



Защита виртуальных систем – сейчас и в ближайшее время

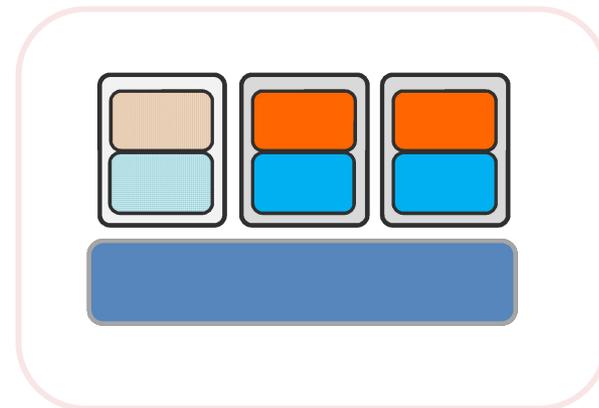
Николай Романов • Технический консультант

Подход к защите VM

На физических и виртуальных серверах угрозы одинаковые.

+ дополнительные особенности:

1. Отключенные VM
2. Разделение ресурсов
3. Рост числа VM
4. Трафик между VM
5. vMotion



Виртуализация и безопасность

Головная боль

- “Более 50% всех виртуальных серверов обеспечивает работу производственных систем, включая наиболее критические из них” (Gartner)
- “По данным оценки на 2009, 60% таких систем были защищены хуже, чем аналогичные аппаратные варианты” (IDC)

Сложности

- Большое количество важных для бизнеса приложений находятся на одном сервере, что повышает риски
- Трафик между VM нельзя обезопасить традиционными средствами

Решение

- Нужен согласованный и адаптивный подход
 - Мобильность:** Защита является частью образа
 - Гибкость:** Прозрачность с точки зрения конфигурирования виртуальной сети
 - Видимость:** Защита от атак на уровне трафика между VM
- Масштабируемость управления за счет интеграции с VMware Virtual Center integration

Уменьшение бреши в плане уязвимостей

Головная боль

- Накладно тестировать и разворачивать обновления

Сложности

- Тесты на полную совместимость съедают много времени
- Патчи ОС не выпускаются сторонними производителями
- Старый софт не обновляется
- Как обеспечить SLA?
- Как обеспечить соответствие по virtual patching?

Решение

- Защита от уязвимостей путем виртуального обновления
 - Применимо в любое удобное время
 - Реже нужно обновлять системы
 - Защита старых приложений
 - Защита на уровне zero-day атак
 - Сотрудники ИТ службы могут заниматься другими делами
- Virtual patching позволяет снизить число задач, связанных с внеплановыми обновлениями на 50%-75%

Безопасность веб приложений

Головная боль

- “34% всех взломов были выполнены через бреши в веб приложениях” (Verizon)
- “75% всех атак были сделаны на уровне приложений” (Gartner)

Сложности

- Традиционная защита периметра не защитит
- Выявление и устранение уязвимостей в веб приложениях занимает время и ресурсы
- Старые приложения нельзя обновить

Решение

- Защита от уязвимостей до их устранения
 - Гибкое управление процессом
 - Уведомление производителя ПО и установка патчей по мере их выпуска
 - Постоянная защита даже для старого ПО
- Защита от zero-day атак

Trend Micro

Лучший в отрасли по защите виртуализированных ЦОД

Selected Virtualization Security Vendors

	Host Based	Anti-Malware	Virtual Appliance	Virtual Zones	Virtual Infrastructure Protection	VM Lifecycle Protection	Log and Patch Management	Configuration Management
Altor			X	X	X	X	X	X
Apani	X			X		X		
Catbird		X	X	X	X	X	X	X
Check Point			X	X	X			
HyTrust					X	X	X	X
IBM-ISS	X		X	X	X	X	X	X
McAfee	X	X	X					
Red Cannon			X		X	X	X	X
Reflex Systems			X	X	X	X	X	X
Stonesoft			X		X		X	
Trend Micro	X	X	X	X	X	X	X	X
Tripware	X				X	X		X
VMware				X	X	X		

DEEP SECURITY 7.0 - VIRTUALIZATION SECURITY

Защита на базе решения Deep Security

“Мультиплатформенная защита критически важных для бизнеса серверов и приложений”

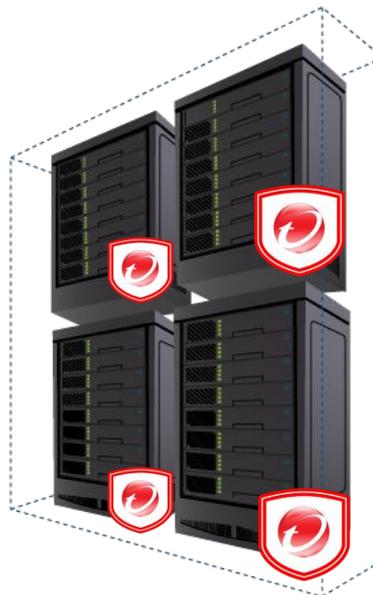
Operating Systems	Windows (2000, XP, 2003, Vista, 2008, 7), Sun Solaris (8, 9, 10), Red Hat EL (4, 5), SuSE Linux (10,11), AIX (5.3,6.1), HP-UX 11i
Database servers	Microsoft SQL Server, Oracle, MySQL, Ingres, PostgreSQL, SAP MaxDB
Web servers	Microsoft IIS, Apache, Apache Tomcat, Microsoft Sharepoint, SAP, Sybase, Oracle
FTP servers	Ipswitch, War FTP Daemon, Microsoft IIS, Linux, Oracle XDB, NetTerm
Backup servers	CA BrightStor, EMC Legato, IBM Tivoli
Storage mgt servers	Symantec, Veritas
DHCP servers	Microsoft DHCP
Mail clients	Outlook Express, MS Outlook, Windows Vista Mail, IBM Lotus Notes, Ipswitch IMail Client
Application Control	Remote Login, Mail Clients, File Sharing, Instant Messaging, Browsers, Web Media,
Suspicious Server Traffic	MS SQL, Telnet, SSL, SSH, SMTP, FTP, HTTP, Oracle, RDP, X11, HTTP over HTTPS
Other applications	Samba, IBM WebSphere, Oracle BEA WebLogic, IBM Lotus Domino Web Access, X.Org, X Font Server prior, Rsync, OpenSSL, Novell Client, LDAP Directories, Internet Explorer, Firefox

Защита серверов/приложений:

Физические

Виртуальные

Облачные



Глубокий
пакетный
анализ
(DPI)

Брандмау
эр

Монитори
нг
целостнос
ти

Анализ
событий
журналов

Антивирус



В рамках DSWA

Q3/2010

Реактивная защита



Уведомления Microsoft по технической безопасности

- Microsoft заблаговременно предоставляют общую информацию по вопросам безопасности продуктов
- Уведомления Microsoft по технической безопасности информируют о найденных уязвимостях и доступных исправлениях, касающихся продуктов Microsoft
- Уведомления Microsoft по технической безопасности выпускаются каждый 2^{ой} вторник ежемесячно и содержат следующую информацию:
 - Обзор уязвимостей
 - ПО, подверженное уязвимостям
 - Уровни угроз и идентификаторы уязвимостей
 - Сопроводительное руководство
 - Часто задаваемые вопросы

Microsoft Active Protections Program (MAPP)

- Microsoft Active Protections Program (MAPP)
 - Программа для разработчиков систем безопасности
 - Участники заранее получают информацию об уязвимости из Microsoft Security Response Center (MSRC), до публикации ее в ежемесячном бюллетене
 - Участники используют эту информацию для обеспечения защиты клиентов сразу после публикации этих данных
- Trend Micro предоставляет защиту своим клиентам **в течение 2 часов** после публикации Microsoft Security Bulletins
 - Это дает возможность клиентам защитить уязвимые системы от атак
 - Системы могут быть пропатчены в течение следующего планового обслуживания

Deep Security



Брандмауэр

- Централизованное управление политиками брандмауэра на сервере
- Набор шаблонов для типовых корпоративных серверов
- Тщательная фильтрация: IP & MAC адреса, порты
- Охватывает весь диапазон IP-протоколов: TCP, UDP, ICMP, IGMP ...



Глубокий пакетный анализ

Включает IDS / IPS, Защиту веб приложений, управление приложениями

Проверяет входящий/исходящий трафик на:

- Протокольные отклонения
- Контент, сигнализирующий об атаке
- Нарушения политик.



Мониторинг целостности

- Мониторинг критических файлов, изменений в системе и реестре
- Критические файлы ОС и приложений (файлы, папки, ключи и значения реестра,

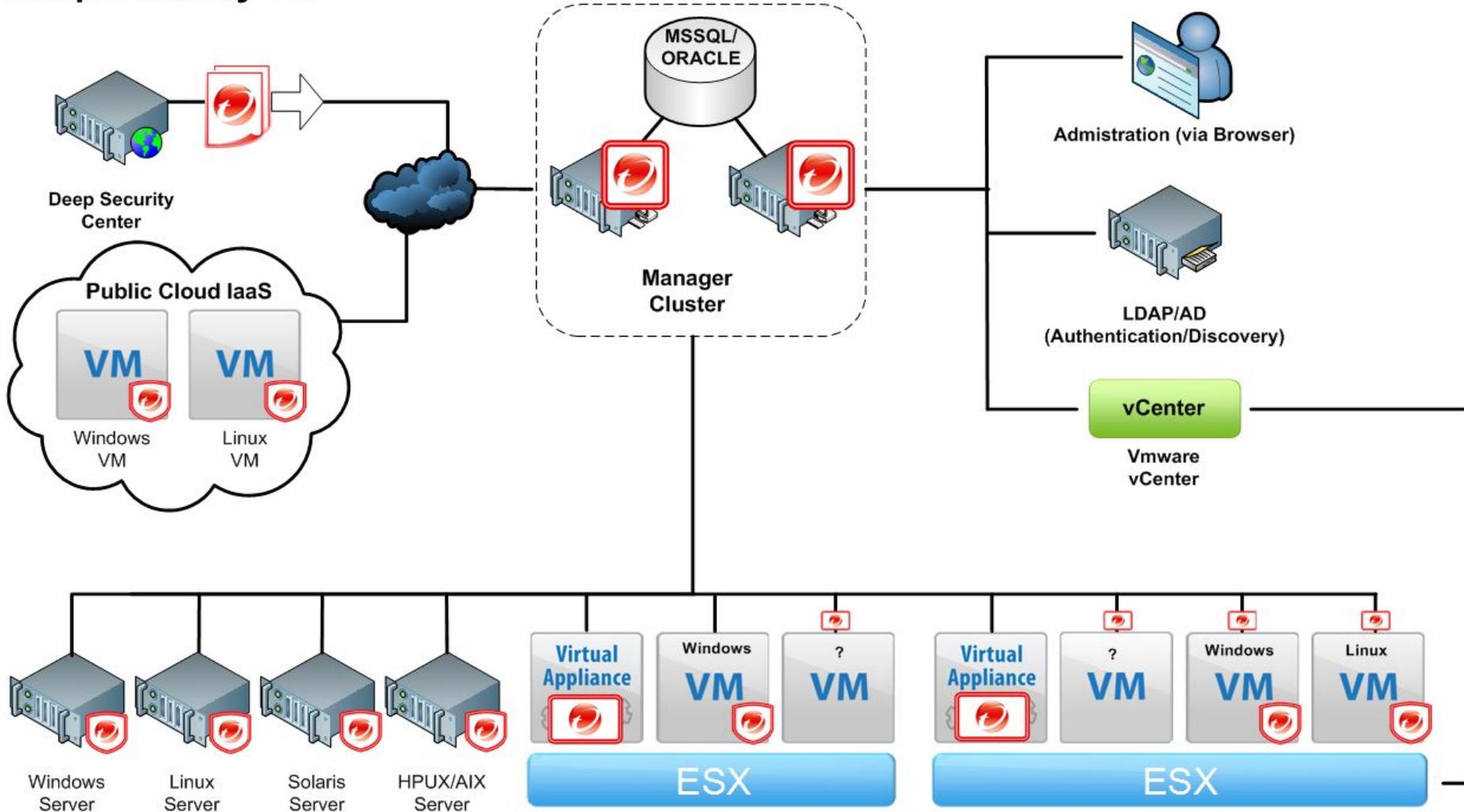


Анализ событий

- Собирает и анализирует записи журналов ОС и приложений для выявления событий системы ИБ.
- Оптимизация правил для выявления важных ИБ событий, скрытых среди множества записей журналов.

Архитектура Deep Security

Deep Security 7.0



Deep Security Manager (DSM)

- Система централизованного управления на базе веб-консоли
- Управление профилями
 - Система гибкого ролевого администрирования (например, делегирование полномочий)
 - Детальная отчетность
 - Рекомендации по сканированию
 - Настраиваемая панель мониторинга
 - Автоматизация планировки задач
 - Обновления ПО и безопасности
 - Интеграция (vCenter, SIEM, Active Directory)
 - Масштабируемость (множество узлов)



Согласованный подход

Согласованный подход

- Агент отключается
- Защита VM обеспечивается на уровне Virtual Appliance



* VMware vSphere 4
VMsafe API

Согласованный подход

- Каждый механизм имеет свои преимущества...

Агент на VM	<ul style="list-style-type: none">• Безопасность: дополнительные модули• Мобильность: vMotion и/или поддержка VM в облаке• Производительность: VM с повышенными требованиями к производительности
Virtual Appliance	<ul style="list-style-type: none">• Защищенность: применимость к любым VM• Совместимость: поддержка ОС, не поддерживаемых Агентом

Совместимость с Агентом - VMware 3.x, Citrix, and Hyper-V
Virtual Appliance – VMware vSphere 4 (ESX 4)

Deep Security Virtual Appliance

Модули защиты	Поддержка	Описание
Firewall	Да	<ul style="list-style-type: none">• Прозрачность в отношении VM• Политики безопасности могут быть применены к каждому NIC• Автоматически применяет политики FW, если Агент на VM не работает
Firewall & DPI	Да	<ul style="list-style-type: none">• Полная поддержка DPI (IDS/IPS, Web App protection, App Control)• Автоматически применяет политик DPI, если Агент на VM не работает
Мониторинг целостности	Нет	<ul style="list-style-type: none">• Нужен Агент на VM
Анализ событий	Нет	<ul style="list-style-type: none">• Нужен Агент на VM

Deep Security 7 – поддержка платформ



- Windows 2000, Windows 7
- 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)



Linux

- Red Hat 4, 5 (32 & 64 bit)
- SuSE 10,11



- VMware ESX 3.x (in-guest Agent)
- VMware vSphere 4 (Virtual Appliance & in-guest Agent)

- HP-UX 11i (11.31)
- AIX 5.3, 6.1

**Integrity
Monitoring
& Log Inspection
modules**

В СКОРОМ ВРЕМЕНИ..

SecureCloud* – защита доступа к данным в виртуализированных ЦОД



Новая модель безопасности — защита вычислительной цепочки

Все среды должны считаться ненадежными.



Когда вся цепочка защищена,

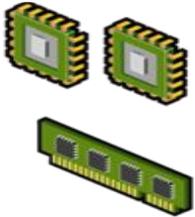
компоненты могут перемещаться

Больше нет привязки к поставщику услуг. Рентабельность общего хранилища растет.

Местоположение не играет роли. Виртуальные «соседи» не имеют значения.

ПОДРОБНОСТИ ПО DEEP SECURITY

vSphere 4 - VMsafe™ APIs



Проверка ЦП/Памяти

- Проверка отдельных сегментов памяти
- Знание состояния ЦП
- Применение политик через разделение ресурсов



Сетевое взаимодействие

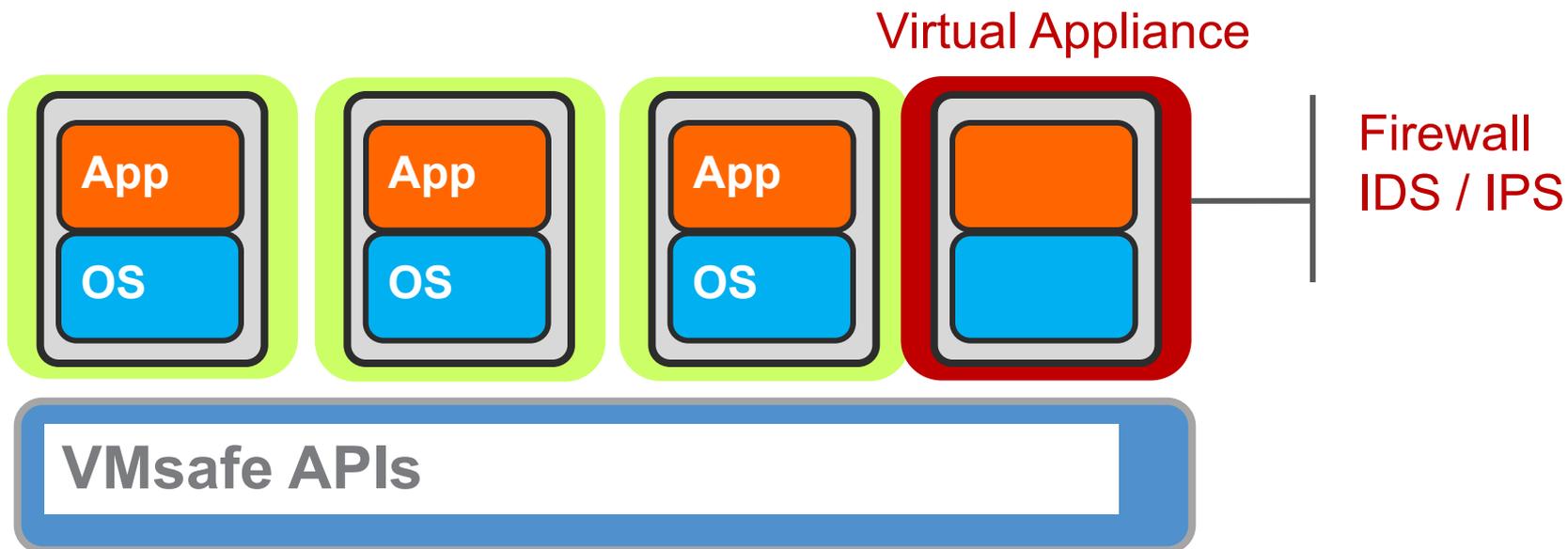
- Просмотр всего входящего/исходящего трафика на узле
- Перехват, просмотр, изменение и копирование входящего/исходящего трафика
- Защита как активная, так и пассивная



Хранилище

- Монтирование и чтение виртуальных дисков (VMDK)
- Проверка записи/чтения всего потока данных на устройствах хранения
- Прозрачное подключение при работе со стеком ESX Storage

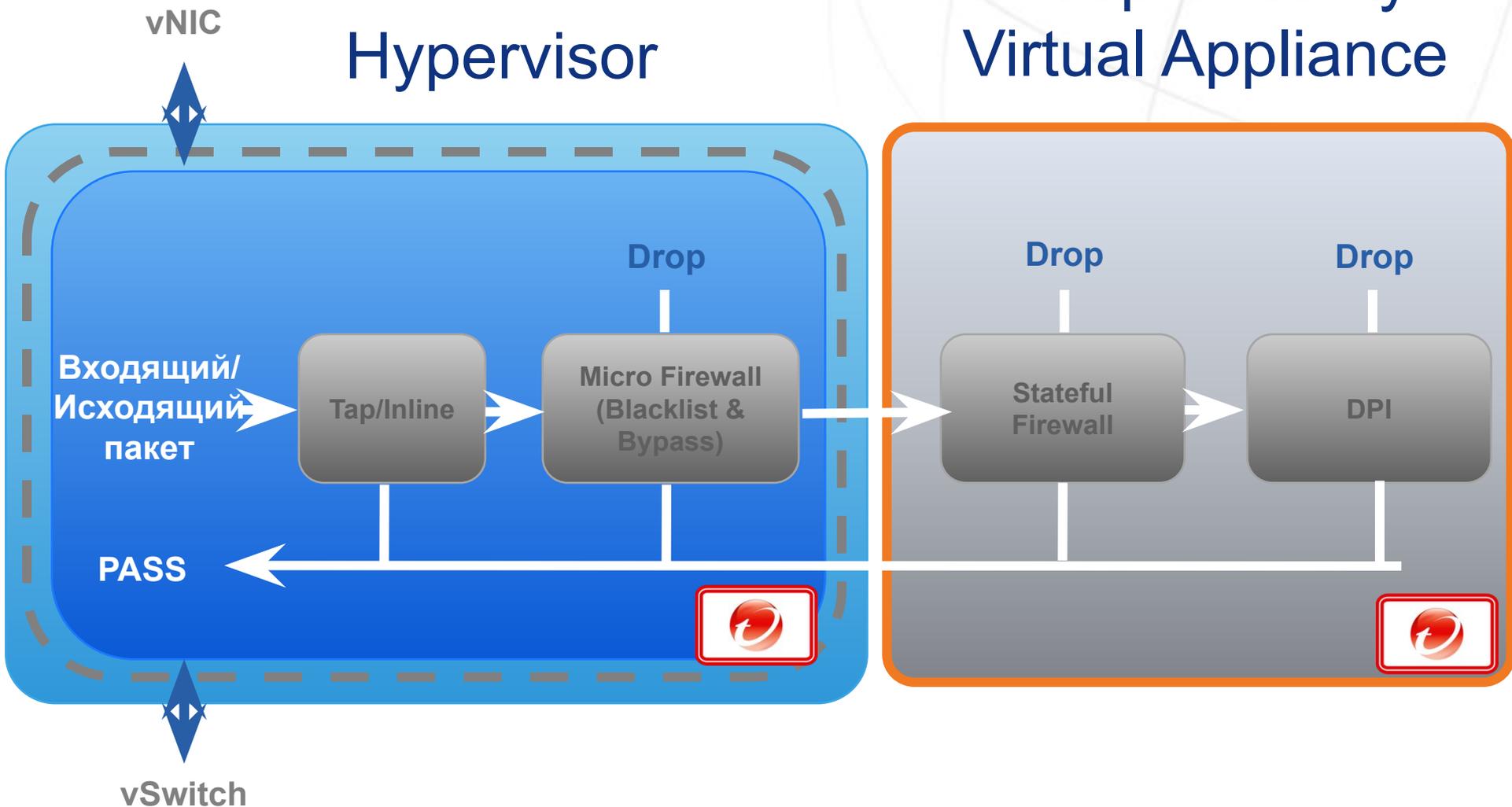
Deep Security Virtual Appliance (совместно с vSphere 4 VMsafe)



- Защита VM через проверку виртуальных компонент
- Защищает VM извне, не требует никаких изменений в VM
- Полная интеграция с vMotion, Storage vMotion, HA с учетом специфики.
- Интеграция с Virtual Center для выявления VM и синхронизации

Внутренняя архитектура

Deep Security Virtual Appliance



ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ DEEP SECURITY 7...

Тэгирование событий

- Система многоцелевого управления событиями
- Не изменяет и не удаляет оригинальные события
- Сценарии:
 - Снижение загруженности (меньшее кол-во событий для анализа; напр., автотэгирование патчей или событий сканера уязвимостей)
 - Алгоритм прохождения событий (прогон событий через оценочные проверки)
 - Выборочные события (отчеты по определенным комбинациям тэгов, как например 'возможна 1 брешь')
 - Интеграция со сторонними системами (системы на основе «тикетов», контроль изменений)



Улучшенное управление событиями

- **Тэги́рование событий**

- Автоматизированное тэги́рование событий по определенному критерию
- Тэги по умолчанию или собственные
- Возможно тэги́рование отдельного события, похожих событий или всех будущих событий (напр., событий похожих на проверку орфографии MS Word)
- Существенно снижает объем анализируемых данных
- Можно по-разному отображать информацию по событиям, на панели мониторинга и при формировании отчетов

- **Тэги можно применять к:**

- Брандмауэру
- DPI
- Мониторингу целостности
- Проверке журналов
- Системным событиям

Тэгирование событий



Потоковые
источники
событий



Доверенные
источники
событий



Админ включил
тэгирование



Узел автоматизированного
тэгирования событий

- События
- Брандмауэр
 - DPI
 - Мониторинг целостности
 - Проверка журналов
 - Системные

Тэгирование событий в Deep Security

Специальные

- События
- Панели мониторинга
- Отчеты

Применены к

- Отдельным событиям
- Схожим событиям
- Последующим схожим событиям

Применение тэгов событиям

The screenshot displays the Trend Micro Deep Security console interface. The main window shows the 'Firewall Events' section with a table of events. A 'Tag Wizard' dialog box is open in the foreground, allowing the user to add tags to selected events. The dialog shows 'Gen' entered in the search field, with 'Generic Attack' and 'Generic Scan' as suggestions. The '3 Selected Firewall Events' radio button is selected. The background table lists various events with columns for Time, Host, Event Origin, Reason, Tag(s), Action, and Rate.

Trend Micro Deep Security

Signed In As: admin | Help | Sign Out

Firewall Events

View Export... (No Grouping)

Period: Last Hour

Host: All Hosts

Time	Host	Event Origin	Reason	Tag(s)	Action	Rate
August 27, 2009 09:20:14	workstation_hwaerr	Agent	Out Of Allowed Policy	Suspicious	Deny	50
				Under Investigation	Deny	500
			Rule: Restricted Interf	Under Investigation	Deny	100
			CK	Under Investigation	Detect Only: I	50
			Rule: Off Domain Enfo	Suspicious Under Investigation	Detect Only: I	250
			Rule: Restricted Interf	Under Investigation	Deny	100
			Allowed Policy	Under Investigation	Deny	500
			Sequence	Suspicious Under Investigation	Deny	250
			Allowed Policy	Under Investigation	Deny	250
			CK	Under Investigation	Deny	125
			Allowed	Under Investigation	Detect Only: I	500
			Tags	er (Ignore)	Deny	50
			Allowed	er (Ignore)	Deny	50
			Sequenc	er (Ignore)	Deny	500
			Allowed		Deny	50
			Allowed Policy	Suspicious	Detect Only: I	250
			Rule: Log Everything	Suspicious	Log Only	100
			Rule: Deny Internal IP	Suspicious	Deny	100
			Allowed Policy	Internal Vulnerability Scanner (Ignore)	Deny	375
			Allowed Policy	Internal Vulnerability Scanner (Ignore)	Detect Only: I	250
			Rule: Restricted Interf		Deny	500

Tag Wizard - Mozilla Firefox

http://jfooster-desktop:8080/WebClient/TagWizard.screen?startingPage=AddTags&type=2

Add Tag(s):

Gen

- Generic Attack
- Generic Scan

3 Selected Firewall Events

Also apply to similar Firewall Events

Include Advanced Options

< Back Next > Cancel

Done

Item 1 to 100 of 365

19 Alerts

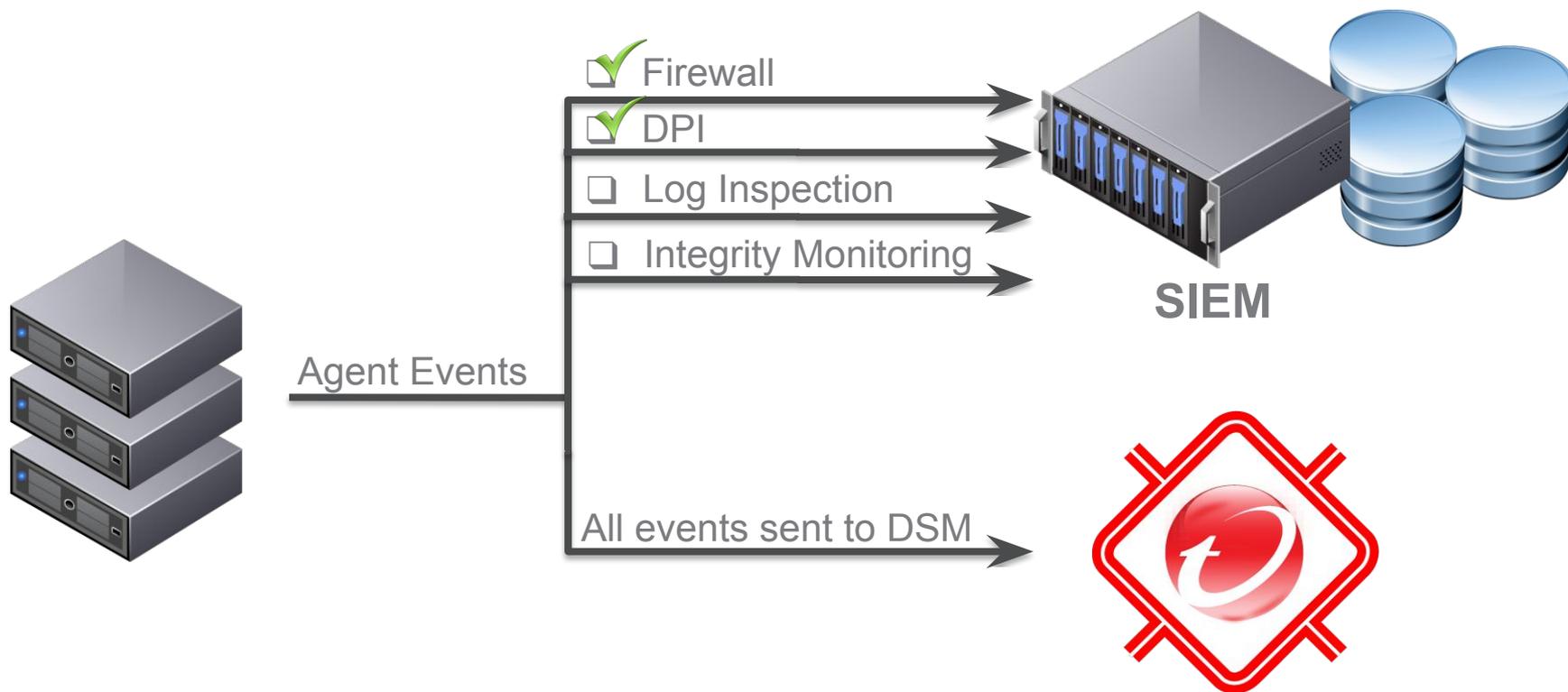
Улучшено управление

- **Мониторинг целостности «на изменение»**
 - Мониторинг изменений системных файлов (файлов и папок) и отчет по этим изменениям в **реальном времени**
 - Данные включены в событие OnChange :
 - Дата и время изменений
 - Измененный или созданный объект
- **Расширенные настройки правил**
 - Настройка правил для Мониторинга целостности и Проверки журналов упрощена за счет GUI
- **Расширены возможности Syslog**
 - Добавлена возможность перенаправления данных через Syslog на основе модулей защиты
 - напр., отправлять события брандмауэра и DPI, исключая события Мониторинга целостности и Проверки журналов

Улучшена интеграция с SIEM

- **Syslog**

- Возможность вкл/выкл поддержки Syslog для каждого модуля Deep Security (FW, DPI, IM, LI) на уровне агента



Расширена масштабируемость

- Улучшена масштабируемость и производительность DSM
 - Добавлена поддержка 64-битных Windows 2003 & 2008
 - Требуется поддержка 64-битного оборудования

	32-битный DSM	64-битный DSM
Виртуально адресуемая память / процесс в пользовательском режиме	2ГБ	4 ГБ
Ограничения физических объемов памяти	4ГБ	32ГБ – Windows 2008 Server Standard
		2 ТБ – Windows 2008 Server Enterprise

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

NIKOLAY_ROMANOV@TRENDMICRO.COM
+7 (926) 202-76-36

ИЛИ

RUSSIA@TRENDMICRO.COM