



Информационная безопасность современности

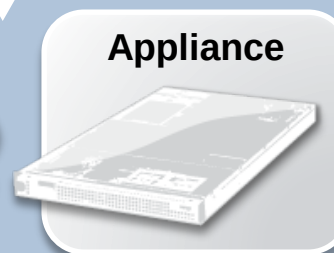
Архитектура TRITON

Комплексное
решение



Общая интеграция

Унификация
платформы

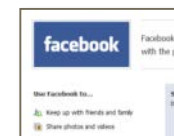
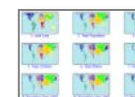
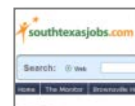
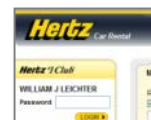


Полный
контроль





Web-филтрация. Web-мониторинг. Web-безопасность.



Определения

Задачи ИБ:

1. Оптимизация использование Интернет в организации.
2. Уменьшение рисков.

- Веб мониторинг
- Веб фильтрация
- Веб защита



Web-сайты сегодня

70% из топ 100 самых популярных Web сайтов хранили или были вовлечены в вредоносную активность в течении последних 6 месяцев.



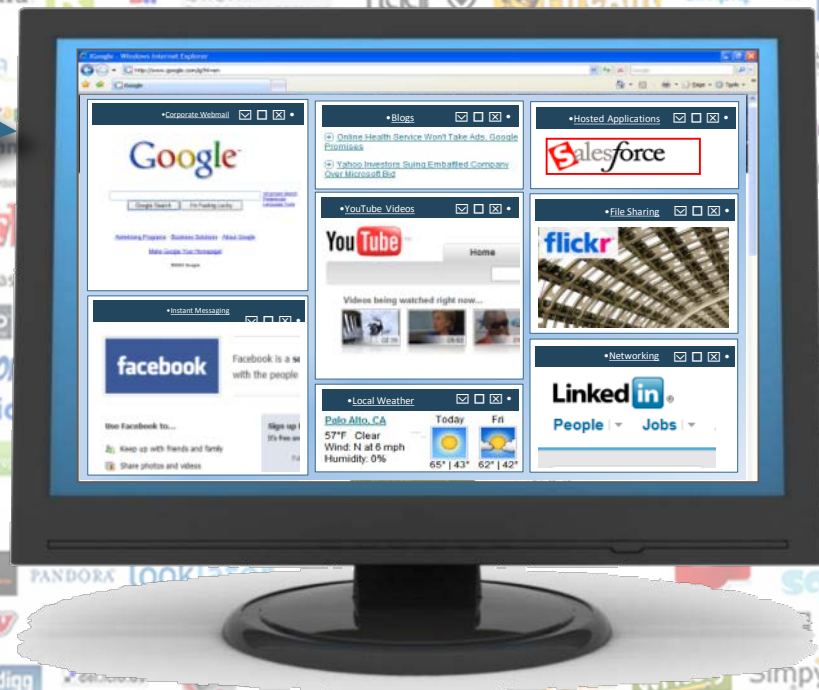
Бизнес растёт с помощью 2.0

Web 2.0 включает

- Социальные сети
- Hosted приложение
- Блоги, Wiki
- Хранение файлов
- RSS потоки

Новые технологии позволяют

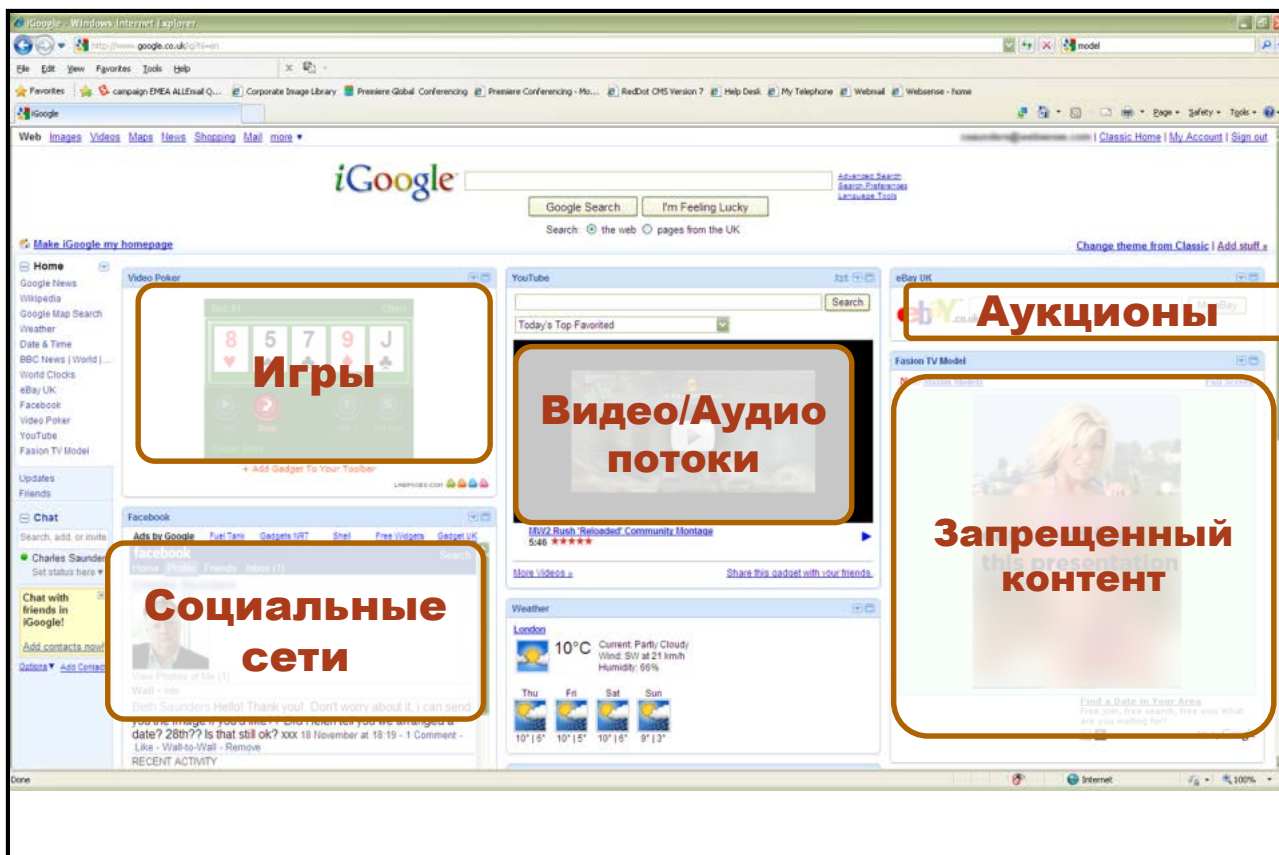
- Создавать, отправлять
- изменять, редактировать
- взаимодействовать
- распространять
- информацию



Статическая URL-фильтрация мертва

Понимание URL ссылки недостаточно.

Необходимо понимание содержимого на странице



Без Websense

The screenshot displays the iGoogle homepage with the following elements:

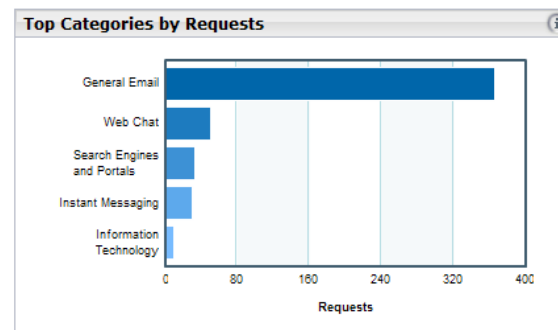
- Top Bar:** iGoogle logo, search bar, and buttons for "Google Search" and "I'm Feeling Lucky". Links for "Advanced Search", "Search Preferences", and "Language Tools" are on the right.
- Left Sidebar:**
 - Home:** Links to "Get new themes" (Super Mario, Street Fighter, Spore, etc.) and "Get artist themes".
 - Email:** Links to "Yahoo Mail", "GMail", "Hotmail: Now w...", and "mail2web.com".
 - demo:** Links to "Proxy Browsing", "Get random we...", "A Gadget to fetc...", "AIM Messenger...", "Search Ebay", "Spanish Word ...", "Bejeweled", "Xroxy Proxy Lists", "Proxy List", and "FreeCalculator P...".
 - Chat:** "Search, add, or invite" section with a contact "Charles Paul De" and a "Set status here" dropdown. Below is a "Chat with friends in iGoogle!" section with an "Add friends now!" link.
 - Options:** "Options" and "Add friends" links.
- Main Content Area:**
 - Bejeweled:** A game widget with a score of 0 and buttons for "NEW GAME", "SIMPLE", "TIMED", and "UPGRADE".
 - Proxy List:** A gadget titled "A Gadget to fetch a website using a proxy" with the message "Information is temporarily unavailable."
 - Spanish Word A Day:** A gadget showing translations: "marino = marine", "reforzar = reinforce / strengthen", and "terrazza = terrace".
 - Get random web proxy:** A gadget titled "Free working web proxies" with a dropdown menu set to "Any" and a "Get web proxy" button.
 - Search Ebay:** A gadget titled "What is Proposition 8?" with an "eBay" logo and a search bar.
 - Proxy Browsing:** A gadget with a text input field containing "http://" and a "Proxy Me!" button.
 - Xroxy Proxy Lists:** A gadget titled "Xroxy Proxy Lists" with links to "Anonymous proxies (Mar 26, 17:35 GMT)", "Distorting list (Mar 26, 17:35 GMT)", and "Transparent only (Mar 26, 17:35 GMT)".
 - AIM Messenger FIXED:** A gadget for eBuddy with fields for "Login", "AIM", "Username", and "Password", a "Forgot your password?" link, and a "Login" button. It also includes a "Sign in silently" checkbox and a "© 2009 eBuddy | FAQ | Top" footer.

C Websense

The screenshot shows the iGoogle homepage with the Google logo and search bar at the top. Below the search bar, there are links for "Advanced Search", "Search Preferences", and "Language Tools". The main content area is divided into several sections:

- Home**: Links to "Get new themes" from Super Mario, Street Fighter, Spore, and more.
- Email**: Links to Yahoo Mail, Gmail, and Hotmail.
- demo**: A section with various links including "Proxy Browsing", "Get random web...", "A Gadget to fetch...", "AIM Messenger...", "Search Ebay", "Spanish Word ...", "Bejeweled", "Xroxy Proxy Lists", "Proxy List", and "FreeCalculator P...".
- Chat**: A section with a "What is Proposition 8?" link.
- Bejeweled**: A game widget with a "Content blocked by your organization" message. The message states: "Reason: This Websense category is filtered: Games. URL: Options: Click [more information](#) to learn more about your access policy. To view sites in this".
- Proxy List**: A widget with a "Content blocked by your organization" message. The message states: "Reason: This Websense category is filtered: Games. URL: Options: Click [more information](#) to learn more about your access policy. To view sites in this".
- A Gadget to fetch a website using a proxy**: A widget with a "Content blocked by your organization" message. The message states: "Reason: This Websense category is filtered: Games. URL: Options: Click [more information](#) to learn more about your access policy. To view sites in this".
- Spanish Word A Day**: A widget with a "Content blocked by your organization" message. The message states: "Reason: This Websense category is filtered: Games. URL: Options: Click [more information](#) to learn more about your access policy. To view sites in this".
- Get random web proxy**: A widget with a "Content blocked by your organization" message. The message states: "Reason: This Websense category is filtered: Games. URL: Options: Click [more information](#) to learn more about your access policy. To view sites in this".
- Xroxy Proxy Lists**: A widget with a "Content blocked by your organization" message. The message states: "Reason: This Websense category is filtered: Games. URL: Options: Click [more information](#) to learn more about your access policy. To view sites in this".
- AIM Messenger FIXED**: A widget with a "Content blocked by your organization" message. The message states: "Reason: This Websense category is filtered: Instant Messaging. URL: Options: Click [more information](#) to learn more about your access policy. Click [Continue](#) to view the site now for work-related purposes. Click [Go Back](#) or use the browser's Back button to return to the previous page. Enjoy AIM without installing additional software. By Whizz and eBuddy".

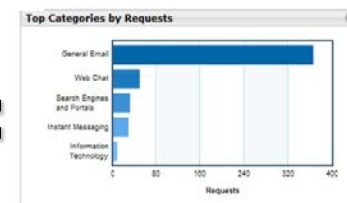
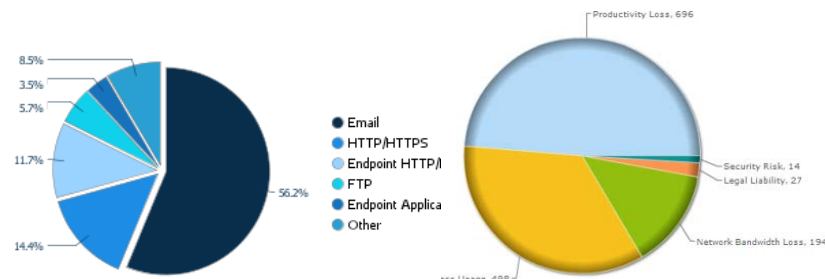
Web Filter



- **Передовое решение WEB-фильтрации**
- **Повышение производительности сотрудников**
- **Оптимизация использования ресурсов Интернет**

Контроль безопасности компании

Web Security



- Набор категорий безопасности URL:

Бот-сети, Шпионские программы

Фишинг и мошенничество, Перехватчики клавиатуры

Вредоносные веб-сайты

Потенциально нежелательные программы

- Службы WEB репутации

Передовое решение WEB-фильтрации

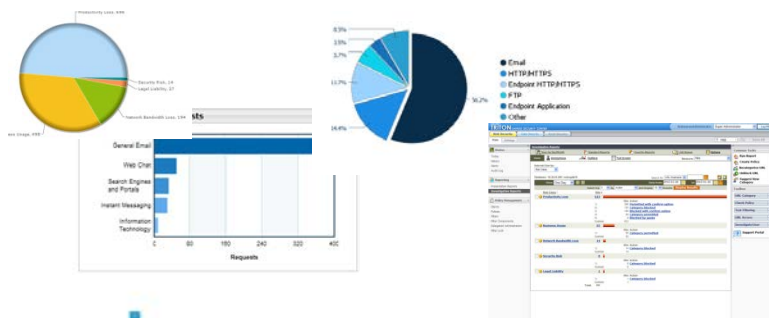
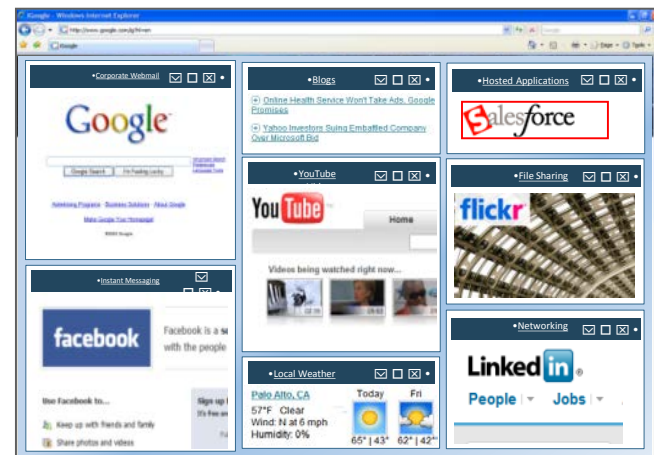
Повышение производительности сотрудников

Оптимизация использования ресурсов Интернет

WEB 2.0 Challenge

Web Security Gateway

- **Контентная фильтрация**
- **Категоризация WEB 2.0**
- **Анализ SSL**
- **Сканирующий Proxy Server**



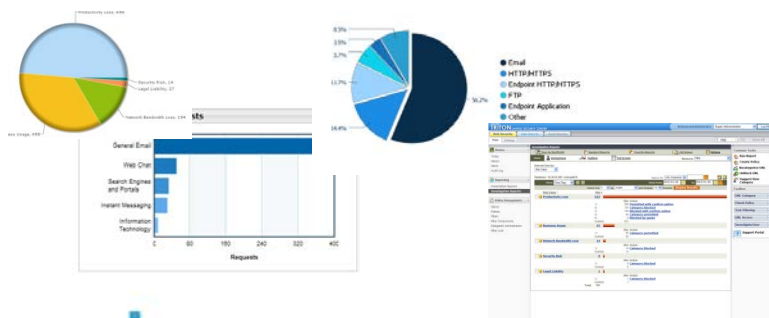
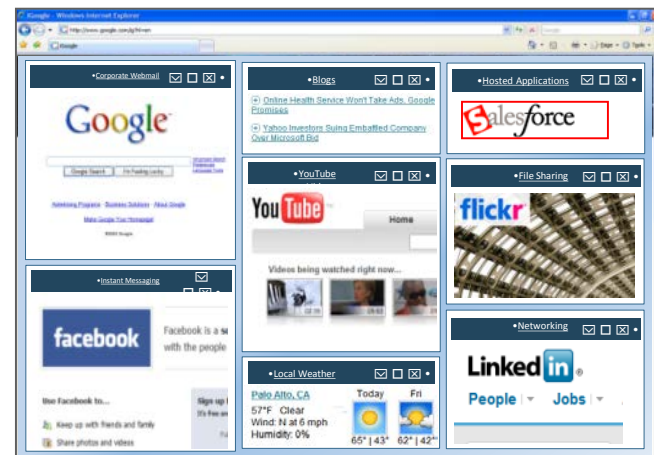
Передовое решение WEB-фильтрации
Повышение производительности сотрудников
Оптимизация использования ресурсов Интернет
Набор категорий безопасности URL

Службы WEB репутации

WEB 2.0 Challenge

Web Security Gateway Anywhere

- **Контентная фильтрация**
- **Категоризация WEB 2.0**
- **Анализ SSL**
- **Сканирующий Proxy Server**
- **Web DLP**
- **Hosted Web Security**



Передовое решение WEB-фильтрации
Повышение производительности сотрудников
Оптимизация использования ресурсов Интернет
Набор категорий безопасности URL

Службы WEB репутации

V10000, V5000 Appliances

- Внедрение передовых решений в сфере безопасности Интернет, данных и электронной почты

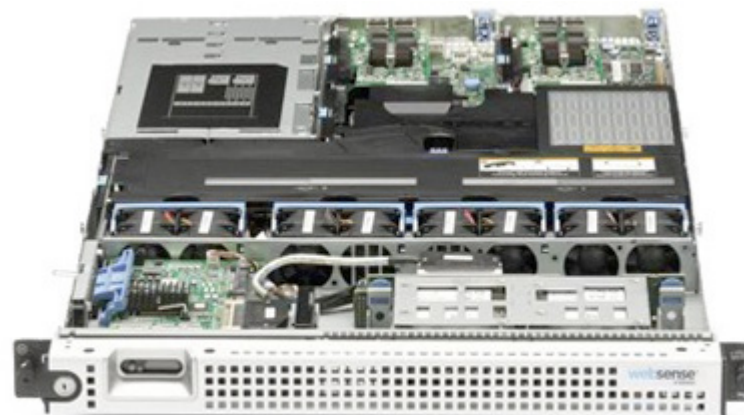
- Расширяемый функционал уровня корпоративного класса, который включает высокую

отказоустойчивость и доступность

- Простоту в использовании благодаря системе централизованного управления и отчетности

- Возможность расширения системы безопасности в будущем

- Привлекательную цену и безупречное качество



ROI

К-во сотрудников с
Internet доступом - 500
Средняя заработная плата
сотрудника - 500\$ (3.13\$ в час)

Результаты в процессе работы
тестового стенда:
минимум 10% времени сотрудники
проводят на интернет сайтах, не
относящихся к работе – минимум 4,5
часов в неделю (10% рабочего
времени)



В итоге убыток:

**3,13\$ з/п в час * 4,5 часа/неделя * 50
недель/год * 500 человек = 352 125\$/год.**

ROI

.....убыток 352 125\$/год.

**Окупаемость решений
 Websense Web Security происходит за
 несколько недель!**

**Сотрудники имеют доступ в интернет,
 который им необходим для
 качественного выполнения работы.**

**Комплексная интеграция
 промышленного прокси-сервера,
 централизованное
 администрирование**





Data Security Solution

Решения для защиты данных

Задачи Data Loss Prevention

Гарантия непрерывности бизнеса путем управления рисками, защита от утечки конфиденциальной информации по всем возможным каналам передачи



Websense Data Security Suite

**Data Loss Prevention технология для
идентификации, мониторинга и защиты
конфиденциальной информации**

- **Сетевое DLP**
- **Endpoint DLP**



Websense Data Security Suite

Функции WebsenseDSS

Data Discover

обнаружение и классификация данных, хранящихся в сети организации

Data Monitor

мониторинг передаваемых данных для выявления нарушения политик безопасности

Data Protect (Data Security Gateway)

мониторинг и предотвращение утечек конфиденциальных данных на основе политик безопасности организации

Data Endpoint

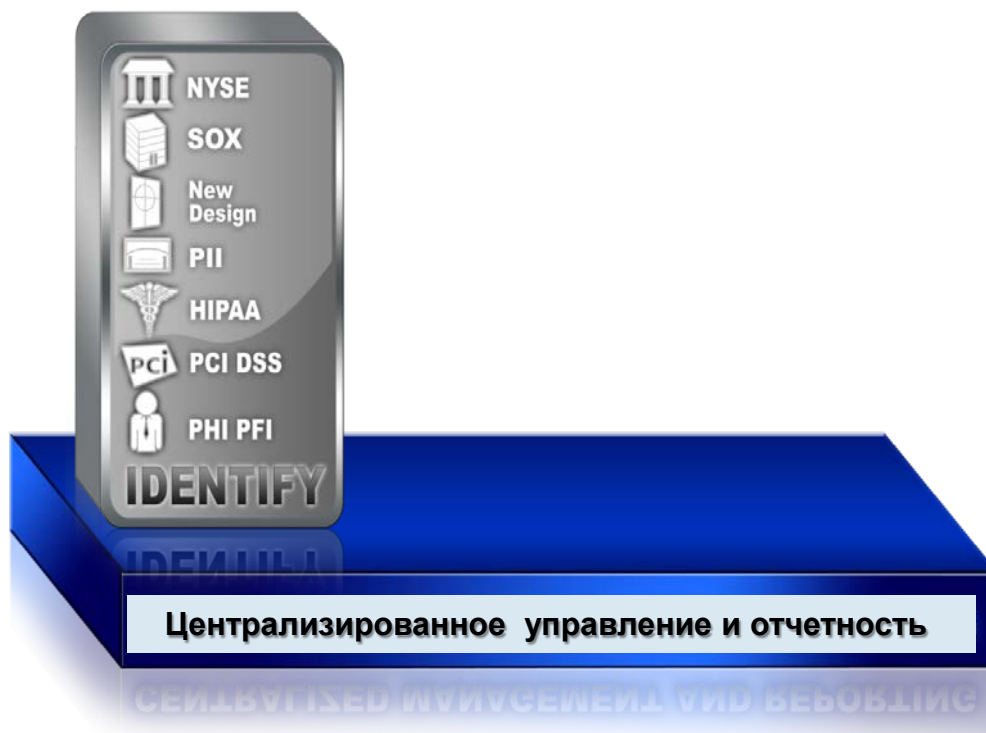
предотвращение утечек данных с компьютеров пользователей.



Websense DLP Solution

Идентификация

Модуль Data Discover



Точная идентификация - PreciseID



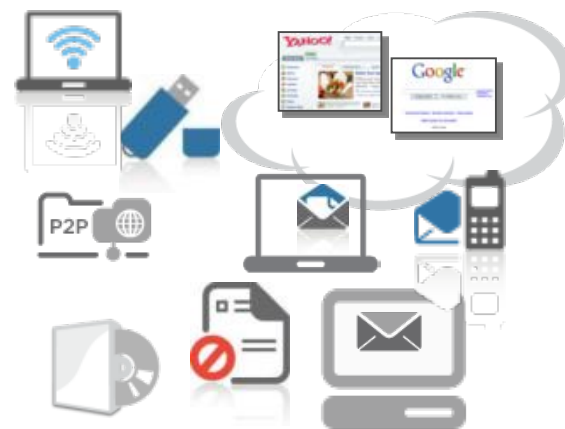
Цифровые отпечатки

Digital Fingerprints

Снятие с файлов одного или несколько «отпечатков» (хэш-функции).

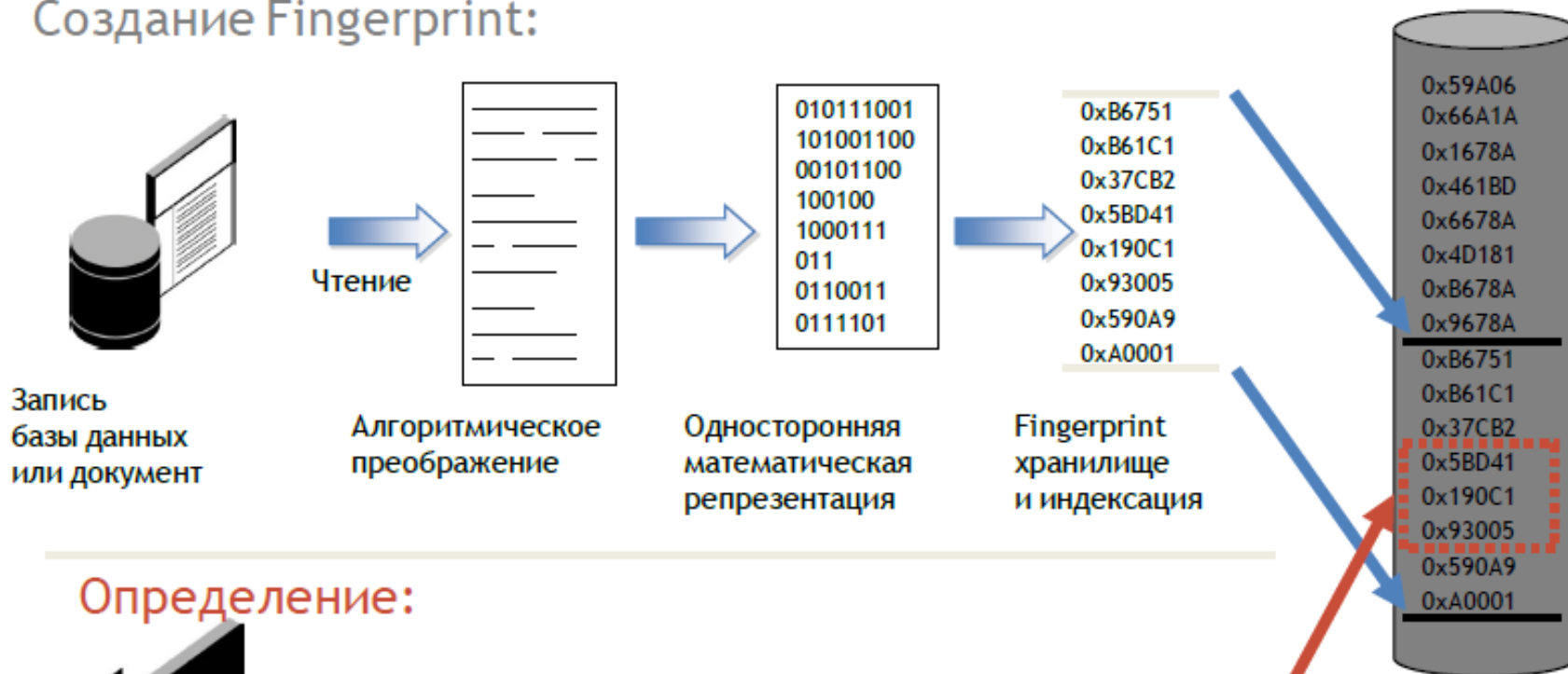
Отпечатки используются для:

- обнаружения защищенных документов в каналах передачи данных
- предотвращения не авторизованных действий с данными (пересылка, печать, копирование и пр.)

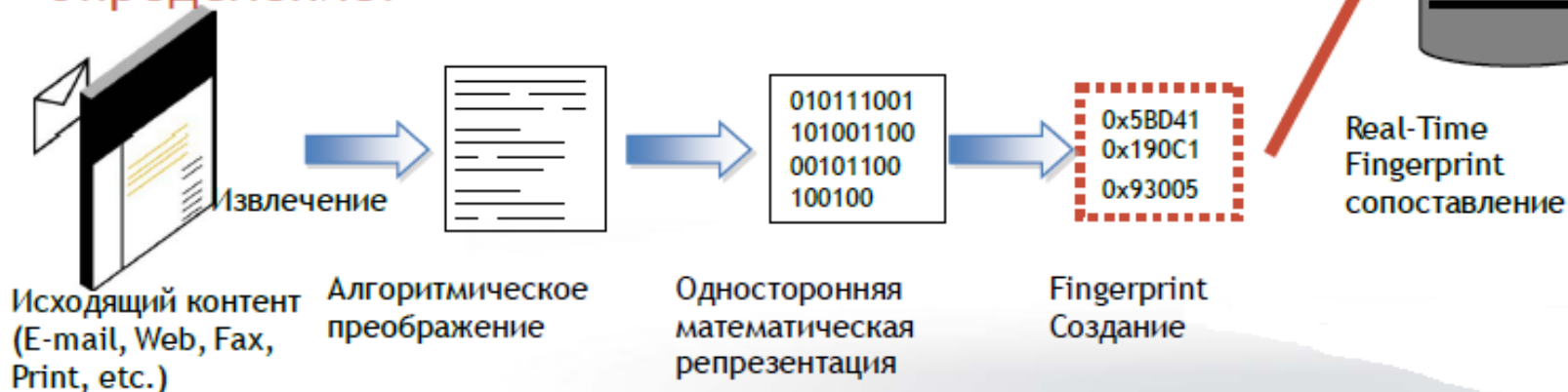


Цифровые отпечатки

Создание Fingerprint:



Определение:



Сценарий идентификации

- Понимание классификаторов
- Снятие отпечатков
- Сканирование одноразово и по расписанию:

Файловые хранилища

Базы данных

Microsoft SharePoint

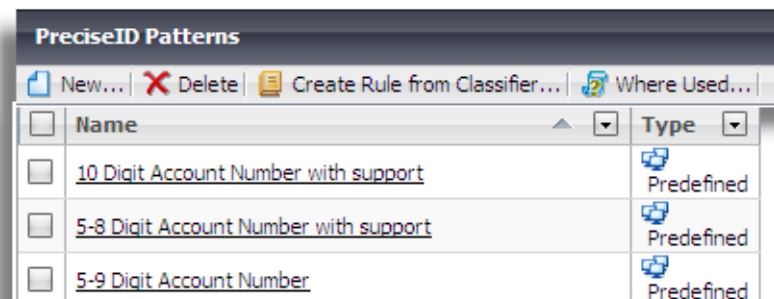
Microsoft Exchange и остальные mail сервера

- Создаем политики по сканированию и мониторингу данных **in rest**

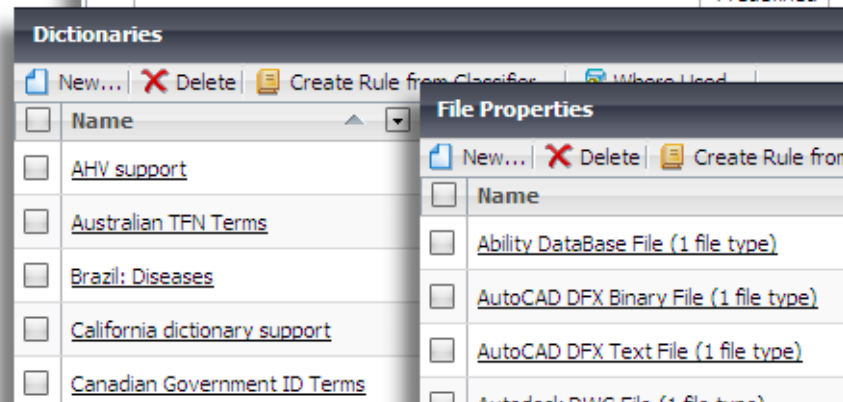


Контентная классификация

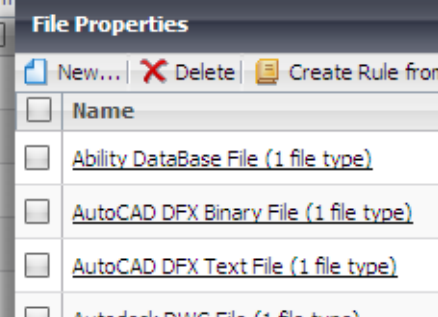
- Стандартные блоки идентификации
- Встроенные классификаторы
 - Образцы
 - Словари
 - Свойства файлов
- Расширение для создания собственных классификаторов



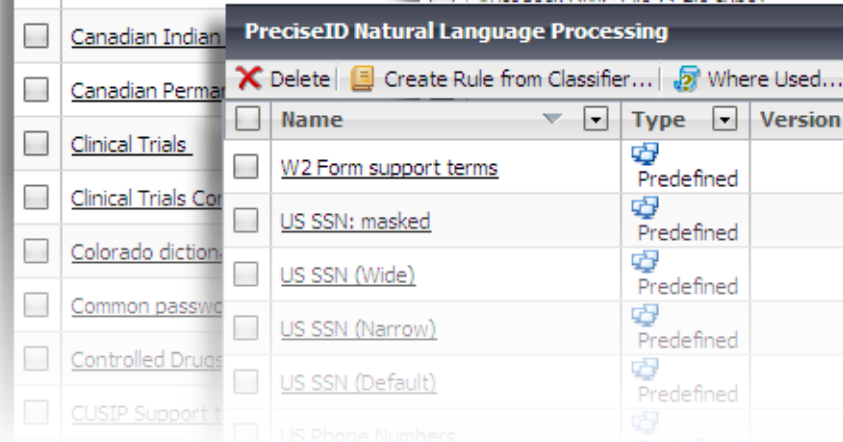
☐	Name	Type
☐	10 Digit Account Number with support	Predefined
☐	5-8 Digit Account Number with support	Predefined
☐	5-9 Digit Account Number	Predefined



☐	Name
☐	AHV support
☐	Australian TFN Terms
☐	Brazil: Diseases
☐	California dictionary support
☐	Canadian Government ID Terms
☐	Canadian Indian
☐	Canadian Perma
☐	Clinical Trials
☐	Clinical Trials Co
☐	Colorado dictio
☐	Common passwo
☐	Controlled Drugs
☐	CUSIP Support



☐	Name
☐	Ability DataBase File (1 file type)
☐	AutoCAD DFX Binary File (1 file type)
☐	AutoCAD DFX Text File (1 file type)
☐	Autodesk DWG File (1 file type)



☐	Name	Type	Version
☐	W2 Form support terms	Predefined	
☐	US SSN: masked	Predefined	
☐	US SSN (Wide)	Predefined	
☐	US SSN (Narrow)	Predefined	
☐	US SSN (Default)	Predefined	
☐	US Phone Numbers	Predefined	

Классификация

Информацию можно классифицировать:

- По произвольному количеству категорий (политик конфиденциального содержимого), определяемых как стандартными шаблонами, так и администратором.
- По уровню критичности инцидента (низкий, умеренный, высокий)
- По любым другим атрибутам инцидента (например, имя и расширение файла, владелец файла, тип АРМ (стационар/ноутбук), и т.д.)

Websense DLP Solution

Мониторинг

Модуль Data Monitor



Monitor

- Более 1000 правил, политик, расширений
- Встроенные шаблоны для типовых данных и регулирования класса конфиденциальности
- Шаблоны соответствия региону и сферы деятельности

The screenshot displays two overlapping windows from the 'Monitor' application. The 'Regions' window, in the background, is titled 'Regions' and contains the instruction 'Select the geographical regions to include in your template preferences:'. It features a tree view with the following options: USA (checked), Canada (checked), Europe (unchecked), Middle East (unchecked), Africa (unchecked), APAC (Asia and Pacific) (checked), and CALA (Central and Latin America) (checked). Under CALA, there are sub-options: Brazil (checked), Mexico (checked), and Other (checked). To the right of the tree is a faint world map. The 'Industries' window, in the foreground, is titled 'Industries' and contains the instruction 'Select the industries to include in your template preferences:'. It lists various industries with checkboxes: Finance and Banking (checked), Insurance (checked), Manufacturer (unchecked), Software (unchecked), Hardware (unchecked), Telco (unchecked), Transportation (unchecked), Healthcare and Pharma (checked), Retail (unchecked), Government (unchecked), Energy and Infrastructure (unchecked), Educational (checked), Entertainment and Media (checked), and Other (checked).

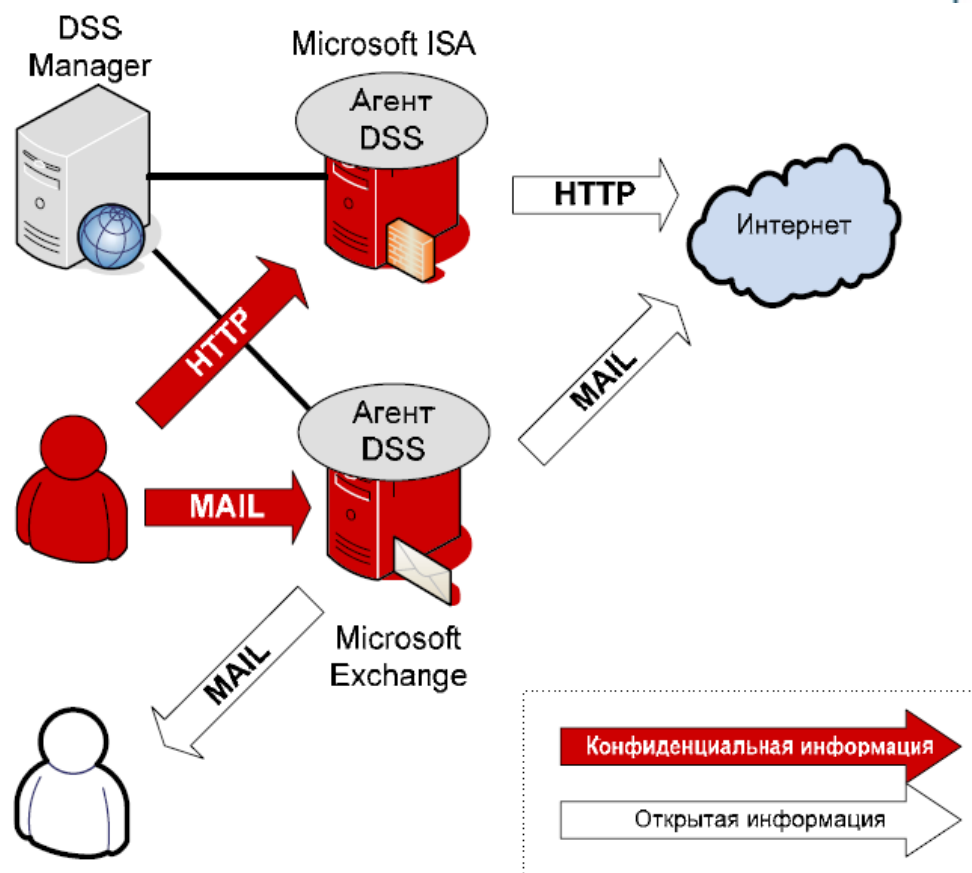
Гибкость политик

- Политика может быть применена к одному каналу коммуникации, многократным каналам или ко всем каналам
 - Web
 - Сетевой принтер
 - Локальный принтер
 - USB
 - LAN Storage
 - CD Burning Apps
 - Email
 - Endpoint Apps
 - Browser
 - CD Burning Apps
 - FTP
 - Instant Messenger
 - P2P Apps

Контроль каналов утечки

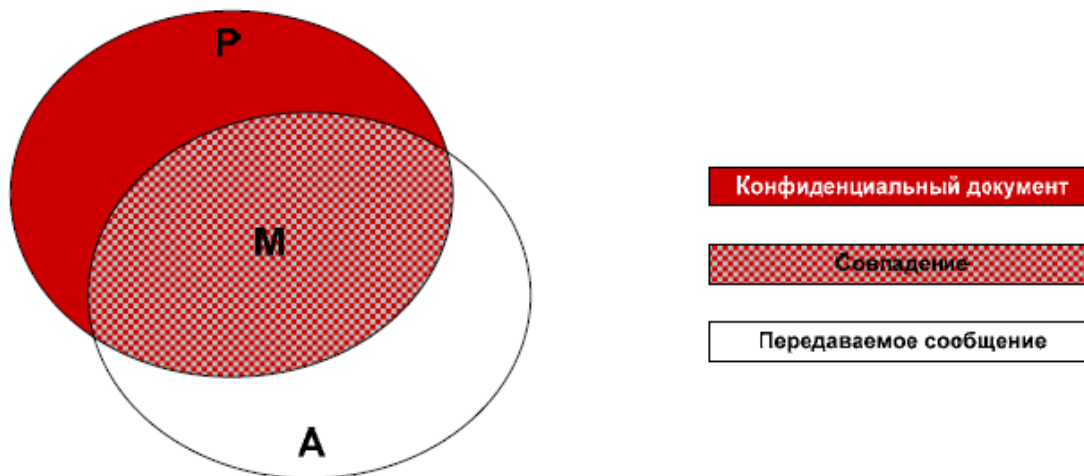
- Все основные каналы утечки, в том числе HTTP, SMTP, FTP, IM (AOL, MSN, Yahoo, ICQ);
- Сетевые принтеры, OCR модуль
- HTTPS (перешифрация сообщений, атака типа man-in-the-middle)
- Контроль «на лету» операций PrintScreen и Copy-Paste
- Контроль сменных носителей, запущенных приложений.

Пример схемы



Примеры срабатывания условий:

- ❑ Сообщение содержит почти весь конфиденциальный документ и много незначущего текста.
- ❑ Почти все сообщение состоит только из одной страницы конфиденциального документа.
- ❑ Сообщение содержит несколько страниц конфиденциального документа и много незначущего текста.



Websense DLP Solution

Мониторинг

Модуль Data Protect



План действий

- Определение действия при нарушении правила
 - Отдельное реагирование для каждого канала
- Определение действий на основе уровня нарушения

The screenshot shows a configuration window titled 'Data Usage'. Inside, there is a section 'Select an action for each channel:' followed by two columns of dropdown menus. The left column lists channels: Email, FTP, Chat, HTTP/HTTPS, Plain text, and Network Printing. The right column lists endpoint-related actions: Endpoint HTTP/HTTPS, Endpoint application, Endpoint removable media, Endpoint LAN, and Endpoint printing. Each dropdown menu contains a list of possible actions, with 'Permit' being the selected action for most channels.

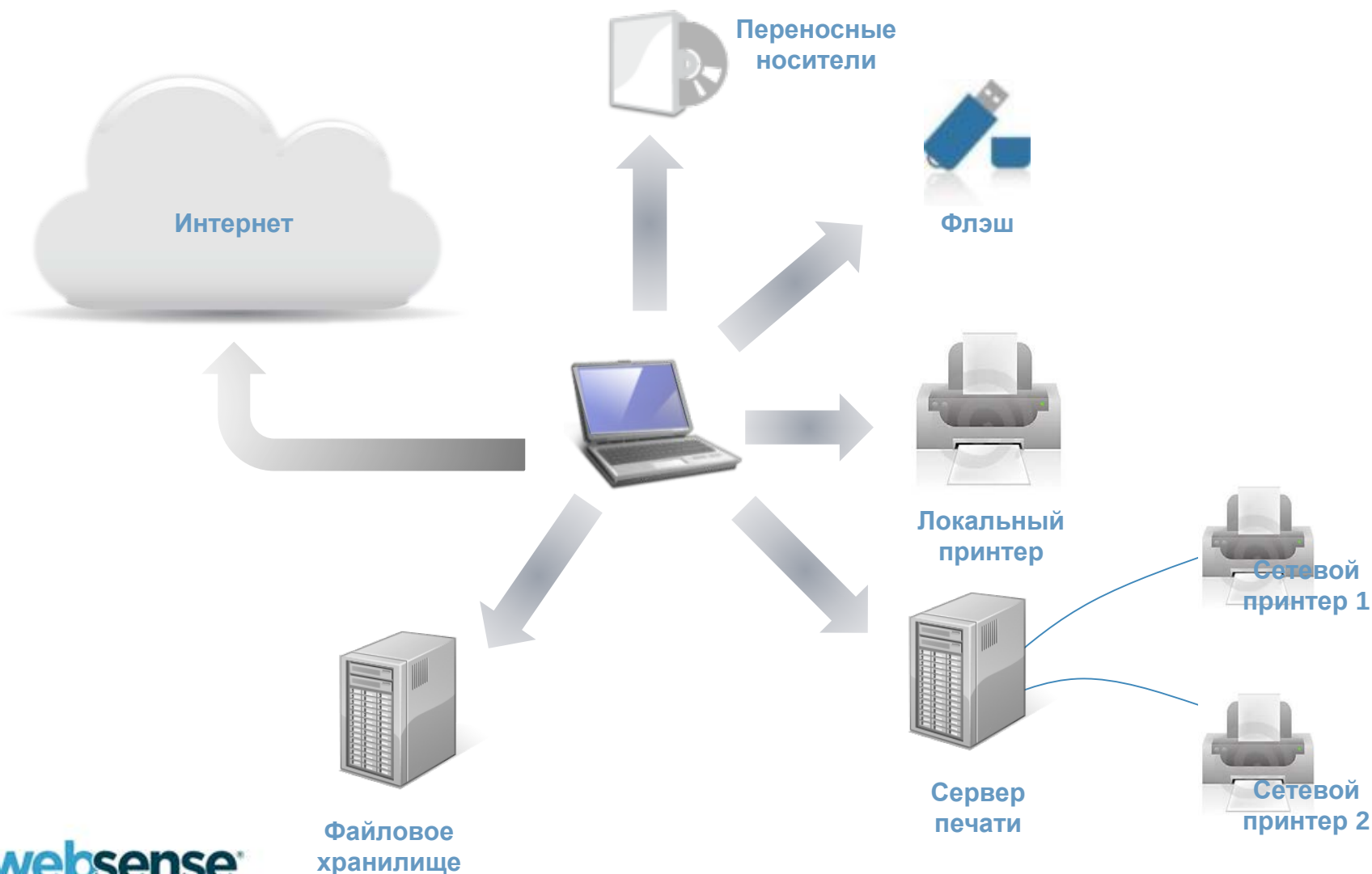
Channel	Action
Email	Quarantine
FTP	Block
Chat	Always permitted
HTTP/HTTPS	Permit
Plain text	Always permitted
Network Printing	Block
Endpoint HTTP/HTTPS	Block
Endpoint application	Confirm
Endpoint removable media	Encrypt
Endpoint LAN	Confirm
Endpoint printing	Permit

* Severity is user-defined based on number of matches

Защита данных на основе мониторинга и идентификации

- Встроенные действия доступны для каналов
 - Разрешить
 - Блокировка
 - Подтверждение
 - Карантин
 - Шифрование
 - Карантин и шифрование при выходе
- Кто может совершать действия
- Какие действия
- В какое время

Защита конечных точек: Data Endpoint



Endpoint DLP

Реализация функционала на рабочей станции

- Идентификация
- Мониторинг
- Защита

Основные задачи:

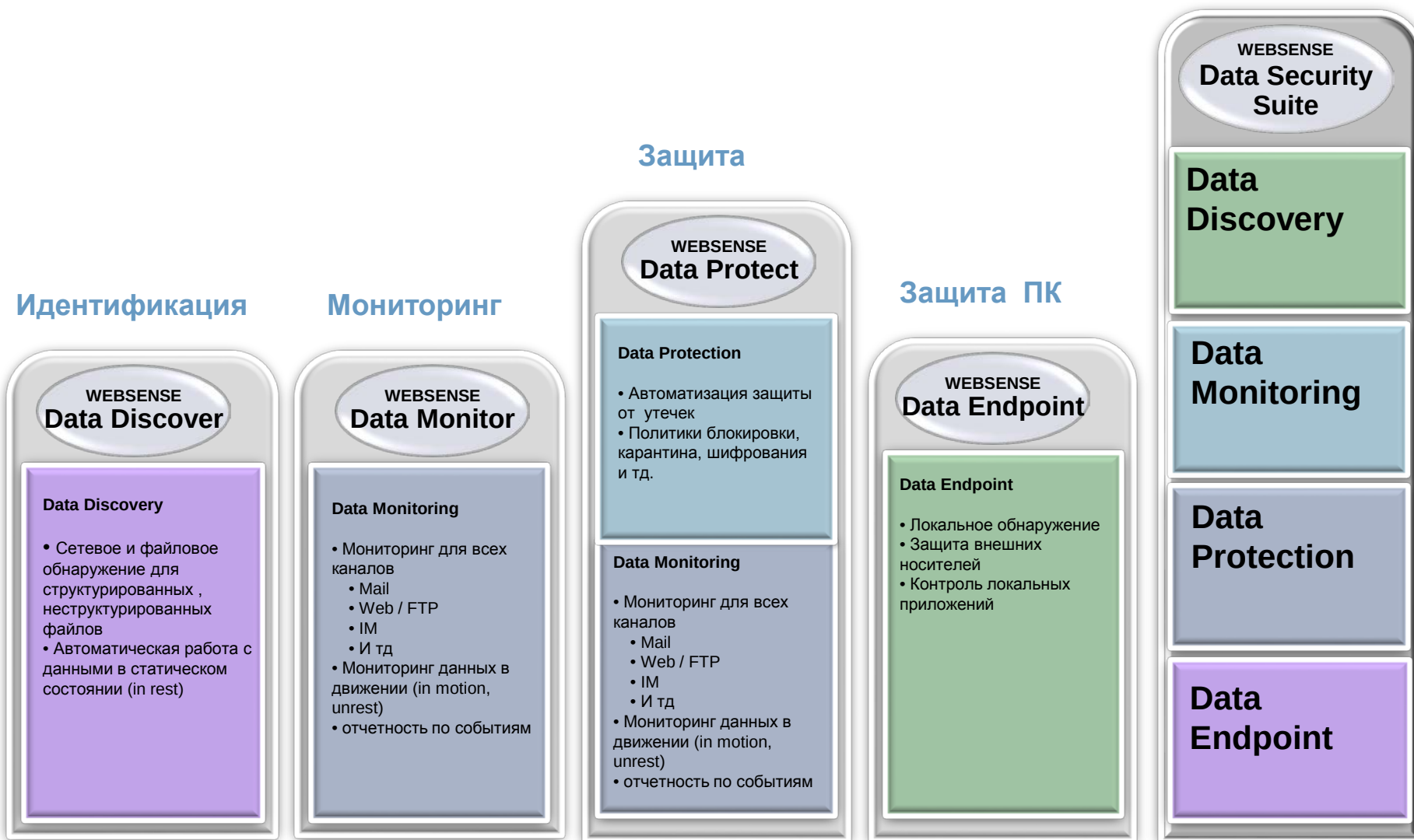
- Буфер обмена
- Работа с мобильными станциями
- Взаимодействие с сетевым DLP по работе с каналами



Управление предотвращением утечки: схема

Кто	Что	Куда	Как	Действие
Отдел кадров	Исходный код	Поставщик услуг	Файл Трансфер	Аудит
Обслуживание клиентов	Бизнес План	Web Storage	Web	Блокировка
Маркетинг	Информация о клиенте	Бизнес партнер	Интернет Мессенджер	Подтверждение
Финансы	M&A Планы	Блог	Peer-to-Peer	Перемещение
Бухгалтерия	Зарплата	Клиент	Электронная почта	Шифрование
Продажи	Финансовые отчеты	Spyware Сайт	Печать	Карантин
Дирекция	Продуктовая линейка	USB	Внешние носители	Подтверждение
Техническая поддержка	Тех. документация	Конкурент	Print Screen	
Инженеры	Инф. о конкурентах	Аналитики	Copy/Paste	

Варианты внедрения



Решение для любой задачи

	Web DLP	Data Monitor	Data Protect	Data Endpoint	Data Discover	Data Security Suite
Data идентификация	●	●	●	●	●	●
Централизованное управление	●	●	●	●	●	●
Уведомление	●	●	●	●	●	●
WEB Мониторинг	●	●	●	●		●
Защита WEB	●		●	●		●
EMAIL Мониторинг		●	●			●
Защита EMAIL			●			●
Загрузки WEB				●		●
Защита внешних LAN				●		●
Контроль внешних устройств				●		●
Контроль приложение				●		●
Обнаружение на конечных точках				●		●
Обнаружение в сети					●	●

Triton Enterprise

TRITON Enterprise:

- Websense Web Security Gateway
- Websense Data Security Suite
- Websense Email Security Gateway

Выгоднее, чем
WSG + DSS отдельно

Комплексное
решение

Web
Security

Data
Security

Email
Security

Сценарий сотрудничества в сделке

- Презентация,
Демонстрация
- Пилотный проект
- Специальные условия



Спасибо!

