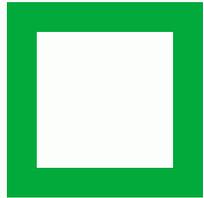


# Безопасность виртуализации

сегодня и завтра



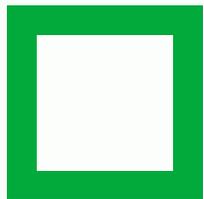
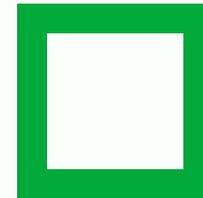
# Что мы видим сегодня?



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



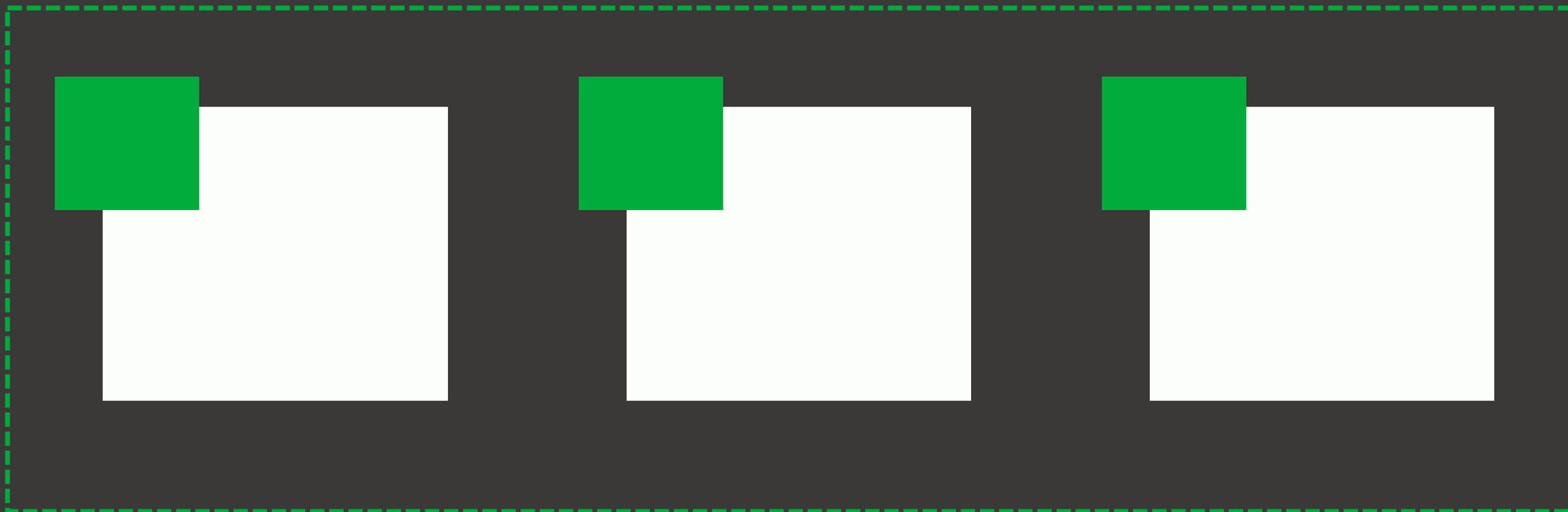
Гибкие сетевые возможности



Гарантированное затирание информации

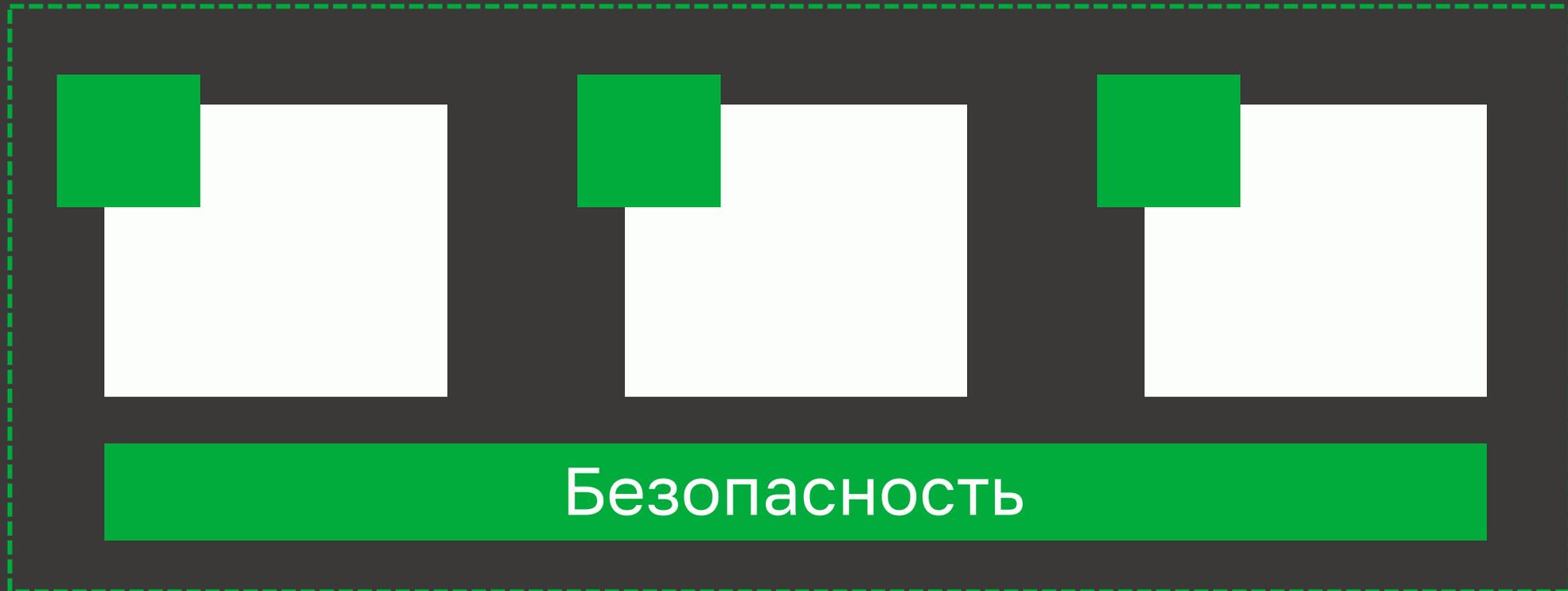
# Безопасность как процесс

ИТ-компоненты



# Безопасность как процесс

ИТ-компоненты



# 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 VM
- выборочная инспекция
- правила привязываются к VM, 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 VM

## Контроль внутри VM

- Secret Net Studio внутри VM
- 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



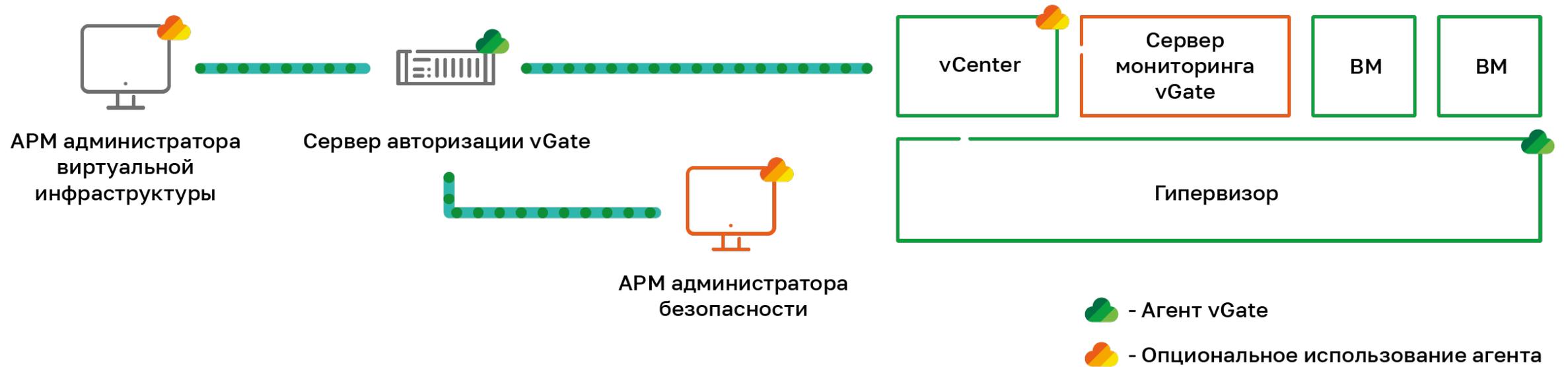
Мониторинг и управление инцидентами



Выполнение требований регуляторов

	<b>СЗИ</b>	<b>МЭ</b>	<b>SDN</b>
VMware vSphere 6.5	+	+	-
VMware vSphere 6.7, 7.0	+	+	+
Альт Сервер Виртуализации 10.1 (OpenNebula 5.10.5, Proxmox 7.2)	+	+	-
P-Виртуализация 7.0.13 (Скала-P Управление 1.98)	+	+	-
zVirt Node 3.3, 4.0	+	Лето 2024	-
РЕД Виртуализация 7.3	+	Лето 2024	-
ROSA Virtualization 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

## Правила фильтрации

Приоритет	Состояние	Имя	Отправитель	Порт отправителя	Направление	Получатель	Порт получателя	Служба	Протокол	Тип пакетов
Выбранные элементы: 0										
<input type="checkbox"/>	1395	Включено	test_rule_6	seg3	Любой	↕ Любое	SEG4	Любой	UDP	Все пакеты
<input type="checkbox"/>	1394	Включено	test_rule_5	SEg2	Любой	→ И				
<input type="checkbox"/>	1393	Включено	test_rule_4	seg3	Любой	↕ Л				
<input type="checkbox"/>	1392	Включено	test_rule_3	SEG4	Любой	↕ Л				
<input type="checkbox"/>	1391	Включено	test_rule_2	sEg1	Любой	↕ Л				
<input type="checkbox"/>	1390	Включено	test_rule_1	sEg1	Любой	↕ Л				
<input type="checkbox"/>	1389	Включено	test_rule	SEG2	Любой	→ И				
<input type="checkbox"/>	100	Включено	правило по умолч...	Любой	Любой	↕ Л				
<input type="checkbox"/>	1	Выключено	правило тесто...	Любой	Любой	↕ Л				

Количество элементов: 9

## 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 сегмента

Имя сегмента

Автодобавление ⓘ

Имя VM содержит

Приоритет ⓘ

**Создание сегментов с  
возможностью автодобавления  
по части имени**

Выберите виртуальные машины для добавления в данный сегмент виртуальной инфраструктуры.

🔍 Имя VM, идентификатор или сервер виртуализации

<input type="checkbox"/>	Имя VM	Идентификатор UUID	Сервер виртуализации	Тип сервера
Выбранные элементы: 0 <a href="#">Выбрать все: 26</a>				
▶ <input type="checkbox"/>	auto_VM_0	4238E0A7-C45D-9C54-3BBA-FC3485369608	192.168.158.124	ESXi-сервер
▶ <input type="checkbox"/>	auto_VM_1	4238A170-C0B8-14C6-747C-8998C7747182	192.168.158.124	ESXi-сервер
▶ <input type="checkbox"/>	auto_VM_10	4238B878-886C-9552-29DA-0395CC93FD89	192.168.158.124	ESXi-сервер

# Сегментирование

Активные сессии

Обновить Свойства Очистить

Правило фильтрации	Действие	Начало сессии	Последняя активность	Сервер виртуализации	Тип сервера	Сегмент отправителя	Отправитель	Порт отправителя	Направление
	Разрешить	24.05.1970, 0:21:18	24.05.1970, 0:21:19	192.168.158.2	Не определен		192.168.240.125	56	Любое
	Блокировать	24.05.1970, 0:21:18	24.05.1970, 0:21:19	192.168.158.1	Не определен		192.168.240.25	20	Исходящее однонаправлен

Количество элементов: 2

Службы

+ [иконки]

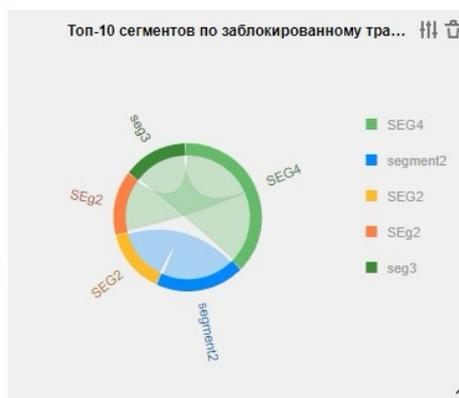
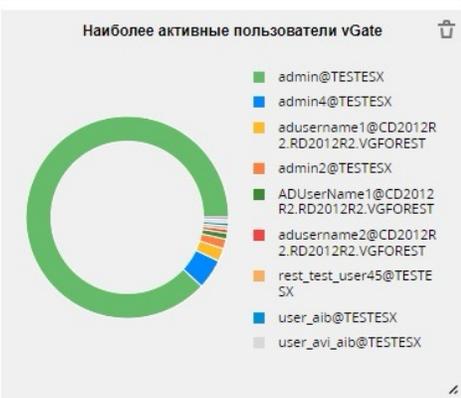
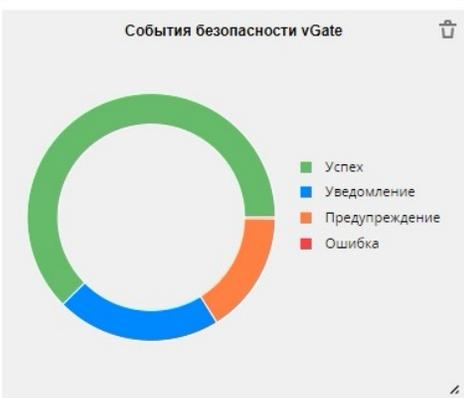
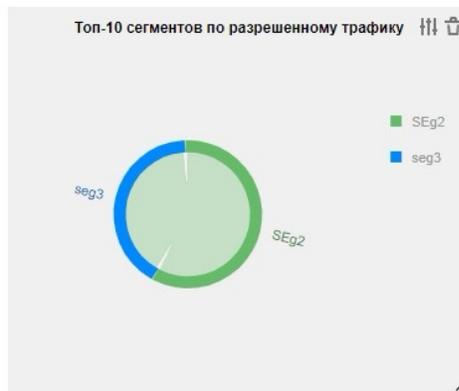
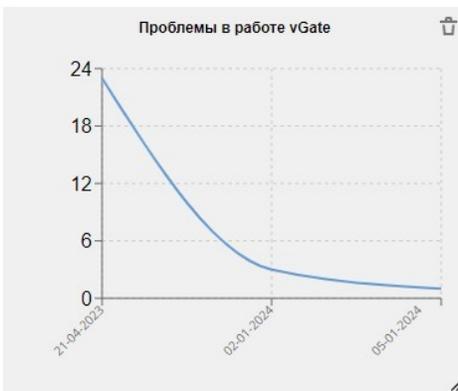
Имя	Протокол	Порт
Выбранные элементы: 0		
<input type="checkbox"/> SURF	UDP	1010
<input type="checkbox"/> SURF	TCP	1010
<input type="checkbox"/> CADLOCK2	UDP	1000
<input type="checkbox"/> CADLOCK2	TCP	1000
<input type="checkbox"/> APPLIX	UDP	999
<input type="checkbox"/> GARCON	TCP	999
<input type="checkbox"/> PUPARP	UDP	998
<input type="checkbox"/> BUSBOY	TCP	998
<input type="checkbox"/> MAITRD	UDP	997
<input type="checkbox"/> MAITRD	TCP	997
<input type="checkbox"/> VSINET	UDP	996

КОНТРОЛЬ СЕССИЙ

КАТАЛОГ СЛУЖБ

# Мониторинг

## Панель мониторинга



# Правила корреляции

Имя правила	Неконтролируемый рост...
Критичность	Высокая <span>▼</span>
Интервал	3 <span>▲▼</span>
	Часы <span>▼</span>
Способ оповещения <span>i</span>	<span>▼</span>
Группировать по <span>i</span>	Пользователь <span>x</span> <span>▼</span>

^ Создание виртуальной ма... x

VMware

Количество i 50 ▲▼

Параметры фильтра:

Объект i ▼

Добавить правило из существующего шаблона

- + Множественные операции удаления виртуальных машин (VMware)
- + Множественные операции с виртуальной машиной (VMware)
- + Операции с критичной виртуальной машиной (VMware)
- + Рестарт гостевой системы виртуальной машины на конкретном сервере (VMware)
- + Однократное удаление виртуальной машины (VMware)
- + Нарушение целостности файлов vGate
- + Множественное нарушение целостности виртуальной машины (VMware)
- + Попытки неудачного входа на сервер авторизации vGate

Шаблоны правил

Кастомные правила

- ✓ Виртуальная машина о...
- + Экспорт виртуальной м...
- + Импорт виртуальной м...
- + Изменение настроек виртуальной машины
- + Миграция виртуальной машины
- Хранилища
- Предупреждения
- Пользователи
- + Создан новый пользователь на ESXi-сервере
- ✓ Неуспешная авторизация пользователя на ESXi-сервере
- + Успешная авторизация пользователя на сервере vCenter или ESXi
- + Смена пароля учетной записи на ESXi-сервере при установленном подключении к vCenter
- + Удаление учетной записи на ESXi-сервере

# Управление инцидентами

Инциденты

Свойства  Пометить как обработанный    

<input type="checkbox"/> Дата и время	Обработано	Критичность	Имя правила	Параметры группировки
Выбранные элементы: 1 <a href="#">Отменить выделение</a>				
<input type="checkbox"/> 09.11.2023, 6:45:22	Нет	Очень высокая	Выход из режима обслуживания_2_R...	TESTVM3
<input type="checkbox"/> 09.11.2023, 6:45:02	Нет	Очень высокая	VmRemovedEventRelatedMsg	TESTVM2
<input type="checkbox"/> 09.11.2023, 6:45:02	Нет	Очень высокая	VmRemovedEventRelatedMsg	TESTVM1
<input checked="" type="checkbox"/> 09.11.2023, 6:45:02	Нет	Очень высокая	Выключение виртуальной машины_R...	564DCDA8-2BD8-B429-A8D7-6EBD523EE169
<input type="checkbox"/> 09.11.2023, 6:45:02	Нет	Очень высокая	Выход из режима обслуживания_2_R...	564DCDA8-2BD8-B429-A8D7-6EBD523EE169
<input type="checkbox"/> 09.11.2023, 6:45:02	Нет	Очень высокая	Выход из режима обслуживания_2_R...	TESTVM2
<input type="checkbox"/> 09.11.2023, 6:45:02	Нет	Очень высокая	Выход из режима обслуживания_2_R...	TESTVM1
<input type="checkbox"/> 09.11.2023, 6:43:41	Нет	Очень высокая	VmRemovedEvent	192.168.158.124
<input type="checkbox"/> 09.11.2023, 6:39:22	Нет	Очень высокая	Выключение виртуальной машины_R...	564DF587-0445-EC30-AED0-06F49656BC3E
<input type="checkbox"/> 09.11.2023, 6:39:22	Нет	Очень высокая	Выход из режима обслуживания_2_R...	564DF587-0445-EC30-AED0-06F49656BC3E
<input type="checkbox"/> 09.11.2023, 6:35:21	Нет	Очень высокая	VmRemovedEventRelatedMsg	AUTO_VM_999992

**Уведомление по:**

- syslog
- Email

# Контроль доступа

Категории конфиденциальности

Уровни конфиденциальности

Сочетания уровней и категорий

Типы объектов

Категории конфиденциальности

Уровни конфиденциальности

Сочетания уровней и категорий

Типы объектов

☰

Выберите типы объектов, для которых будет осуществляться мандатный контроль доступа. После включения новых типов может потребоваться выполнить анализ согласованности назначенных меток конфиденциальности.

- Сетевой адаптер
- Сервер виртуализации
- Виртуальная сеть
- Хранилище данных
- Пользователь
- Виртуальная машина
- Распределенный виртуальный коммутатор
- Сервер vCenter

Имя	☑	🛡	🛡	🛡	🛡	🛡	🛡
Желтый	☑	☑	☑	☑	☑	☐	☑
Зеленый	☑	☐	☑	☑	☑	☑	☑
Красный	☑	☑	☐	☑	☐	☑	☑
Оранжевый	☑	☑	☑	☑	☑	☑	☐
Синий	☑	☑	☑	☑	☑	☑	☑

управление уровнями  
и цветовыми категориями  
конфиденциальности

# Разграничение доступа

## Правила доступа

🔍

Сервер
🏠 Все серверы
🔄 172.28.5.44
🏠 192.168.158.124
🏠 192.168.158.125
🔄 192.168.158.151
🔒 192.168.158.161
🏠 PSC12R2U2.CD2012R...
🏠 VCENTER12R2U2.CD...

Кол-во строк 100 ▾

+ ▾ ✎ 🗑️ ⚡ Включить ⏻ Выключить 🔍 🗑️

<input type="checkbox"/>	Имя	Описание	Сервер	Состояние
Выбранные элементы: 0				
<input type="checkbox"/>	Удаленный доступ	Разрешить удаленный д	192.168.158.161	Включено
<input type="checkbox"/>	AccessToWeb1		192.168.158.161	Включено
<input type="checkbox"/>	stagging	stagging	172.28.5.44	Включено
<input type="checkbox"/>	Администрирование ...	Доступ к службе управл	192.168.158.161	Включено
<input type="checkbox"/>	Администрирование ...	Статус операций по упр:	192.168.158.161	Включено
<input type="checkbox"/>	Администрирование ...	Статус операций по упр:	192.168.158.161	Включено
<input type="checkbox"/>	Администрирование ...	Администрирование сер	192.168.158.161	Включено
<input type="checkbox"/>	client	Доступ к веб-консоли vC	192.168.158.161	Включено
<input type="checkbox"/>	Доступ к консоли VM	Доступ к консоли VM	192.168.158.124	Включено

## Шаблоны

Управление виртуальной инфраструктурой ESXi-с...	🔴
Доступ к консоли виртуальной машины	🔴
Доступ по протоколу SSH	🔴
Проверка доступности хоста (команда ping)	🔴
Разрешить поиск DNS-имен	🔴
Доступ к контроллеру домена в защищаемом пери...	🔴
Доступ пользователя к vCenter	🔴
Доступ View Connection Server к vCenter	🔴
Доступ администратора к View Connection Server	🔴
Доступ к отчетам для vGate Report Viewer	🔴
Администрирование сервера авторизации vGate	🔴
Администрирование сервера авторизации vGate с ...	🔴
SNMP-мониторинг	🔴
Разрешить прием SNMP-уведомлений	🔴
Разрешить удаленный доступ к рабочему столу	🔴
Разрешить доступ к службе аутентификации на се...	🔴

# Политики безопасности

Шаблон	
Политика	VMware 7 SCG
Политик	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 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	VMware 7 SCG
	АС 1В и 1Б
Политик	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

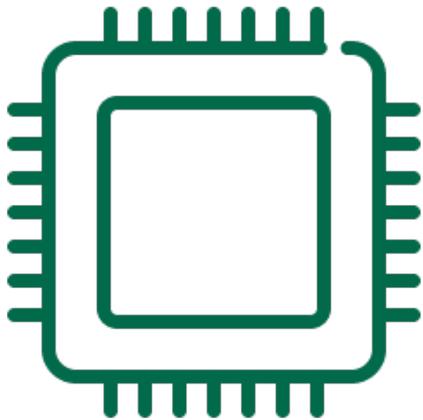
Имя	PolicySet1
Описание	PolicySet1
Шаблон	Пользовательский набор x v
Политика	v + v

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	🔒 III
Запрет отсылки информации о производительности ESXi-сервера гостевым системам	🔒
Использование протокола CHAP для iSCSI устройств	🔒 III
Контроль за доступом через dvfilter Network API	🔒 III
Настройки логирования виртуальных машин на ESXi-сервере	🔒 III
Ограничение размера информационных сообщений от виртуальной машины в VMX-файле	🔒 III
Отключение ненужных устройств	🔒 III
Отключить передачу сообщений VIX API от виртуальной машины	🔒
Предотвращение шпионажа других пользователей на удаленных консолях администратора	🔒
Разделение сетей консоли управления и виртуальных машин	🔒



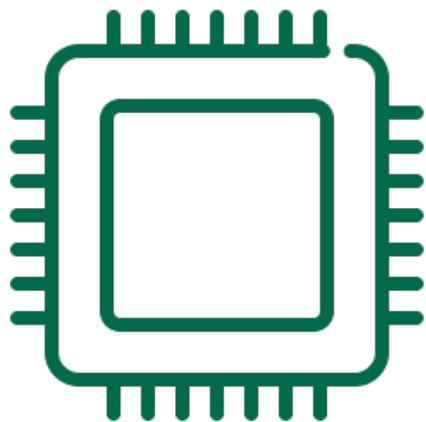
## Кастомные наборы политик

# Лицензирование

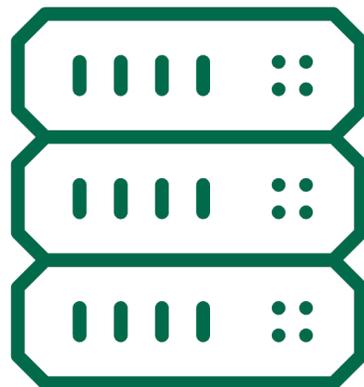


лицензируется  
по количеству  
физических процессоров

# Лицензирование

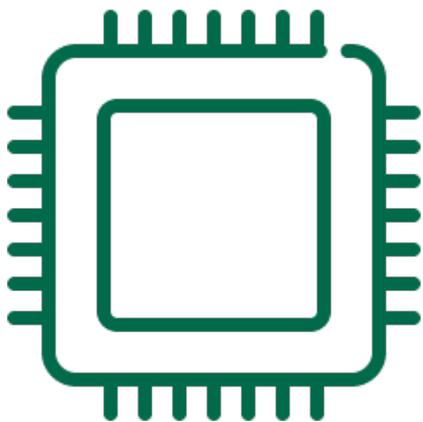


лицензируется  
по количеству  
физических процессоров

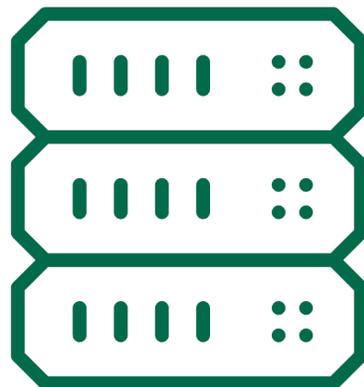


сервер авторизации  
входит в стоимость  
лицензии

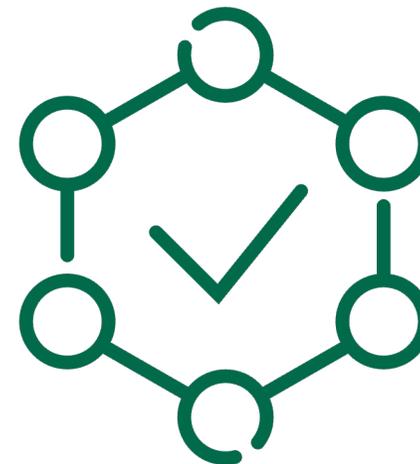
# Лицензирование



**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

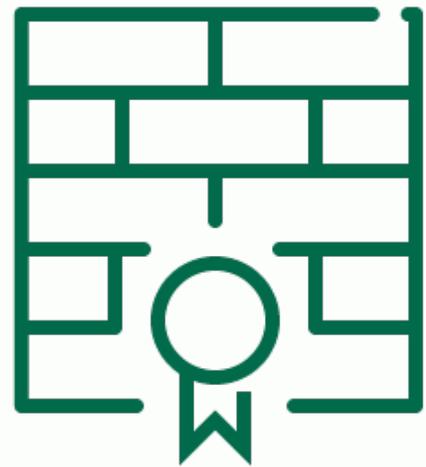
## Enterprise

горячее резервирование  
несколько серверов авторизации  
контроль операций

## Standard

базовый функционал  
соответствие требованиям  
маленькие инфраструктуры

# Преимущества



## Межсетевой экран

- сертифицированный
- уровня гипервизора
- SDN

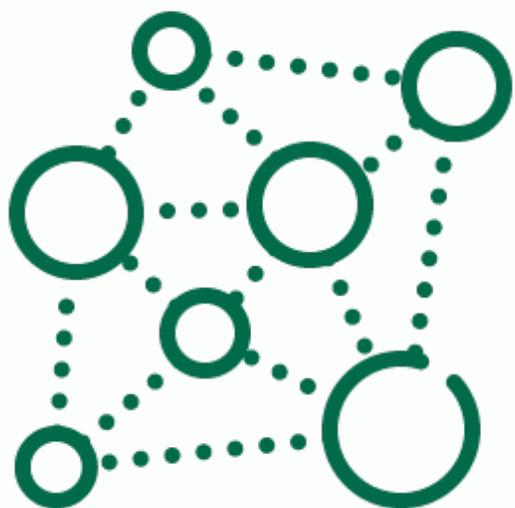
# Преимущества



## Мониторинг и аудит

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

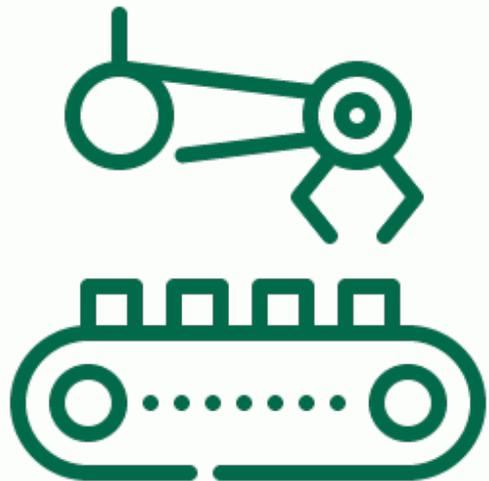
# Преимущества



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](mailto:KeyProjects@securitycode.ru)

[www.securitycode.ru](http://www.securitycode.ru)