5NINE SOFTWARE | Передовая защита и управление Microsoft Cloud Platform

Современный подход к построению ИБ гибридного облака. Безопасность как сервис

Юрий Бражников
Директор 5nine Software по России и СНГ

О 5nine Software

Компания основана в 2009
Более 100.000 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

18x Microsoft® MVP Most Valuable Professional

Windows Server 2016 Certified
Windows Server 2012 R2 Certified
Windows Server 2012 Certified

Microsoft Partner
Gold Datacenter

5NINE SOFTWARE | Передовая защита и управление Microsoft Cloud Platform

Партнерство 5nine с другими вендорами

Безопасность

Bitdefender

KASPERSKY lab

SNORT

ThreatTrack

Оборудование

HYPERGRID

NUTANIX

xBYTE TECHNOLOGIES
www.xByte.com • 888-xByte-IT

Программное обеспечение

CLOUD CRUISER

VEEAM
IT JUST WORKS!™

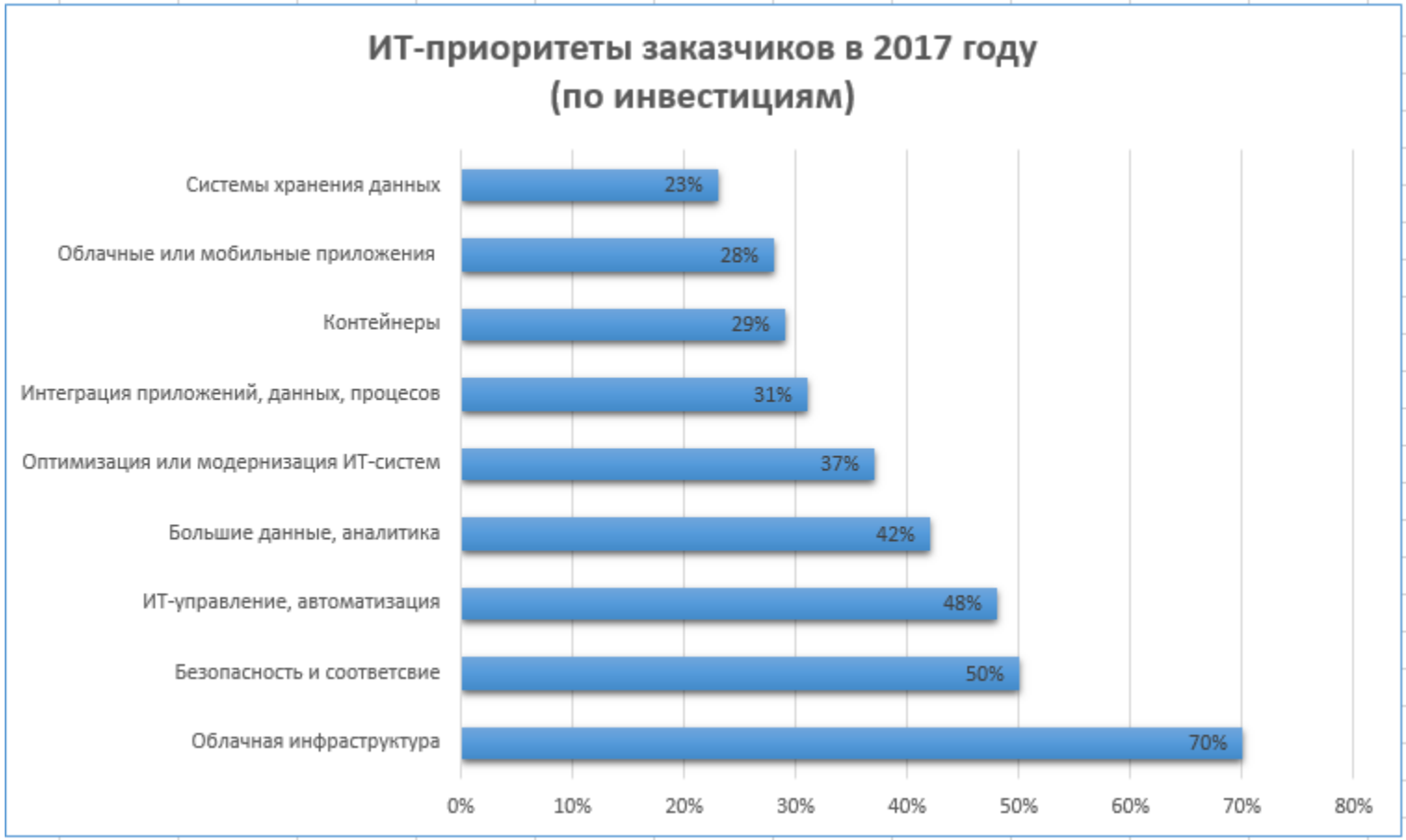
StarWind SOFTWARE

unidesk

Основные тренды 2017

Исследование, проведенное Rad Hat на своей клиентской базе показало:

1. Облака станут ИТ-приоритетом: 70% опрошенных назвали облачную инфраструктуру основным направлением для инвестиций в 2017 году. 50% планируют направить средства на обеспечение безопасности, 48% на улучшение управления инфраструктурой (автоматизация, оркестрация)
2. Стратегия развертывания: 38% пользователей выбирает частное облако, а 30% — гибридное, остальные – аутсорсинг и публичное облако
3. Главные задачи ИТ: 63% стремятся сократить затраты, 53% — повысить производительность, 43% — усилить безопасность.



Конвергенция ИТ и ИБ

Исторически ИБ и ИТ существуют параллельно, создавая 2 инфраструктуры оборудования, ПО, средств мониторинга и управления. Это приводит к:

- Неэффективной трате ресурсов
- Усложнению процесса обеспечения комплексной безопасности
- Появлению «слепых пятен» в инфраструктуре и усложнению взаимодействия подразделений ИТ и ИБ

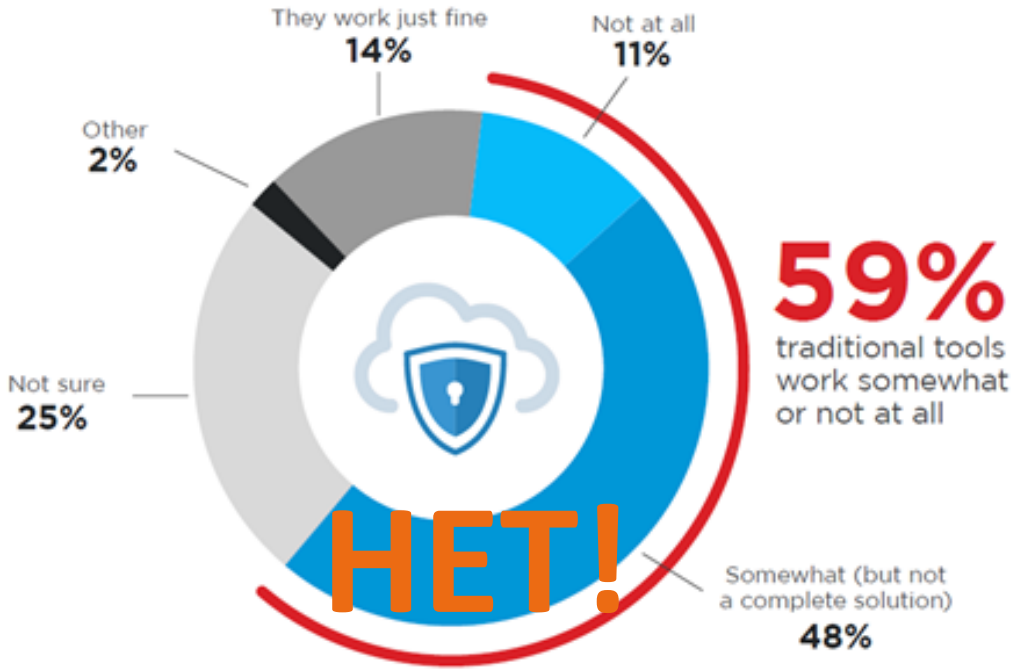
Взаимовыгодная конвергенция

- По данным Gartner, в корпорациях и организациях виртуализировано до 75% приложений
- В виртуальной среде можно использовать единые средства управления, мониторинга и безопасности для ИБ и ИТ с разделением ролей и функций
- По данным опроса 5nine среди крупных корпоративных клиентов, 90% заинтересованы в объединений управления ИТ и ИБ на платформе System Center

Старые технологии не защищают облачную инфраструктуру

- Классические антивирусные технологии были нацелены в первую очередь на защиту рабочих мест, ПК
- Основной целью хакеров теперь являются гибридные ЦОД, а не отдельные ПК и почтовые рассылки
- Использование только сигнатурного метода для АВ и СОВ стало не эффективным
- Ресурс физических серверов ограничен и делится между ВМ
- Существенно выросла база сигнатур и ее размер влияет на производительность ПК

Вопрос: Насколько эффективны традиционные сетевые СЗИ для облачной инфраструктуры?



К чему приводит игнорирование изменений в ИТ и использование устаревших технологий ИБ

1. Русский международный банк раскрыл в своей отчетности, что 21 января 2016 г. на него была совершена хакерская атака, в результате которой с корсчета банка в ЦБ было похищено 508 млн руб.

2. 29 февраля 2016 г. хакеры вывели с корсчета Металлинвестбанка в ЦБ 667 млн руб.

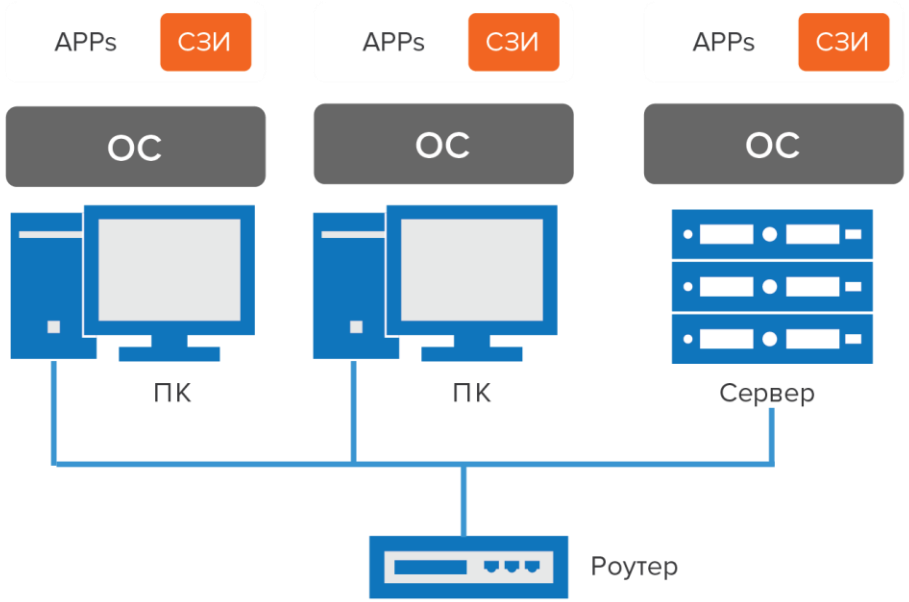
3. Хакеры украли деньги Центробанка Бангладеш со счета в ФРС США. Распоряжение о проведении оплаты было полностью подтверждено системой SWIFT в соответствии со всеми стандартными протоколами аутентификации.

4. Международная группировка хакеров Carbanak похитила со счетов клиентов 100 банков и других финансовых институтов в 30 странах мира $300-900 млн.

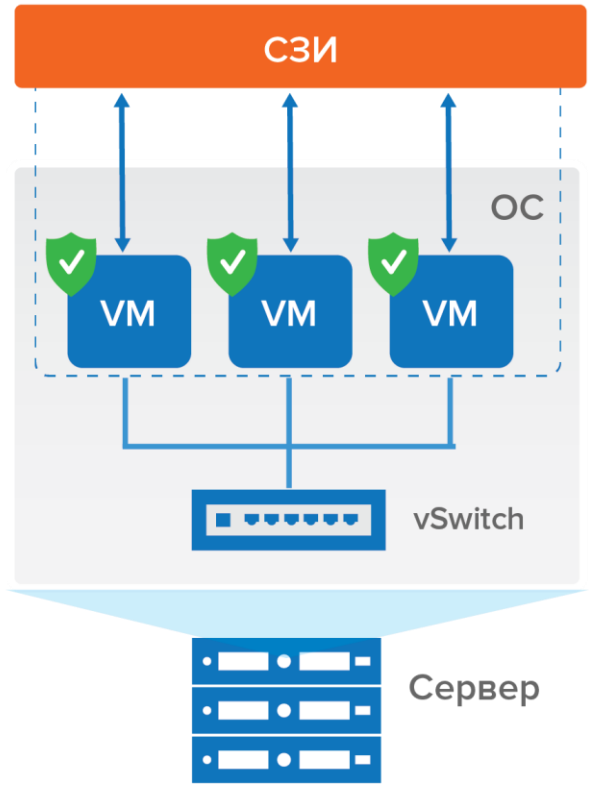
5. В США хакеры украли данные о пластиковых картах почти 70 миллионов клиентов у американской розничной сети Target, и банкам пришлось потратить $200 млн на их перевыпуск.

Различие методов защиты в физической и виртуальной среде

СЗИ для физической среды



Традиционные технологии с агентами на ВМ



Почему использование агентных СЗИ не эффективно для виртуальной среды

1. Многие вирусы и злоумышленники стараются блокировать работу агента в ВМ

2. Атаки на уровне виртуальной сети или с одной ВМ на другую не определяются аппаратными СОВ, контролирующих физическую среду и атаки in/out

3. Использование агентов в ВМ повышает риск атаки, т.к. требует дополнительного открытого порта на МСЭ для управления

4. Базы сигнатур и антивирусный агент потребляют большой объем ресурсов ВМ, приводя к понижению производительности хоста и количества ВМ

5. При инфицировании одной или нескольких ВМ на хосте или одновременном сканировании повышается кол-во обращений к дискам, что приводит к антивирусному шторму и деградации производительности хоста

Рекомендации ЦБ РФ по «Обеспечению информационной безопасности при использовании технологии виртуализации»

Глава 9 «Рекомендации по обеспечению ИБ виртуальных машин» :

9.6. «Рекомендуемым решением является использование средств защиты от воздействия вредоносного кода на уровне гипервизора без установки агентского ПО на виртуальные машины.»

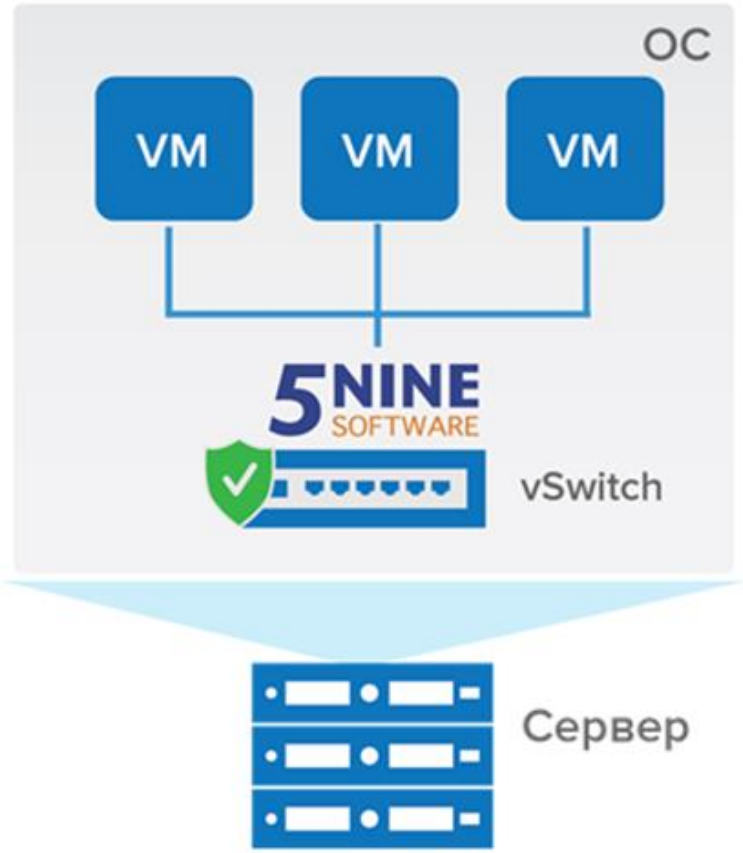
Повышение безопасности виртуальной среды при помощи безагентных СЗИ

Безагентные СЗИ:

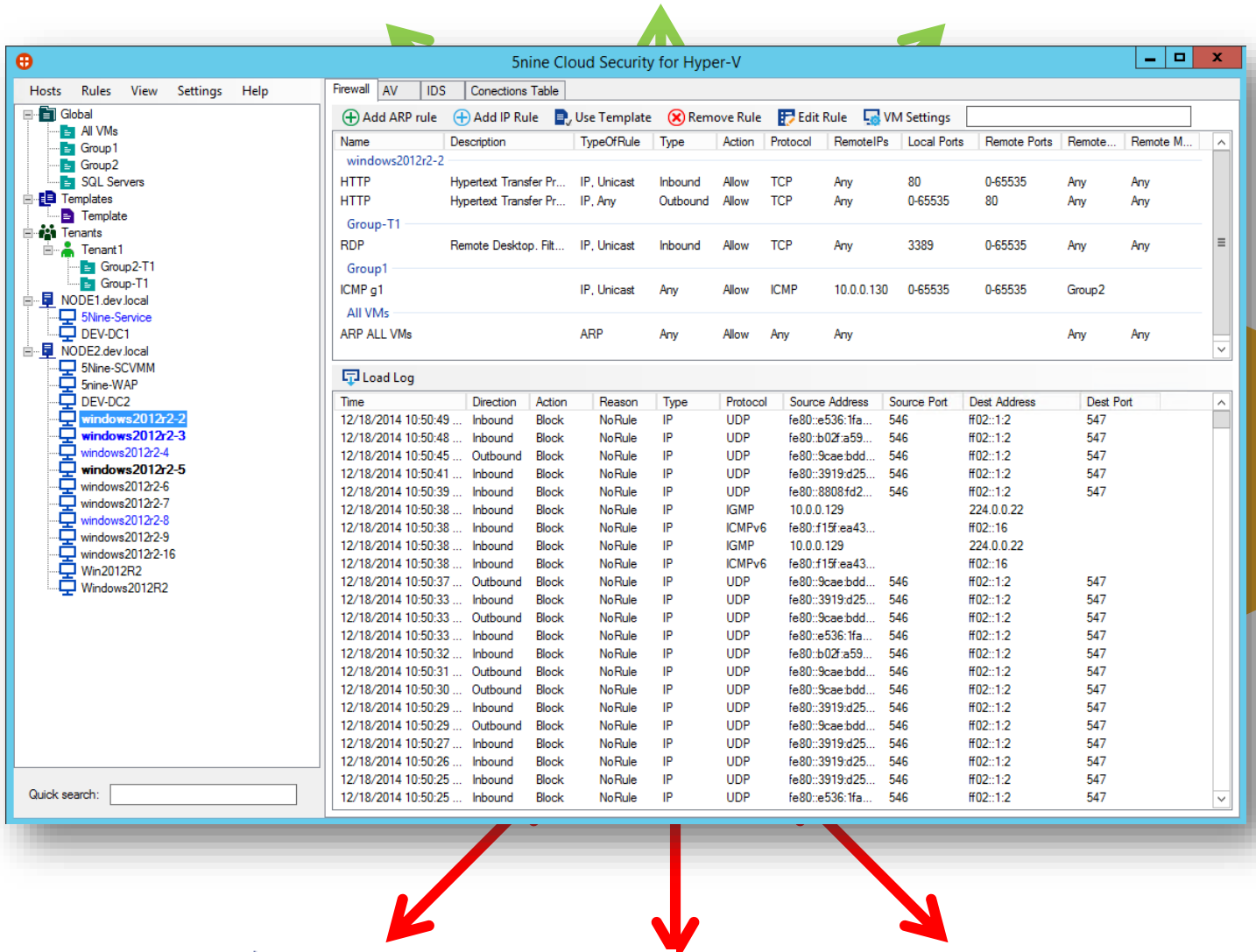
1. Защищают от возможности отключения или блокирования агента в ВМ.
2. Уменьшают влияние персонала или пользователей на безопасность.
3. Понижают трудоемкость обеспечения безопасности: нет необходимости проверять и обновлять сигнатуры на каждой ВМ. Эти процедуры автоматически выполняются на хосте.
4. Помогают избежать конфликта ресурсов, таких как антивирусные штормы.
5. До 30% уменьшают потребление ресурсов хоста за счет новых технологий сканирования, увеличивают плотность виртуализации и ROI проекта.

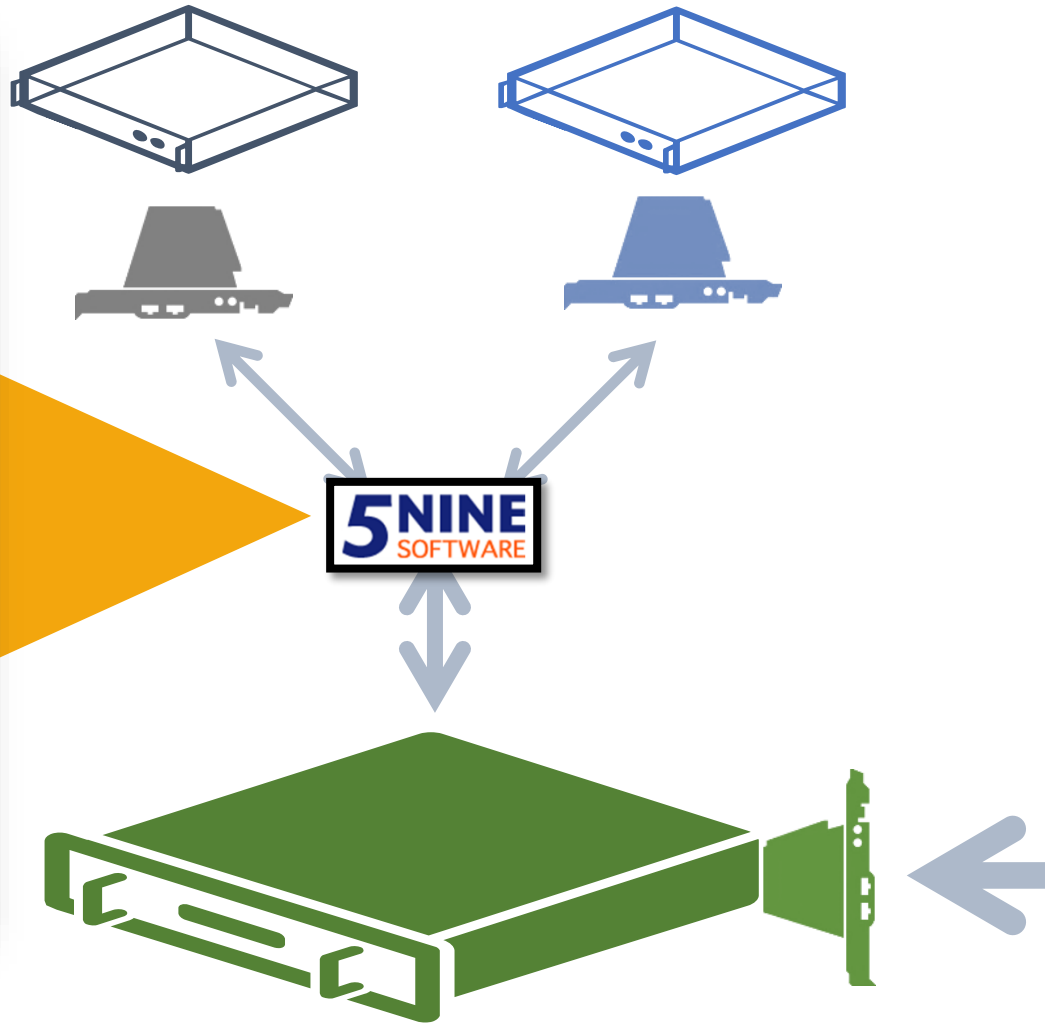
5nine Cloud Security –современное СЗИ для гибридного облака

- Многоуровневая защита: **межсетевой экран, безагентный антивирус, система обнаружения вторжений** в едином решении
- Простота управления и интеграция в средства управления инфраструктурой
- Защита базируется на сервере, а не АРМ пользователя
- СЗИ интегрировано в ОС, что расширяет ее возможности, уменьшает потребляемый ресурс. Современные СЗИ позволяют **экономить до 30% ресурсов** сервера и **работают до 70 раз быстрее** классических
- Безагентный способ защиты, не зависящий от действий пользователя и его гостевой ОС



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

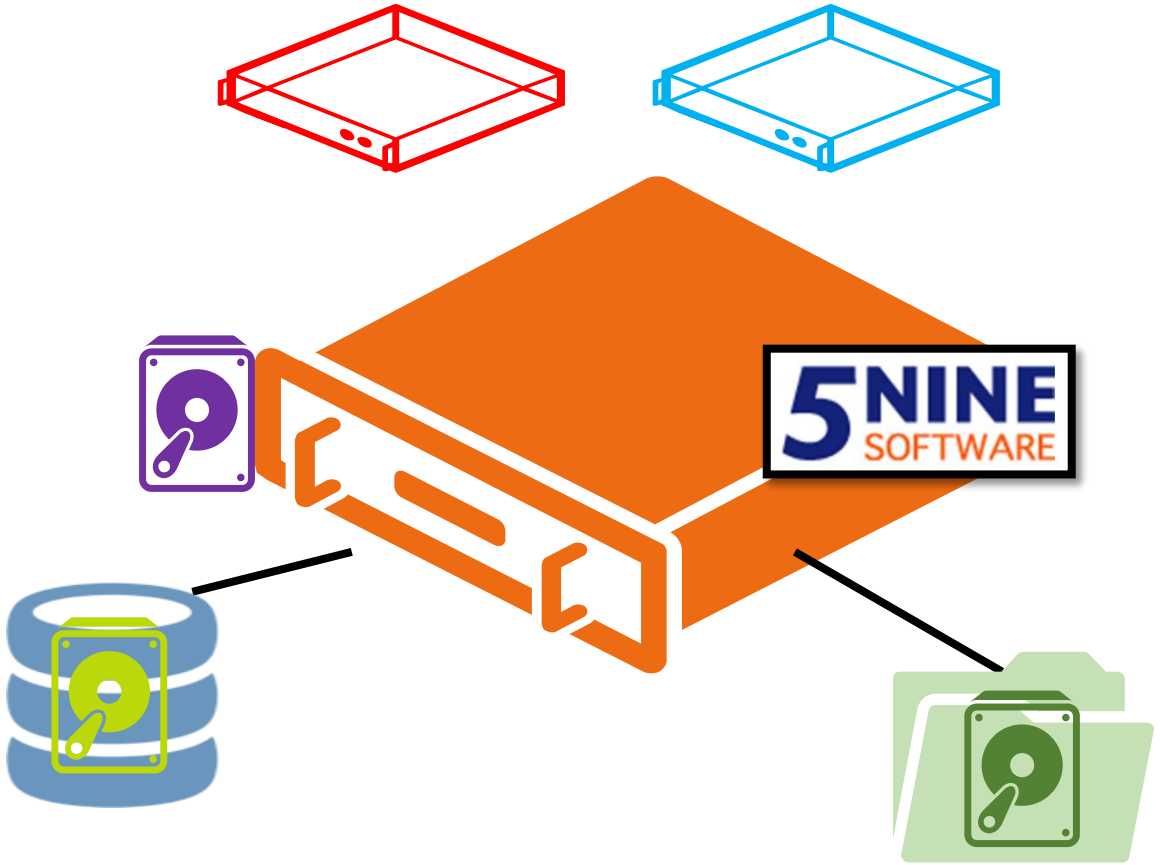




5NINE SOFTWARE | Передовая защита и управление Microsoft Cloud Platform

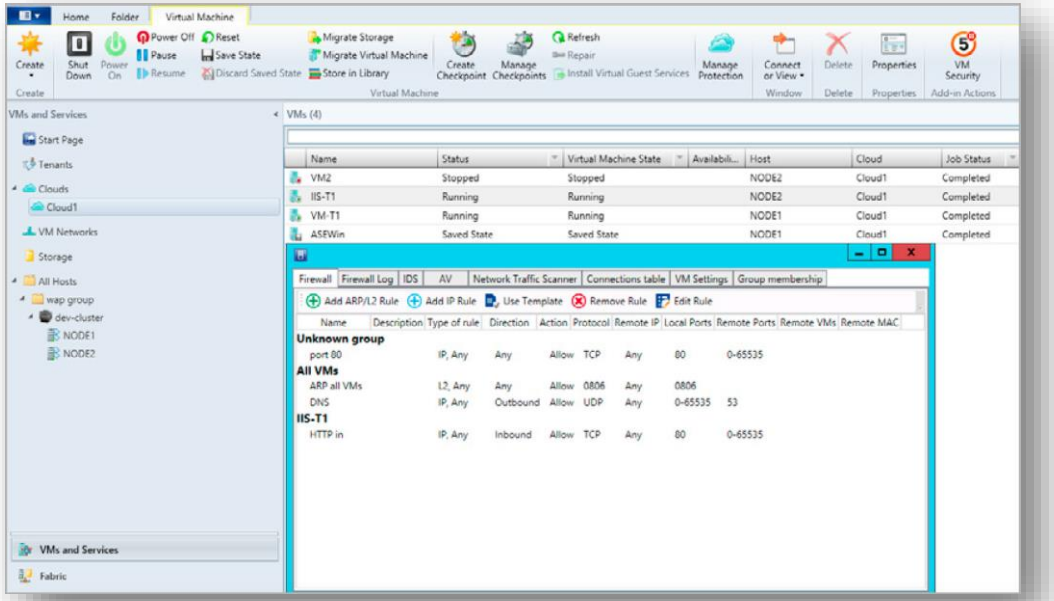
Автоматизация задач управления безопасностью

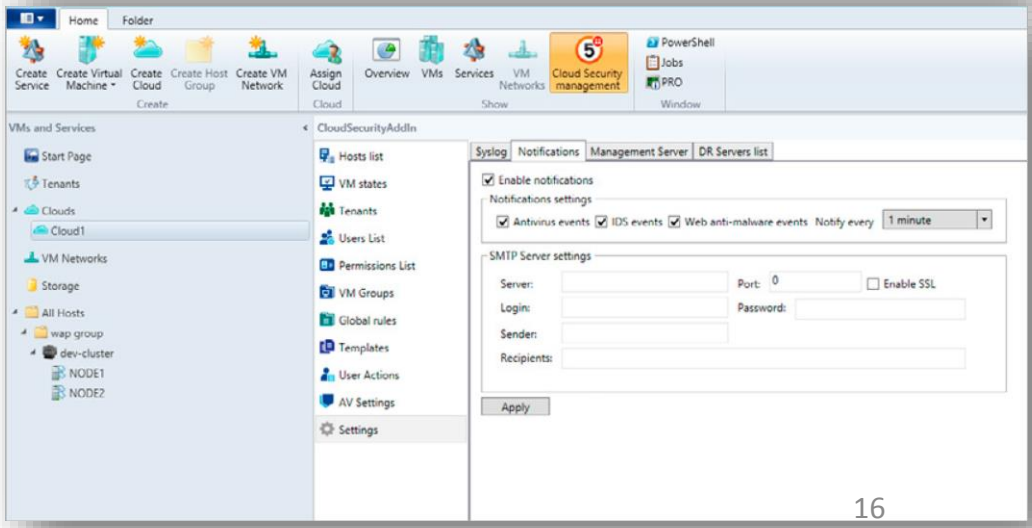
- Поддержка PowerShell
- Назначение задач по расписанию
- Быстрое масштабирование
- Уменьшает возможность ошибок персонала



Централизованное управление безопасностью ВМ через System Center VMM

- 5nine Cloud Security Plugin позволяет интегрировать СЗИ в SC VMM и управлять аппаратными и виртуальными ресурсами из одной консоли
- Автоматизирует применение политик безопасности для защиты хостов и ВМ
- Масштабирует управление безопасностью всей среды виртуализации предприятия, в том числе территориально распределенной и гибридной





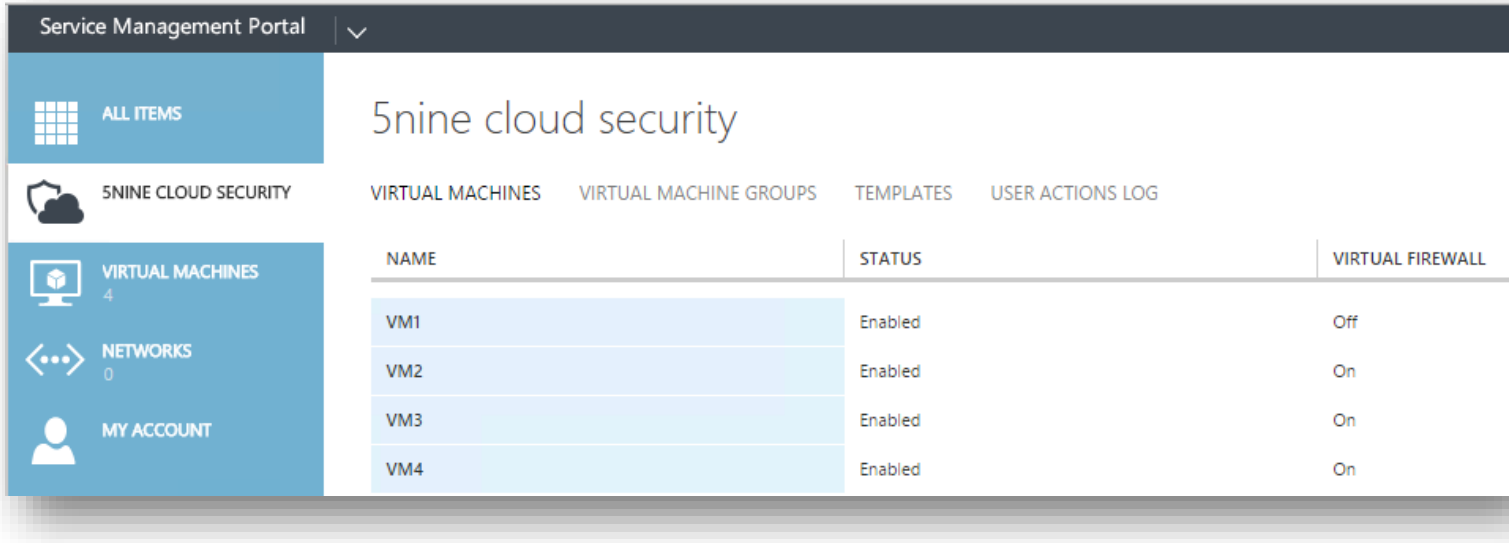
5NINE SOFTWARE | Передовая защита и управление Microsoft Cloud Platform

Расширение 5nine Cloud Security для Azure Pack

Защита ВМ в качестве сервиса
Позволяет компаниям и организациям организовать удобный и безопасный портал для разработчиков (в т.ч. Site Reliability Engineering) и подрядчиков, предоставить безопасность ВМ в качестве сервиса (SECaaS)

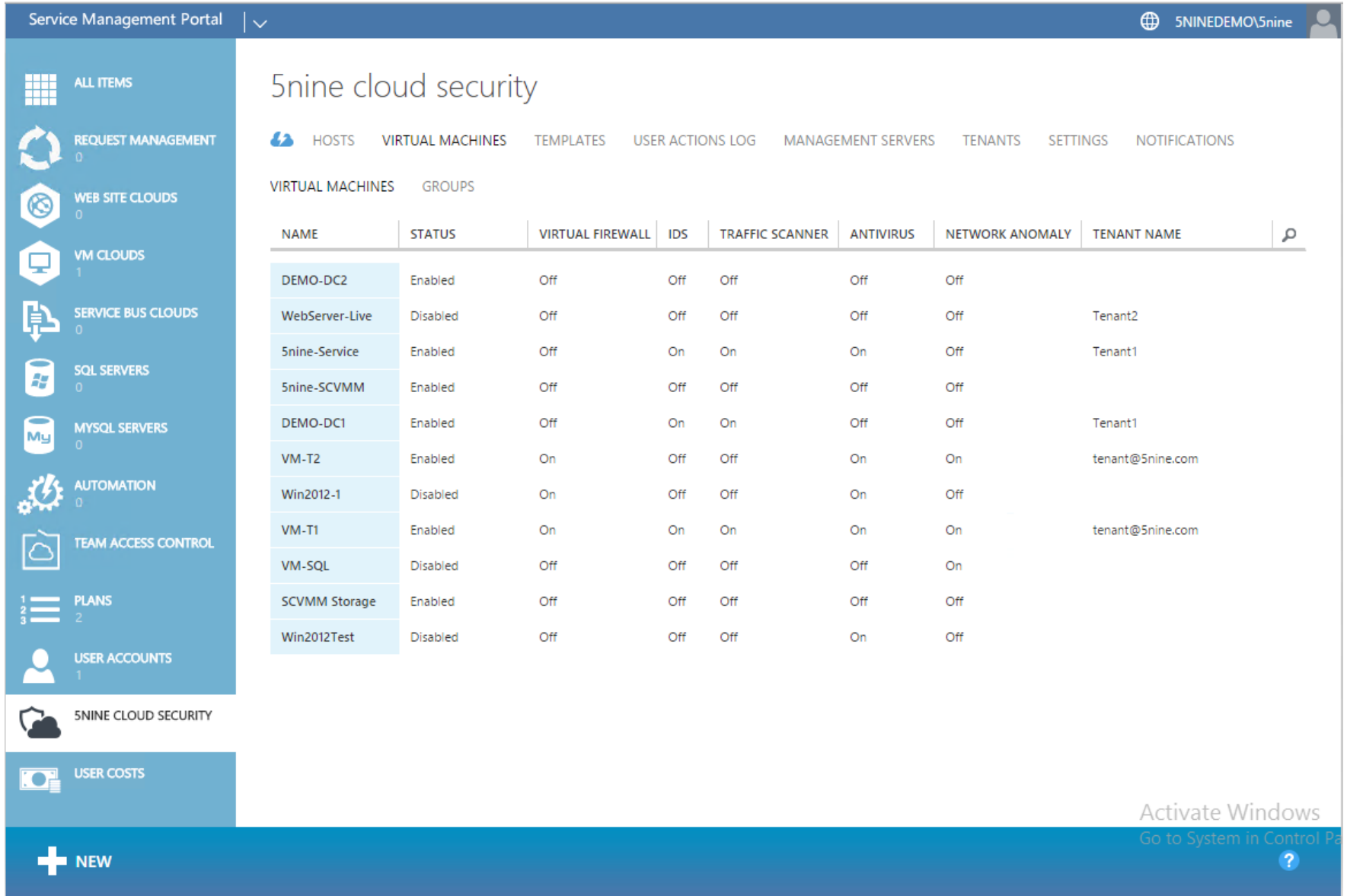
Virtual Firewall, антивирус и IDS

- Межсетевой многопользовательский экран изолирует ВМ и группы в среде Hyper-V
- IDS
- Поддерживает защиту ВМ под Linux и Windows
- Online Traffic Scanner
- Безагентное антивирусное сканирование по расписанию для групп

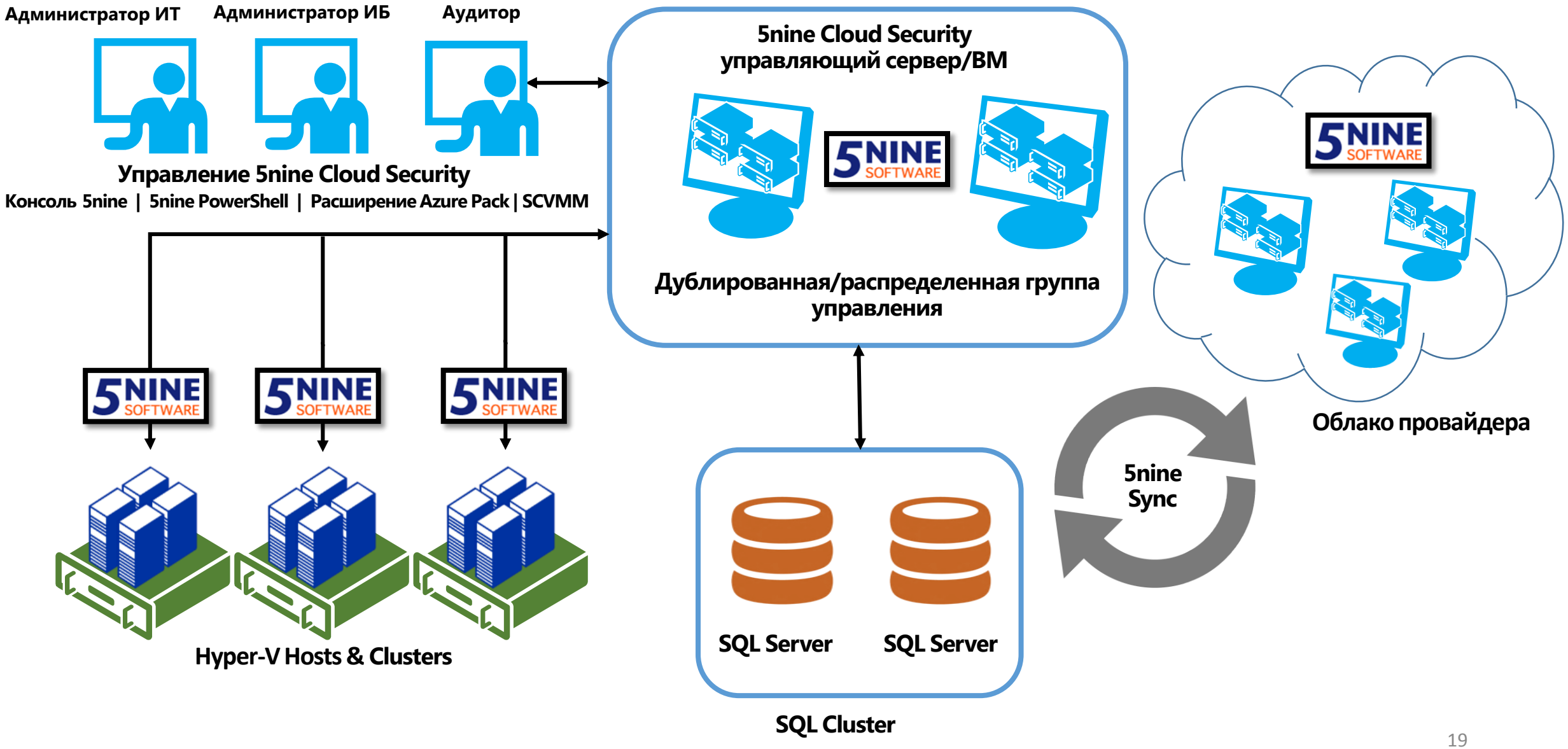


5NINE SOFTWARE | Передовая защита и управление Microsoft Cloud Platform

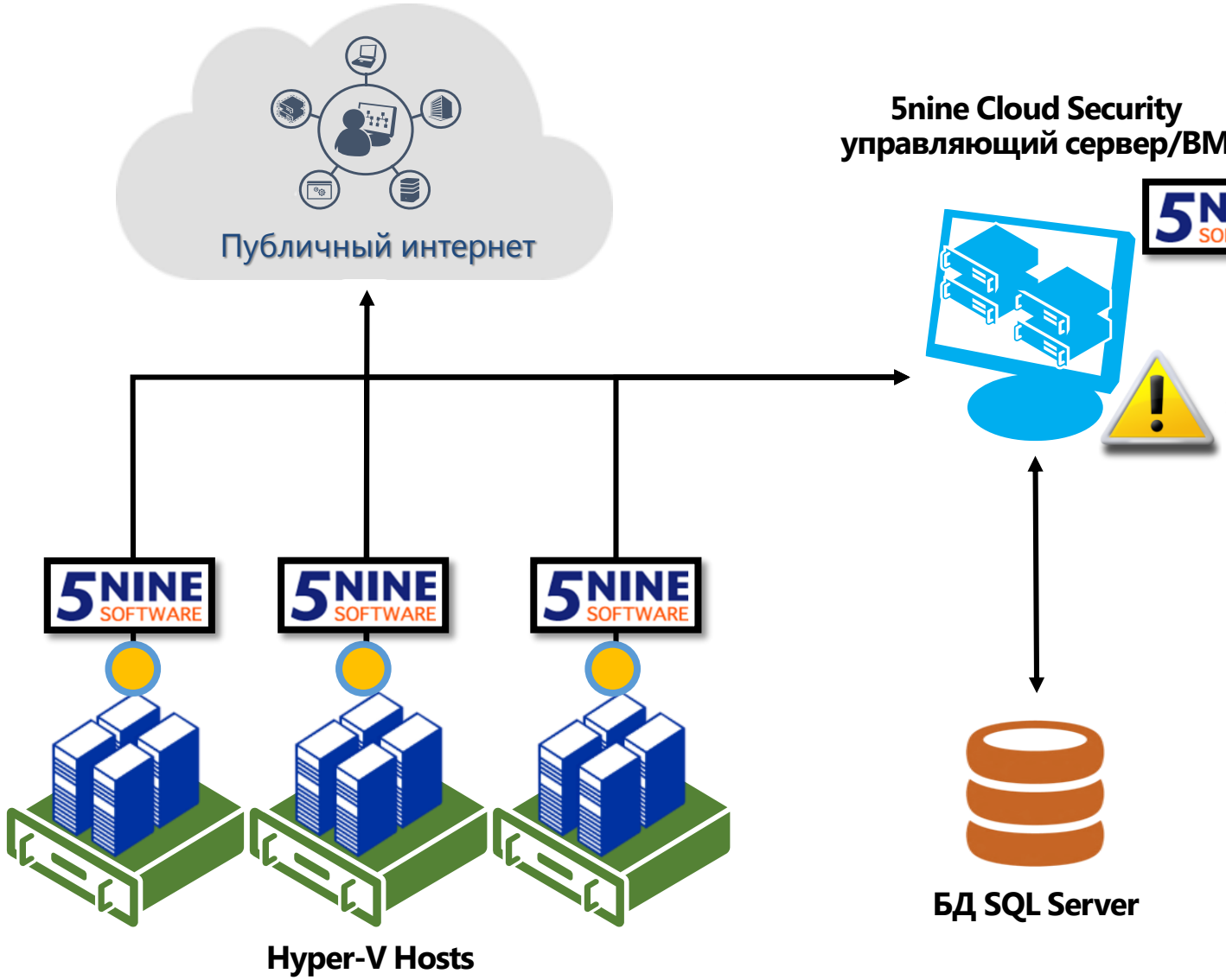
Управление безопасностью ВМ в 5nine Cloud Security WAP Extension



Безопасность для гибридной инфраструктуры с высокой доступностью



Поведенческий анализ и прогноз – основа СЗИ нового поколения



Bitdefender

KASPERSKY lab

ThreatTrack

SNORT

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

Почему предусмотрительные руководители выбирают современные безагентные СЗИ

Безопасность разработанная для Windows Server Hyper-V

- Разработан и оптимизирован специально для Microsoft Hyper-V
- Расширение функциональности виртуального коммутатора Hyper-V
- Безагентная безопасность
- Комплексная защита и соответствие требованиям законодательства. Импортозамещение

Многоуровневая защита виртуальных машин

- Интегрированные межсетевой экран, антивирус, система обнаружения вторжений
- Изолирует и защищает ВМ по ID, имени, группе, пользователю. SPI/DPI
- Поддерживает безопасность виртуальных сетей и многопользовательский режим
- Обеспечивает активное обнаружение угроз

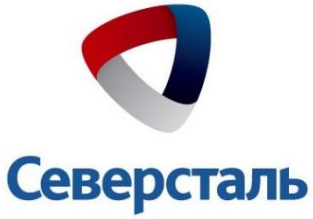
Упрощение работы администраторов ИТ и ИБ

- Централизованное управление инфраструктурой, безопасностью и мониторинг виртуальной среды
- Разделение ролей администраторов ИБ, ИТ и аудитора.
- Делегирование роли администратора тенанту
- Анализ логов событий ИБ для аудита
- Простое масштабирование и автоматизация

Повышение отдачи от инвестиций в Hyper-V

- Повышает плотность виртуализации и показатель консолидации
- Низкое потребление ресурсов ВМ. Увеличивает производительность системы до 30%
- Предоставление Безопасности как услуги (SECaaS) без начальных инвестиций

Клиенты 5nine Software



Хостинговые компании – клиенты 5nine Software

5NINE SOFTWARE | Передовая защита и управление Microsoft Cloud Platform

Спасибо за внимание!

Юрий Бражников
Директор 5nine Software по России и СНГ

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