WEBSENSE.

B SECURITY

Предотвращение информационных потерь

Вступление

- *Утечка информации-самый крупный источник потерь и ущерба (особенно авторизированных пользователей)*
- До сих пор самые большие ресурсы уделяются защите от внешних врагов
- Почему? Очень трудно защищаться от людей,с которыми вы встречаетесь в вашей столовой за обедом.

Знайте Вашего врага

- **Первый вид: не злоумышленный пользователь**
  - **Честная ошибка**
  - Работа на дому(The Boss needs it done Yesterday!)
  - Желание выслужиться или порадовать коллегу (he asks so nicely…)
  - Закадычный друг, товарищ, приятель
- Такие события происходят ежедневно почти в каждой организации

Второй вид:Проблематичные политики,методы и процессы

- Политики,допускающие двоякое толкование – никто по-настоящему не знает что можно,а что нет.
- конфликтные политики: запрещающие одному и требующие от другого.

YES! **NO!**

- Слишком запутанные политики, затрудняющие обеспечение выполнения.

- *ТРЕТИИ ВИД:* ***ЗЛОУМЫШЛЕННИКИ!!!!***

- МОТИВЫ:

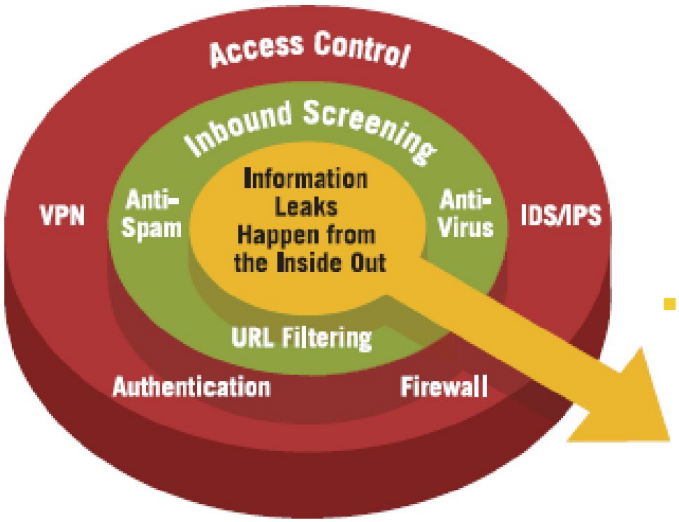
Эмоциональные: гнев,раздражение, месть

  - Жадность: Обман; мошенничество, деловой шпионаж,
  - коммерция,базированная на наличие внутренней информации.
  - Большинство из них могут быть не технарями,но могут причинить значителный ущерб

4 МИФА О ПОТЕРЕ ИНФОРМАЦИИ

Миф 1-ый

- Миф 1: Самая большая угроза утечки информации это – внешние атаки



- системы обнаружения, фаэрволы, виртуальная часть сети, управление цифровыми правами, безопасное управление контентом, на самом деле реальная угроза утечки информации находится внутри компаний.

WEBSENSE.

Реальность1

- По данным Michigan State University Identity Theft Lab, было установлено, что более чем 50% случаев кражи информации произошли внутри компании и были совершенны сотрудниками, которые имели законный доступ к конфиденциальной информации о клиентах.

- **Доверенный сотрудник представляет собой самый большой риск утечки информации**

Миф 2-ой

- Миф 2: Существующие меры предосторожности такие как: обучение персонала и установление внутренних правил безопасности эффективно предотвращают возможную утечку

  После серьезных нарушений защиты информации в американских банках ChoicePoint, Bank of America и Lexis/Nexis, Сенат США принял законопроект National Identity Theft Notification в соответствии, с которым компании должны извещать клиентов о краже их личных данных.
- Несмотря на законные и административные меры предосторожности количество случаев утечки информации стремительно растет, поскольку применить существующие правила на практике очень сложно.

Реальность 2

- **Компании полагаются на установленные правила, процесс документации и обучение персонала, но эти меры предосторожности не достаточно эффективны для усиления безопасности**
- **Компании должны приложить все усилия, чтобы сократить пробел между установленными корпоративными правилами и существующей реальностью путем установления контрольных точек внутри структуры для обнаружения возможной утечки.**
- **Реальность 2: Установленные правила, обучение персонала это правильные решения, но мало эффективные в мире электронной информации.**

Миф 3

- **Миф 3: Если нет официальных данных об утечки информации, то компании уверены, что эта проблема не существует вообще.**

- **Большинство компаний не имеют ни малейшего понятия о том, какие типы информации передаются по сети каждый день, и в каком количестве. Практически невозможно обнаружить отрывки или фрагменты документов после применения операций (вырезать и вставить) и внесения незначительных изменений в большие документы.**

- **Любое решение по предотвращению информационной утечки должно быть ненавязчивым для пользователей, но обеспечивать точное обнаружение возможных нарушений.**

- **Реальность 3: Предотвращение утечки информации требует точного и очевидно-ясного обнаружения передачи конфиденциальных данных для обеспечения полной осведомленности о потенциальной утечке.**

Миф 4-ый

- **Миф 4: Существующие решения электронной безопасности останавливают утечку информации, защищая от вирусов путем архивации сообщений.**

- **меры безопасности, такие как антивирусы и архивация не предотвращают основную причину утечки информации.**

- **программы-архиваторы регистрируют все передачи после их осуществления, но не принимают никаких мер по предотвращению несанкционированного раскрытия конфиденциальных данных в реальном времени.**
- **В среднем компания со штатом в 1 тысячу сотрудников посылает до 6 миллионов электронных сообщений за год, не имея понятия, что именно передается по сети. Если только 2% этих сообщений содержат конфиденциальную информацию, то до 120 тысяч сообщений подвергаются ежегодному риску.**

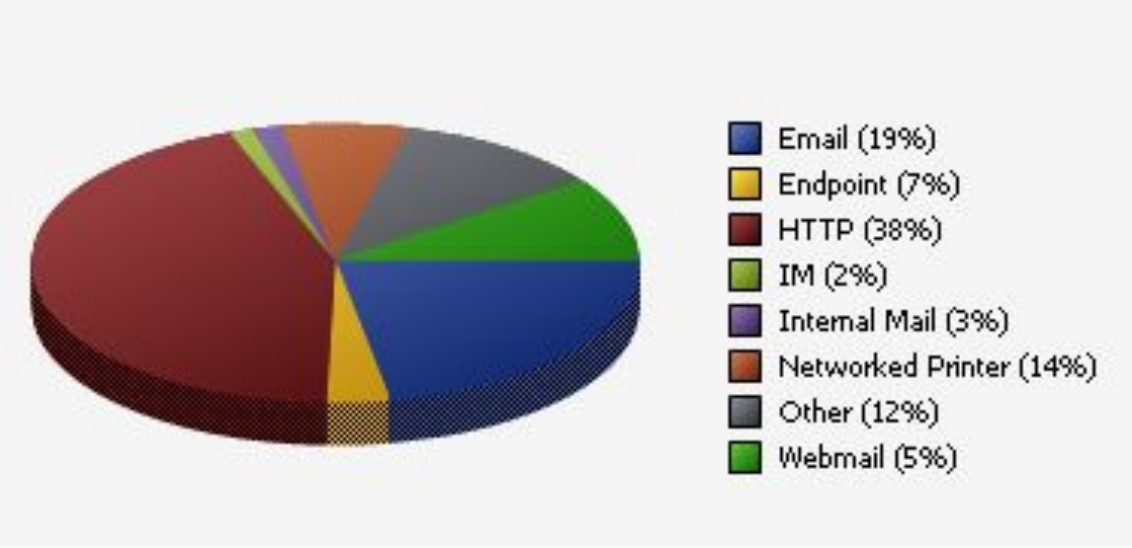
- **Реальность 4: Контроль над исходящим контентом и коммуникационными каналами обеспечивает обнаружение и остановку утечки конфиденциальной информации, дополняя решения безопасности электронной почты.**

Сложности связанные с защитой информации

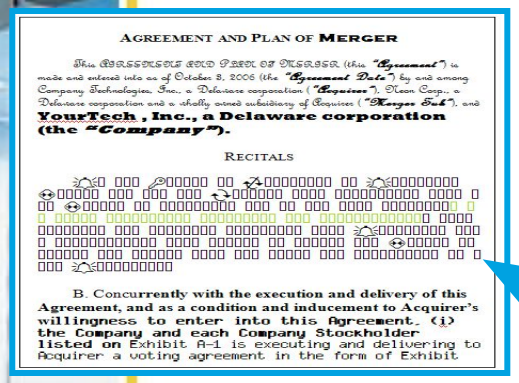
"85% опрошенных заявляют что после потерь данных клиентов или служащих за последние 24 месяца были нанесены значительные убытки"
– 2007 Ponemon Institute

"В среднем потери данных обходятся компаниям в $5 милионов" – Network World, 2006

- Большое количество источников:
- Отправка обычных сообщений, передача конфиденциальных данных по сетевым протоколам типа электронной почты (SMTP), через webmail (по HTTP или HTTPS, FTP), Instant Messaging а также через сетевую печать



Изменение структуры документа


AGREEMENT AND PLAN OF MERGER

This AGREEMENT AND PLAN OF MERGER (this "Agreement") is made and entered into as of October 3, 2006 (the "Agreement Date") by and among Company Technologies, Inc., a Delaware corporation ("Acquirer"), Neon Corp., a Delaware corporation and a wholly owned subsidiary of Acquirer ("Merger Sub"), and YourTech , Inc., a Delaware corporation (the "Company").

RECITALS

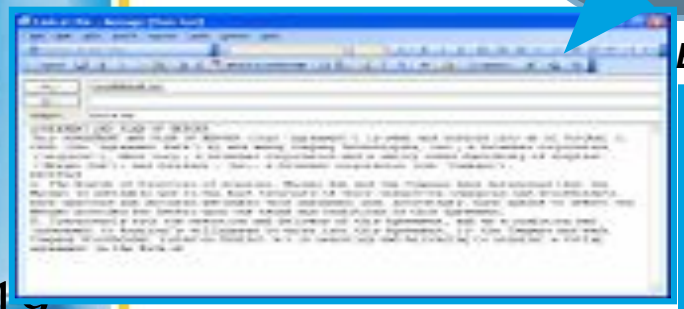
B. Concurrently with the execution and delivery of this Agreement, and as a condition and inducement to Acquirer's willingness to enter into this Agreement, (i) the Company and each Company Stockholder listed on Exhibit A-1 is executing and delivering to Acquirer a voting agreement in the form of Exhibit

Манипуляции с форматом файла

Манипуляции со структурой

Скрытые данные

Копировать& вставить



Наводнение данными

Вставленные файлы

AGREEMENT AND PLAN OF MERGER

This AGREEMENT AND PLAN OF MERGER (this *"Agreement"*) is made and entered into as of October 3, 2006 (the *"Agreement Date"*) by and among Company Technologies, Inc., a Delaware corporation (*"Acquirer"*), Neon Corp., a Delaware corporation and a wholly owned subsidiary of Acquirer (*"Merger Sub"*), and Outreach , Inc., a Delaware corporation (the *"Company"*).

RECITALS

A. The Boards of Directors of Acquirer, Merger Sub and the Company have determined that the Merger is advisable and in the best interests of their respective companies and stockholders, have approved and declared advisable this Agreement and, accordingly, have agreed to effect the Merger provided for herein upon the terms and conditions of this Agreement.

B. Concurrently with the execution and delivery of this Agreement, and as a condition and inducement to Acquirer's willingness to enter into this Agreement, (i) the Company and each Company Stockholder listed on Exhibit A-1 is executing and delivering to Acquirer a voting agreement in the form of

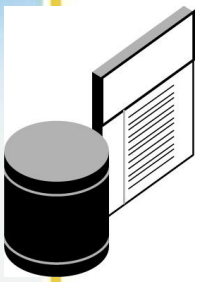
WEBSENSE.

Программа Оценка Рисков

Обзор программы

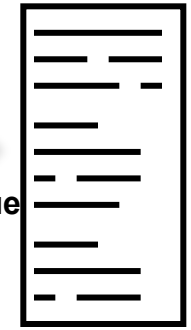
- 14- ти дневная Программа Оценки Риска включает установку устройств внутри организации для мониторинга информационного потока конфиденциальных данных
  - Данная программа позволяет определить проблемы и пробелы в существующей системе безопасности
- Не прерывает нормальный рабочей процесс и документооборот
- Простая установка
  - Отсутствие необходимости распределять корпоративные ресурсы и сетевое оборудование

Дактилоскопия



База данных или документ

Извлечение



Алгоритм преобразования

0101110011
0100110000
101100
100100
1000111
011
0110011
0111101

Одностороннее математическое преобразование

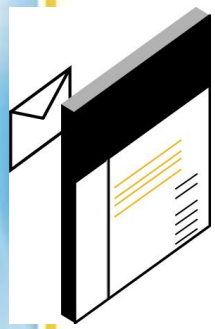
0xB6751
0xB61C1
0x37CB2
0x5BD41
0x190C1
0x93005
0x590A9
0xA0001

Хранилище кодов & Индексация

0x59A06
0x66A1A
0x1678A
0x461BD
0x6678A
0x4D181
0xB678A
0x9678A
0xB6751
0xB61C1
0x37CB2
0x5BD41
0x190C1
0x93005
0x590A9
0xA0001

Сопоставление в реальном времени

Детектирование



Исходящий контент (E-mail, Web, Fax, Принтера, etc.)

Извлечение

Алгоритм преобразования

0101110011
0100110000
101100
100100

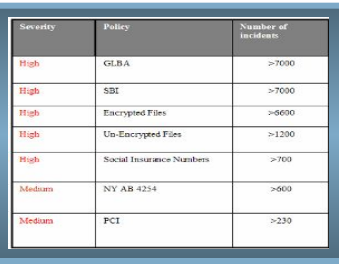
Одностороннее математическое преобразование

0x5BD41
0x190C1
0x93005

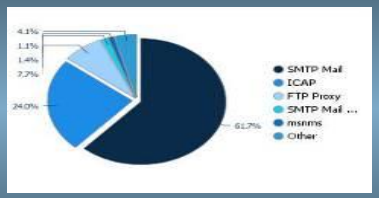
Создание дактилоскопии

Первых 4 шага:

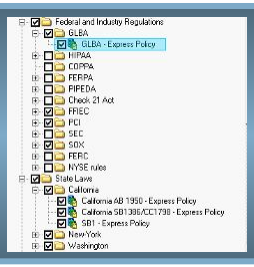
Шаг 1: Установить мониторинг сети
- Установка: 2 часа

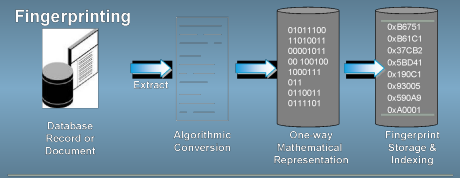


Severity	Policy	Number of incidents
High	GLBA	>7000
High	SBI	>7000
High	Encrypted Files	>6600
High	Un-Encrypted Files	>1200
High	Social Insurance Numbers	>700
Medium	NY AB 4254	>600
Medium	PCI	>230

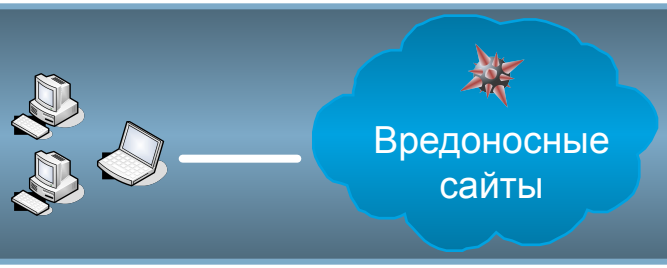


Шаг 2: Выберите политики которые отобразят все грани вашей секретной информации

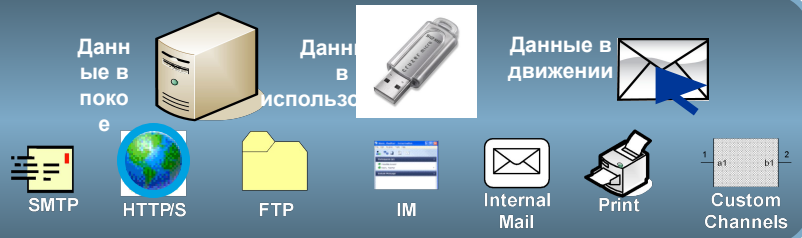




Шаг 3: Ждем неделю, следим за трафиком и определяем какая информация уходит и куда

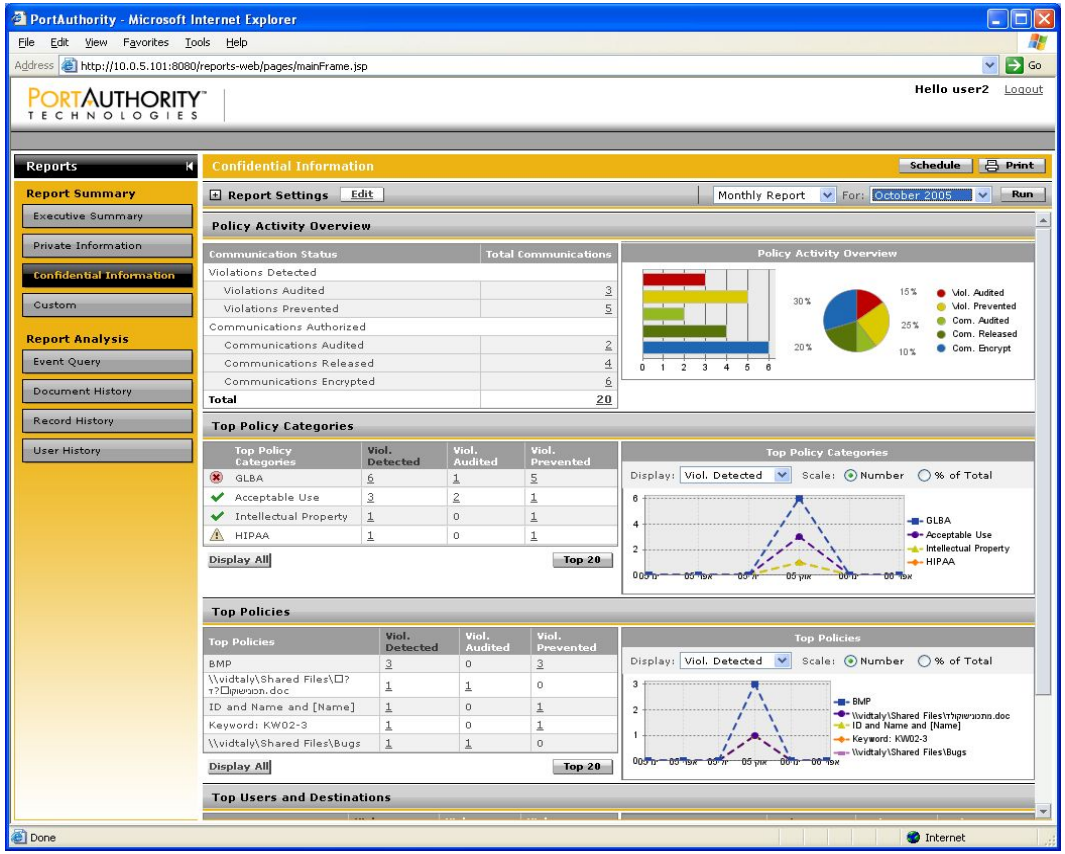


Шаг 4: Создание политик информационной безопасности



Потерянная личная и конфиденциальная информация

- Отдельная панель отчетов для конфиденциальной информации



WEBSENSE.

Неавторизированные получатели конфиденциальных данных

- Информация о получателях личной информации
  - Top получателей
  - Детальный обзор каждого события
  - Анализ каждого события
- Количество событий

Top Destinations	Viol. Detected	Viol. Audited	Viol. Prevented
[redacted]	9	1	8
[redacted]	2	1	1
[redacted]	1	1	0
[redacted]	1	1	0
[redacted]	1	1	0

Display All Top 20

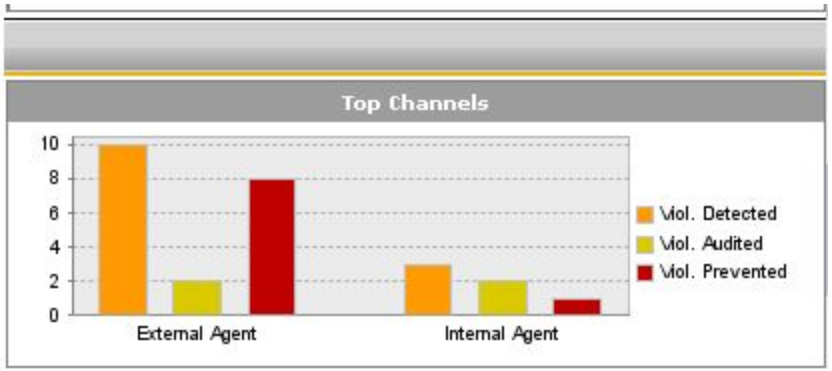
Процесс информационных потерь

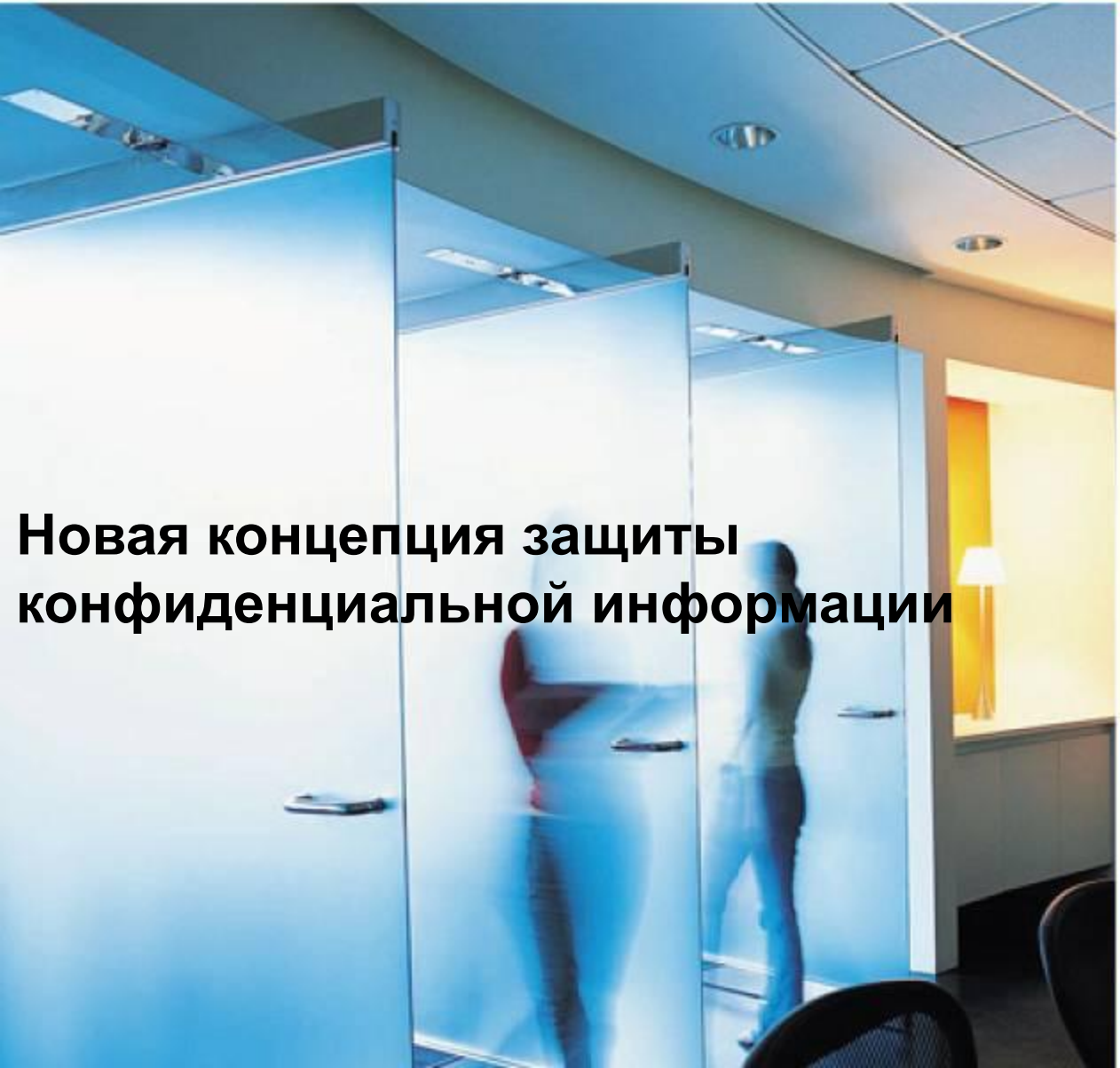
- Определение самых часто использованных каналов утечки информации
- .

Top Channels

Top Channels	Viol. Detected	Viol. Audited	Viol. Prevented
External Agent	10	2	8
Internal Agent	3	2	1

Display All | Top 20





Новая концепция защиты конфиденциальной информации

Комплексная защита

- Данных в движении: внешние и внутренние каналы передачи
- Данных в покое: конечные носители, ноутбуки и сервера
- Данных в использовании: копии на USB, CD-R, Wi-Fi, LPT, Floppy…
- Случайных и умышленных действий сотрудников
- Баз данных, систем управления документами, а также для более чем 370 форматов документов
- Интеграция с web security

Современный подход предотвращения информационными потерями

- Защита информации клиентов и компании
  - Структуированных и неструктуированных данных
- Точное выявление чувствительного контента
  - Данный контент уникален для каждой организации
- Обеспечение достоверного регуляторного соответствия

- Прозрачность пользователей
- Management and reporting
  - Предопределённые и индивидуальные политики и отчёты
  - Интреграция с деловыми рабочими процессами
- Легкая интеграция с существующими ИТ структурами

Итог

Современный подход к предотвращению информационных потерь.

Всесторонний контроль	**Защита данных в движении, в покое и данных в использовании**
Распознавание контента	**точная идентификация ваших данных**
Простое управление (3 клика)	**простота в управлении, в системе отчетов**
Интегрированная защита	**Мониторинг, предотвращение и контроль в одном устройстве**

Статистические данные об утечке конфиденциальной информации

Статистические данные

Данные совместного исследования 2004 года Computer Institute и ФБР (2004 CSI/FBI Computer Crime and Security Survey):

- **51% опрошенных не сообщили о случаях нарушения информационной безопасности правоохранительным органам, посчитав, что это может повредить имиджу в глазах общественности и негативно повлиять на стоимость акций;**

WEBSENSE.

Информационная потеря: Как это происходит?

80-90% информационных потерь происходят непреднамеренно и случайно

Gartner

утечка через е-майл -риск фактор номер 1

5% е-майлов содержит конфиденциальную информацию

* Source: PortAuthority Deployments

Статистические данные

68 % организаций теряют секретные данные через доверенных сотрудников.

2007 Обзор компьютерных преступлений ФБР

Средняя стоимость потери данных компаний $5 миллионов.

Network World 2007

- *ежегодный объем деловой переписки увеличится на 25% - 30% до 2009 года.*

Статистические данные

Данные ежегодного исследования проблем ИТ-безопасности (2005 Ernst & Young Global Information Security Survey):

- *В среднем от внутреннего вмешательства потери компании составляют 2.7 миллиона долларов, в то время как потери от внешнего вмешательства оцениваются в 57 тысяч долларов;*

- *Только 1 из 5 сотрудников, зная о кражах информации другими сотрудниками, сообщает об этом ИТ персоналу;*

Защитите свои ДАННЫЕ

Защитите своих КЛИЕНТОВ

Защитите свой БИЗНЕС