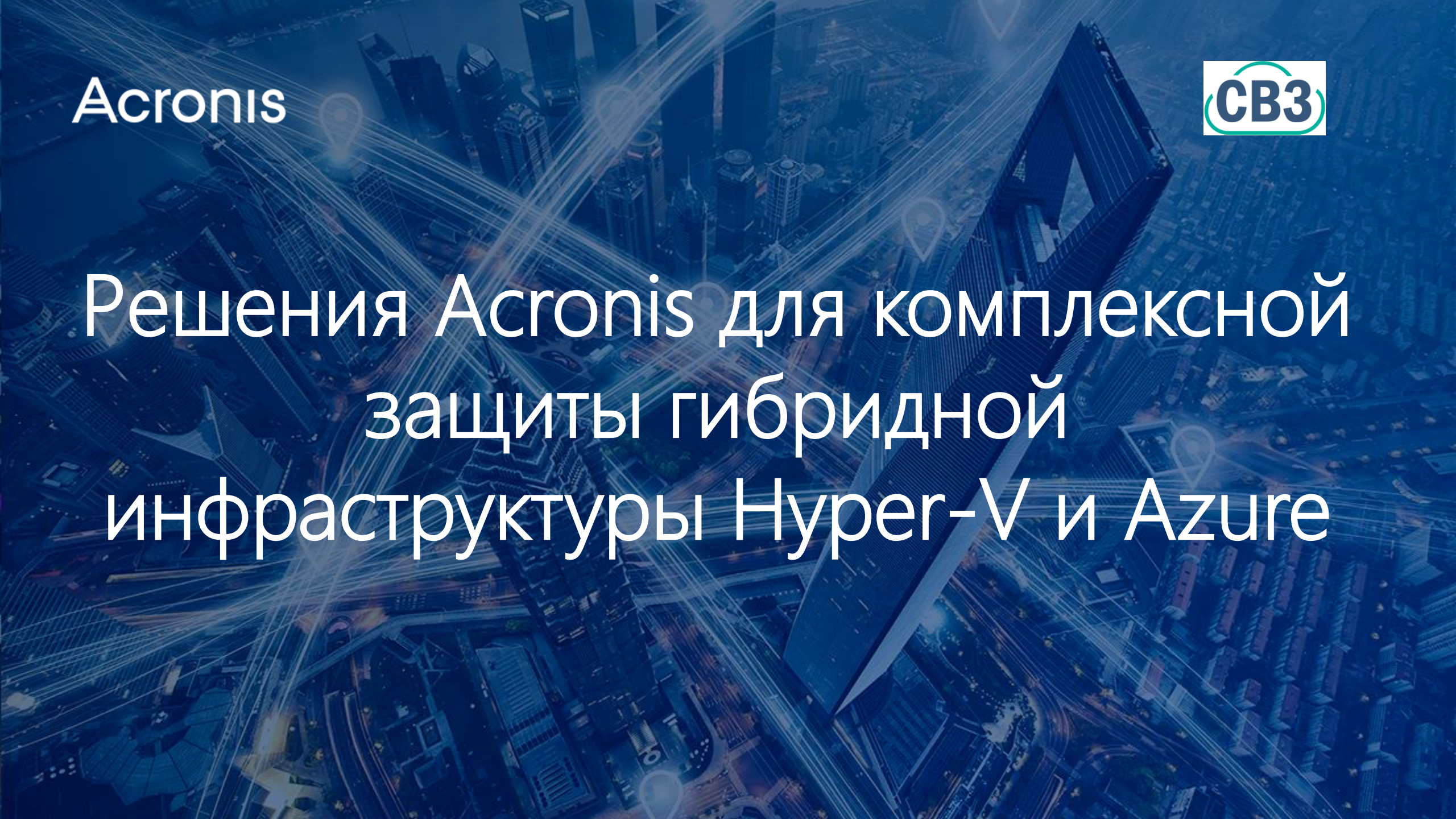


Решения Acronis для комплексной защиты гибридной инфраструктуры Hyper-V и Azure

О 5nine Software

- Компания основана в 2009. С 2019 года принадлежит Acronis
- Более 100.000 клиентов различных размеров по всему миру, во всех отраслях экономики
- Единственный в мире, кроме Microsoft, разработчик решений по управлению гибридной инфраструктурой Hyper-V/Azure и обеспечению комплексной безопасности на уровне гипервизора Windows Server
  - Acronis Cloud Security – комплексная безагентная безопасность Hyper-V и Azure
  - Acronis Cloud Manager –управление, мониторинг, бэкап и сетевая инфраструктура SDN гибридного облака для предприятий любого размера
  - Acronis Cloud Migration – решение по миграции ВМ с VMware на Hyper-V, в Azure и AWS

Microsoft Partner
Gold Datacenter

Acronis

Проблемы защиты гибридной среды

CSA (Cloud Security Alliance) провел в 2021 году опрос 1900 работников ИТ и ИБ.
Выводы:

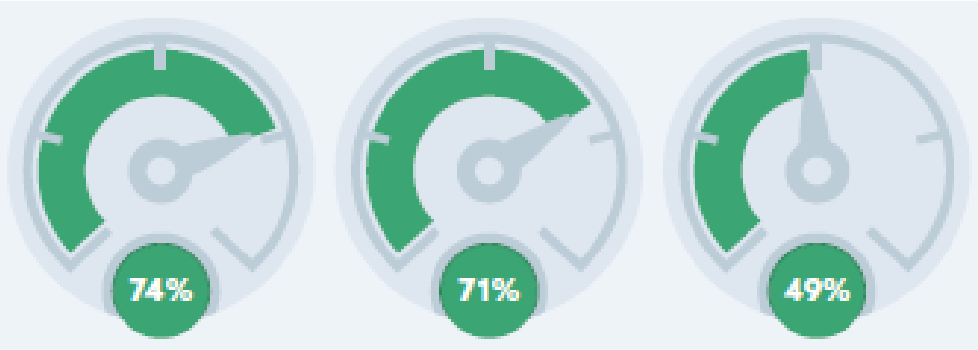
Облачные провайдеры не обеспечивают полной защиты пользователей своими СЗИ

74% -используют встроенные облачные СЗИ провайдеров

71%- используют дополнительные решения провайдеров

49% - используют виртуальные МСЭ и другие продукты

для обеспечения безопасности облаков



cloud security alliance®

Acronis

Что сегодня нужно пользователю гибридной среды

Сложная среда, недостаток экспертизы (47%) и персонала (32%) заставляет компании искать новые продукты для повышения безопасности гибридной среды

Пользователи ищут продукты для решения проблем:

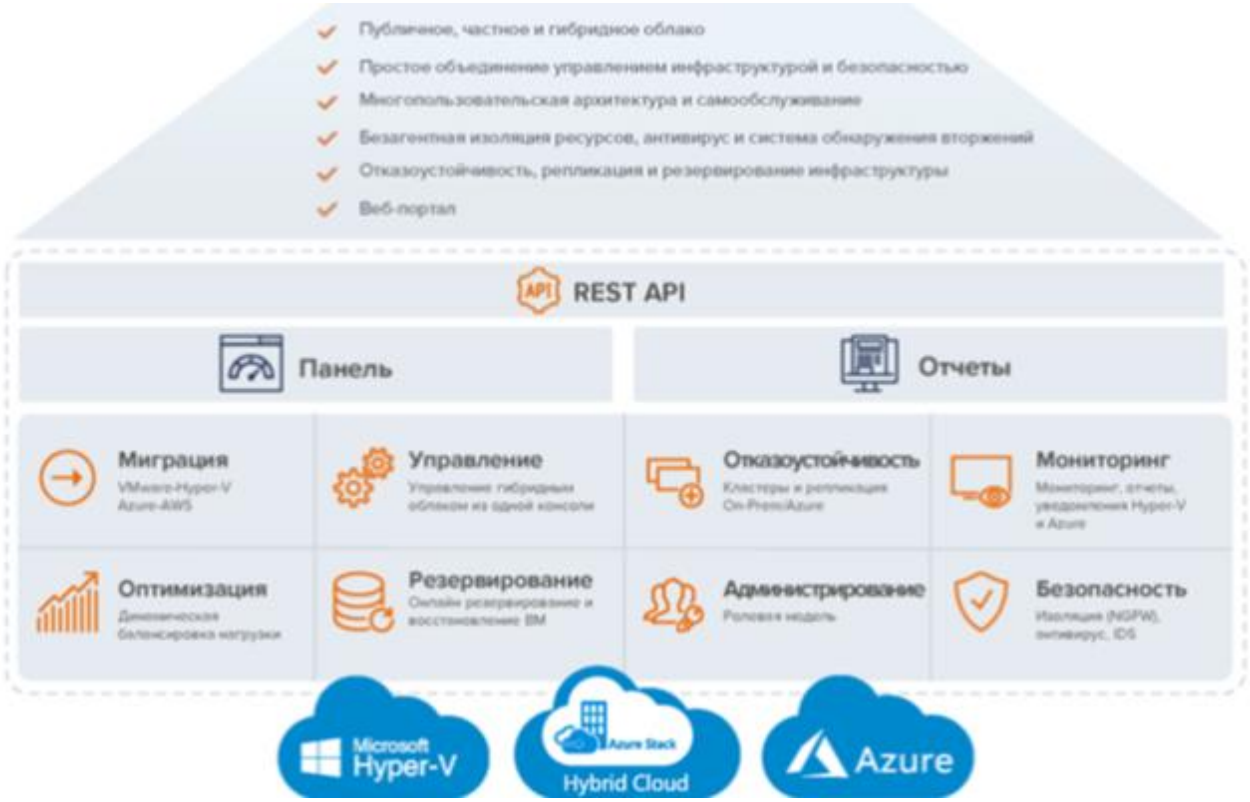
- Контроля и мониторинга гибридной среды
- Проактивной защиты от сетевых угроз
- Проактивного обнаружения проблем с конфигурацией
- Унификации и автоматизации разных уровней защиты
- Отчетов о соответствии законодательству и стандартам ИБ
- Упрощения настройки правил
- Упрощения миграции нагрузок из ЦОД в облако

cloud security alliance®

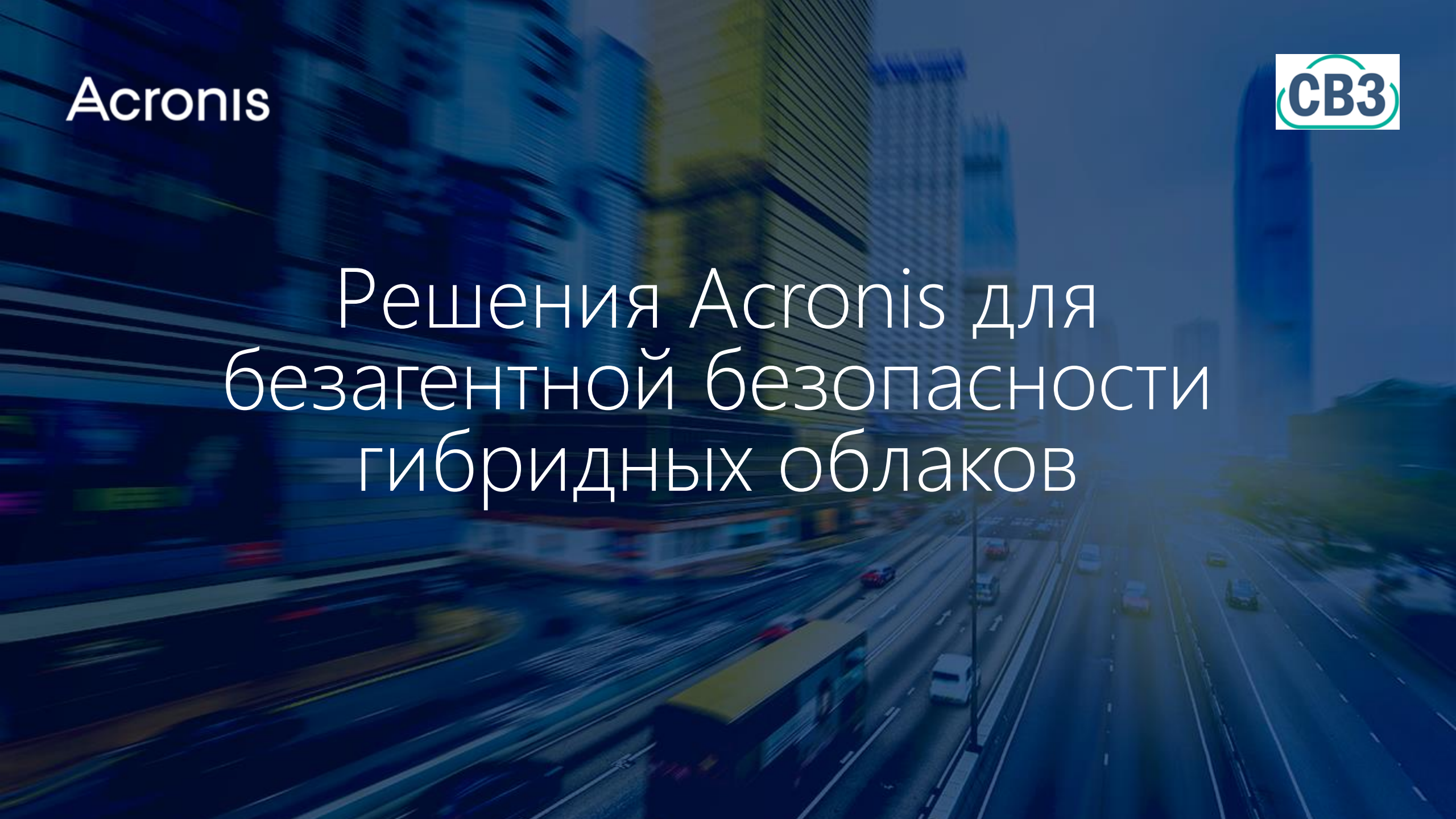
Acronis

Комплексное решение для контроля и безопасности гибридной инфраструктуры от Acronis

- Виртуализация Microsoft Hyper-V
- Acronis Cloud Manager для управления, мониторинга и резервирования
- Acronis Cloud Security –комплексное безагентное средство защиты своего ЦОД и Azure
- Автоматизация и интеграция с существующими системами мониторинга и ИБ
- Веб-портал для управления инфраструктурой и ее безопасностью
- Миграция ресурсов между ЦОД и облаком



Acronis



Решения Acronis для безагентной безопасности гибридных облаков

Почему использование агентных СЗИ не эффективно для гибридной среды

Агентные	Безагентные (Acronis Cloud Security)
Агент в ВМ блокируется вирусами и злоумышленниками	Среда виртуализации защищена от отключения или блокирования агента в ВМ. Уменьшается влияние персонала или пользователей на безопасность.
Атаки на уровне виртуальной сети или с одной ВМ на другую не определяются аппаратными IDS, контролирующих физическую среду и атаки in/out	Контролирует трафик внутри гипервизора и обнаруживает атаки с ВМ на ВМ
Использование агентов в ВМ повышает риск атаки, т.к. требует дополнительного открытого порта на МСЭ для управления	Антивирус работает на хосте , а не в ВМ
Базы сигнатур и антивирусный агент потребляют большой объем ресурсов хоста, приводя к понижению производительности и количества ВМ	До 30% уменьшают потребление ресурсов хоста за счет новых технологий сканирования, увеличивают плотность виртуализации м сканируют до 70 раз быстрее
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	Помогают избежать конфликта ресурсов, таких как антивирусные штормы
Необходимо обновлять базу сигнатур в каждой ВМ	Понижается трудоемкость обеспечения безопасности: нет необходимости проверять и обновлять сигнатуры на каждой ВМ. Эти процедуры автоматически выполняются на хосте

Acronis

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

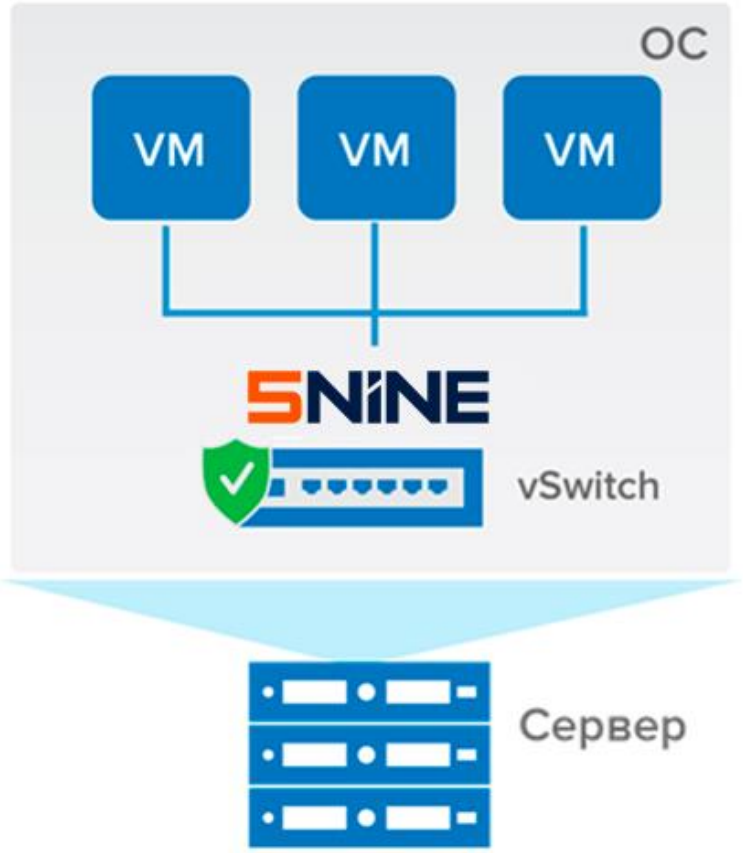
Глава 9 «Рекомендации по обеспечению ИБ виртуальных машин» :

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

Acronis

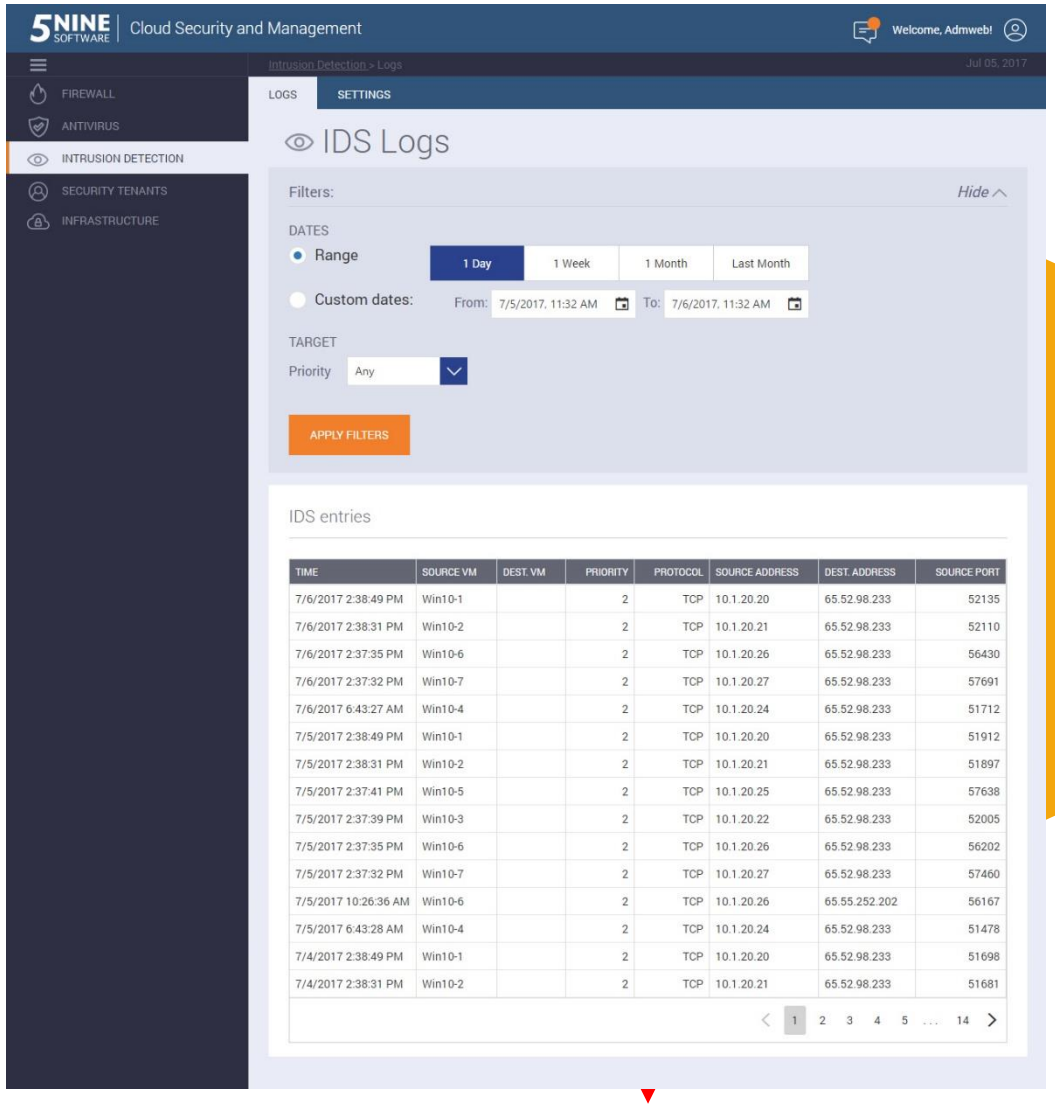
Acronis Cloud Security -современное безагентное СЗИ для Hyper-V на уровне гипервизора

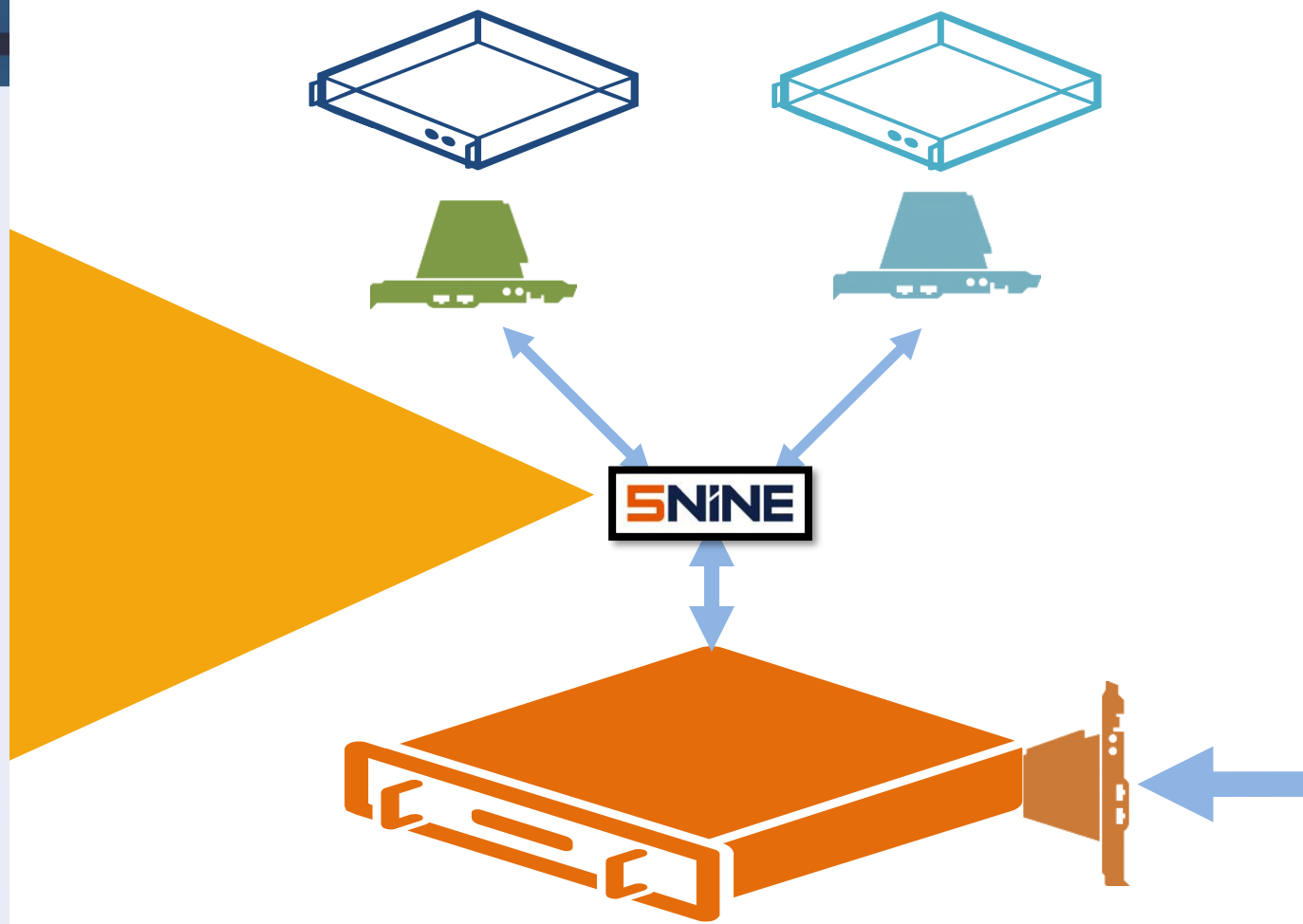
- Многоуровневая защита: межсетевой экран, безагентный антивирус, система обнаружения вторжений в едином решении
- Микросегментация инфраструктуры для защиты от атак. Поддержка SDNv2
- Простота управления и интеграция в средства управления инфраструктурой, что расширяет ее возможности
- Малое потребление ресурсов. Acronis Cloud Security экономит до 30% ресурсов сервера и работает до 70 раз быстрее традиционных СЗИ
- Безагентный способ защиты. Не требует установки агента в каждую ВМ
- Мониторинг, контроль доступа, логирование. Интеграция с SIEM
- Соответствие требованиям 152-ФЗ, Приказам ФСТЭК №17 и 21, PCI DSS, другим отраслевым стандартам
- Веб-портал для SECaaS



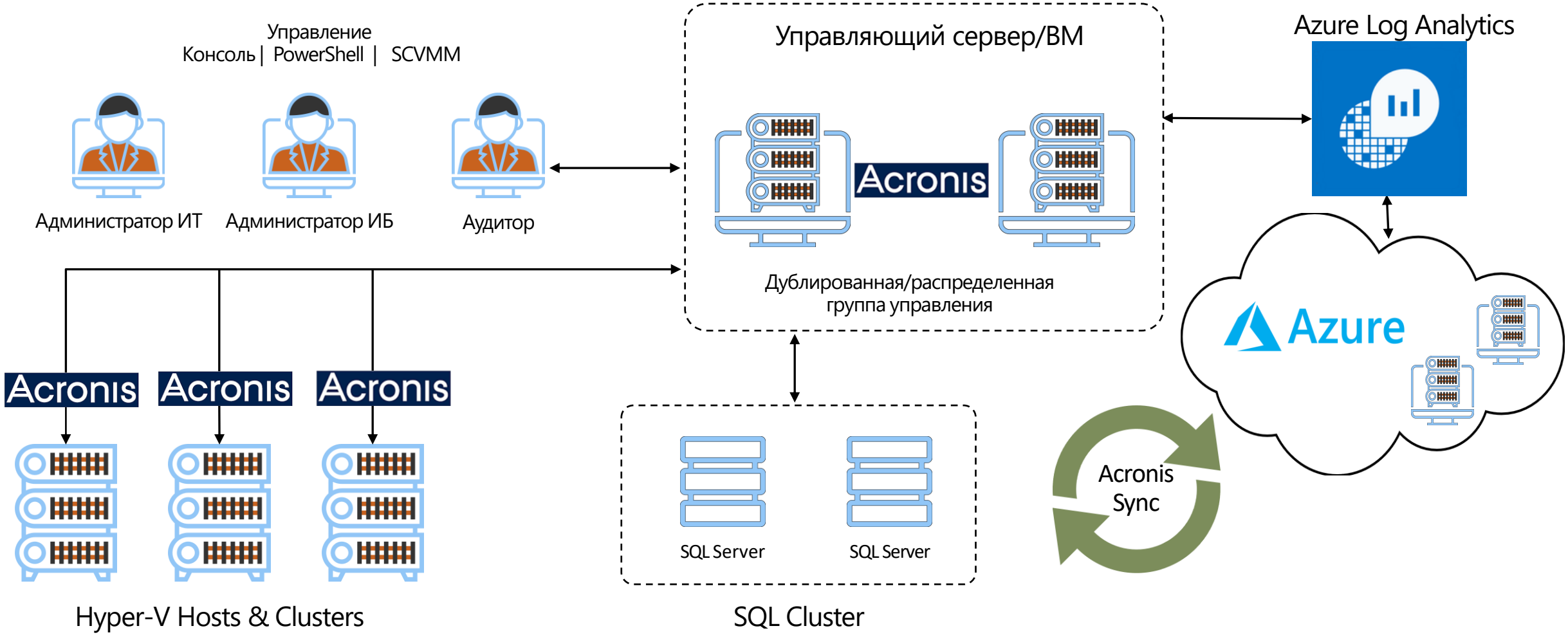
Acronis

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

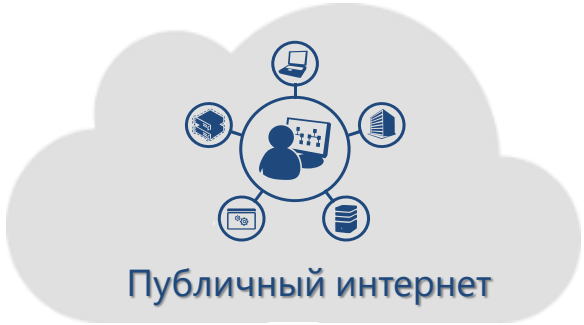




Безопасность с высокой доступностью для гибридной инфраструктуры



Поведенческий анализ и прогноз – основа СЗИ нового поколения

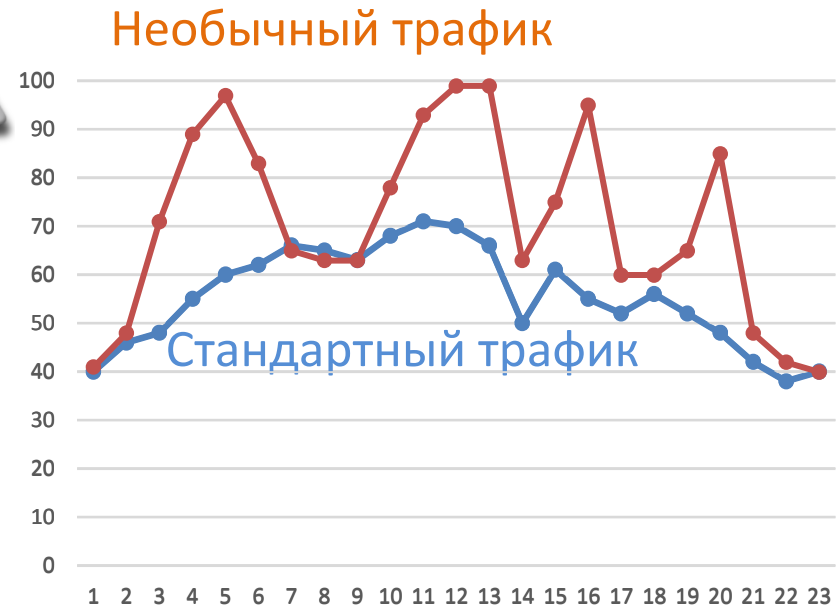


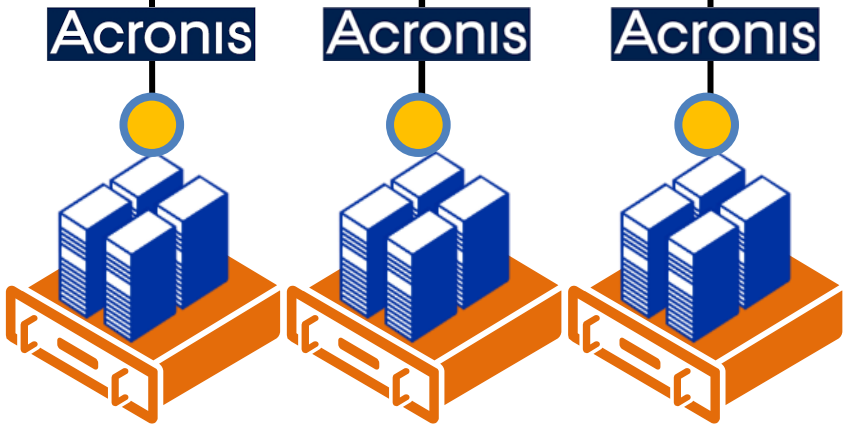
Acronis Cloud Security
управляющий сервер/ВМ

Bitdefender

SNORT

Acronis



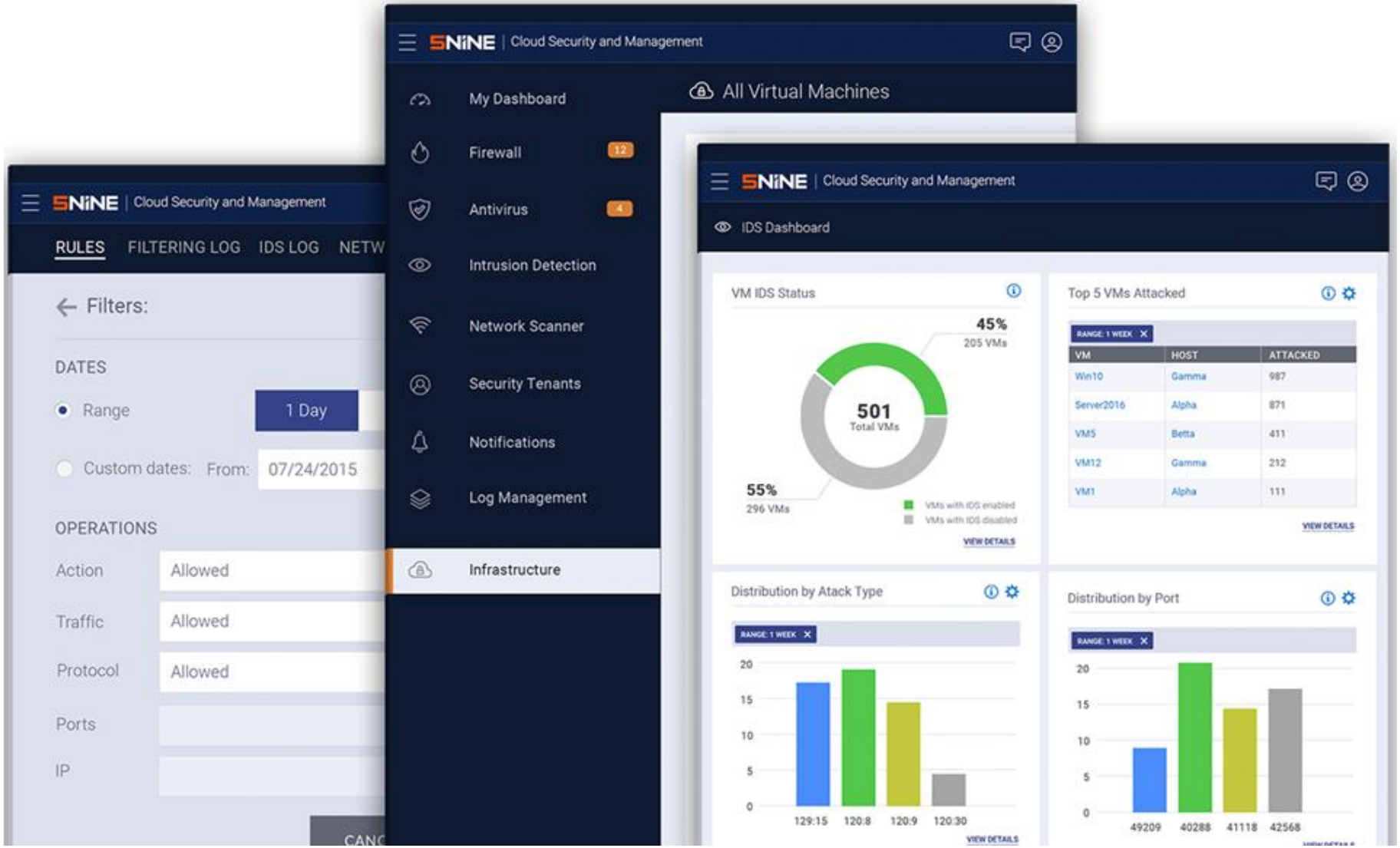


Hyper-V Hosts

БД SQL Server

Acronis

Веб-портал для управления инфраструктурой и безопасностью

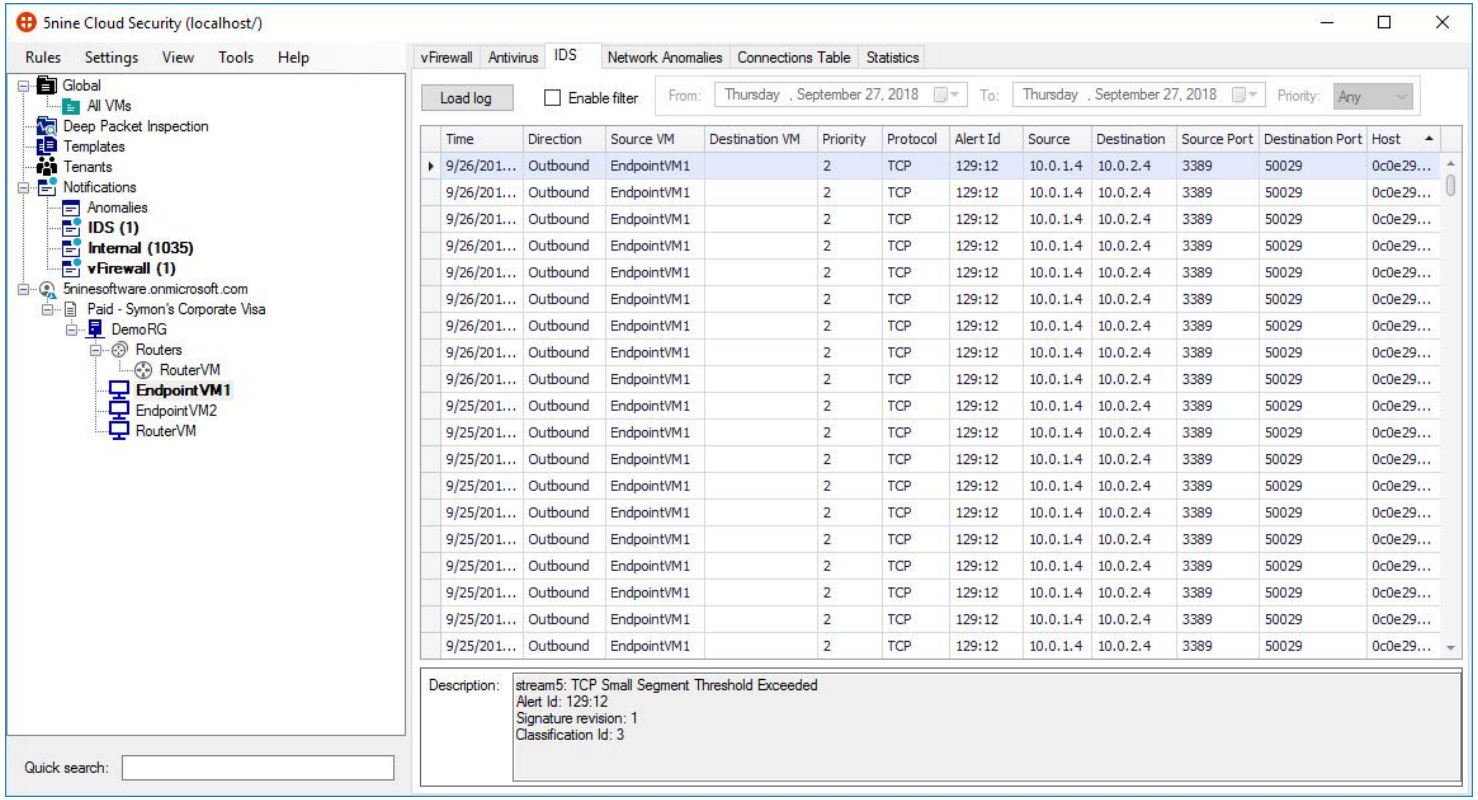


Acronis для Microsoft Azure

Acronis Cloud Security for Azure

Acronis Cloud Security for Azure обеспечивает:

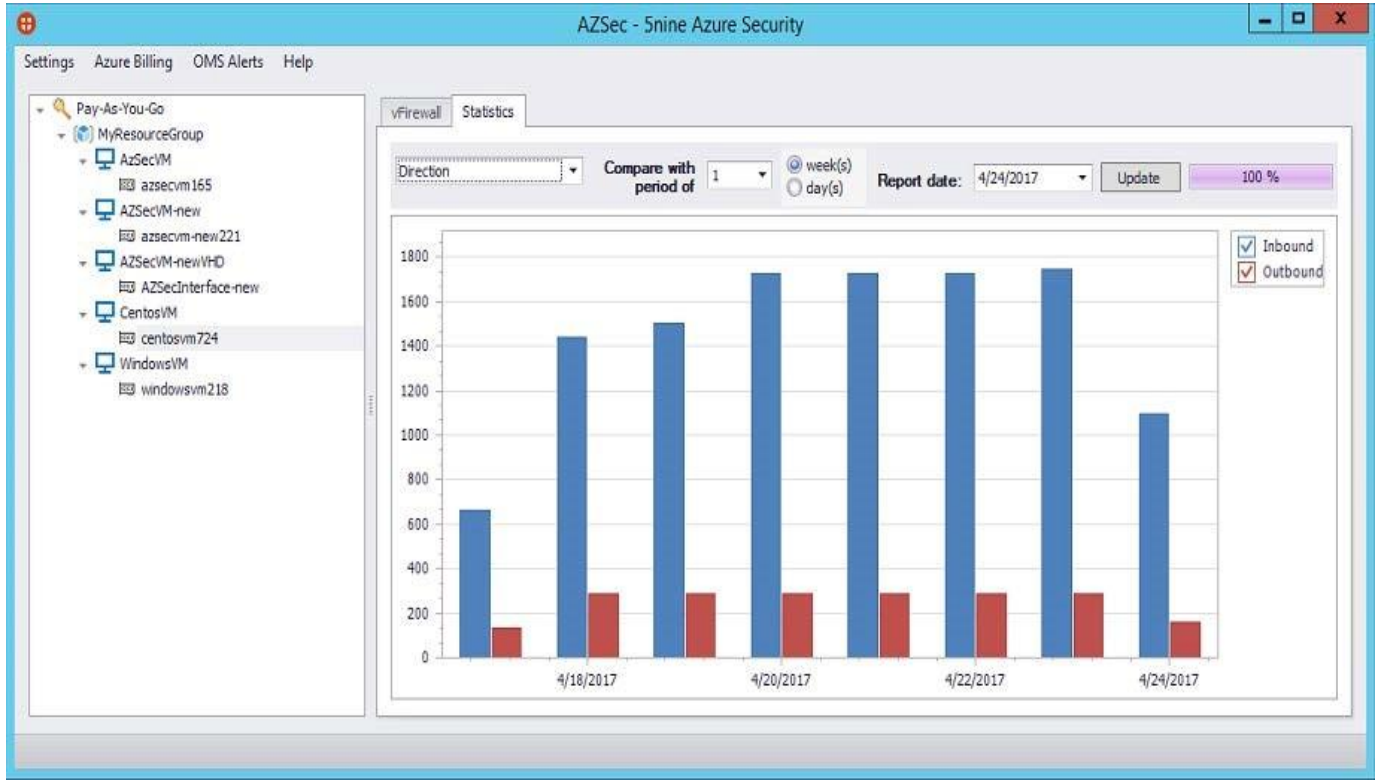
- Централизованное управление безопасностью
- Управление подписками Azure
- Виртуальный межсетевой экран
- Deep Packet Inspection (DPI)
- Безагентный антивирус
- Система обнаружения вторжений (IDS)
- Качество обслуживания (QoS)
- Ведение журнала внутренних событий и действий пользователей
- Ролевая модель
- Оповещения по электронной почте
- Выполнение требований законодательства и аудит информационной безопасности



Acronis

Интеграция безопасности облака и ЦОД позволяет

- Объединить защиту и контроль гибридной инфраструктуры предприятия в едином решении
- Использовать интеграцию с сервисами Microsoft Azure для повышения безопасности
- Решить проблемы отдела ИБ при миграции в Azure



Acronis

Acronis Cloud Manager- решение для управления гибридным облаком

Acronis Cloud Manager

Современное решение для централизованного управления тысячами ВМ в географически распределенных ЦОД для крупных компаний обеспечивает в одной консоли:

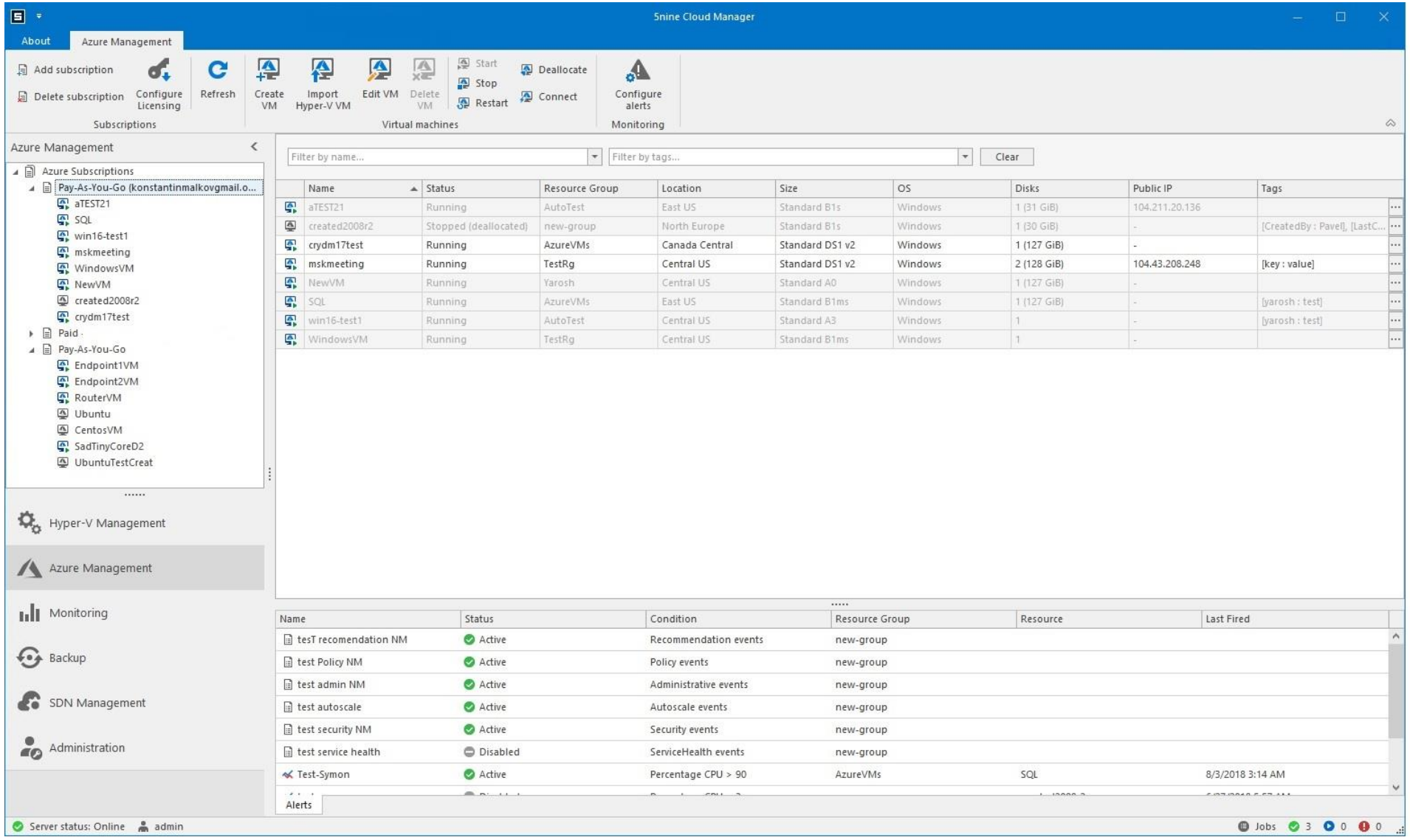
- Контроль доступа администраторов к группам серверов, ресурсам и управлению виртуальными машинами
- Управление ресурсами в Azure и в своем ЦОД в одной консоли
- Мониторинг, обнаружение и решение проблем с производительностью
- Автоматизированное резервное копирование, восстановление и репликация данных
- Поддержка отказоустойчивых кластеров
- Поддержка контроллера сети Software Defined Networking (SDN). Создание и управление виртуальными сетями

Веб-портал для удаленного управления и предоставления услуг

Любые сценарии - крупные компании и сервис-провайдеры

Acronis

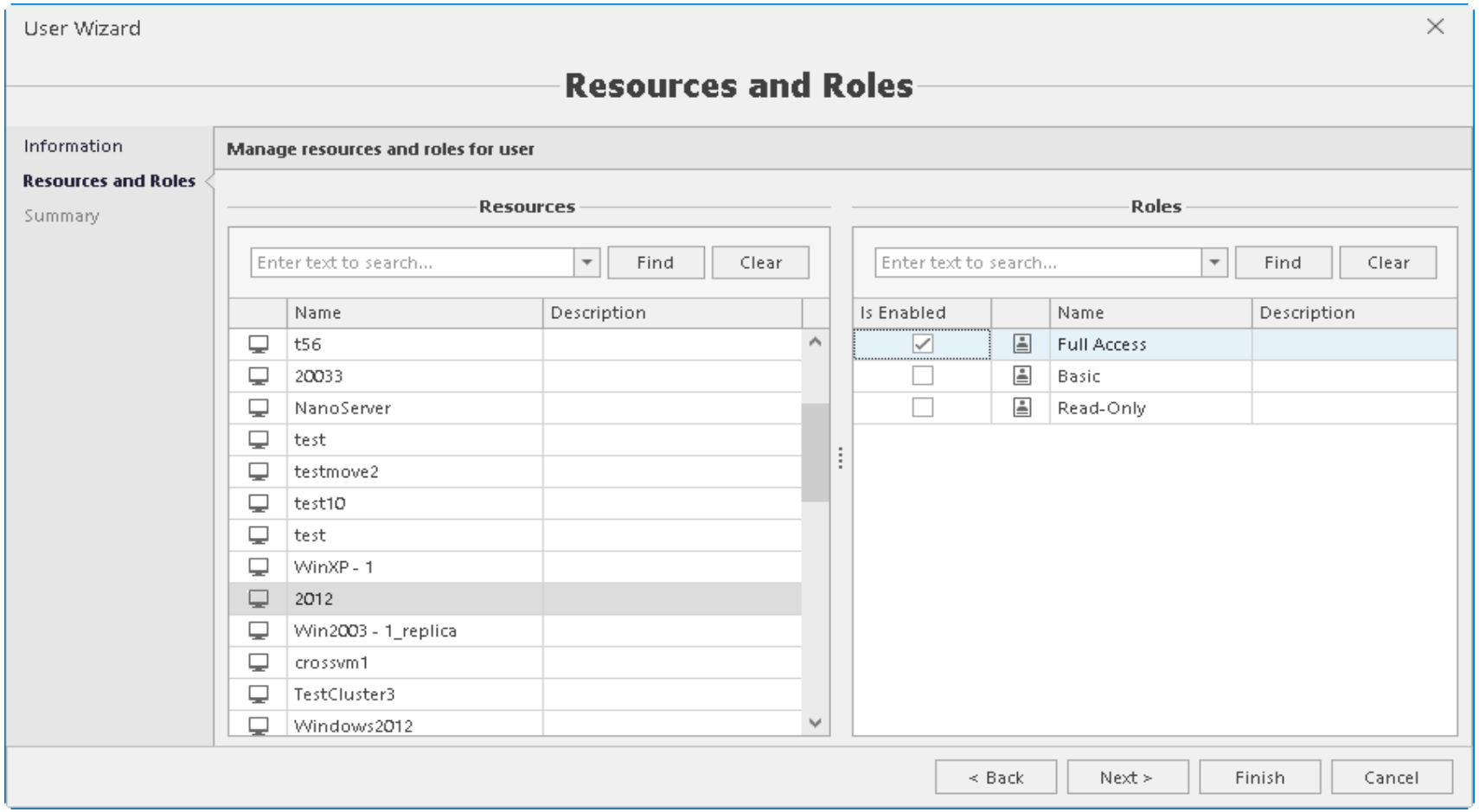
Пользовательский интерфейс



Acronis

Управление пользователями, клиентами и ролями

- Acronis Cloud Manager поддерживает мультитенантные среды
- Acronis Cloud Manager поддерживает ролевую модель доступа к управлению
- Администратор назначает клиентов, пользователей, их роли и соответствующие им ресурсы



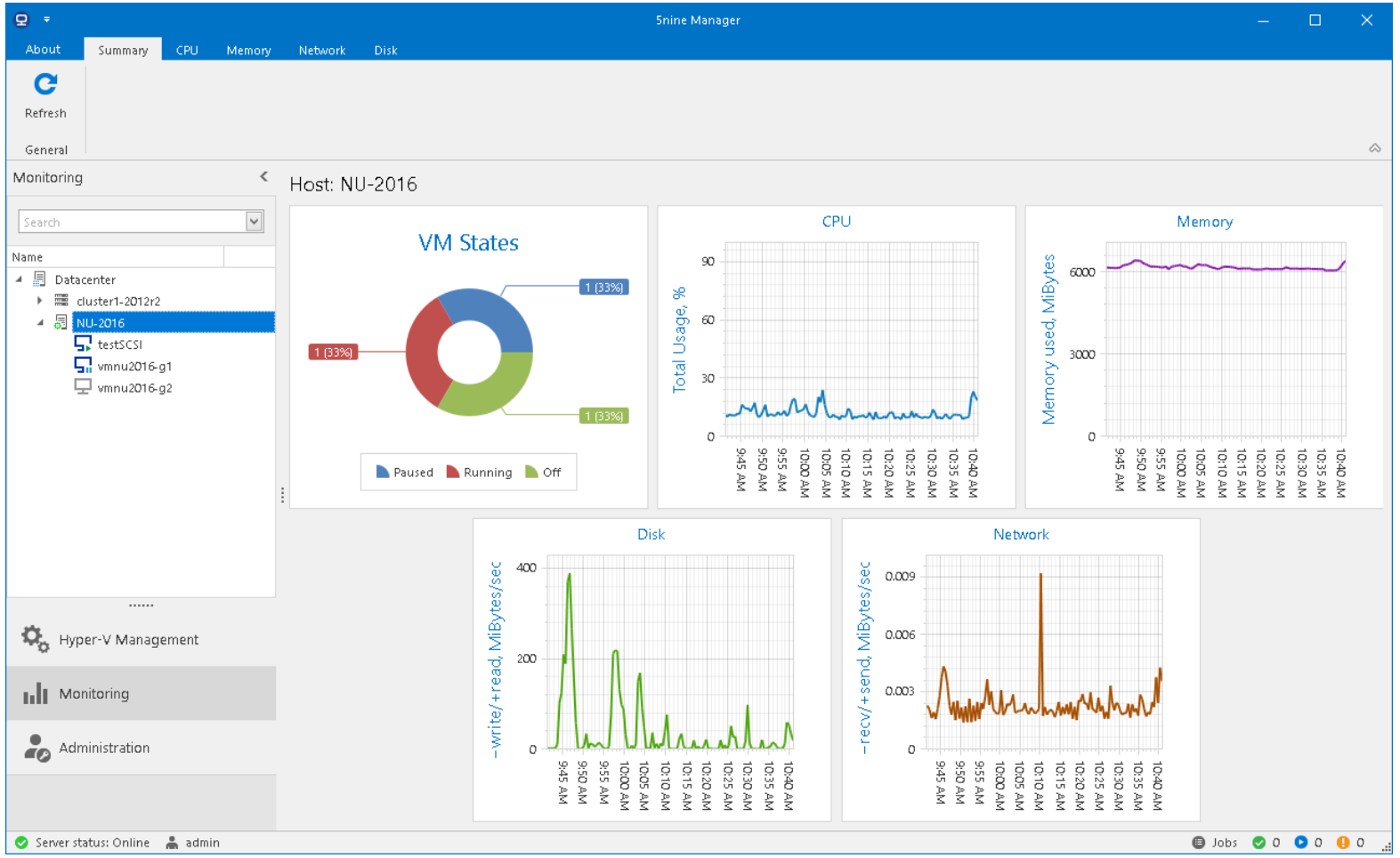
Acronis

Мониторинг Hyper-V и Azure

Acronis Cloud Manager обеспечивает мониторинг:

- Обобщённых данных
- CPU
- Памяти
- Сети
- Кластеров
- Хостов
- Дисков

Предусмотрена настройка уведомлений администраторов о событиях по электронной почте

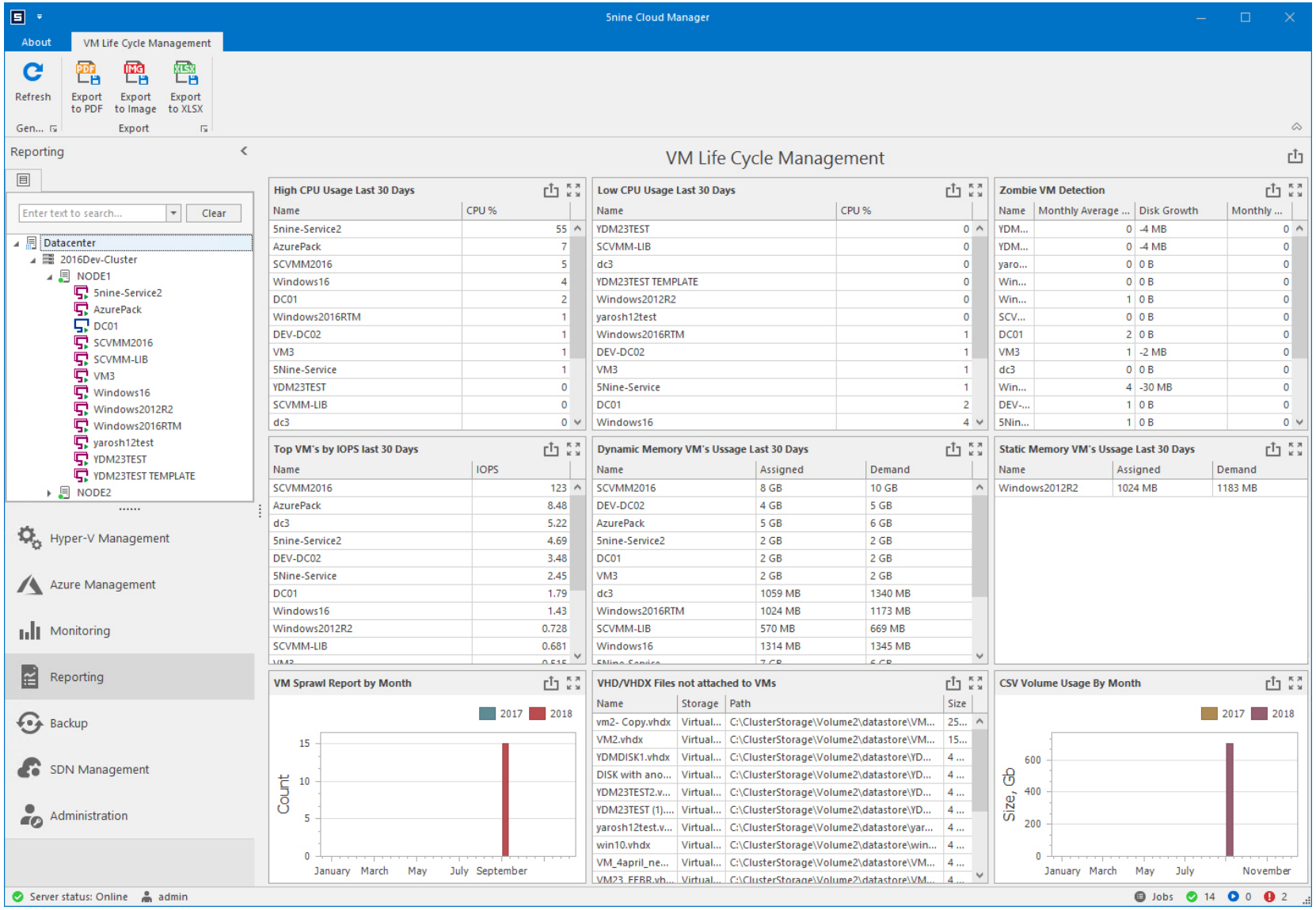


Acronis

Отчеты

Acronis Cloud Manager обеспечивает отчеты с экпортом в PDF, PNG или XLSX:

- Min/max использование ЦП;
- ВМ с наибольшим количеством IOPS;
- Использование динамической и статической памяти;
- Использование общих томов кластера (CSV)
- другие

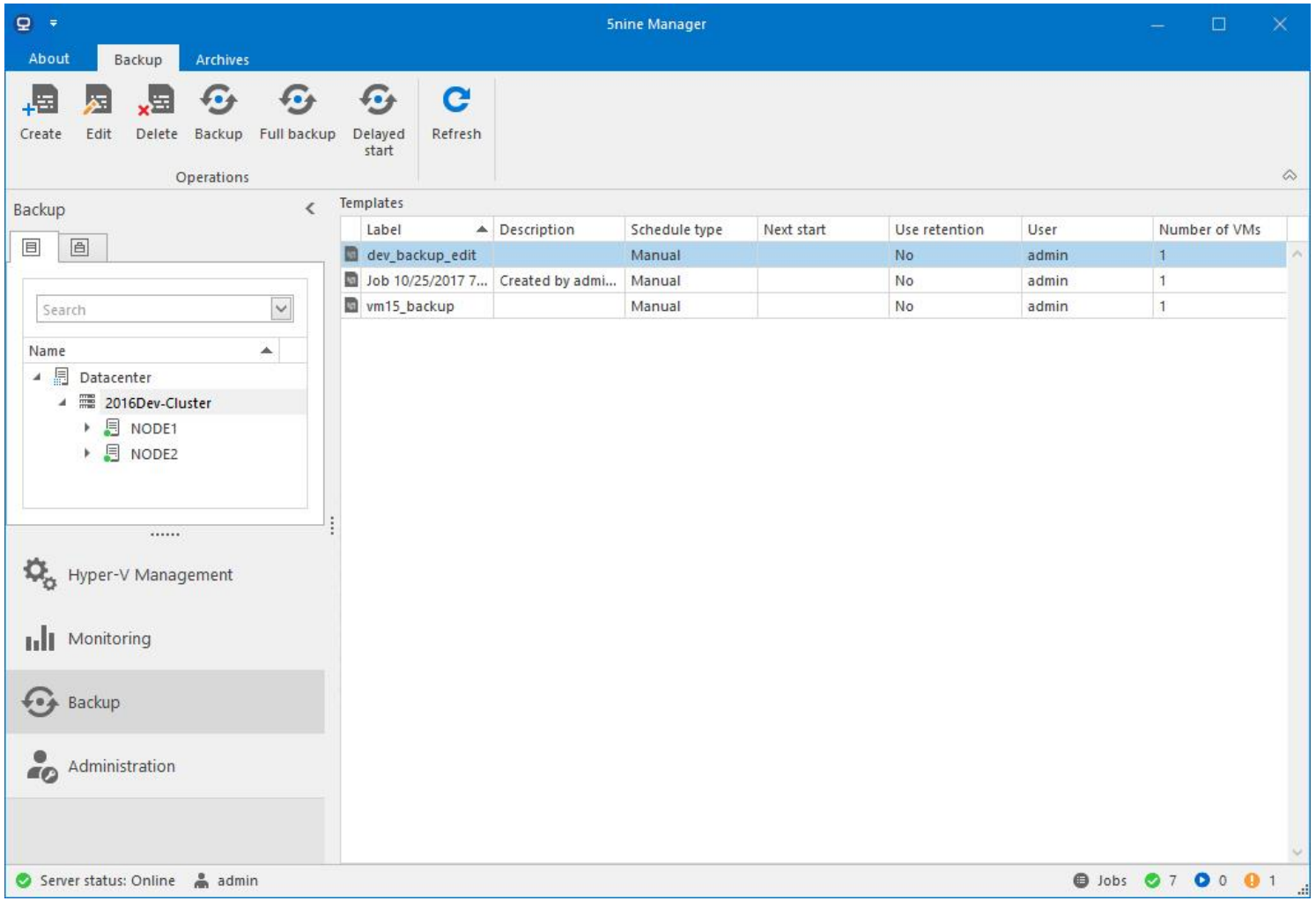


Acronis

Резервное копирование

Acronis Cloud Manager поддерживает следующие функции резервного копирования:

- Создание заданий по расписанию, отложенных заданий, просмотр, редактирование, удаление и управление текущими и выполненными заданиями;
- Настройка параметров резервного копирования: кодировки, степени сжатия, разделения на блоки, параметров хранения/удаления старых файлов и др.
- Полное и инкрементальное резервное копирование
- Бэкап в Azure

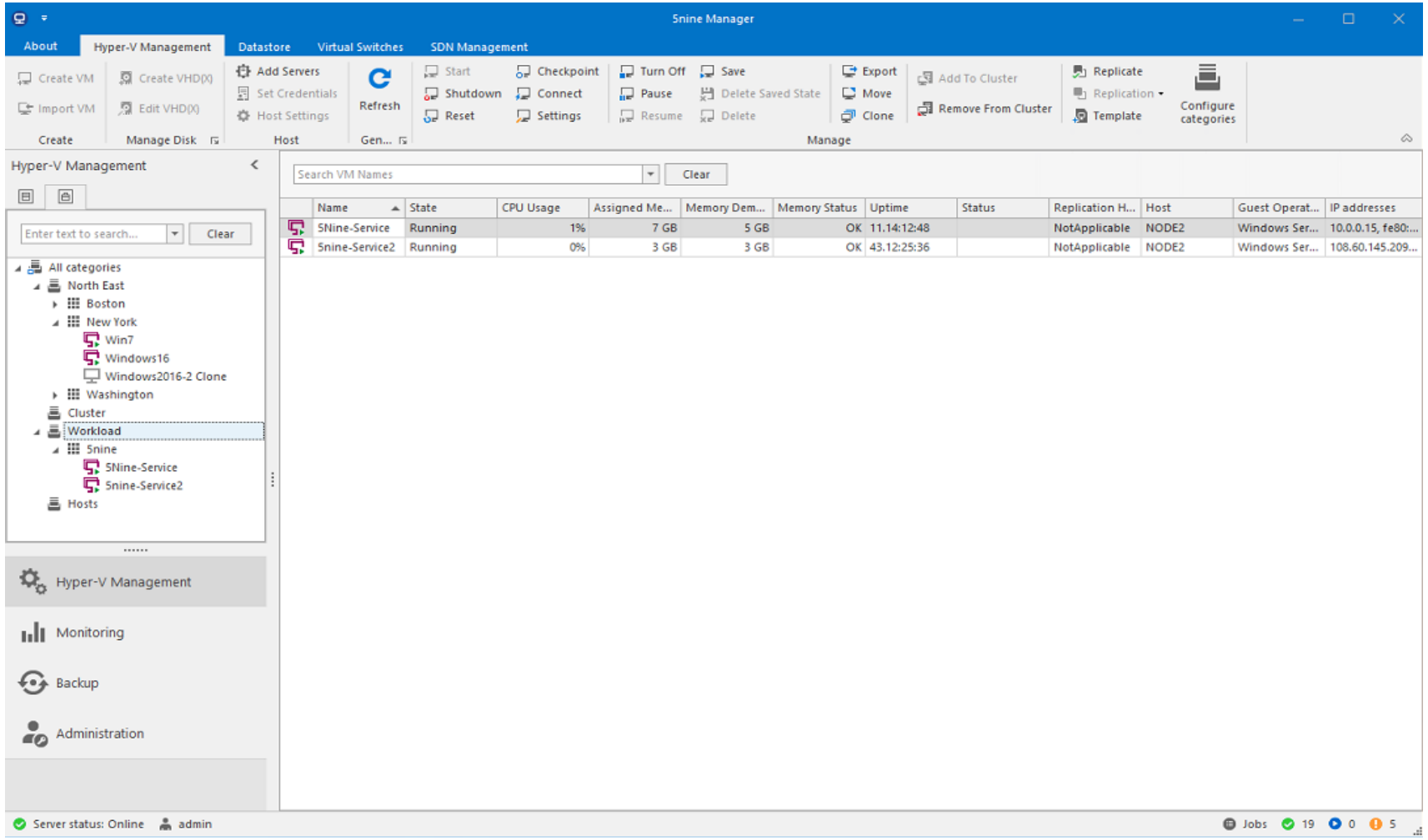


Acronis

Логическая группировка ресурсов

Ресурсы можно группировать:

- Приложениям
- Функциям
- Расположению
- Администрированию
- Другим признакам



Acronis

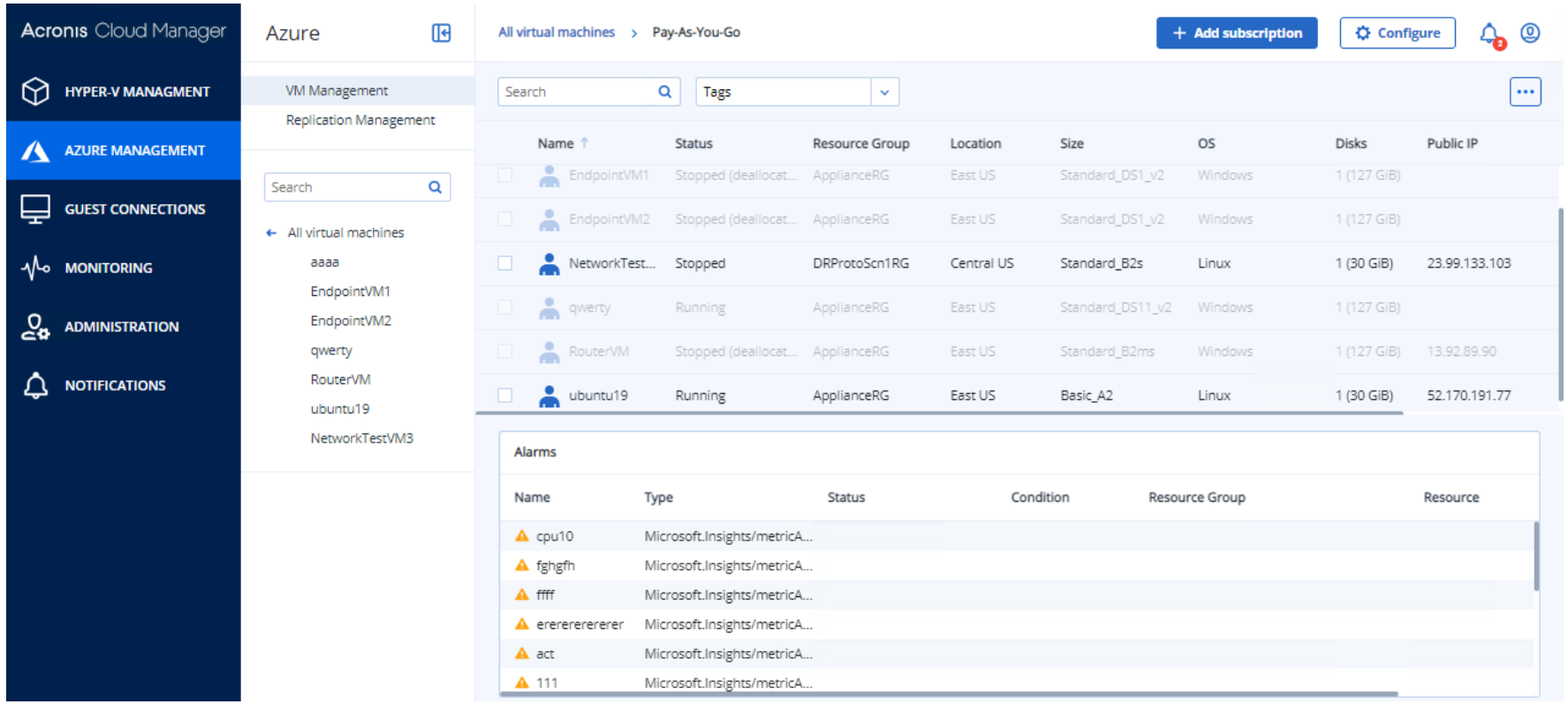
Веб-портал

С веб-порталом для управления Acronis Cloud Manager вы сможете:

• Безопасно управлять и мониторить инфраструктуру Hyper-V и Azure через веб-портал

• Разделить ресурсы между отделами, предприятиями или клиентами и ограничить права на управление для групп пользователей через ролевую модель для безопасности

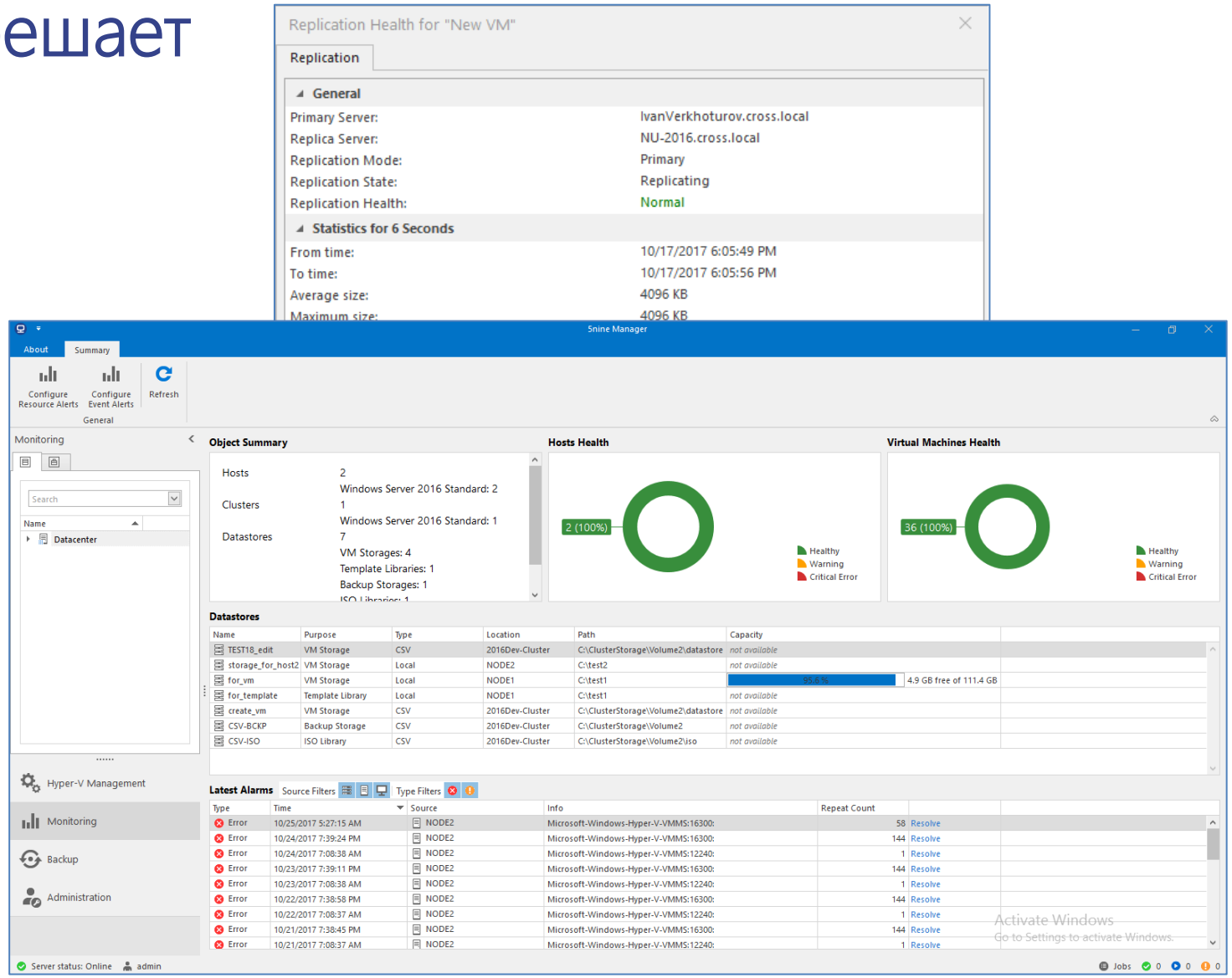
• Удаленно управлять миграцией и репликацией ВМ



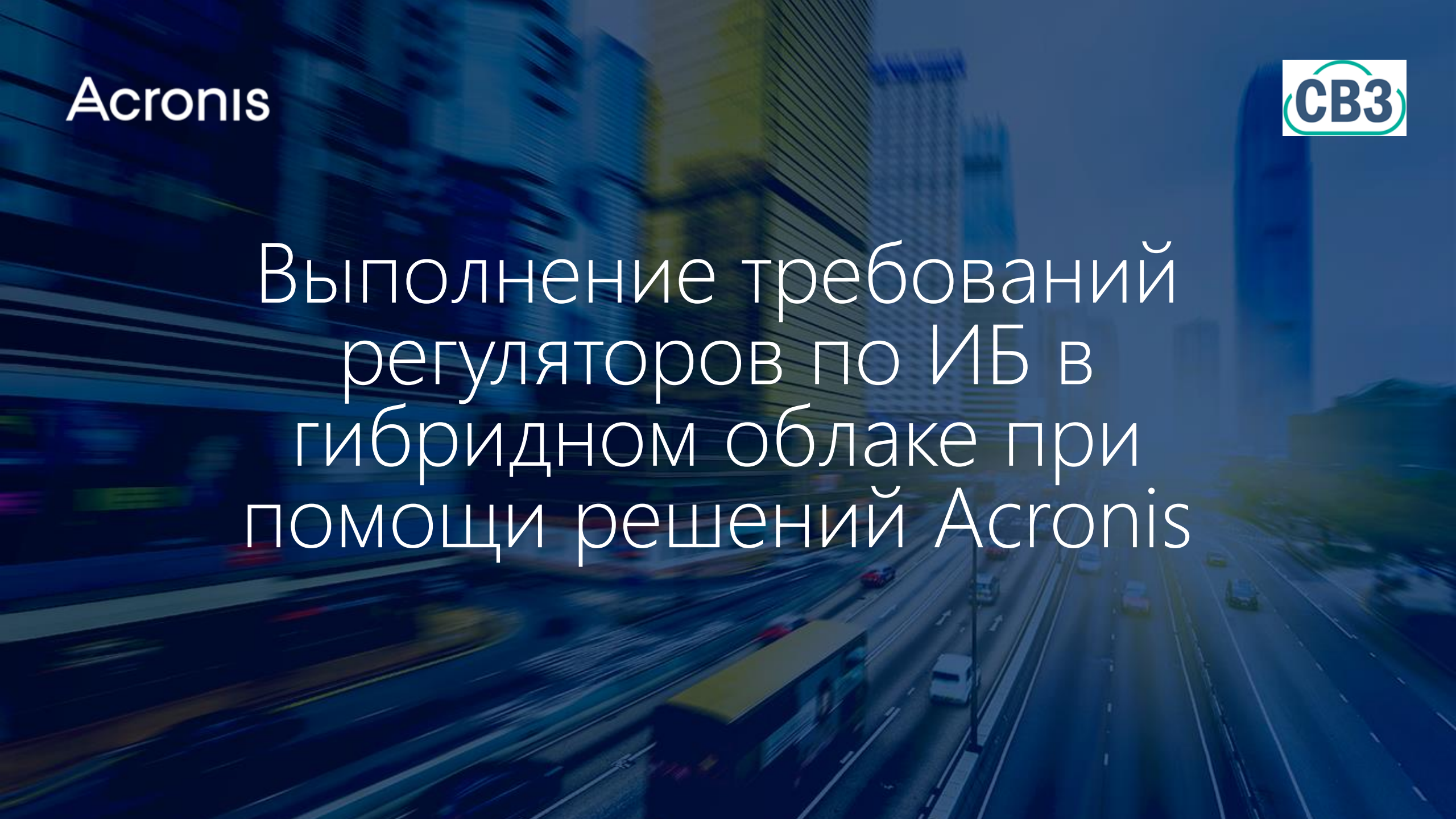
Acronis

Acronis Cloud Manager решает проблемы:

- Централизованного управления гибридным облаком
- Миграции нагрузок в облако
- Мониторинга гибридного облака
- Повышения безопасности управления через разделение прав доступа
- Экономии средств и ресурсов на рутинные операции
- Защиты информации через автоматическое резервирование и восстановление, в т.ч. от вирусов шифраторов



Acronis



Выполнение требований регуляторов по ИБ в гибридном облаке при помощи решений Acronis

Выполнение 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.

Acronis

Acronis Cloud Security и Hyper-V Windows Server для PCI DSS

Цели контроля	Требования PCI DSS	Реализация при помощи Acronis Cloud Security
Построение и сопровождение защищённой сети	1. Установка и обеспечение функционирования межсетевых экранов для защиты данных держателей карт	Acronis 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	Acronis 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	Acronis 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	Acronis 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 Acronis Cloud Security. Интеграция с централизованными системами сбора данных позволяет обеспечить необходимую длительность хранения информации
	11. Регулярное тестирование систем и процессов обеспечения безопасности	Acronis 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

Как решения Acronis помогают защитить гибридную среду

Многоуровневая защита: микросегментирование при помощи при межсетевого экрана, безагентный антивирус, система обнаружения вторжений в едином решении

Интеграция в средства управления инфраструктурой, такие как Windows Server и Azure Log Analytics для расширения возможностей защиты.

Безагентный способ защиты уменьшил потребление ресурсов до 30%, а скорость сканирования выросла до 70 раз. Снизилась зависимость от действий персонала

Веб-портал упростил управление безопасностью и ресурсами

Решение для Azure упростило защиту в облаке, позволило поддерживать единые политики безопасности в облаке и в своем ЦОД, контролировать события безопасности, получать уведомления о возможных инцидентах, повысить скорость реакции на атаки и выполнить требования регуляторов и аудиторов

Acronis

Клиенты Acronis -5nine

Acronis

Больше информации и тестирование продуктов Acronis-5nine :

Управление гибридным облаком https://svzcloud.ru/acronis-cloud-manager/

Управление датацентром https://svzcloud.ru/acronis-manager-standard/

Безопасность гибридного облака https://svzcloud.ru/acronis-cloud-security/

Миграция https://svzcloud.ru/acronis-cloud-migration/

Acronis