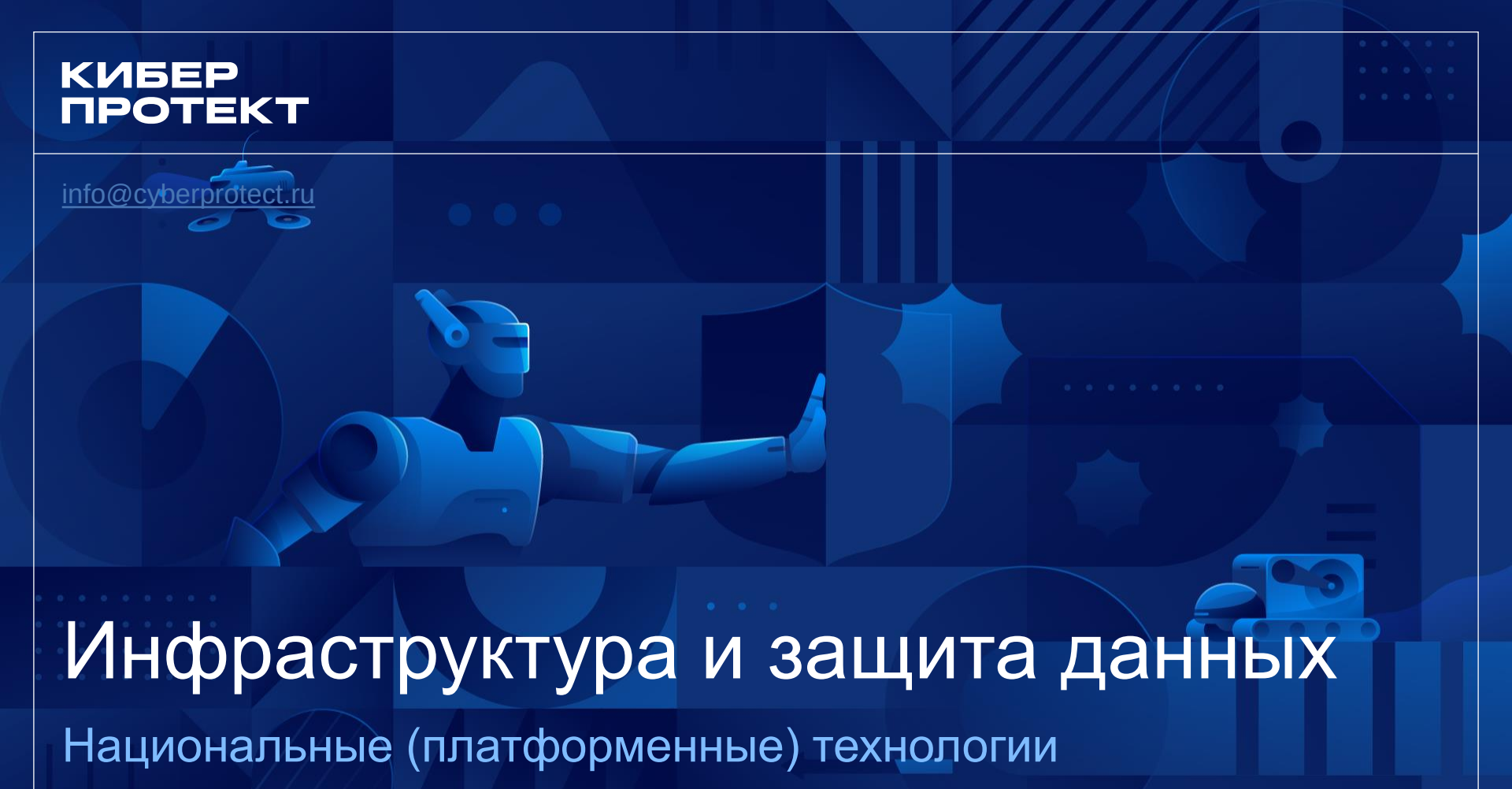
КИБЕР ПРОТЕКТ

info@cyberprotect.ru



Инфраструктура и защита данных

Национальные (платформенные) технологии

Отечественный вендор

Программных продуктов, лидирующих в своих классах

Компания, география присутствия, примеры внедрений

ИТ-кластер Физтехпарк
Москва

Технопарк Иннополис
Татарстан

ОСНОВАНИЕ
2016
КОМПАНИИ

Продукты

ISO 9001:2015

КИБЕР Бэкап

Системы резервного копирования

Бэкап Облачный

Бэкап Персональный — СКОРО

КИБЕР Инфраструктура

Гиперконвергентная инфраструктура

Платформа для Датацентров и внутренние сервисы

КИБЕР Файлы — СКОРО

Защищённый внутренний сервис файлового обмена и совместной работы

КИБЕР Протего

Предотвращение утечек всех типов данных

Обеспечение непрерывности бизнеса

Базируется на организованном взаимодействии ИТ и ИБ

ИТ	Точки пересечения	ИБ
Зона ответственности **Определить и внедрить технологии** обеспечения и оптимизации бизнес-процессов и процессов безопасности	Заказчик и исполнитель Потребности ИБ трансформируются в ИТ проекты	Зона ответственности **Выявить угрозы,** разработать и **внедрить комплекс организационно-технических мер** противодействия
	Общие угрозы Напр., вирусы-вымогатели	
Фокус **Доступность, удобство** использования, **производительность**	Соответствие требованиям ИТ в значительной степени функционирует в ограничениях, задаваемых ИБ	Фокус **Безопасность**

Соответствие требованиям регуляторов

Недостижимо без использования систем резервного копирования и предотвращения утечек

Примеры требований

ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций

ФЗ-152 О персональных данных

ФЗ-187 О безопасности КИИ

Payment Card Industry Data Security Standard

Типичный состав мер прямо или косвенно включает

- Хранение архивов различных систем
- Контроль отсутствия уязвимостей
- Эшелонированная защита от вредоносного кода
- Предотвращение утечек информации
- Резервирование ПО, тех. средств, данных, виртуальной инфраструктуры
- Обеспечение возможности восстановления, защита резервных копий

КИБЕР ПРОТЕКТ

КИБЕР Бэкап

Централизованная система резервного копирования и восстановления, комплексной защиты систем, данных и резервных копий, в т.ч. от вирусов-вымогателей и криптомайнеров

КИБЕР Протего

Программный комплекс предотвращения утечек всех типов данных в хостовой реализации

КИБЕР ПРОТЕКТ

info@cyberprotect.ru

Кибер Бэкап

Резервное копирование, восстановление и комплексная защита данных

Кибер Бэкап

Резервное копирование и защита данных

Управление

- ПАНЕЛЬ МОНИТОРИНГА
  - Обзор
  - Оповещения
  - Действия
- УСТРОЙСТВА
- ПЛАНЫ
- ХРАНИЛИЩЕ РЕЗЕРВНЫХ КОПИЙ
- ОТЧЕТЫ
- НАСТРОЙКИ

Резервное копирование *и защита*

Резервное копирование

Активная защита от вирусов-шифровальщиков и криптомайнеров

Оценка уязвимостей

Хранение

Восстановление

Файлы, почтовые сервисы, БД

Мгновенное восстановление
RTO – **15 секунд**

Миграция
P2V, V2V, V2P, P2P

Гранулярное восстановление
Напр., **до уровня файлов**

Восстановление на **«неродное»**, новое, «голое» **железо**

Поддерживаемые системы

Файловые

FAT16/32
NTFS
Ext2 / Ext3 / Ext4
ReFS
ReiserFS3 / FS4
JFS
XFS
Linux SWAP

Физические
включая legacy ОС

Виртуальные
в т.ч. в безагентском режиме

Enterprise Cloud Platform VeiL KVM

Приложения

ORACLE PostgresPro

Объекты резервного копирования и защиты

Azure	Windows Server	Windows PC	Exchange	SQL Server
Share Point	Active Directory	Hyper-V	Microsoft 365	Mac OS
Linux Server	РЕДОС Муром	Альт Линукс 9	Astra Linux SE	РОСА Кобальт
VMware vSphere	Oracle x86 VM Server	Oracle Database	Red Hat Virtualization	Linux KVM
Citrix XenServer	Virtuozzo	Nutanix	SAP HANA	Postgres Pro PostgreSQL, Jatoba

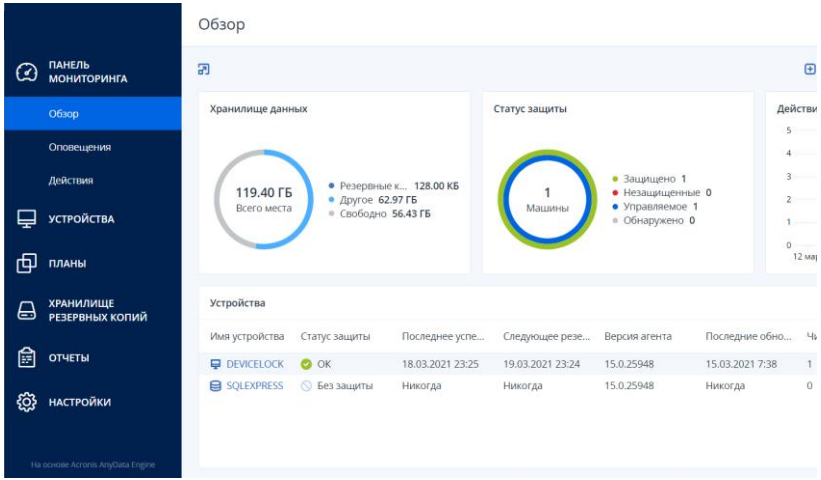
Централизованное администрирование

Веб-консоль

Единый инструмент **для всех задач**

Полностью **настраиваемые** средства управления

Визуальная интерактивная **аналитика и отчёты** по инфраструктуре и задачам



Ролевая модель администрирования

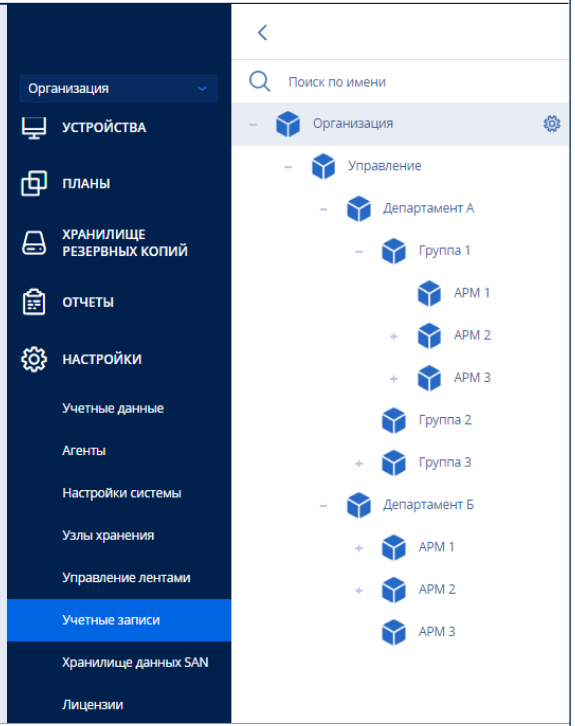
Роли

- **Полный** доступ
- Только **чтение**
- **Аудит**

Назначение ролей **учётным записям или группам** в т.ч. службы каталогов Active Directory

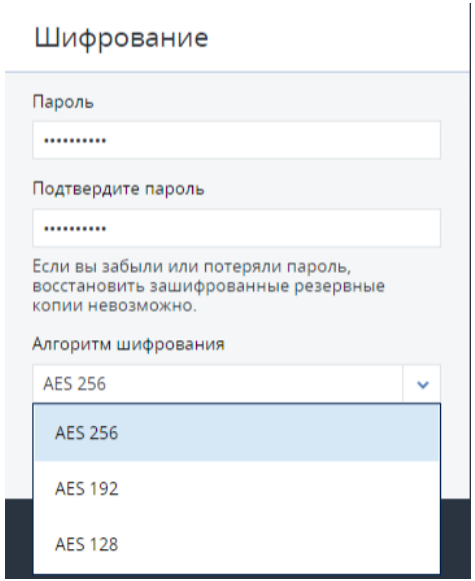
Локализации

- Русскоязычная
- Англоязычная



Защита резервных копий шифрованием

Шифрование резервных копий



Агентом резервного копирования **при** их **создании**

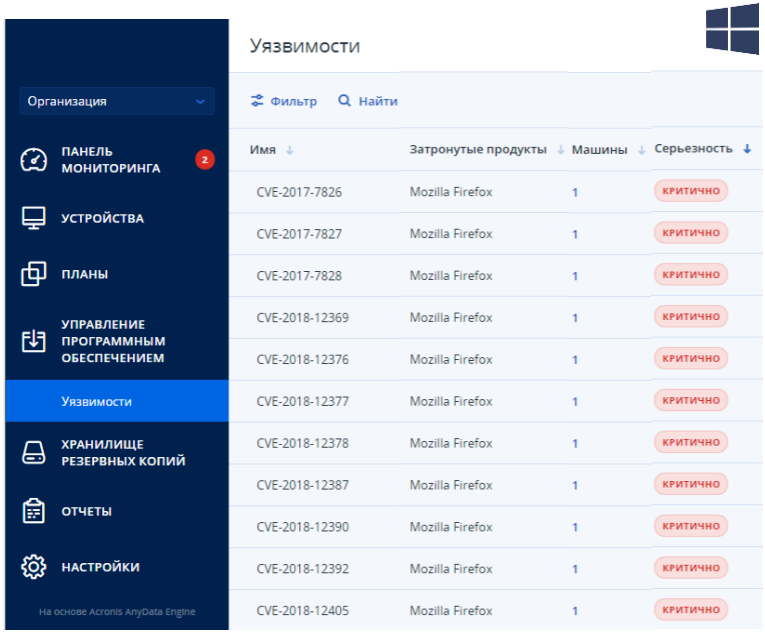
Узлом хранения при записи в управляемое хранилище

Возможно **двойное шифрование**

Оценка уязвимостей

НЕЛИЦЕНЗИРУЕМЫЙ МОДУЛЬ

Актуальные базы уязвимостей операционной системы, веб-браузеров, продуктов Adobe, Oracle, Java, другого программного обеспечения



плохие

Единый метод – разные цели

Сканирование операционной системы и используемых приложений **на предмет наличия открытых уязвимостей**

хорошие

атака

исправление

***обнаружение** уязвимости*

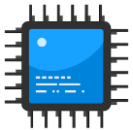
Активная защита от вирусов-вымогателей

НЕЛИЦЕНЗИРУЕМЫЙ МОДУЛЬ

Непрерывно обучаемый выявлению и устранению угроз ИИ

Машинное обучение выявлению **несанкционированных операций шифрования**

обновления в дистрибутивах



Модуль Активной Защиты

мониторинг

Системы и хранилища

Устройство модуля

Драйвер

Анализирует содержимое и тип данных до и после изменения

Предполагает активность зловредного ПО **при выявлении изменения типа** содержимого

Служба

Тревожное **оповещение**

Остановка процесса

Восстановление данных из кэша

КИБЕР ПРОТЕКТ

info@cyberprotect.ru

Кибер Протего

Программный комплекс предотвращения утечек всех типов данных в хостовой (агентской) реализации

Исходный продукт DeviceLock DLP

25+ лет разработки, миллионы инсталляций по всему миру

1996 — Первая коммерческая версия **DeviceLock**

- Рост числа контролируемых локальных каналов утечки, возможностей их контроля
- Контроль каналов сетевых коммуникаций
- Анализ и фильтрация содержимого → **DeviceLock DLP**
- Virtual DLP
- Контроль хранимых данных

2020 — Поглощение со стороны Acronis International GmbH

2021 — Релиз продукта **Кибер Протего**

Контекстный и контентный контроль

Используемых, передаваемых и хранимых данных

Контроль каналов утечки

Устройства

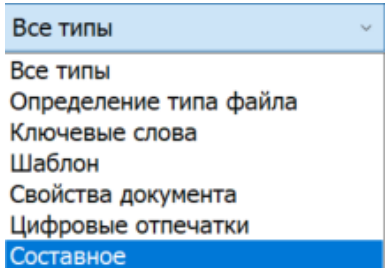
- BlackBerry-устройства
- Bluetooth
- FireWire-порт
- iPhone-устройства
- MTP
- Palm
- USB-порт
- WiFi
- Windows Mobile
- Буфер обмена
- Гибкий диск
- Жесткий диск
- ИК-порт
- Ленточные накопители
- Оптический привод
- Параллельный порт
- Последовательный порт
- Принтер
- Съемные устройства
- ТС-устройства

Коммуникации

- FTP
- HTTP
- IBM Notes
- ICQ Messenger
- IRC
- Jabber
- Mail.Ru Агент
- MAPI
- Skype
- SMB
- SMTP
- Telegram
- Telnet
- Viber
- Web-поиск
- Web-почта
- WhatsApp
- Zoom
- Поиск работы
- Социальные сети
- Торрент
- Файловые хранилища

Контроль данных

Анализ и фильтрация содержимого данных, передаваемых по контролируемым каналам утечек и хранимых в поддерживаемых хранилищах



Контроль данных в хранилищах

- В агентском **или безагентском** режиме
- Подключённые **съёмные устройства** хранения
- Общие сетевые папки **SMB**
- Хранилища **NAS/SAN**
- Ноды **Elasticsearch**
- **Папки синхронизации** облачных хранилищ
- Репозитории электронной почты **(.ost, .pst)**

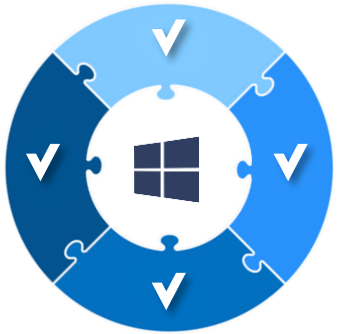
Агенты DLP

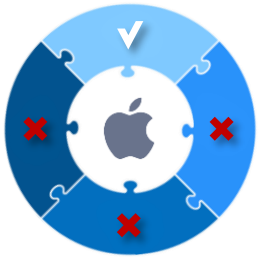
Для Windows и Mac OS

Модуль контроля устройств	Модуль контроля коммуникаций	Модуль контроля данных	Модуль UAM
Обязательный	Опциональный	Опциональный	Опциональный
Контроль портов, интерфейсов ПК, приводов и устройств, канала печати и терминальных сессий	Контроль протоколов, почты, веб-сервисов, мессенджеров, поисковых запросов и карьерных ресурсов	Анализ и фильтрация **содержимого** данных, передаваемых на устройства и через каналы коммуникаций	**Видеозапись** экрана пользователя, сведений о запущенных процессах, **кейлоггер**

Единый агент с лицензируемыми функциональными модулями*

Разные возможности агентов для разных операционных систем





*Применимо к агенту для ОС Windows

Virtual DLP

АГЕНТ DLP

Технология контроля удалённых рабочих мест и виртуальных сред

Устройства

Проброшенные внутрь терминальной сессии

- **Диски**
  Съёмные, жесткие
- Оптический **привод**
- Последовательный **порт**
- **Принтеры**

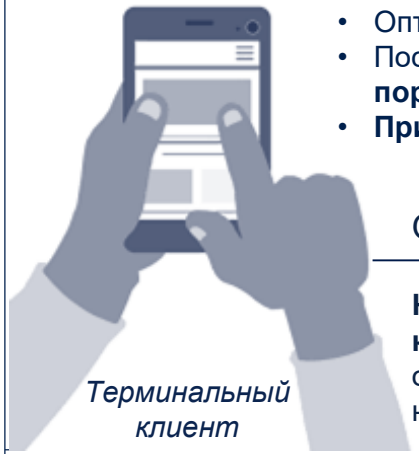
Буфер обмена

Различные типы данных

- Файлы
- Текст
- Изображения
- Аудио
- Данные, не принадлежащие ни к одной из этих категорий

Терминальный сервер с агентом

Права пользователя	Разрешено	Запрещено
Основные		
Чтение с подключенного диска	☑	☐
Запись на подключенный диск	☐	☑
Доступ к последовательному порту	☑	☐
Доступ к USB-устройствам	☑	☐
Буфер обмена входящий текст	☑	☐
Буфер обмена исходящий текст	☐	☑
Буфер обмена входящие изображения	☑	☐
Буфер обмена исходящие изображения	☐	☑
Буфер обмена входящие аудио данные	☑	☐
Буфер обмена исходящие аудио данные	☐	☑
Буфер обмена входящие файлы	☑	☐
Буфер обмена исходящие файлы	☐	☑
Буфер обмена входящие неизвестные данные	☑	☐
Буфер обмена исходящие неизвестные данные	☐	☑



Терминальный клиент

Особенности осуществления контроля

Контекстный и контентный, в обоих направлениях

Контроль вне зависимости от пользовательской ОС без установки дополнительных приложений

Отдельные **политики** DLP **для каждого пользователя**

ORACLE
CITRIX
vmware

Повышение информированности пользователей

Мера профилактики, существенно снижающая количество инцидентов

Защита агента и связанных служб **от отключения**

Защита системных компонентов и записей реестра от изменения

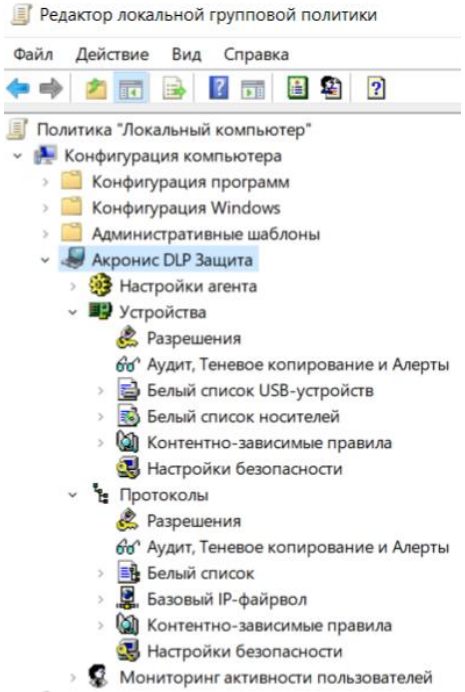
Проверка целостности агента и связанных компонентов

Защита от действий пользователей с правами **локальных администраторов и антируткитов**

Отсутствие необходимости скрывать факт работы решения → Профилактический эффект поддержания дисциплины

Полная интеграция в групповые политики

В домене Active Directory

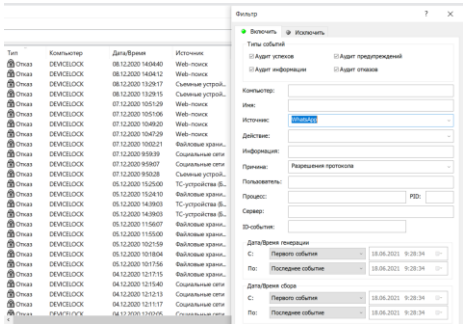


- **Объекты и механизмы** распространения групповых политик используются **как инфраструктура** представления и передачи управляющей информации между компонентами *Кибер Протего*
- **Управляется** без выделенного сервера для управления **через оснастку** для редактора групповых политик
- Встроенные конфигурируемые **пакеты MSI** к развёртыванию
- **Никакого импорта** объектов / .admx **темплейтов**

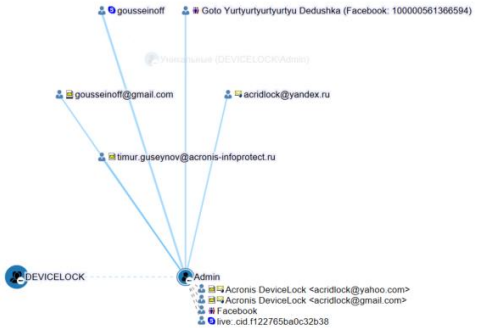
Журналы, видеозаписи и полнотекстовый поиск

Реактивная работа с инцидентами

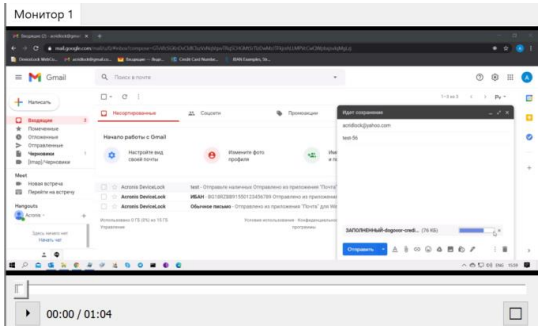
Фильтрация логов и теневых копий



Анализ связей



Просмотр видеозаписей

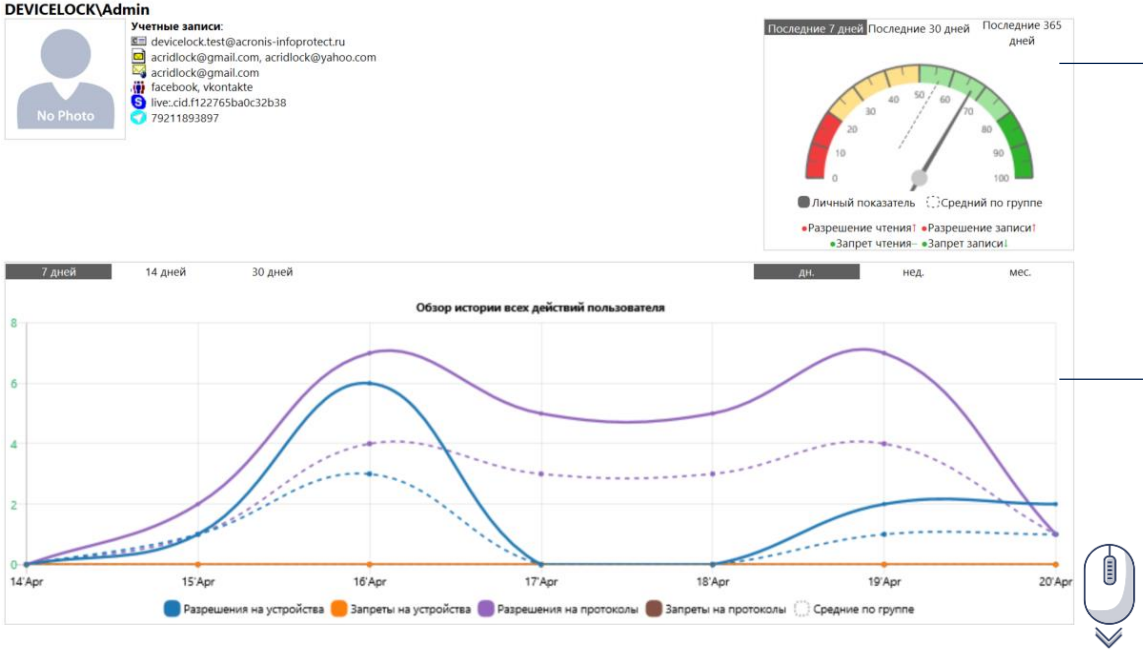


Полнотекстовый поиск в данных журналов и теневых копиях

Пример: секретно конфиденциальный, "секретно конфиденциальный", секретно AND конфиденциальный, секретно OR конфиденциальный

Досье (карточка) пользователя

Проактивная работа с рисками утечек



Поведенческий анализ

Индикатор отклонения от нормы

- Визуальное **представление сравнения среднего уровня** активности за период **с нормальным** уровнем
- Позволяет выявить изменения в поведении и **определить степень девиации**

Статистический анализ

Обзор действий пользователя

- Визуальное представление активности: **разрешенные и запрещённые операции**
- **Сравнение** со средними значениями **по группе**

Неотображённые элементы

- Актуальный граф связей
- Табличные и графические отчёты по журналам

КИБЕР ПРОТЕКТ

info@cyberprotect.ru

Кибер Инфраструктура

Кластеризация ресурсов любого стандартного оборудования

Типы ИТ-инфраструктур

Традиционная

Различные не связанные / слабо связанные между собой **компоненты**

Конвергентная

Стандартные **ПАК-блоки** трёхуровневой инфраструктуры

Гиперконвергентная

Полное абстрагирование от аппаратного уровня, стандартные блоки создаются из любого оборудования

Сценарий роста размера ИТ-инфраструктуры

Тип инфраструктуры	Традиционная	Конвергентная	Гиперконвергентная
 **Рост размера** инфраструктуры и объёма данных	**Разнообразие** производителей и моделей **аппаратного** обеспечения **усложняет** планирование и реализацию закупок, внедрение, эксплуатацию	**Простота** планирования и реализации закупок, внедрения, эксплуатации	**Простота** планирования и реализации закупок, внедрения, эксплуатации
 Рост требований **к масштабируемости** инфраструктуры	**Постоянное решение типовых проблем**	Ограниченно гибкий, **привязанный к конкретному вендору / интегратору ассортимент** аппаратного обеспечения	**Неограниченно гибкий ассортимент** аппаратного обеспечения, **возможность использования старого оборудования**
 Рост требований **к скорости** внедрения изменений	**Низкая скорость** внедрения изменений	**Высокая скорость** внедрения изменений	**Высокая скорость** внедрения изменений
Эффективность	НИЗКАЯ	ВЫСОКАЯ	

Сценарий недобровольного ограничения выбора поставщиков

Сбои в цепочках поставок, курсовые/валютные эффекты, регуляторы с обеих сторон границы

Тип инфраструктуры	Традиционная	Конвергентная	Гиперконвергентная
Невозможность получить (вообще или на разумных условиях) выбранное аппаратное обеспечение: • Серверы • Процессоры • Память • Диски • Другое оборудование	**Вынужденный поиск замены** с подходящими характеристиками в искусственно суженном ассортименте **Рост спроса** на подходящие заменители при ограниченном предложении **неизбежно ухудшает условия** их поставки	**Рост стоимости** для заказчиков **зарубежных вендоров** **Проблемы** сбоев в цепочках поставок **могут решаться вендором,** но до определённого предела, и **в итоге всё равно приводят к ухудшающимся условиям поставки**	**Широчайший и, в принципе, неисчерпаемый выбор** среди всего разнообразия **стандартного оборудования** **Любые** вычислительные **узлы и хранилища** данных **заменяется любыми другими,** в т.ч. приобретёнными на вторичном рынке
Эффективность	НИЗКАЯ	СРЕДНЯЯ*	ВЫСОКАЯ

*В умеренно-оптимистичных сценариях

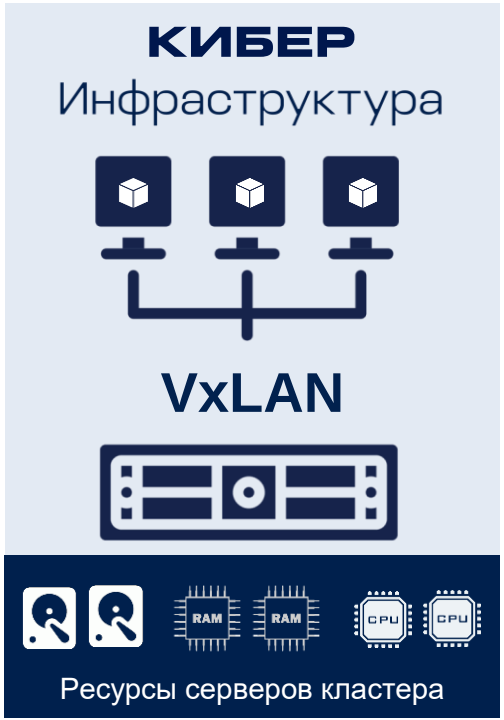
Кибер Инфраструктура

Кластеризация ресурсов стандартного оборудования

Виртуализация

Программно-определяемая виртуальная частная сеть

Программно-определяемое хранилище



Централизованное управление

Высокая доступность

Стандартное отраслевое оборудование

Базовые сценарии использования, масштабирование

Виртуализация

Хостинг и полный контроль жизненного цикла **виртуальных машин**

Поддержка высоконагруженных, в т.ч. бизнес-критичных **приложений и сервисов**

Высокая доступность с георепликацией и автоматизированным плановым / аварийным **переносом нагрузок между кластерами**

Вертикальное и горизонтальное масштабирование

Хранение

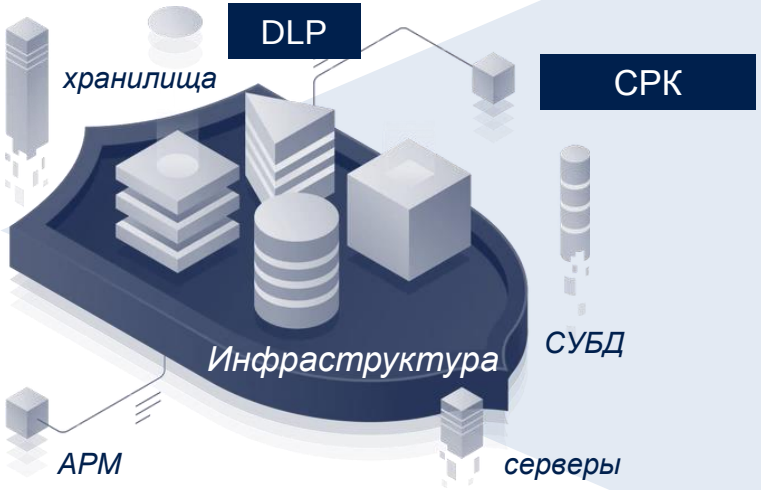
Архивы / резервные копии / **холодные данные**
Хранилище резервных копий для СРК *Кибер Бэкап*

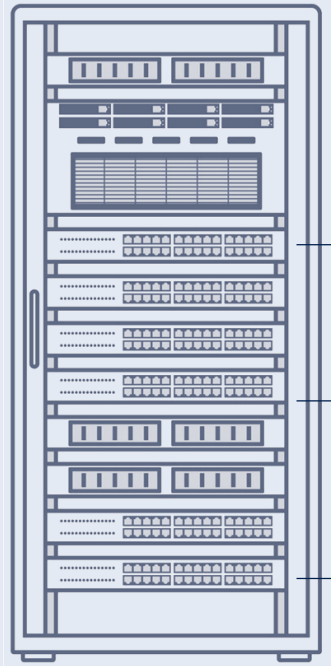
Хранилище **общего назначения / файловое**
Доступный и полностью управляемый обмен файлами по протоколу NFS

Объектное хранилище **S3**
Совместимо с большинством готовых S3-приложений

Блочное хранилище **горячих данных**
Идеально для критических / высокопроизводительных баз данных

Ядро платформы





КИБЕР Инфраструктура

виртуализация, хранилище

КИБЕР Протего

контроль каналов утечки и данных, хранилищ

резервное копирование

КИБЕР Бэкап

КИБЕР ПРОТЕКТ

info@cyberprotect.ru

Благодарю за внимание

Вопросы?