5NINE SOFTWARE | Защита и управление Microsoft Hyper-V
№1 в мире

Развертывание безопасности как услуги (SECaaS) на платформе Microsoft Cloud OS/Azure Pack

Юрий Бражников
Глава российского офиса
5nine Software

О 5nine Software

- Российская разработка средств управления и обеспечения безопасности виртуализации. Microsoft Gold Datacenter и ISV Partner. Основана в 2009
- Более 80.000 клиентов различных размеров по всему миру, во всех отраслях экономики
- №1 разработчик решений по обеспечению безопасности и управлению Hyper-V
  - 5nine Cloud Security – безагентная безопасность Hyper-V, System Center и Azure Pack
  - 5nine Manager – комплексное управление и мониторинг кластеров Hyper-V для предприятий малого и среднего бизнеса
  - 5nine V2V Easy Converter – решение по бесплатной миграции ВМ с VMware на Hyper-V

www.5nine.ru

Microsoft Partner
Gold Datacenter

CERTIFIED FOR Windows Server 2008 R2

Windows Server 2012 Certified

Windows Server 2012 R2 Certified

DATALINE Member of INLINE Technologies Group | HSBC | KPOK | Goldman Sachs | hp

ING | verizon | GM | Газпром трансгаз Югорск | Kodak | GMX

MVP Microsoft® Most Valuable Professional

5nine Software реализовало проекты по защите инфраструктуры и предоставлению SECaaS в десятках ЦОД по всему миру.

Старые технологии перестают защищать инфраструктуру

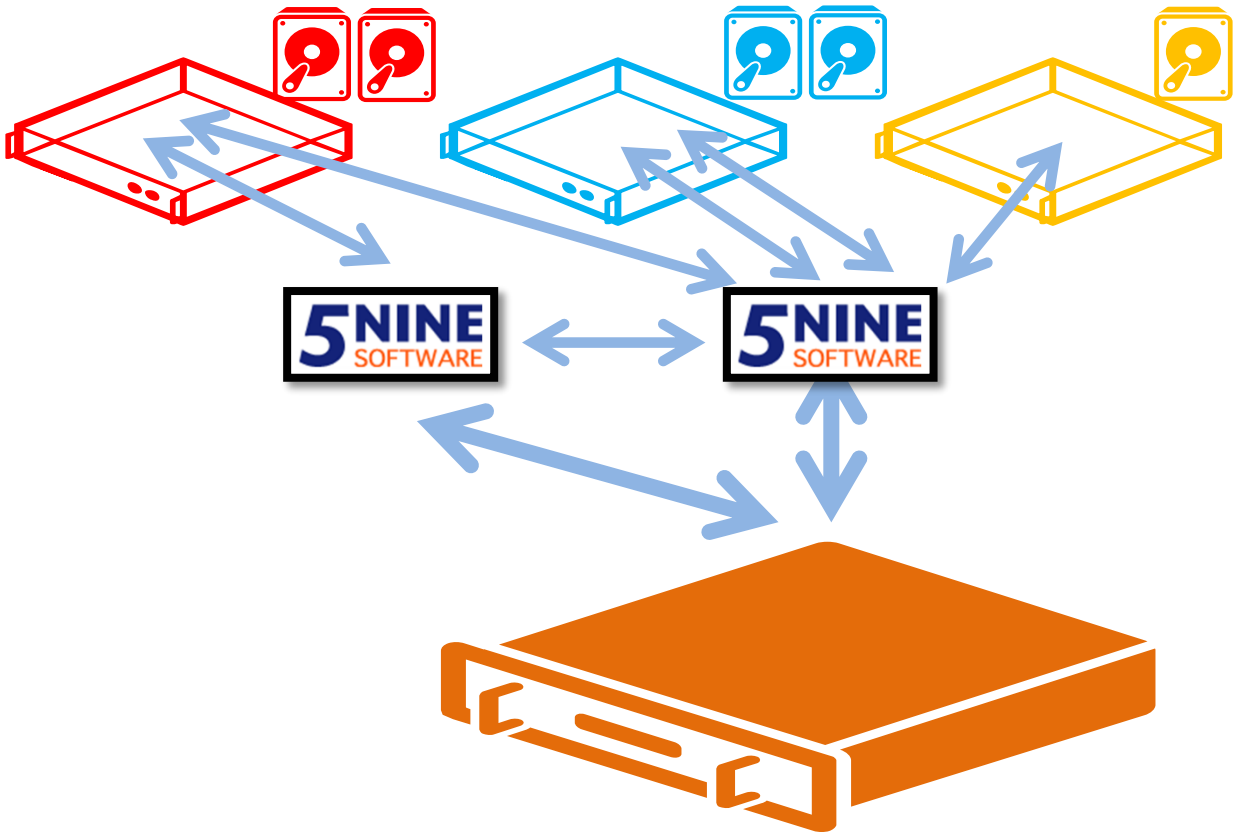
«… классические антивирусы обречены на неудачу… выпуск локальных решений для защиты персональных компьютеров -не прибыльный бизнес»,
«…компании необходимо это учитывать в своей стратегии».

Брайан Дай (Brian Dye)
Старший Вице-президент Symantec по информационной безопасности
Wall Street Journal, 09.2014

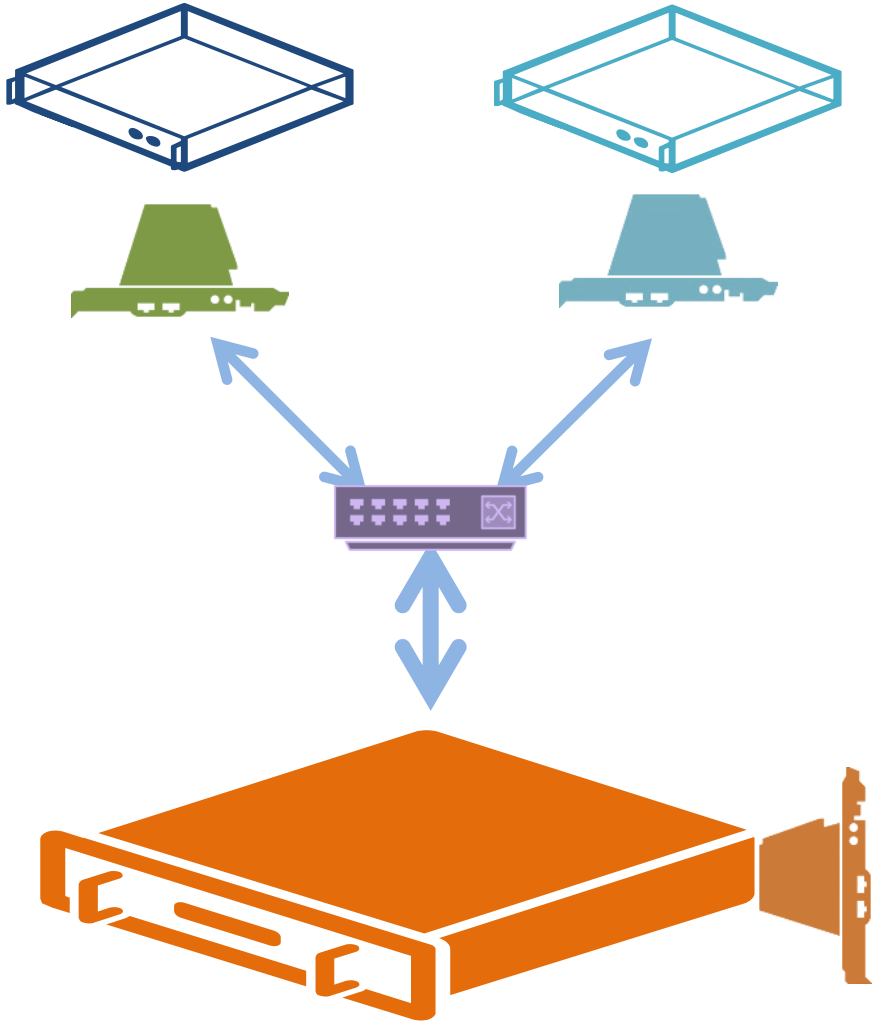
- Классические антивирусные технологии были нацелены в первую очередь на защиту рабочих мест, ПК
- Основной целью хакеров теперь являются ЦОД, а не отдельные ПК и почтовые рассылки
- Существенно выросла база сигнатур и ее размер влияет на производительность ИС
- Ресурс физических серверов ограничен и делится между ВМ.

Автоматическая и немедленная защита виртуальной среды

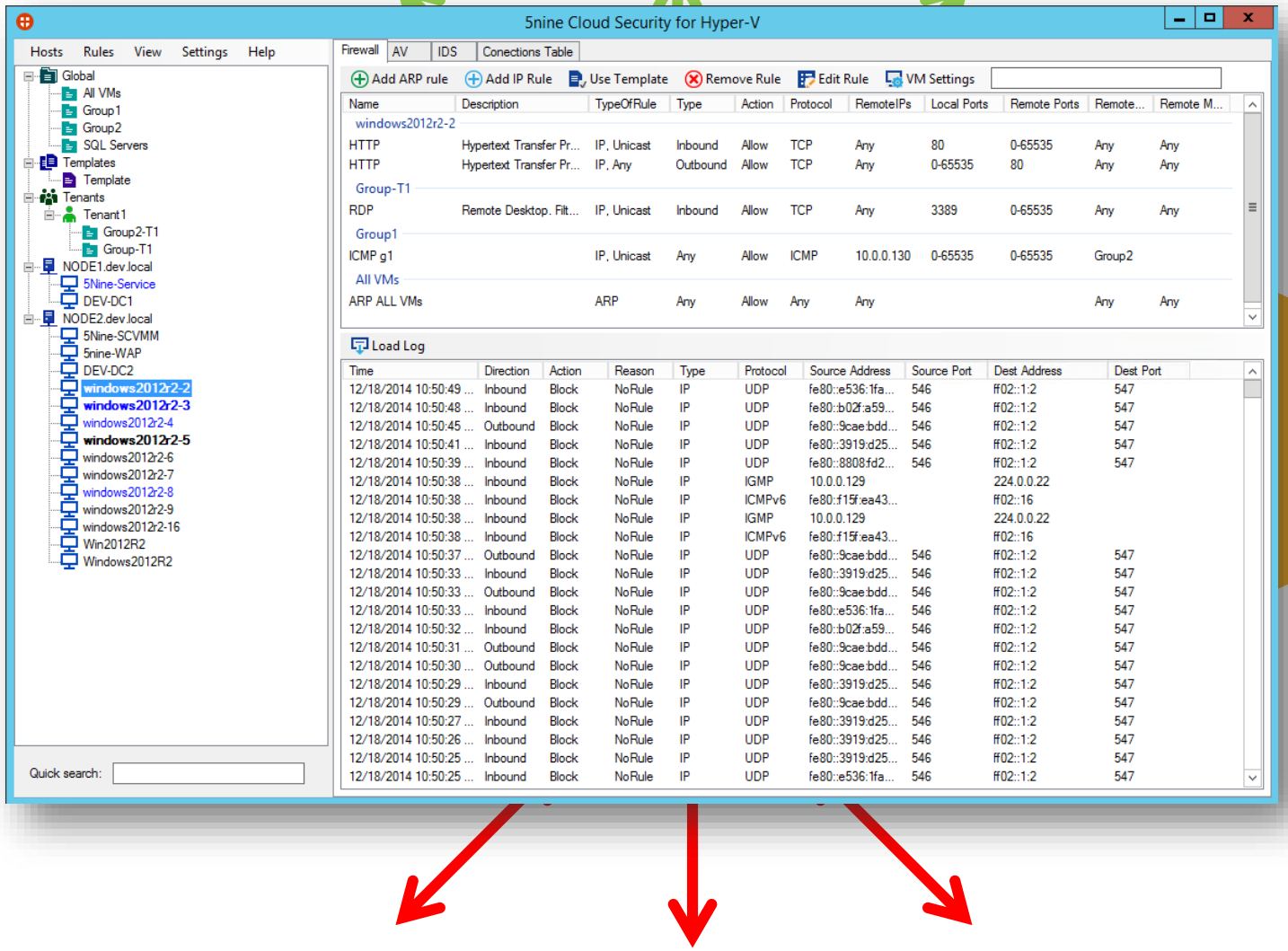
- Обеспечение безопасности для виртуальной среды отличается от физической
- Совместное использование ресурсов небезопасно
- Обеспечить безопасность виртуальной среды при помощи традиционного “endpoint protection” невозможно
  - Требуется установка
  - Требуется время
  - Потребляет много ресурсов
- Виртуальные среды динамичны
  - ВМ
  - Виртуальные диски
  - Виртуальные сети
  - Виртуальные коммутаторы

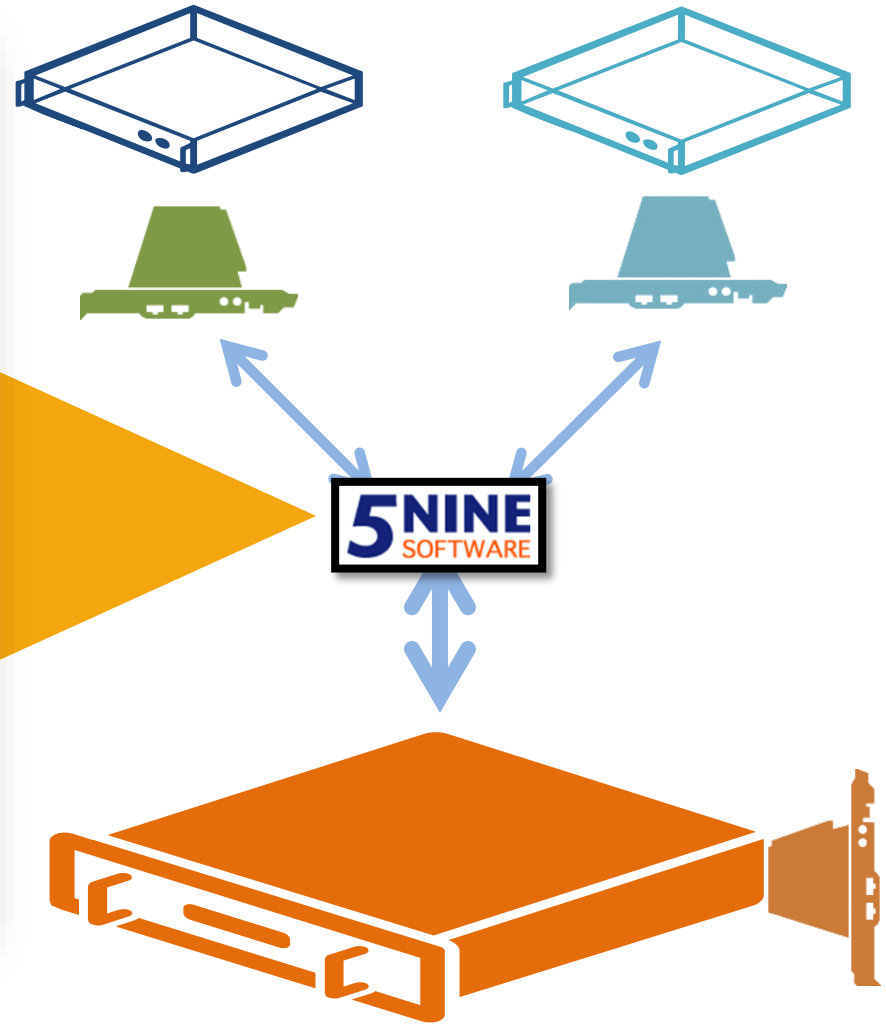


Как обеспечивается безопасность на уровне гипервизора



Защита на уровне хоста Hyper-V при помощи МСЭ, Антивируса и IDS

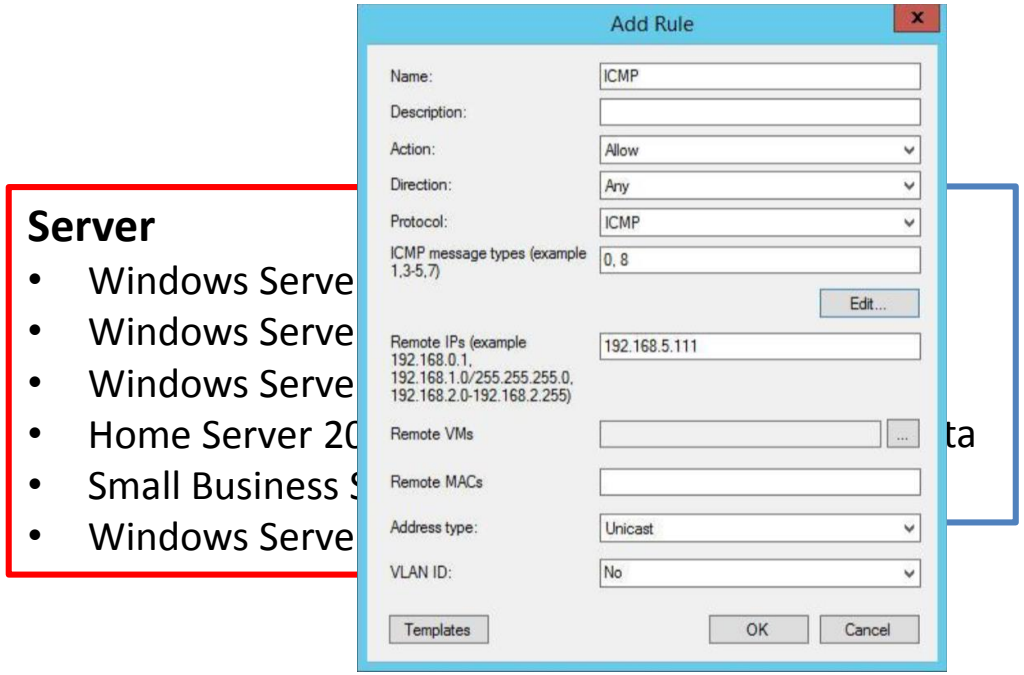




Best Practice

Используйте единый МСЭ для всех ВМ

- Управляйте трафиком на уровне сети
  - TCP, UDP, GRE, ICMP, IGMP, etc.
  - DPI для HTTP и DNS



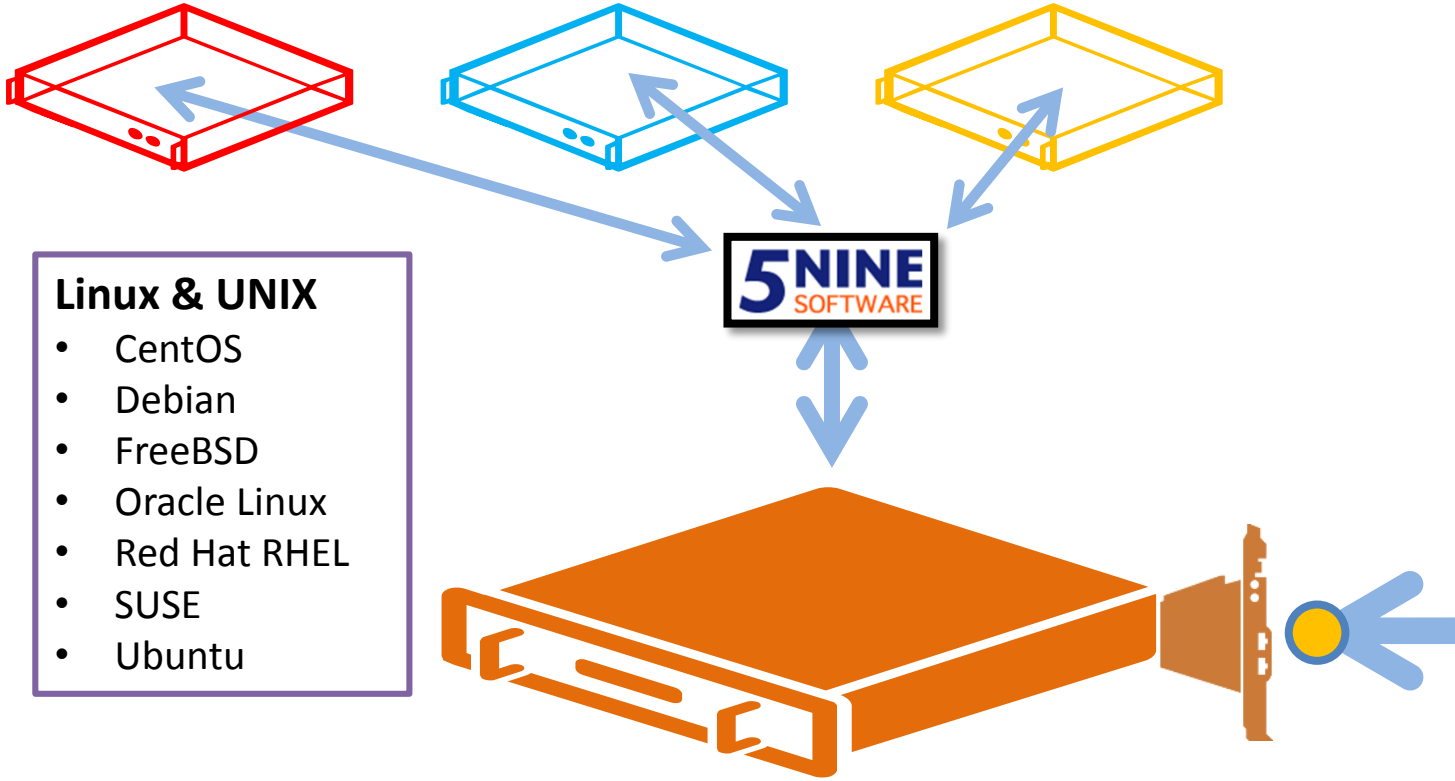
Server

- Windows Serve
- Windows Serve
- Windows Serve
- Home Server 20
- Small Business S
- Windows Serve

ta

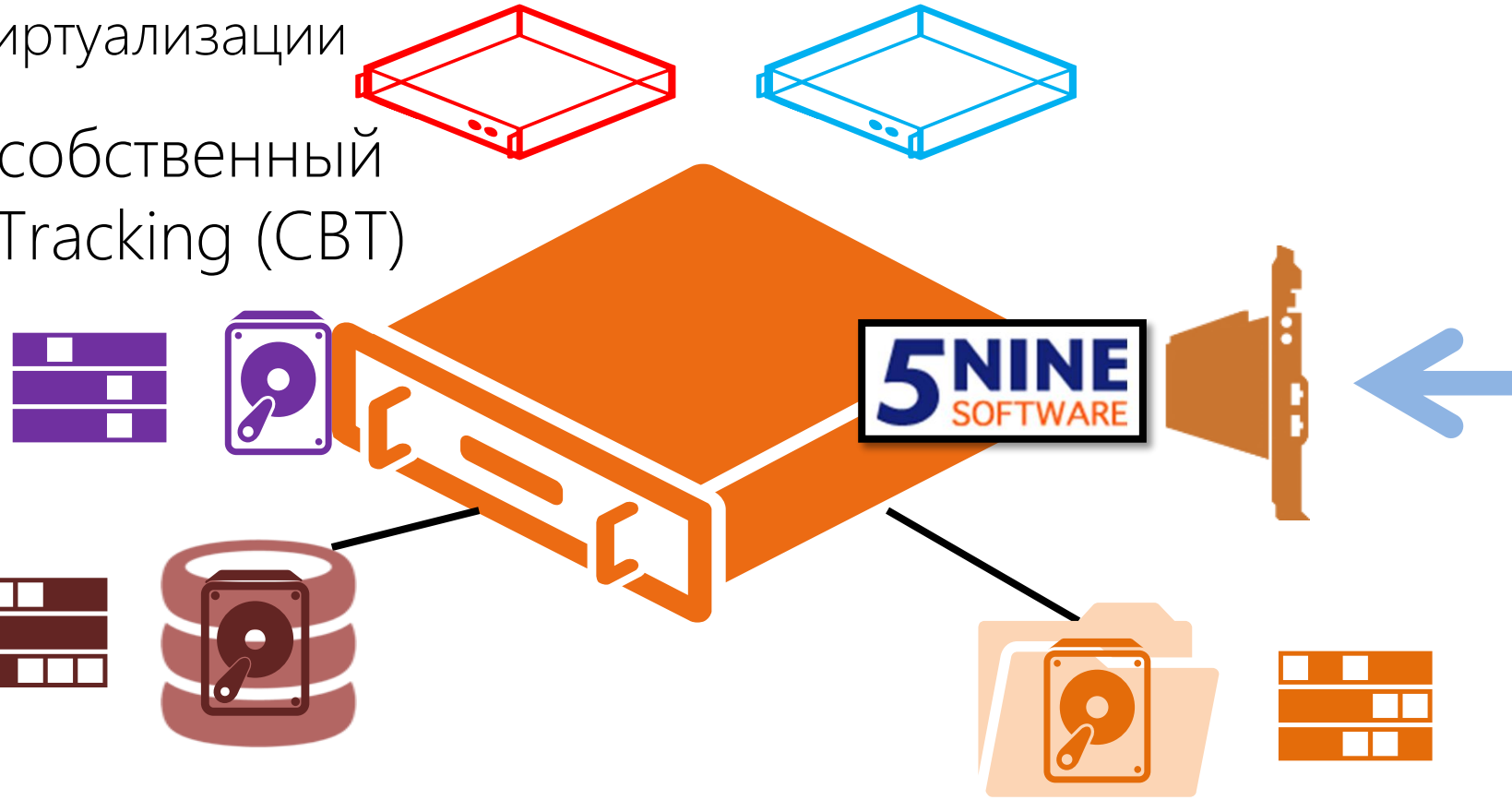
Linux & UNIX

- CentOS
- Debian
- FreeBSD
- Oracle Linux
- Red Hat RHEL
- SUSE
- Ubuntu



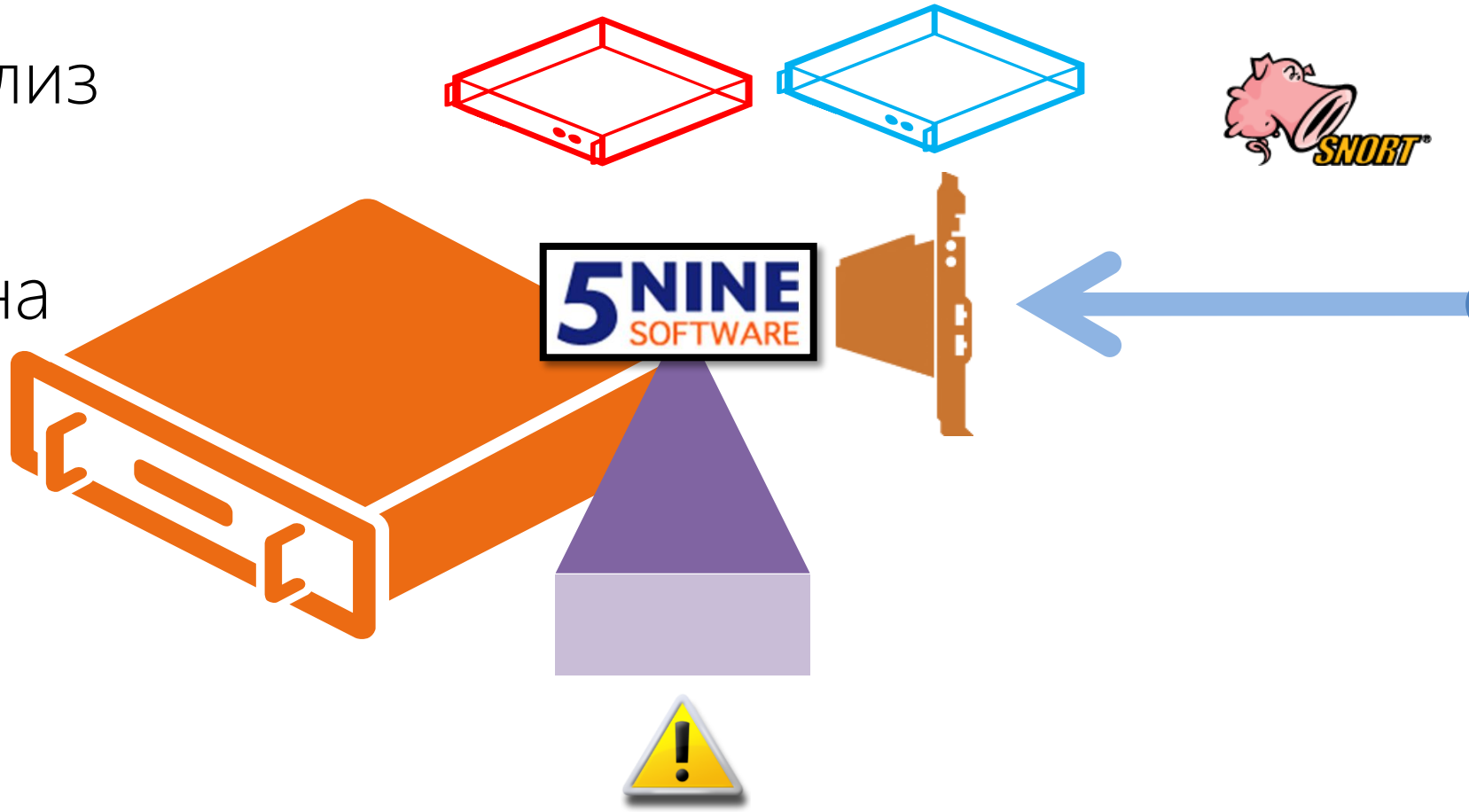
Быстрое AB сканирование без влияния на производительность

- Агентное сканирование приводит к “антивирусным штормам”
  - Понижает производительность всех ВМ на хосте
  - Уменьшает плотность виртуализации
- 5nine использует свой собственный драйвер Change Block Tracking (CBT)
  - Сканирует только изменившиеся блоки на диске
  - Скорость сканирования до 70x



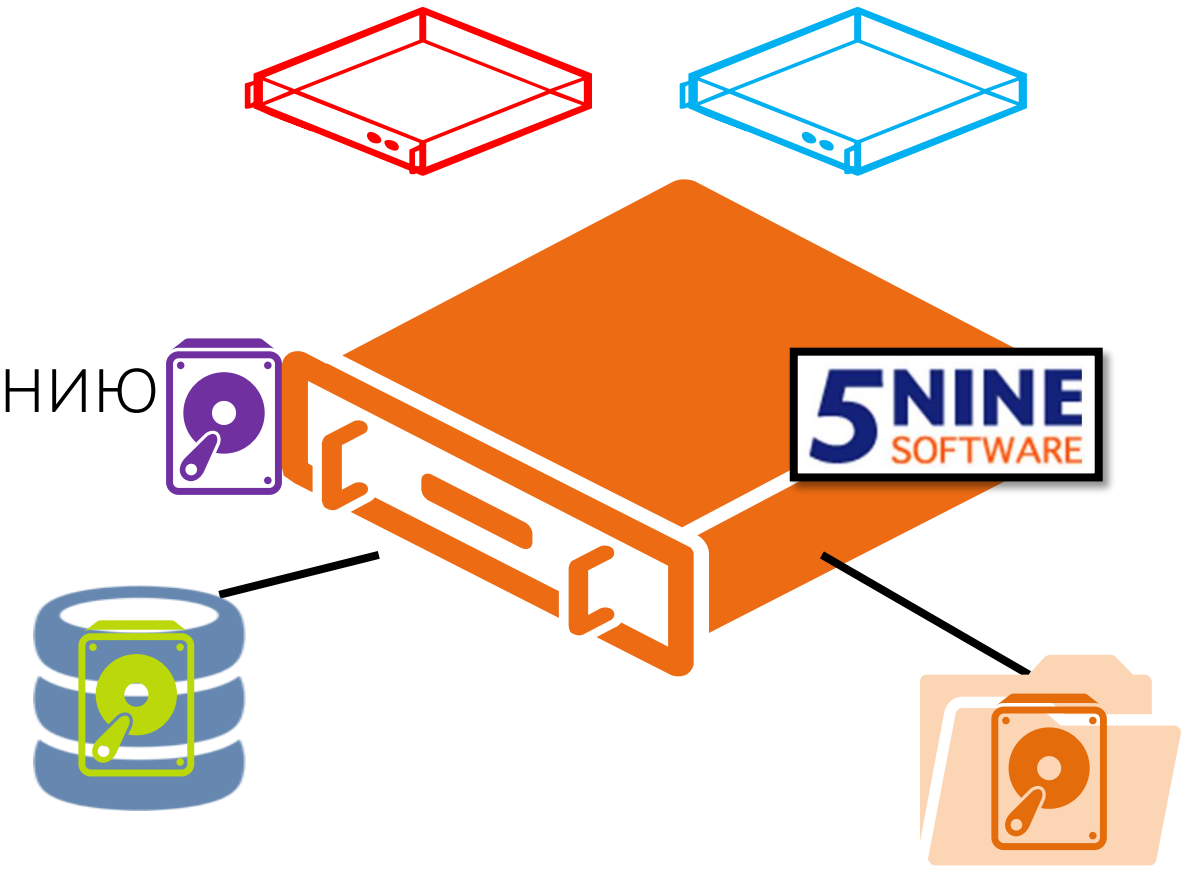
Активное обнаружение угрозы вторжения

- Немедленное обнаружение угрозы при помощи Snort for Buisness
- Эвристический анализ
- Автоматическое уведомление админа
  - Email
  - PowerShell
  - Логи событий



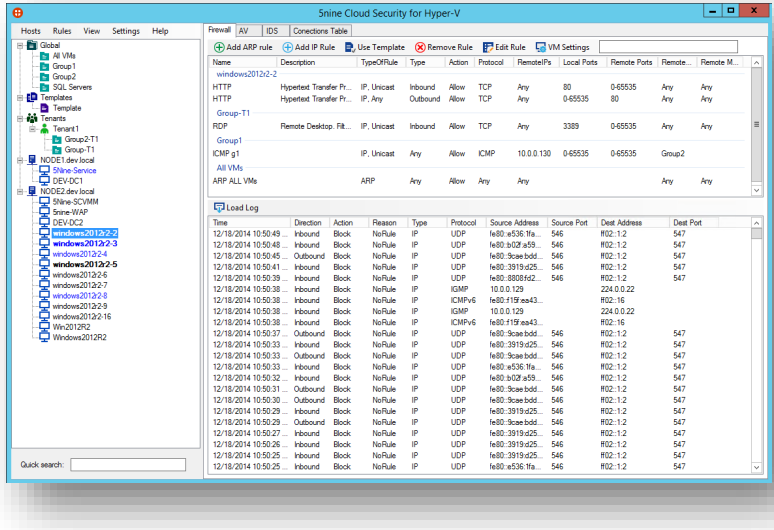
Автоматизация задач управления безопасностью

- Поддержка PowerShell
- Назначение задач по расписанию
- Быстрое масштабирование
- Уменьшает возможность ошибок персонала



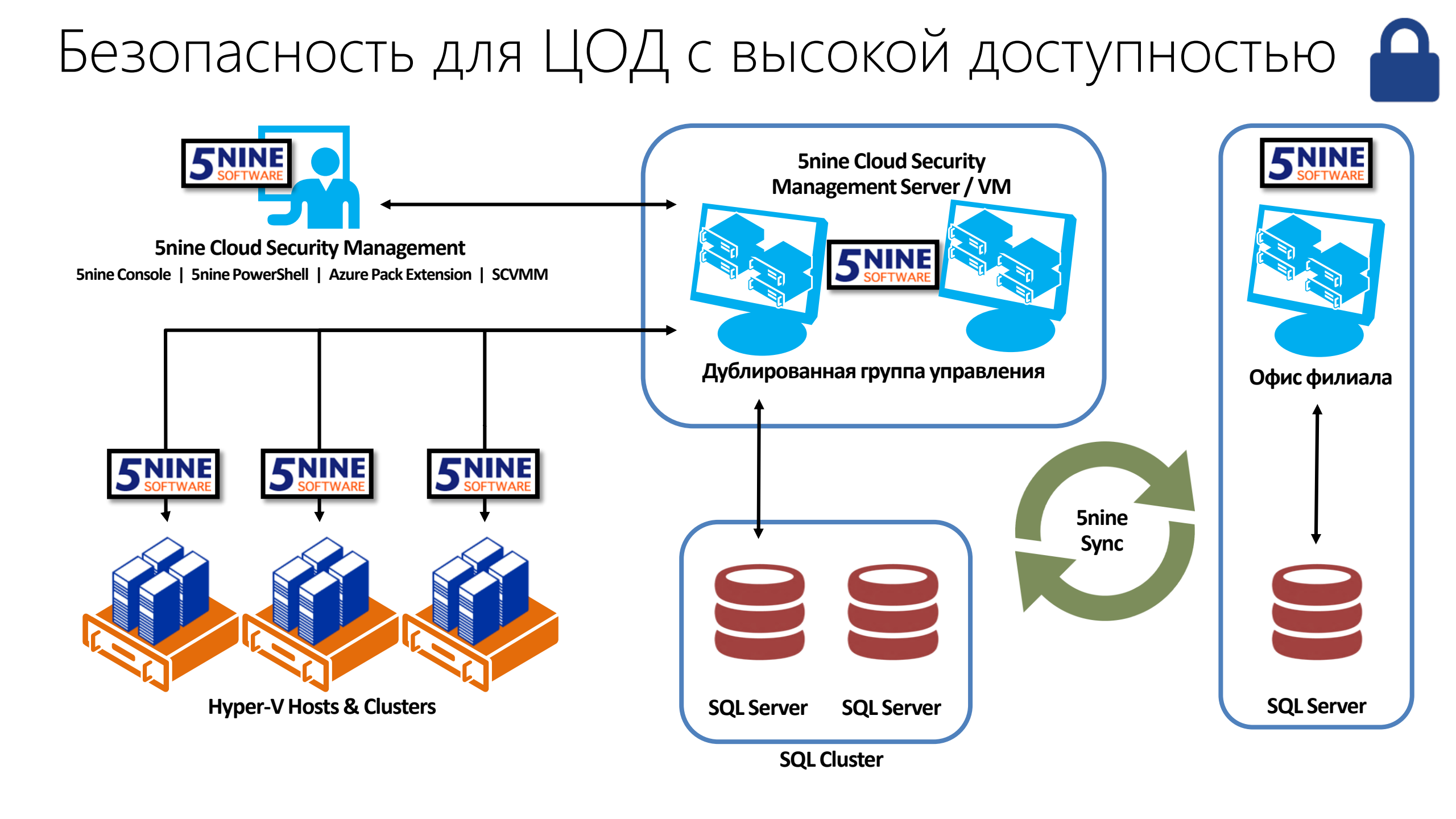
5nine Cloud Security

Комплексное решение по обеспечению безопасности и соответствия законодательству, разработанное специально для Hyper-V

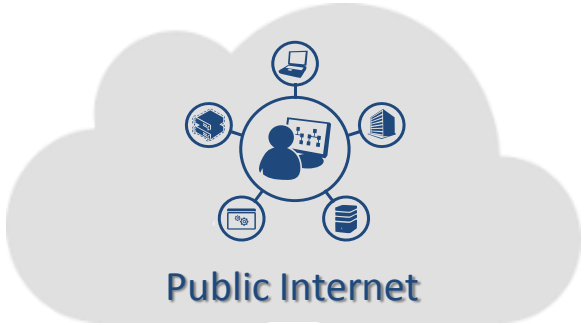


- Усиливает защиту виртуальной среды Hyper-V при помощи:
  - Многопользовательского межсетевого экрана
  - Безагентного антивируса Лаборатории Касперского
  - Обнаружения угроз в виртуальной сети
  - Обнаружения вторжений на уровне приложений
  - Безопасность как сервис (SECaaS) при помощи Azure Pack (WAP)
  - System Center Virtual Machine Manager (SCVMM) Plugin
  - Логирования событий безопасности
- Увеличивает производительность хостов, потребляя минимум ресурсов при высоком быстродействии
- Автоматизирует защиту ВМ, виртуальных сетей и хранилищ

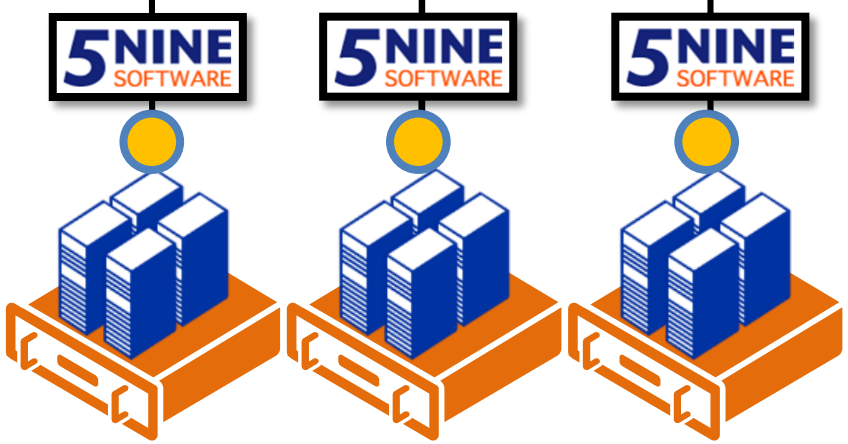
Безопасность для ЦОД с высокой доступностью



Защита от входящих, исходящих и внутренних угроз

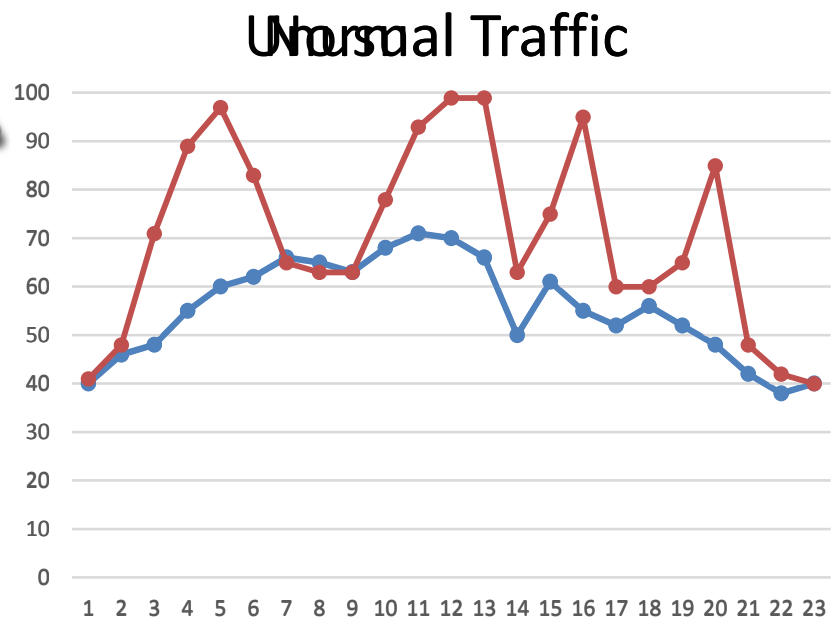


5nine Cloud Security Management Server / VM

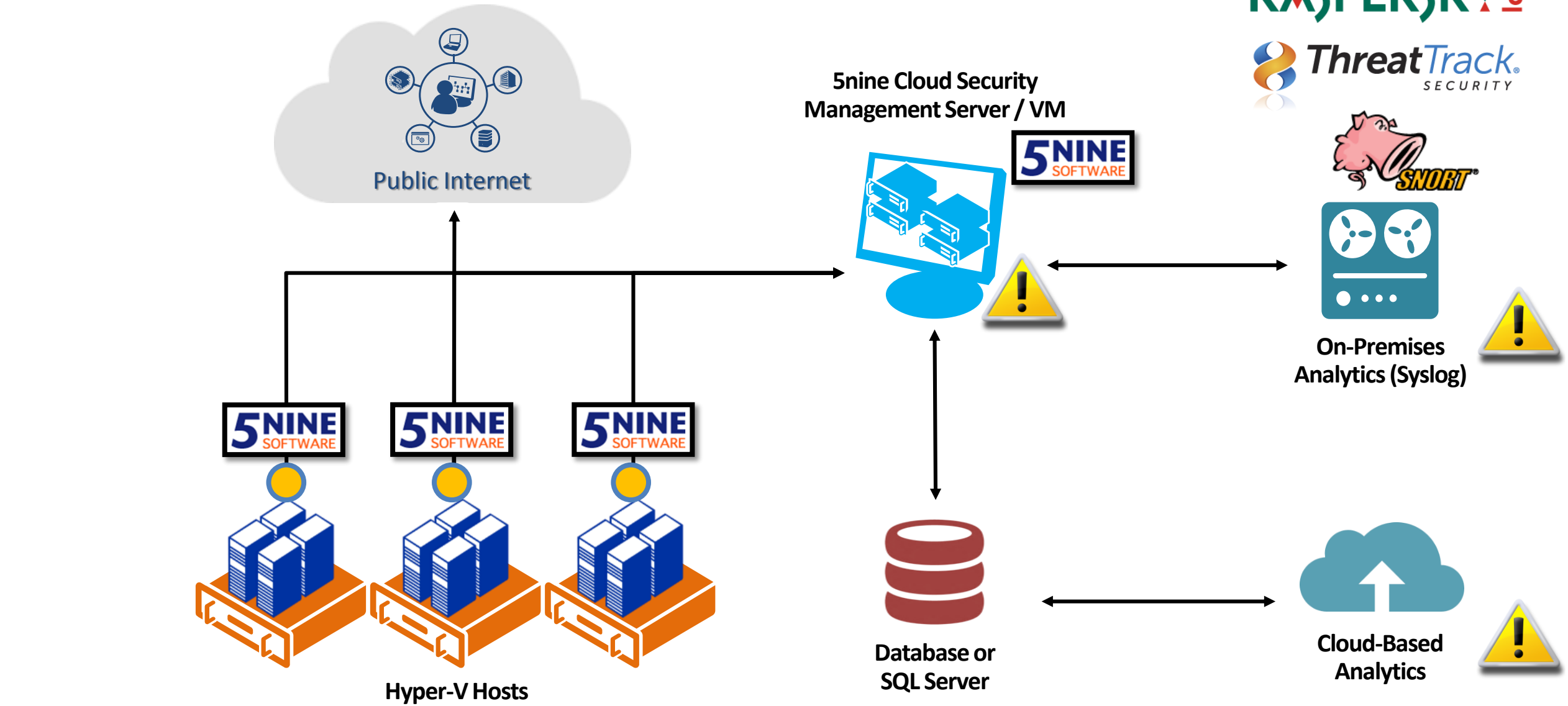


Hyper-V Hosts

Database or SQL Server



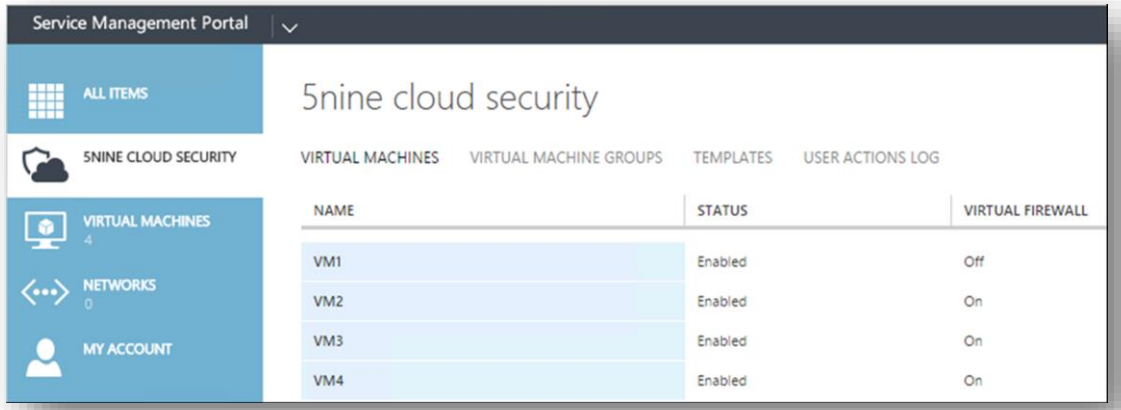
Расширенная платформа для аналитики



Azure Pack (WAP) Extension

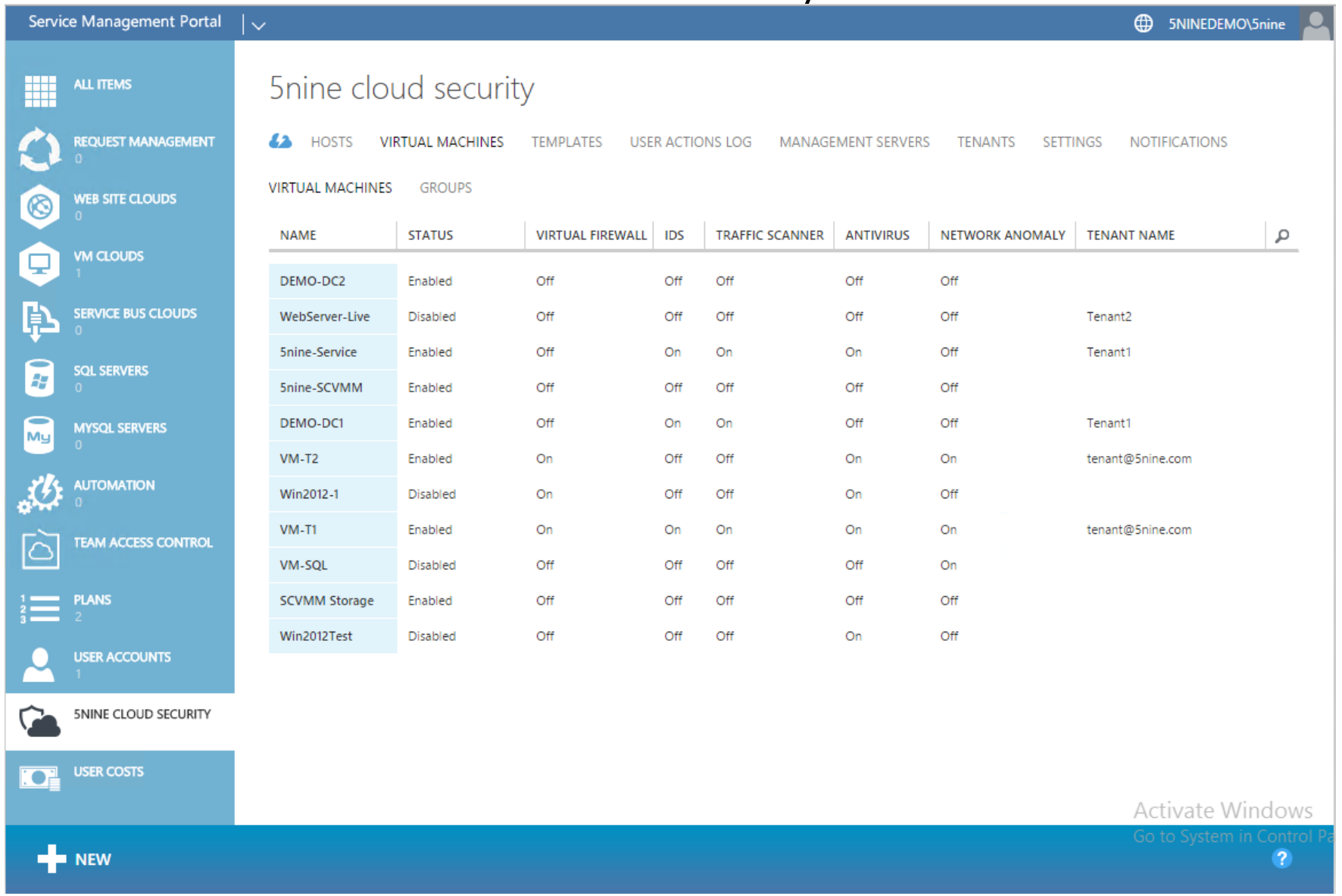
Безопасность как сервис (SECaaS) для защиты инфраструктуры ЦОД и ресурсов клиента

- Добавляет новую услугу, увеличивая монетизацию и выполнить требования законодательства
- Обеспечить изоляцию для ВМ и групп в многопользовательской среде
- Устранить угрозы не только снаружи , но и внутри виртуальной среды
- Автоматически защищать ВМ и группы
- Увеличить плотность ВМ и групп на каждом хосте
- Упростить управление безопасностью ресурсов для клиентов (кнопки on/off)
  - МСЭ, антивирус и СОВ для ВМ и групп
  - Шаблоны настроек МСЭ для разных ролей BMs
- Продукт доступен по SPLA



Azure Pack (WAP) allows you to run Azure services in your datacenter on your hardware

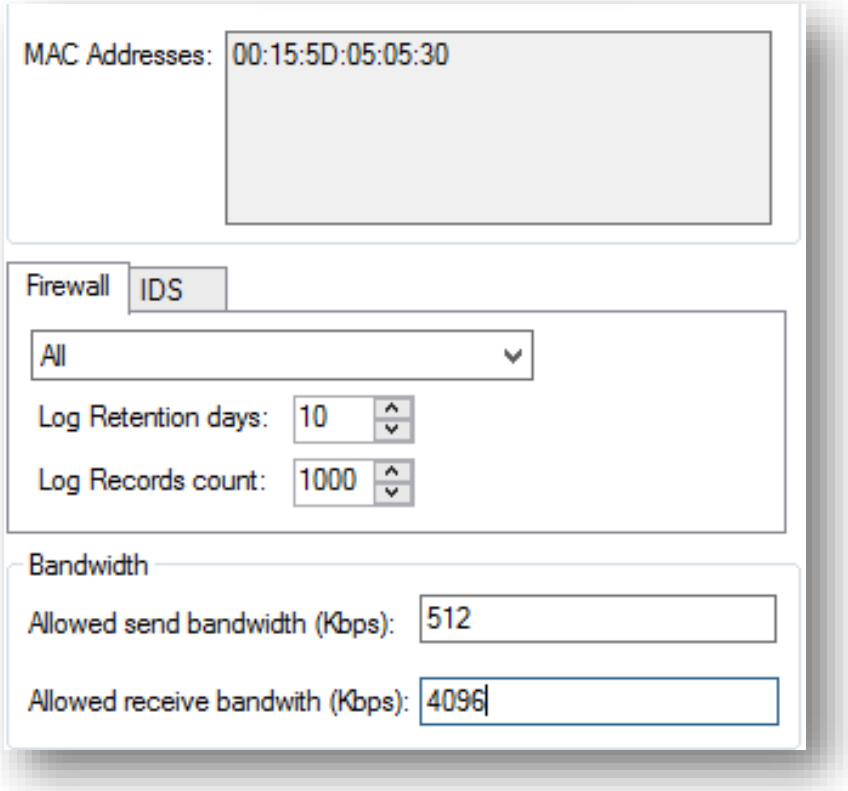
Управление безопасностью ВМ в 5nine Cloud Security WAP Extension



Best Practice

Изолируйте всех и управляйте ресурсами

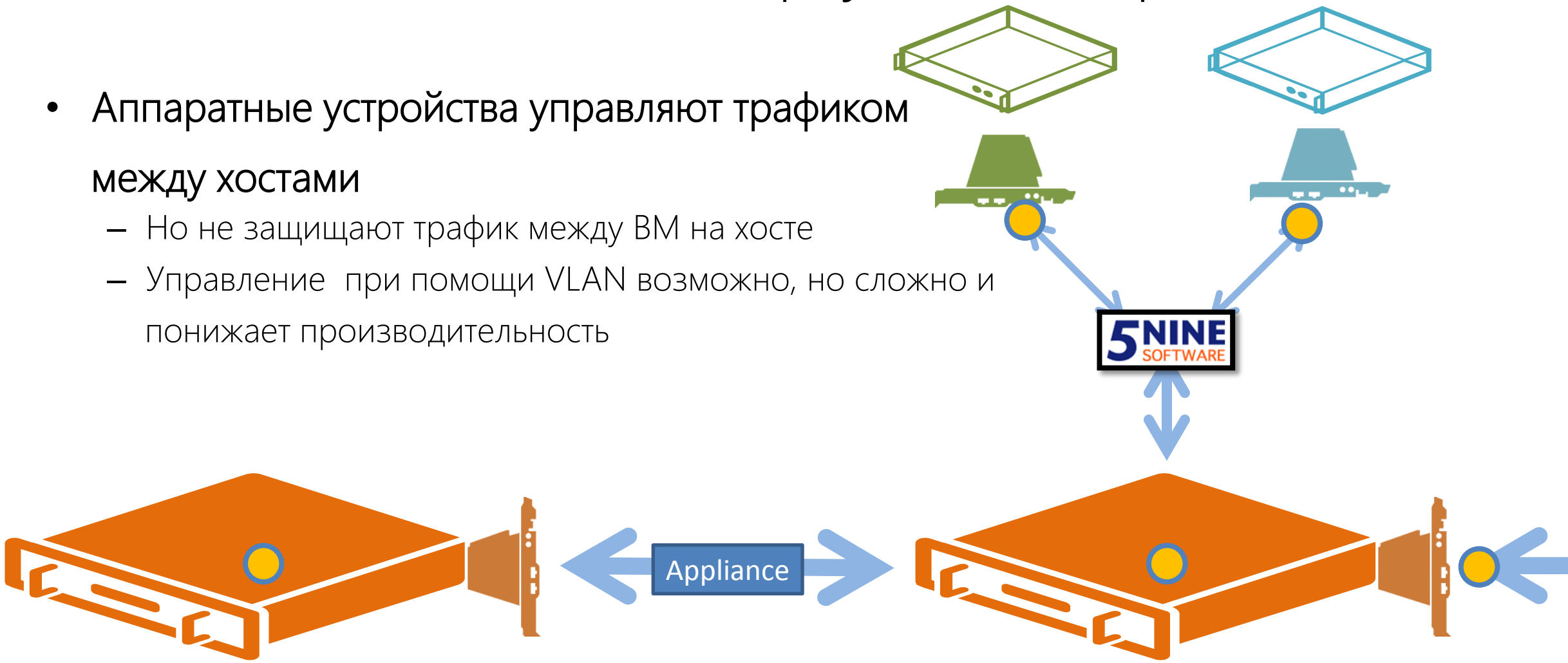
- Изоляция и приватности актуальны для облаков
  - ВМ не должна влиять на хост
  - ВМ не должна влиять на другие ВМ
- Используйте QoS для управления скоростью полосы пропускания трафика к ВМ и от нее



Best Practice

Избегайте аппаратных средств для обеспечения безопасности виртуальной среды

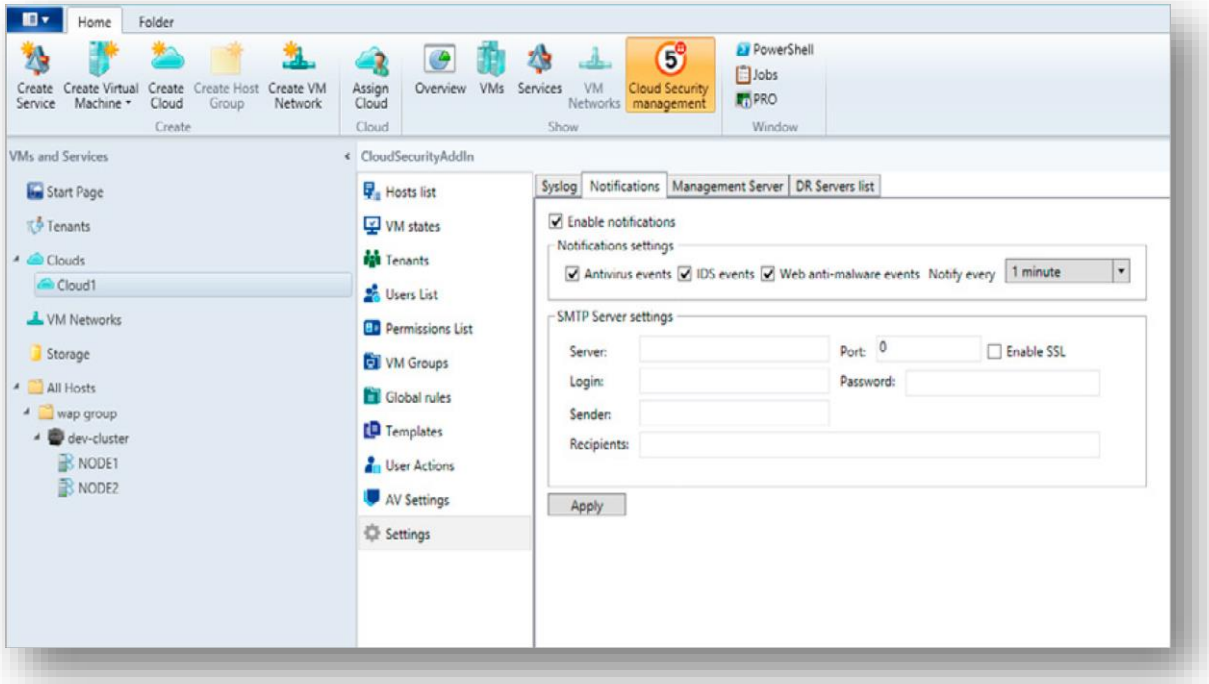
- Аппаратные устройства управляют трафиком между хостами
  - Но не защищают трафик между ВМ на хосте
  - Управление при помощи VLAN возможно, но сложно и понижает производительность



Best Practice

Не доверяйте пользователям

- Многие клиенты не заботиться о безопасности
  - Управляйте безопасностью за них
  - Управляйте обновлением сигнатур
  - Обеспечьте, чтобы защита не была отключена:
    - Случайно
    - Умышленно
    - По злом умыслу
- Централизованно следите за трафиком и анализируйте действия клиентов



Windows Server Hyper-V и 5nine Cloud Security для Hyper-V для выполнения Приказов ФСТЭК № 17 и № 21

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы				Как 5nine Security и экосистема Microsoft Windows Server Hyper-V помогает реализовать меры по обеспечению безопасности
		4	3	2	1	
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы		+	+	+	**5nine Cloud Security** является multi-tenant решением с делегированием прав доступа
СОВ.1	Обнаружение вторжений			+	+	Модуль IDS продукта **5nine Cloud Security** реализует обнаружение и блокирование вторжений для защищаемых виртуальных машин без установки агентов.
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+	**5nine Cloud Security** позволяет реализовать сбор и анализ регистрируемых событий от серверов виртуальной инфраструктуры.
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры			+	+	**5nine Cloud Security** позволяет реализовать управление (фильтрацию, контроль соединений) потоками информации между виртуальными машинами и внешними источниками без необходимости установки агентов в виртуальных машинах.
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+	**5nine Cloud Security** позволяет реализовывать антивирусную защиту и управление ей для защищаемых серверов и рабочих станций
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей			+	+	**5nine Cloud Security** позволяет реализовать управление (фильтрацию, контроль соединений) потоками информации между виртуальными машинами и внешними источниками без необходимости установки агентов в виртуальных машинах.

5nine Cloud Security и Hyper-V Windows Server для PCI DSS

Цели контроля	Требования PCI DSS	Реализация при помощи 5nine Cloud Security
Построение и сопровождение защищённой сети	1. Установка и обеспечение функционирования межсетевых экранов для защиты данных держателей карт	5nine Cloud Security обеспечивает защиту при помощи многопользовательского межсетевого экранана
	2. Неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности	Реализуется при помощи стандартных средств контроля доступа Windows Server и службы Active Directory
Защита данных держателей карт	3. Обеспечение защиты данных держателей карт в ходе их хранения.	Это требование относится к ограничению физического доступа и не относятся к защите среды виртуализации.
	4. Обеспечение шифрования данных держателей карт при их передаче через общедоступные сети	5nine Cloud Security не имеет функции криптографии, однако он поддерживает передачу шифрованного трафика по виртуальной сети, защищая его, как любой другой вид трафика.
Поддержка программы управления уязвимостями	5. Использование и регулярное обновление антивирусного программного обеспечения	5nine Cloud Security является единственным безагентным антивирусным решением для Hyper-V.Сигнатуры могут обновляться как с ресурсов производителя, так и с локального сервера обновлений для увеличения защищенности в соответствии с рекомендациями PCI DSS
	6. Разработка и поддержка безопасных систем и приложений	5nine Cloud Security обладает механизмом контроля целостности компонентов безопасности и дает возможность изолировать среду разработки/тестирования и производственного функционирования за счет использования групп безопасности
Реализация мер по строгому контролю доступа	7. Ограничение доступа к данным держателей карт в соответствии со служебной необходимостью	Реализуется при помощи стандартных средств контроля доступа Windows Server и службы Active Directory
	8. Идентификация и аутентификация доступа к системным компонентам	Реализуется при помощи стандартных средств контроля доступа Windows Server и службы Active Directory
	9. Ограничение физического доступа к данным держателей карт	Это требование относится к ограничению физического доступа и не относятся к защите среды виртуализации
Регулярный мониторинг и тестирование сети	10. Контроль и отслеживание всех сеансов доступа к сетевым ресурсам и данным держателей карт.	Реализуется при помощи стандартных средств контроля доступа Windows Server и системы логирования событий безопасности 5nine Cloud Security. Интеграция с централизованными системами сбора данных позволяет обеспечить необходимую длительность хранения информации.
	11. Регулярное тестирование систем и процессов обеспечения безопасности	5nine Cloud Security постоянно регистрирует и контролирует и анализирует статистические данные о сетевом трафике, пакетах и их размерах.
Поддержка политики информационной безопасности	12. Разработка, поддержка и исполнение политики информационной безопасности	Это требование относится к администрированию процессов объекта защиты.

Что нового в 5nine Cloud Security v7.1

- Соответствие требованиям законодательства по защите информации (152-ФЗ и др.)
- Мониторинг для физических NIC, подключенных к vSwitch
- Защита parents partition хоста
- Эвристический анализ трафика Системой обнаружения вторжений
- Обеспечение детального контроля над трафиком HTTP/DNS при помощи DPI
- Выбор профиля антивирусного сканирования для ВМ и групп.
- Автоматизация конфигурирования политик безопасности с расширенной поддержкой PowerShell

5NINE SOFTWARE | Защита и управление Microsoft Hyper-V
№1 в мире

Спасибо за внимание!

Юрий Бражников
Глава российского офиса
5nine Software

Телефон: +7 (495) 777-32-82
Email: info@5nine.ru
Сайт: www.5nine.ru