

Next Generation Datacenters & the Realities of Virtualisation Security

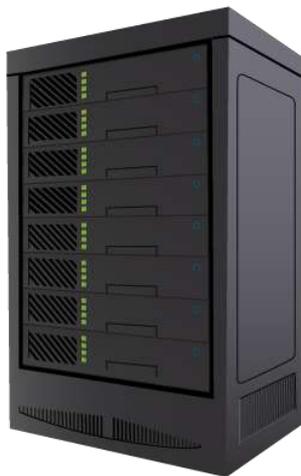
Simon Young • General Manager, Server Security EMEA

Agenda

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

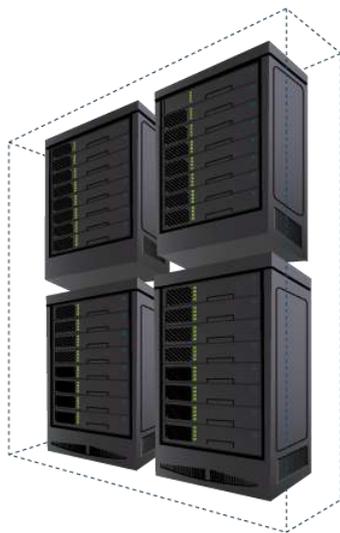
The Dynamic Datacenter

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*

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.

High profile breaches



May-2008: Security breach cost \$12.6 million so far, including legal costs and fines from MasterCard and Visa. [More](#)

[>>](#)



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

[More >>](#)



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

[More >>](#)



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

[More >>](#)



Mar-2009: Hackers hijack PII for 45,000 employees & retirees. [More >>](#)



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 >>](#)

Threat Environment



- **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*

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

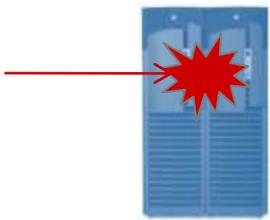
- HITECH, Breach notifications, civil litigation

“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”

Perimeter defences alone are no longer sufficient

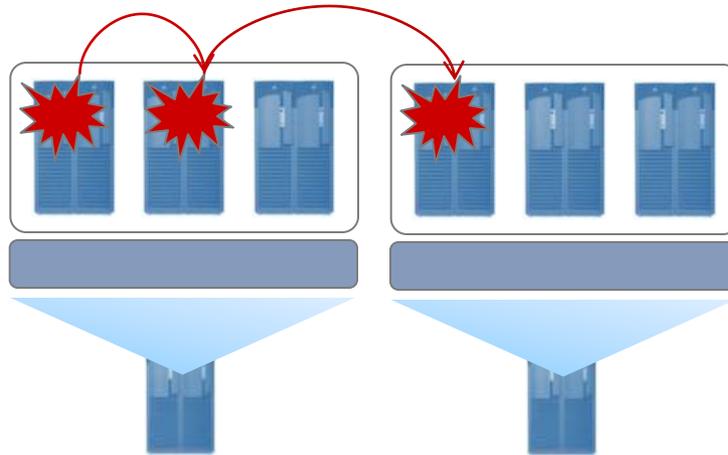
Physical Servers



Servers under pressure

- Encrypted attacks
- Wireless networks
 - Insider attacks
 - Web app attacks

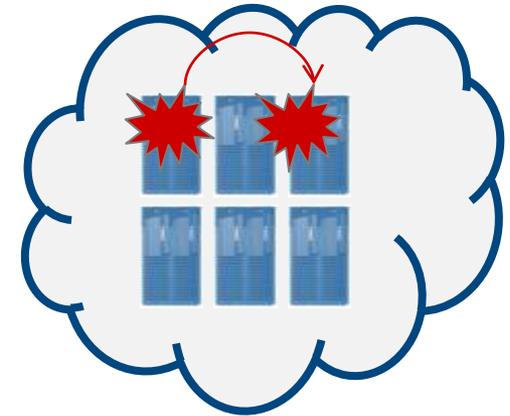
Virtualized Servers



Servers in motion

- Hosting workloads of different sensitivities
 - vMotion challenges
- VMs introduced quickly

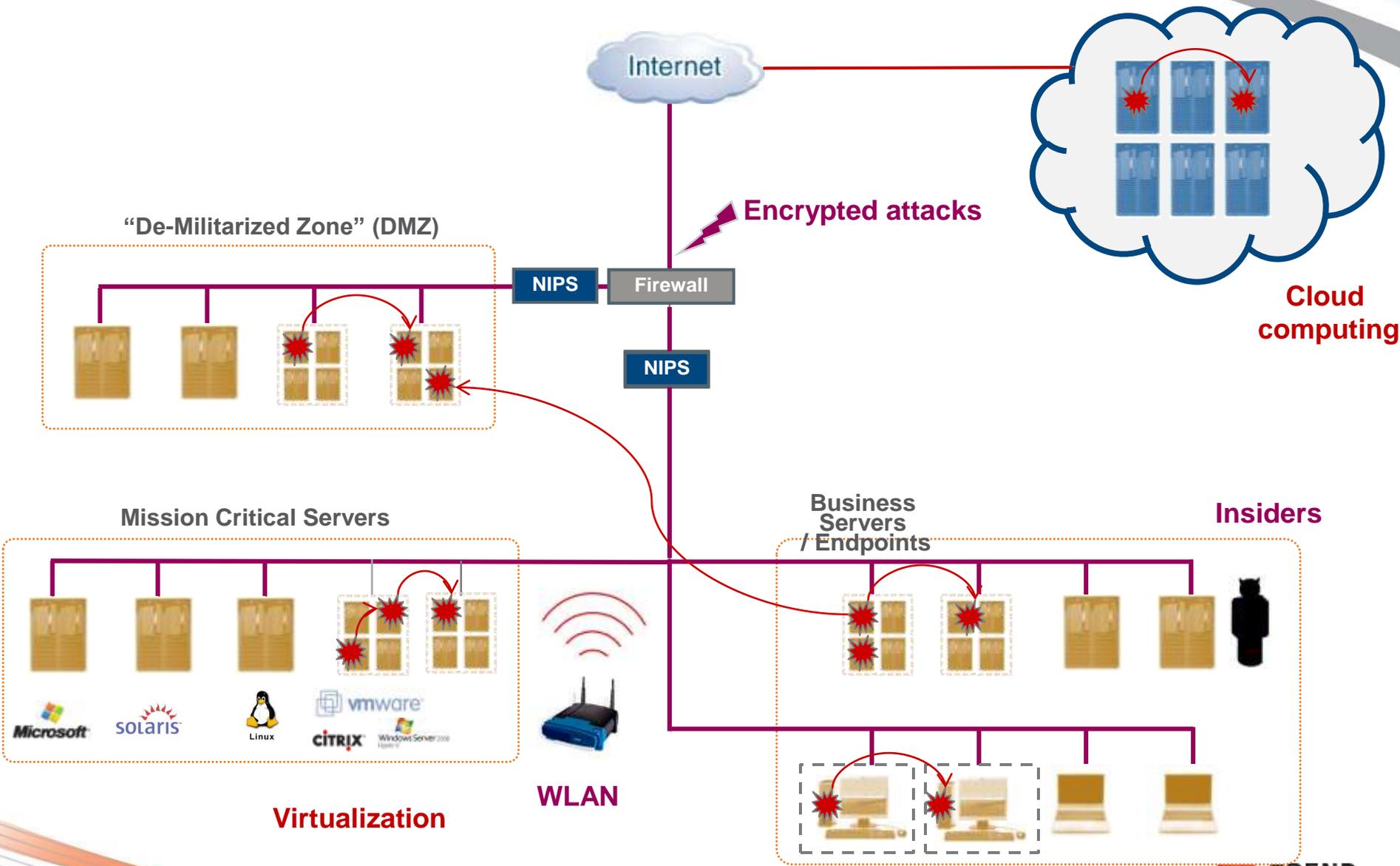
Cloud Computing



Servers in the open

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

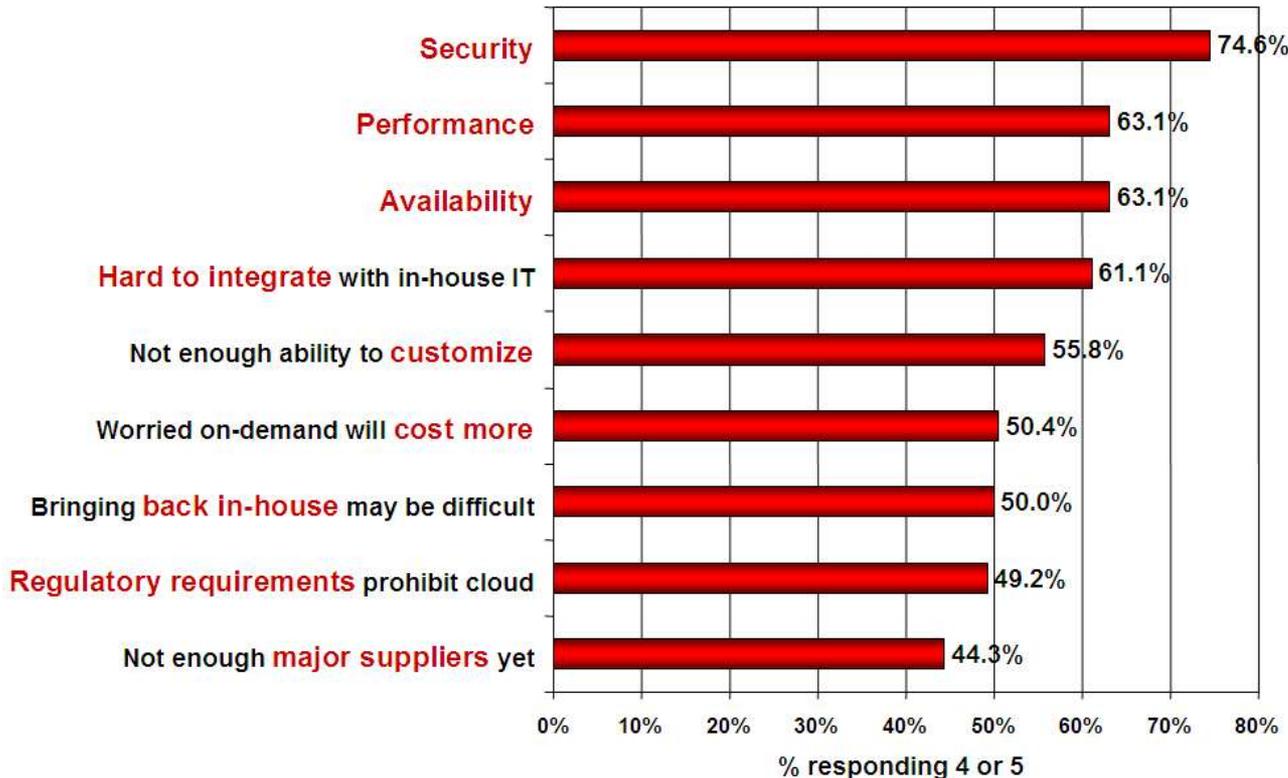
Perimeter is cracking



Cloud security is a recognised concern

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



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**

Source: IDC Enterprise Panel, August 2008 n=244

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		✓

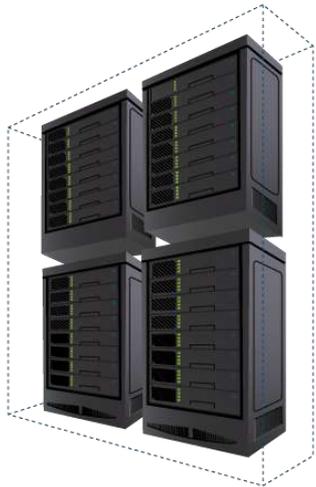


Dynamic Virtual Machines

Dynamic:



Security challenges



- Reverted
- Paused
- Restarted
- Cloned
- Moved

- 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

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”

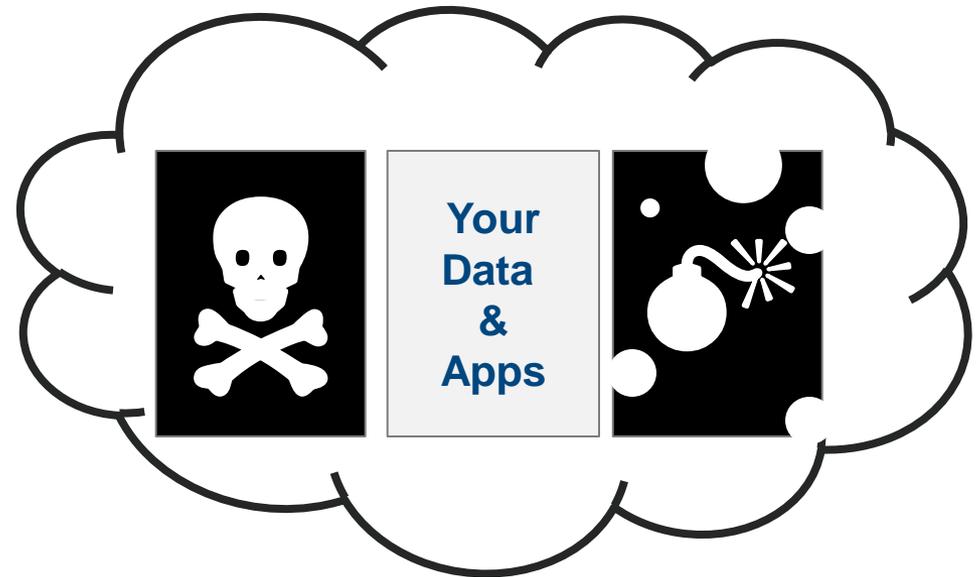
IBM, 2008

IBW' 2008

end of year”

System & Data Integrity

**“59% of
data breaches
resulted from
hacking and
intrusions”
*Verizon, 2008***



Security Issues:

- Shared physical infrastructure
- Malicious or unauthorised changes

Policy & Compliance

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

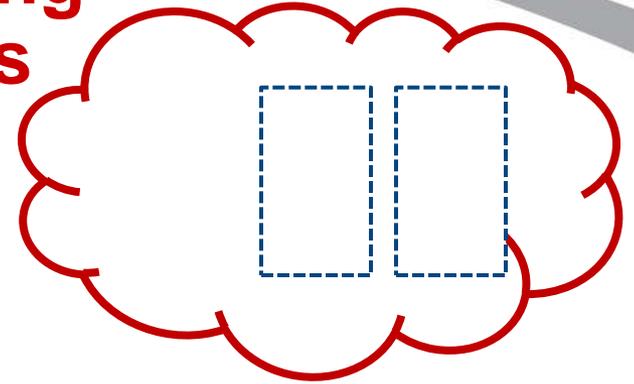


Challenge:
How do you
prove compliance
when your servers
are in the cloud?

are in the cloud?
prove your servers?

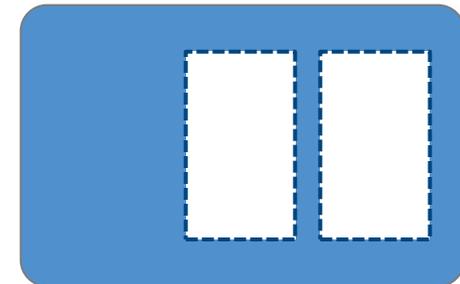
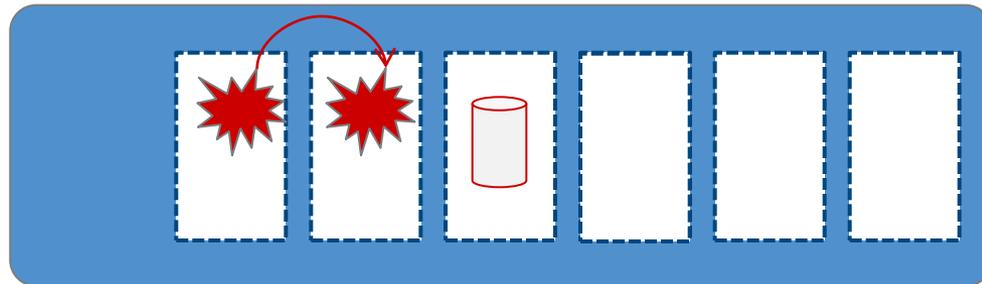
Leveraging Virtualisation Infrastructure for improved security

Virtualisation & Cloud Computing Create New Security Challenges



Inter-VM
attacks

PCI Mobility Cloud Computing

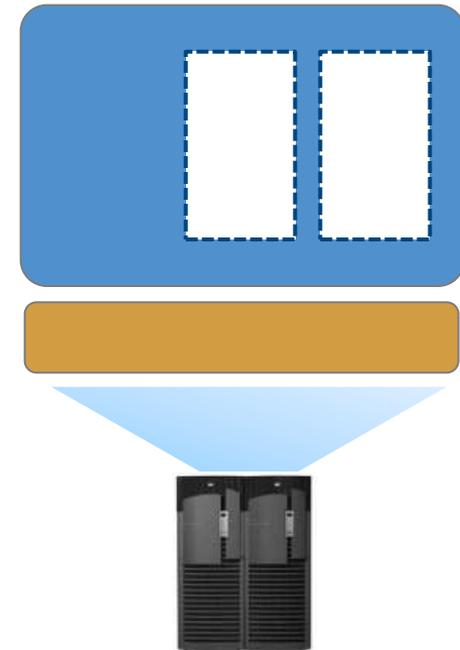
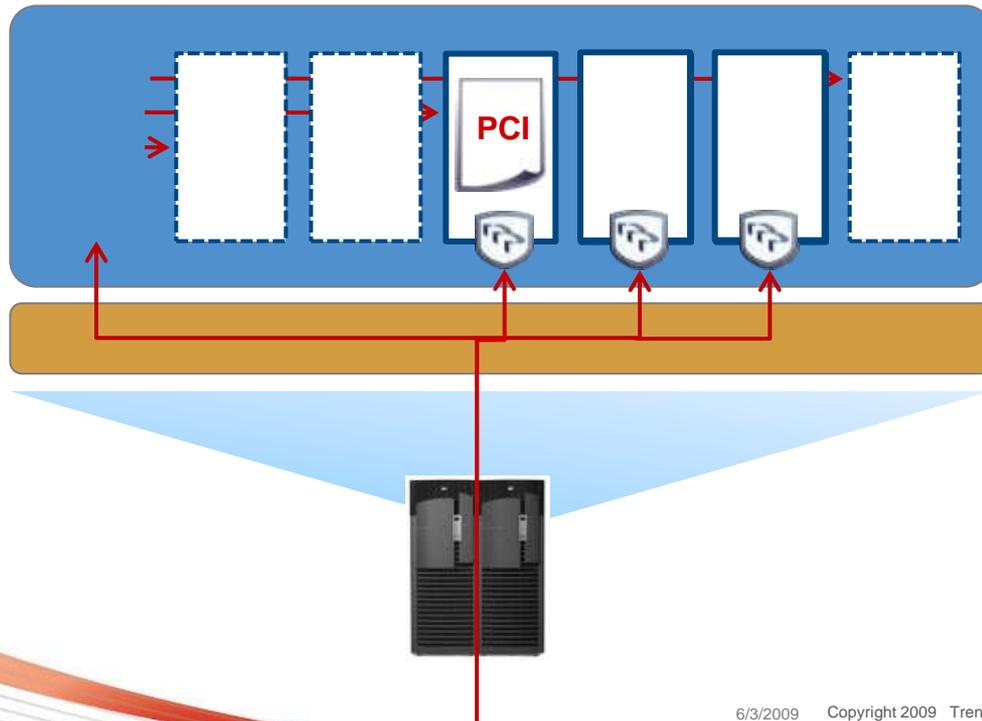
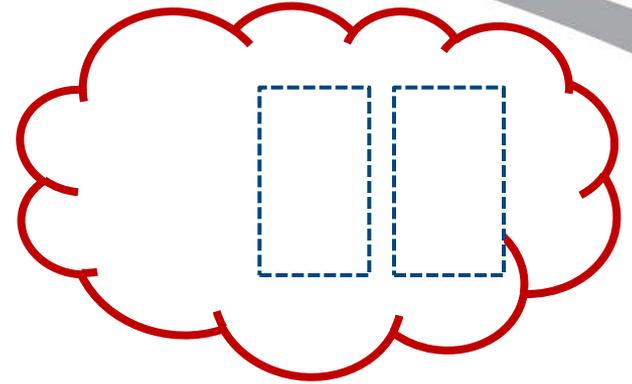


Hypervisor

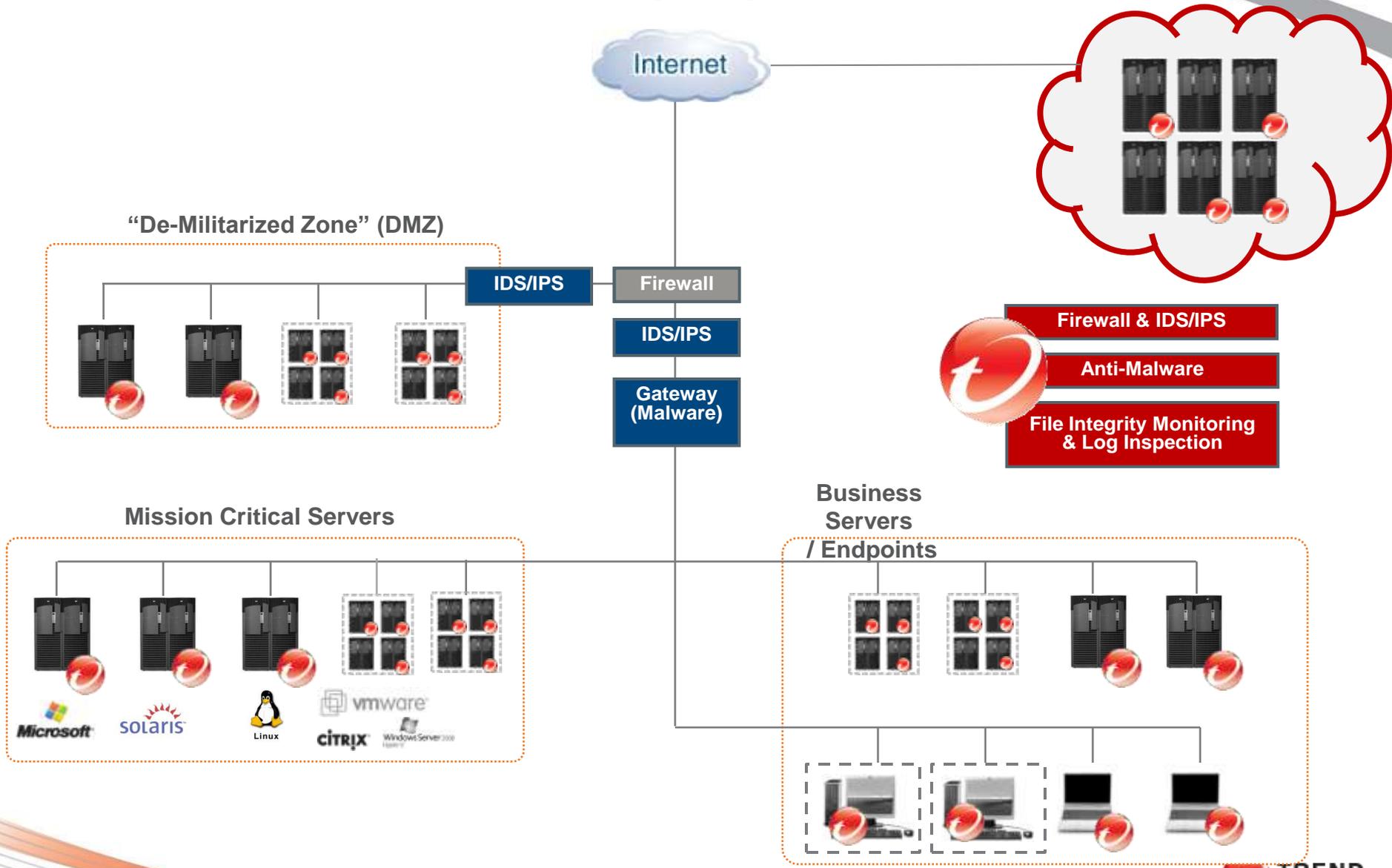
Hypervisor



Coordinated Approach



Retreat To The Server (VM)!





Securing Your Web World



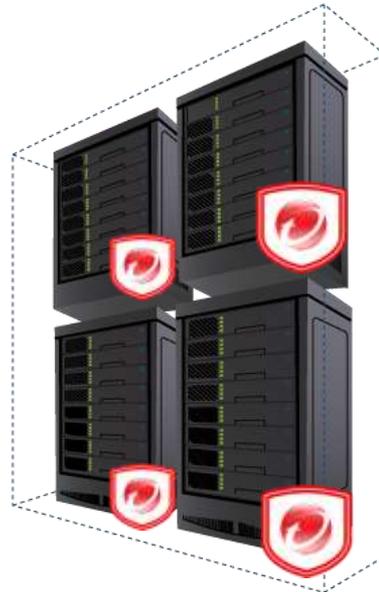
Deep Security 7 Overview

What is Deep Security?

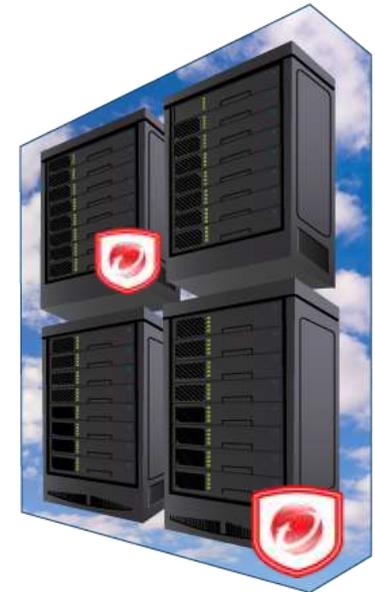
PHYSICAL



VIRTUAL



CLOUD



Deep Packet Inspection		
IDS / IPS	Web App. Protection	Application Control

Firewall

Integrity Monitoring

Log Inspection



Architecture

PHYSICAL

VIRTUAL

CLOUD



Security Updates

Alerts

Deep Security Manager

IT Infrastructure Integration

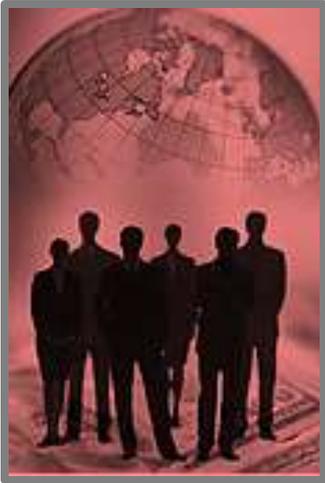
- vCenter
- SIEM
- Active Directory
- Log correlation
- Web services

Security Center

Reports

Security Updates

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

Certifications



Common Criteria

Evaluation Assurance Level 3 Augmented (EAL 3+)

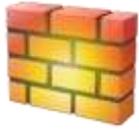
- Achieved certification **across more platforms** (Windows, Solaris, Linux) **than any other** host-based intrusion prevention product.
 - Higher certification than any other HIPS vendor
 - Validated against US National Security Agency defined profile for IDS
-



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

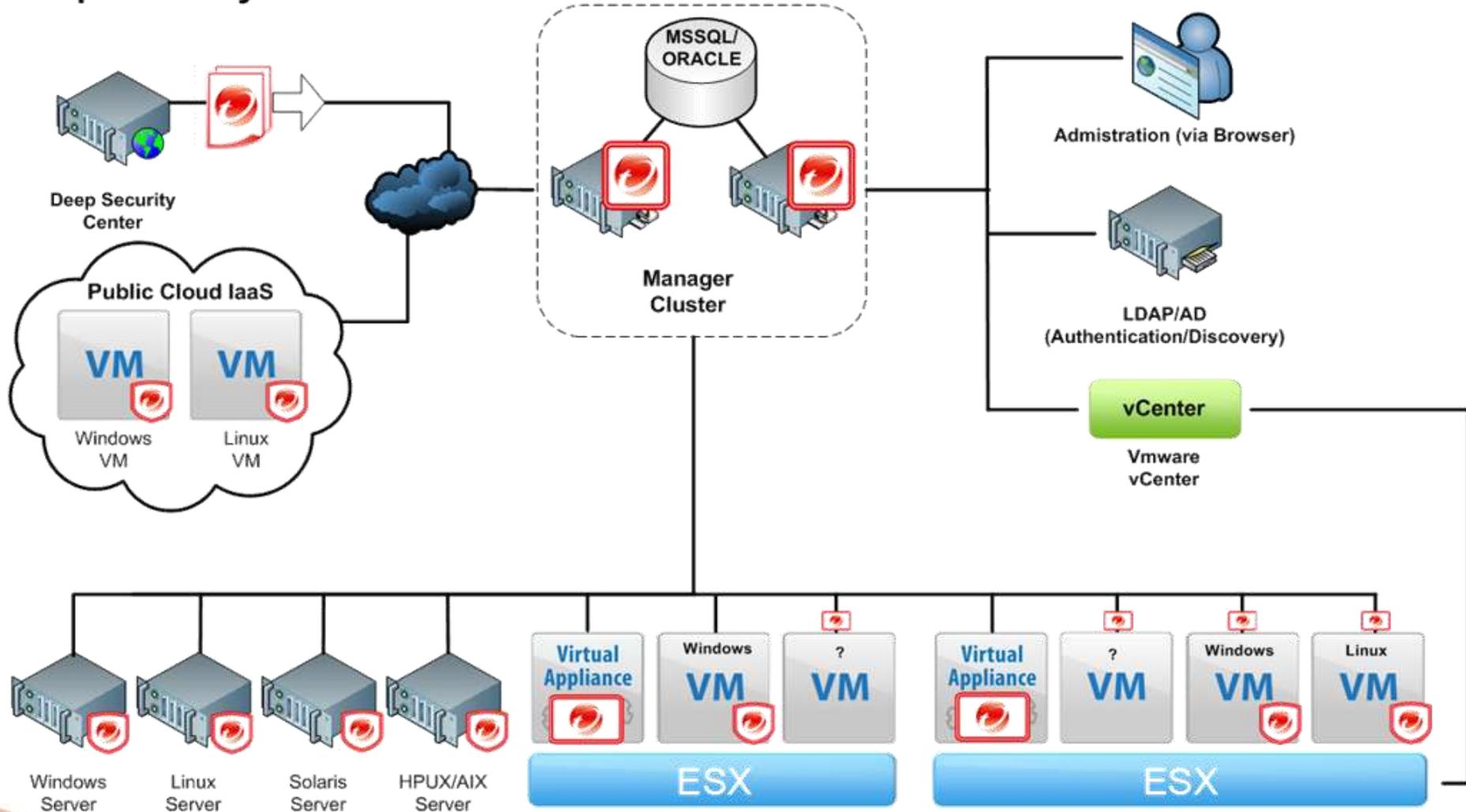


Log Inspection

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

Deep Security 7 Overview

Deep Security 7.0



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



Security Profile

The screenshot displays the Trend Micro Deep Security Manager interface in a Mozilla Firefox browser window. The main window is titled "Security Profiles" and shows a list of various security profiles on the left-hand side, including Deep Security Manager, Deep Security Virtual Appliance, DHCP Server, DNS and WMI Server, FTP Server, Mail Server, Microsoft SQL Server, MySQL Server, Oracle SQL Server, test, Web Server, Windows Laptop, Windows Mobile Laptop, and Windows Workstation. The "Web Server" profile is selected and its details are shown in a separate window titled "Web Server Details".

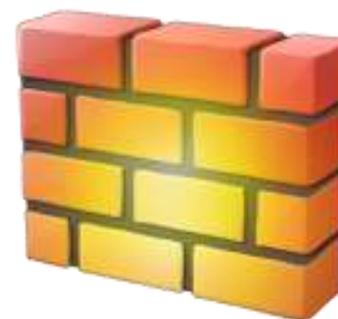
The "Web Server Details" window shows the following configuration:

- Name:** Web Server
- Description:** A base profile for Web Servers. Customization of this profile may be required based on platform and applications.
- Status:**
 - Firewall: On, 3 rules
 - DPI: Detect, 7 rules
 - Integrity Monitoring: On, 1 rule
 - Log Inspection: On, no rules
 - HostID Usage: 11
- Host(s) Using This Security Profile:**

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



Firewall

The screenshot shows the 'Firewall Rules' configuration page in a Mozilla Firefox browser. The address bar shows the URL 'https://training4119/Details.screen?hostID=61'. The left sidebar contains a tree view of configuration categories, with 'Firewall Rules' selected. The main content area displays a table of firewall rules. The table has columns for Name, Priority, Direction, Frame Type, Protocol, Source IP, Source MAC, Source Port, and Destination. There are two groups of rules: 'Allow (4)' and 'Force Allow (1)'. The 'Allow (4)' group includes rules for ICMP, TCP/UDP, ARP, and Deep Security Manager. The 'Force Allow (1)' group includes a rule for NetBios Name Service.

Name	Priority	Direction	Frame Type	Protocol	Source IP	Source MAC	Source Port	Dest
Allow (4)								
<input checked="" type="checkbox"/> Allow solicited ICMP replies	0 - Lowest	Incoming	IP	ICMP	Any	Any	N/A	Any
<input checked="" type="checkbox"/> Allow solicited TCP/UDP replies	0 - Lowest	Incoming	IP	TCP+UDP	Any	Any	Any	Any
<input checked="" type="checkbox"/> ARP	0 - Lowest	Incoming	ARP	N/A	N/A	Any	N/A	N/A
<input checked="" type="checkbox"/> Deep Security Manager	0 - Lowest	Incoming	IP	TCP	Any	Any	Any	Any
Force Allow (1)								
<input checked="" type="checkbox"/> NetBios Name Service	2 - Normal	Incoming	IP	UDP	Any	Any		NetBios - ns (137) Any

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

The screenshot displays the Trend Micro Management Console interface. The browser window title is "127.0.0.1 Details - Mozilla Firefox" and the address bar shows "https://training4119/Details.screen?hostID=61".

Left Navigation Tree:

- 127.0.0.1
 - Interfaces
 - Alerts
 - Firewall
 - Firewall Events
 - Firewall Rules
 - Stateful Configurations
 - Deep Packet Inspection
 - DPI Events
 - DPI Rules
 - IDS/IPS
 - Application Control
 - Web Application Prot
 - Application Types
 - SSL Configurations
 - Integrity Monitoring
 - Integrity Monitoring Eve
 - Integrity Monitoring Rule
 - Log Inspection
 - Log Inspection Events
 - Log Inspection Rules
 - Log Inspection Decoder
 - System
 - System Events
 - System Settings
 - Overrides

Main Content Area:

Deep Packet Inspection

Deep Packet Inspection

- Inherit
- On
- Off

Inline DPI Behavior (Behavior when Network Engine Mode is Inline)

- Prevent
- Detect

The Network Engine is operating Inline. This means that when Deep Packet Inspection is "On", it can operate in Prevent or Detect mode as specified above. To switch between Inline and Tap Mode, click [here](#).

Recommendations

Last Scan for Recommendations: October 5, 2009 09:51
Total Recommendations: 158 DPI Rule(s) recommended for assignment

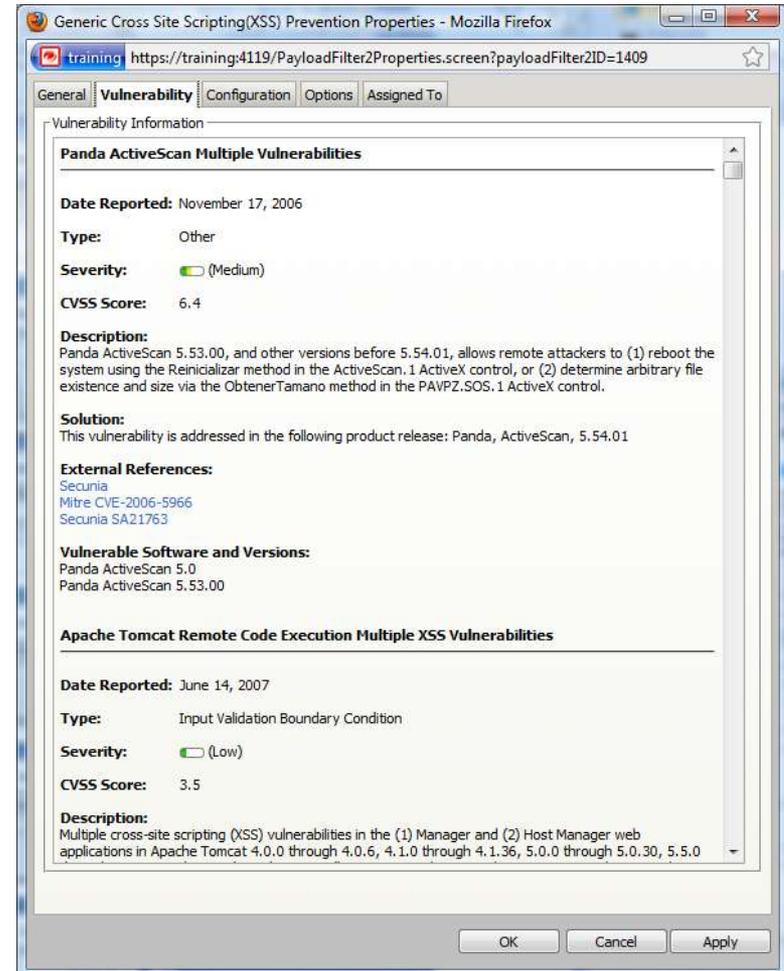
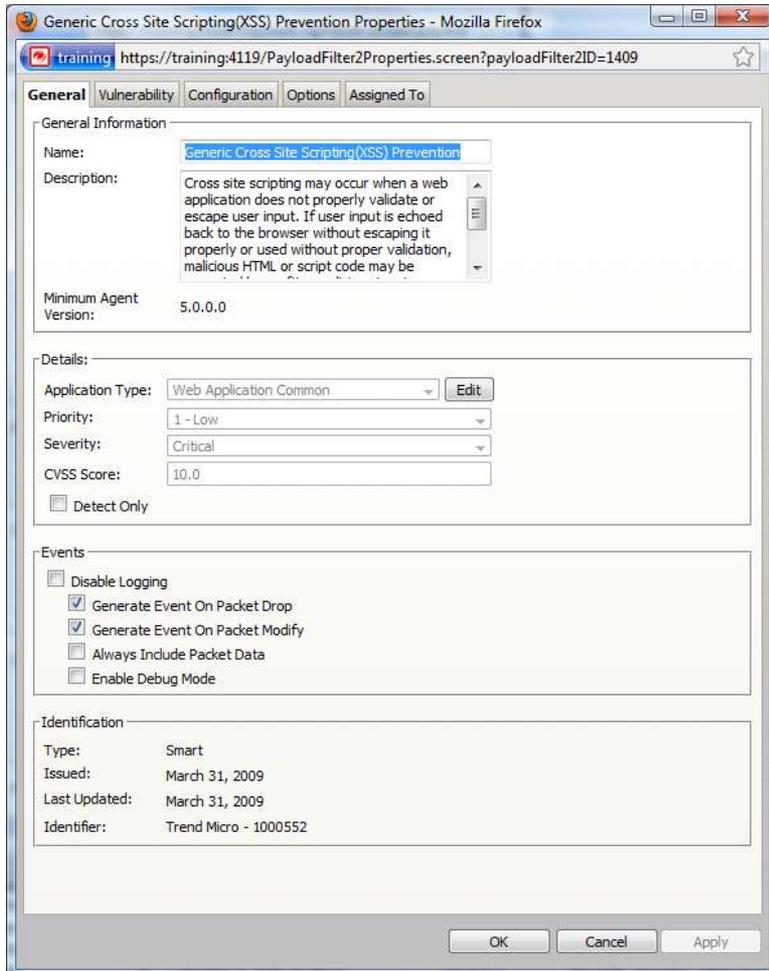
Automatically assign/unassign recommended DPI Rules to Host during Recommendation Scans:

Recommendation Scan

The screenshot displays the 'DPI Rules' configuration page in a web browser. The left sidebar shows a navigation tree with categories like 'Interfaces', 'Alerts', 'Firewall', 'Deep Packet Inspection', 'DPI Rules', 'IDS/IPS', 'Application Control', 'Web Application Protection', 'Application Types', 'SSL Configurations', 'Integrity Monitoring', 'Log Inspection', and 'System'. The main content area shows a table of DPI rules with columns for Name, Priority, Severity, Mode, Type, CVE, CVSS Score, and Last Updated. The table lists various rules for different applications and services, such as Microsoft SQL Server, DHCP Client, DNS Client, DNS Server, FTP Server, and Outlook Express. A 'Save' button is located at the bottom right of the table.

Name	Priority	Severity	Mode	Type	CVE	CVSS Score	Last Updated
Database Microsoft SQL (1)							
1000917 - Microsoft SQL Server XP_C4D 2 - Normal	Medium	Prevent	Exploit	N/A	5.8	October	
DHCP Client (1)							
1000861 - Microsoft Windows DHCP Client 2 - Normal	Critical	Prevent	Exploit	CVE-2006-2372	10.0	December	
DNS Client (2)							
1000862 - Microsoft Windows DNS Client 2 - Normal	Critical	Prevent	Vulnerability	CVE-2006-3441	10.0	June 2	
1002657 - DNS Insufficient Socket Entropy 2 - Normal	Medium	Detect Only	Smart	CVE-2008-1447	6.4	July 25	
DNS Server (2)							
1003330 - DNS Server Vulnerability In Wt 2 - Normal	Low	Prevent	Vulnerability	CVE-2009-0093	3.5	March	
1003663 - BIND Dynamic Update DoS 2 - Normal	Medium	Prevent	Exploit	CVE-2009-0696	4.3	August	
FTP Server IIS (2)							
1003698 - Microsoft IIS FTPd Remote Bu 2 - Normal	Critical	Prevent	Exploit	CVE-2009-3023	9.0	September	
1003704 - Microsoft IIS FTPd Unspecific 2 - Normal	Medium	Prevent	Exploit	CVE-2009-2521	6.8	September	
Mail Client Outlook Express (2)							
1003148 - Microsoft Outlook Express Mal 2 - Normal	High	Detect Only	Vulnerability	N/A	N/A	January	
1003149 - Microsoft Outlook Express Mal 2 - Normal	High	Detect Only	Vulnerability	N/A	N/A	January	
Mail Client Windows (1)							
1000244 - Microsoft Windows EOT File Rv 2 - Normal	High	Prevent	Vulnerability	CVE-2006-0010	7.5	October	
NetBIOS Name Service (1)							
1003325 - WINS Server Vulnerability In V 2 - Normal	Medium	Prevent	Vulnerability	CVE-2009-0093, CVE-2009-0094	5.5	March	

DPI Detail



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

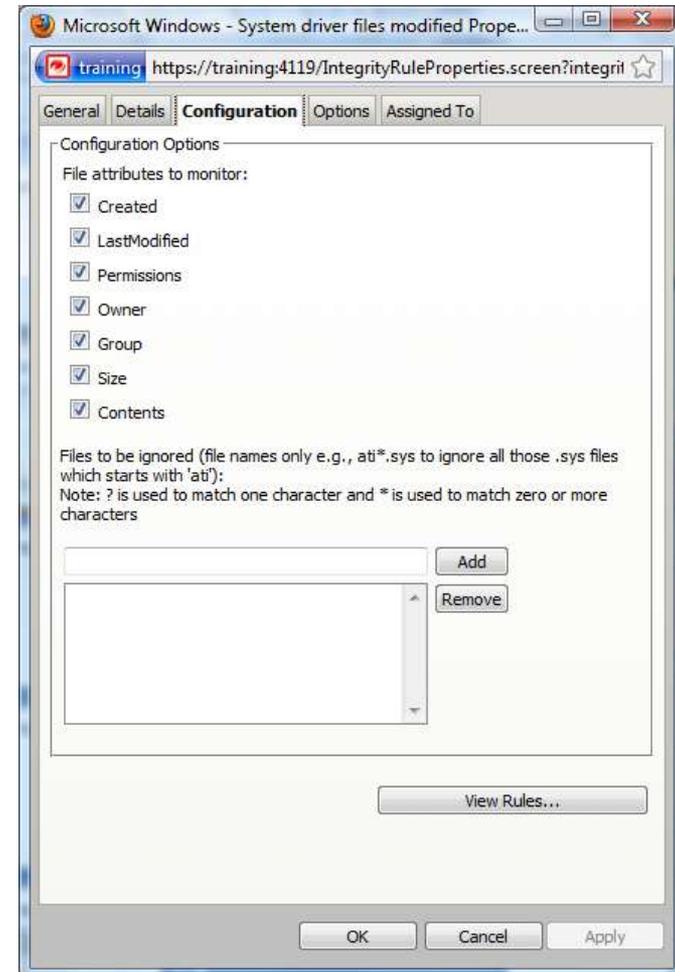
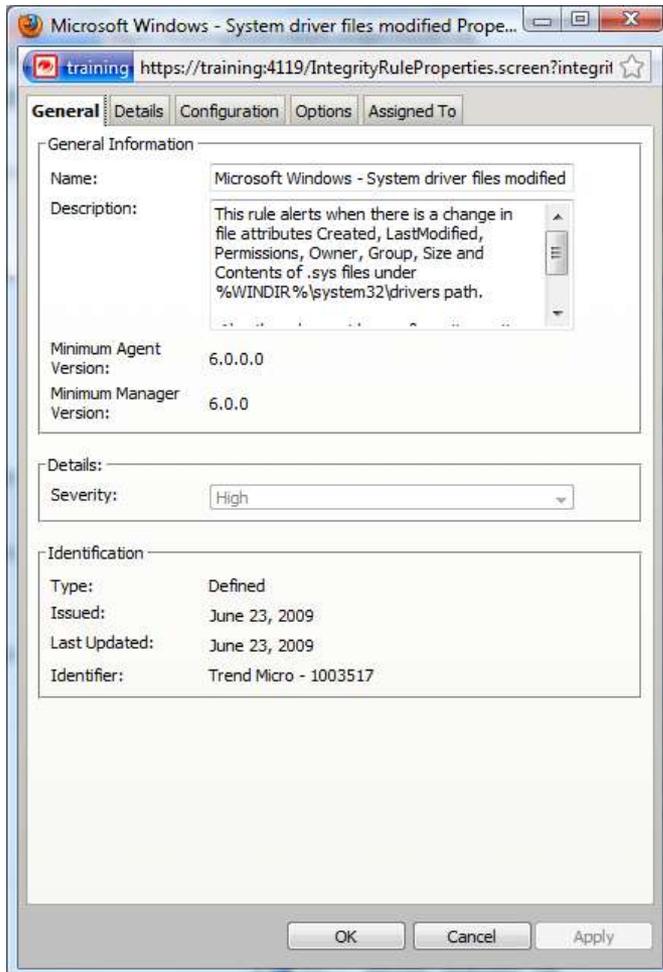
Integrity Monitoring

The screenshot shows a web browser window titled "127.0.0.1 Details - Mozilla Firefox" with the URL "https://training4119/Details.screen?hostID=61". The interface is for configuring Integrity Monitoring on a host. On the left is a navigation tree with categories like Interfaces, Alerts, Firewall, Deep Packet Inspection, IDS/IPS, Application Control, Web Application Prot, Application Types, SSL Configurations, Integrity Monitoring (selected), Log Inspection, and System. The main content area is titled "Integrity Monitoring" and contains several sections:

- Integrity Monitoring:** Includes radio buttons for "Inherit", "Real Time" (selected), "On", and "Off".
- Integrity Scan:** Shows "Last Full Scan For Changes: October 5, 2009 10:59" and a "Scan For Changes" button.
- Baseline:** Shows "Last Integrity Baseline Created: October 5, 2009 11:27" and buttons for "Rebuild Baseline" and "View Baseline".
- Recommendations:** Shows "Last Scan for Recommendations: October 5, 2009 10:51" and "Total Recommendations: 28 Integrity Monitoring Rule(s) recommended for assignment". It includes a dropdown menu for "Automatically assign recommended Integrity Monitoring Rules to Host during Recommendation Scans:" set to "Inherited (No)", and buttons for "Scan For Recommendations" and "Clear Recommendations".

A "Save" button is located at the bottom right of the interface.

Integrity Monitoring Configuration



Log Inspection



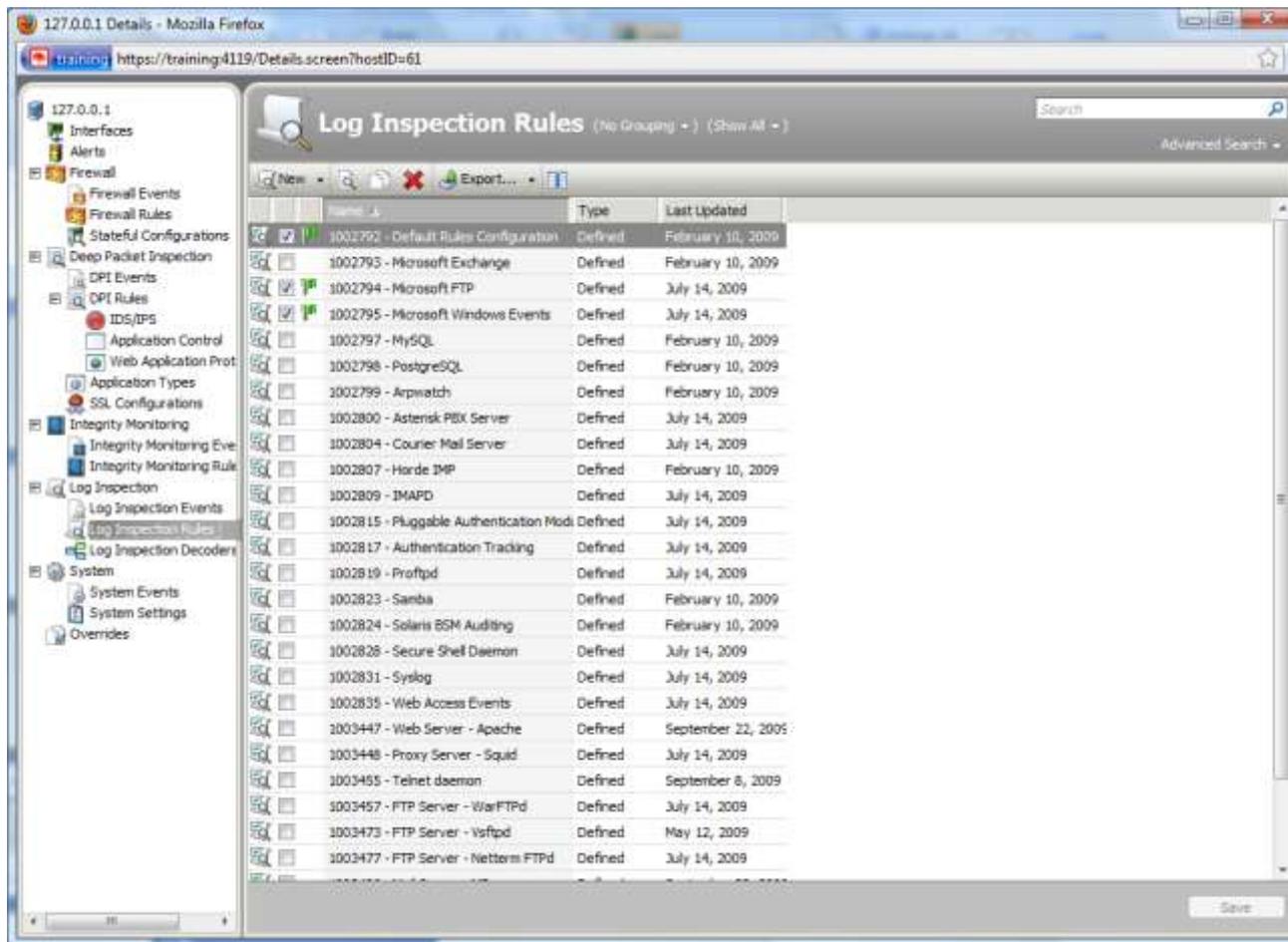
Getting visibility into important security events buried in log files

- 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

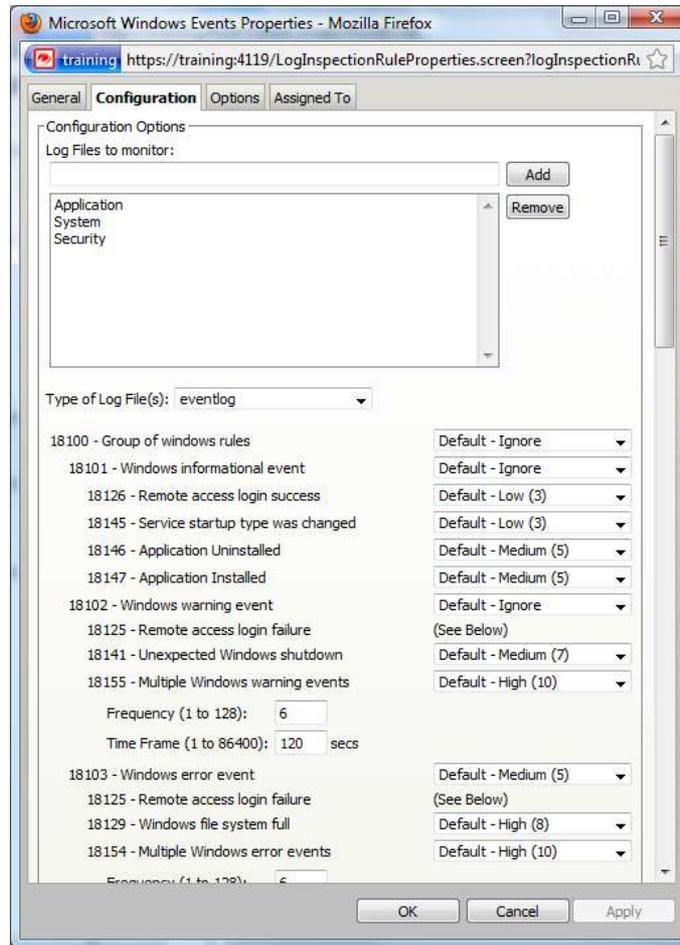
Log Inspection



The screenshot shows the Trend Micro Log Inspection Rules interface. The left sidebar contains a tree view of configuration categories, with 'Log Inspection' selected. The main area displays a table of rules with columns for Name, Type, and Last Updated. The table lists various system and application-specific rules, such as 'Default Rules Configuration', 'Microsoft Exchange', and 'MySQL'. A search bar and 'Advanced Search' link are visible at the top right of the main area.

Name	Type	Last Updated
1002792 - Default Rules Configuration	Defined	February 10, 2009
1002793 - Microsoft Exchange	Defined	February 10, 2009
1002794 - Microsoft FTP	Defined	July 14, 2009
1002795 - Microsoft Windows Events	Defined	July 14, 2009
1002797 - MySQL	Defined	February 10, 2009
1002798 - PostgreSQL	Defined	February 10, 2009
1002799 - Arpwatch	Defined	February 10, 2009
1002800 - Astensik PBX Server	Defined	July 14, 2009
1002804 - Courier Mail Server	Defined	July 14, 2009
1002807 - Horde IMP	Defined	February 10, 2009
1002809 - IMAPD	Defined	July 14, 2009
1002815 - Pluggable Authentication Mod	Defined	July 14, 2009
1002817 - Authentication Tracking	Defined	July 14, 2009
1002819 - Proftpd	Defined	July 14, 2009
1002823 - Samba	Defined	February 10, 2009
1002824 - Solaris BSM Auditing	Defined	February 10, 2009
1002828 - Secure Shell Daemon	Defined	July 14, 2009
1002831 - Syslog	Defined	July 14, 2009
1002835 - Web Access Events	Defined	July 14, 2009
1003447 - Web Server - Apache	Defined	September 22, 2005
1003448 - Proxy Server - Squid	Defined	July 14, 2009
1003455 - Telnet daemon	Defined	September 8, 2009
1003457 - FTP Server - WarFTpd	Defined	July 14, 2009
1003473 - FTP Server - Vsftpd	Defined	May 12, 2009
1003477 - FTP Server - Netterm FTPD	Defined	July 14, 2009

Log Inspection Configuration





Deep Security for Virtualisation

Category	Requirement
NW Segmentation & VM Zoning	<ul style="list-style-type: none">– Isolation of virtual machines on shared servers– Independent of vSwitches and network architecture– Stateful firewall, groupings, security policy enforcement
Virtualisation Security Mgmt	<ul style="list-style-type: none">– Automation via web services API, template deployment– VMsafe coordinated approach– Visibility into virtual and physical servers, server state
Integrity Monitoring & Log	<ul style="list-style-type: none">– 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	<ul style="list-style-type: none">– 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	<ul style="list-style-type: none">– 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

Prevents Data Breaches & Business Disruptions

➤ Internal policies

➤ PCI & other requirements

Enables Compliance

➤ Detailed reports document prevented attacks & compliance status

Supports Operational Cost Reductions

➤ **Prioritize secure coding efforts**

➤ **Manage unscheduled patching**

➤ **Provides security necessary to realise virtualisation savings**

➤ **Increased value from SIEM investments**



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.



Vision

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



THANK YOU!

