TREND MICRO™ Securing Your Web World

Защита виртуальных систем – сейчас и в ближайшее время

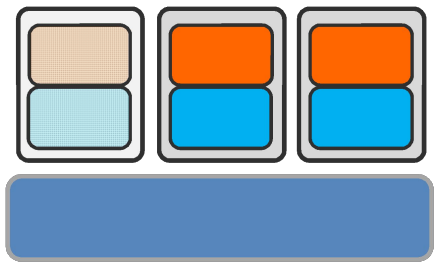
Николай Романов • Технический консультант

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



TREND MICRO

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-Mal ware	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		

Nemertes Research 2009

TREND MICRO

DEEP SECURITY 7.0 - VIRTUALIZATION SECURITY

TREND MICRO

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, PostgresSQL, 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

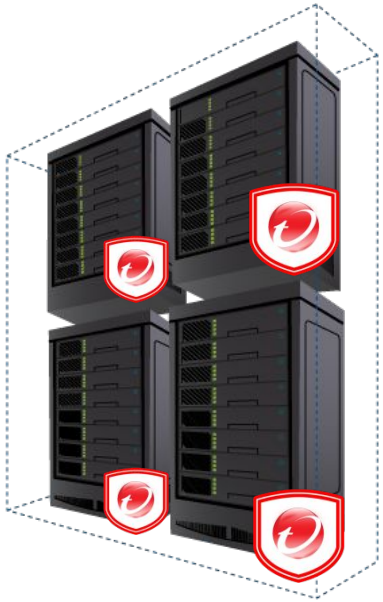
TREND MICRO

Защита серверов/приложений:

Microsoft
solaris
Linux
vmware
AIX
hp
HP-ux

Физические

Виртуальные



Облачные

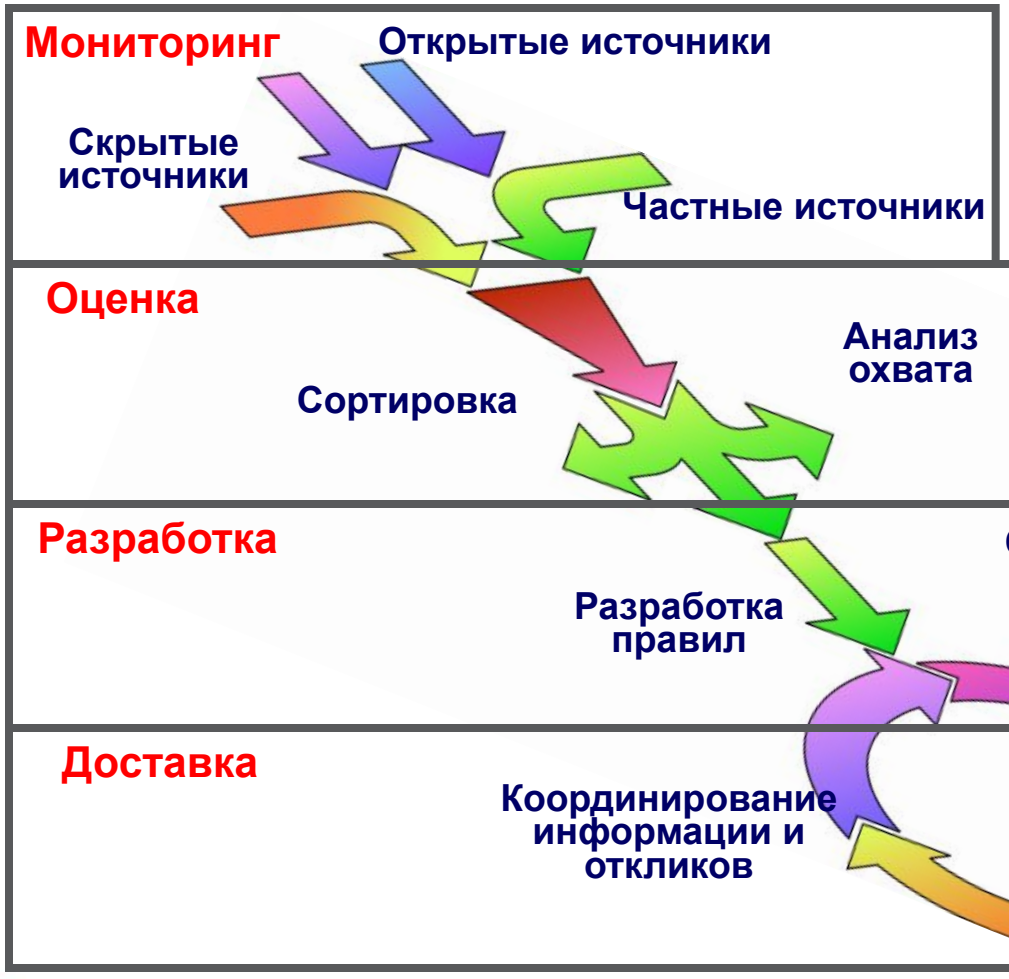
- Глубокий пакетный анализ (DPI)
- Брандмауэр
- Мониторинг целостности
- Анализ событий журналов
- Антивирус

В рамках DSVA

Q3/2010

TREND MICRO

Реактивная защита



Автоматизированный мониторинг

- SANS
- CERT
- Консалтинг вендоров
- Bugtraq
- VulnWatch
- PacketStorm
- Securiteam
- Telus (Assurent)

Сортировка приложений

- Широкий спектр охватываемых серверных, настольных и специализированных приложений
- Рекомендации по каждому правилу

Разработка правил

- Эксплойт/Атака
- Уязвимость
- Уловки/Аномалии/Трафик

Отклик

- Автоматизировано
- В течение нескольких часов

TREND MICRO

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 2ой 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

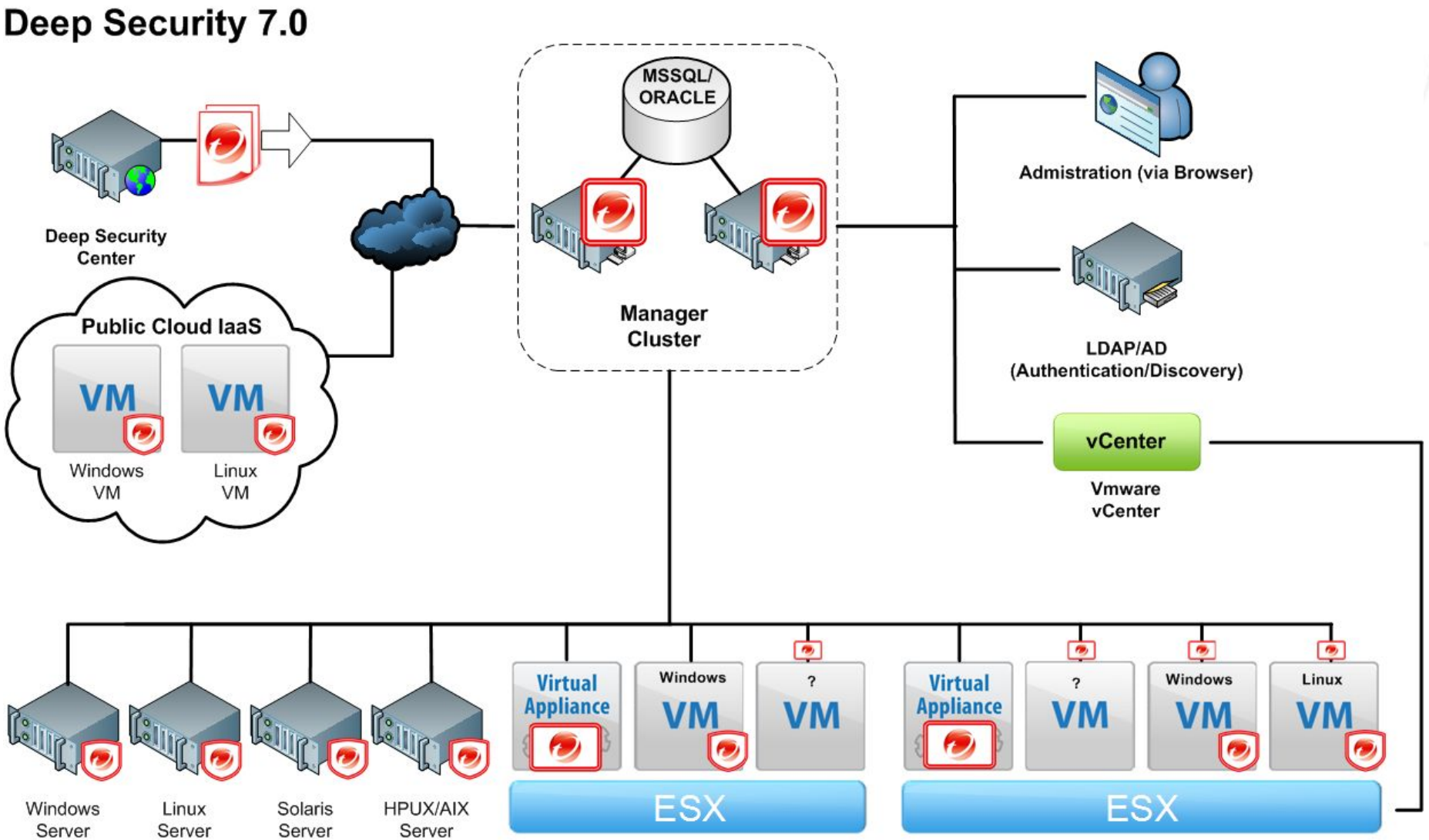
- Мониторинг критических файлов, изменений в системе и реестре
- Критические файлы ОС и приложений (файлы, папки, ключи и значения реестра,

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.

TREND MICRO

Архитектура Deep Security



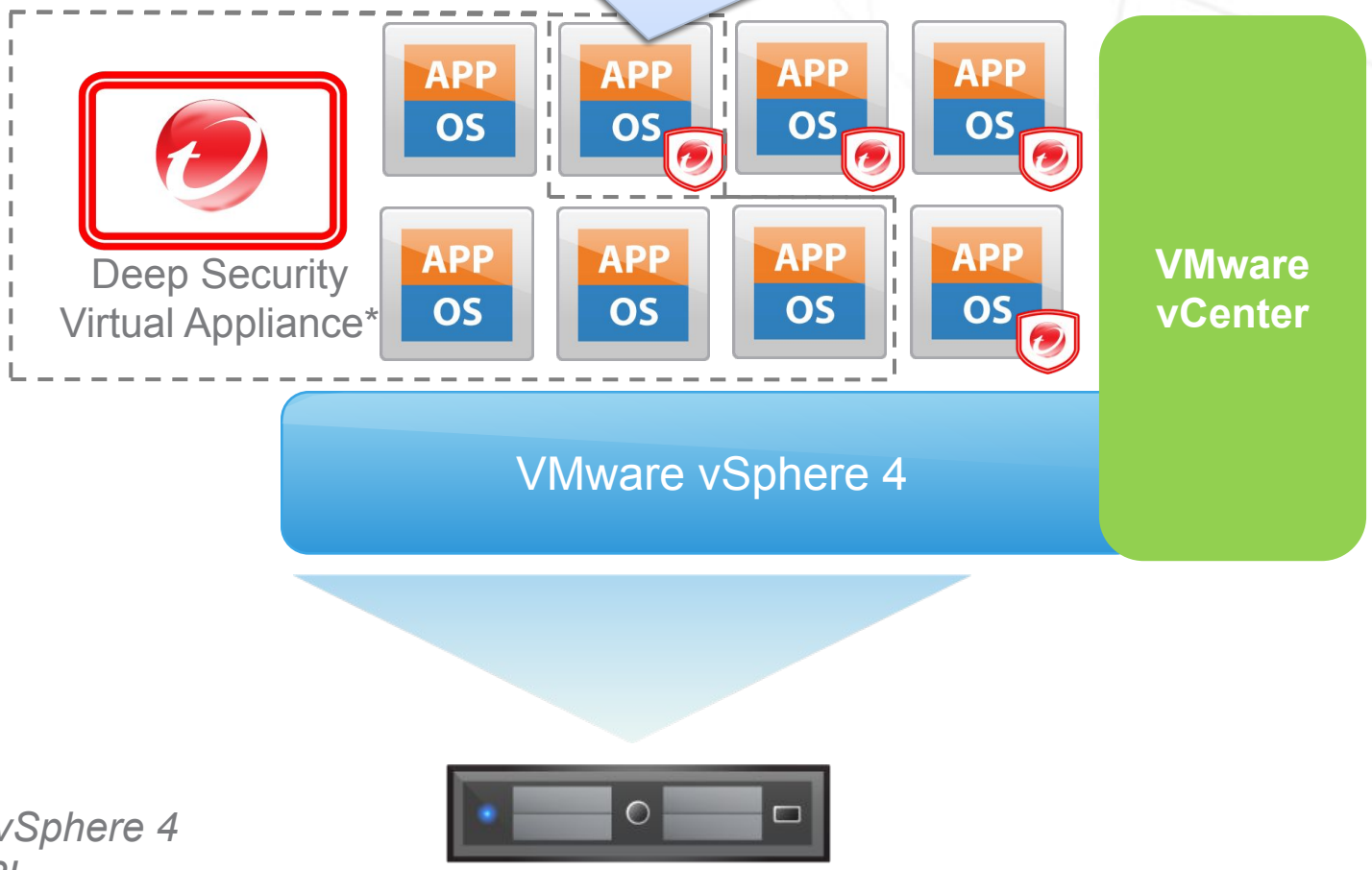
Deep Security Manager (DSM)

- Система централизованного управления на базе веб-консоли
- Управление профилями
  - Система гибкого ролевого администрирвоания (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)

TREND MICRO

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	• **Безопасность:** дополнительные модули • **Мобильность:** vMotion и/или поддержка VM в облаке • **Производительность:** VM с повышенными требованиями к производительности
Virtual Appliance	• **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	• 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	• Полная поддержка DPI (IDS/IPS, Web App protection, App Control) • Автоматически применяет политик DPI, если Агент на VM не работает
Мониторинг целостности	Нет	• Нужен Агент на VM
Анализ событий	Нет	• 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)

- 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

Много клиентов на одном физическом сервере — возможность атаки через гипервизор

Неважно: границы моего виртуального сервера защищены брандмауэром.

Общая сеть внутри брандмауэра

Неважно: работа в локальной сети ведется как в общедоступной.

Общий брандмауэр — наименьший общий знаменатель — менее детальный контроль

Неважно: работа в локальной сети ведется как в общедоступной.

Легко копируемые образы машин: у кого еще есть копия вашего сервера?

Неважно: без меня можно загрузить мой сервер, но разблокировать мои данные нельзя.

Общее хранилище: защищает ли сегментация клиентов от атак?

Неважно: мои данные зашифрованы (никаких хлебных крошек).

SecureCloud* – в состоянии бета-тестирования с апреля 2010 по август 2010. Подробности и возможность принять участие в тестировании: http://trendbeta.com

Новая модель безопасности — защита вычислительной цепочки

Все среды должны считаться ненадежными.

Когда вся цепочка защищена,

компоненты могут перемещаться

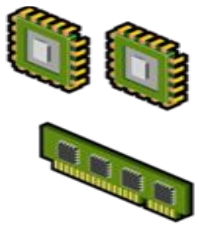
Больше нет привязки к поставщику услуг. Рентабельность общего хранилища растет.

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

TREND MICRO

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

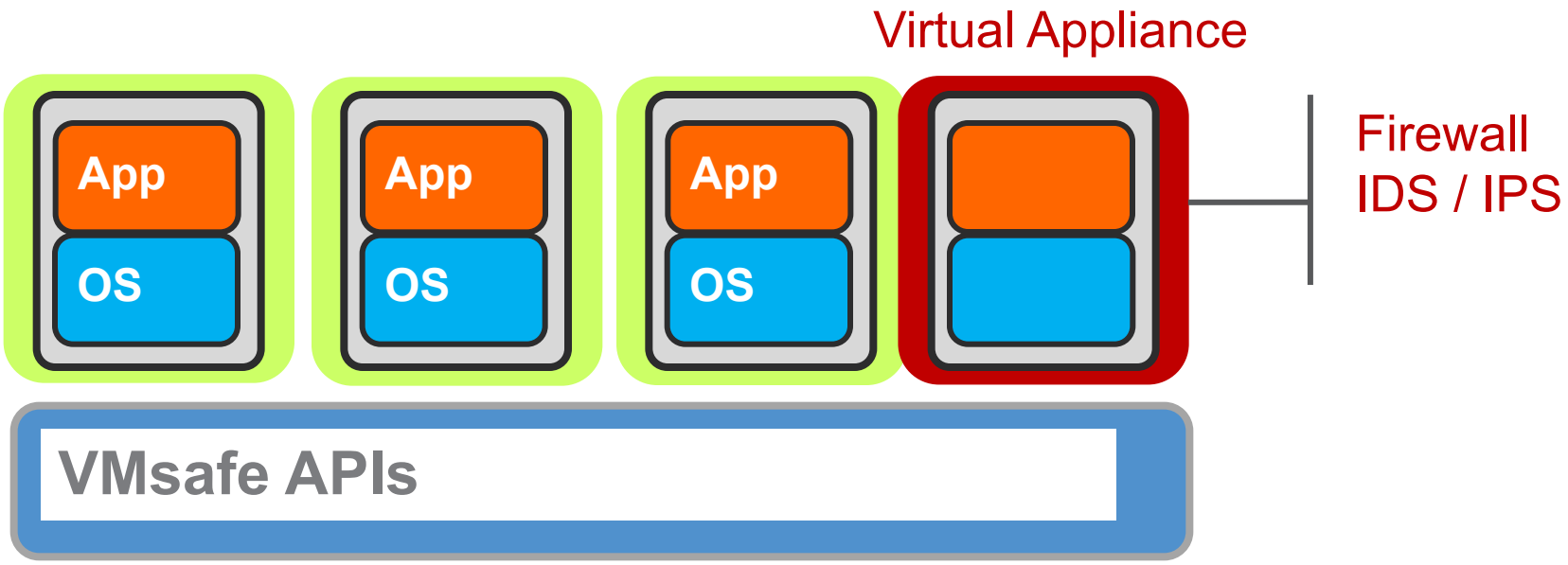
- Просмотр всего входящего/исходящего трафика на узле
- Перехват, просмотр, изменение и копирование входящего/исходящего трафика
- Защита как активная, так и пассивная

Хранилище

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

TREND MICRO

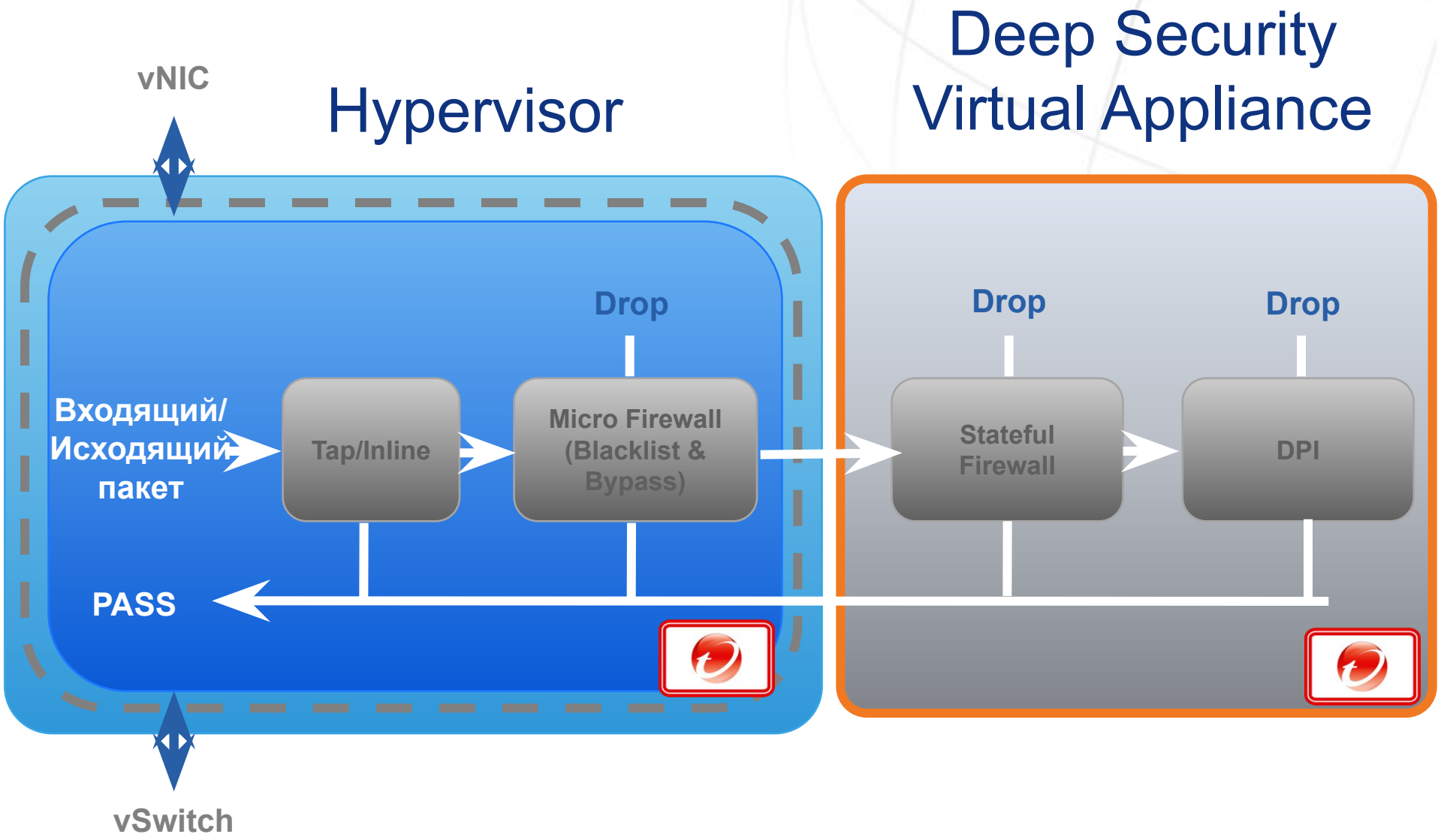
Deep Security Virtual Appliance (совместно с vSphere 4 VMsafe)



- 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

TREND MICRO

Внутренняя архитектура



ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ DEEP SECURITY 7…

TREND MICRO

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)

TREND MICRO

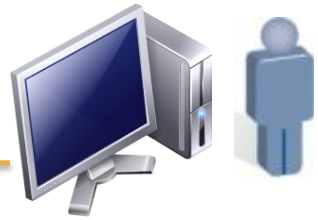
Улучшенное управление событиями

- **Тэгирование событий**
  - Автоматизирование тэгирование событий по определенному критерию
  - Тэги по умолчанию или собственные
  - Возможно тэгирование 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



Admin включил тэгирование

Узел автоматизированного тэгирования событий

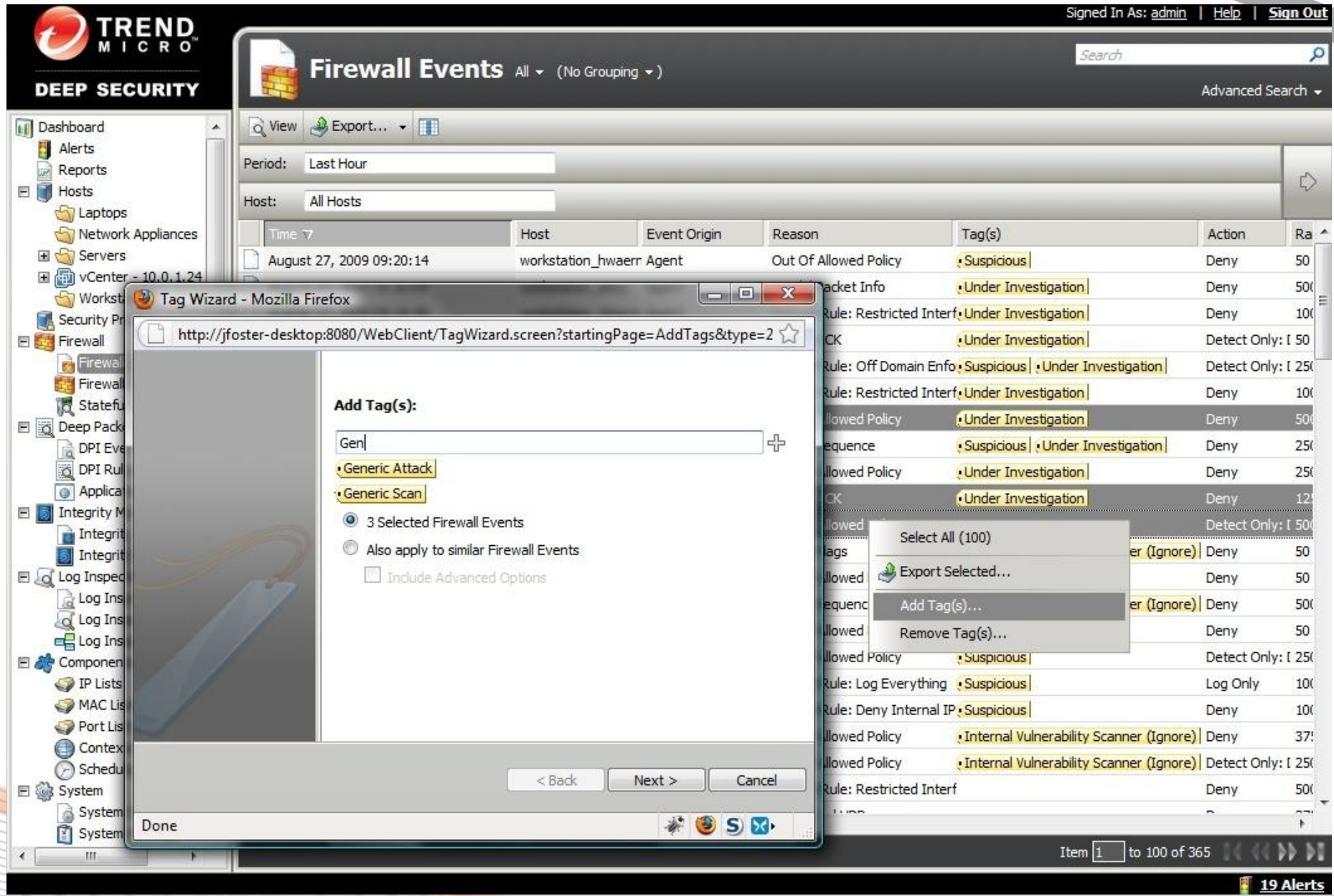
События
- Брандмауэр
- DPI
- Мониторинг целостности
- Проверка журналов
- Системные

Тэгирование событий в Deep Security
Специальные
- События
- Панели мониторинга
- Отчеты

Применены к
- Отдельным событиям
- Схожим событиям
- Последующим схожим событиям

TREND MICRO

Применение тэгов событий

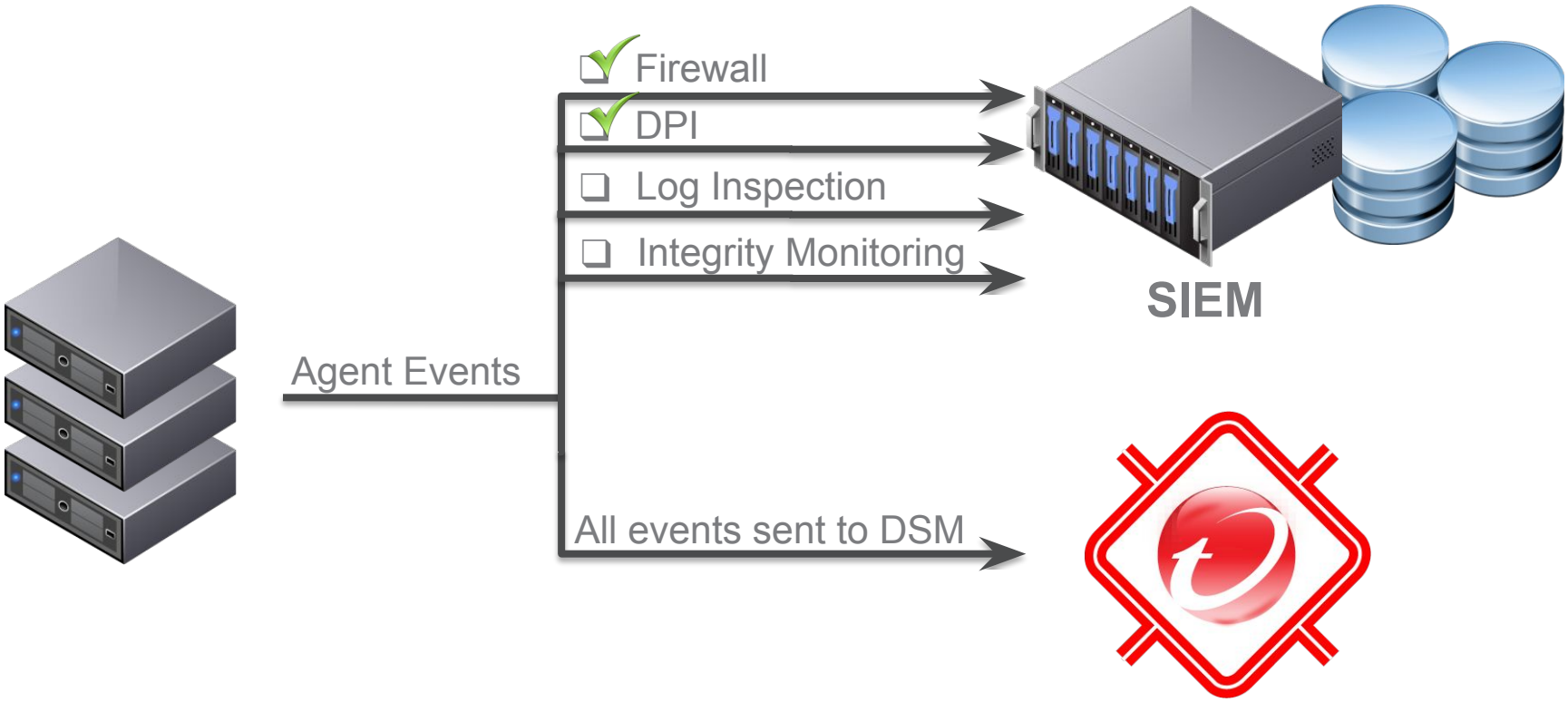


Улучшено управление

- **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



TREND MICRO

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

TREND MICRO