КОД безопасности

Безопасность виртуализации

сегодня и завтра

Что мы видим сегодня?

- Растянутый во времени переход с VMware
- Отсутствие явного лидера среди отечественных вендоров виртуализации
- Разделение задач сетевой защиты и защиты от НСД

Механизмы СЗИ

Защита жизненного цикла

Доверенная загрузка

Контроль привилегий

Унифицированность

Видимость

Межсетевое экранирование до L4/L7

Сегментация

Software Defined Networking

Прозрачность работы

Сетевая защита

Механизмы СЗИ

Защита жизненного цикла

Доверенная загрузка

Контроль привилегий

Унифицированность

Видимость

+ Регулятор

Межсетевое экранирование до L4/L7

Сегментация

Software Defined Networking

Прозрачность работы

+ Регулятор

Сетевая защита

- Похоже, что этот функционал встроен в современные среды виртуализации

~~– Похоже, что этот функционал встроен в современные среды виртуализации~~


Контроль доступа

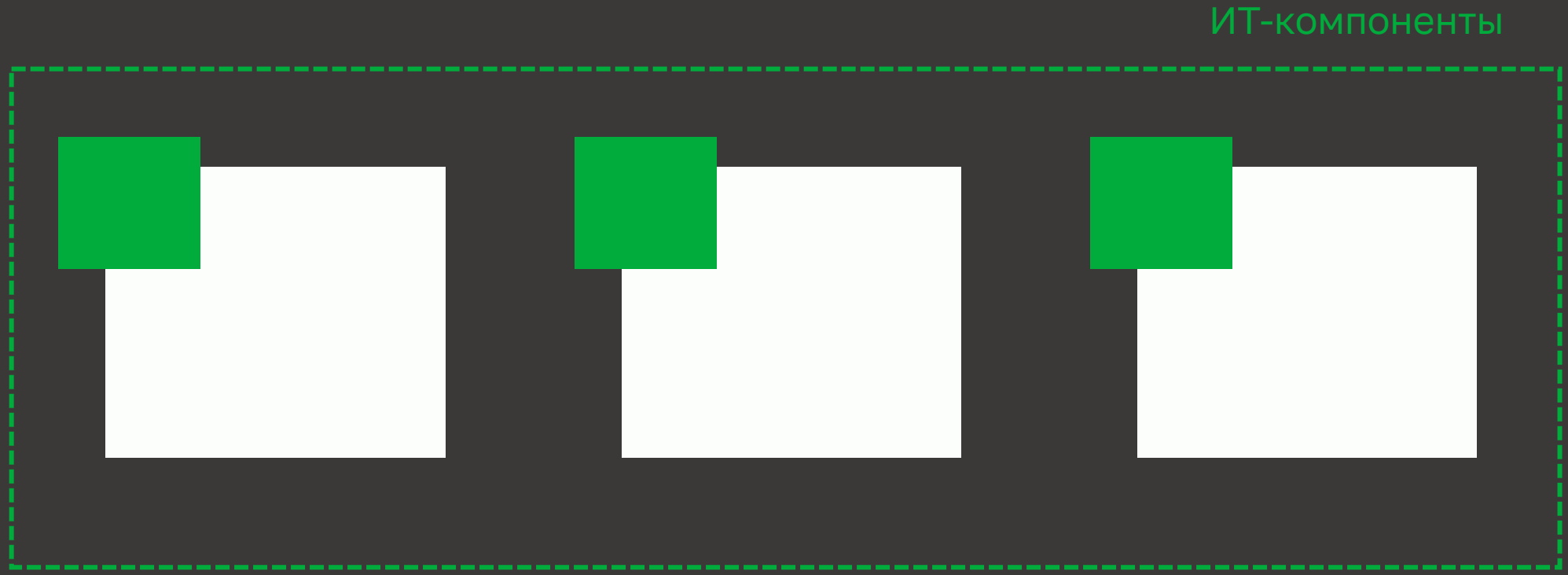

Гетерогенность


Контроль целостности

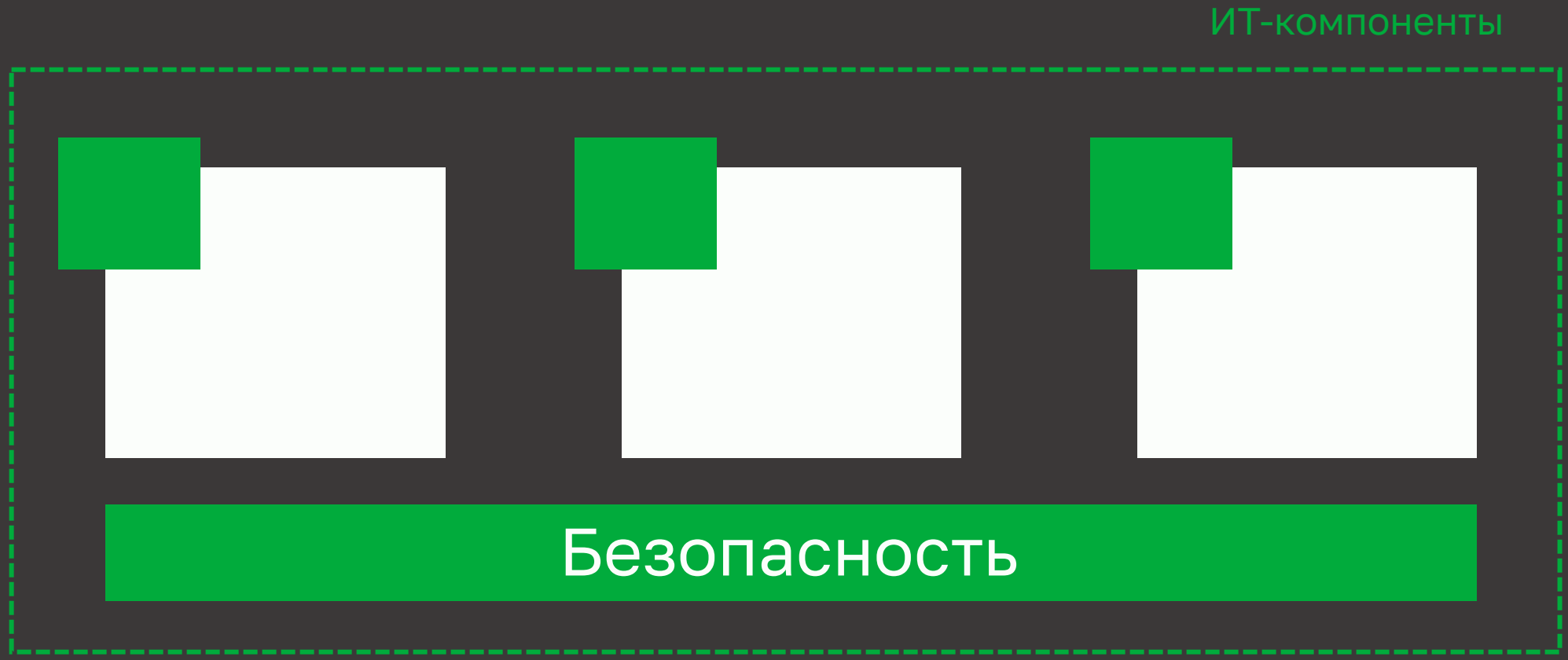

Гибкие сетевые возможности


Гарантированное затирание информации

Безопасность как процесс



Безопасность как процесс



Подробнее о сетях

Виртуальный NGFW

Особенности:

в контексте виртуализации

- высокая стоимость

- не подходит для сегментации внутри виртуальной инфраструктуры

- сложность администрирования

- необходим при использовании продвинутых механизмов защиты

Подробнее о сетях

МЭ уровня гипервизора

Особенности:

в контексте виртуализации

- не влияет на производительность

- гибкая сегментация

- устанавливается на гипервизор, не на ВМ

- выборочная инспекция

- правила привязываются к ВМ, не к адресу

Выбор решения исходит из потребностей
а не функционала

О других механизмах

Мультиарендность

- выделение сегментов внутри организации
- выделение сегментов во вне

SDN

- замена VMware NSX
- построение L2-связности между ВМ

Контроль внутри ВМ

- Secret Net Studio внутри ВМ
- единая консоль управления

Службы каталогов

- работа с пользователями AD
- работа с пользователями ALD Pro

Решаемые задачи

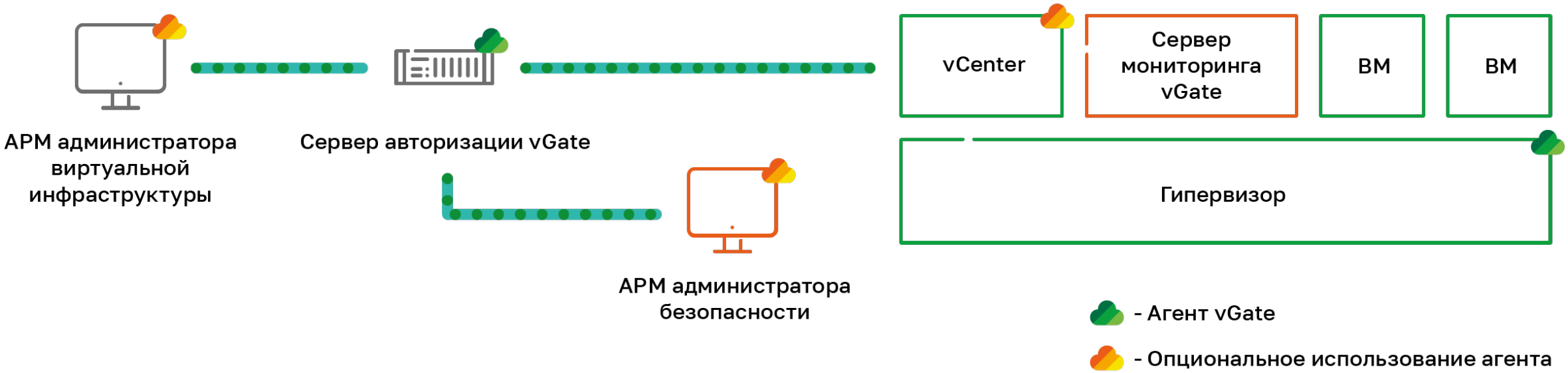
vGate

Средство микросегментации и защиты жизненного цикла виртуальных машин

- Защита от несанкционированных операций в виртуальной среде
- Защита от специфических для виртуализации угроз
- Контроль привилегированных пользователей
- Микросегментация
- Мониторинг и управление инцидентами
- Выполнение требований регуляторов

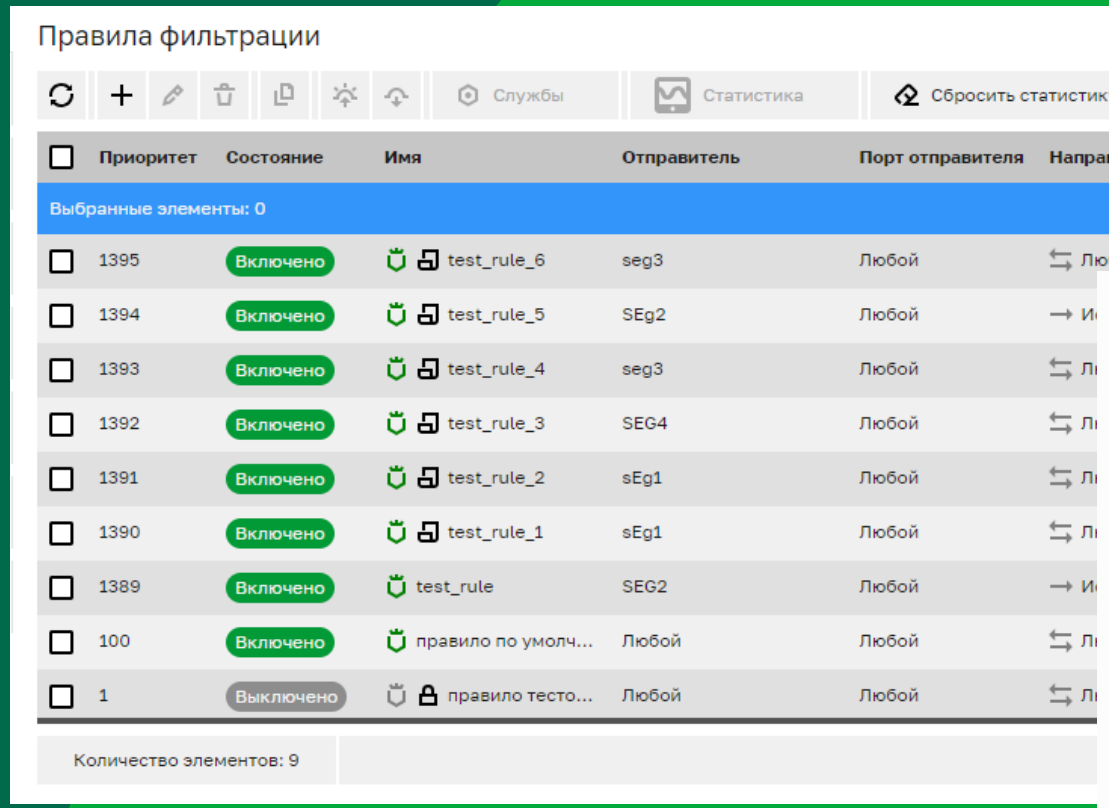
	СЗИ	МЭ	SDN
VMware vSphere 6.5	+	+	-
VMware vSphere 6.7, 7.0	+	+	+
Альт Сервер Виртуализации 10.1 (OpenNebula 5.10.5, Proxmox 7.2)	+	+	-
Р-Виртуализация 7.0.13 (Скала-Р Управление 1.98)	+	+	-
zVirt Node 3.3, 4.0	+	Лето 2024	-
РЕД Виртуализация 7.3	+	Лето 2024	-
ROSA Virtulization 2.1	+	Лето 2024	-
SpaceVM 6.2.0, 6.2.1	+	2025*	-
HostVM 4.4.8 в составе oVirt Node 4.4.8	+	Лето 2024	-
Utinet Glovirt 2.1.1	+	Лето 2024	-
OpenNebula 6.4.0.1 в составе Ubuntu 20.04.5 LTS	+	+	-
Proxmox 7.4-1, 8.0-2	+	+	-
ПК СВ «Брест» by Astra	-	Лето 2024	-
Vmmanager by Astra	-	2025*	-
ECP Veil	Лето 2024	2025*	-

Архитектура



Сегментирование

+ SDN



Создание правил фильтрации

для:

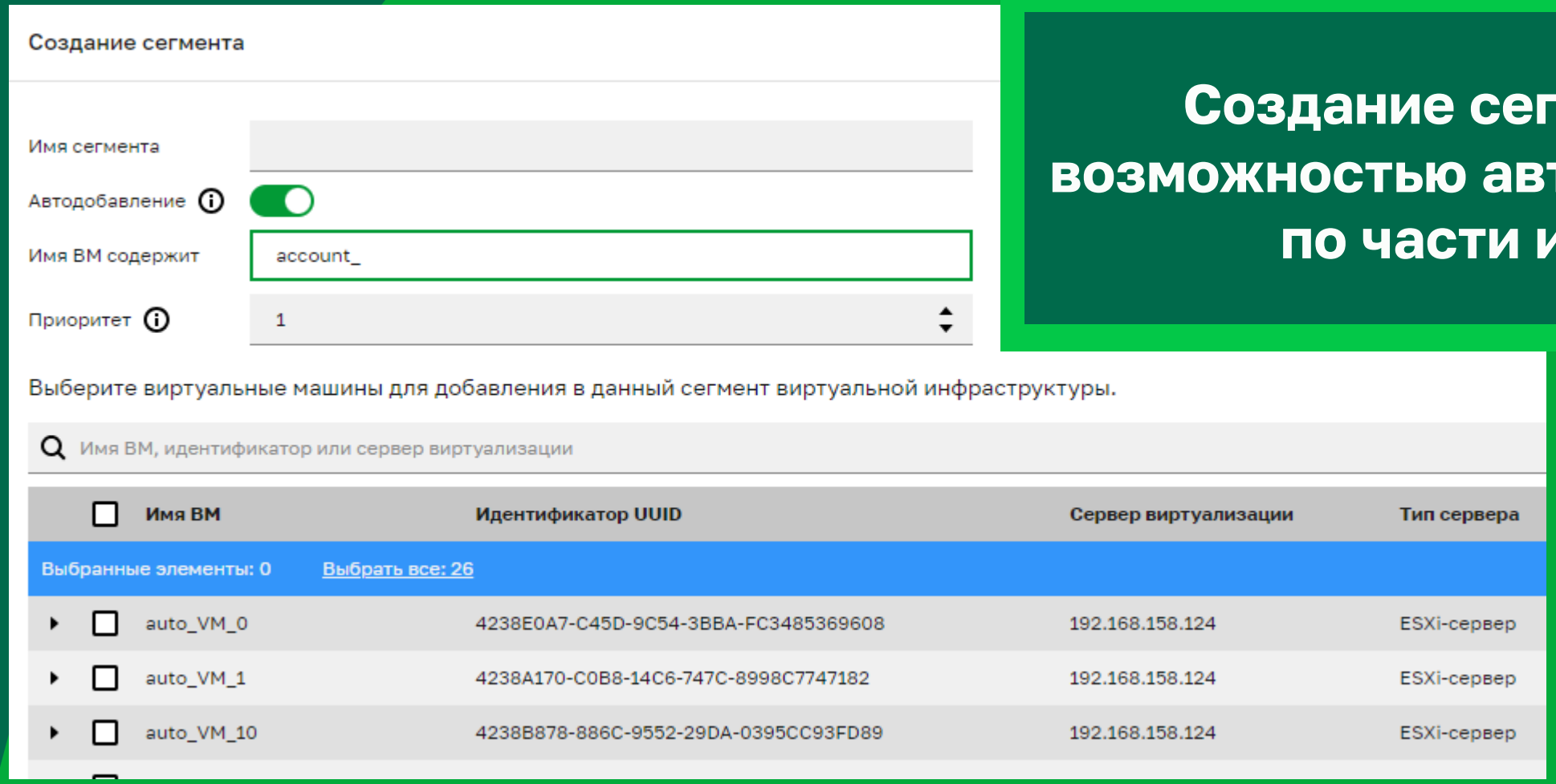
- IP-адресов
- диапазона IP-адресов
- подсетей
- сегмента
- виртуальной машины
- MAC-адреса

по:

- направлению
- протоколу
- службе
- порту
- типу фрагментации
- действию

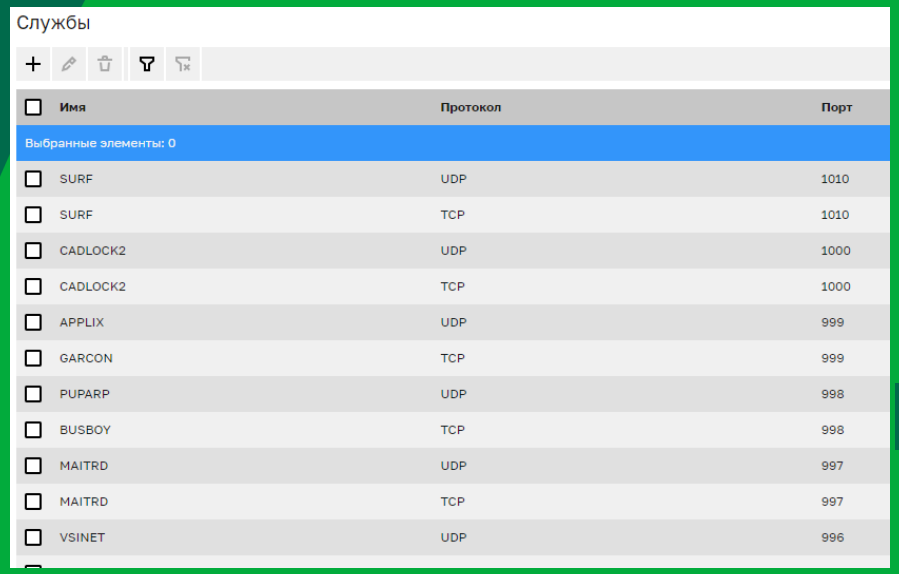
Сегментирование

Создание сегментов с возможностью автодобавления по части имени



Сегментирование

контроль сессий

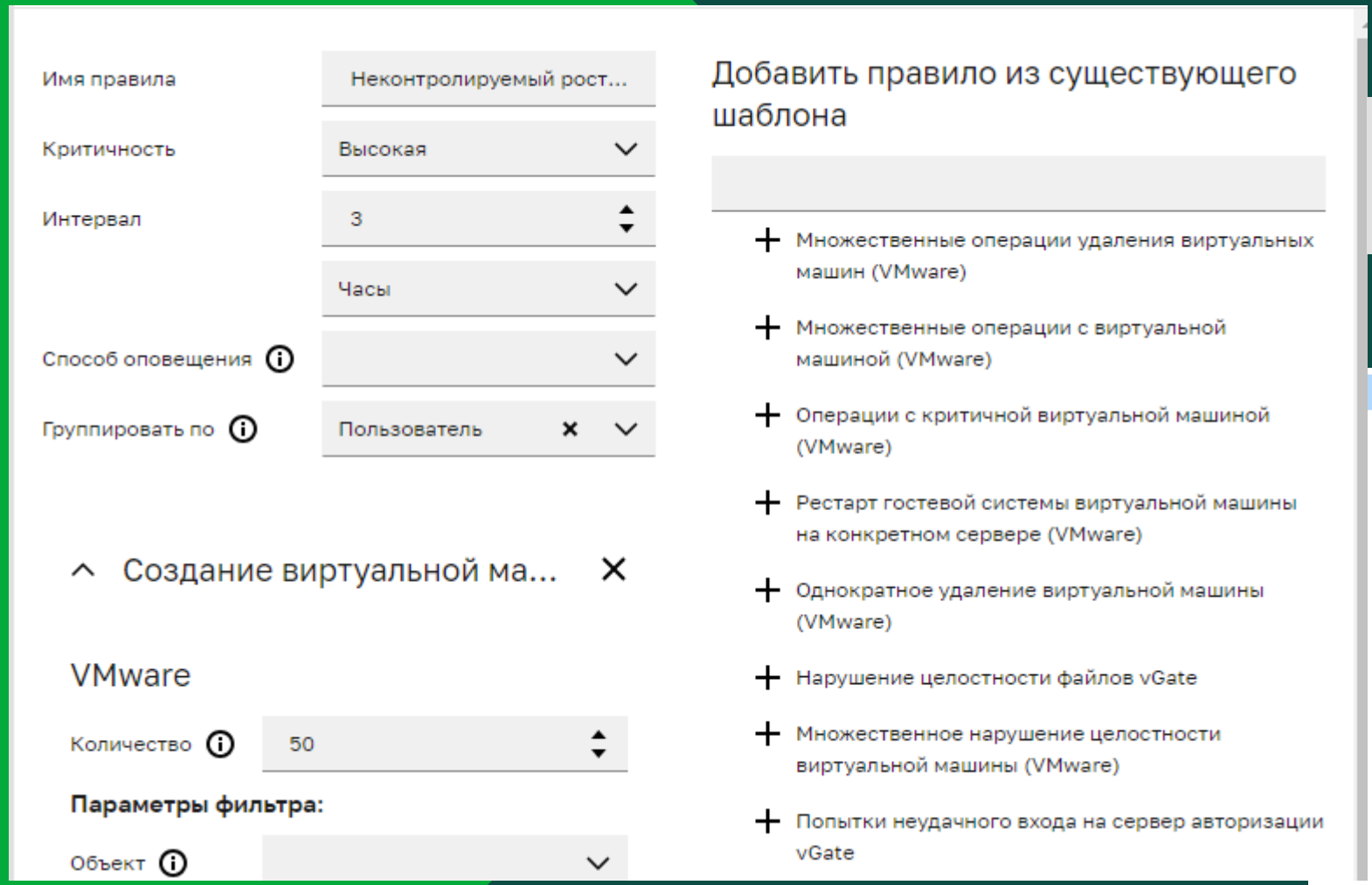


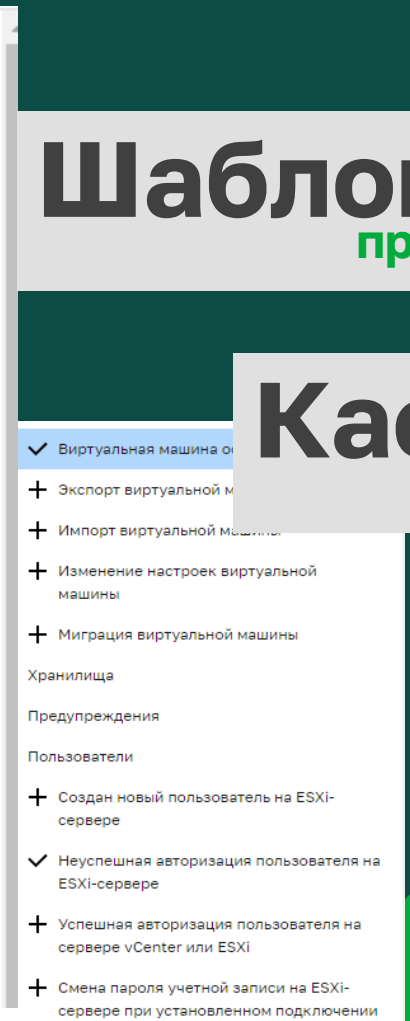
каталог служб

Мониторинг


Панель мониторинга
Тепловая карта событий аудита
Ноя-22
Дек-22
Янв-23
Фев-23
Мар-23
Апр-23
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
0
0-100
100-2000
2000-5000
5000-10000
10000+
Проблемы в работе vGate
24
18
12
6
0
21-04-2023
02-01-2024
05-01-2024
Топ-10 сегментов по разрешенному трафику
SEg2
seg3
Объекты и учетные записи по категориям к...
60
45
30
15
0
Сетевые адаптеры vSphere
ESXi-серверы
KVM-серверы
Хранилища данных Скала-Р
ВМ KVM
Виртуальные сети vSphere
Хранилища данных vSphere
Учетные записи
ВМ vSphere
Без категории
Желтый
Зеленый
События безопасности vGate
Успех
Уведомление
Предупреждение
Ошибка
Наиболее активные пользователи vGate
admin@TESTESX
admin4@TESTESX
adusername1@CD2012R2.RD2012R2.VGFOREST
admin2@TESTESX
ADUserName1@CD2012R2.RD2012R2.VGFOREST
adusername2@CD2012R2.RD2012R2.VGFOREST
rest_test_user45@TESTESX
user_aib@TESTESX
user_avi_aib@TESTESX
Нарушение целостности виртуальных машин
4
+4
Активные правила фильтрации
47
+47
Виртуальные машины, для которых осущес...
37
+37
Топ-10 сегментов по заблокированному тра...
seg3
SEg2
SEG2
SEG4
segment2
SEG4
segment2
SEG2
SEg2
seg3

Правила корреляции

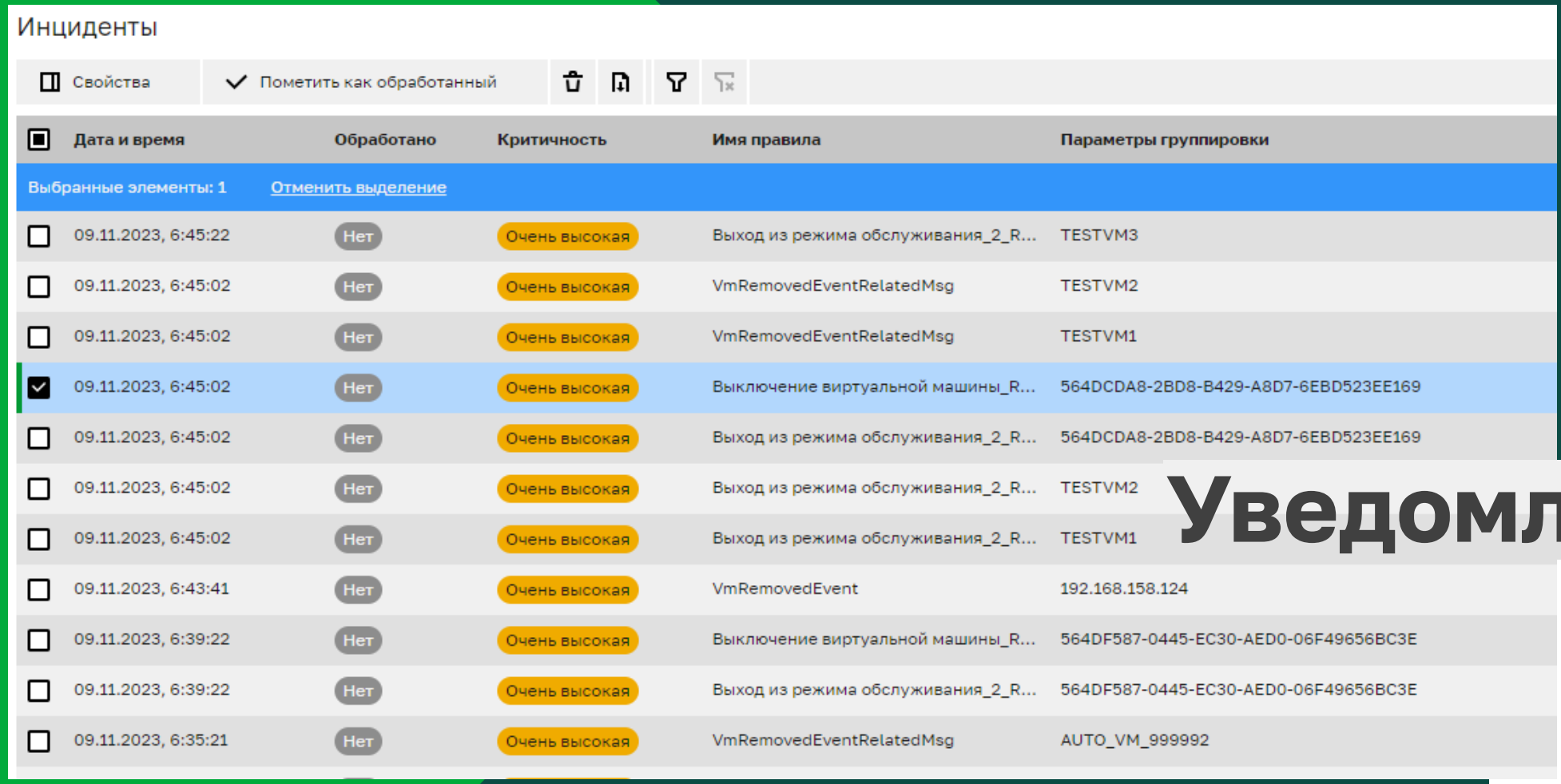




Шаблоны правил

Кастомные правила

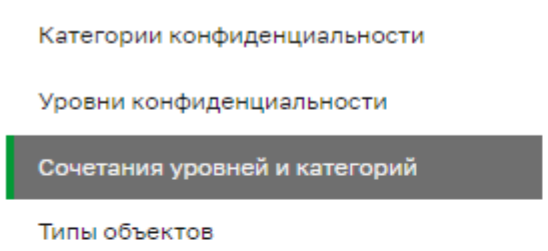
Управление инцидентами

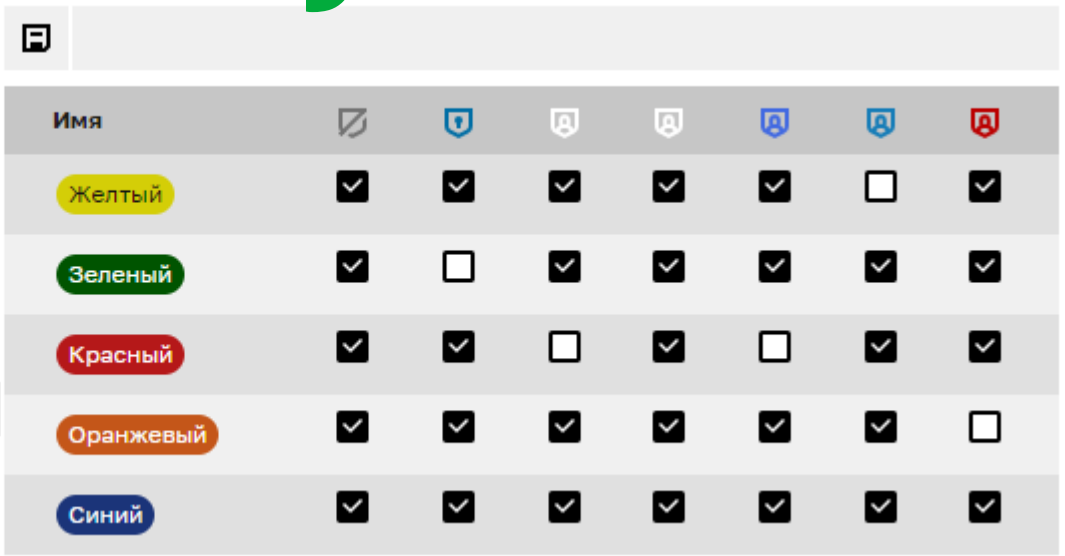


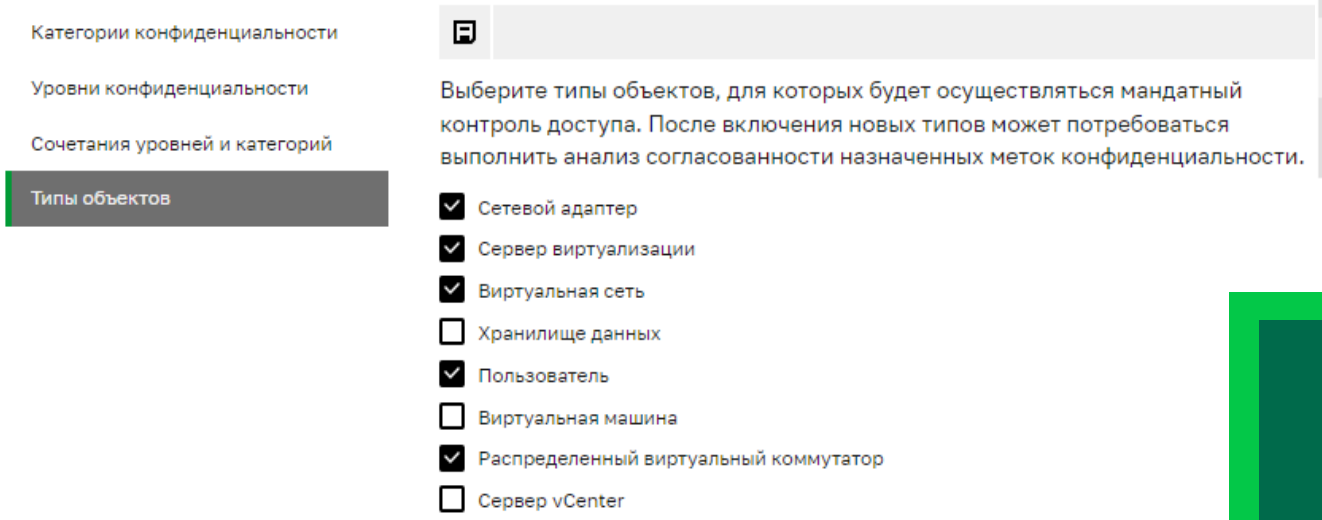
Уведомление по:

- syslog
- Email

Контроль доступа

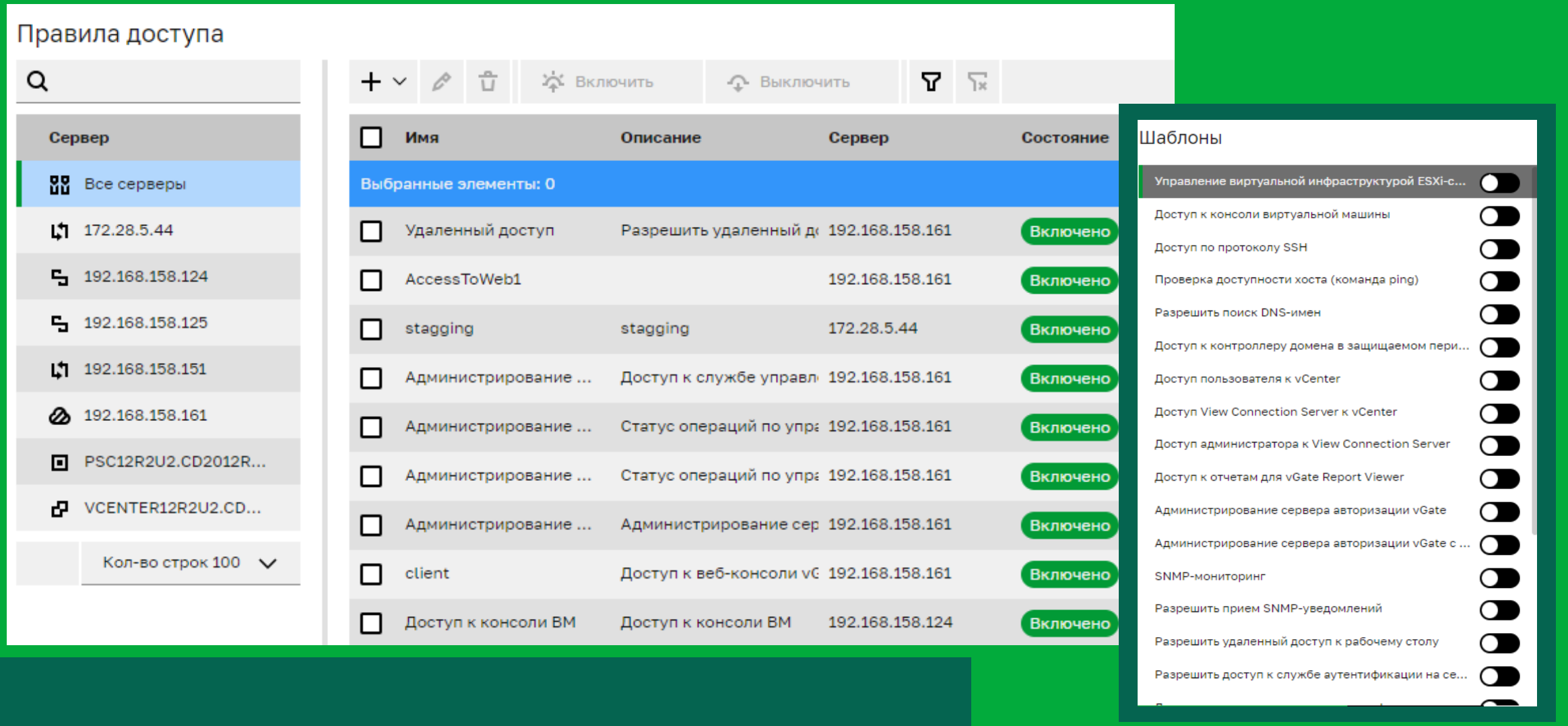




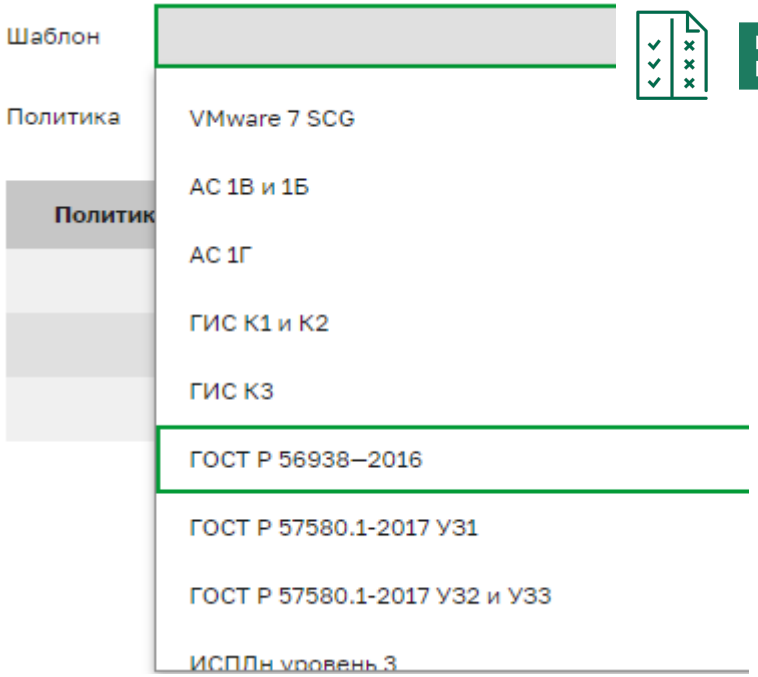


управление уровнями и цветовыми категориями конфиденциальности

Разграничение доступа



Политики безопасности



Встроенные

шаблоны политик

- PCI DSS v3.2
- VMware 6.5 SCG
- VMware 6.7 SCG
- VMware 7 SCG
- CIS for ESXi 6.5
- CIS for ESXi 6.7
- CIS for ESXi 7.0
- АС 1Г, 1Б, 1В
- КИИ К1, К2, К3
- СТО БР ИСПДн-Д
- СТО БР ИСПДн-Б
- СТО БР ИСПДн-И
- СТО БР ИСПДн-С
- ИСПДн уровни 1, 2, 3
- ГИС К1, К2, К3
- СТО БР уровень 2
- СТО БР уровни 3 и 4
- ГОСТ Р 56938-2016
- ГОСТ Р 57580.1-2017 У31
- ГОСТ Р 57580.1-2017 У32
- ГОСТ Р 57580.1-2017 У33

Политики безопасности

Шаблон

Политика

Политик

VMware 7 SCG

АС 1В и 1Б

АС 1Г

ГИС К1 и К2

ГИС К3

ГОСТ Р 56938—2016

ГОСТ Р 57580.1-2017 У31

ГОСТ Р 57580.1-2017 У32 и У33

ИСПДн уровень 3

Встроенные

Кастомные

наборы политик

Имя PolicySet1

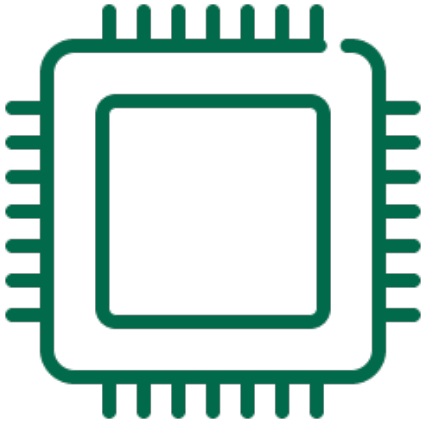
Описание PolicySet1

Шаблон Пользовательский набор

Политика

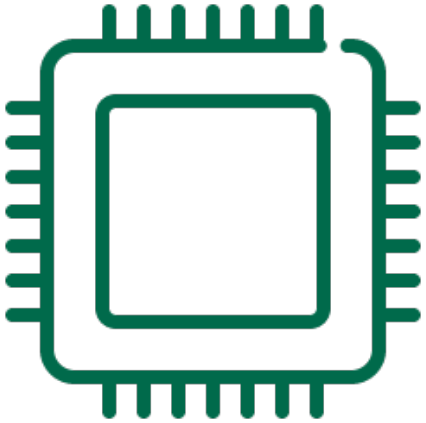
Политика	Действия
Включить фильтр BPDU на ESXi-сервере для предотвращения отключения от портов физическ	
Запрет VM Monitor Control	
Запрет доступа к консоли виртуальной машины по протоколу VNC	
Запрет некоторых скрытых возможностей	
Запрет отсылки информации о производительности ESXi-сервера гостевым системам	
Использование протокола CHAP для iSCSI устройств	
Контроль за доступом через dvfilter Network API	
Настройки логирования виртуальных машин на ESXi-сервере	
Ограничение размера информационных сообщений от виртуальной машины в VMX-файле	
Отключение ненужных устройств	
Отключить передачу сообщений VIX API от виртуальной машины	
Предотвращение шпионажа других пользователей на удаленных консолях администратора	
Разделение сетей консоли управления и виртуальных машин	

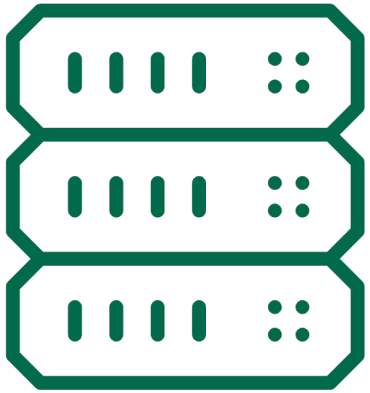
Лицензирование



лицензируется по количеству физических процессоров

Лицензирование

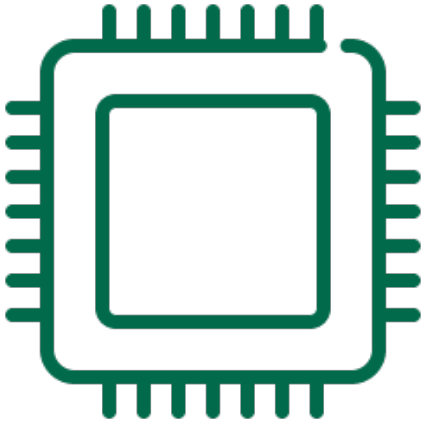




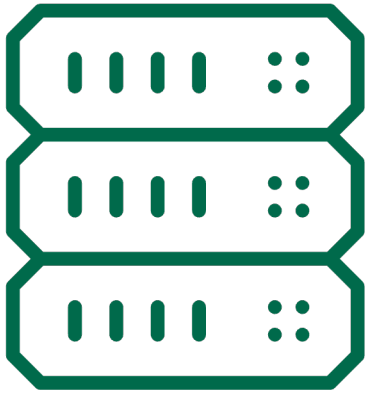
лицензируется по количеству физических процессоров

сервер авторизации входит в стоимость лицензии

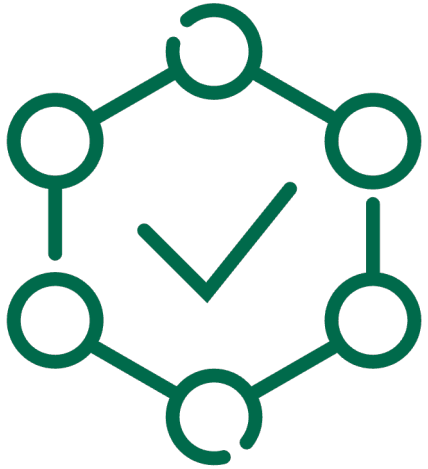
Лицензирование



лицензируется по количеству физических процессоров



сервер авторизации входит в стоимость лицензии



лицензия универсальна для каждой платформы виртуализации

Standard

базовый функционал
соответствие требованиям
маленькие инфраструктуры

Enterprise

горячее резервирование
несколько серверов авторизации
контроль операций

Standard

базовый функционал
соответствие требованиям
маленькие инфраструктуры

Enterprise Plus

межсетевой экран
сканер compliance
мониторинг + отчеты

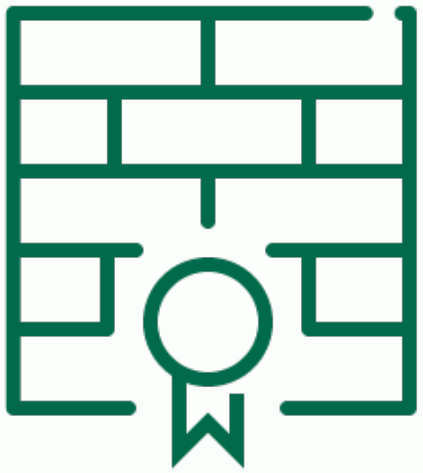
Enterprise

горячее резервирование
несколько серверов авторизации
контроль операций

Standard

базовый функционал
соответствие требованиям
маленькие инфраструктуры

Преимущества



Межсетевой экран

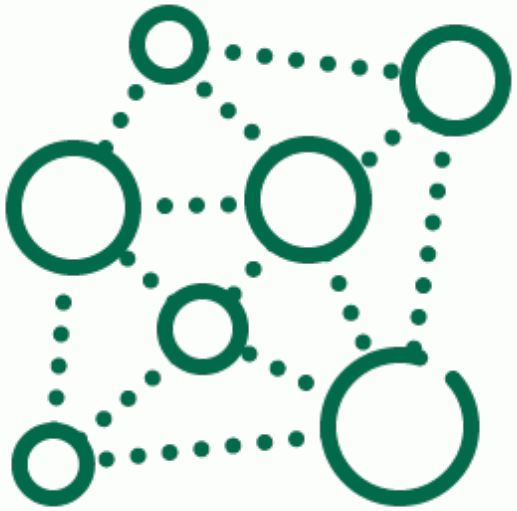
- сертифицированный
- уровня гипервизора
- SDN

Преимущества

Мониторинг и аудит

- в реальном времени
- инциденты+ syslog
- дашборды и отчеты

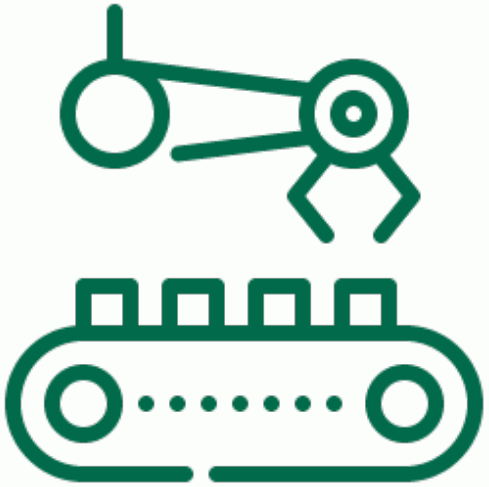
Преимущества



Применение в
неоднородных
инфраструктурах

- KVM
- СКАЛА-Р
- VMware

Преимущества



Автоматизация

- автодобавление
- сканер соответствия
- шаблоны

Сертификаты

ФСТЭК России

vGate R2 (защита конфиденциальной информации)

5 класс защищенности СВТ
4 уровень доверия
4 класс защиты МЭ тип Б

Применяется для защиты

- ГИС до К1 включительно
- ИСПДн до УЗ1 включительно
- АС до класса 1Г включительно
- АСУ ТП до К1 включительно
- ЗОКИИ до 1 категории включительно

Спасибо

за внимание!

KeyProjects@securitycode.ru

www.securitycode.ru