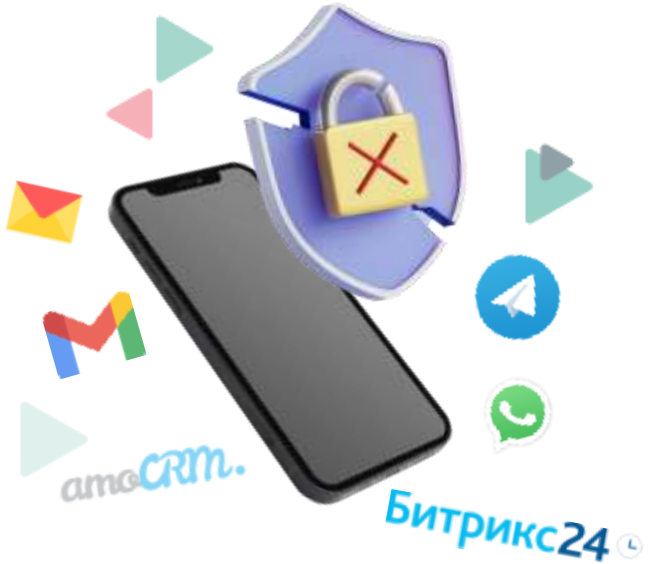
ИТЗ
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

CONEWS CONFERENCES

Что с защитой мобильных устройств?

— роль MDM в современной архитектуре кибербезопасности

Мобильные устройства: часть ИБ или «вне зоны покрытия»?



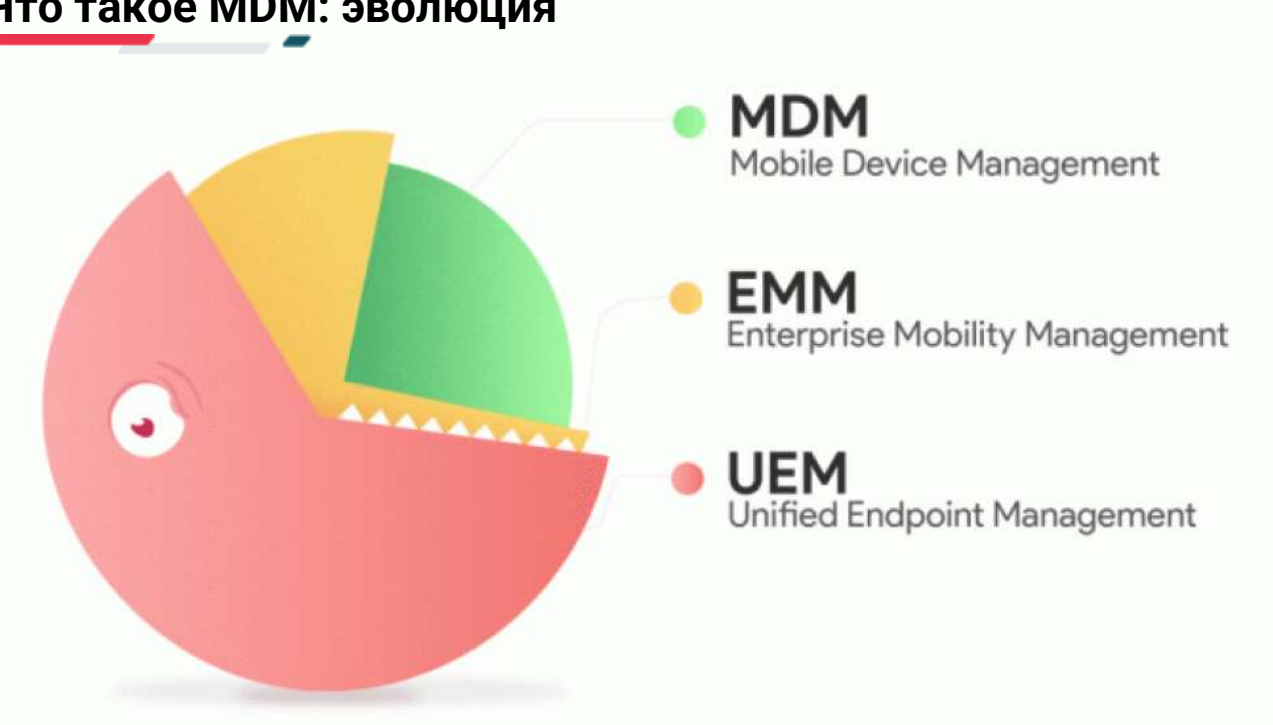
Что защищается — и что остаётся в

Что защищают традиционные меры — и что остаётся без внимания

Мера	Что защищает	Что не видит
VPN	Канал	Состояние устройства, malware
Антивирус	Некоторые угрозы	Поведение системы, zero-click атаки
MFA	Идентификацию	Root, jailbreak, утечку через приложения

Если вы не контролируете устройство — вы не контролируете доступ.

Что такое MDM: эволюция



MDM — это Mobile Device Management, UEM — Unified Endpoint Management — чуть более широкий класс, который может управлять не только смартфонами, но и ноутбуками, планшетами, иногда даже терминалами.

Что делает MDM — глазами ИБ

Возможность	Для чего в ИБ
Проверка состояния	Не даёт работать со взломанных устройств
Применение политик	Гарантирует, что устройство защищено
Блокировка / стирание	Реакция на утерю, взлом, увольнение
Интеграция с SOC / XDR	Автоматическое реагирование на инциденты

MDM — это не “сервис настройки телефона”
Это контроль доступа и защита от

Twitter — хронология атаки

без MDM

1. Фишинг
2. SIM-своппинг
3. Успешный вход
4. Взлом аккаунтов

с MDM

1. Доступ только с доверенного устройства
2. Вход невозможен

Al Jazeera — zero-click атака

MDM позволяет быстро отозвать доступ и стереть рабочую среду

Мобильные устройства — уже часть вашей ИБ.

1. Традиционные меры ≠ контроль устройства
2. MDM = контроль доступа и реакция
3. Угрозы — не теория, а практика
4. Решения есть, архитектура – ваш выбор

… вопрос в том, управляемая ли.

ИТЗ
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

CONEWS CONFERENCES

Дмитрий Костров

Начальник отдела по защите информации ООО СИБ МИР