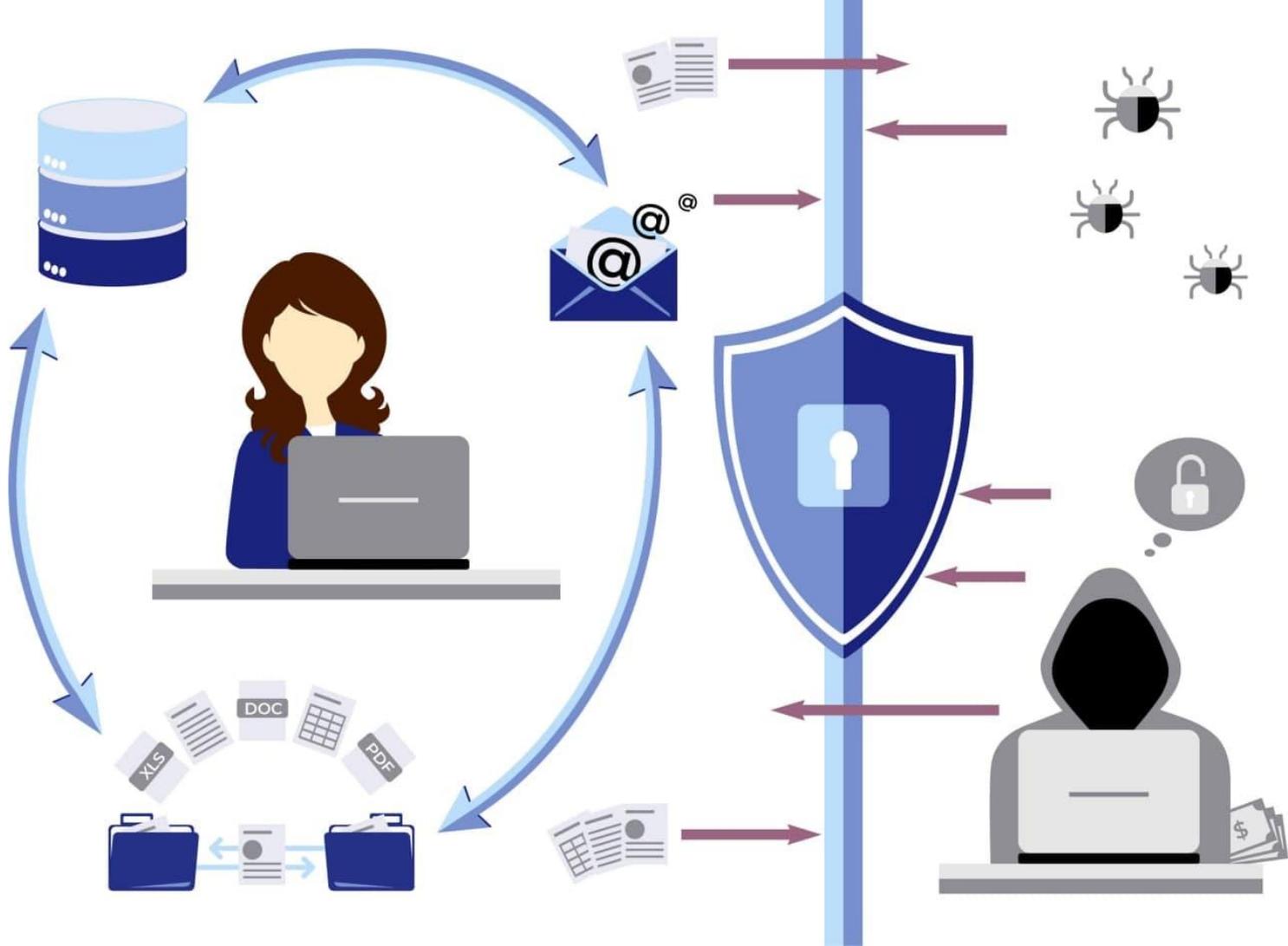




Как DCAP помогает перейти к модели Zero Trust

Роман Подкопаев





Принципы Zero Trust

1

Все объекты не
надежны по
умолчанию

2

Доступ с
наименьшими
привилегиями

3

Комплексный
мониторинг
безопасности

Источник: <https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/>



С ЧЕГО НАЧАТЬ ПЕРЕХОД НА ZERO TRUST?



ЗАЩИТА ДАННЫХ КАК ОСНОВА ИБ-СТРАТЕГИИ



Чтобы защитить данные, важно знать:

1

Какие документы
и файлы содержат
ценную информацию

2

Каким объемом таких
данных владеет
компания и где они
находятся?

3

Кто является
владельцем, у кого
есть доступ к
просмотру и
редактированию?

Как работает DCAP



Поиск данных, требующих защиты, по содержимому и внешним атрибутам.

Анализ и категоризация

2

Определение избыточных (нерегламентированных) прав, нарушения доступа.

Оценка рисков

4

Поиск дубликатов, устаревших данных и учетных записей, версий и активаций ОС.

Актуальность файлов и ПО

6

1

Сбор данных

Аудит Active Directory, рабочих станций, файловых серверов, почтовых серверов.

3

Создание матрицы доступа

Наглядная матрица доступа пользователей к файлам, папкам и почтовым ящикам.

5

Мониторинг

Непрерывный анализ событий системы и действий пользователей.

Панель Рекомендаций Makves DСAP

MAKVES admin

Рекомендации

ПОЛЬЗОВАТЕЛИ

Отключите неактивных пользователей Количество: 37 Важность: 🔴

Отключите пользователей, которые уже 2 месяца не осуществляли вход в домен Показать/скрыть список ▾

	Имя	Риск-фактор	Аккаунт	NT-имя
<input type="checkbox"/>	Иванов Иван	26	ivanov	ИВАНОВ
<input checked="" type="checkbox"/>	Петров Петр	78	petrov	ПЕТРОВ
<input type="checkbox"/>	Сидоров Сидор	26	sidorov	СИДОРОВ
<input type="checkbox"/>	Сидорова Анна	78	sidorova	СИДОРОВА
<input type="checkbox"/>	Сидорова Мария	26	sidorova_m	СИДОРОВА

📄 Экспорт ✉ Переслать по почте 👁 Просмотреть учетную запись ➔ Отключить пользователя

Проинспектируйте пользователей с высоким риском Количество: 2 Важность: 🔴

Проверьте обоснованность параметров и поведение пользователей Показать/скрыть список ▾

Проинспектируйте атипичных пользователей Количество: 4 Важность: 🔴

Проинспектируйте пользователей с высоким уровнем атипичности Показать/скрыть список ▾

Установите срок действия пароля Количество: 31 Важность: 🟡

Установите срок действия пароля для пользователей, у которых он не установлен Показать/скрыть список ▾

Установите обязательный ввод пароля Количество: 2 Важность: 🟡

Установите обязательный ввод пароля для пользователей, для которых он необязателен Показать/скрыть список ▾

Удалите пустые группы Количество: 88 Важность: 🟢

Случаи из практики



Ненаследуемые
права



ФЗ-152, GDPR
Персональные
данные в открытом
доступе



Неактивные
пользователи



Не обязательные
пароли / без срока
действия



Незащищенные
дубликаты



«Временные» доступы
к ресурсам для
подрядчиков и
аудиторов

Особенности MAKVES DCAP

Активная реакция на инцидент

Устранение выявленных рисков в интерфейсе системы.

Продвинутый модуль аналитики

Контроль параметров всех сущностей системы позволяет вовремя реагировать на внутренние и внешние угрозы.

Не нарушает контуров безопасности

Выявляет конфиденциальную информацию в документах без создания теневого копий на выделенном ресурсе.

Песочница Makves

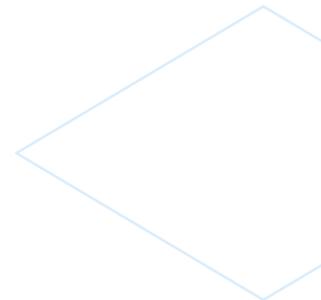
Моделирование последствий изменения прав пользователей.

Бесшовная интеграция

Интегрируется с любыми корпоративными программами и сервисами через REST.API.

Настраиваемые дашборды

Кастомизированная панель сводки с возможностью добавления виджетов по всем объектам анализа.



Zero Trust с Makves

1

Проверяйте, что хранится в сетевых папках и на ПК

2

Классифицируйте данные (152-ФЗ, ФСТЭК, GDPR, коммерческая тайна...)

3

Изучайте действия пользователей с ценными файлами и права доступа

Все объекты не надежны по умолчанию

- Обнаружение и классификация чувствительных данных
- Приоритизация данных с учетом рисков
- Выявление, изоляция и удаление неактуальных данных
- Настройка политик безопасности для пользователей, компьютеров, почты
- Управление правами доступа пользователей и групп пользователей
- Автоматический отзыв прав доступа
- Непрерывный мониторинг доступа
- Обнаружение аномальной активности
- Оценка и устранение рисков
- Настройка автоматического реагирования
- Интеграция с SIEM, DLP...

Доступ с наименьшими привилегиями

Комплексный мониторинг безопасности



МЫ НА СВЯЗИ

+7-495-150-54-06

sales@makves.ru

www.makves.ru