Актуальные вопросы централизованного управления средствами защиты информации конечных точек

ЕГОР КОЖЕМЯКА

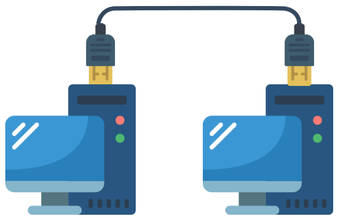
ДИРЕКТОР ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU

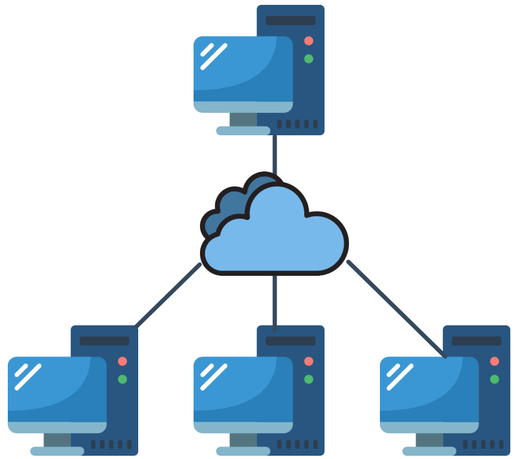
WEB: WWW.DALLASLOCK.RU

Развитие подходов к управлению ИБ

Локальные ПК



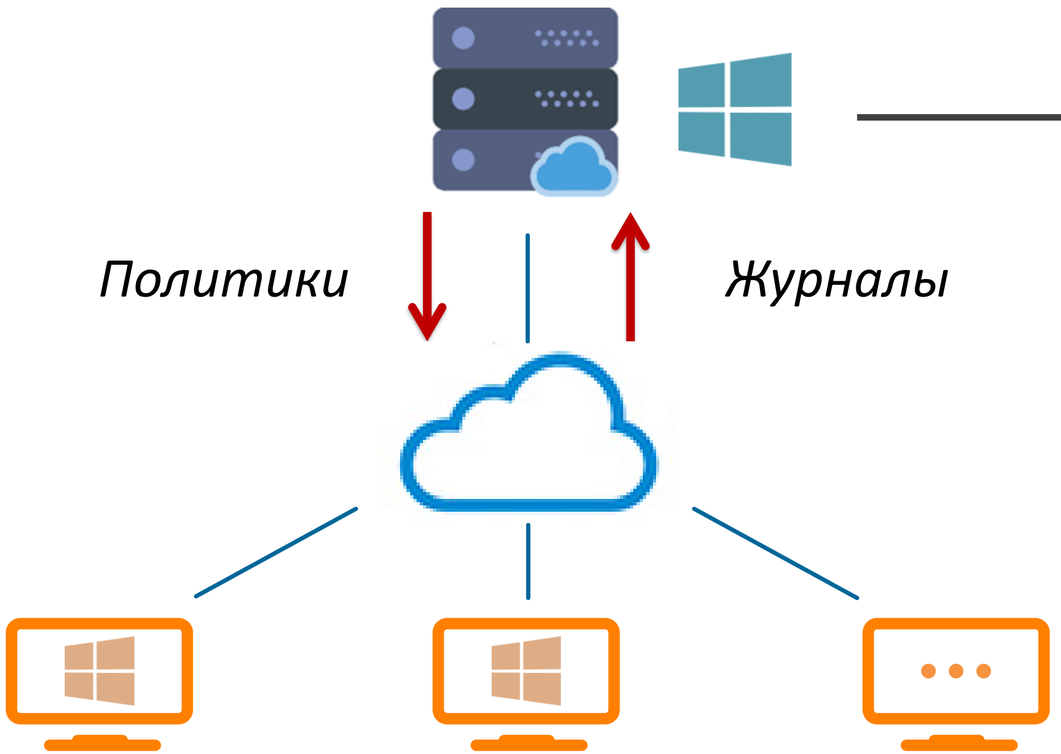
Удалённое администрирование



Централизованное управление:

- однотипными агентами
- разнотипными агентами
- сторонними решениями

Центры управления СЗИ до импортозамещения



Центр управления работает под управлением ОС Windows

Управление однотипными клиентскими СЗИ

Тренды импортозамещения

Для защиты применяются сертифицированные СЗИ от НСД

Защита рабочих станций и серверов

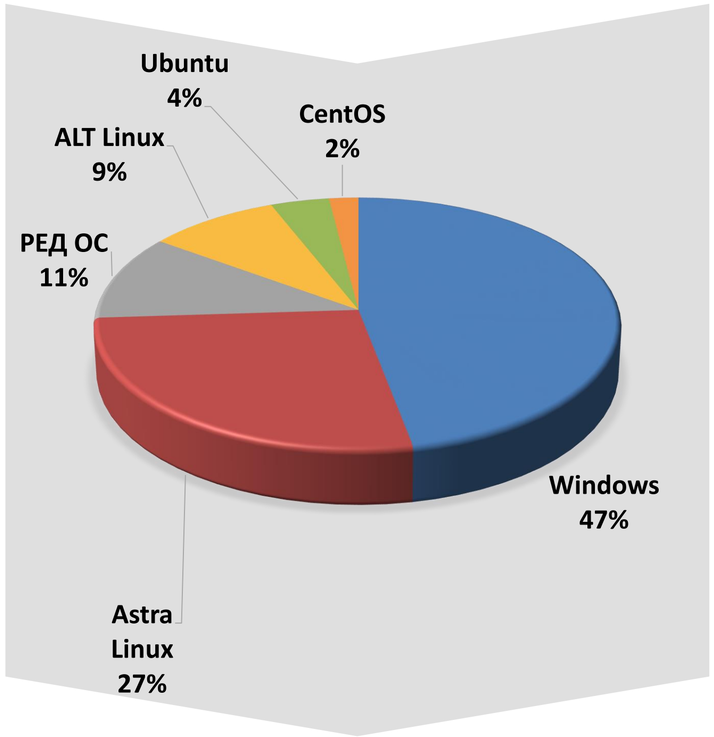
Windows → Linux → Отечественные операционные системы

Для защиты применяются сертифицированные СЗИ ВИ

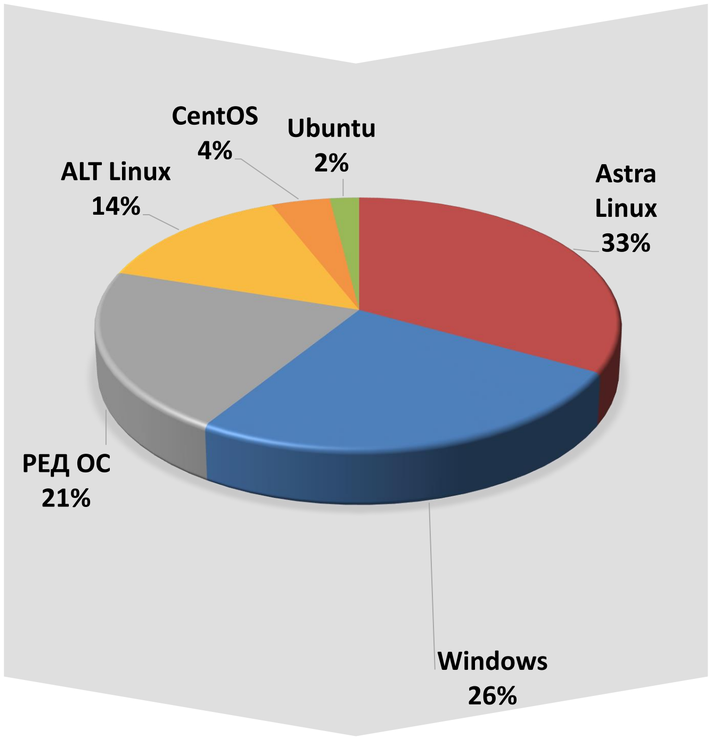
Защита среды виртуализации

VMware, Hyper-V → KVM, oVirt → Отечественные платформы виртуализации

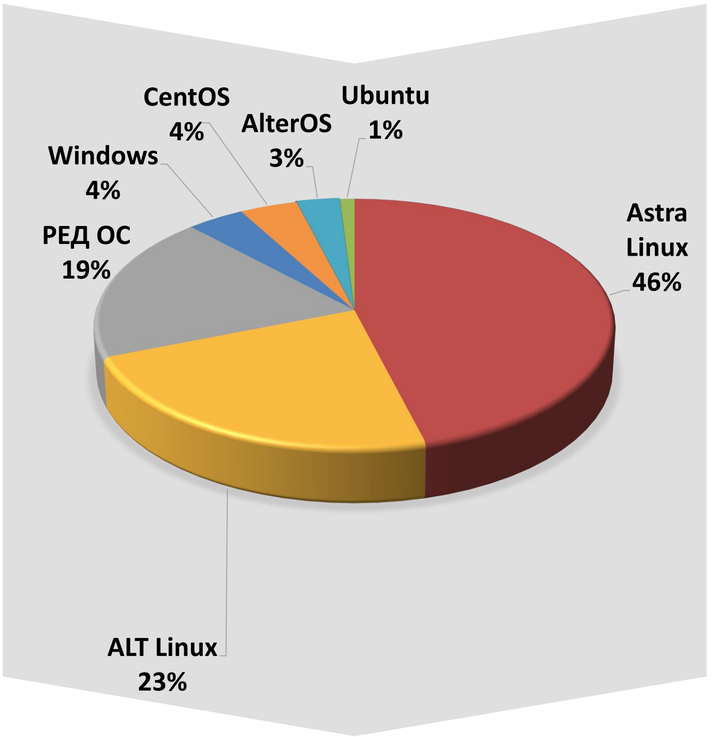
Наиболее популярные ОС в проектах по защите информации конечных точек в 2021, 2022, 2023 (прогноз)



2021



2022

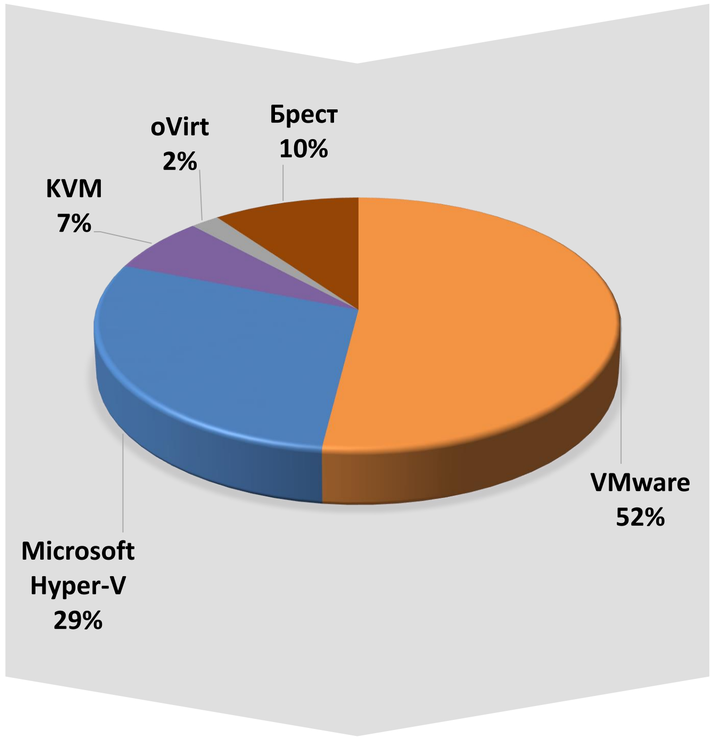


2023

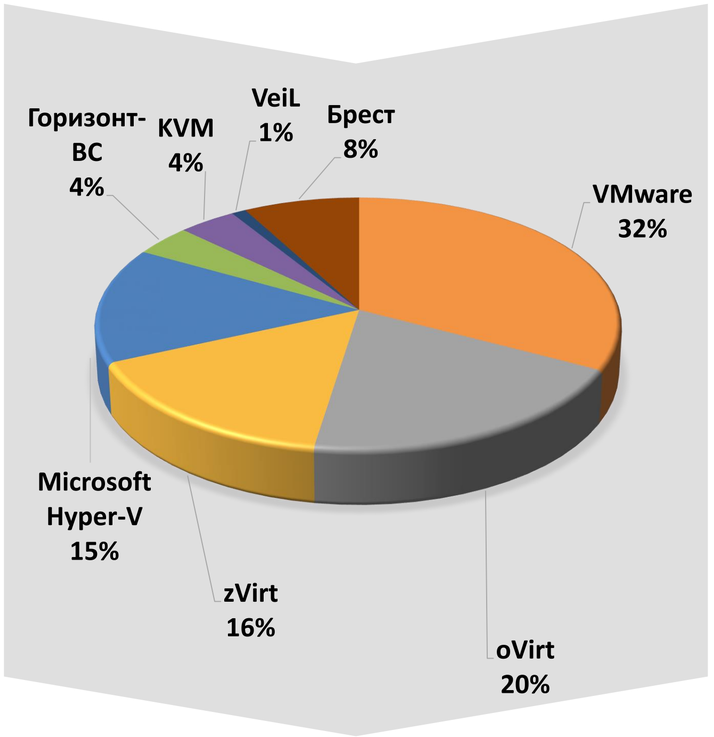
(прогноз)

Результаты опроса ключевых партнёров ЦЗИ ГК «Конфидент», январь - февраль 2023 г.

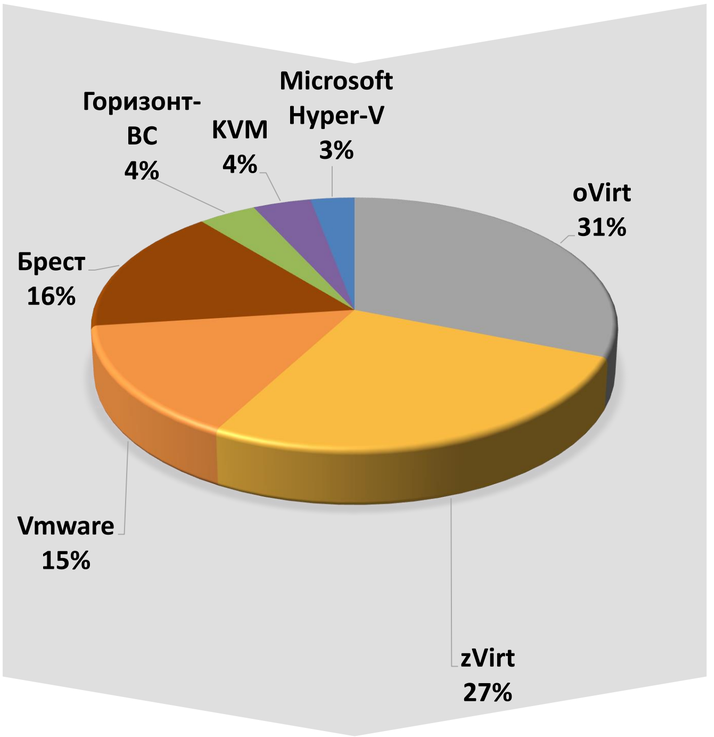
Наиболее популярные системы виртуализации в проектах по защите информации в 2021, 2022, 2023 (прогноз)



2021



2022

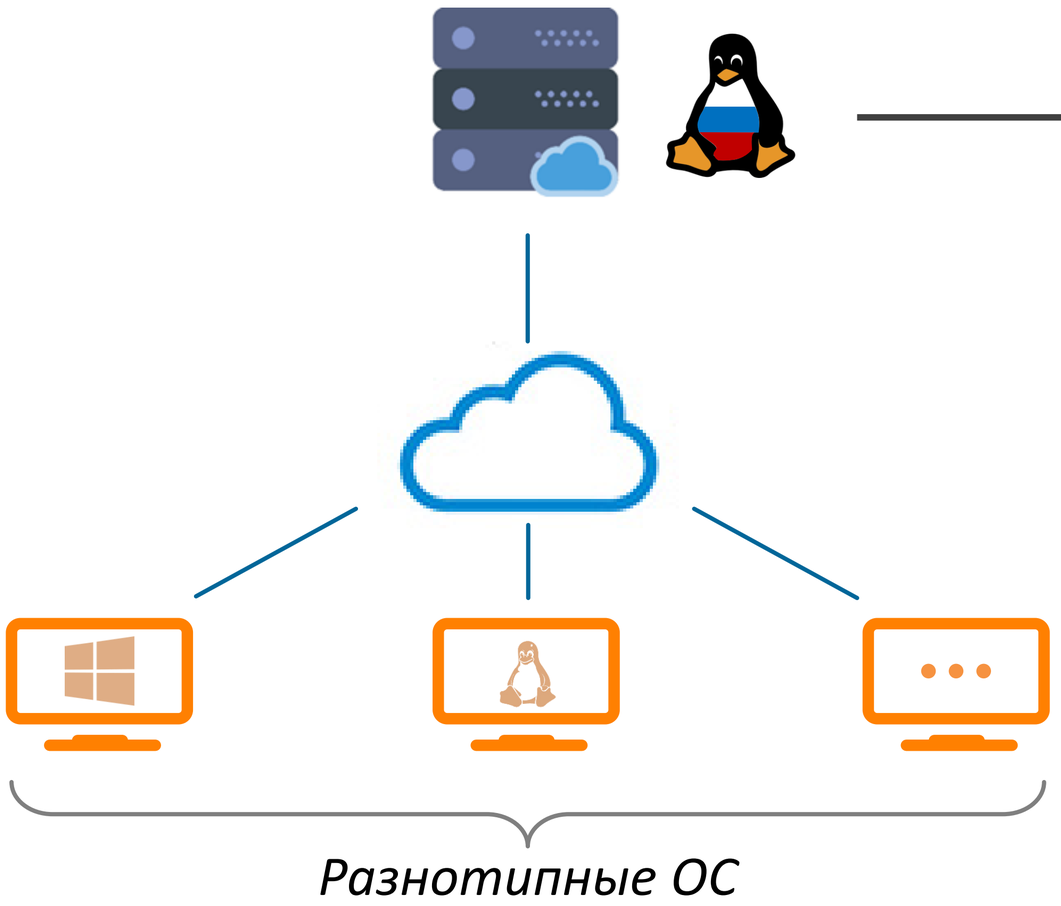


2023

(прогноз)

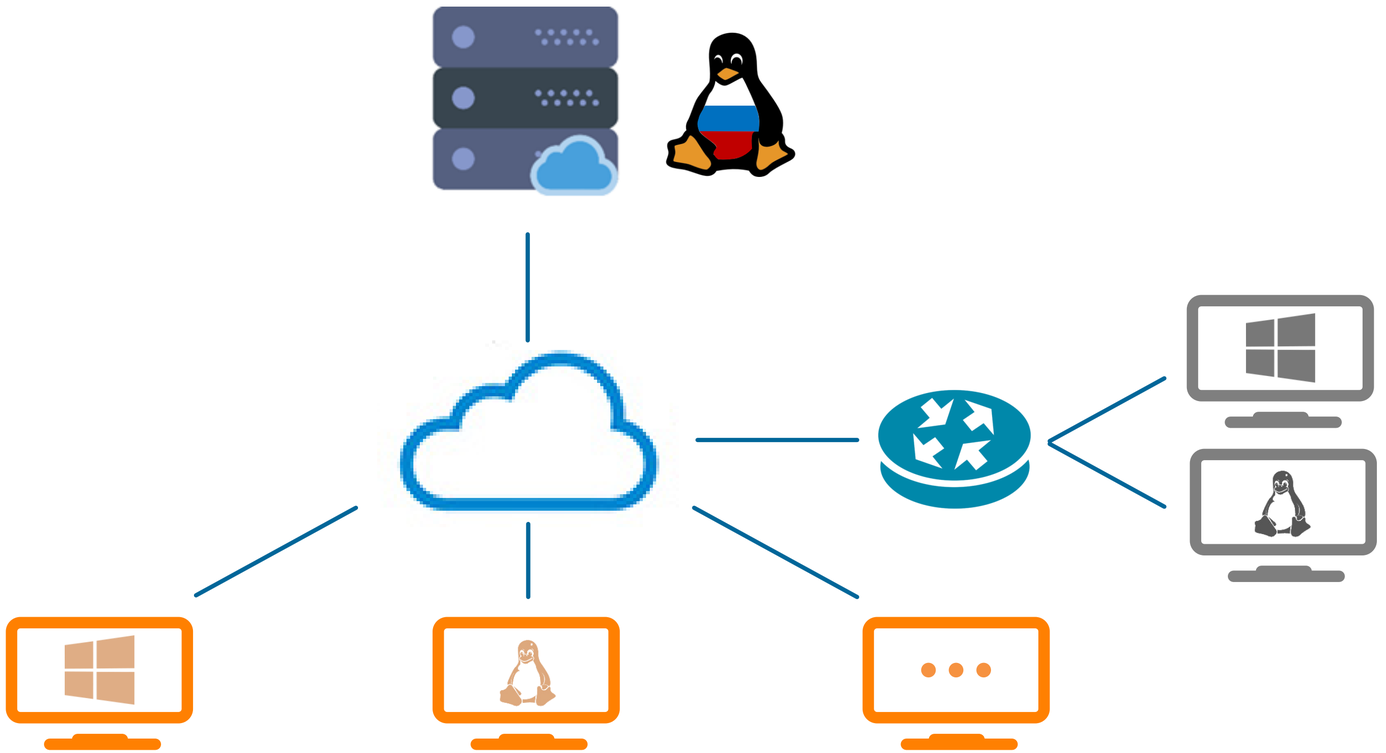
Результаты опроса ключевых партнёров ЦЗИ ГК «Конфидент», январь - февраль 2023 г.

Особенности централизованного управления СЗИ сейчас



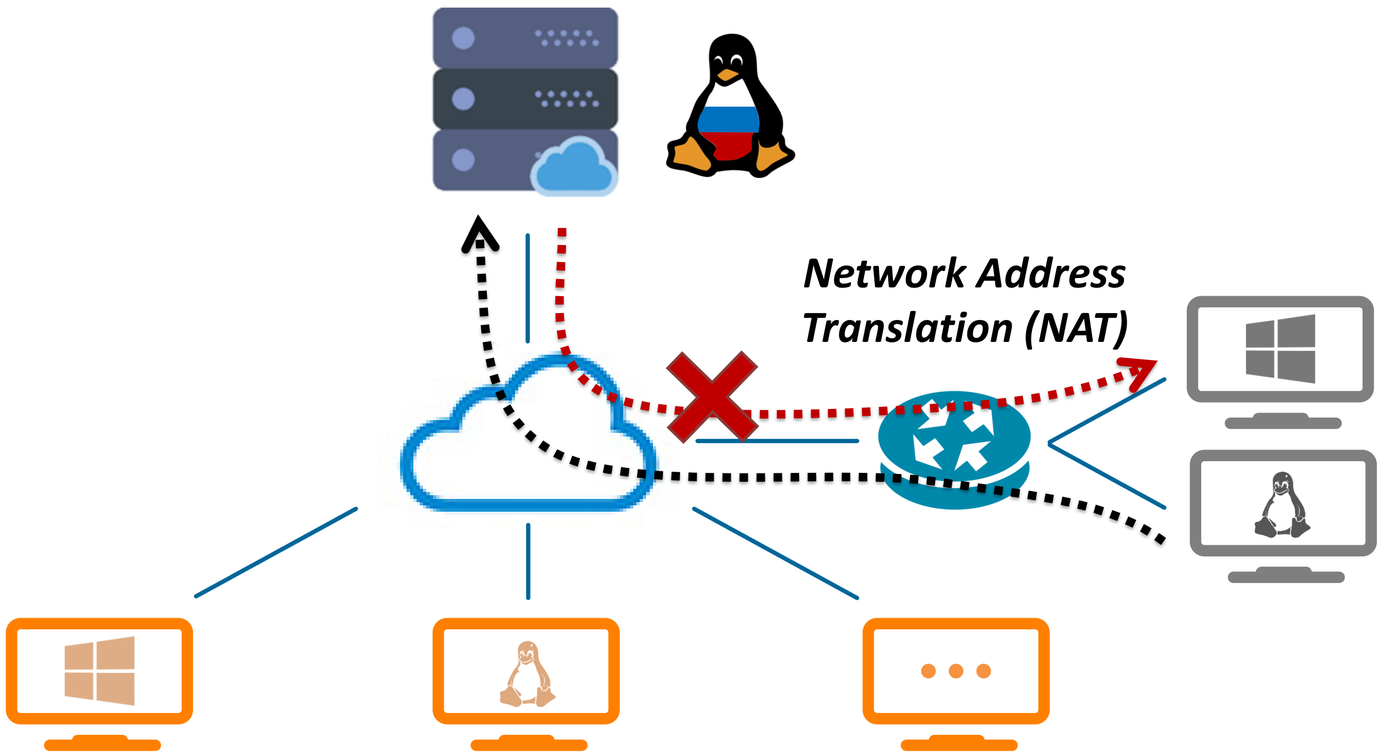
Центр управления работает под управлением российских ОС

Особенности централизованного управления СЗИ сейчас



Проблема учёта и настройки удалённых АРМ в подведомственных учреждениях и при дистанционной работе: не всегда есть возможность установить СЗИ

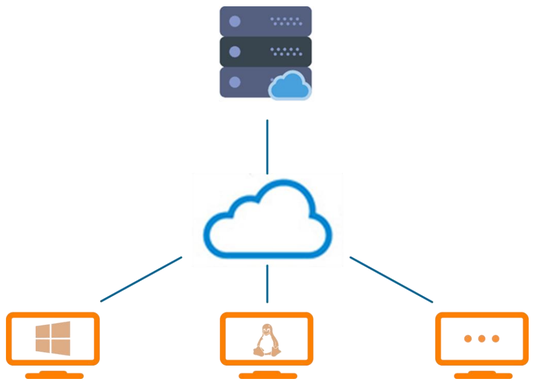
Особенности централизованного управления СЗИ сейчас



Проблема доступа к АРМ, находящимися за NAT и проблема сбора журналов

Система защиты информации должна отвечать новым вызовам

Центр управления

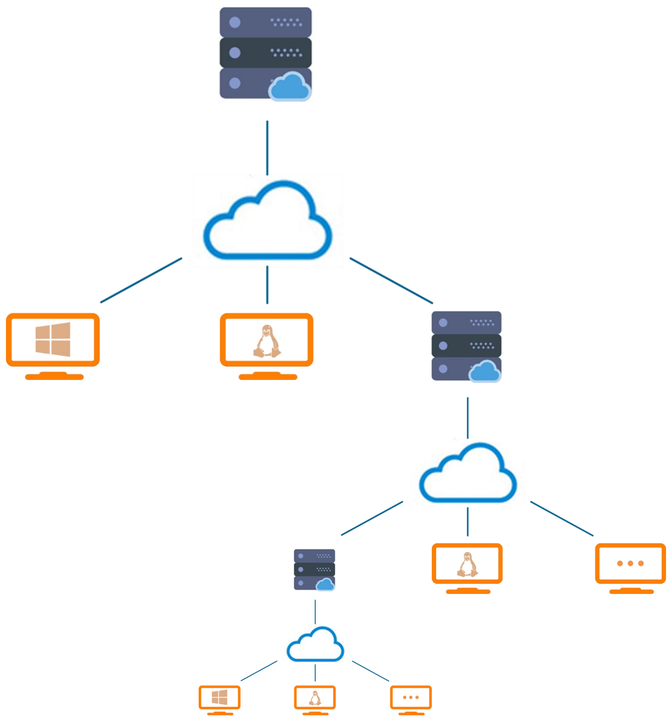


Современные требования к Центру управления информационной безопасностью:

- Поддержка сертифицированных отечественных ОС
- Управление клиентскими частями под Windows и Linux, СДЗ, поддержка российских ОС, а также возможность удалённого подключения к ним
- Возможность получать журналы с незащищённых АРМ
- Наличие встроенного VNC-клиента
- Работа за NAT (Network Address Translation)
- Бесперебойная работа в больших инфраструктурах и при «слабом» сетевом соединении

Единый центр управления Dallas Lock

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK



Кросс-платформенное решение для централизованного управления ИБ предприятия

1 **Поддержка российских ОС, в том числе сертифицированных по требованиям ФСТЭК России**

2 **У правление СЗИ под Windows, Linux, российскими ОС, СДЗ**

3 **Работа за NAT (Network Address Translation)**

4 **Наличие встроенного агента под Windows и Linux/российские ОС**

Иерархическая структура доменов безопасности, контроль целостности настроек сетевого оборудования, не требователен к ресурсам.

Наиболее востребованные у заказчиков дополнительные функции

Результаты опроса авторизованных пользователей портала dallaslock.ru, сентябрь 2022 - январь 2023 г.

Отношение к наложенным СЗИ как к классу решений для защиты конечных точек

75% опрошенных отмечают, что наложенные СЗИ полезны и необходимы для защиты информации

Результаты опроса ключевых партнёров ЦЗИ ГК «Конфидент», январь - февраль 2023 г.

Выводы

1. Процесс перевода ИТ-инфраструктур заказчиков на отечественные решения близок к завершению
2. Некоторые сегменты ИТ-инфраструктуры остаются реализованными на старых решениях/платформах
3. Заказчики предъявляют повышенные требования к централизованному управлению ИБ
4. Заказчики и партнеры отмечают недостаток встроенных в ОС/платформы защитных механизмов

Спасибо за внимание!

ЕГОР КОЖЕМЯКА

ДИРЕКТОР ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU