КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Тренды развития сертифицированных средств защиты информации в современных реалиях

Евгений Мардыко

**КОММЕРЧЕСКИЙ ДИРЕКТОР
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»**

EMAIL: ISC@CONFIDENT.RU

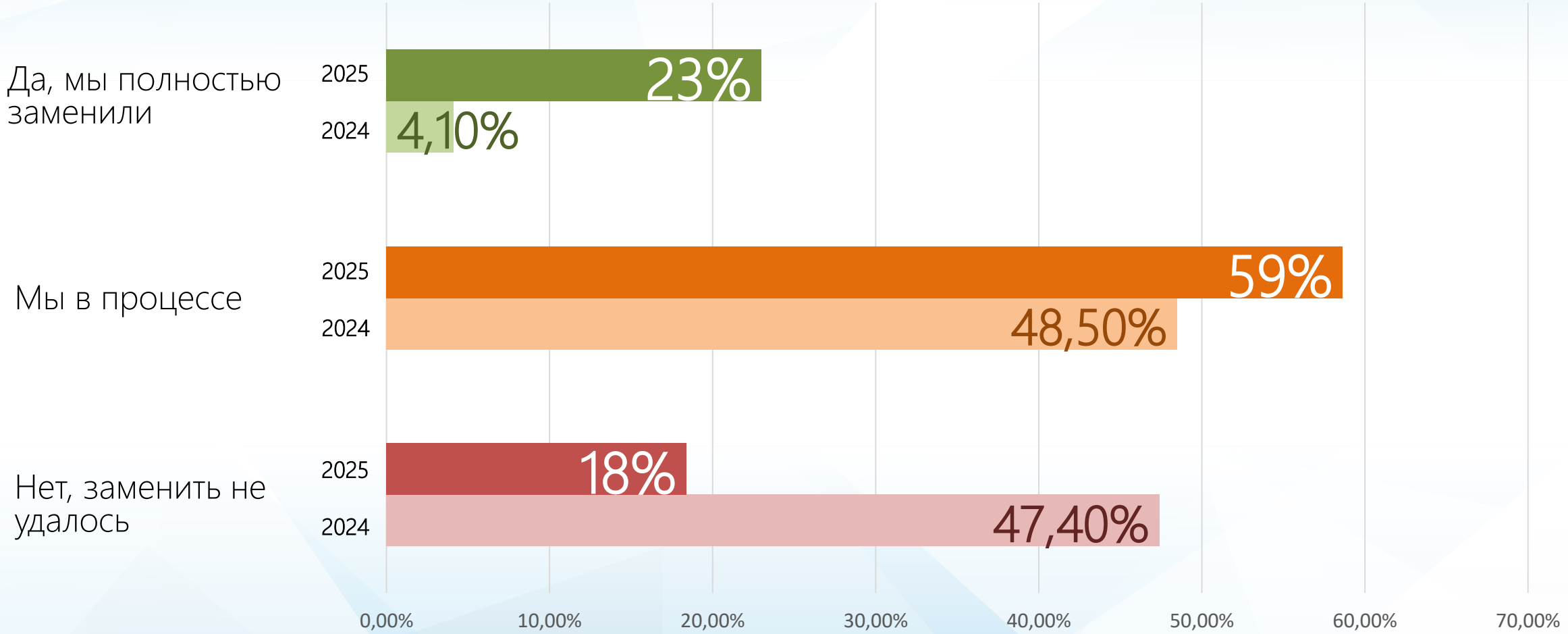
WEB: WWW.DALLASLOCK.RU

Кратко о продуктовой линейке Dallas Lock

> 6500

проектов ежегодно реализуется в России с использованием продуктов Dallas Lock

Смогли ли вы заменить иностранные решения и сервисы на отечественные?



Ключевые проблемы построения систем ИБ

- Импортозамещение – это длительный и сложный процесс
- Гетерогенные среды сложны в управлении, учете, применении единых политик и сохранении их при обновлении и миграции
- Отсутствие взаимосвязанности решений различных вендоров
- Усложнение атак злоумышленниками
- Усиление требований регуляторов
- Недостаток кадров

О продуктах

Dallas Lock 8.0

Dallas Lock Linux

СДЗ Dallas Lock

СЗИ ВИ Dallas Lock

Набор решений для защиты информации в физических и виртуализированных средах с централизованным управлением

ЕЦУ Dallas Lock

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Новое в продуктах

СЗИ Dallas Lock Linux

- отказ от технологии подмены ядра
- расширен список поддерживаемых ОС
- сертификат МЭ
- сертификат СОВ
- удалённое управление модулем СКН и МЭ*

СЗИ Dallas Lock 8.0

- защита от вирусов-шифровальщиков
- централизованное управление модулем МЭ*
- мастер настроек СОВ*
- блокировка телеметрии Windows
- автозапуск определенного процесса в Безопасной среде

СЗИ ВИ Dallas Lock

- поддержка гипервизоров на базе KVM и oVirt, а также VMWare и Hyper-V рамках единой лицензии
- администрирование и аудит из единой веб-консоли
- управление полностью реализовано на отечественных решениях

СДЗ Dallas Lock

- три форм-фактора СДЗ ПР: PCI-E, mini PCI-E, M2
- СДЗ уровня BIOS со щадящим режимом использования микросхемы BIOS и широким спектром совместимости
- централизованное управление*

*возможно при наличии ЕЦУ

СЗИ Dallas Lock Linux

сертифицированная система защиты информации накладного типа для защиты конфиденциальной информации.

Построение комплексной системы защиты информации в гетерогенной среде

+

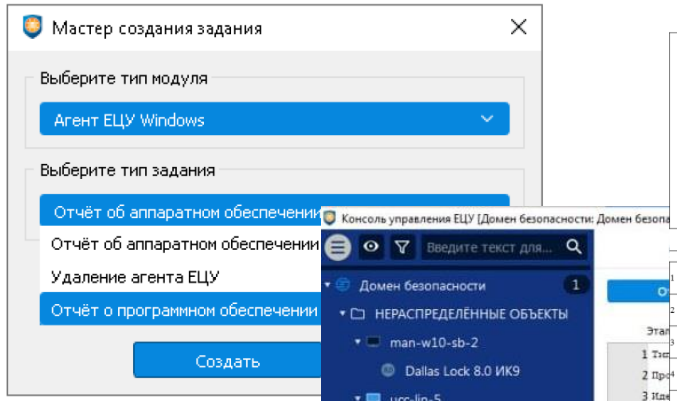
универсальная лицензия на СЗИ

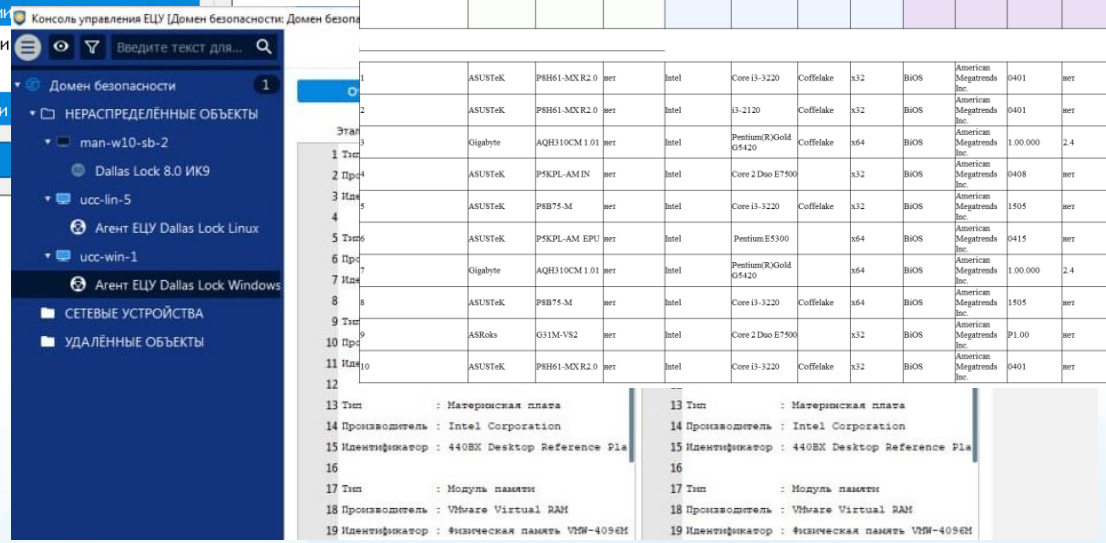
Единый центр управления – кросс-платформенное решение для централизованного управления ИБ предприятия

- Иерархическая структура доменов безопасности
- Контроль целостности настроек сетевого оборудования
- Работа за NAT
- Управление Dallas Lock 8.0/Linux, СДЗ, СЗИ ВИ
- Поддержка российских ОС
- Не требователен к ресурсам, поддержка работы десятков тысяч АРМ одновременно

Примеры использования решений

Организация с 400 подведомственными учреждениями по всему региону. Разнородный парк техники.
Задача: в короткий срок подобрать СДЗ.
Решение: 8 организаций, 3922 АРМ, 5 рабочих дней. ЕЦУ + агент ЕЦУ Dallas Lock.





№ пп	Материнская плата			Процессор				BIOS/UEFI					Операционная система						Оперативная память		Метод аутентификации на данный момент	
	Марка	Модель	Наличие дискретной видеокарты, если да, то какая	Марка	Модель	Поколение	Архитектура	Тип: BIOS или UEFI	Марка	Версия BIOS	Версия UEFI, если есть	Поддерживаемые режимы загрузки: UEFI или Legacy, UEFI/Legacy	Возможность перезаписи BIOS (да/нет)	Текущая ОС: Windows или Linux	Версия ядра, для Linux	В каком режиме установлена: UEFI или Legacy	Планируется ли замена на сертифицированную ОС			Тип	Объём, Гб	Пароль	Токены, если да то какие: карта, USB токен, магнитный ключ (таблетка), и тд.
																	Название, редакция	Версия ядра.	В каком режиме планируется установка: UEFI или Legacy				
1	ASUSTeK	P8H61-MX R2.0	нет	Intel	Core i3-3220	Coffelake	x32	BIOS	American Megatrends Inc.	0401	нет	Legacy	нет	Windows 7 Профессиональная		Legacy	Astra Linux Special Edition	5.15	UEFI	DDR2	2	Пароль	нет
2	ASUSTeK	P8H61-MX R2.0	нет	Intel	i3-2120	Coffelake	x32	BIOS	American Megatrends Inc.	0401	нет	Legacy	нет	Windows 7 Профессиональная		Legacy	Astra Linux Special Edition	5.15	UEFI	DDR2	2	Пароль	нет
3	Gigabyte	AQH310CM 1.01	нет	Intel	Pentium(R)Gold G5420	Coffelake	x64	BIOS	American Megatrends Inc.	1.00.000	2.4	UEFI/Legacy	нет	Linux Mint 20.1	Linux 5.4.0-65-generic (x86_64)	UEFI	Astra Linux Special Edition	5.15	UEFI	DDR3	8	Пароль	нет
4	ASUSTeK	P5KPL-AM IN	нет	Intel	Core 2 Duo E7500		x32	BIOS	American Megatrends Inc.	0408	нет	Legacy	нет	Windows 7 Профессиональная		Legacy	Astra Linux Special Edition	5.15	UEFI	DDR2	2	Пароль	нет
5	ASUSTeK	P8B75-M	нет	Intel	Core i3-3220	Coffelake	x32	BIOS	American Megatrends Inc.	1505	нет	Legacy	нет	Windows 7 Профессиональная		Legacy	Astra Linux Special Edition	5.15	UEFI	DDR2	2	Пароль	нет
6	ASUSTeK	P5KPL-AM EPU	нет	Intel	Pentium E5300		x64	BIOS	American Megatrends Inc.	0415	нет	Legacy	нет	Windows 10 pro		Legacy	Astra Linux Special Edition	5.15	UEFI	DDR2	2	Пароль	нет
7	Gigabyte	AQH310CM 1.01	нет	Intel	Pentium(R)Gold G5420		x64	BIOS	American Megatrends Inc.	1.00.000	2.4	UEFI/Legacy	нет	Linux Mint 20.1	Linux 5.4.0-65-generic (x86_64)	UEFI	Astra Linux Special Edition	5.15	UEFI	DDR3	8	Пароль	нет
8	ASUSTeK	P8B75-M	нет	Intel	Core i3-3220	Coffelake	x64	BIOS	American Megatrends Inc.	1505	нет	Legacy	нет	Windows 7 Профессиональная		Legacy	Astra Linux Special Edition	5.15	UEFI	DDR2	2	Пароль	нет
9	ASRoks	G31M-VS2	нет	Intel	Core 2 Duo E7500		x32	BIOS	American Megatrends Inc.	P1.00	нет	Legacy	нет	Windows 7 Профессиональная		Legacy	Astra Linux Special Edition	5.15	UEFI	DDR2	4	Пароль	нет
10	ASUSTeK	P8H61-MX R2.0	нет	Intel	Core i3-3220	Coffelake	x32	BIOS	American Megatrends Inc.	0401	нет	Legacy	нет	Windows 7 Профессиональная		Legacy	Astra Linux Special Edition	5.15	UEFI	DDR2	2	Пароль	нет

```
Тип             : Материнская плата
Производитель   : Intel Corporation
Идентификатор   : 440BX Desktop Reference Pla

Тип             : Модуль памяти
Производитель   : VMware Virtual RAM
Идентификатор   : Физическая память VMW-4096M
```

```
Тип             : Материнская плата
Производитель   : Intel Corporation
Идентификатор   : 440BX Desktop Reference Pla

Тип             : Модуль памяти
Производитель   : VMware Virtual RAM
Идентификатор   : Физическая память VMW-4096M
```

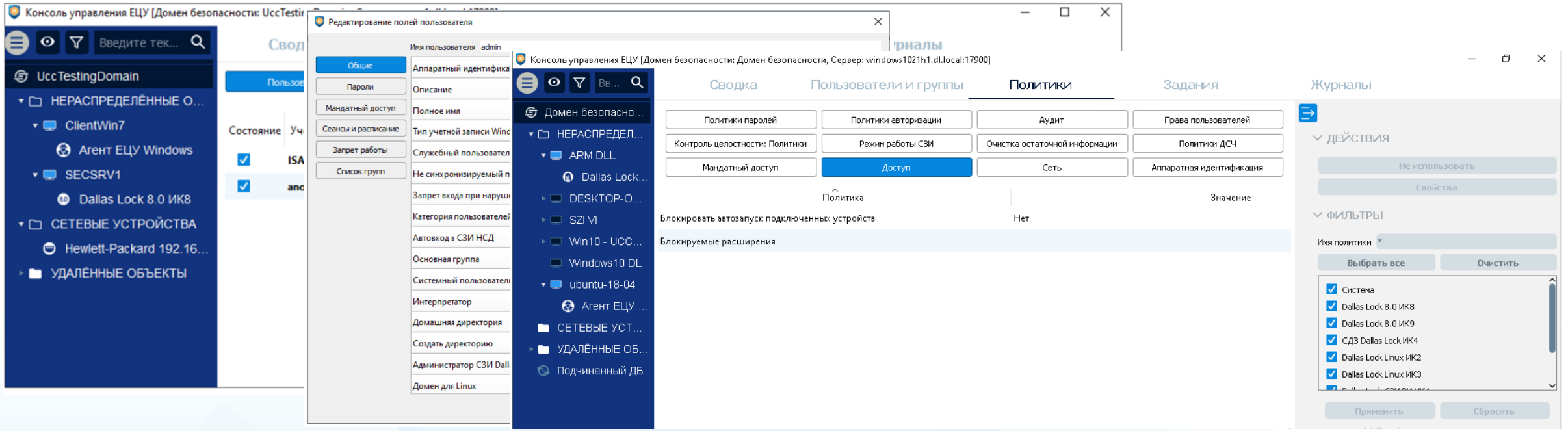
Итог: получен перечень совместимых устройств и систематизированы в группы, несовместимые для дальнейшего формирования плана внедрения.

Примеры использования решений

Организация в стадии объединения нескольких подразделений с разными доменными структурами на Windows. Планируют переход на Linux. Используют СЗИ Dallas Lock.

Задача: организовать централизованное управление политиками безопасности групп пользователей, которые не соотносятся с доменной структурой, так как она будет меняться в дальнейшем.

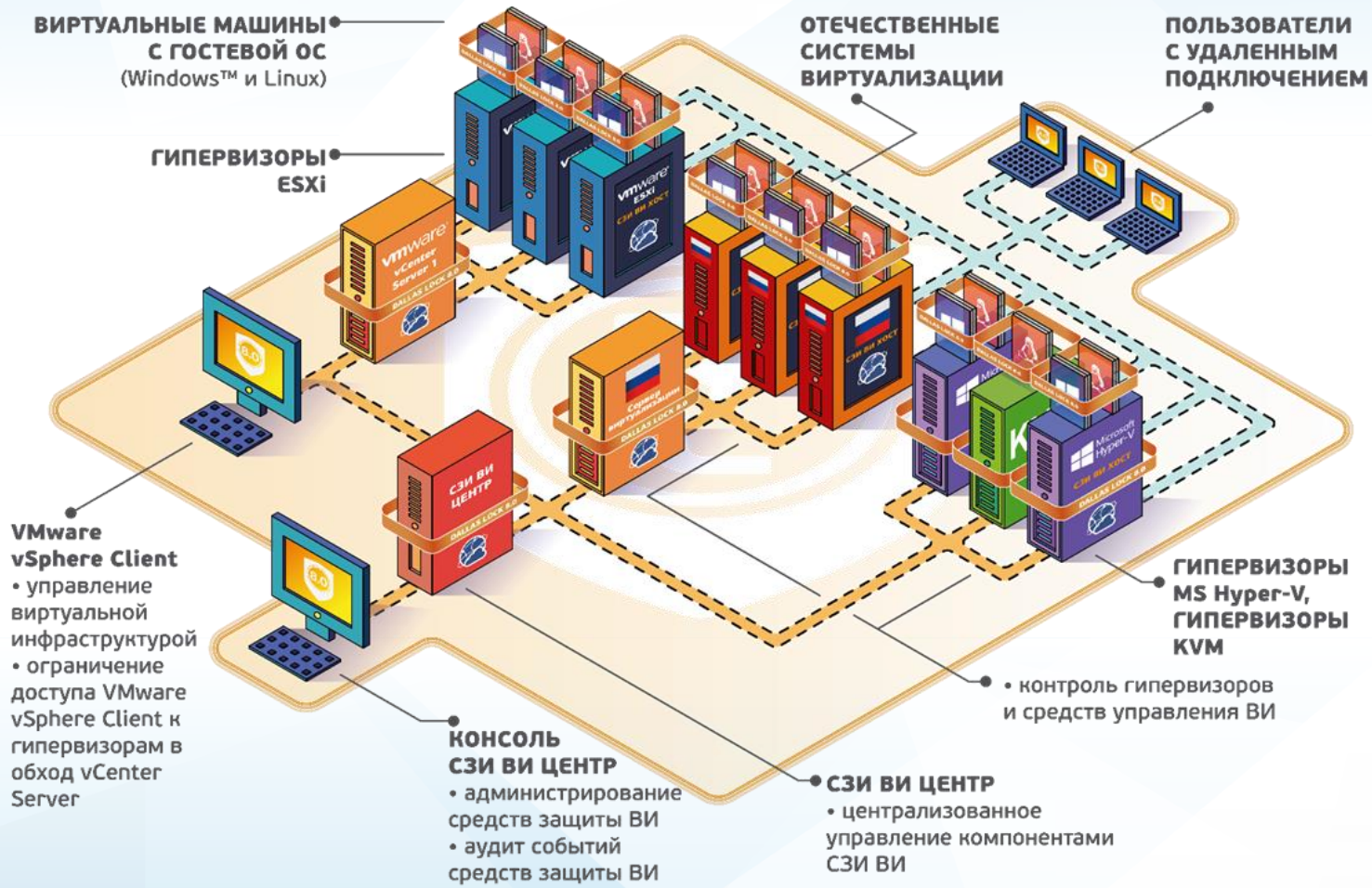
Решение: построение дерева безопасности в ЕЦУ Dallas Lock, перевод DL 8.0 на универсальный.



Итог: заказчик получил возможность централизованного управления учетными записями и политиками безопасности в группах, а также возможность удаленного доступа к АРМ и мониторинга событий безопасности с дальнейшей отправкой данных в SIEM.

Примеры использования решений

Информационный центр региона в рамках ЦОД использует VMware. Находятся в состоянии подбора отечественной среды виртуализации.
Задача: защитить имеющийся гипервизор от НСД без дополнительных затрат на постепенный переход на отечественные системы виртуализации в дальнейшем.
Решение: СЗИ ВИ.
Итог: на текущий момент произведен частичный переход на отечественный гипервизор. Управление СЗИ ВИ включено в ЕЦУ для комплексного управления инфраструктурой и дальнейшей передачи инцидентов в SIEM.



КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Шлюз безопасности WAF Dallas Lock – новый продукт 2024

Включен в единый реестр российского ПО
Запись в реестре № 21831 от 15.03.2024 г.

Сертификат ФСТЭК России № 4863 от 8.10.2024 года
по 4 классу защиты МЭ (ИТ.МЭ.Г4.ПЗ)
по 4 классу защиты МЭ (ИТ.МЭ.Б4.ПЗ)
по 4 классу защиты СОВ уровня сети (ИТ.СОВ.С4.ПЗ)
по 4 уровню доверия (УД 4)

WAF (Web Application Firewall) — межсетевой экран уровня веб-сервера

UTM (Unified Threat Management) — МЭ уровня логических границ сети и СОВ уровня сети

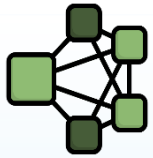
- Защита серверов и сервисов корпоративной сети
- Защита веб-приложения от нелегитимных запросов «из коробки»
- Поддержка работы с любыми гипервизорами в виртуальной инфраструктуре

Шлюз безопасности WAF Dallas Lock. Ключевые возможности

- На прикладном уровне: анализ трафика веб-приложений и обнаружение вторжений
- На транспортном и сетевом уровне: обнаружение атак на сетевую инфраструктуру

- Защита от угроз из списка OWASP TOP 10, XSS, CSRF, bruteforce-атак
- Инспекция SSL/TLS
- GEO IP фильтр

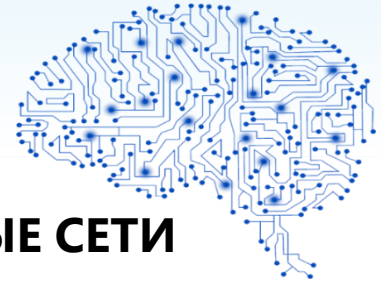
- Защита от DoS/DDoS
- Поддержка протокола HTTP 2.0/3.0



- Работа в режиме отказоустойчивого кластера
- Графическая панель мониторинга системы с отображением статистики
- Централизованный мониторинг и управление защитой из ЕЦУ Dallas Lock

Шлюз безопасности WAF Dallas Lock

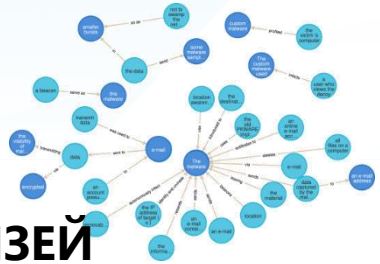
1



НЕЙРОННЫЕ СЕТИ

- комплексный анализ данных для обнаружения аномалий или нешаблонных атак
- возможность обучаться на больших объемах данных и находить скрытые зависимости между признаками угроз
- минимизация ложных срабатываний, приводящих к блокировке трафика и нарушению работы

2



ГРАФ СВЯЗЕЙ

- интерактивное представление модели нормального поведения пользователей
- предоставление подробной информации о структуре сайта и возможных переходах
- возможность уточнения и изменения модели поведения пользователей

3

ЗАЩИТА ОТ DDoS

- усиление механизмов защиты от DoS/DDoS атак на транспортном уровне модели OSI

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Стремление к согласованности при построении СЗИ важно для обеспечения **взаимосвязанной защиты** от разных вендоров

Технологические партнерства

Наличие согласованных протоколов обмена данными

POSITIVE TECHNOLOGIES

ASTRA LINUX®

RUSIEM

base alt

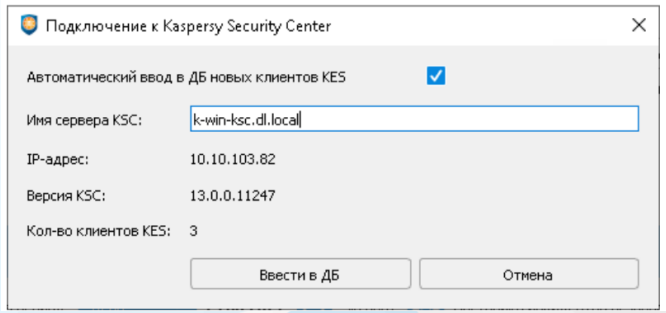
РЕДОС

Сертификаты совместимости

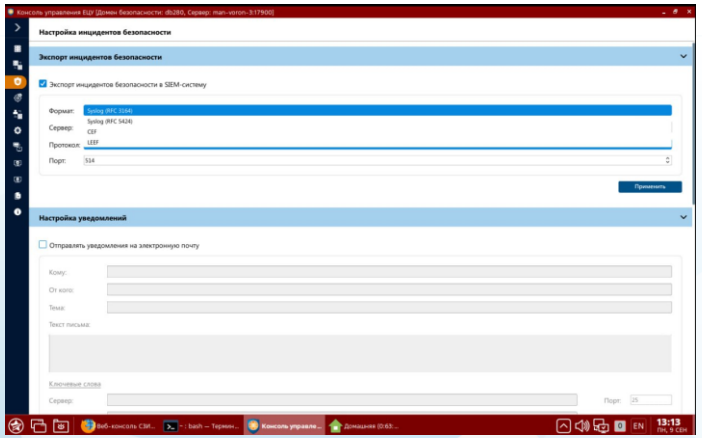
Практика проверки корректной работы в рамках одной ИС совместно с:

- SIEM
- САВЗ
- ВИ
- DLP
- ОС

Интеграция с Kaspersky Security Center для получения данных о состоянии, логов, журналов и запуска задач обновления баз данных и сканирования



Выгрузка в SIEM



Планы 2025

1

Создание совместных бандлов с ведущими производителями отечественных ОС:

- Продукты DL расширяют функционал ОС и повышают общий уровень защищенности инфраструктуры
- Централизованная настройка и управление из единой консоли ЕЦУ
- Экономия бюджета

2

Из МЭ и СОВ в EDR:

- Расширение функционала текущих модулей обнаружения и реагирования для повышения уровня защищенности инфраструктуры
- Централизованная настройка и управление из единой консоли ЕЦУ
- Привычный интерфейс с новым функционалом

3

Новое решение класса NAC для контроля и управления сетевым доступом:

- Помогает внедрять и контролировать политики подключения устройств и пользователей к сетям
- Централизованная настройка и управление из единой консоли ЕЦУ
- Повышение уровня защищенности инфраструктуры

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Спасибо за внимание!

Евгений Мардыко

КОММЕРЧЕСКИЙ ДИРЕКТОР
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

EMAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU