TREND MICRO

Stallion

Securing Your Web World

Security for Virtual Server Environments

Trend Micro Core Protection for Virtual Machines
Trend Micro Deep Security

Veli-Pekka Kusmin
Pre-Sales Engineer

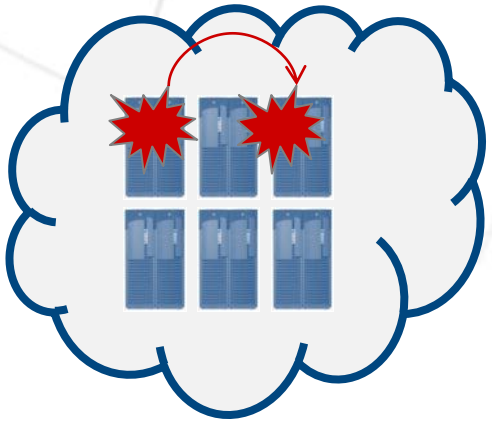
Trend Micro Channel Confidential
June 2010

Security challenges in Virtual Environment

- Datacenter trends
- Securing VMs
  - Traditional approach
  - Problems

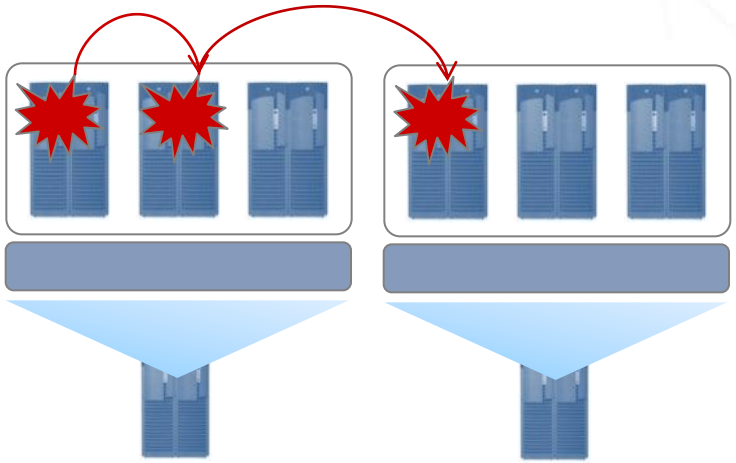
Trends in the Datacenter

Cloud



Servers in the open

Virtualized

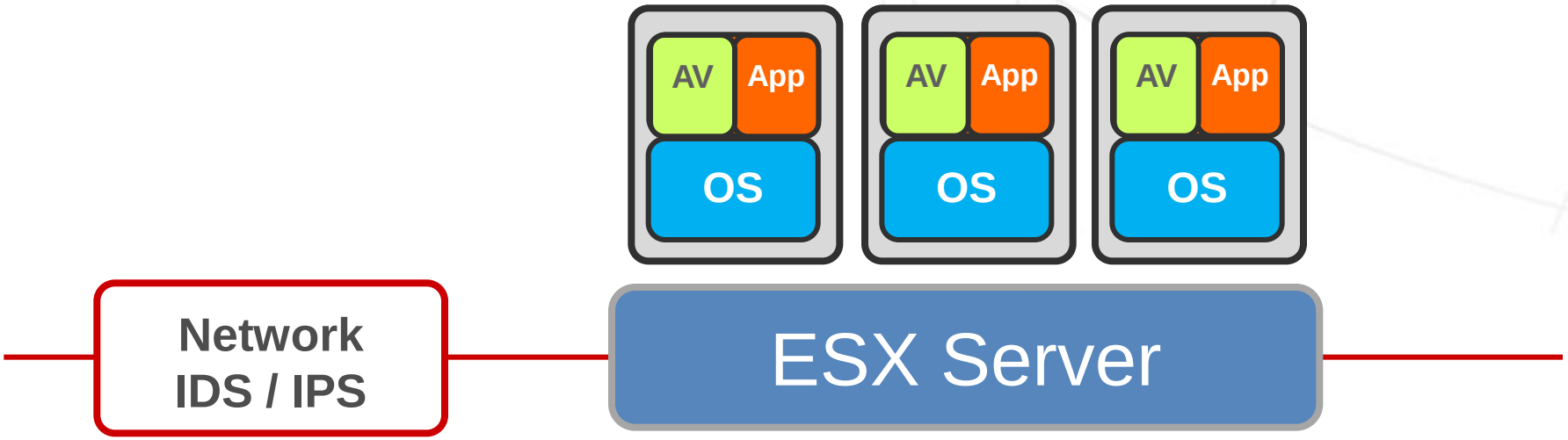


Servers virtual and in motion

Physical

Servers under pressure

Securing Virtual Servers the Traditional Way



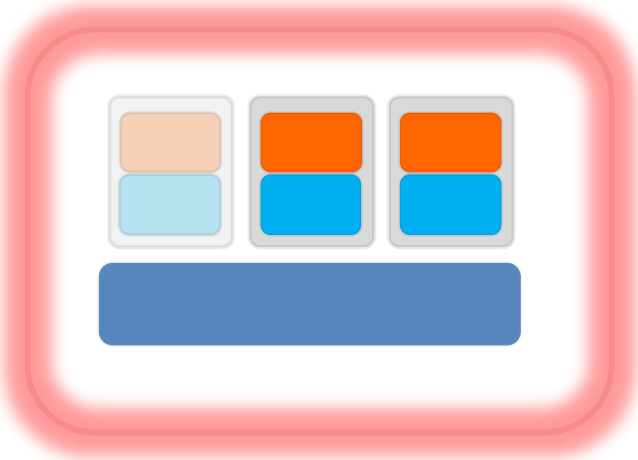
- **Anti-virus:** Local, agent-based protection in the VM
- **IDS / IPS:** Network-based device or software solution

Virtual Machines Need Specialized Protection

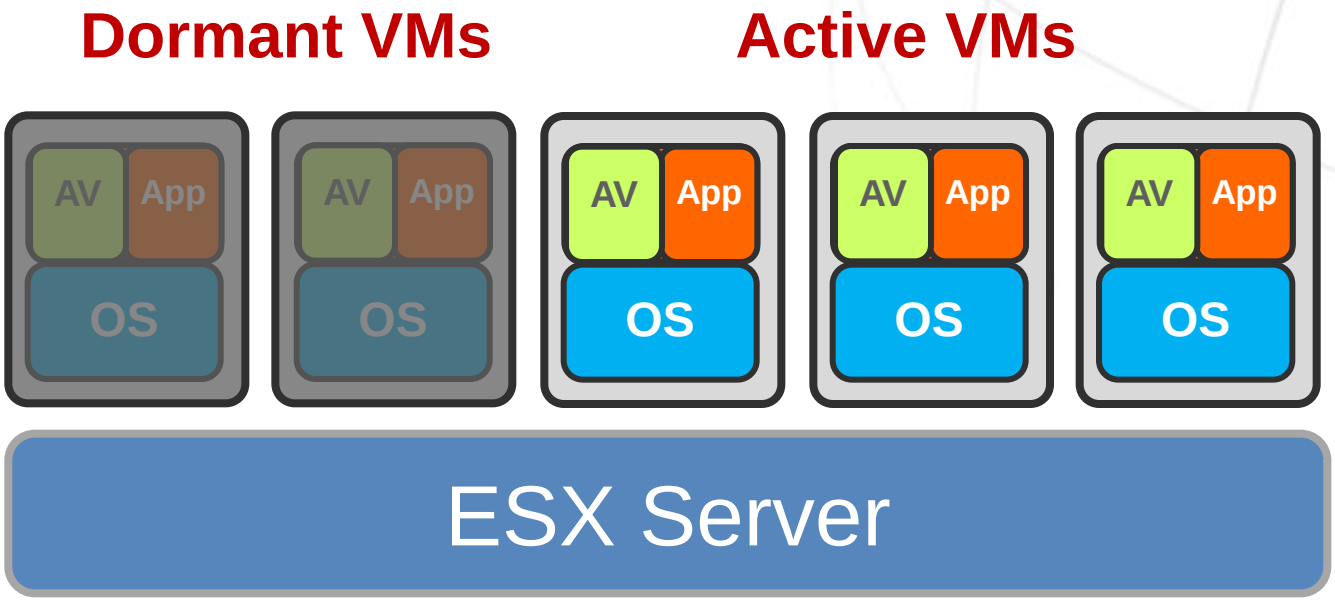
Same threats in virtualized servers as physical.

+ New challenges:

1. Dormant VMs →
2. Resource contention →
3. VM Sprawl →
4. Inter-VM traffic →
5. vMotion →



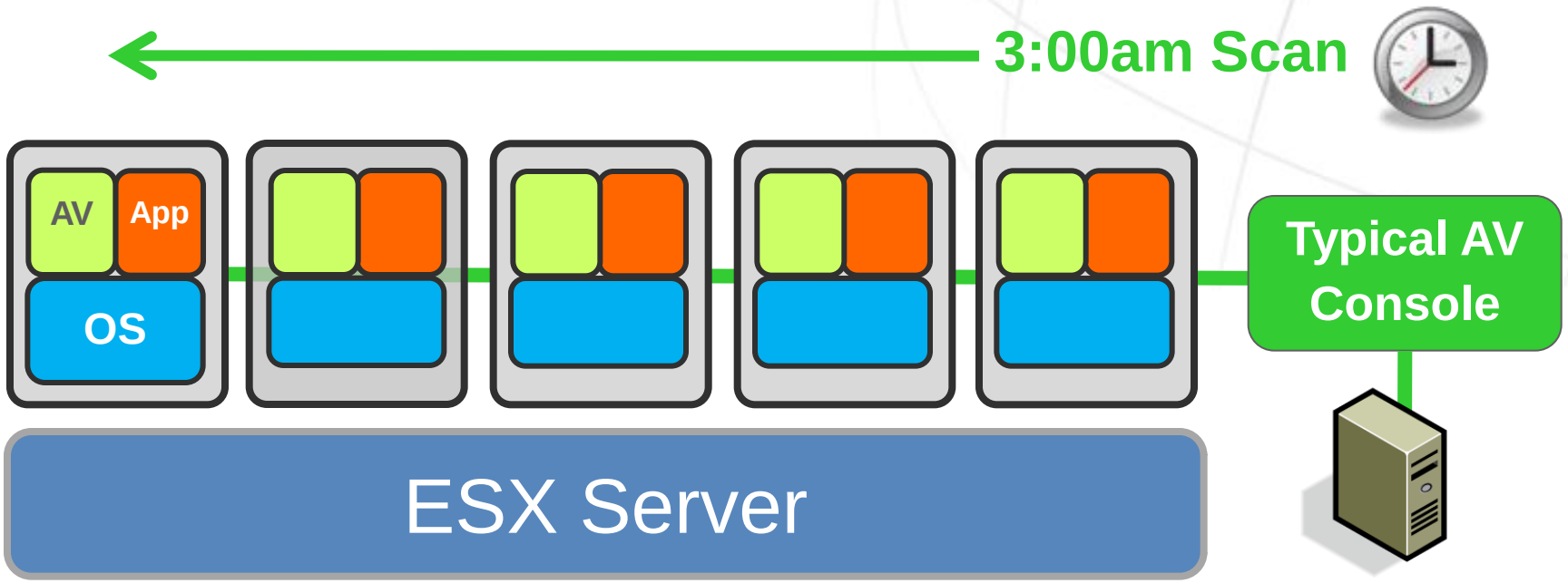
Problem 1:
Dormant VMs are unprotected



Dormant VMs includes VM templates and backups:

- Cannot run scan agents yet still can get infected
- Stale AV signatures

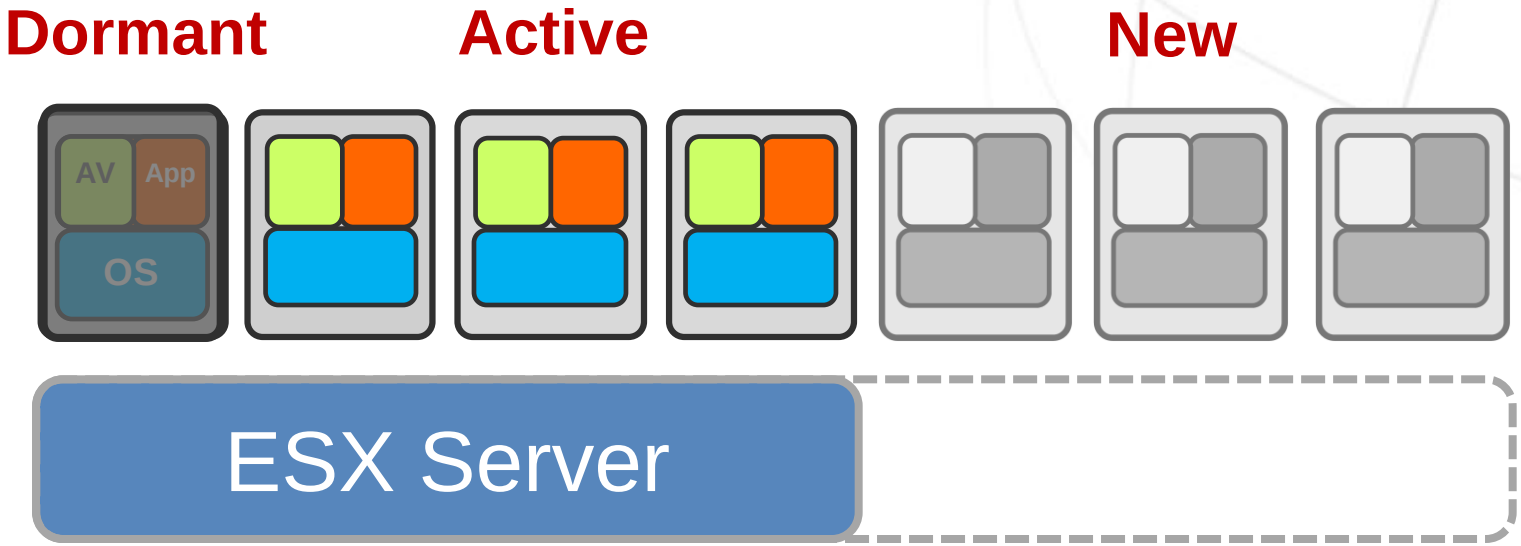
Problem 2:
Full System Scans



Resource Contention with Full System Scans

- Existing AV solutions are not VM aware
- Simultaneous full AV scans on same host causes severe performance degradation
- No isolation between malware and anti-malware

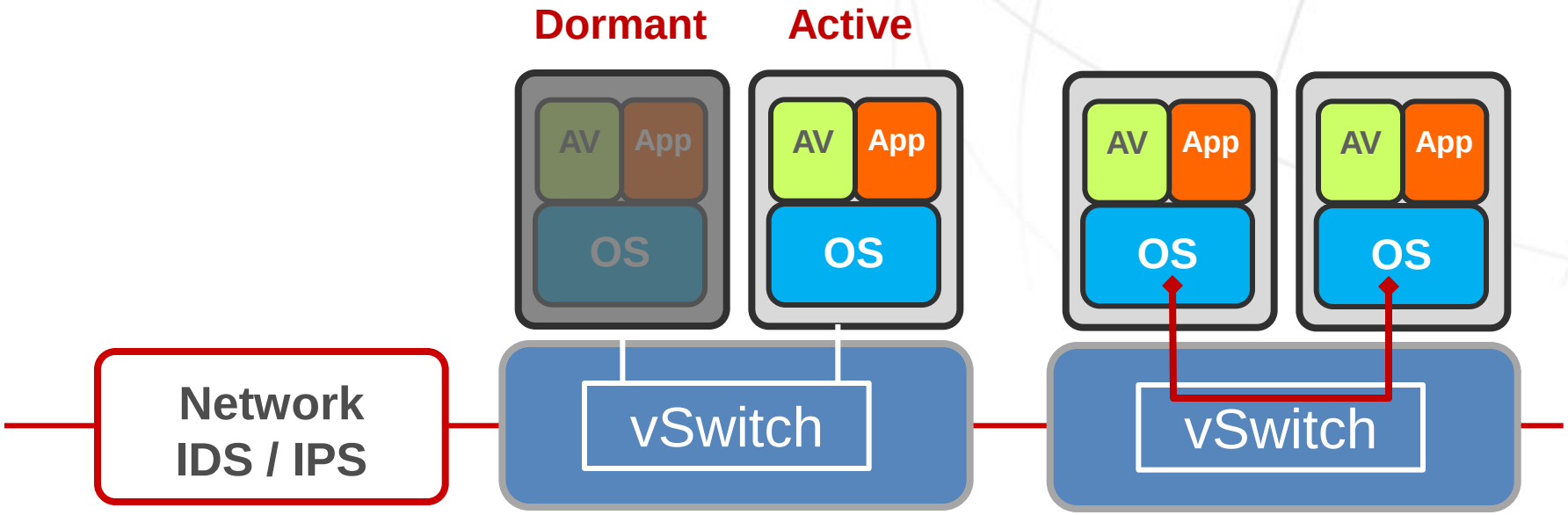
Problem 3:
VM Sprawl



Managing VM Sprawl

- Security weaknesses replicate quickly
- Security provisioning creates bottlenecks
- Lack of visibility into, or integration with, virtualization console increases management complexity

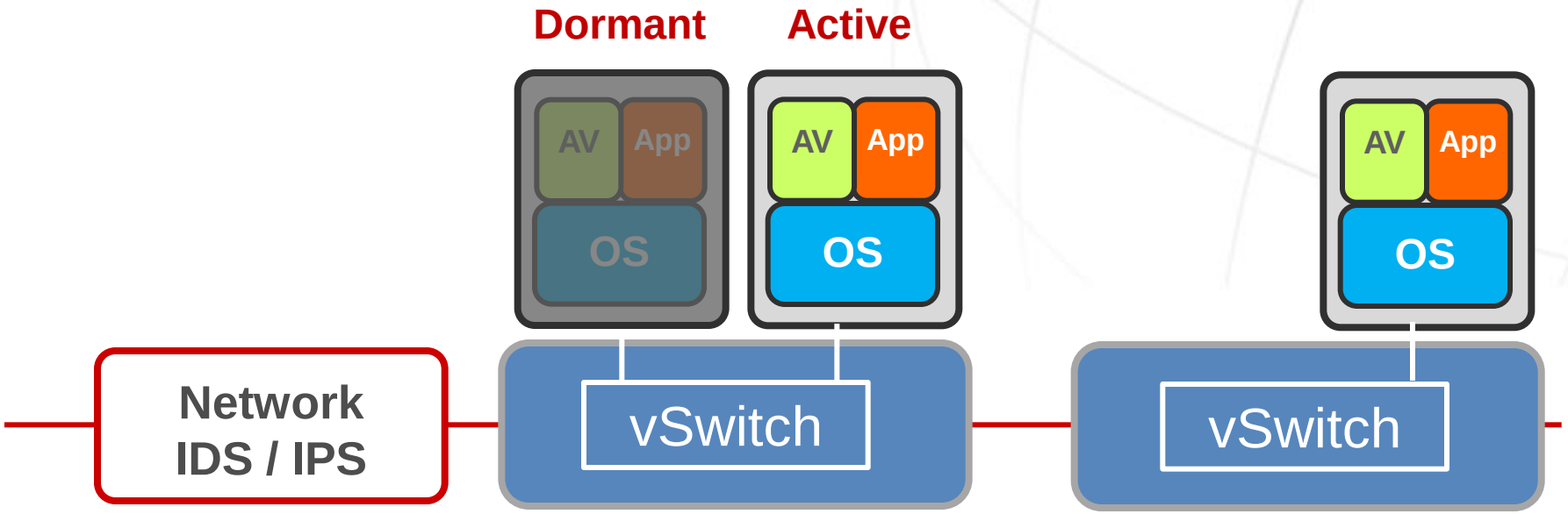
Problem 4:
Inter-VM Traffic



Inter-VM traffic

- NIDS / NIPS blind to intra-VM traffic
- First-generation security VMs require intrusive vSwitch changes

Problem 5:
VM Mobility



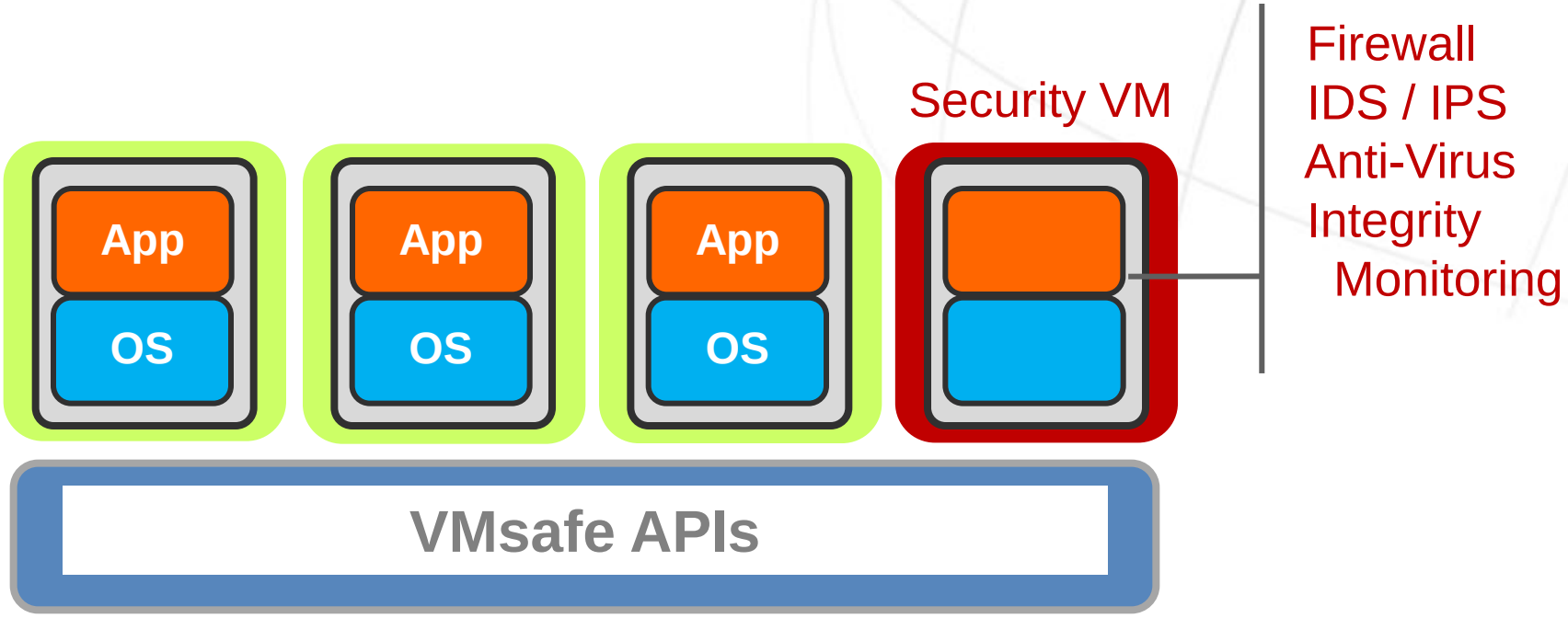
vMotion & vCloud:

- Reconfiguration required: cumbersome
- VMs of different sensitivities on same server
- VMs in public clouds (IaaS) are unprotected

The Solution

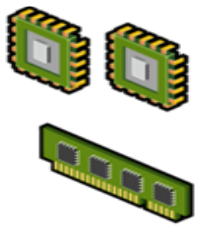
- VMware VMsafe
- The Trend Micro approach

Introducing VMsafe



- 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.

VMsafe™ APIs



CPU/Memory Inspection

- Inspection of specific memory pages
- Knowledge of the CPU state
- Policy enforcement through resource allocation

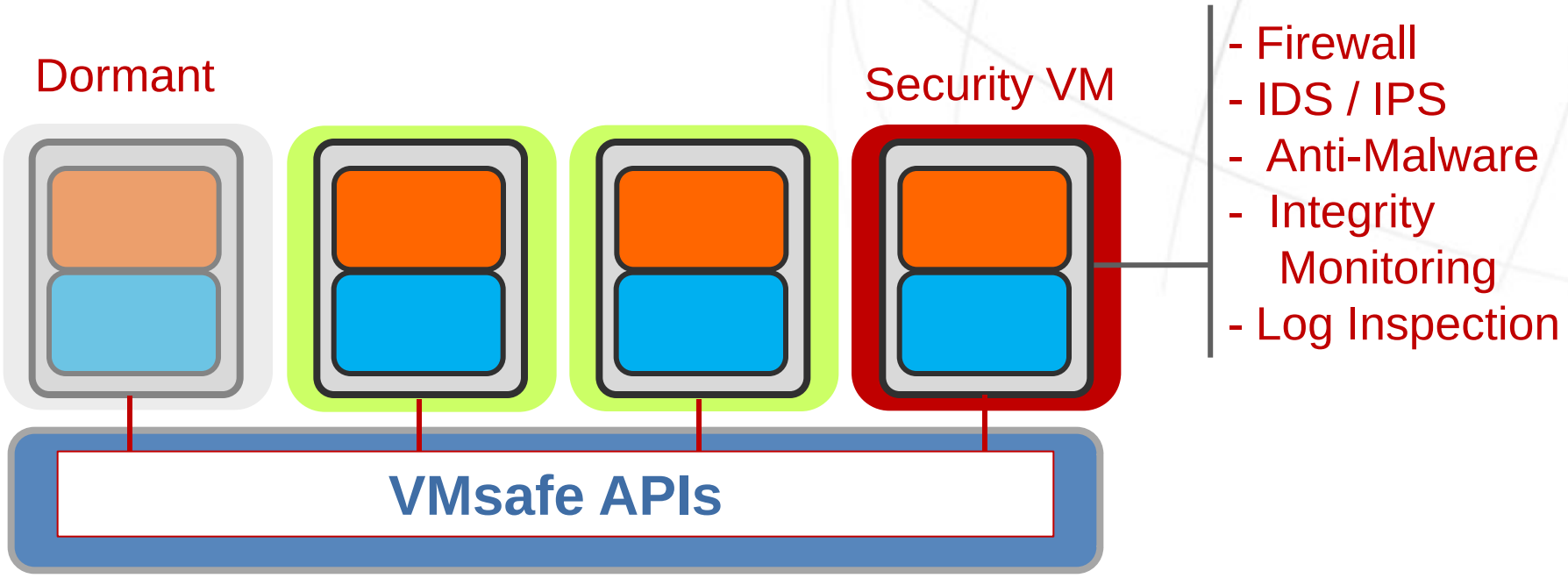
Networking

- View all IO traffic on the host
- Intercept, view, modify and replicate IO traffic
- Provide inline or passive protection

Storage

- Mount and read virtual disks (VMDK)
- Inspect IO read/writes to the storage devices
- Transparent to device & inline with ESX Storage stack

The Trend Micro Approach



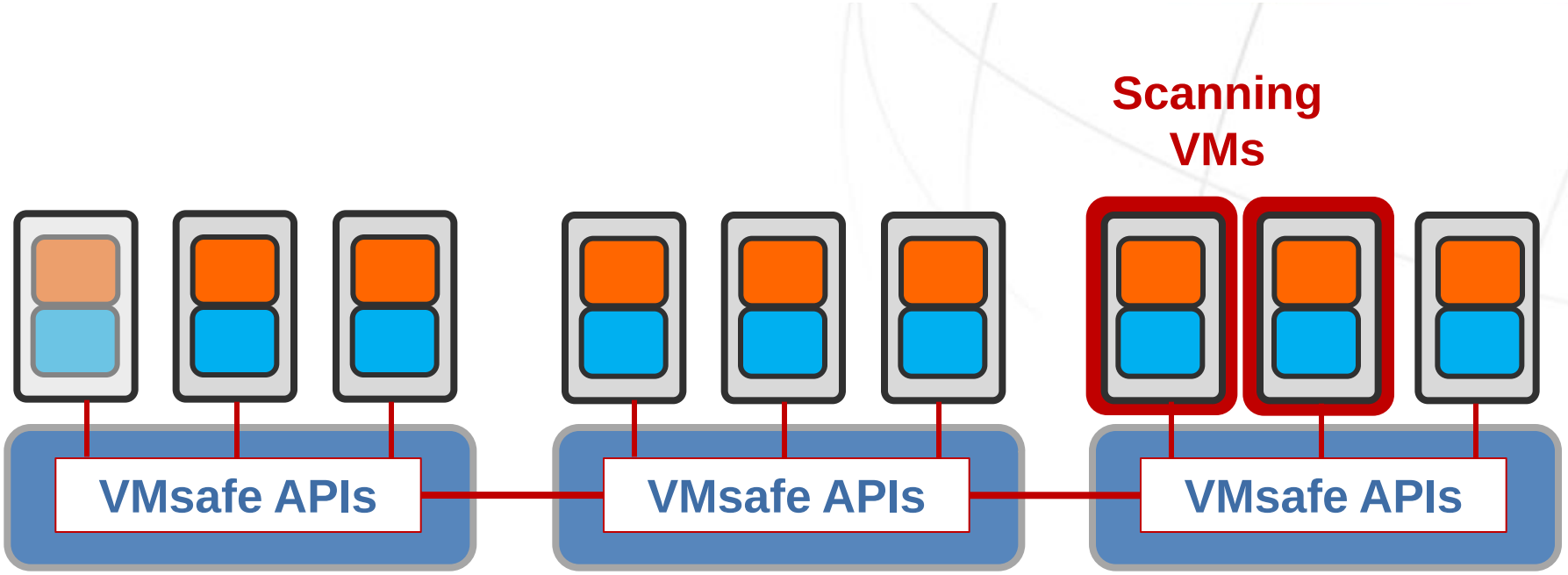
Comprehensive, coordinated protection for <u>all</u> VMs

- Local, agent-based protection in the VM
- Security VM that secures VMs from the outside
- Multiple protection capabilities
- Integrates with VMware vCenter and VMsafe

The Solution 1

- Trend Micro Core Protection for Virtual Machines

Anti-Malware Scanning VM - TM Core Protection for VMs



- Anti-malware scanning for target VMs from outside
- Integrates VMsafe VDDK APIs to mount VM disk files
- Full scans of dormant & active VMs from scanning VM
- Immunizes the protection agent from disruptive activities

Trend Micro Core Protection for Virtual Machines

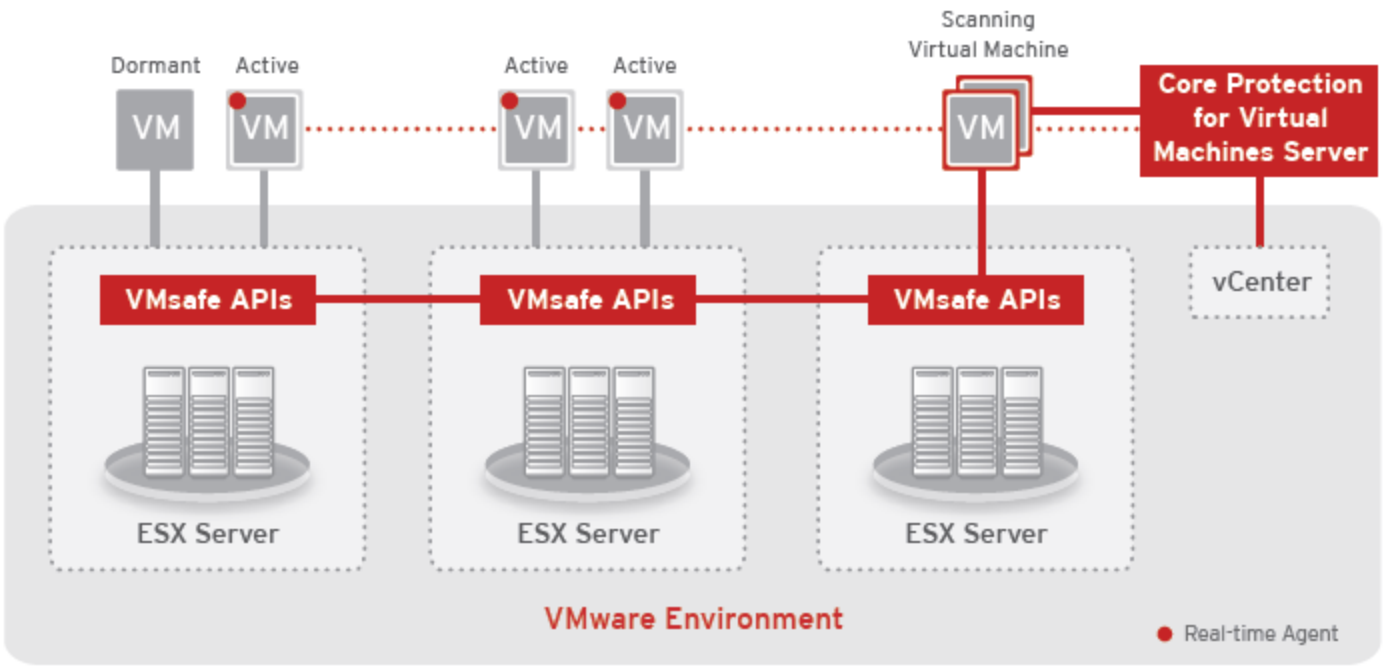
More Protection

- First virtualization-aware anti-malware product in the market
- Secures dormant and active VMs efficiently
- New VMs auto-scanned on creation and auto-assigned to a scanning VM
- Supports VI3 and vSphere 4 (needs vCenter)

Less Complexity

- Flexible Management: Through standalone web console, as a plugin to Trend Micro OfficeScan or through VMware vCenter
- Flexible Configuration: Can be configured with multiple scanning VMs on any ESX/ESXi (or physical) server
- Flexible Deployment: CPVM can be setup to co-exist with OSCE or competitive products if necessary (not ideal*)

Core Protection for Virtual Machines



CPVM System Requirements

SYSTEM REQUIREMENTS	
Server	
Operating system	Microsoft™ Windows™ Server 2003 or 2003 R2 32-bit Enterprise Edition with Service Pack 1 or 2
Hardware	800MHz processor, 512MB RAM, 1GB disk space, Network Interface Card (NIC)
Web server	Microsoft Internet Information Server (IIS) on Windows Server 2003: version 6.0
Web console	300MHz processor, 128MB RAM, 30MB disk space, Microsoft Internet Explorer™ 6.0 or Microsoft Internet Explorer™ 7.0
Scanning Agent	
Operating system	Microsoft Windows XP Professional 32-bit Edition, Microsoft Windows Server 2003 or 2003 R2 32-bit Enterprise Edition
Hardware	300MHz processor, 256MB RAM (512MB for Update Agents), 200MB disk space (700MB for Update Agents), Network Interface Card (NIC)
Real-Time Agent	
Operating system	Microsoft Windows 2000 Server, Windows XP Professional 32-bit, Windows Server 2003 (or 2003 R2) 32-bit, Microsoft Windows Server 2003 (or 2003 R2) 64-bit , Windows Server 2008, Windows Vista Enterprise 32-bit, Windows Vista Business 64-bit
Virtual Machine Properties	1 CPU, 128MB RAM, 200MB disk space, Network Interface Card (NIC) VMware
Platform Support	
VMware	VMware VI3 (ESX 3.5, ESXi, vCenter 2.5), vSphere 4.0

Note: VMware vCenter is required in order for Core Protection for Virtual Machines to work.

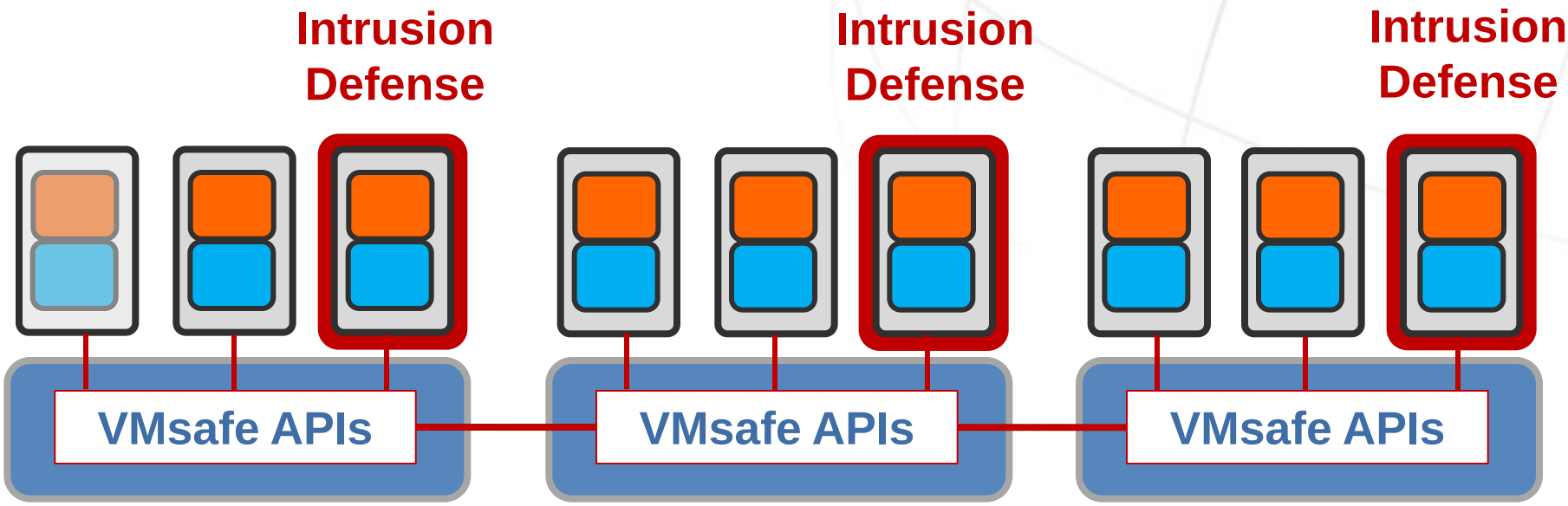
Core Protection for Virtual Machines

- While server virtualization increases efficiency in the data center, it also challenges the security of the IT environment. Traditional security imported from the physical world cannot fully protect virtual environments which are particularly vulnerable when virtual machines are dormant or offline as they are unable to protect themselves with a virus scan agent and signature updates. Also, resource-intensive security operations such as scheduled full system scans can significantly degrade the performance of the host and render the security ineffective, especially when initiated concurrently on multiple virtual machines. To fully realize the cost and productivity advantages of virtualization, enterprises need content security that is architected specifically to secure today's highly virtualized datacenter.
- Trend Micro™ Core Protection for Virtual Machines enables enterprises to maximize the economic benefits of virtualization without compromising the security of their datacenter. Specifically designed for VMware ESX/ESXi environments, this virtualization-aware solution leverages the VMsafe APIs from VMware to secure both active and dormant virtual machines. Layered protection uses dedicated scanning virtual machines coordinated with real-time agents within each virtual machine.

The Solution 2

- Trend Micro Deep Security

Intrusion Defense VM - TM Deep Security



- Intrusion Defense provides IDS/IPS & firewall protection
- Integrates VMsafe-NET APIs (firewall & IDS/IPS)
- Enforces security policy
- Newly emerging VMs are automatically protected

Trend Micro 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, Virtual Patching

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.

Firewall

Decreases the attack surface of physical and virtual servers

- Centralized 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

Deep Packet Inspection

IDS/IPS

- **Vulnerability rules**: shield known vulnerabilities from unknown attacks (virtual patching)
- **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

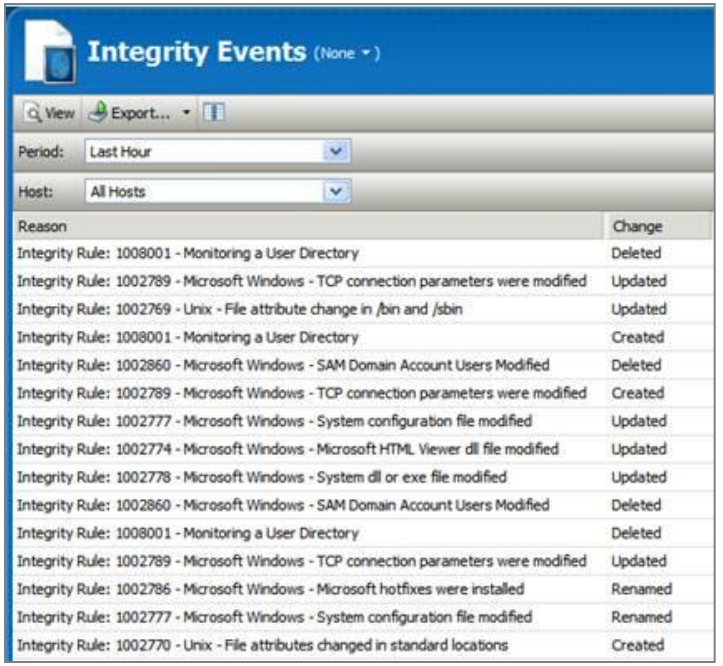
Integrity Monitoring

Monitors files, systems and registry for changes

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

Useful for:

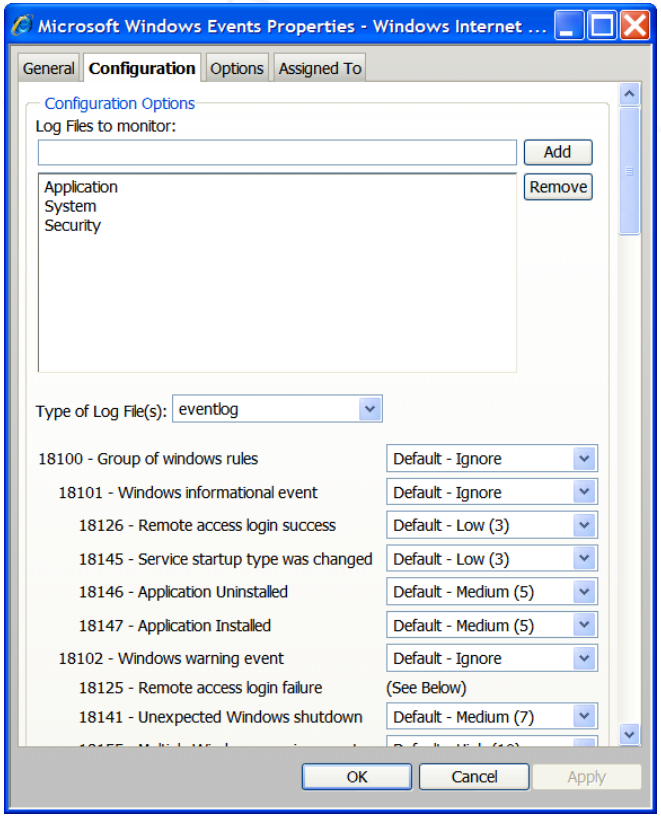
  - Meeting PCI compliance
  - Alerting on errors that could signal an attack
  - Alerting on critical system changes



Log Inspection

Getting visibility into important security events buried in log files

- Collects & analyzes operating system and application logs for security events
- Rules optimize 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



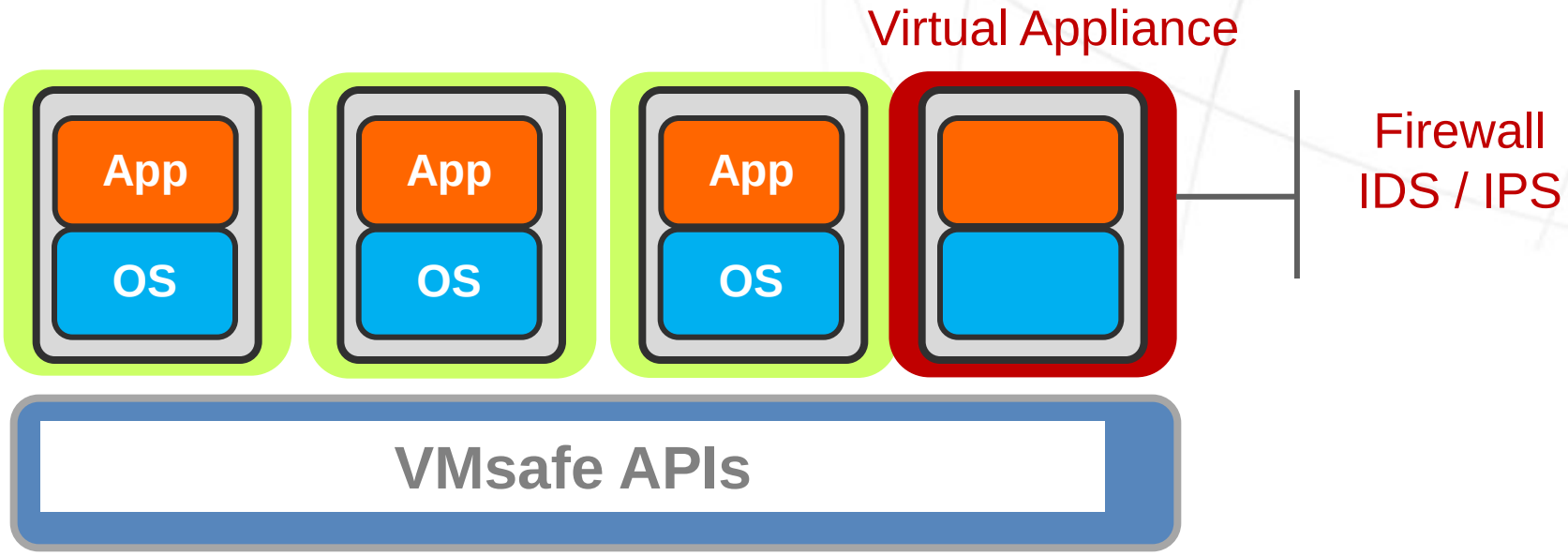
Useful for:

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

Deep Security: Platforms protected

Microsoft	• Windows 2000, Windows 7 • Windows XP, 2003 (32 & 64 bit) • Vista (32 & 64 bit) • Windows Server 2008 (32 & 64 bit) • HyperV (Guest VM)
solaris	• 8, 9, 10 on SPARC • 10 on x86 (64 bit) • Solaris 10 partitions
Linux	• Red Hat 3 • Red Hat 4, 5 (32 & 64 bit) • SuSE 9, 10
VIRTUALIZED BY vmware	• VMware ESX Server (Guest VM) • Virtual Center integration
CITRIX	• XenServer Guest VM
Integrity Monitoring & Log Inspection modules	• HP-UX 11i v2 • AIX 5.3

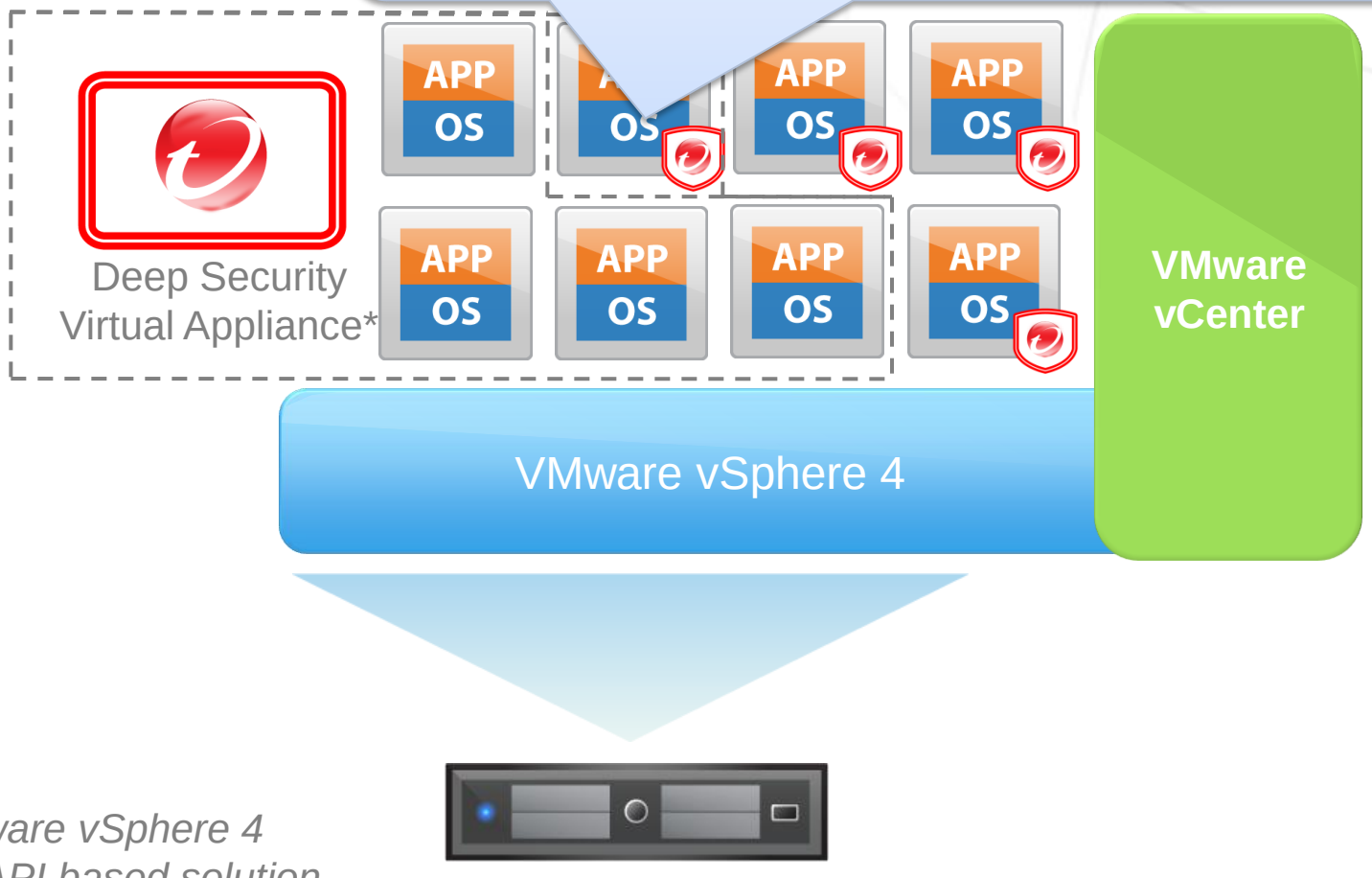
Deep Security 7.0 - Virtual Appliance (vSphere 4 VMsafe based)



- Protect the VM by inspection of virtual components
- Secures VMs from the outside, no changes required to VM
- Complete integration with, and awareness of, vMotion, Storage VMotion, HA, etc.
- Virtual Center integration for VM discovery & synchronization

Deep Security 7.0 Virtual Appliance

Coordinated Security Approach
- Agent Disappears (removed / reverted to previous snapshot)
- Virtual Appliance auto-protects VM

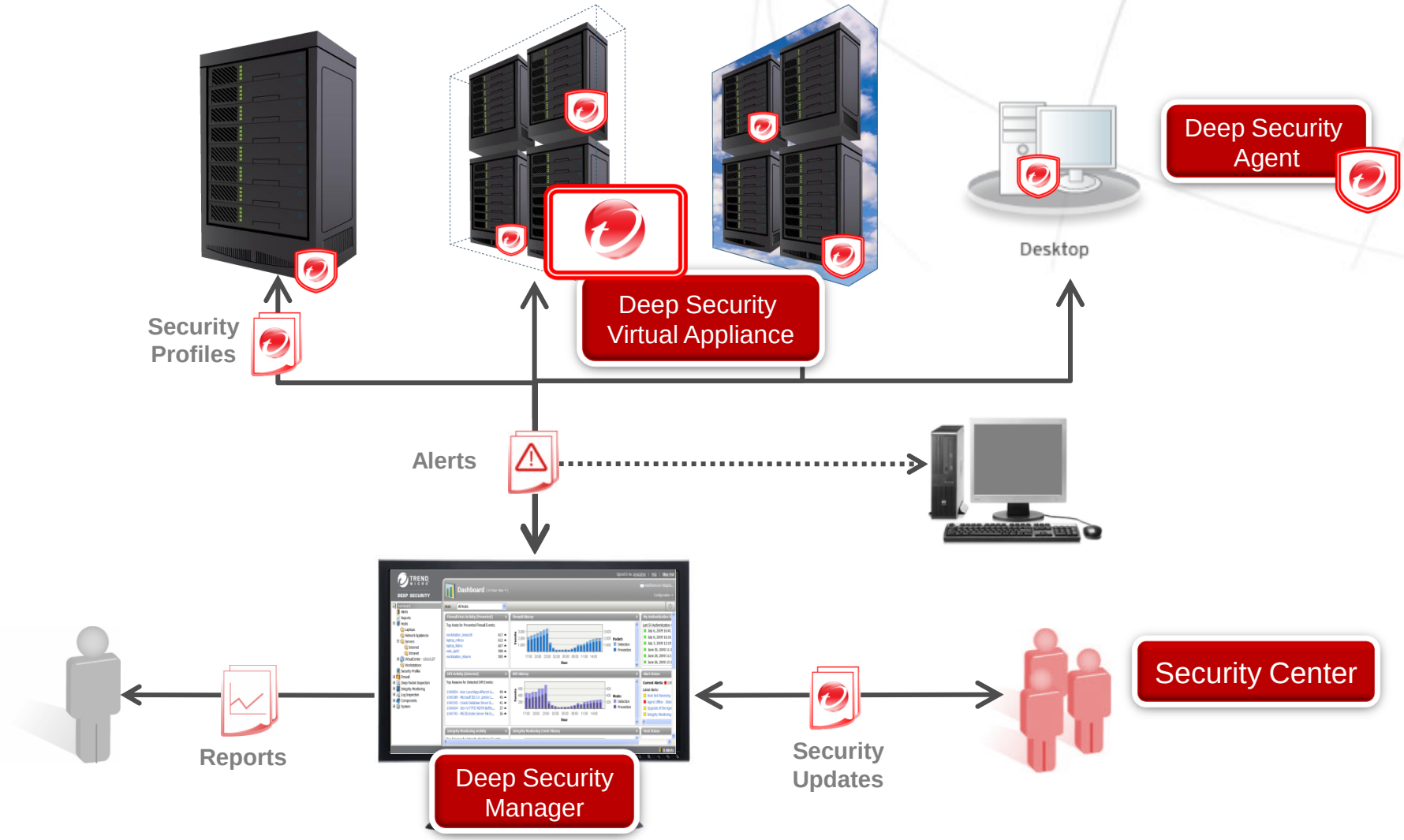


** VMware vSphere 4*
VMsafe API based solution

Deep Security 7.0 Virtual Appliance

Protection Modules	Supported	Description
Firewall	Yes	• Transparent to the VM • Security policies can be assigned on a per network interface basis • Auto-enforce FW policies if Agent in VM is offline or no longer running
Firewall & DPI	Yes	• Full DPI support (IDS/IPS, Web App protection, App Control) • Auto-enforce DPI policies if Agent in VM is offline or no longer running
Integrity Monitoring	No	• Requires Agent in VM
Log Inspection	No	• Requires Agent in VM

Deep Security 7.0 Components



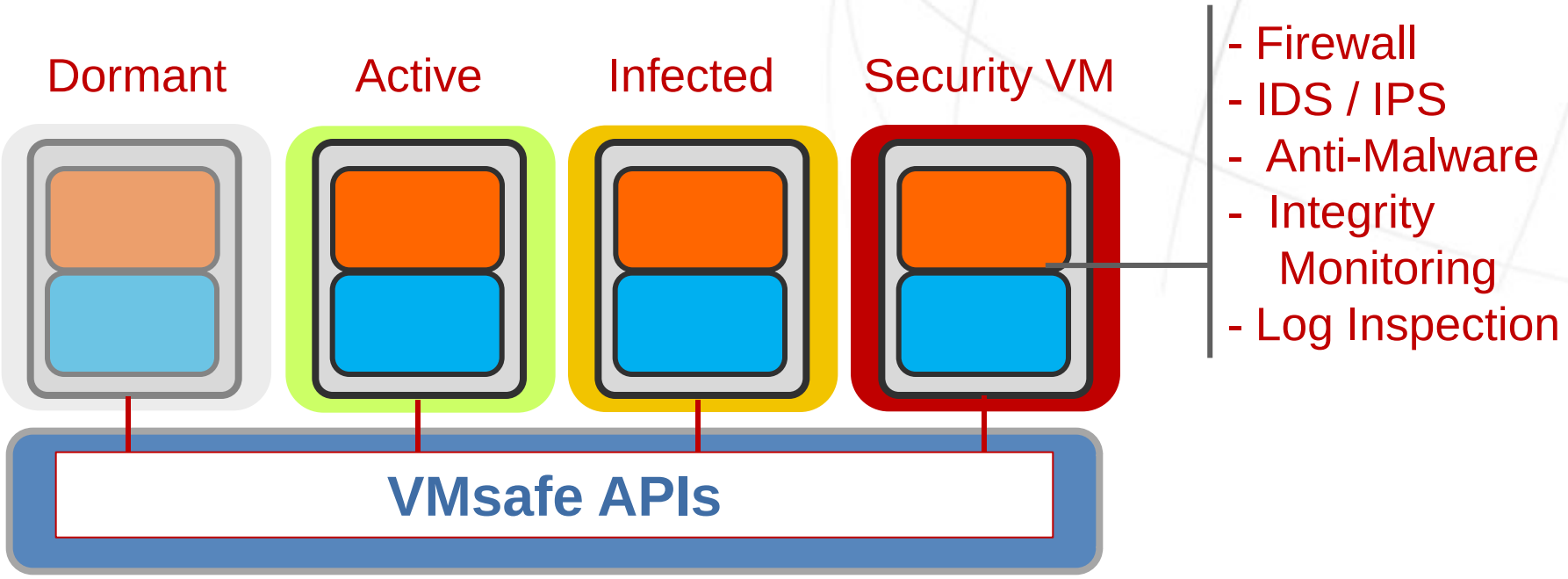
Deep Security 7.0

- Enterprises are increasingly online and data-centric, and no matter what the purpose—connecting partners, personnel, suppliers, or customers—applications face a growing danger of cyber attacks. These targeted threats are greater and more sophisticated than ever before, and data security compliance becomes more stringent every day. Your company needs uncompromising security that enables you to modernize your datacenter with virtualization and cloud computing without reducing performance.
- Trend Micro delivers streamlined, integrated products, services, and solutions that cost-effectively protect sensitive data and minimize risk. Deep Security is comprehensive server and application protection software that enables physical, virtual, and cloud computing environments to become self-defending. Whether implemented as software, virtual appliance, or in a hybrid approach, this solution minimizes overhead, streamlines management, and strengthens transparent security for virtual machines. Deep Security also addresses a wide range of compliance requirements, including six major PCI compliance requirements with web application-layer firewall, IDS/IPS, file integrity monitoring, and network segmentation.

An Example

- Stopping Conficker

How It Works: Stopping Conficker



- **Firewall**: Limits VMs accessing a VM with vulnerable service
- **IDS/IPS:** Prevent MS008-067 exploits
- **Anti-Malware:** Detects and cleans Conficker
- **Integrity Monitoring:** Registry changes & service modifications
- **Log Inspection:** Brute force password attempts

Summary

- Trend Micro Core Protection for VMs 1.0
- Trend Micro Deep Security 7.0

Available from Trend Micro

TODAY

Trend Micro Core Protection for VMs 1.0

- Anti-malware protection for VMware virtual environments

Trend Micro Deep Security 7.0

- Firewall, IDS/IPS, Integrity Monitoring & Log Inspection
- Runs in VMs with vCenter integration
- Virtual Appliance complements agent-based protection

Q3 2010

Trend Micro Deep Security 7.5

- CPVM technology integrated into Deep Security as an anti-malware module

Available from Stallion

TODAY

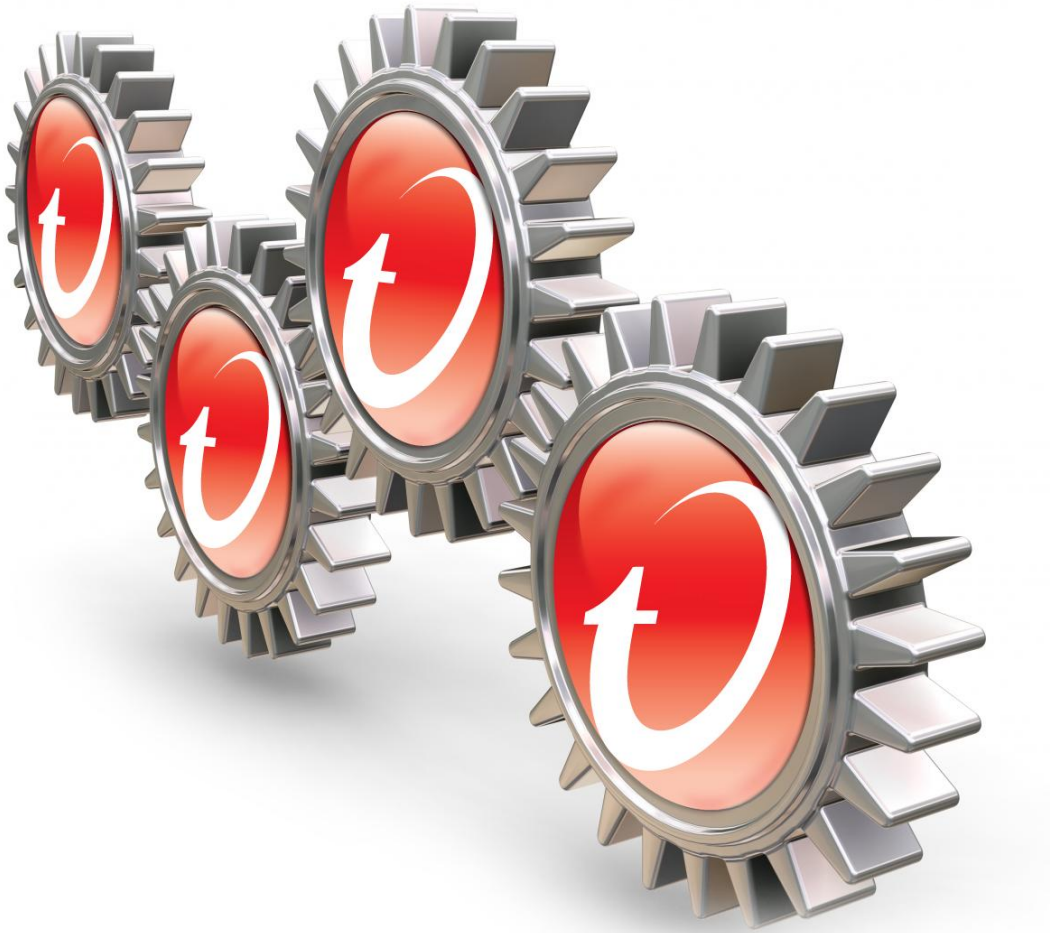
Trend Micro Core Protection for VMs 1.0

- Prices and evaluation licenses
- Demonstrations

Trend Micro Deep Security 7.0

- Prices and evaluation licenses
- Demonstrations

Demo



Trend Micro | Securing Your Web World



Veli-Pekka Kusmin
Pre-Sales Engineer

Trend Micro Baltics & Finland
Porkkalankatu 7 A, 5th floor
FI-00180 Helsinki
Finland
Telephone +358 9 5868 620
Direct +358 9 5868 6212
Fax +358 9 753 1098
Mobile +358 40 596 7181
veli-pekka_kusmin@trendmicro.com
http://www.trendmicro-europe.com