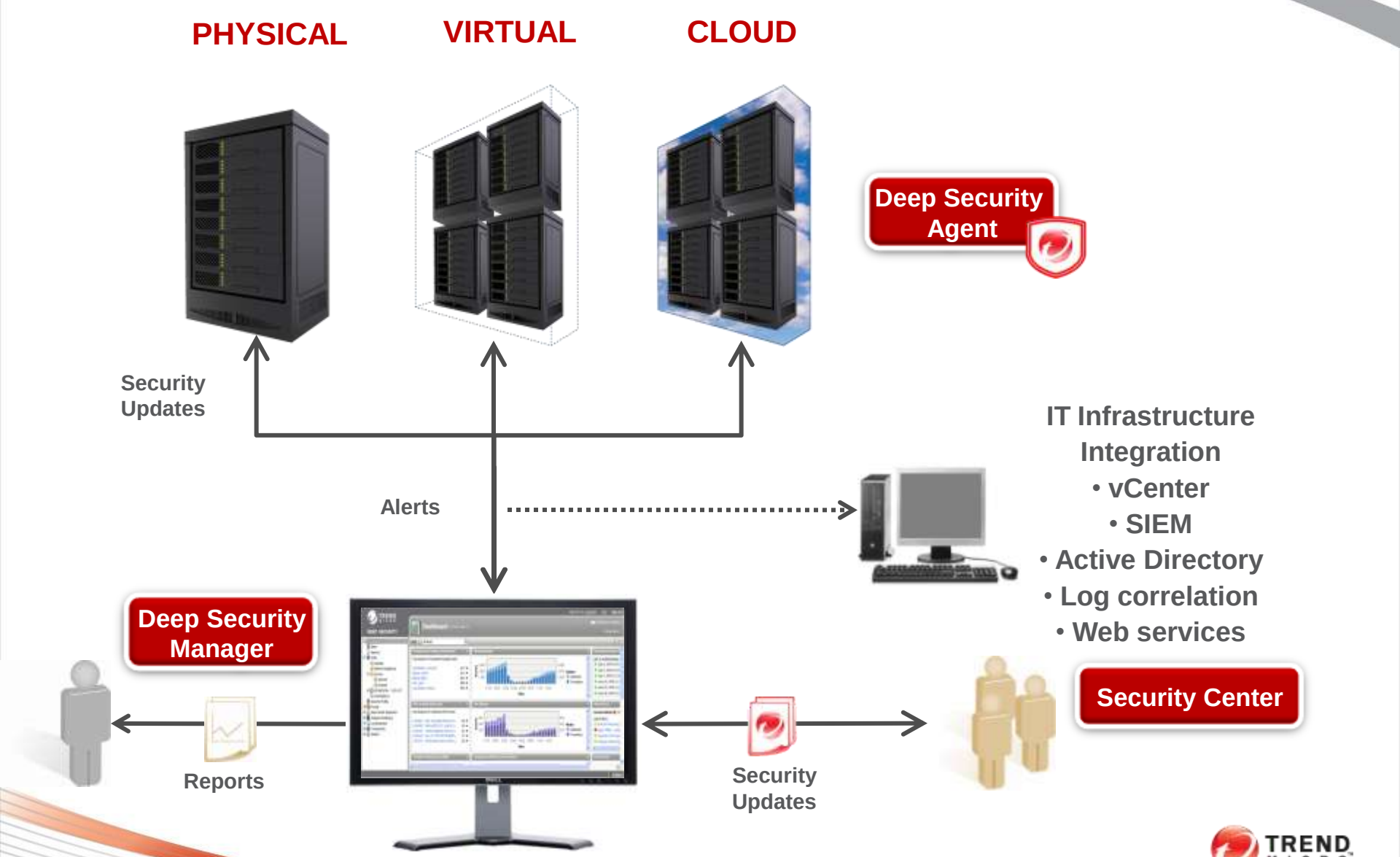
Integrity Monitoring

Log Inspection

Microsoft solaris Linux CITRIX vmware

TREND MICRO

Architecture



TREND MICRO

Security Center:
Dedicated Team of Security Experts

- Track global vulnerabilities
  - 100+ sources of information (public, private, govt): SANS, CERT, Bugtraq, VulnWatch, PacketStorm, and Securiteam
  - Member of Microsoft Active Protections Program
- Respond to new vulnerabilities and threats
  - Advisories & Security updates
- Six-step, rapid response process supported by automated tools
- On-going research to improve overall protection mechanisms

Deep Security: Platforms protected

- Windows 2000
- Windows XP, 2003 (32 & 64 bit)
- Vista (32 & 64 bit)
- Windows Server 2008 (32 & 64 bit)

- 8, 9, 10 on SPARC
- 10 on x86 (64 bit)

- Red Hat 3
- Red Hat 4, 5 (32 & 64 bit)
- SuSE 9, 10

- VMware ESX/ESXi Server (guest OS)
- VMware Server (host & guest OS)

Integrity Monitoring & Log Inspection modules

- HP-UX 11i v2
- AIX 5.3

TREND MICRO

Certifications

Common Criteria

Evaluation Assurance Level 3 Augmented (EAL 3+)

- Achieved certification across more platforms (Windows, Solaris, Linux) than any other host-based intrusion prevention product.
- Higher certification than any other HIPS vendor
- Validated against US National Security Agency defined profile for IDS

NSS Labs

- Third Brigade Deep Security is the first product to pass NSS Labs' PCI Suitability testing for Host Intrusion Prevention Systems (HIPS).
- Across Windows, Solaris and Linux

Deep Security Modules

Firewall

- Centralized management of server firewall policy
- Pre-defined templates for common enterprise server types
- Fine-grained filtering: IP & MAC addresses, Ports
- Coverage of all IP-based protocols: TCP, UDP, ICMP, IGMP …

Deep Packet Inspection

Enables IDS / IPS, Web App Protection, Application Control

Examines incoming & outgoing traffic for:

- Protocol deviations
- Content that signals an attack
- Policy violations.

Integrity Monitoring

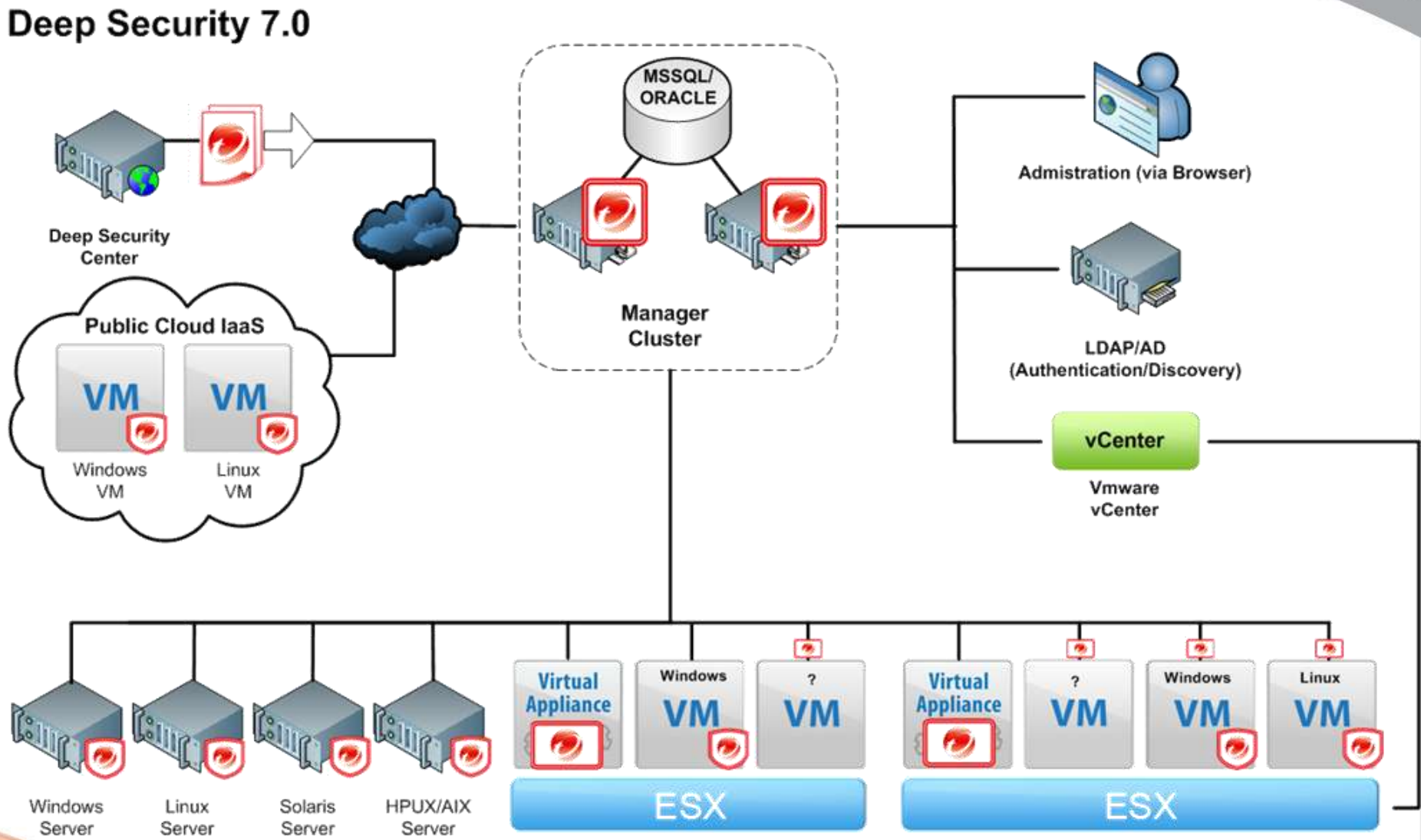
- Monitors critical files, systems and registry for changes
- Critical OS and application files (files, directories, registry keys and values)
- Flexible, practical monitoring through includes/excludes
- Auditable reports

Log Inspection

- Collects & analyzes operating system and application logs for security events.
- Rules optimize the identification of important security events buried in multiple log entries.

TREND MICRO

Deep Security 7 Overview



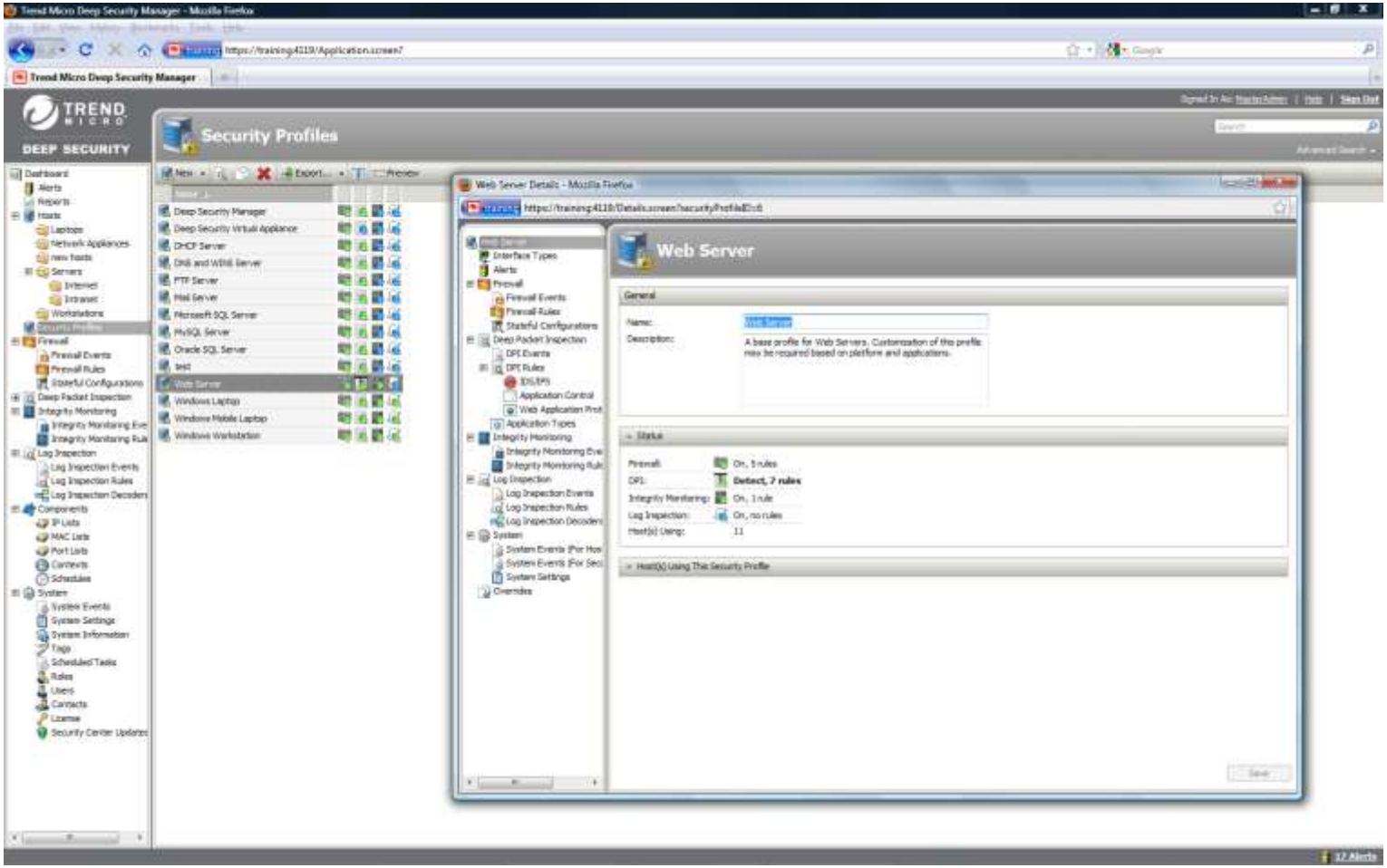
Deep Security Manager

- Centralised, web-based management system
- Manage security profiles
  - Multiple & delegated admin
  - Detailed reporting
  - Recommendation scan
  - Customisable dashboard
  - Automation through scheduled tasks
  - Web services API
  - Software and security updates
  - Integration (VMware vCenter, SIEM, Active Directory)
  - Scalable infrastructure (multiple nodes)

Deep Security Manager Dashboard

TREND MICRO

Security Profile



TREND MICRO

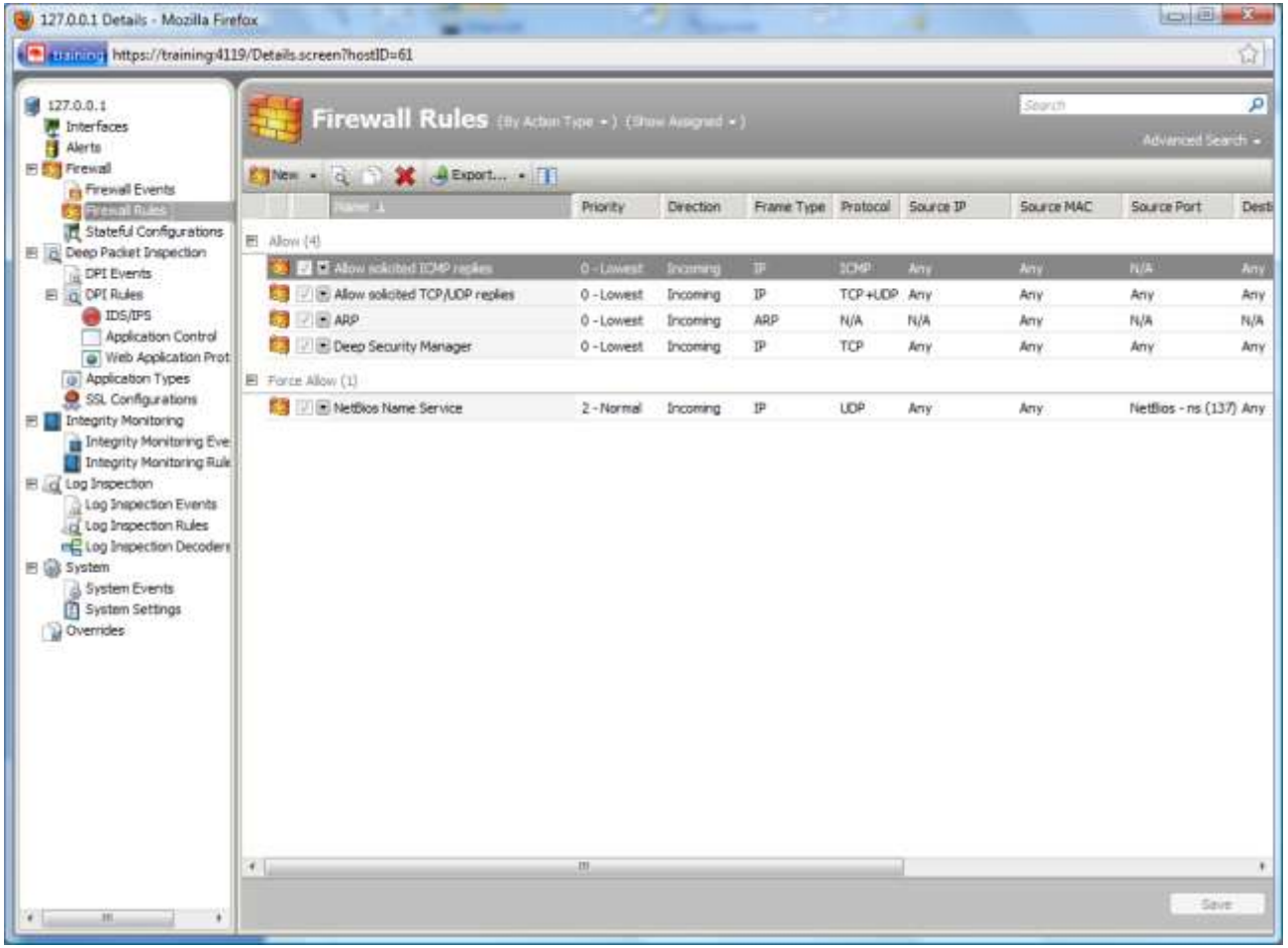
Firewall

Decreases the attack surface of physical and virtual servers

- Centralised management of server firewall policy
- Pre-defined templates for common enterprise server types
- Virtual machine isolation
- Fine-grained filtering
  - IP & MAC addresses, Ports
- Coverage of all IP-based protocols
  - TCP, UDP, ICMP, …
- Coverage of all frame types (IP, ARP, …)
- Prevents Denial of Service (DoS) attacks
- Design policies per network interface
- Detection of reconnaissance scans

TREND MICRO

Firewall



TREND MICRO

Deep Packet Inspection

IDS/IPS

- **Vulnerability rules**: shield known vulnerabilities from unknown attacks
- **Exploit rules**: stop known attacks
- **Smart rules**: Zero-day protection from unknown exploits against an unknown vulnerability
- Microsoft Tuesday protection is delivered in synch with public vulnerability announcements.
- On the host/server (HIPS)

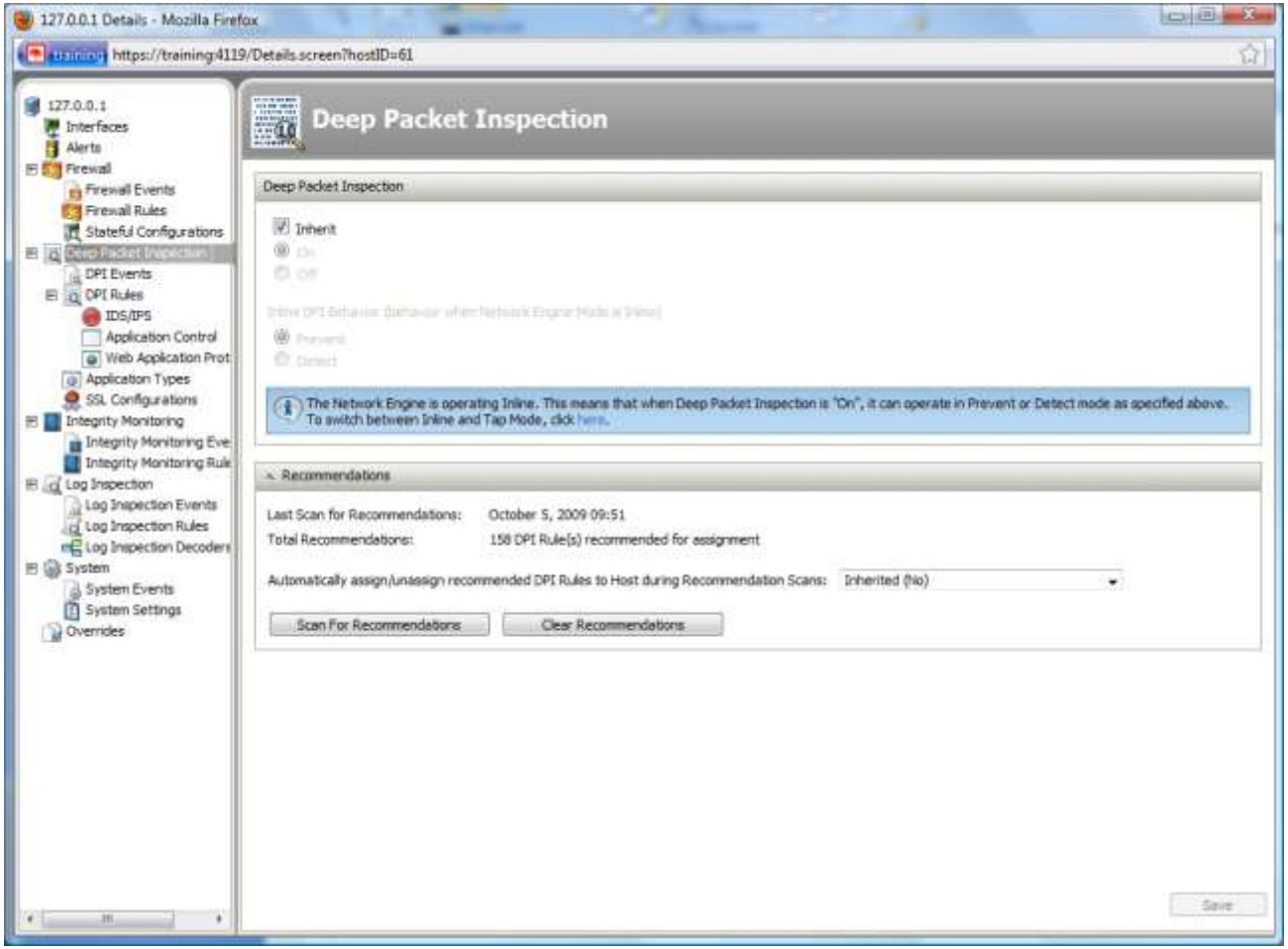
Web Application Protection

- Enables compliance with PCI DSS 6.6
- Shield vulnerabilities in custom web applications, until code fixes can be completed
- Shield legacy applications that cannot be fixed
- Prevent SQL injection, cross-site scripting (XSS)

Application Control

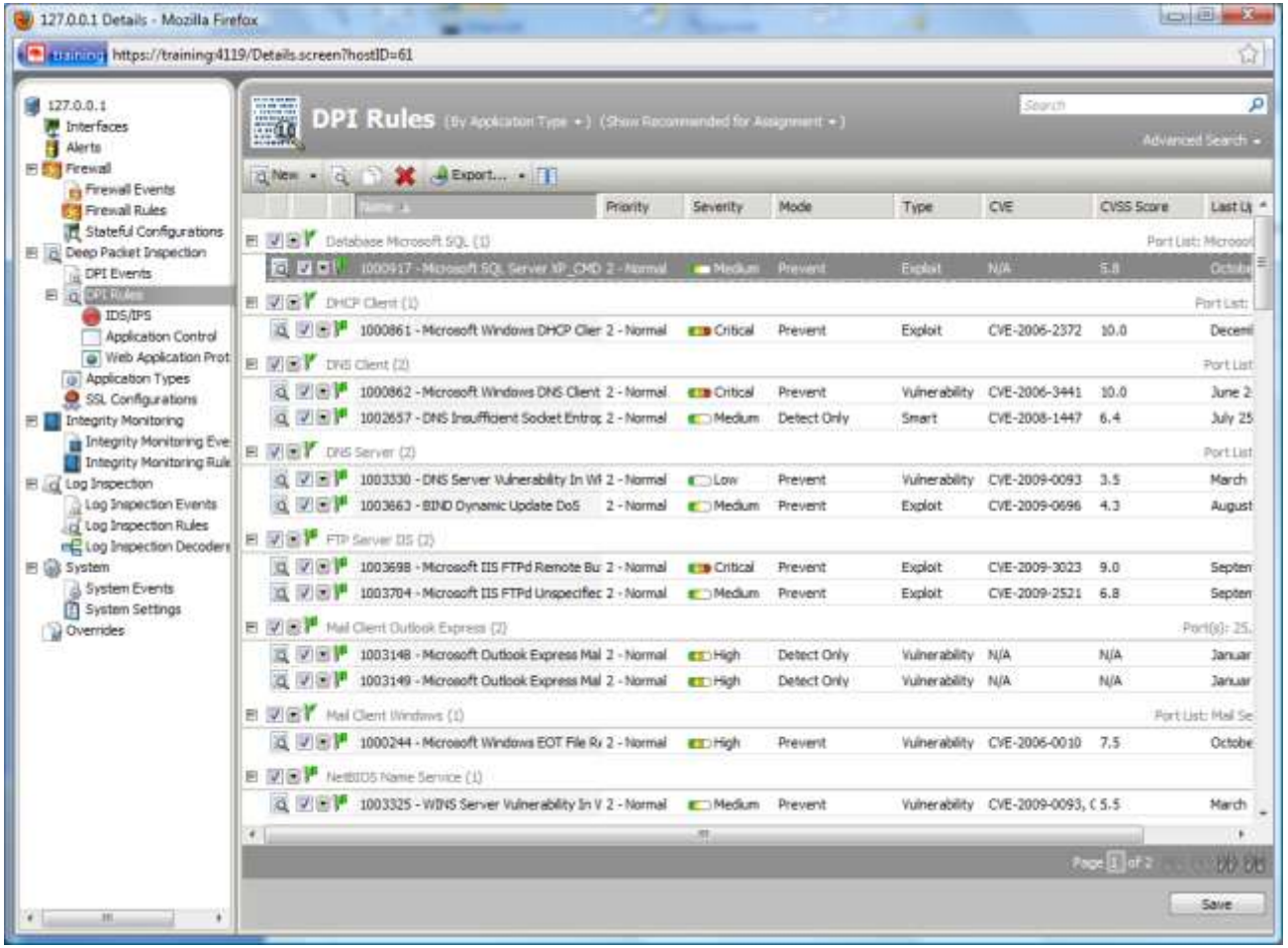
- Detect suspicious inbound/outbound traffic such as allowed protocols over non-standard ports
- Restrict which applications are allowed network access
- Detect and block malicious software from network access

Recommendation Scan



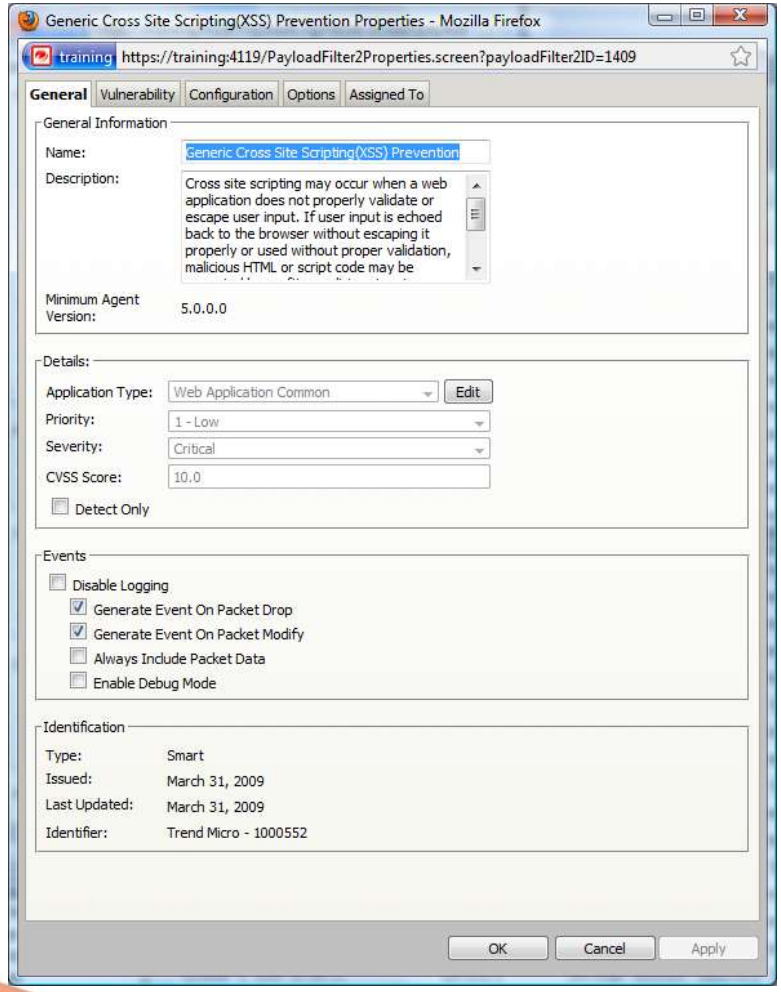
TREND MICRO

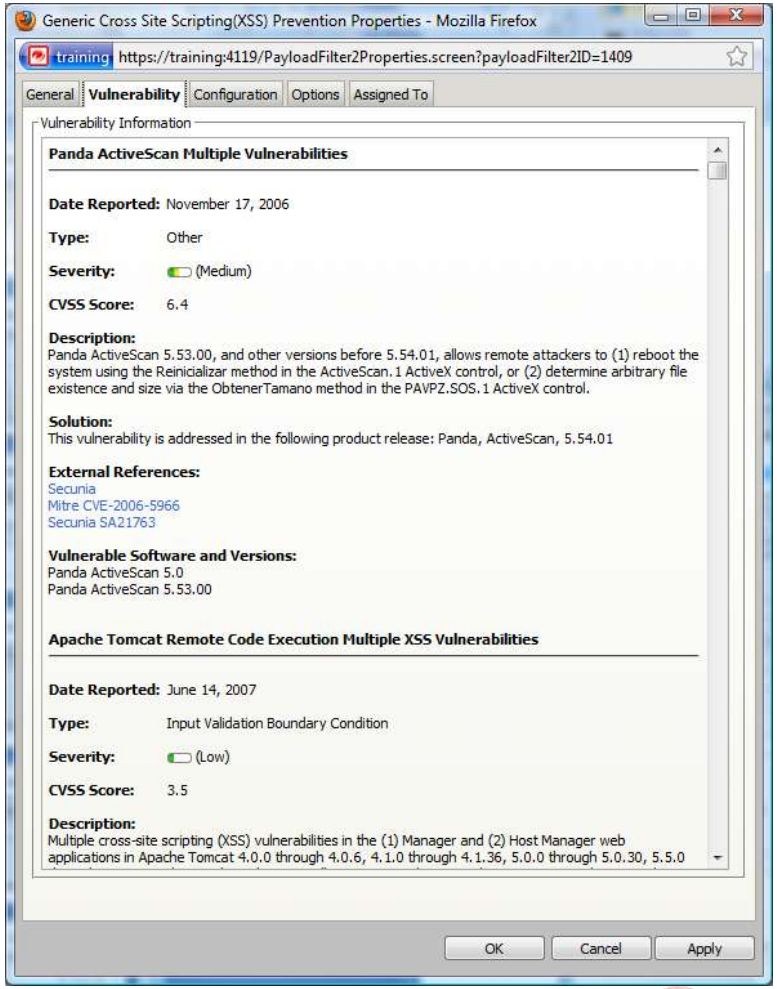
Recommendation Scan



TREND MICRO

DPI Detail





TREND MICRO

Integrity Monitoring

Monitors files, systems and registry for changes

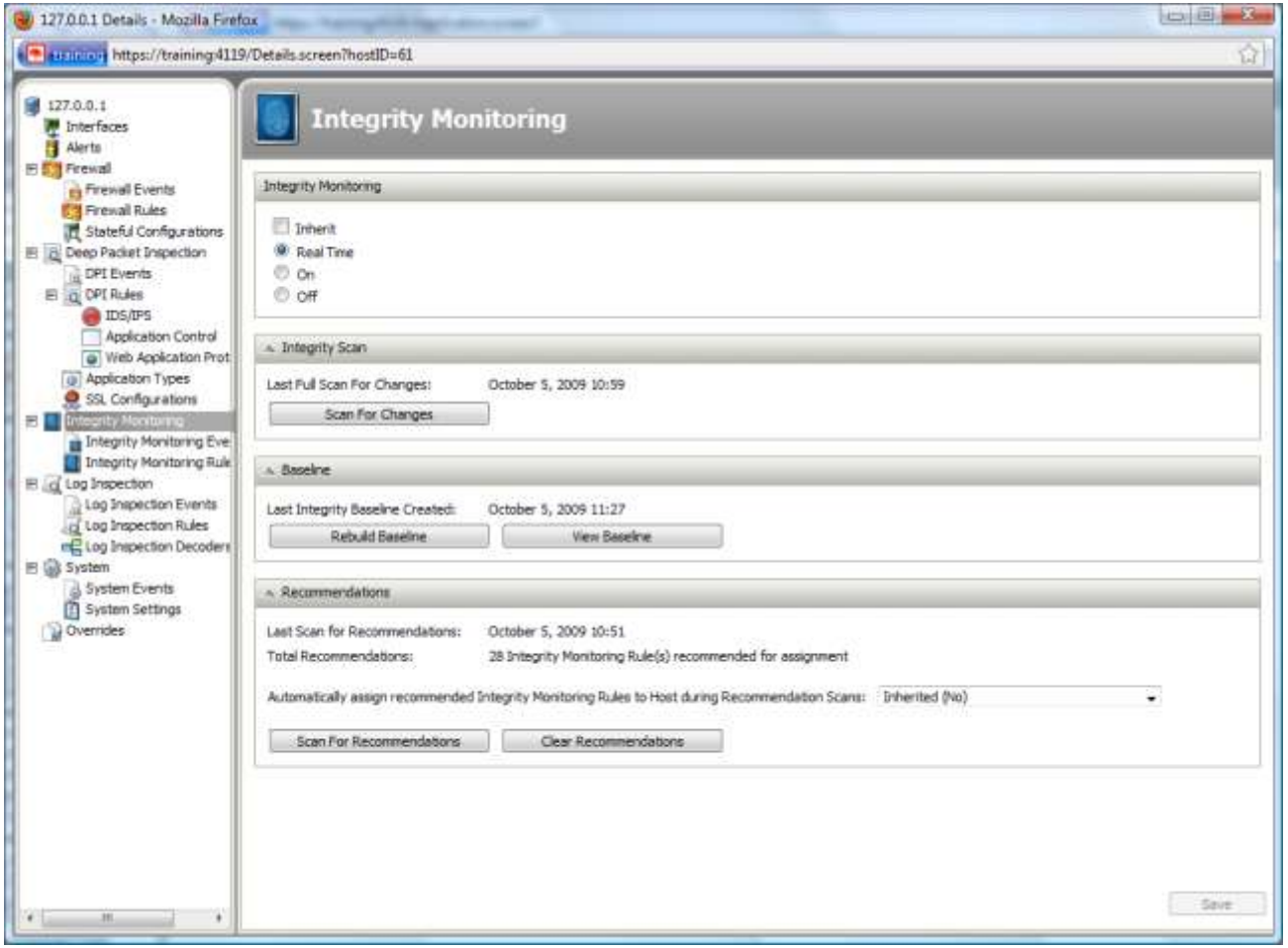
- Critical OS and application files (files, directories, registry keys and values, etc.)
- On-demand or scheduled detection
- Extensive file property checking, including attributes (PCI 10.5.5)
- Monitor specific directories
- Flexible, practical monitoring through includes/excludes
- Auditable reports

Useful for:

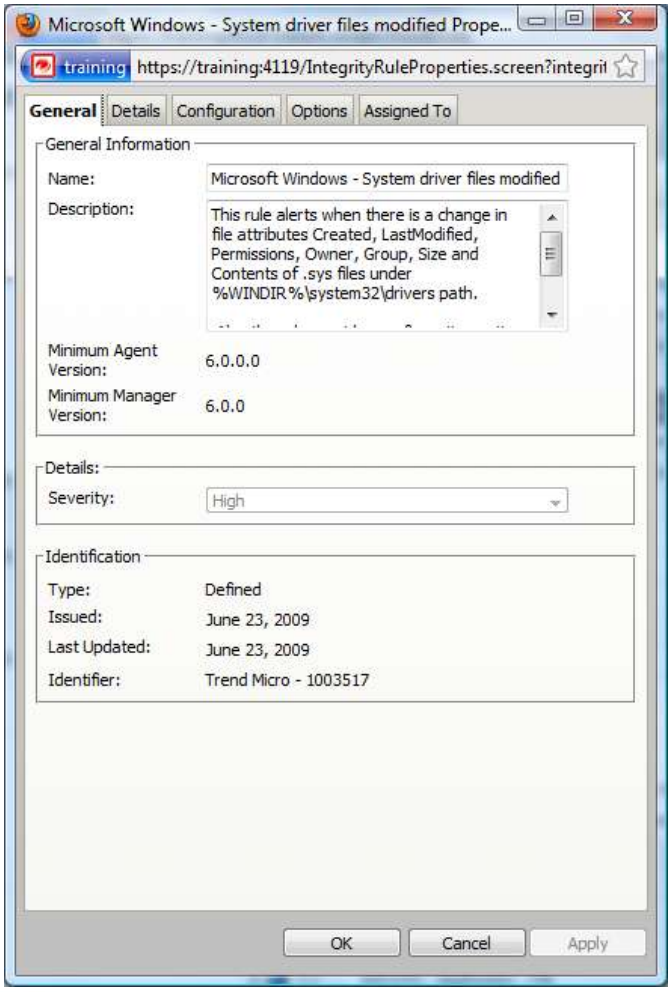
  - Meeting PCI compliance
  - Alerting on errors that could signal an attack
  - Alerting on critical system changes

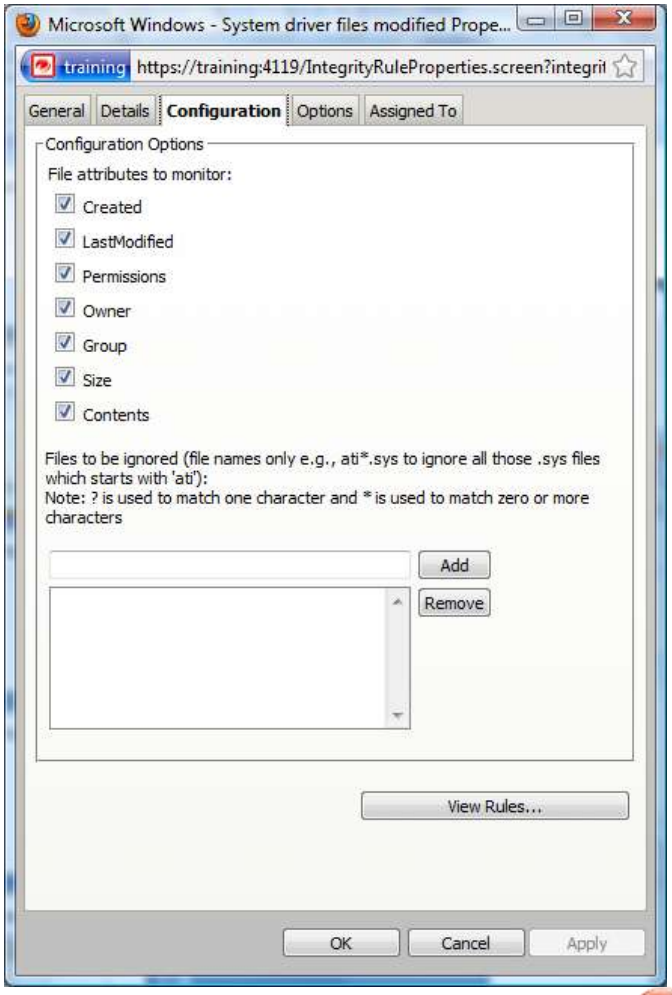
TREND MICRO

Integrity Monitoring



Integrity Monitoring Configuration





TREND MICRO

Log Inspection

Getting visibility into important security events buried in log files

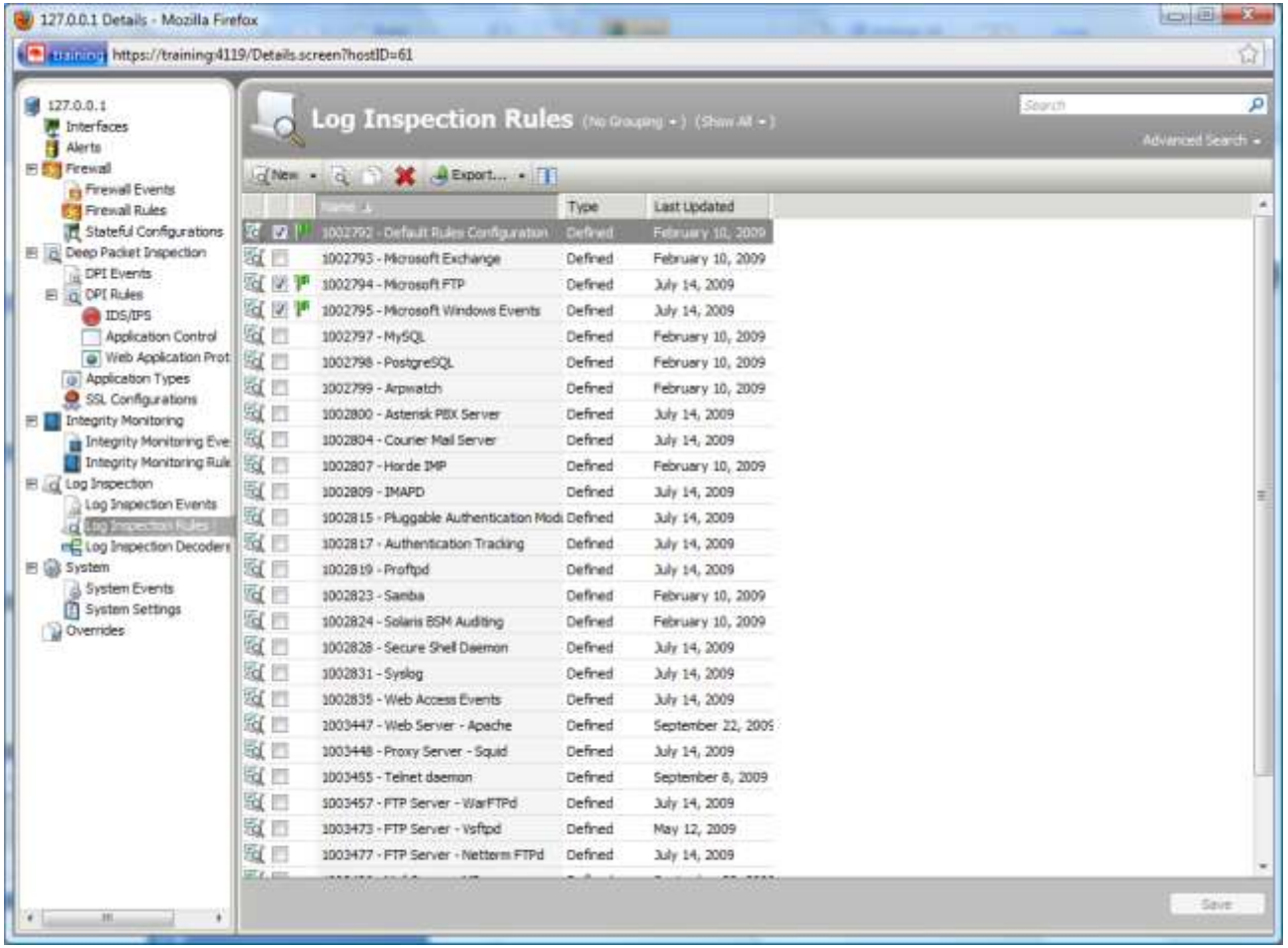
- Collects & analyses operating system and application logs for security events.
- Rules optimise the identification of important security events buried in multiple log entries.
- Events are forwarded to a SIEM or centralized logging server for correlation, reporting and archiving.

Useful for:

- Suspicious behaviour detection
- Collection of security-related administrative actions
- Optimised collection of security events across your datacenter
- Advanced rule creation using OSSEC rule syntax

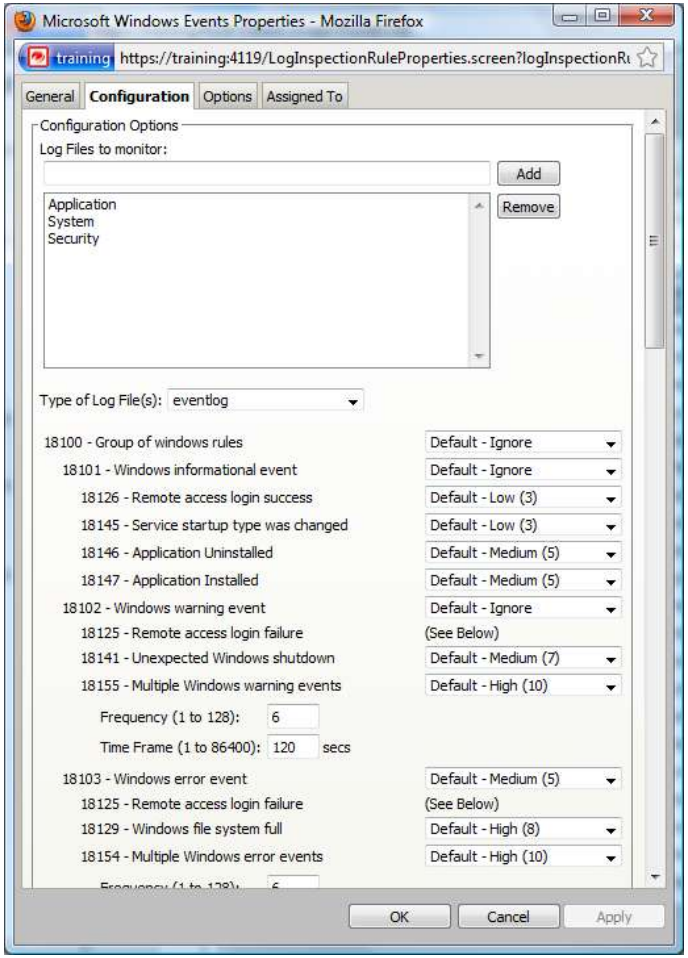
TREND MICRO

Log Inspection



TREND MICRO

Log Inspection Configuration



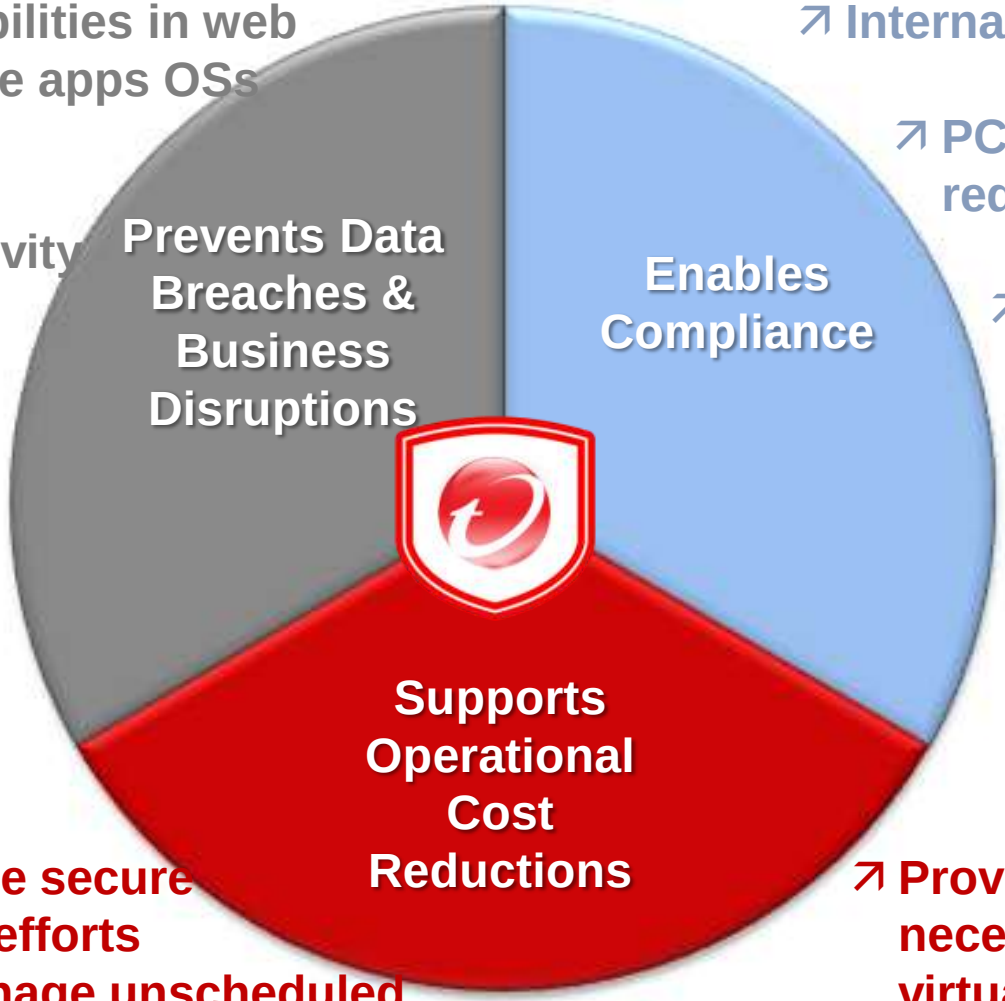
TREND MICRO

Deep Security for Virtualisation

Category	Requirement
NW Segmentation & VM Zoning	– Isolation of virtual machines on shared servers – Independent of vSwitches and network architecture – Stateful firewall, groupings, security policy enforcement
Virtualisation Security Mgmt	– Automation via web services API, template deployment – VMsafe coordinated approach – Visibility into virtual and physical servers, server state
Integrity Monitoring & Log	– Monitor critical system, application, log files for changes – Forward system and application log events via Syslog to centralized logging servers or SIEMS
IDS / IPS & Virtual Patching	– InterVM attack prevention – Protection against known & zero-day attacks – Shield until patching: <30 day patching required – Shield systems that can't be patched – Suspicious behavior detection – Detailed audit logs & SIEM integration
Web Application Protection	– Protection against Web-based attacks such as SQL Injection, Cross-Site Scripting, and many more – Deployed where WAF cannot reach

Deep Security: Key benefits

- Shield vulnerabilities in web apps, enterprise apps OSs
- Detect & block suspicious activity



- Internal policies
- PCI & other requirements
- Detailed reports document prevented attacks & compliance status

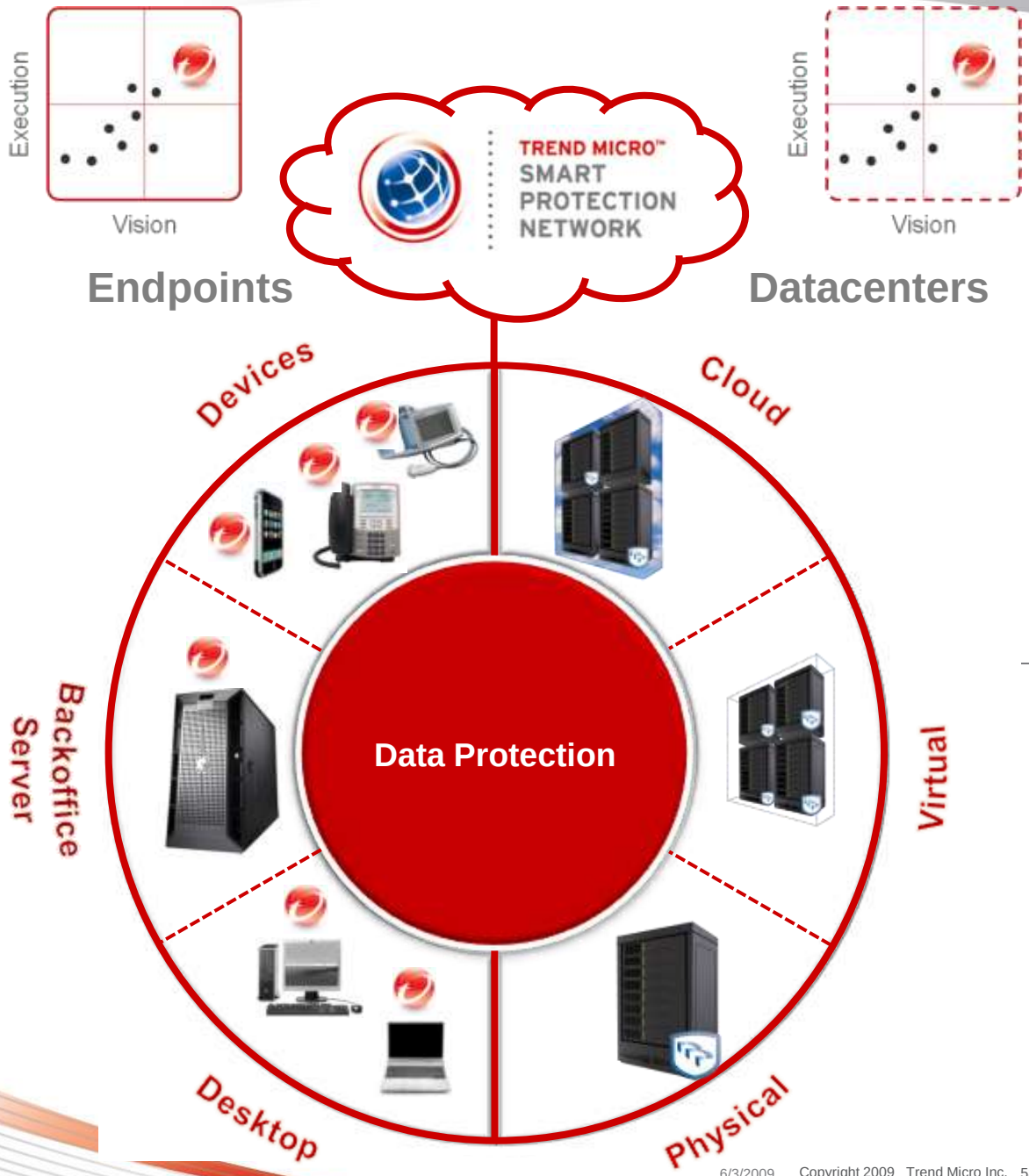
- Prioritize secure coding efforts
- Manage unscheduled patching
- Provides security necessary to realise virtualisation savings
- Increased value from SIEM investments

TREND MICRO

Evolution of Server & Application Protection Systems

Past	Today
Perimeter security	Security at the server / VM
Appliance-based	Software-based
Threat protection: Basic, external attacks	Threat protection: Basic to sophisticated internal & external attacks
Firewall IDS/IPS Vulnerability Scan	Firewall IDS/IPS Vulnerability Scan Web Application Protection File Integrity Monitoring Log Inspection Configuration Assessment
Weak / limited integration	Enterprise Integration: Virtualisation Management platform (vCenter), SIEM.

TREND MICRO



Vision

Every network-connected host must be able to defend itself from attacks.

TREND MICRO

THANK YOU!

TREND MICRO