

Обзор современных технологий и программного обеспечения для защиты от инсайдеров

Ванерке Роман

ЗАО «ДиалогНаука»



- 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



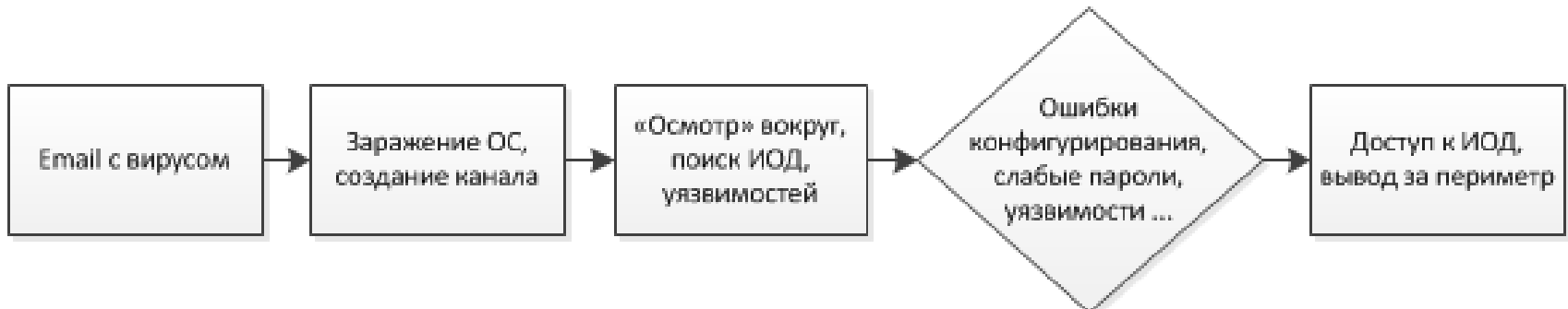
Стратегические планы, новые продукты, изменения, маркетинговые акции



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**



Среднее время обнаружения атак в днях





- 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)

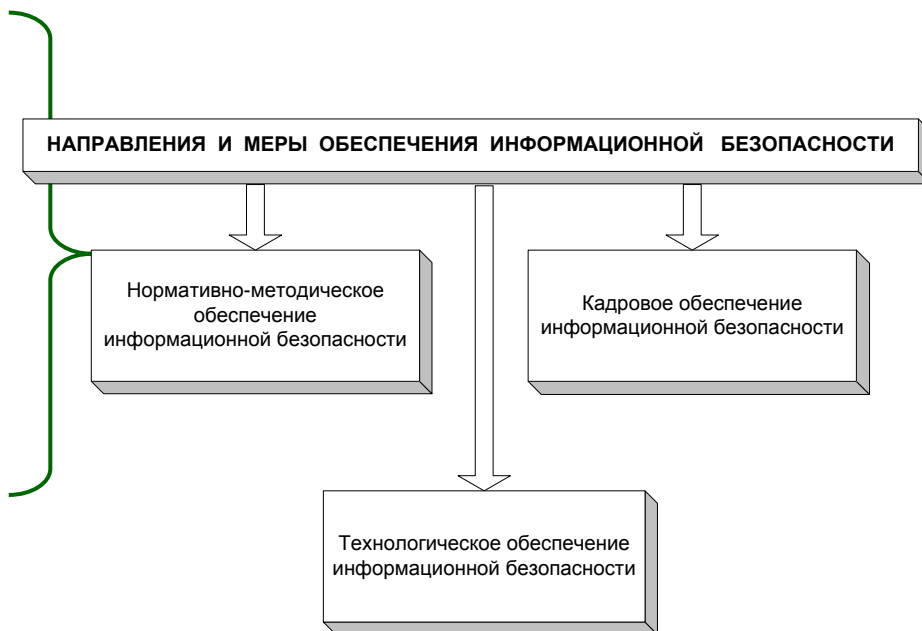


- Минимизация рисков
- Соответствие требованиям (Compliance)
 - ФЗ о ПДн
 - Соглашения с контрагентами
 - PCI DSS
 - ISO 27000
- Повышение эффективности бизнеса (увеличение выручки)
- Уменьшение стоимости продуктов и услуг



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

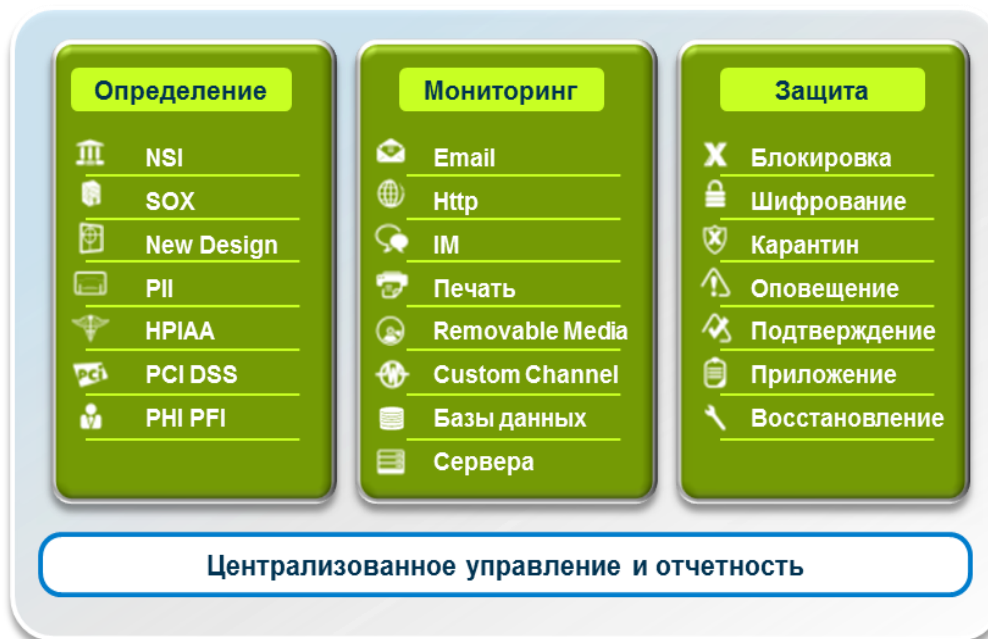
Websense Data Security

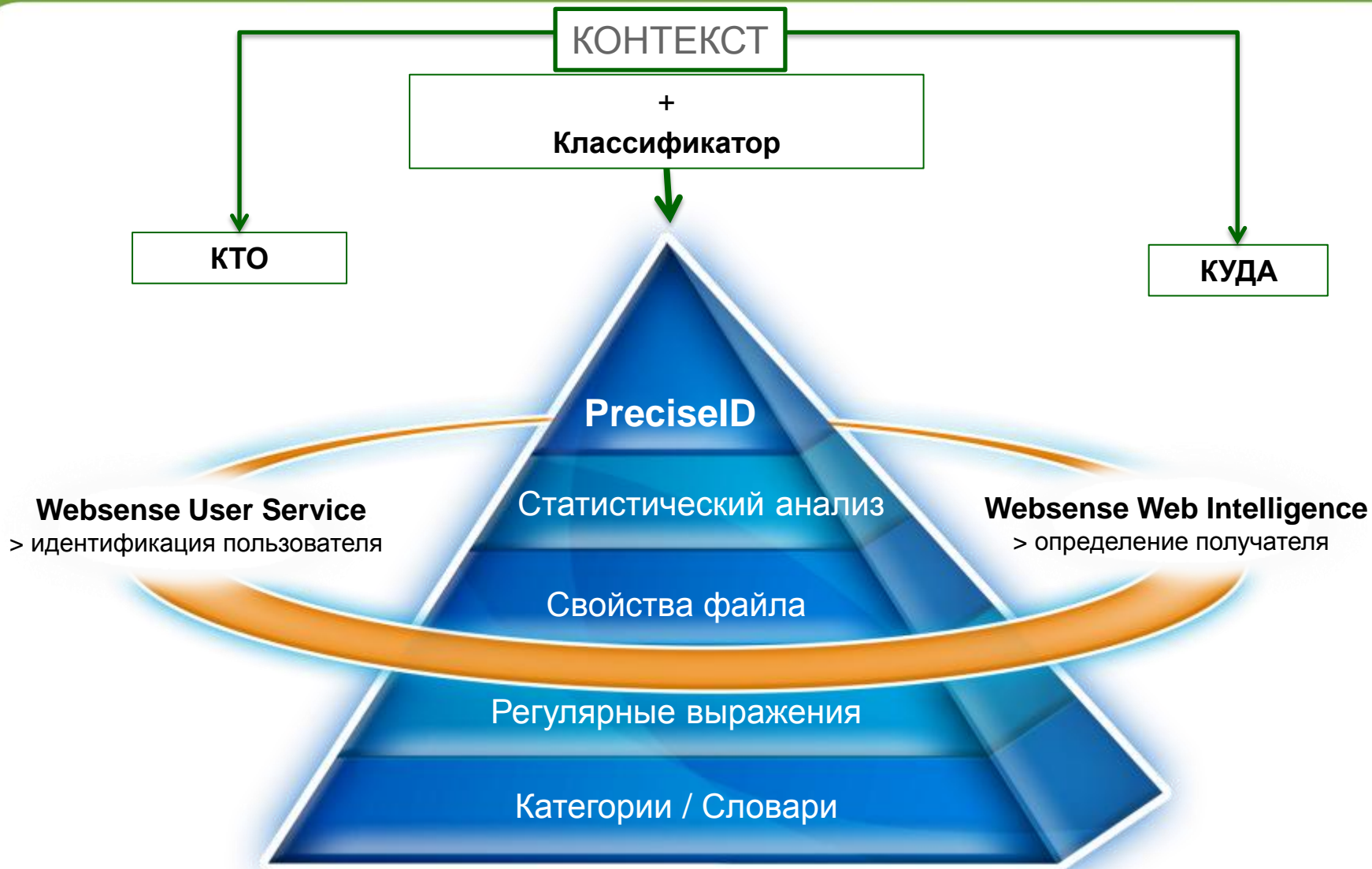




Лидирующая на рынке технология DLP для обнаружения, мониторинга и защиты конфиденциальных данных

- **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

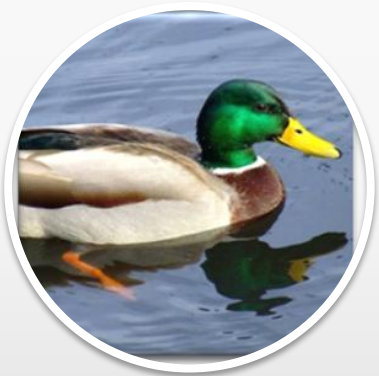




Websense Data Security

Технологии идентификации ИОД





Готовые
политики



Цифровые
отпечатки

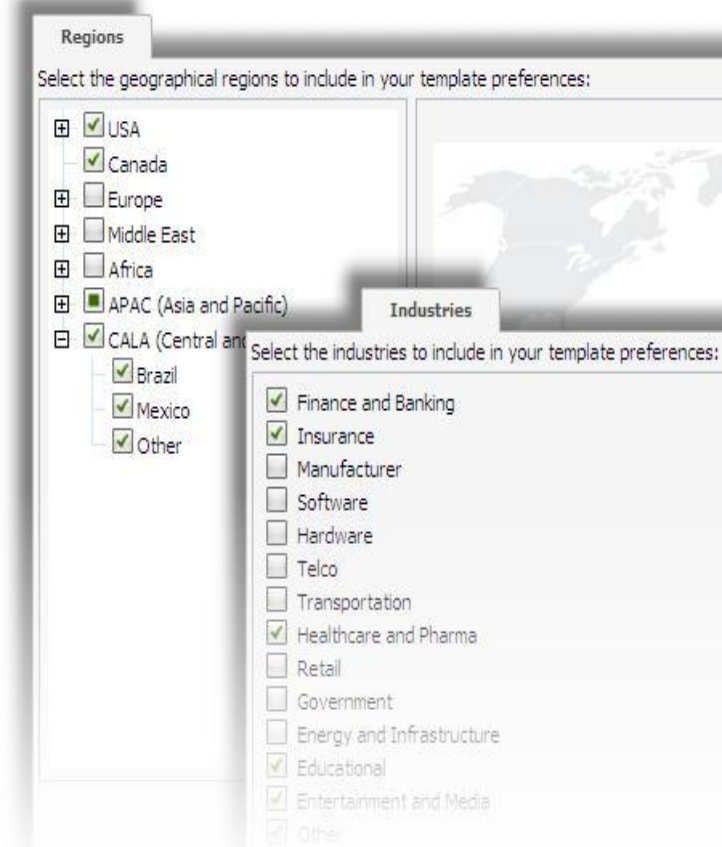


Machine
Learning





- 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



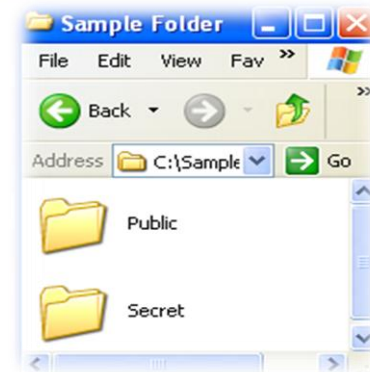
- Подключение к базе данных через ODBC

- Снятие цифровых отпечатков непосредственно с БД
- Данные не покидают БД
- Инкрементальные обновления базы отпечатков при росте исходной базы



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

Начало



Этап 1

- Маркетинговые материалы



Этап 2

- Маркетинговый план



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

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



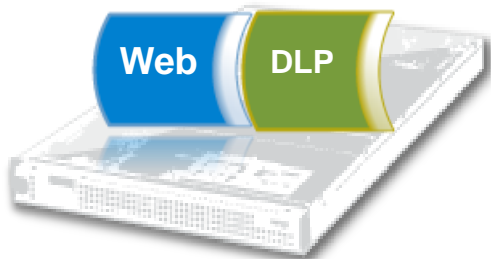


* Требуется прокси

** 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



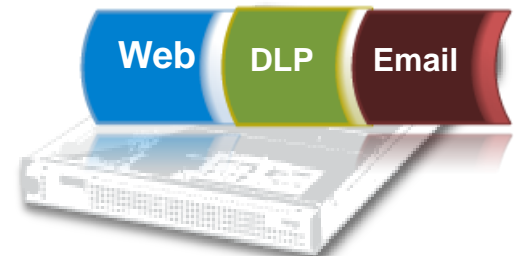
Web Security Gateway

- 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

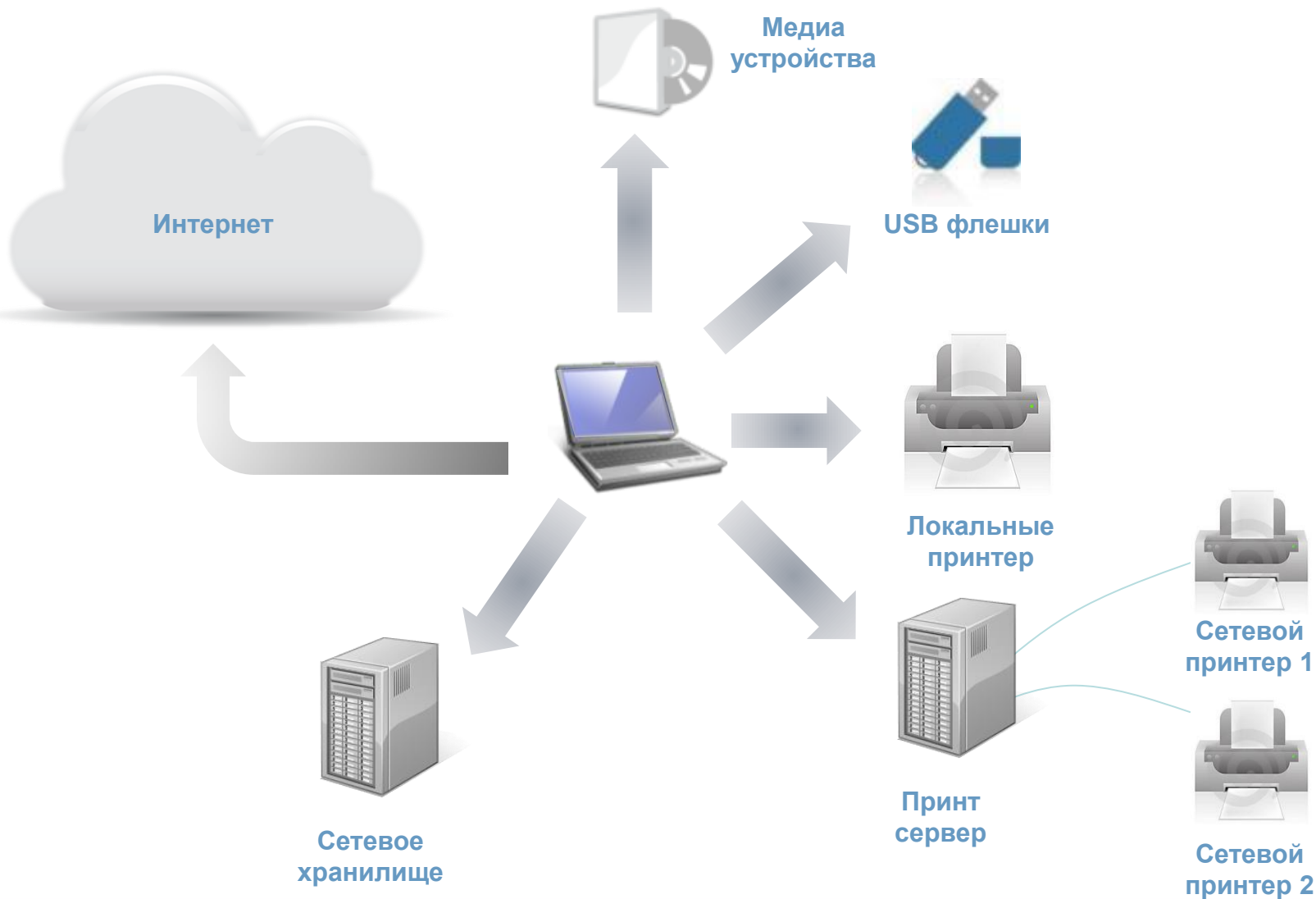
Endpoint DLP

*Использование
(Data-in-Use)*





Каналы утечки на уровне АРМ





Детектирование и реагирование



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

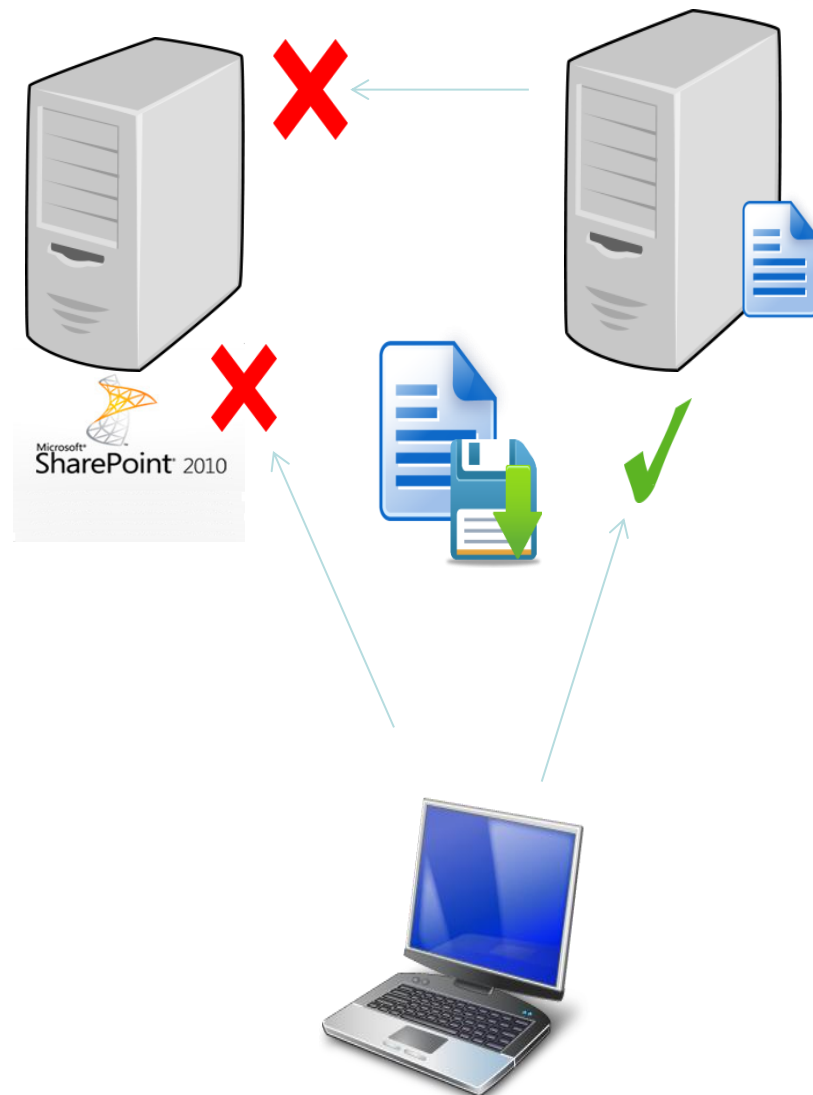
New... Delete

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

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



- 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



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

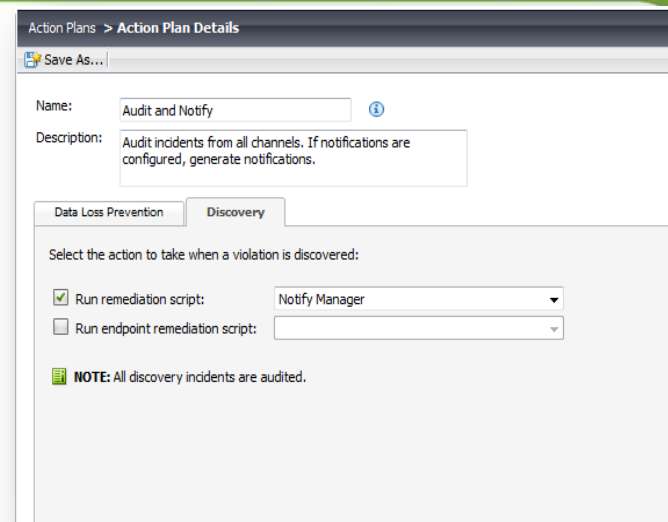
Гибридный



- Лучшее вариант
- Использование любой комбинации



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



Move/Quarantine



Encrypt**



Classification Tag
(Microsoft FCI)



Apply EDMR**



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

WEBSENSE®
TRITON UNIFIED SECURITY CENTER

Web Security | **Data Security** | Email Security

Main | Settings

Incidents & Reports

- Data Usage >
- Data Discovery >

Policy Management

- Data Usage Policies
- Data Discovery Policies
- Data Discovery Tasks >
- Content Classifiers >
- Resources >

Status & Logs

Today

- System Health
- Endpoint Status
- Traffic Log
- System Log
- Audit Log

Today

System Alert Summary

- ✓ Your subscription is valid
- ⓘ 35 data usage policies are confi
- ⓘ 16 discovery policies are configu
- ✓ Data Security is linked to Web S
- ✓ All essential settings have been

Data Usage Incidents - Data c

Incidents by Severity

Time Period	Incidents
1-5 AM	~20
5-9 AM	130

Last data usage incident received at:



- 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



The screenshot shows the Websense Triton Unified Security Center interface. The top navigation bar includes 'Web Security', 'Data Security' (highlighted), and 'Email Security'. Below this, there are tabs for 'Main' and 'Settings'. The left sidebar contains a navigation menu with categories: 'Incidents & Reports' (Data Usage, Data Discovery), 'Policy Management' (Data Usage Policies, Data Discovery Policies, Data Discovery Tasks, Content Classifiers, Resources), and 'Status & Logs' (Today, System Health, Endpoint Status, Traffic Log, System Log, Audit Log). The main content area shows a 'System Alert Summary' with several status messages, including 'Your subscription is valid', '35 data usage policies are configured', '16 discovery policies are configured', 'Data Security is linked to Web Security', and 'All essential settings have been configured'. Below this is a section for 'Data Usage Incidents - Data Usage' which includes a bar chart titled 'Incidents by Severity'. The chart shows a peak of 130 incidents at 1-5 AM and a lower count of 52 incidents at 5-9 AM. The y-axis is labeled 'Incidents' and ranges from 0 to 130. The x-axis shows time intervals: 1-5 AM and 5-9 AM.

- 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



Автоматизация реагирования





Принятие мер



Список инцидентов



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 Informat...	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 Informat...	Medium	13.66 KB	22 May, 2012, 09:34:32 PM
197907	win-gbjme6t5tkd	C:\test\Formal_Structured_p...	General Sensitive Informat...	High	54.26 KB	22 May, 2012, 09:33:47 PM
197961	win-gbjme6t5tkd	C:\test\Client List.PDF	General Sensitive Informat...	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 Informat...	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 Informat...	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) 10
- Rule: Sensitive Private: EU Credit Card Number
 - EU Credit Cards (Script) 10
- Rule: PCI Audit: CCN without validation
 - Credit Cards Pattern (Script) 10
- Rule: PCI Audit: Wide
 - Credit Cards (Extra-Wide) (Script) 10
- Rule: PCI Audit: CCN with CVV
 - PCI Audit: CCN with CVV (Script) 1
- Rule: Sensitive Private: US Credit Card Number
 - Credit Cards (Default) (Script) 10
- Rule: PCI Audit: CCN - High Accuracy
 - Credit Cards (Default) (Script) 10
- Rule: Credit Cards - Default
 - Credit Cards (Default) (Script) 10

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

Триггеры нарушения



Детали инцидента





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

Show All

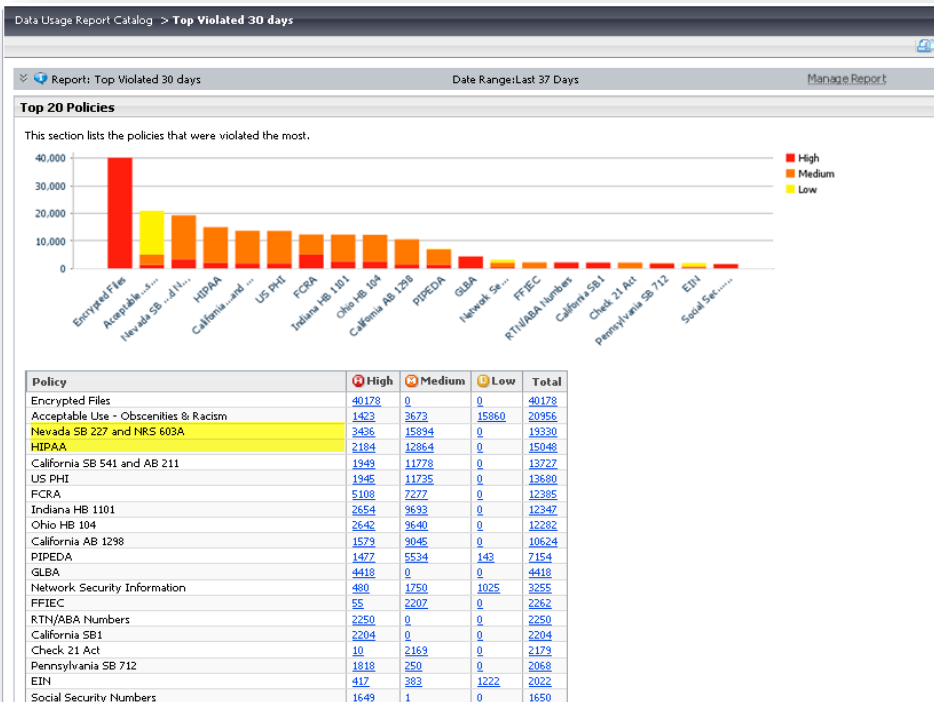
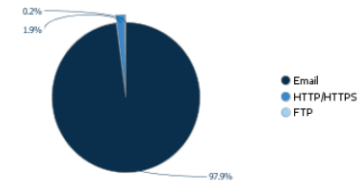
URL Category	High	Medium	Low	Total
General Email	157	289	278	724
Social Networking	8	36	265	309
Web Chat	0	2	265	267
Advertisements	7	30	81	118
Search Engines and Portals	16	47	35	98
Uncategorized	44	5	37	86
Information Technology	1	12	69	82
Internet Radio and TV	0	7	60	67
Government	30	0	37	67
Games	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



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

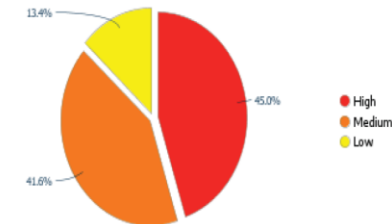
Top 5 Channels

Channel	Incidents
Email	93362
HTTP/HTTPS	1780
FTP	180



Incidents by Severity

Severity	Incidents
High	42887
Medium	39660
Low	12784



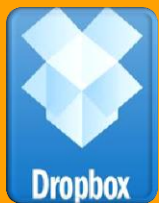


Случайные



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

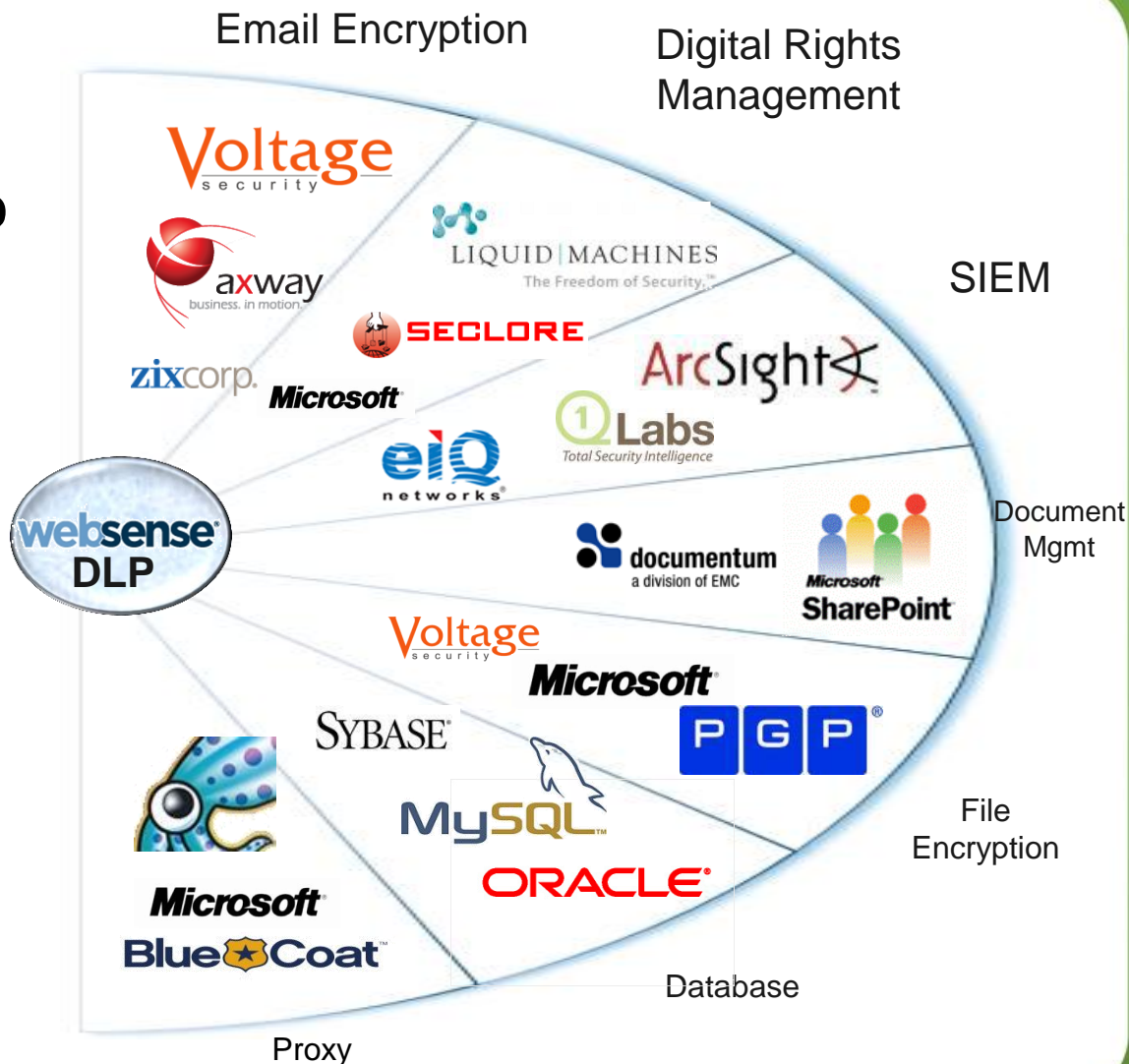
Data Security

Интеграция технологий



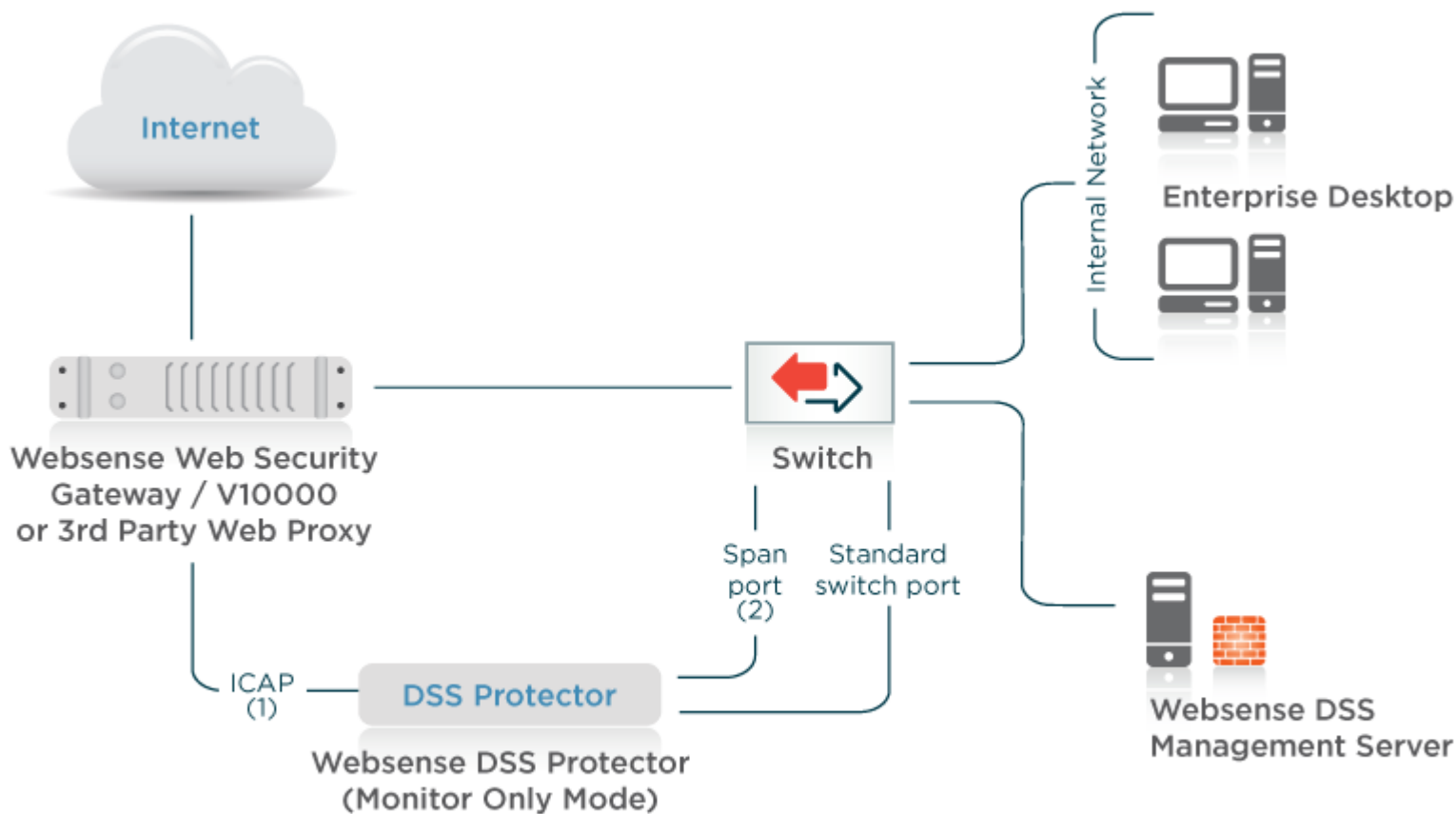


- DLP – это краеугольный камень программ по защите данных
- Основанный на стандартах обеспечивает совместимость с решениями третьих компаний (Open API и ICAP)





Архитектура Пассивный мониторинг



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

Решение Websense DLP

Пакеты





Data Security Suite

Data Endpoint

Data Security Gateway

Data Discover

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

LAN Storage Control

USB Portable Decrypt.

Applic. Data Controls

Mobile Email DLP

Monitor & Respond

Data-in-Use

Data Identification

TRITON Console



❖ Software

Mobile Email DLP

Monitor & Respond

Data-in-Motion

Data Identification

TRITON Console



❖ Appliance or Software

Scan & Remediate

Data-at-Rest

Data Identification

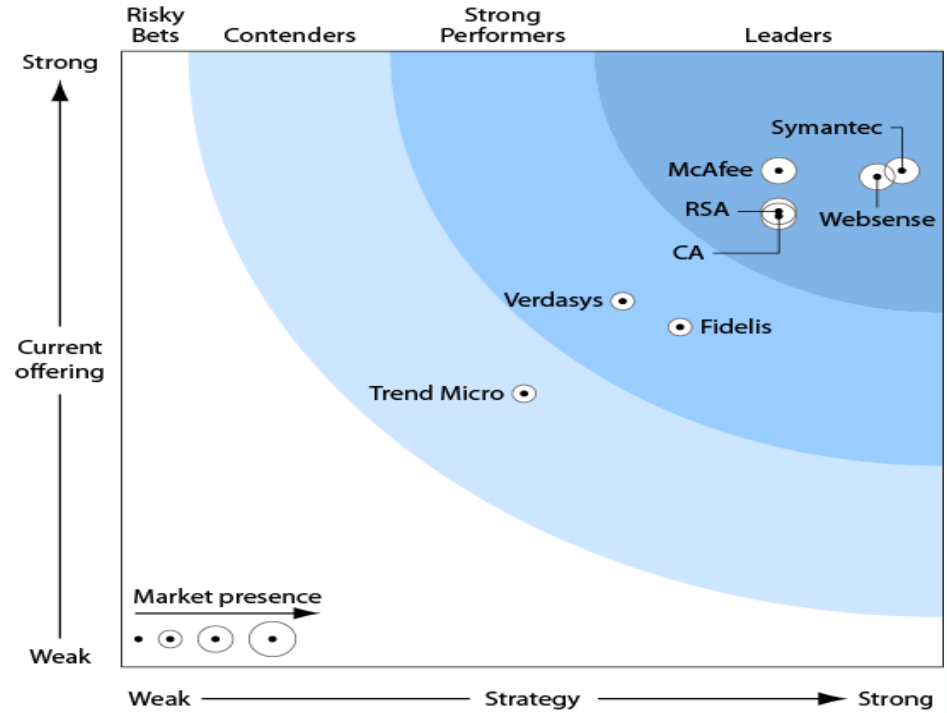
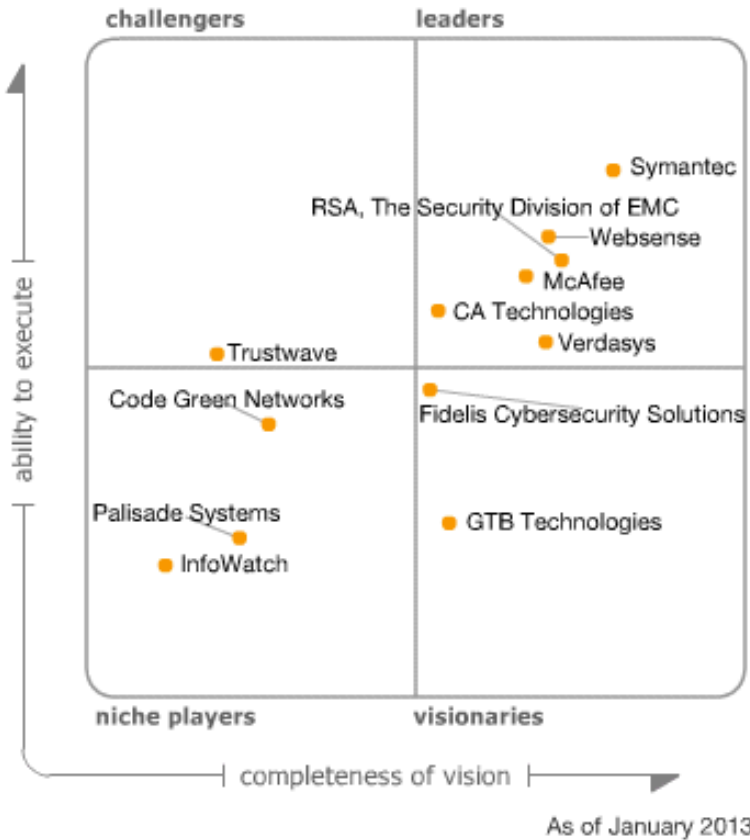
TRITON Console



❖ Software



Gartner, Forester

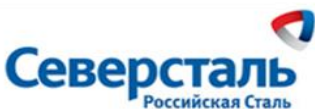




Финансовый сектор



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 неблагонадежных сотрудников. Лояльность персонала
- **Отдел ИТ:**
 - Снижение нагрузки на сотрудников ИТ, привлекающихся к расследованию инцидентов



ЗАО «ДиалогНаука»

Телефон: +7 (495) 980-67-

Факс: +7 (495) 980-67-75

Роман Ванерке

<http://www.DialogNauka.ru>

e-mail: rv@DialogNauka.ru