

Websense Data Security

защита от утечки
конфиденциальной информации

Ванерке Роман

*Руководитель отдела
технических решений*

ЗАО «ДиалогНаука»



- Базовые понятия
- Проблематика утечек данных
- Основные этапы проекта
- Архитектура и возможности Websense Data Security
- Пример использования Websense Data Security
- Выводы



- ЗАО «ДиалогНаука» создано 31 января 1992 года. Учредители - СП «Диалог» и Вычислительный центр РАН.
- Первыми и самыми известными отечественными продуктами, поставляемыми компанией, были Aidstest, ADinf, Sheriff, Doctor Web и DSAV.
- С 2004 года по настоящее время «ДиалогНаука» - системный интегратор, консультант и поставщик комплексных решений в сфере защиты информации.



- **Информация ограниченного доступа (ИОД)** - информация представляющая ценность для ее владельца, доступ к которой ограничивается на законном основании
- **Инсайдер (внутренний злоумышленник)** – сотрудник Компании, член какой-либо группы людей, имеющей доступ к ИОД, недоступной широкой публике. Может действовать изнутри Компании
- **Внешний злоумышленник (хакерство, вредоносный код)** – постороннее лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Действует извне, за периметром Компании.



Что является ценным для Компании?



Клиентская база (физические и юридические лица)



Схемы работы

Условия работы



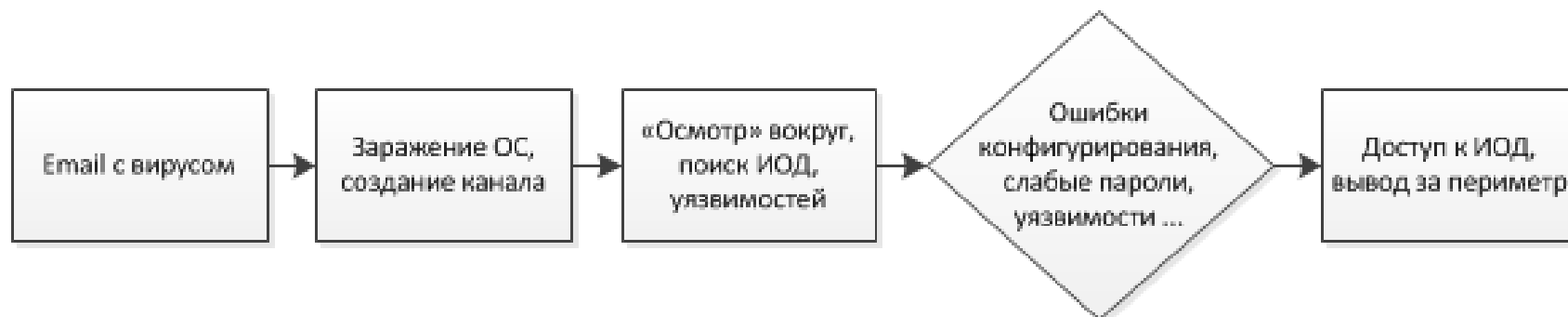
Стратегические планы, новые продукты, изменения, маркетинговые акции



Персональные данные, HR и прочее



- **Внешний злоумышленник** – кража информации с целью перепродажи (хакеры, конкуренты)
 - Хакерство (использование различных уязвимостей), вредоносный код
 - Web, Email
- **Внутренний злоумышленник (инсайдер)** – выгодно продать, открыть свой бизнес, попросить повышения
 - Прямой доступ к данным
 - Web, Email, USB, IM (Skype, ICQ)



Основные этапы атаки



- Прямые, финансовые убытки (уход клиентов к конкурентам, потеря контрактов и т.д.)
- Потеря лояльности клиентов, партнеров, репутационный ущерб
- Потеря производительности (нарушение бизнес-процессов в Компании)
- Преследование по закону (штрафы, судебные разбирательства)



- По западной статистике стоимость утечки одной записи ~ **200\$** (прямые убытки, затраты на решение проблемы, оповещение, судебные тяжбы и т.п.)
- Оценить репутационные риски крайне трудно
 - По разным оценкам от 5% годовой выручки до потери бизнеса.
- Законопроект № 12389-6 «О внесении изменений в КоАП РФ».
 - Ст. 13.11. Нарушение установленного законодательством РФ порядка обработки ПДн:
 - Для должностных лиц – от 30 000 до 50 000 руб.
 - Для юридических лиц – от **200 000 до 500 000 руб.**
 - Повторное нарушение:
 - Для должностных лиц – 50 000 руб. или дисквалификация до года
 - Для юридических лиц – от **500 000 до 1 000 000 руб.**



- Минимизация рисков
- Соответствие требованиям (Compliance)
 - ФЗ о ПДн
 - Соглашения с контрагентами
 - PCI DSS
 - ISO 27000
- Повышение эффективности бизнеса (увеличение выручки)
- Уменьшение стоимости продуктов и услуг



Основные этапы проекта построения комплексной системы защиты от утечек

- Идентификация и классификация ИОД, определение собственников информации, бизнес-процессы
- Приоритезация ИОД по степени риска, требованиям аудита и регуляторов
- Определение политик хранения, обработки и передачи, как часть общего подхода к защите ИОД
- Выбор и развертывание системы защиты от утечек
- Разработка документации, обучение сотрудников
- Превентивное автоматическое реагирование
- Регулярный контроль и оценка эффективности







- Использование современных решений для выявления утечек ИОД
 - Анализатор информации на основе многих алгоритмов детектирования и измерения степени схожести
 - Охват всех основных каналов бизнес-коммуникаций
 - Автоматизированная система учета и обработки инцидентов
 - Отчеты для задач управления рисками на предприятии
- Обеспечение антивирусной защиты, реализация системы управления уязвимостями, регулярный анализ правил МЭ, построение системы управления доступ
- Создание системы мониторинга информационной безопасности



- Обучение администраторов безопасности, ответственных за установку и обслуживание средств защиты
- Обучение пользователей, работающих со средствами защиты
- Аттестация специалистов по результатам программы обучения
- Укомплектование подразделений предприятия сотрудниками, ответственными за выполнение работ по защите от угроз безопасности



- **ROI** – плохо применима для оценки систем ИБ
- **ROSI** – оценка затрат потенциального ущерба (утечки) к стоимости владения системой (ТСО)
 - Необходима оценка рисков, чтобы понимать возможный ущерб при утечке тех или иных данных
- **ALE** – учитывается стоимость одной утечки и количество утечек в год
 - Необходимо знать стоимость одного инцидента
 - Необходимо иметь статистику по инцидентам в Компании



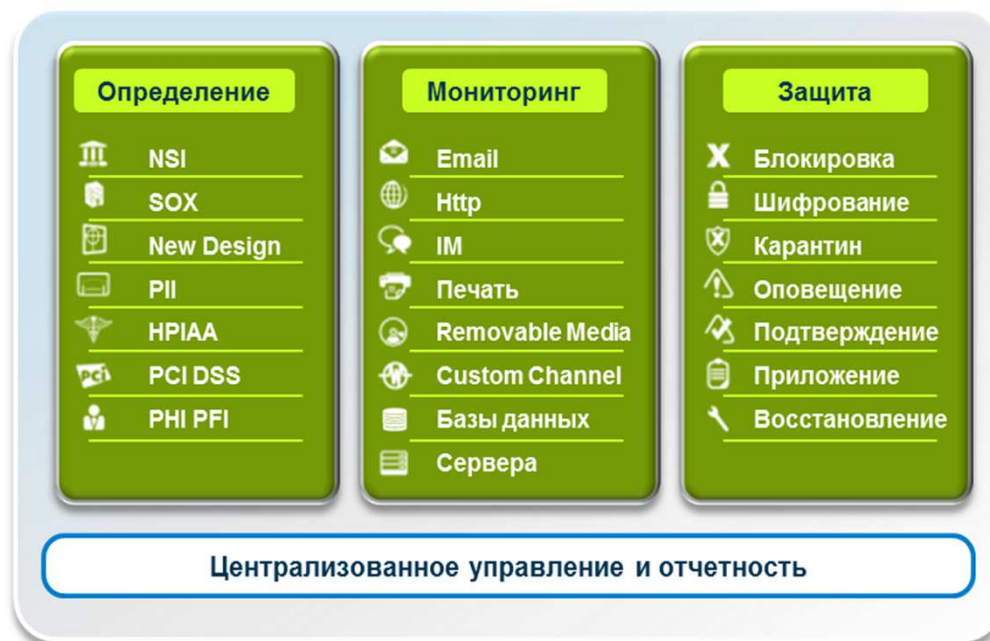
Сравнение Websense с InfoWatch

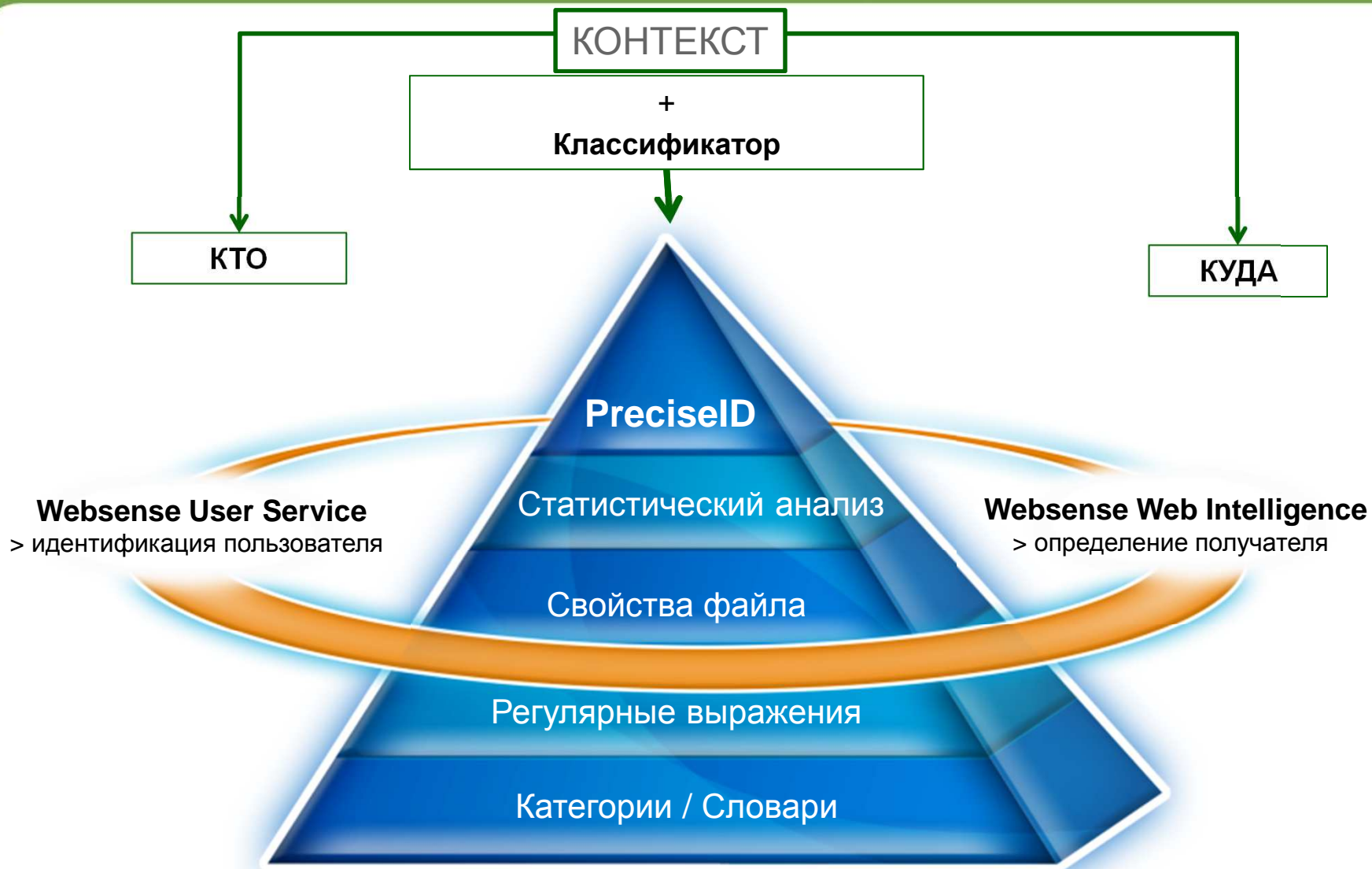
Websense Data Security Suite	InfoWatch Traffic Monitor Enterprise
Технология цифровых отпечатков PreciseID™ (международный патент), 27+ алгоритмов опознавания конфиденциальной информации	Лингвистический анализатор локальной разработки; технология цифровых отпечатков (выпущена в конце 2009 года)
Обнаружение ИОД из СУБД методами цифровых отпечатков	отсутствует
SMTP, HTTP/HTTPS, FTP, ICQ, Skype, сетевая и локальная печать, съемные носители	SMTP, HTTP/HTTPS, ICQ, сетевая и локальная печать, съемные носители
Аудит и обнаружение ИОД в сети и на рабочих станциях	отсутствует
Достаточно использования СУБД MS SQL Express	Использование промышленной СУБД Oracle 11g
Средняя трудоемкость внедрения	Высокая трудоемкость внедрения



Лидирующая на рынке технология DLP для обнаружения, мониторинга и защиты конфиденциальных данных

- **Единые политики**
 - Предлагает унифицированный механизм создания политик
 - Управление всеми аспектами политики Data Loss Prevention
 - Мощные возможности мониторинга по отслеживанию всех изменений данных (хранимых и при перемещении)
- **Низкая ТСО и сложность**
 - Модульная архитектура позволяет наиболее гибко соответствовать требованиям покупателя
 - Простое развертывание и меньшее число серверов





Websense Data Security

Технологии идентификации ИОД





Готовые
политики



Цифровые
отпечатки

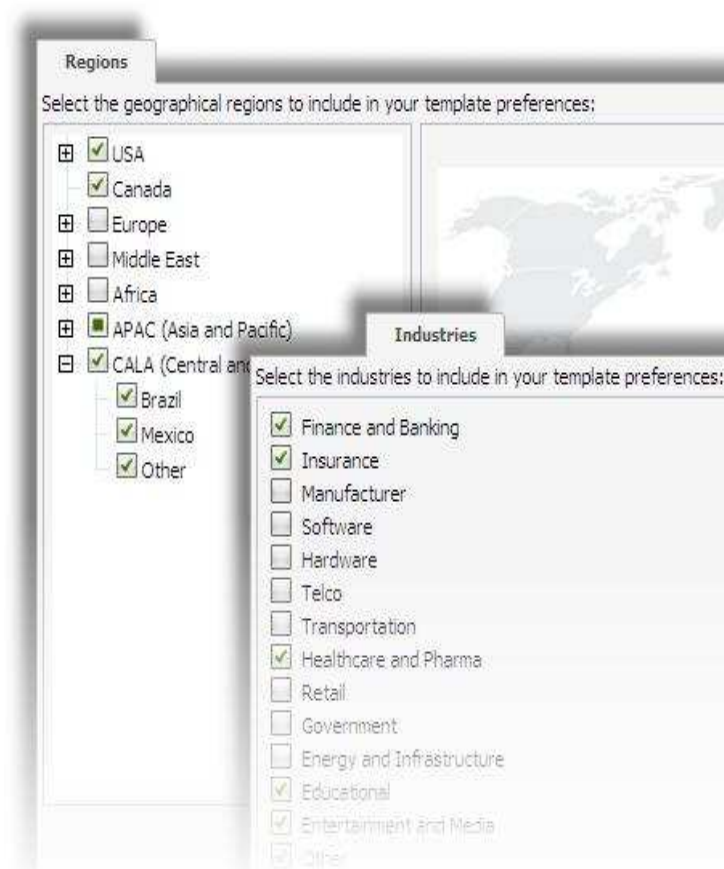


Machine
Learning





- Различные классификаторы
 - Регулярные выражения, ключевые слова, словари
- Более 1100 готовых политик «из коробки», в том числе для РФ
- Удобный мастер настройки политик
- Определяет типы данных например: ПДн, РСІ





- Цифровые отпечатки – все режиме для чтения:
 - Баз данных
 - Сетевых каталогов
 - SharePoint
 - SalesForce.com
- Подключение к базе данных через ODBC
 - Снятие цифровых отпечатков непосредственно с БД
 - Данные не покидают БД
 - Инкрементальные обновления базы отпечатков при росте исходной базы





Высокая устойчивость к изменению

Данные внутри защищённого файла

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

AGREEMENT AND PLAN OF MERGER

(This is a small, illegible version of the document shown in the main text box.)

Изменение формата

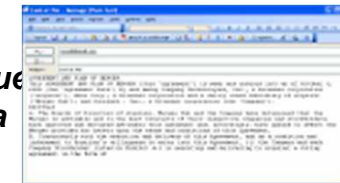
Изменение типа файла



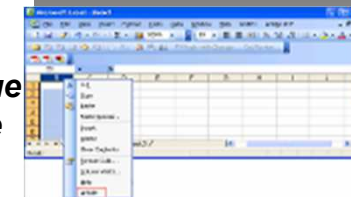
Зашумление (flooding)



Копирование и вставка



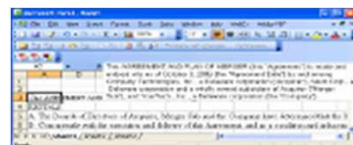
Скрытые данные



Встраиваемые файлы

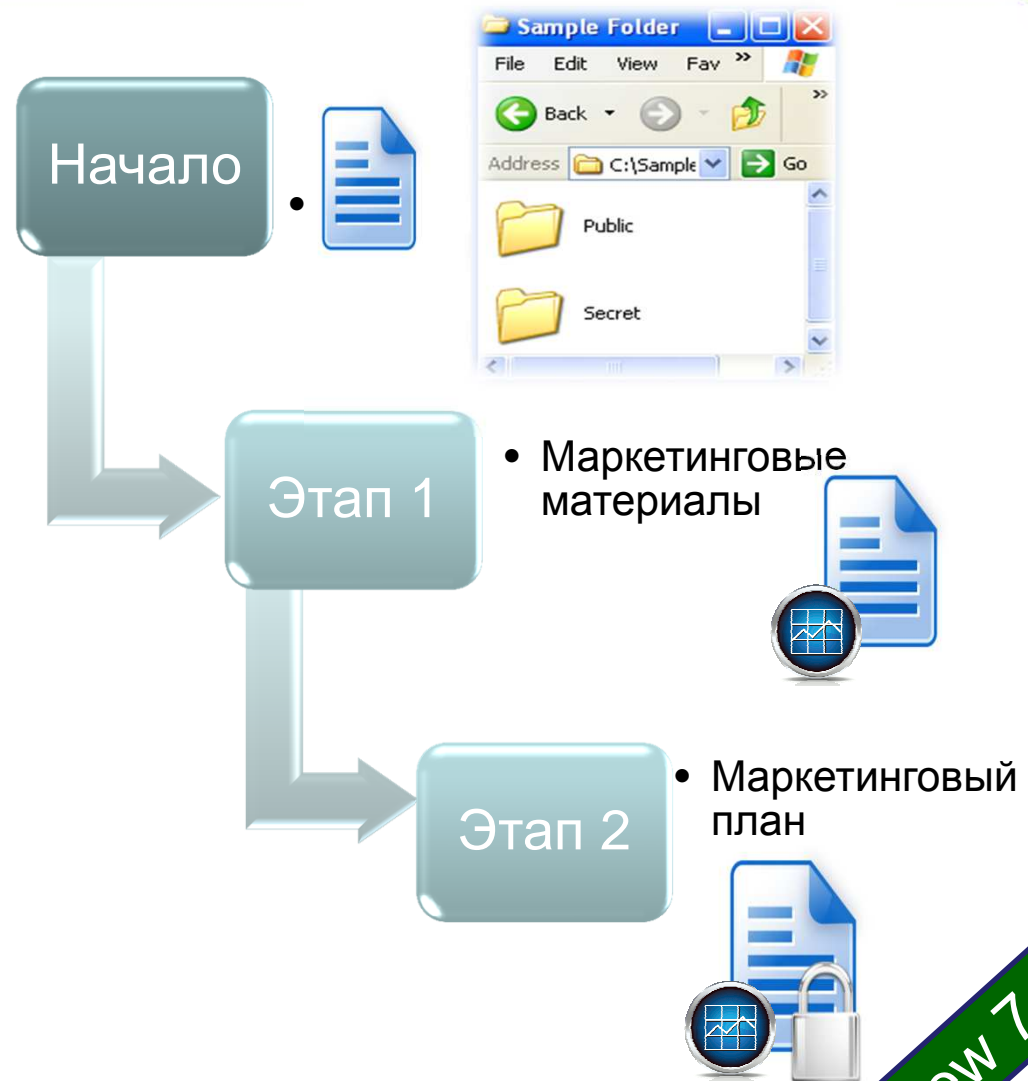


Изменение структуры





- **Удобный**
 - Необходимо только указать каталог с документами
- **Масштабируемость**
- **Высокая точность**
 - Двухэтапный подход
 - Этап 1 – определение типа данных
 - Этап 2 – определение, является ли конфиденциальным



New 7.7

- Используется механизмы оптического распознавания
- Определение КИ в картинках
 - Screen captures
 - Scanned checks
 - Scanned receipts
 - Fax pages
 - и т.п.
- Доступен для Web, Email и хранилищ

The screenshot displays the TRITON Unified Security Center interface. On the left, a sidebar lists system modules such as Load Balancing, DSS Server on left, Endpoint Serv, Policy Engine, Forensics Rep, Primary Finger, Crawler lafaaf, DSS Server on ep, Endpoint Serv, Policy Engine, and SMTP Agent. The main area shows a scanned document with handwritten text and a table. A red box highlights a specific area of the document with the text "This is where the mouse was last located". Another red box highlights a different area with the text "Don't know where this comes from". Below the document, there is a scanned check from Towne Bank for \$101.00, dated 1-18-07. The check includes the name THOMAS OR MARY ANDERSON and the address 2000 PLEASANT RD ANYWHERE, USA 12345. The check number is 101 and the amount is \$101.00. The check is signed and has a MICR line at the bottom: 4305 140894901 234 56 7890 010.

New 7.7



Идентификация «медленных» утечек

- Идентификация утечек за промежутки времени

❖ Within 2 Hours

From: John Doe Sent: 3:01 PM
To: Joe Smith
Cc:
Subject: Customer Information

Joe,

Here is a customer information:



From: John Doe Sent: 3:01 PM
To: Joe Smith
Cc:
Subject: ❖ Customer Information

From: John Doe Sent: 3:14 PM
To: Joe Smith
Cc:

From: John Doe Sent: 3:17 PM
To: Joe Smith
Cc:

From: John Doe Sent: 4:45 PM
To: Joe Smith
Cc:
Subject: Customer Information

Joe,

From: John Doe Sent: 4:50 PM
To: Joe Smith
Cc:
Subject: Re: Customer Information

Joe,

Here is another customer information:
Jane Brown CCN: 1234-2345-3456-4567

New 7.7



- Распознавание типов файлов – около 400 форматов
 - Например, возможна блокировка зашифрованных файлов, документов САПР и файлов баз данных
 - Работа со свойствами файлов (имя, тип, размер)

Сетевая DLP

*Передача
(Data-in-Motion)*





- Смотрим – Не трогаем
- Видим входящий и исходящий незашифрованный трафик

SPAN-порт



- Смотрим и трогаем
- Прокси для Web & FTP
- MTA для Email
- ActiveSync для Mobile

In-Line



- Сетевые принтеры

Агент

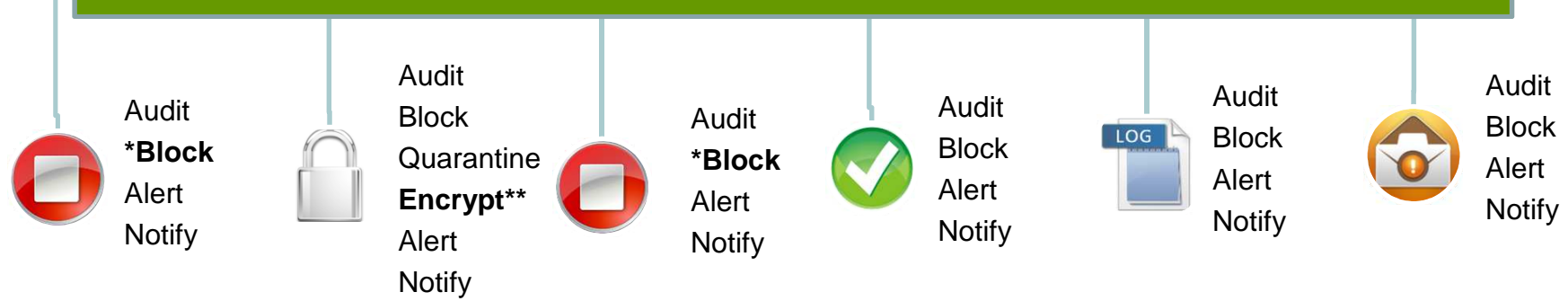




Сетевая DLP



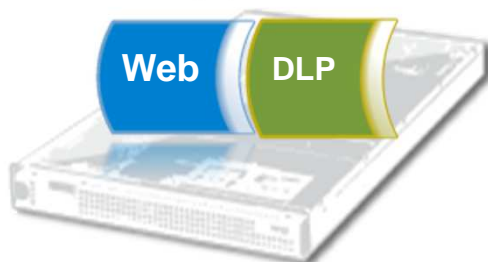
РЕАКЦИЯ В ЗАВИСИМОСТИ ОТ КАНАЛА



* Требуется прокси
** Требуется шлюз шифрования



- Родная интеграция с промышленным DLP для решений Web и Email
- Работает на ПАК Websense V-Series
- Не требуется сторонних решений прокси и шлюзов шифрования



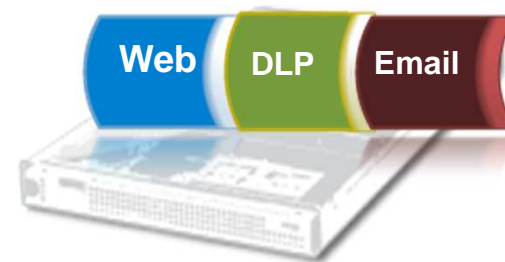
Web Security Gateway

- Промышленный DLP для Web
- Инспекция SSL
- Расширенная защита от веб-угроз



Email Security Gateway

- Промышленный DLP для Email
- Исходящее шифрование Email
- Anti-virus / Anti-spam
- URL Sandboxing



TRITON Security Gateway

- Интегрированная Web & Email DLP
- Инспекция SSL
- Исходящее шифрование Email
- Расширенная защита от веб-угроз



Competitor Alerts

Data: HIPAA
Source: 10.14.222.21
Channel: Web
Destination: 92.10.219.62

Websense Alerts

Data: HIPAA & PII, Customer Database
Source: Tina Doh x1234
tinad@acmehospital.com
Title: Associate
Dept. Accounting
Manager: Mike Brown
Channel: Web
Destination: gmail.com
Type: Personal webmail site
Location: Mountain View, CA

Интеграция Websense Web и Data Security.

Разрешение IP источника и назначения в реальном времени.

Dramatically Reduces Operational Bottlenecks:

Manual look up of source and destination IP address

Approx. 10 minutes each

Hundreds to thousands web incidents a day

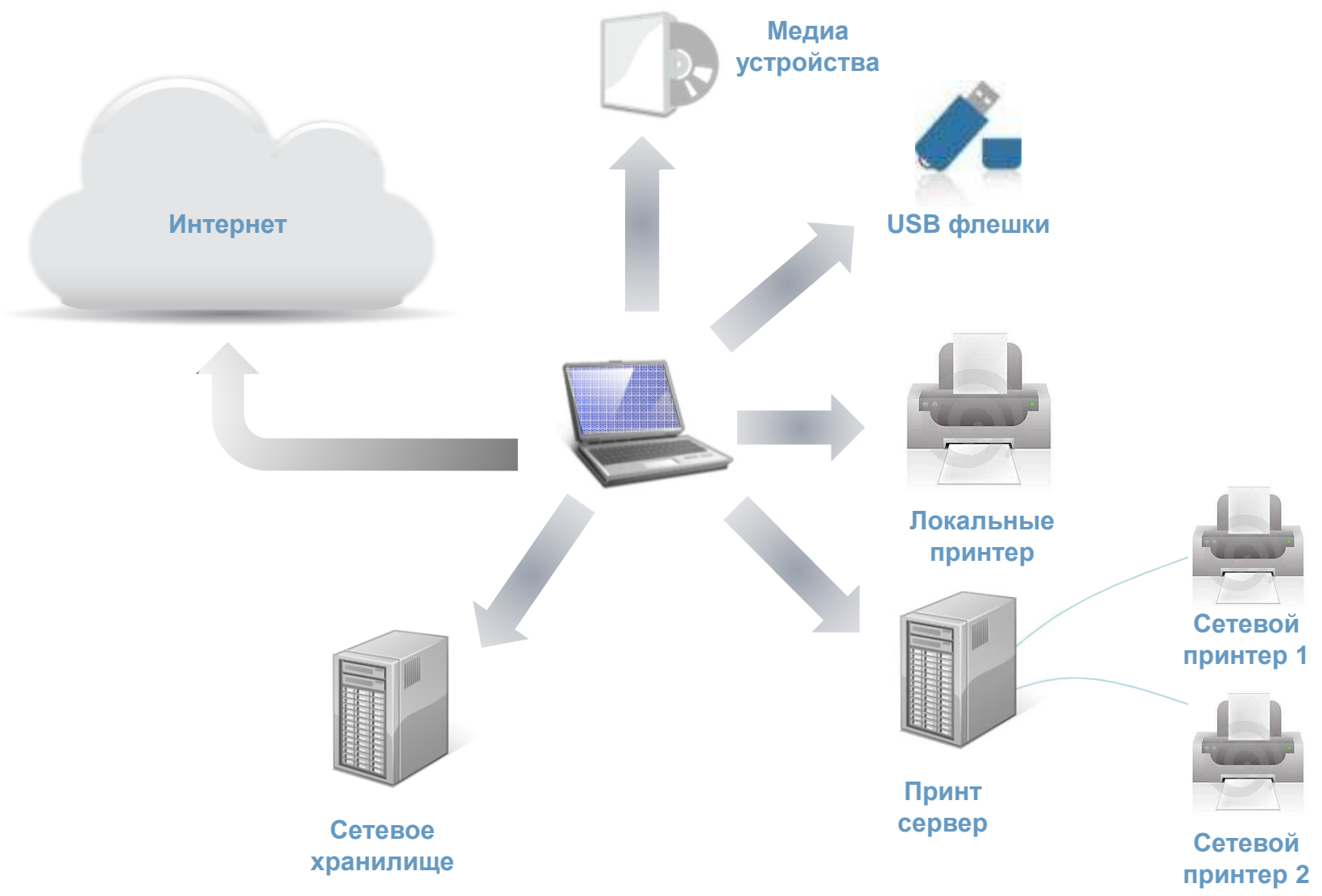
Endpoint DLP

*Использование
(Data-in-Use)*





Каналы утечки на уровне АРМ





Endpoint DLP



Приложения



Съемные устройства



Хранилища

ВАРИАНТЫ РЕАГИРОВАНИЯ



- Permit
- Confirm**
- Block
- Email
- Quarantine
- Alert
- Notify



- Permit
- Confirm
- Block
- Encrypt to USB**
- Alert
- Notify



- Alert/Log
- Scripts**
- Encrypt
- Tombstone
- Quarantine
- EDRM



- **Контроль приложений:**

- Copy/Cut/Paste
- Файловый доступ
- Print Screens



- Применяется к конкретным группам приложений

Resources > Endpoint Application Groups

New... Delete

Create or view a list of application groups you want to monitor on the endpoint, aside from those on the default Websense list.

Name	Applications	Description	Endpoint Operations
Browsers	Firefox ,IE ,Chrome ,Safari ,Opera	Software that interprets HTTP content...	Cut/Copy ,Paste ,File Access
CD Burners	Alcohol 120% ,CD-Mate ,Acoustica MP3 ...	Software that enables to burn files o...	File Access
Email	Eudora ,Microsoft Office Outlook ,Peg...	Software that enables the sending and...	Paste ,File Access
Encryption Software	Windows Privacy Tray ,File Encryption...	Software that is used for encryption ...	File Access
FTP	Flash FXP 3.6 build 1240 ,Leech FTP ,...	Software that enables the sending and...	File Access
IM	AIM ,MSN messenger (live) ,Windows Me...	Software that enables the sending and...	Paste ,File Access
Office Applications	Notepad ,Adobe Reader ,Wordpad ,OpenO...	Software for data reading and writing	Cut/Copy
Online medical (online)	AllegianceMD ,INGENIX ,ECLIPSYS ,eCi...	Online medical records	Cut/Copy ,Download
P2P	eMule ,BitComet ,Ares ,Azureus ,KaZaa...	Software that enables file search and...	Paste ,File Access
Packaging Software	WinRAR ,7-Zip File Manager ,WinZip	Software that is used for packaging a...	File Access
Portable Devices	Fsquirt ,BTStackServer ,WCESMgr ,Irfp	Software that is used to communicate ...	File Access
SaaS (online)	HostAnalytics ,Intacct ,CRM.com ,NetS...	Software as a service applications	Cut/Copy ,Download



• **Вариант 1: Требуется DLP Endpoint**

- Родное шифрование с помощью DLP Endpoint
- Не требуется пароль
- Для дешифрования требуется DLP Endpoint



• **Вариант 2: Портативное шифрование**

- Родное шифрование с помощью DLP Endpoint
- Утилита для дешифрования копируется на USB
- Пользователь задает пароль
- Дешифрование с внешних систем с использованием утилиты дешифрования

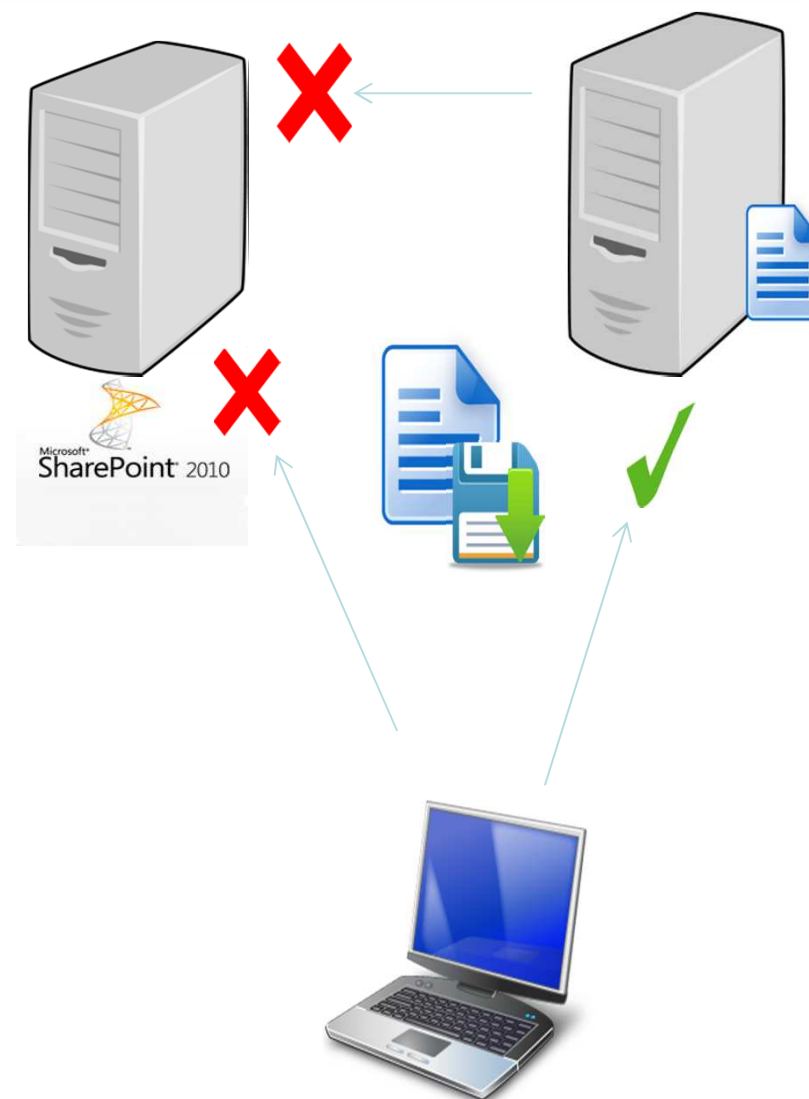


Пользователь задает пароль





- Контроль мест хранения конфиденциальных данных
- Преимущества:
 - Управление распространением данных (контроль границ ИСПДн, например)
 - Минимизация неавторизованного доступа
 - Улучшенное управление данными





- **Функции защиты агента:**
 - Служба не может быть остановлена в оснастке “Services”
 - Процесс будет перезапущен, если был принудительно завершен
- **Отключение защиты для задач обслуживания**
 - Использование административного пароля





**Клиенты
Endpoint**

Windows 7 32 & 64 bit
Windows Vista 32 & 64 bit
Windows XP 32 & 64 bit
Windows Server 2008 32 & 64 bit
Windows Server 2003 32 & 64 bit
MAC OSX 10.6 – Snow Leopard – 32 & 64 bit
MAC OSX 10.7 – Lion – 32 & 64 bit
Linux - USB and Discovery



v. 7.7.2 (Август 2012)

- Removable media write
- CD write
- Discovery
- File Access
- Endpoint LAN
- Endpoint Email
- Trusted Applications
- Anti-Tampering

Websense DLP

*Хранение
(Data-at-Rest)*





Безагентский



- Discovery в сети
- Проведение через LAN/WAN
- Управление с помощью Расписания

Агент



- Локальный Discovery
- Самое быстрое Discovery
- Управляется через Расписание, утилизацию CPU, электропитание

Гибридный



- Лучшее вариант
- Использование любой комбинации



- Гибкая настройка расписания задач Discovery
 - Единожды или Повторяющиеся в определенные дни/часы

Click to select the hour(s) to perform the scan. Re-click to clear selection.
 Click a day to select the entire day. Click an hour to select that hour for all days.

	12 am	1 am	2 am	3 am	4 am	5 am	6 am	7 am	8 am	9 am	10 am	11 am	12 pm	1 pm	2 pm	3 pm	4 pm	5 pm	6 pm	7 pm	8 pm	9 pm	10 pm	11 pm	12 am
All	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
Mon	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Tue	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Wed	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Thu	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Fri	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Sat	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Sun	■	■	■	■	■	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

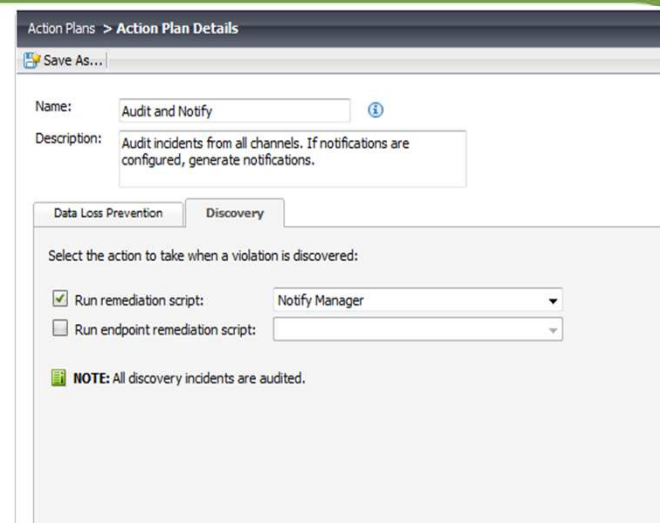
Legend: ☐ Do not scan ■ Scan

Note: If you select more hours than the scan takes, this scan does not repeat. It restarts next day.



Расширенные возможности реакции на инцидент

- Remediation Scripts
 - Доступно несколько ГОТОВЫХ скриптов
 - Настраиваемые
- Доступные действия



Move/Quarantine



Encrypt**



Classification Tag
(Microsoft FCI)



Apply EDRM**



Purge/Delete



** Требуется стороннее решение

Websense DLP

Управление и отчетность





- Единая Web-консоль для управления всеми решениями Websense
- Ролевое управление и отчетность
- Управлением всеми компонентами DLP
 - Каналы TruWeb и TruEmail DLP
 - Enterprise Suite
 - Настройка отдельных модулей Data Security
 - Data Security Gateway
 - Data Endpoint
 - Data Discovery

The screenshot shows the Websense TRITON Unified Security Center interface. At the top, there are tabs for 'Web Security', 'Data Security' (which is highlighted in yellow), and 'Email Security'. Below these are 'Main' and 'Settings' buttons. The main content area is divided into several sections:

- Incidents & Reports:** Includes links for 'Data Usage' and 'Data Discovery'.
- Policy Management:** Includes links for 'Data Usage Policies', 'Data Discovery Policies', 'Data Discovery Tasks', 'Content Classifiers', and 'Resources'.
- Status & Logs:** Includes links for 'System Health', 'Endpoint Status', 'Traffic Log', 'System Log', and 'Audit Log'.

On the right side, there is a 'Today' summary section with a 'System Alert Summary' showing several status checks with green checkmarks:

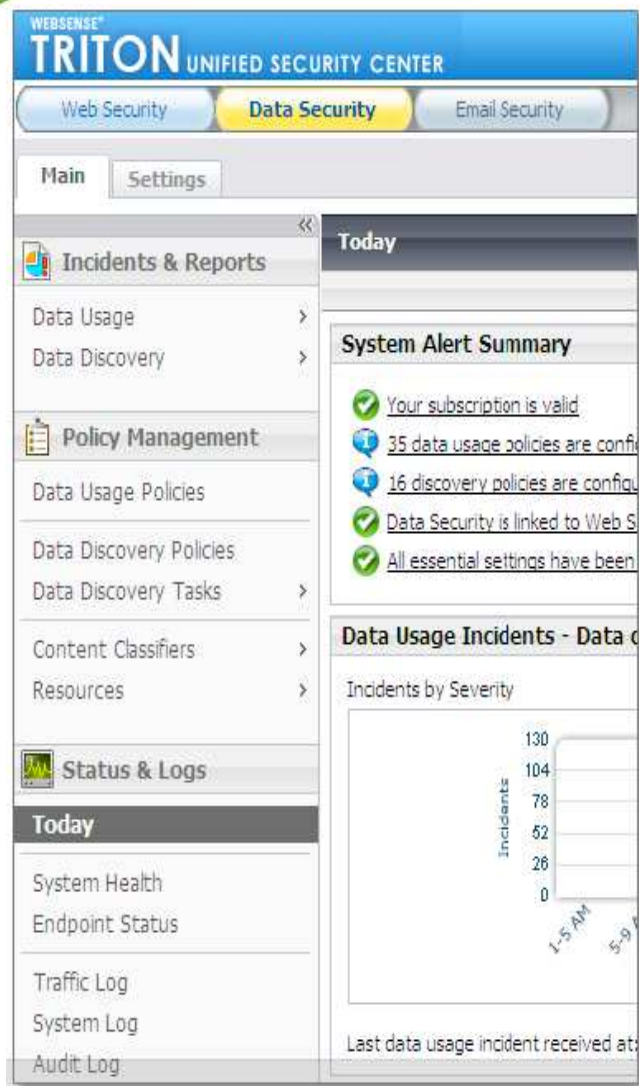
- Your subscription is valid
- 35 data usage policies are configured
- 16 discovery policies are configured
- Data Security is linked to Web Security
- All essential settings have been configured

Below the alerts is a 'Data Usage Incidents - Data Usage' section featuring a line graph titled 'Incidents by Severity'. The graph shows a sharp increase in incidents starting around 1:5 AM, reaching a peak of approximately 130 incidents by 5:00 AM. The y-axis is labeled 'Incidents' and ranges from 0 to 130. The x-axis shows time intervals from 1:5 AM to 5:00 AM.

At the bottom right, it states 'Last data usage incident received at:' followed by a partially visible timestamp.



- Несколько Dashboard'ов
- Показывает состояние:
 - System Health и активности
 - **Топ** нарушенных политик по серьезности
 - **Топ** каналов утечки по серьезности
 - **Топ** нарушителей политики
 - **Топ** мест хранения конфиденциальной информации



- Создание политик
 - Выбор способ идентификации (Классификатор)
 - Выбор каналов для мониторинга
 - Расписание задач Discovery
 - Установка серьезности и реакции

- Расследование инцидентов

- Отчетность



- Политика может быть применена к одному или нескольким каналам
- Возможности гранулированного реагирования в зависимости от канала и серьёзности инцидента

Data Usage

Select an action for each channel:

Email:	<input type="text" value="Quarantine"/>	Endpoint HTTP/HTTPS:	<input type="text" value="Block"/>
FTP:	<input type="text" value="Block"/>	Endpoint application:	<input type="text" value="Confirm"/>
Chat:	<input type="text" value="Always permitted"/>	Endpoint removable media:	<input type="text" value="Encrypt"/>
HTTP/HTTPS:	<input type="text" value="Permit"/>	Endpoint LAN:	<input type="text" value="Confirm"/>
Plain text:	<input type="text" value="Always permitted"/>	Endpoint printing:	<input type="text" value="Permit"/>
Network Printing:	<input type="text" value="Block"/>		<input type="text" value="Permit"/>

Permit
Block
Confirm

Применение политик в зависимости от местоположения

The screenshot displays the TRITON Unified Security Center interface. The main report is titled "Web Channel - Destination by Severity and Geolocation" and shows a world map with a callout for "North America and Central America" with a total of 19 incidents. A detailed map of the United States shows state-level incident counts: California (19), High (0), Medium (19), and Low (0). A filter dialog is open at the bottom, showing an "Available List" of countries with "Brazil" selected, and a "Selected List" containing "All".

Select the destination(s) to include in the filter then click >. Use the Display field to change destination types. Use the

Display: Geographical locations

Filter by: *

You can include wildcards.

Available List:

- Botswana
- Brazil
- Brunei
- Bulgaria
- Burkina Faso
- Burma

Selected List:

Include (6) Exclude (0)

All

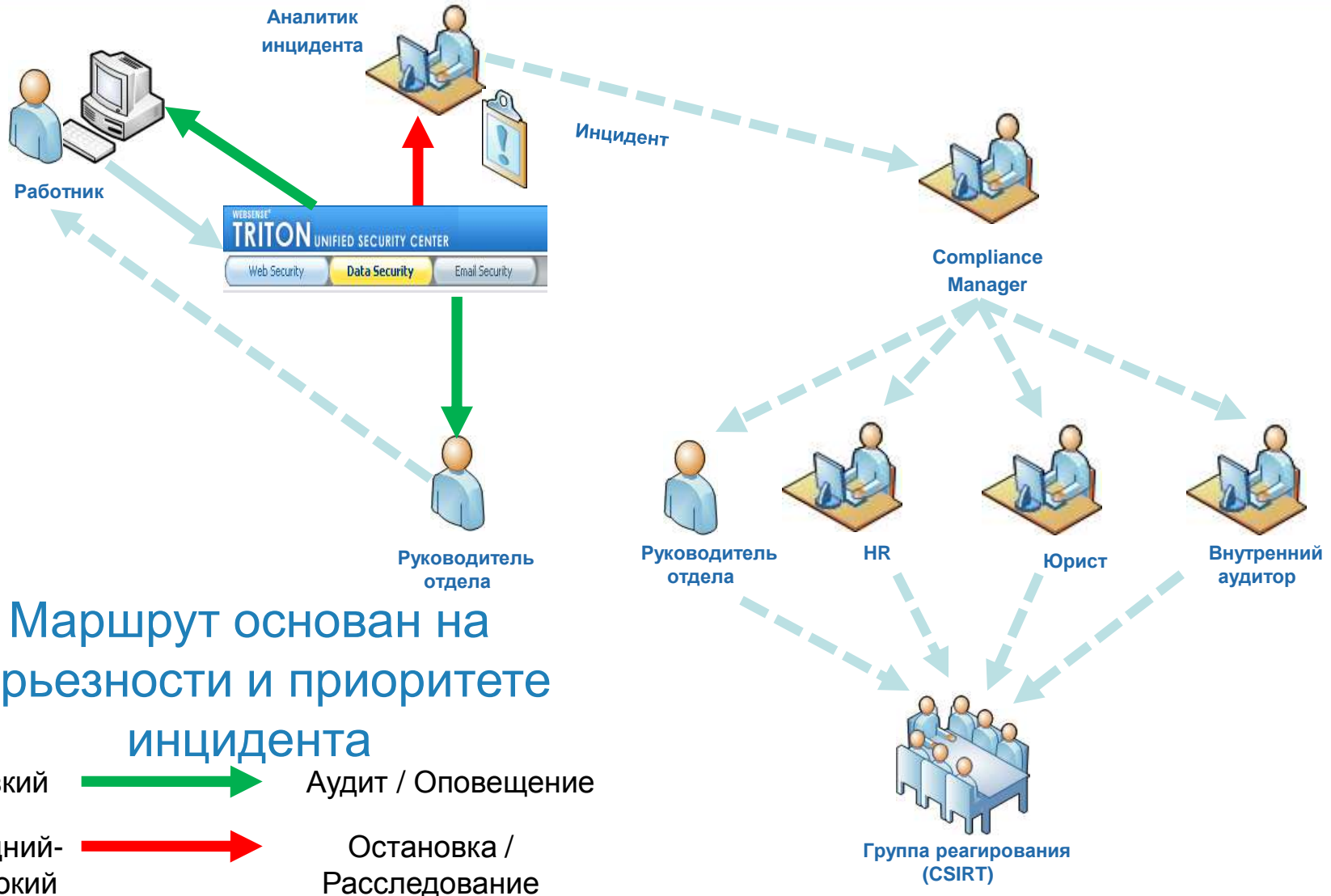
Adding an item will override 'All'

New 7.7



Автоматизация реагирования







Принятие мер

Список
ИНЦИДЕНТОВ

Триггеры
нарушения

Детали
инцидента

Incidents

Workflow Remediate Escalate Settings View Refresh

Report: Incidents Manage Report

Showing 66 incident(s)

ID	Host Name	File Full Path	Policies	Severity	File Size	Incident Time
196903	win-gbjme6t5tkd	C:\test\SC3.txt	General Sensitive Informati...	High	53.15 KB	22 May. 2012, 09:35:11 PM
200287	win-gbjme6t5tkd	C:\test\Sam's.txt	PCI Audit for discovery	Medium	25 B	22 May. 2012, 09:34:58 PM
197101	win-gbjme6t5tkd	C:\test\Order Information.docx	PCI Audit for discovery	Medium	45.81 KB	22 May. 2012, 09:34:52 PM
197501	win-gbjme6t5tkd	C:\test\My CCN.txt	PCI Audit for discovery	Medium	33 B	22 May. 2012, 09:34:44 PM
200251	win-gbjme6t5tkd	C:\test\My Card.txt	PCI Audit for discovery	Medium	41 B	22 May. 2012, 09:34:39 PM
196828	win-gbjme6t5tkd	C:\test\MR 1.docx	General Sensitive Informati...	Medium	13.66 KB	22 May. 2012, 09:34:32 PM
197907	win-gbjme6t5tkd	C:\test\Formal_Structured_p...	General Sensitive Informati...	High	54.26 KB	22 May. 2012, 09:33:47 PM
197961	win-gbjme6t5tkd	C:\test\Client List.PDF	General Sensitive Informati...	High	14.59 KB	22 May. 2012, 09:33:09 PM
197896	win-gbjme6t5tkd	C:\test\CC Form.doc	PCI Audit for discovery	Medium	28.5 KB	22 May. 2012, 09:33:01 PM
196967	win-gbjme6t5tkd	C:\test\Backup\SC3.txt	General Sensitive Informati...	High	53.15 KB	22 May. 2012, 09:32:55 PM
197747	win-gbjme6t5tkd	C:\test\Backup\PC 1.txt	PCI Audit for discovery	Medium	33 B	22 May. 2012, 09:32:45 PM
196953	win-gbjme6t5tkd	C:\test\Backup\C3.txt	PCI Audit for discovery	Medium	25 B	22 May. 2012, 09:32:33 PM
197739	win-gbjme6t5tkd	C:\test\Backup\C2.txt	PCI Audit for discovery	Medium	41 B	22 May. 2012, 09:32:29 PM
197066	win-gbjme6t5tkd	C:\test\Old\SC3.txt	General Sensitive Informati...	High	53.15 KB	22 May. 2012, 09:32:25 PM

Incident: 197961 Severity: High Channel: Discovery Discovery Type: File System Tune Policy

Display: Violation triggers

- Rule: PCI : Credit Cards - Default
 - Credit Cards (Default) (Script)
- Rule: Sensitive Private: EU Credit Card Number
 - EU Credit Cards (Script)
- Rule: PCI Audit: CCN without validation
 - Credit Cards Pattern (Script)
- Rule: PCI Audit: Wide
 - Credit Cards (Extra-Wide) (Script)
- Rule: PCI Audit: CCN with CVV
 - PCI Audit: CCN with CVV (Script)
- Rule: Sensitive Private: US Credit Card Number
 - Credit Cards (Default) (Script)
- Rule: PCI Audit: CCN - High Accuracy
 - Credit Cards (Default) (Script)
- Rule: Credit Cards - Default
 - Credit Cards (Default) (Script)

Properties History

File Details

File path: C:\test\Client List.PDF

Host Name: win-gbjme6t5tkd

File Size: 14.59 KB

Date Created: 22 May. 2012, 09:24:41 PM GMT +0300

Date Accessed: 22 May. 2012, 09:24:41 PM GMT +0300

Checksum: 10609473258888014282

File Owner: S-1-5-32-544

Incident Details

Severity: High

Status: New

Channel: Discovery

Analyzed by: Policy Engine bubble

Detected by: FCI Agent on WIN-GBJME6T5TKD

Event time: 22 May. 2012, 09:33:04 PM

Incident time: 22 May. 2012, 09:33:09 PM

Assigned to: Unassigned

Incident tag: PCI

Discovery Task

Task name: FCI Discovery Task

Discovery Type: File System

Close



Управление инцидентом с использованием почты

- Выбор действий из оповещения:
 - изменение серьезности
 - эскалация
 - назначение
 - игнорирование
 - и др.

WEBSense® Data Security

Date: 26 Oct. 2009, 4:23 PM
From: admin@websense.com

Email was quarantined
Message was quarantined and can be released. The message violated 6 policies.

Message to user
A policy breach was found and the transaction was blocked.
Sender: john@mycompany.com
Subject: A private message from the manager

Incident Details

Severity: Medium
Channel: Mail (encrypted)
Action: Block

Detected by: Protector on lemonade
Analyzed by: Policy Engine lemonade

Source: Jamesd@thiscompany.com
Manager: Dave James
IP Address: 10.23.33.2
Hostname: jamesd

Destination: origin@live.com
State: California
City: San Diego

Subject: A message from the company

Violation Triggers

Rule: Non Acceptable Usage
Policy: My policy
8 Values: 1234-1262-4783-3487 ; 8378-3474-384...
1234-1262-4783-3487 ; 8378-3474-384...

Rule: Credit Card Number
Policy: My policy
3 Values: 1234-1262-4783-3487 ; 8378-3474-384...
... ; 2981-2376-3852-2893

History

Date	Name	Details
30 Mar. 2008, 11:22 AM	jackb	assigned incidents to Dave Smith
29 Mar. 2008, 10:25 AM	donc	assigned to jackb
26 Mar. 2008, 10:35 PM	donc	incident received

Actions

Change severity to: [High](#) [Medium](#) [Low](#)
Change status to: [New](#) [In Process](#) [Closed](#)
Escalate to: [Source's manager](#)
More Actions: [Release all](#) [Assign](#) [Ignore](#) [Add comments](#)

Release by Reply
You are authorized to release this quarantined message.
To release this message, simply reply to this email making sure that the following **Quarantine release code** appears in the body of your reply.

Quarantine release code: <!--_Block Start_ Do not alter this block #%H^BBB EVrPJcgnn9se6t+ZImt3f2U5ziB/DFrWZ/sZ n8jyB6rAqp8dJLURYCv/IPIA9kzJrlyjeotzWhbl VV+PKdGN8Xg6hmtn3ZpSIWN/rCymJV0mfMkKW0BxSxgJoTg9v+qk5GH0 UkDzrToQT+JRIQbc Vb2Ww8lCSv8IaDUKIQ0= bbbvH%# __Block End__ -->

Actions

Change severity to: [High](#) [Medium](#) [Low](#)
Change status to: [New](#) [In Process](#) [Closed](#)
Escalate to: [Source's manager](#)
More Actions: [Release all](#) [Assign](#) [Ignore](#) [Add comments](#)

New 7.7



- Дает представление
 - Топ Web получателей по...
 - Топ Email получателей
 - Топ источников, соверш...
 - Топ нарушенных полити...
- Используется для:
 - Приоритезации меропри...
 - снижения риска
 - Определения необходи...
 - работников
 - Тюнинга политик
 - Определения «неправи...
 - процессов
 - Демонстрации соответс...
 - требованиям регулятор...

Show All

URL Category	High	Medium	Low	Total
General Email	157	289	278	724
Social Networking	8	36	265	309
Web Chat	0	2	265	267
Advertisements	7	30	81	118
Search Engines and Portals	16	47	25	88
Uncategorized	44	5	37	86
Information Technology	1	12	69	82
Internet Radio and TV	0	7	60	67
Government	20	0	37	67
Games	0	10	57	67
Business and Economy	2	2	36	40
Shopping	2	4	23	29
Job Search	1	25	2	28
Financial Data and Services	24	0	1	25
Personal Network Storage and Backup	0	5	17	22
Message Boards and Forums	0	1	16	17
Entertainment	0	5	8	13
Reference Materials	7	4	1	12
Advocacy Groups	0	0	11	11
News and Media	1	4	6	11
Educational Institutions	0	1	9	10
Travel	0	2	7	9
Instant Messaging	0	0	8	8
Illegal or Questionable	7	0	0	7
Professional and Worker Organizations	0	0	7	7
Society and Lifestyles	0	0	6	6
Blogs and Personal Sites	0	0	6	6
Streaming Media	0	1	5	6
Sports	0	0	5	5
Service and Philanthropic Organizations	0	1	4	5
Proxy Avoidance	0	0	2	2
Hosted Business Applications	0	2	0	2
Gay or Lesbian or Bisexual Interest	0	0	2	2
Phishing and Other Frauds	2	0	0	2
Personals and Dating	0	0	2	2

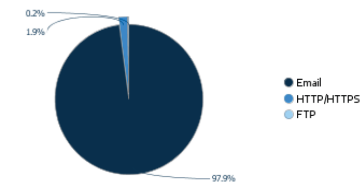


Сводные отчеты для руководства

- Могут запускаться по расписанию
- Топ инцидентов за последние 24 часа
- Итоговые отчеты за 30, 60, 90 дней
- Трендовые отчеты
- И другие...

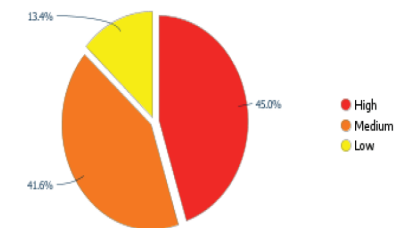
Top 5 Channels

Channel	Incidents
Email	93362
HTTP/HTTPS	1780
FTP	189



Incidents by Severity

Severity	Incidents
High	42887
Medium	39660
Low	12784




Data Usage Report: Catalog > Top Violated 30 days

Report: Top Violated 30 days Date Range: Last 37 Days Manage Report


Top 20 Policies

This section lists the policies that were violated the most.


Policy	High	Medium	Low	Total
Encrypted Files	40178	0	0	40178
Acceptable Use - Obscenities & Racism	1423	3673	15860	20956
Nevada SB 227 and NRS 603A	3436	15894	0	19330
HIPAA	2184	12864	0	15048
California SB 541 and AB 211	1949	11778	0	13727
US PHI	1945	11735	0	13680
FCRA	5108	7277	0	12385
Indiana HB 1101	2654	9693	0	12347
Ohio HB 104	2642	9640	0	12282
California AB 1298	1579	9045	0	10624
PIPEDA	1477	5534	143	7154
GLBA	4418	0	0	4418
Network Security Information	480	1750	1025	3255
FFIEC	55	2207	0	2262
RTN/ABA Numbers	2250	0	0	2250
California SB1	2204	0	0	2204
Check 21 Act	10	2163	0	2173
Pennsylvania SB 712	1818	250	0	2068
EIN	417	383	1222	2022
Social Security Numbers	1649	1	0	1650




Случайные




ОБУЧЕНИЕ РАБОТНИКОВ
Готовые шаблоны, оповещения/подтверждения, самостоятельный релиз




Преднамеренные (незлоумышленные)




ВИДИМОСТЬ
Уникальные совпадения, действия по серьезности инцидента, Source и Destination Awareness, Drip DLP




Инсайдер



РАСШИРЕННОЕ ДЕТЕКТИРОВАНИЕ
Drip DLP, контроль приложений, OCR распознавание



Внешний злоумышленник



WEBSNSE SECURITY LABS (ACE)
Дешифрование SSL, URL категории, геолокация, неавторизованное шифрование

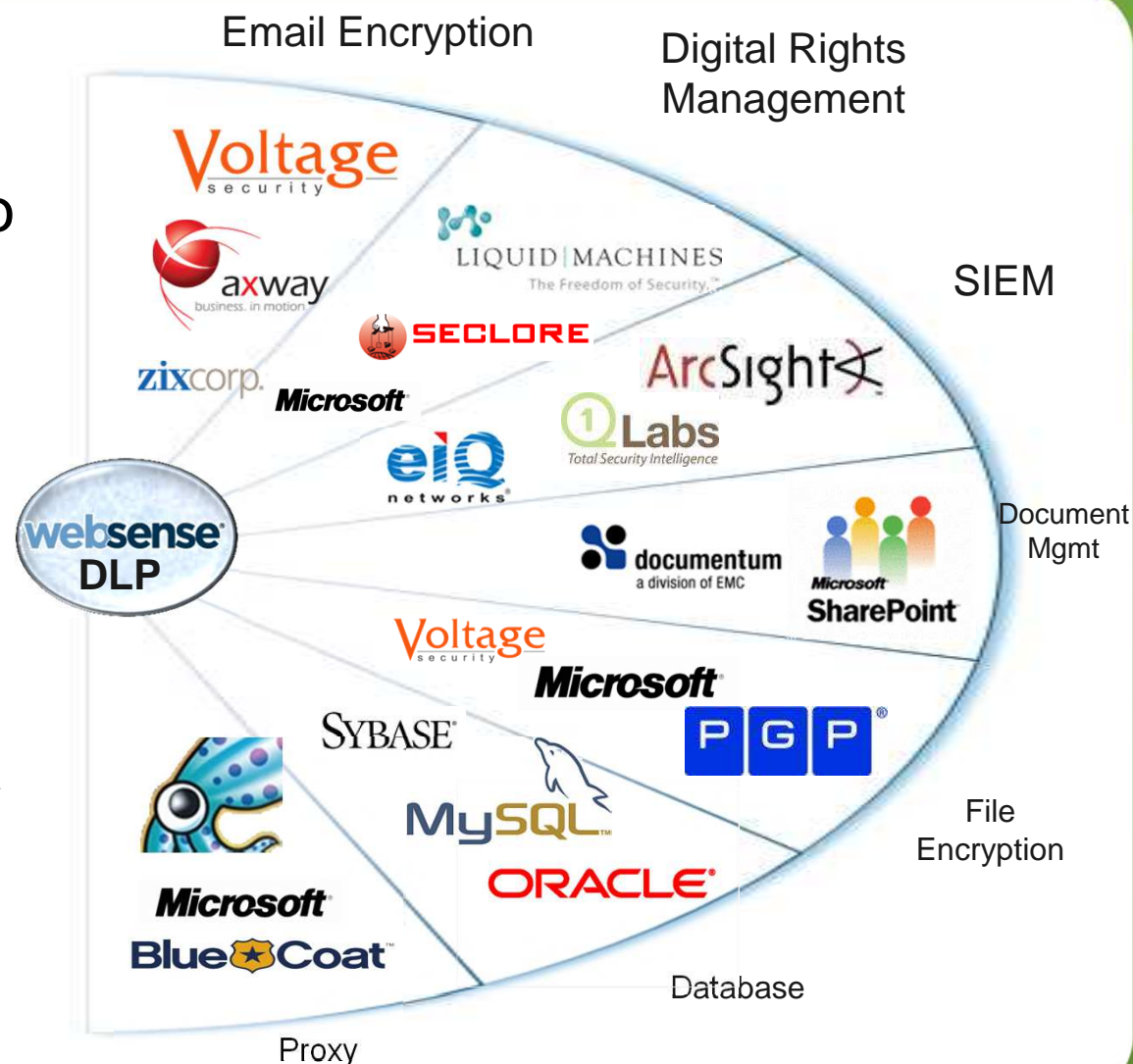
Data Security

Интеграция технологий



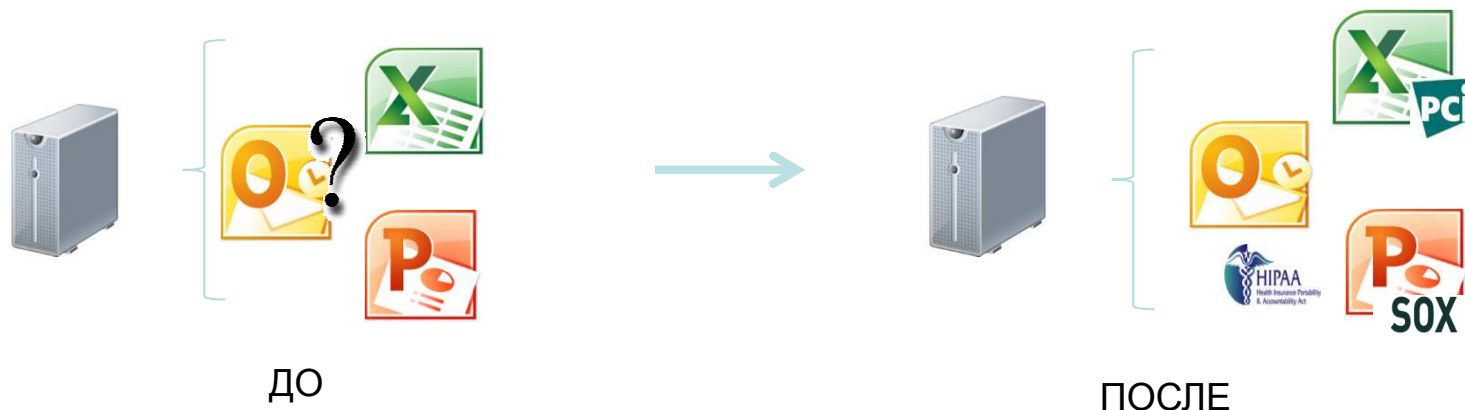


- DLP – это краеугольный камень программ по защите данных
- Основанный на стандартах обеспечивает совместимость с решениями третьих КОМПАНИЙ (Open API и ICAP)



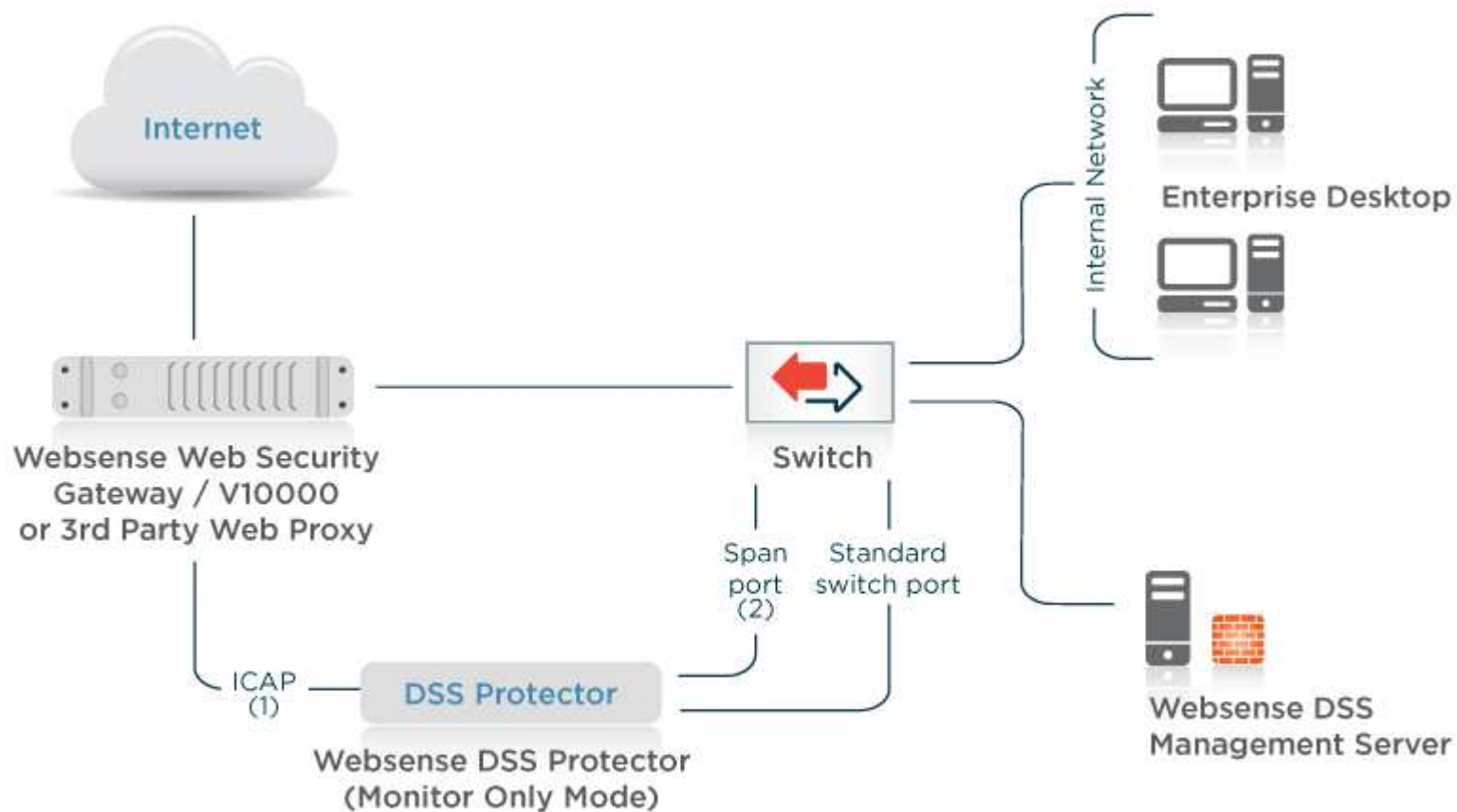


- Обеспечивает классификацию данных
- Microsoft File Classification Infrastructure использует Websense DLP для классификация контента как он сохраняется на сервере
- Конфиденциальные документы тегируются на основе контента (PCI, SOX, HIPAA)
- Microsoft Dynamic Access Control назначает Группам/Пользователям права доступа к КИ





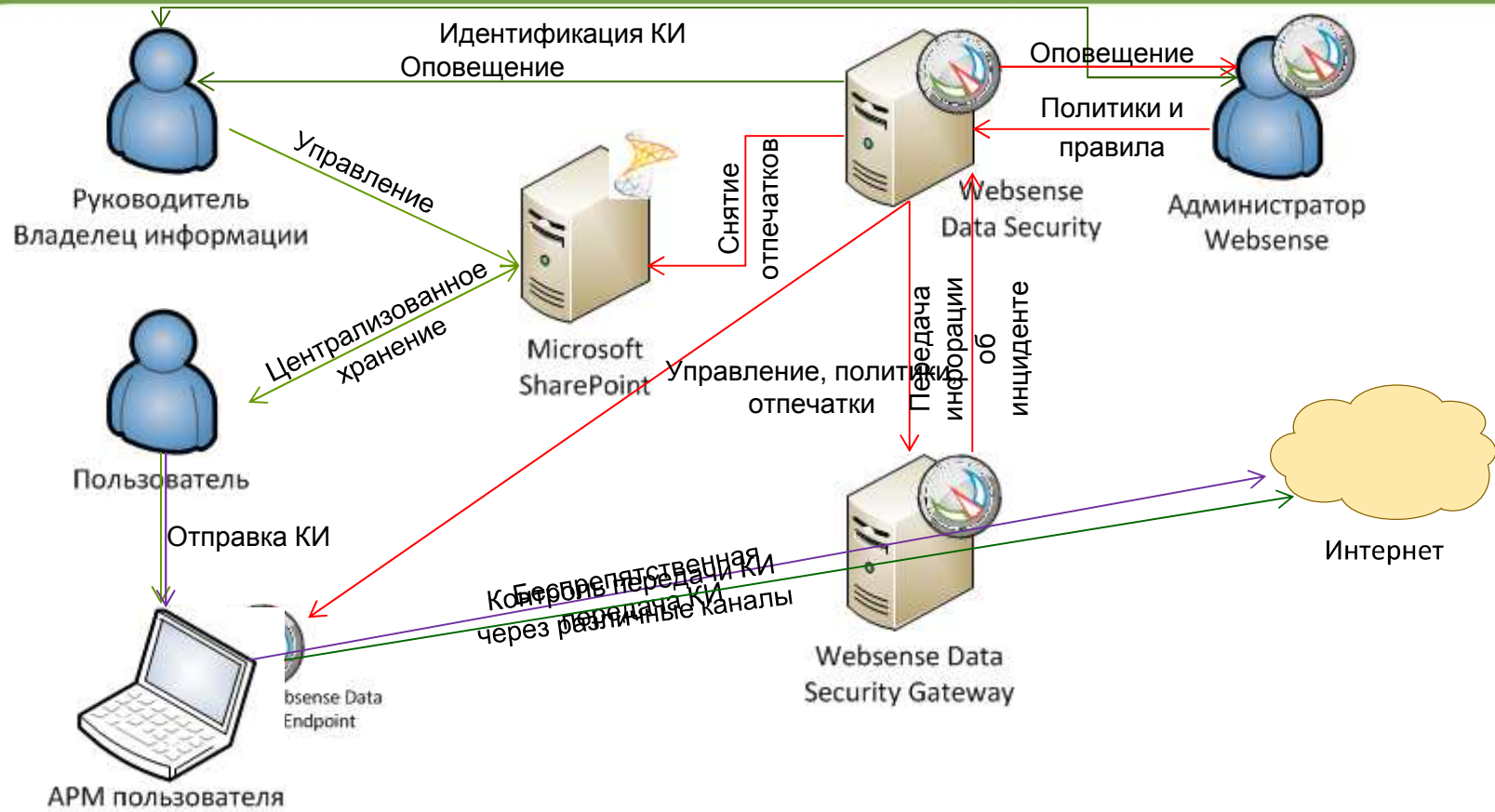
Архитектура Пассивный мониторинг



(1) HTTP, HTTP/S (2) HTTP, SMTP, FTP, IM, other



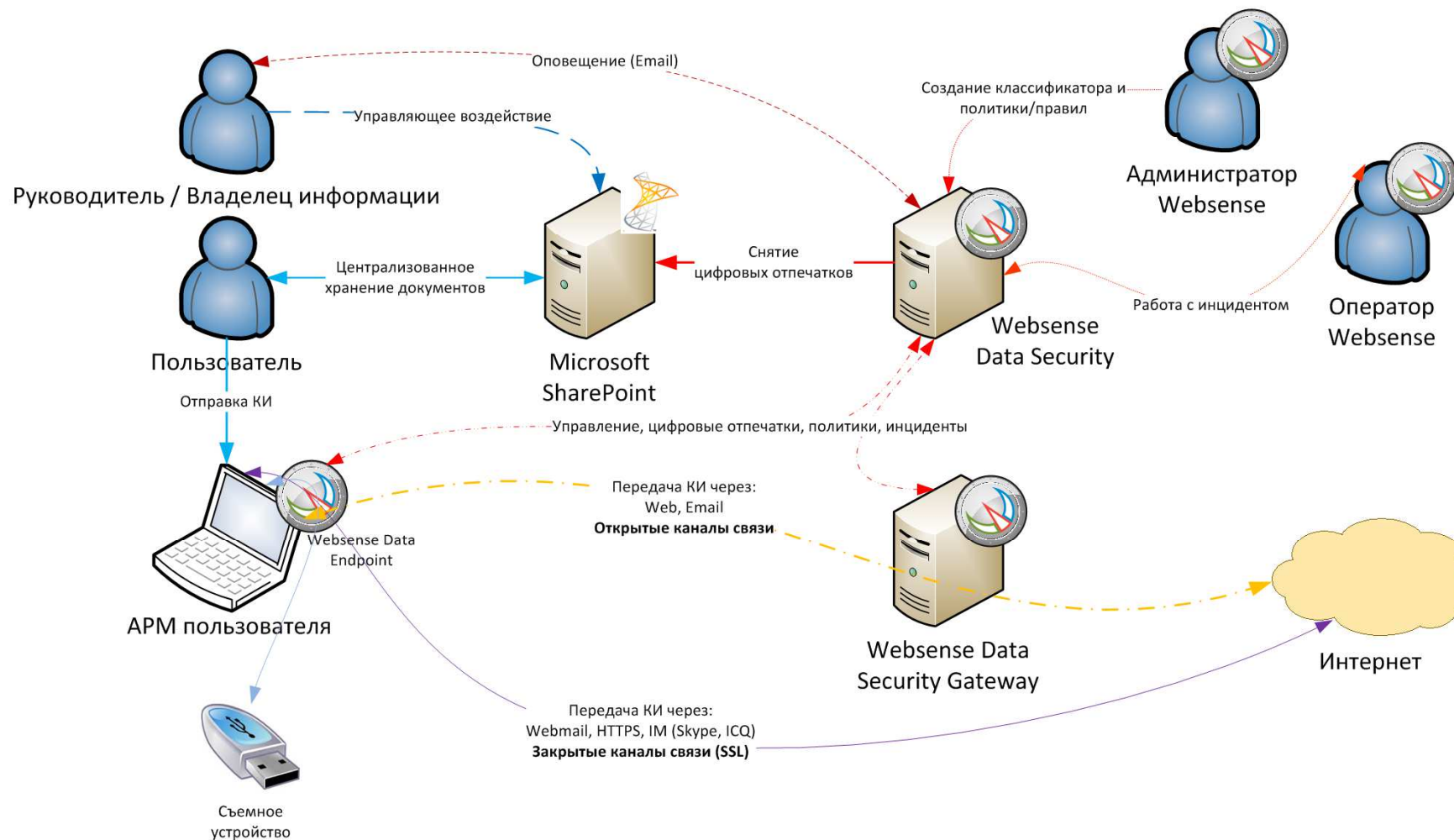
Пример. Интеграция с SharePoint



Простые и удобные механизмы интеграции системы в инфраструктуру для работы с Ки



Тоже самое, только картинка посложнее 😊



Решение Websense DLP

Пакеты





Data Security Suite

- LAN Storage Control
- USB Portable Decrypt.
- Applic. Data Controls
- Mobile Email DLP
- Monitor & Respond
- Scan & Remediate
- Data Risk Mgmt.
- Data Identification
- TRITON Console

❖ Appliance or Software

Data Endpoint

- LAN Storage Control
- USB Portable Decrypt.
- Applic. Data Controls
- Mobile Email DLP
- Monitor & Respond
- Data-in-Use
- Data Identification
- TRITON Console

❖ Software

Data Security Gateway

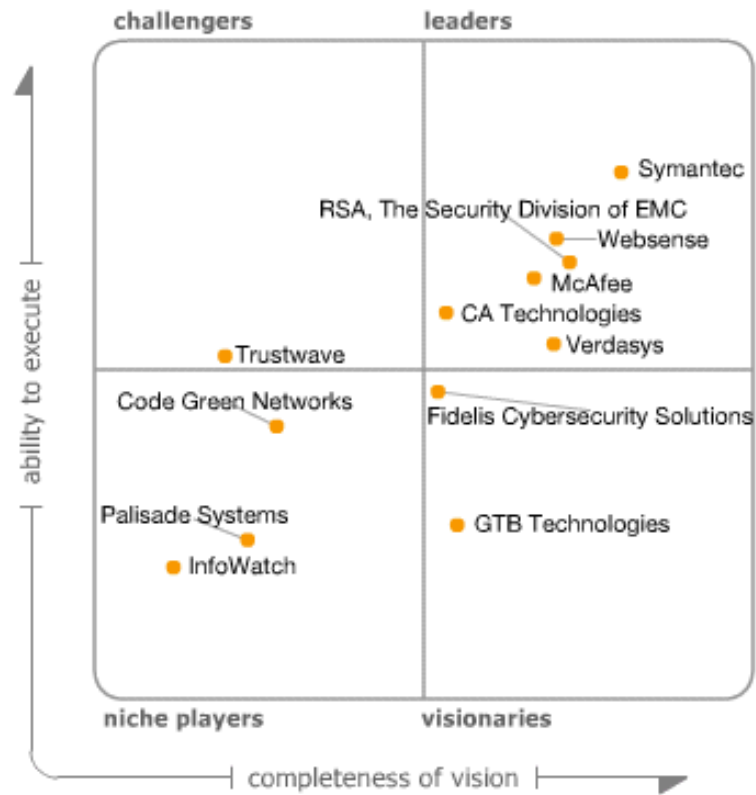
- Mobile Email DLP
- Monitor & Respond
- Data-in-Motion
- Data Identification
- TRITON Console

❖ Appliance or Software

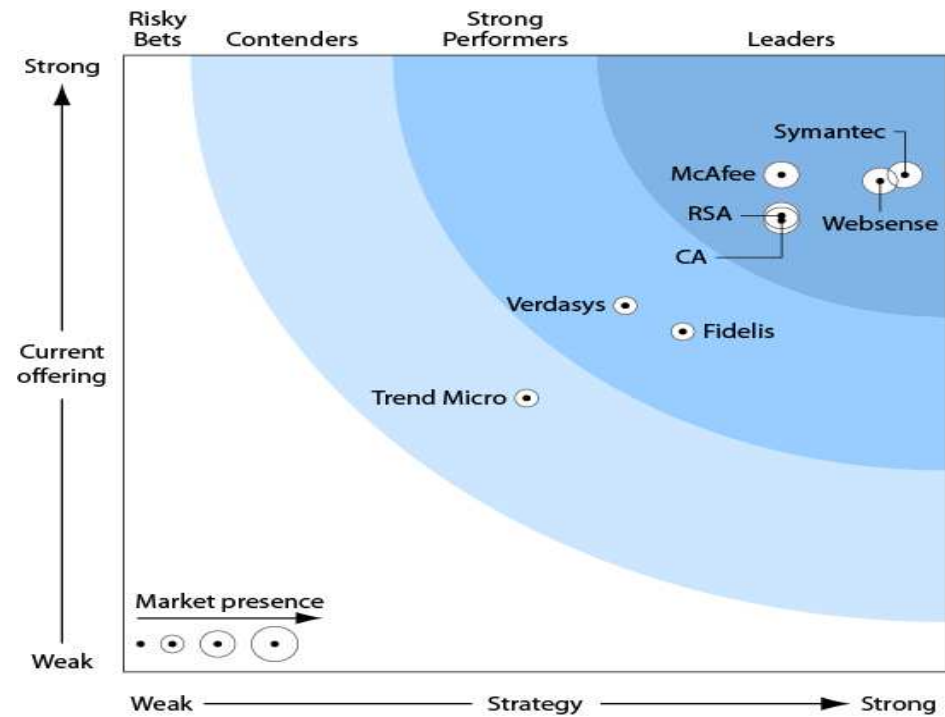
Data Discover

- Scan & Remediate
- Data-at-Rest
- Data Identification
- TRITON Console

❖ Software



As of January 2013

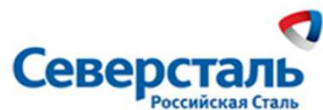




Финансовый сектор



Промышленность



«Сахалин Энерджи»
Быть ведущим источником энергии
для Азиатско-Тихоокеанского региона

Телекоммуникации





- Комплексный подход к построению системы защиты
 - Более 90% утечек за прошлый год, согласно отчету Verizon, можно было предотвратить используя достаточно дешевые средства и способы защиты
- Руководство компании:
 - Минимизация финансовых потерь, репутационных рисков
- Отдел ИБ:
 - Предотвращение и расследование инцидентов, связанных с утечкой конфиденциальной информации
- Отдел HR:
 - Выявление неблагонадёжных сотрудников. Лояльность персонала
- Отдел ИТ:
 - Снижение нагрузки на сотрудников ИТ, привлекающихся к расследованию инцидентов



Вопросы?

ЗАО «ДиалогНаука»

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

Роман Ванерке

<http://www.DialogNauka.ru>

e-mail: rv@DialogNauka.ru