Anti-Malware
Anti-Malicious Software

Независимый информационно-аналитический центр

DLP-системы – современные средства борьбы с инсайдерами

Илья Шабанов
Управляющий партнер

Anti-Malware
Anti-Malicious Software

План презентации

- Что такое DLP с точки зрения аналитика?
- Рынок средств защиты от утечки конфиденциальных данных в России
  - Состояние рынка
  - Объем рынка и основные игроки
- Тенденции на рынке
  - Технологические тенденции
  - Эволюция применимости
  - Интеграция со сторонними решениями
- Новые вызовы

Anti-Malware
Anti-Malicious Software

Чем можно защититься от утечек?

Средство защиты	Применение	Минусы
Классические антивирусы и сетевые экраны	Возможное обнаружение атаки	Бесполезны против целевых атак или действий инсайдеров
Шифрование	Защита от случайных утечек	Бесполезны против умышленных утечек
DLP-решения, включая близкие к ним (например, контроль портов)	Обнаружение несанкционированных действий с конфиденциальными данными	Недостаточно эффективны против умышленных утечек, могут быть сложны во внедрении
Rights Management Services (RMS)	Защита от случайных утечек	Бесполезны против умышленных утечек, сложны во внедрении и использовании

Anti-Malware
Anti-Malicious Software

Что такое DLP?

DLP-продукт обнаруживает и/или блокирует несанкционированную передачу конфиденциальной информации (утечку) по каналам:

- Электронная почта (трафик SMTP, POP3, IMAP)
- Веб-ресурсы (трафик HTTP, HTTPS и FTP)
- ICQ, Jabber, MSN, Skype, P2P-клиенты
- Сетевая печать
- Передача на внешние устройства

Anti-Malware
Anti-Malicious Software

Что такое DLP?

Атрибуты современной DLP-системы:

- Создание политик контроля данных
- Анализ контента и действий с ним (создание, копирование, изменение, передача и т.д.)
- Анализ контекста действий с данными (кем, кому и как передаются данные)
- Возможности блокирования утечки
- Оповещение о произошедшей или успешно заблокированной утечке
- Архив событий и инструменты пост-анализа для расследований

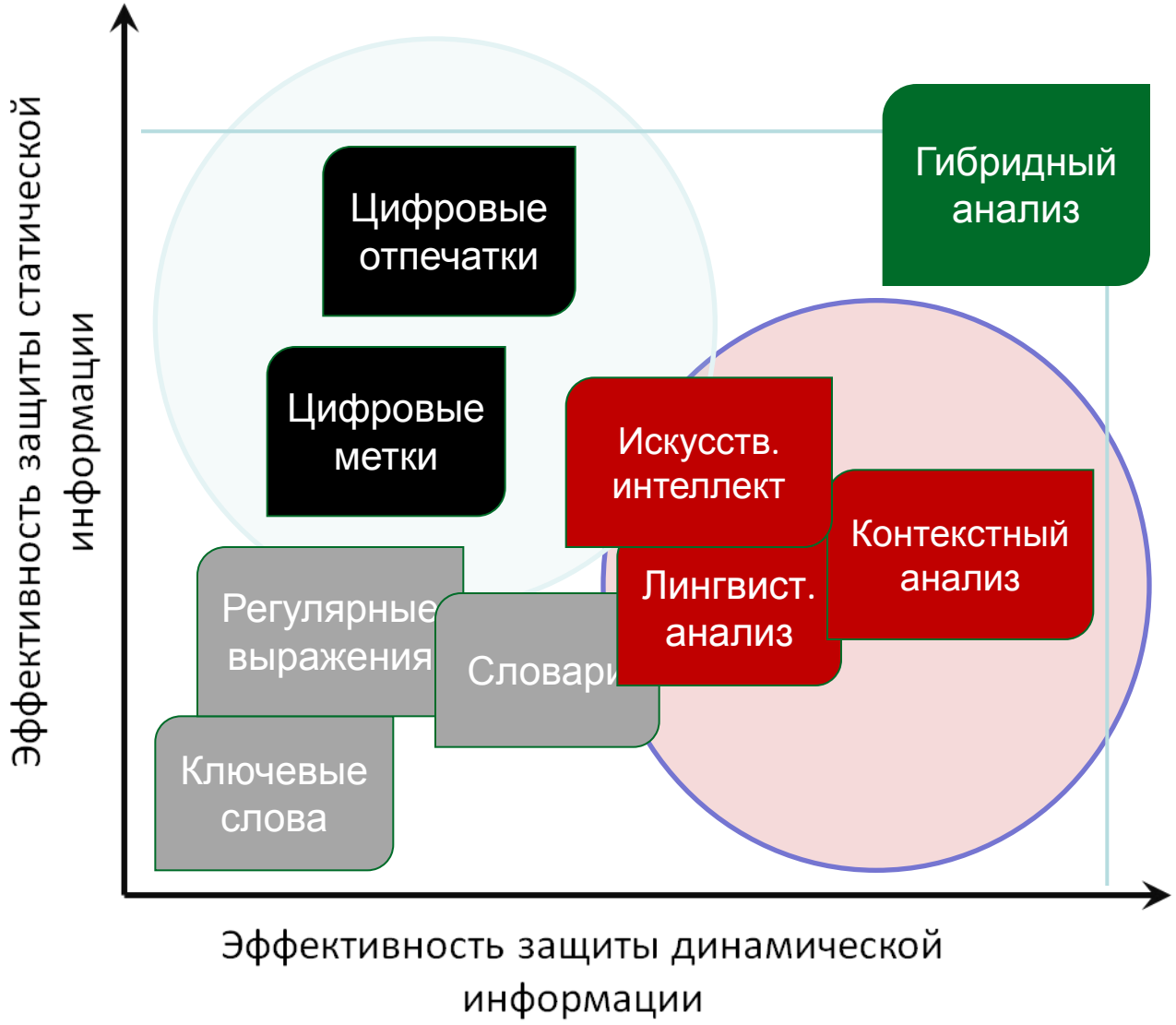
Anti-Malware
Anti-Malicious Software

Технологии защиты от утечек

Технология	Особенности и преимущества
Словари и регулярные выражений	Позволяет обнаруживать утечки данных, содержащих наборы слов или цифр
Лингвистический и контекстный анализ	Проактивная защита только конфиденциальных данных, сразу после их создания
Цифровые отпечатки или метки	Защита редко изменяемых конфиденциальных данных, которые были предварительно найдены и проиндексированы
Искусственный интеллект	Самообучающиеся алгоритмы детектирования

Anti-Malware
Anti-Malicious Software

Эффективность технологий



Эффективность гибридного анализа выше благодаря слиянию наиболее эффективных технологий

Anti-Malware
Anti-Malicious Software

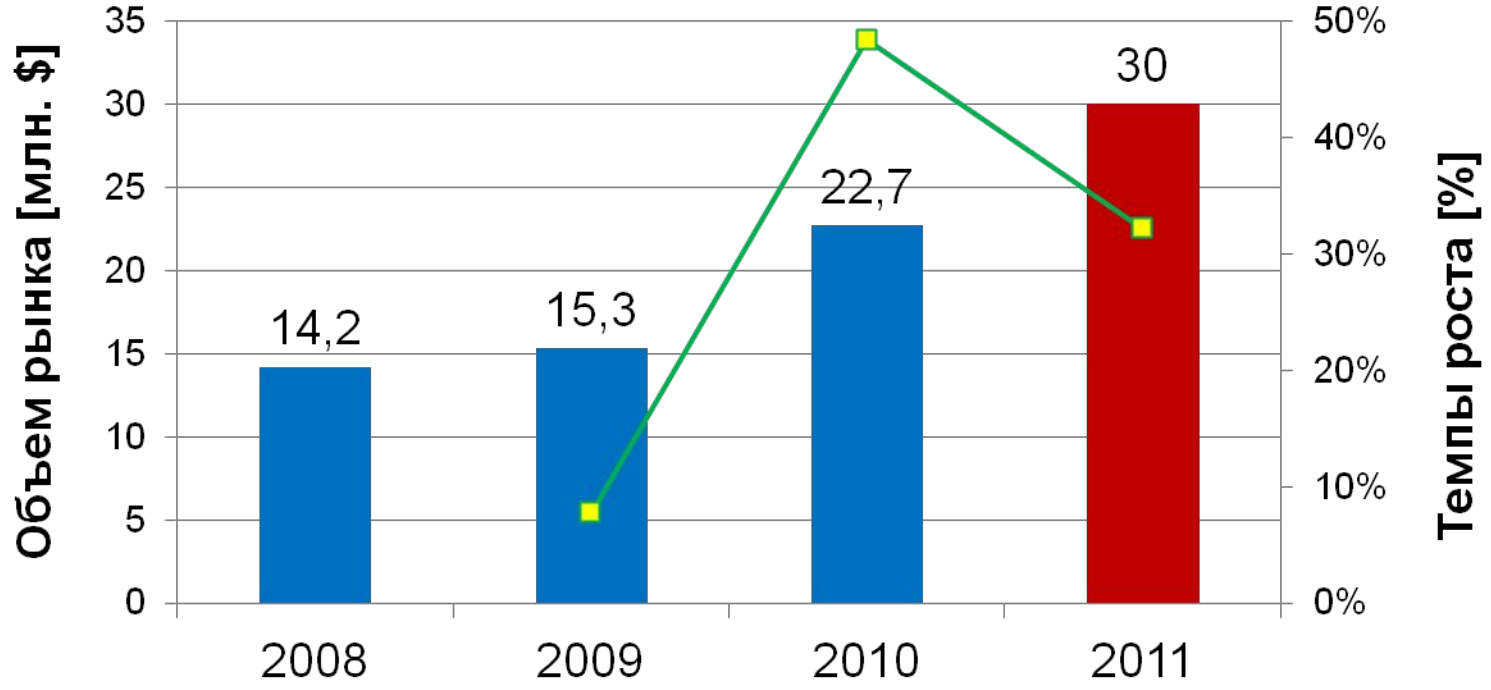
Рынок средств защиты

Какой DLP покупают в России?

Anti-Malware
Anti-Malicious Software

Объем DLP-рынка в России

Объем DLP-рынка в России в 2008-2010 годах (млн. USD)

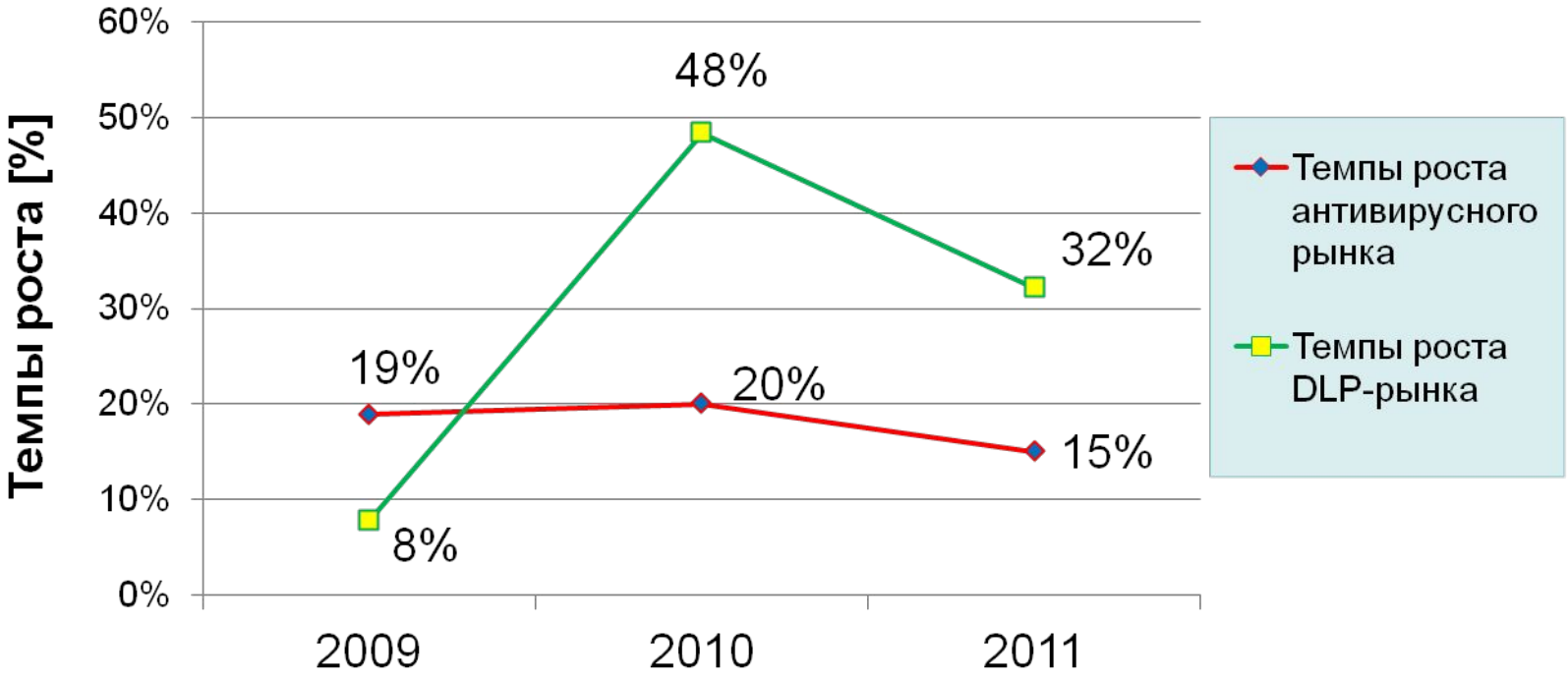


«Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2008-2010», Anti-Malware.ru, апрель 2010
«Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2009-2011», Anti-Malware.ru, июль 2011

Anti-Malware
Anti-Malicious Software

Темпы роста DLP-рынка в России

Объем DLP-рынка в России в 2008-2010 годах (млн. USD)

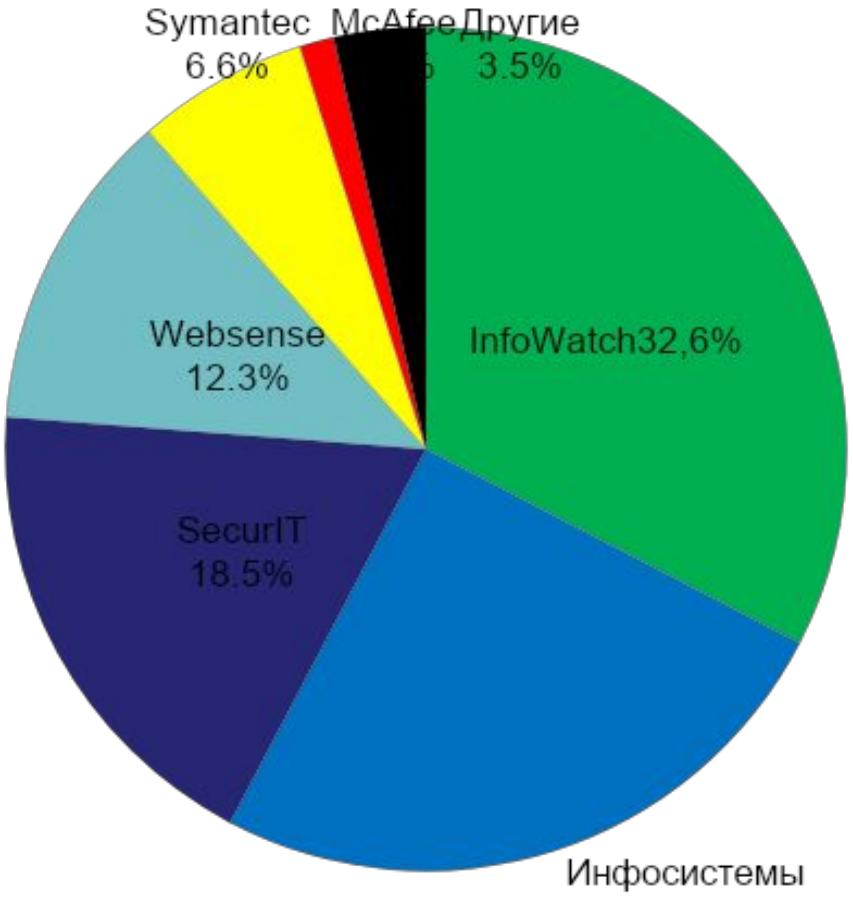


«Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2008-2010», Anti-Malware.ru, апрель 2010
«Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2009-2011», Anti-Malware.ru, июль 2011

Anti-Malware
Anti-Malicious Software

Основные игроки DLP-рынка в России

Доли рынка участников DLP-рынка в России в 2010 году

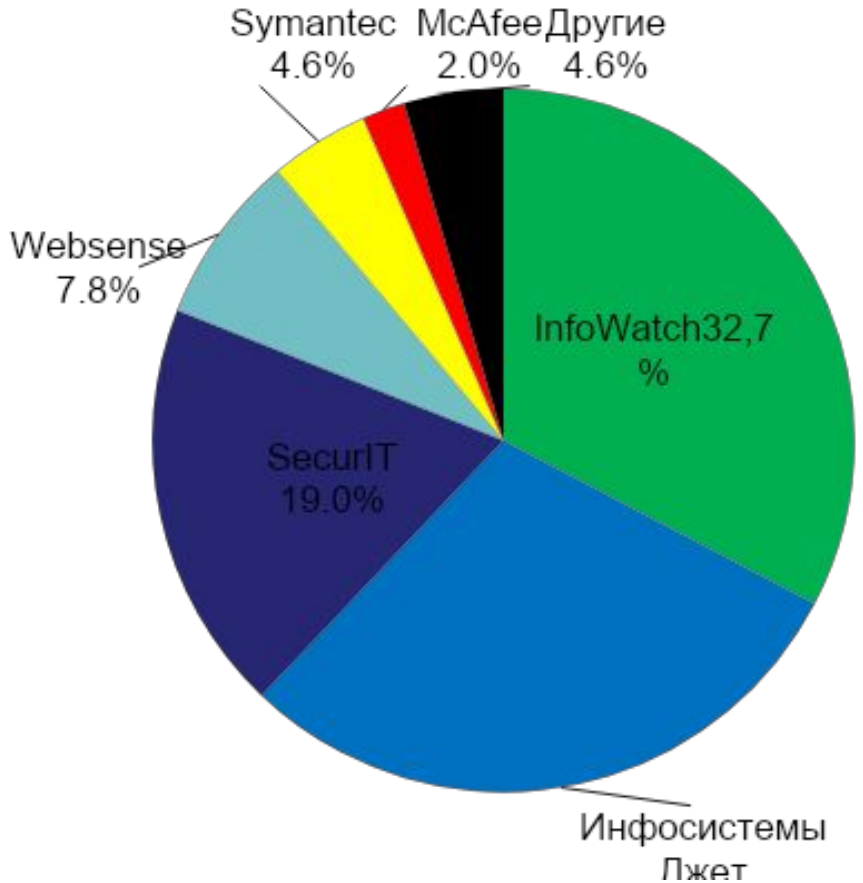


«Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2009-2011», Anti-Malware.ru, июль 2011

Anti-Malware
Anti-Malicious Software

Основные игроки DLP-рынка в России

Доли рынка участников DLP-рынка в России в 2009 году



«Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2008-2010», Anti-Malware.ru, апрель 2010

Anti-Malware
Anti-Malicious Software

Основные игроки DLP-рынка в России

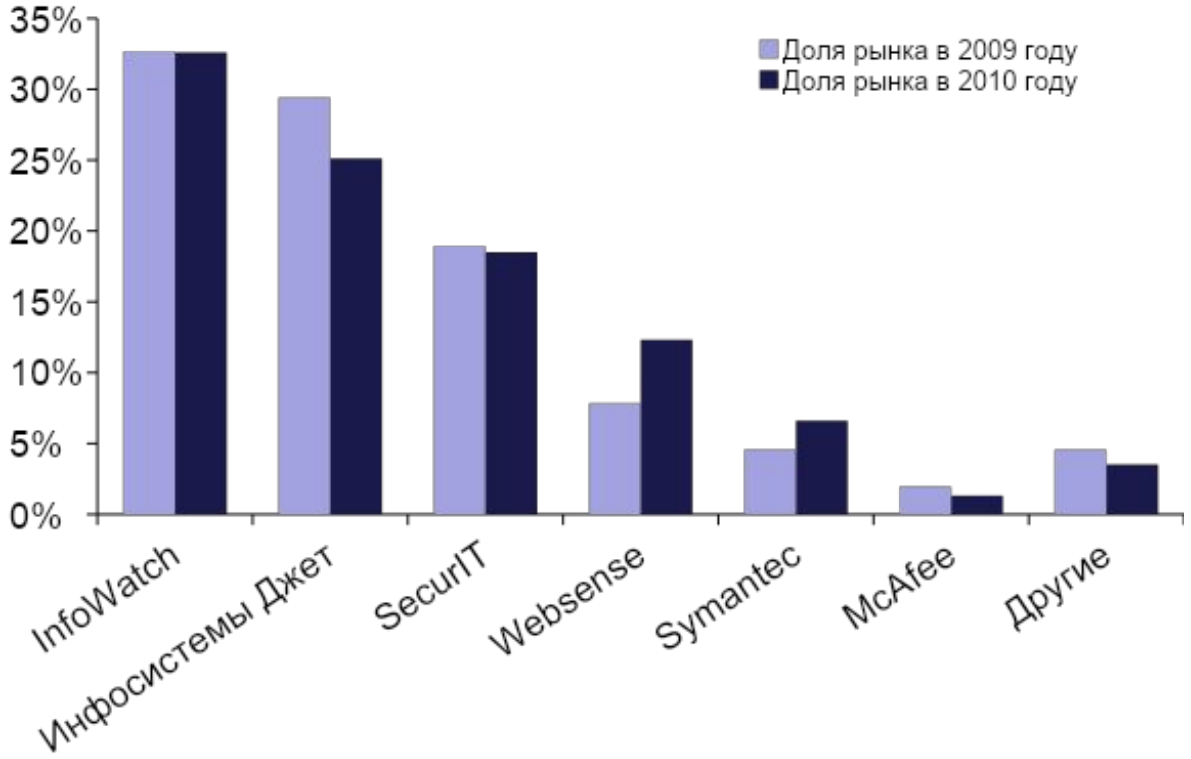
Производитель	Доля рынка 2009	Доля рынка 2010	Изм. доли рынка 2009-2010
InfoWatch	32,7%	32,6%	-0,1%
Инфосистемы Джет	29,4%	25,1%	-4,3%
SecurIT	19,0%	18,5%	-0,5 %
Websense	7,8%	12,3%	4,5%
Symantec	4,6%	6,6%	2,0%
McAfee	2,0%	1,3%	- 0,6%
Другие	4,6%	3,5%	-1,1%

«Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2009-2011», Anti-Malware.ru, июль 2011

Anti-Malware
Anti-Malicious Software

Основные игроки DLP-рынка в России

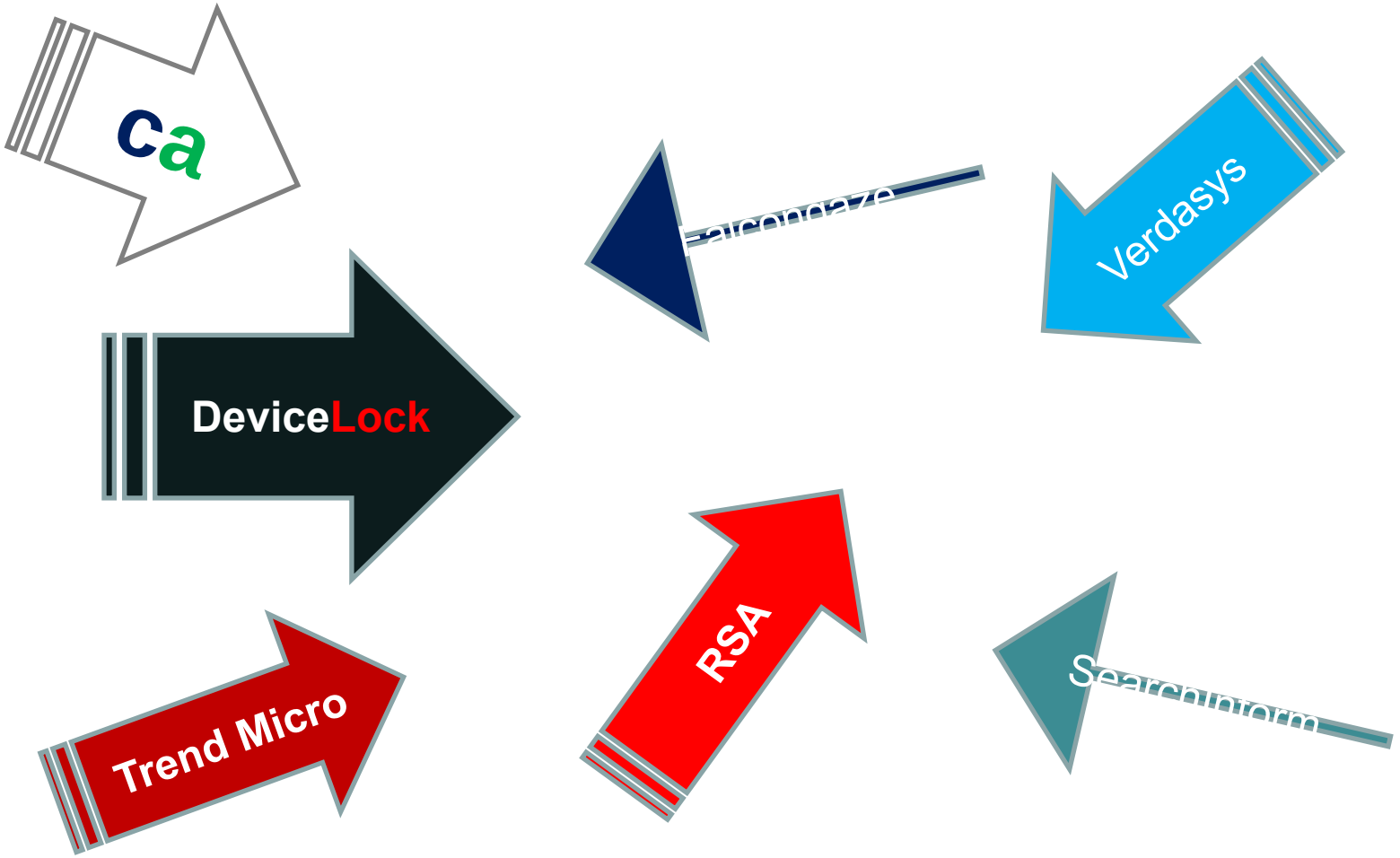
Изменение долей DLP-рынка в России в 2010 году



«Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2008-2010», Anti-Malware.ru, апрель 2010

Новые игроки DLP-рынка в России

Конкуренция на рынке постоянно возрастает



Anti-Malware
Anti-Malicious Software

Краткая картина рынка

- Объем российского рынка DLP пока остается небольшим и он постепенно «размывается».
- Уровень конкуренции на рынке растет быстрее, чем его объем.
- Тема утечек из российских компаний остается крайне закрытой. Внутренним угрозам не уделяется большего внимания.
- Против рынка работает привитый за годы некоторыми вендорами стереотип о сложности и дороговизне защиты от утечек.

Для выхода на массового потребителя нужны другие решения – проще, дешевле, удобнее.

Anti-Malware
Anti-Malicious Software

Рыночные тенденции

Что ожидать в ближайшем будущем?

Anti-Malware
Anti-Malicious Software

Технологические тренды

- Рост функциональности и зрелости продуктов
  - Контроль большего количества каналов
  - Совершенствование систем анализа событий
  - Упрощение внедрения и настройки
- Совершенствование технологий детектирования
  - Гибридные технологии
  - Самообучающиеся статистические технологии
- Автоматизация начальной настройки и обучения системы

Массовый потребитель ждет простого и эффективного решения по адекватной цене

Anti-Malware
Anti-Malicious Software

Расширение применимости

- Предотвращение нежелательных или криминальных действий сотрудников
- Контроль настроения внутри компании
- Контроль действий сотрудников на рабочем месте
- Расследование инцидентов

Функции современных DLP-решений выходят далеко за рамки первоначального определения этого рынка

Anti-Malware
Anti-Malicious Software

Интеграция

Интеграция со сторонними решениями:

- Системы шифрования данных
- Rights Management Services (RMS)
- Заимствование функций систем контроля деятельность персонала
- Интеграция функцией в состав комплексных шлюзовых продуктов (UTM)

Anti-Malware
Anti-Malicious Software

Новые вызовы

Как отвечать на глобальные вызовы IT-рынка?

- Контроль мобильных устройств
- Виртуализация и «облака»
- Утечки связанные не использование вредоносных программ
- Сквозные политики безопасности, автоматическое принятие решений (логические триггеры)

DLP-рынок пока не предлагает решений этих проблем, делаются только первые шаги

Спасибо за внимание!

Вопросы?

Илья Шабанов

Ilya.shabanov@anti-malware.ru

http://www.anti-malware.ru