

WEBSense TRITON APX ОБЗОР КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ

Роман Ванерке

Руководитель отдела технических решений
ЗАО «ДиалогНаука»

05 мая 2015 года

- Актуальные проблемы ИБ
- Общее описание Websense TRITON APX
- Возможности Websense AP-WEB
- Возможности Websense AP-DATA

Ландшафт угроз меняется



Целенаправленные атаки



Кража данных



Расследование

7 Stages of Advanced Threats

1

Recon



2

Lure



3

Re-
direct



4

Exploit
Kit



5

Dropper
File



6

Call
Home



7

Data
Theft



Новые требования ИБ



Защита от целенаправленных атак



Защита от кражи данных



Дашборд по угрозам / Оповещение
в зависимости от уровня угрозы



Отчетность и расследование /
Интеграция с SIEM

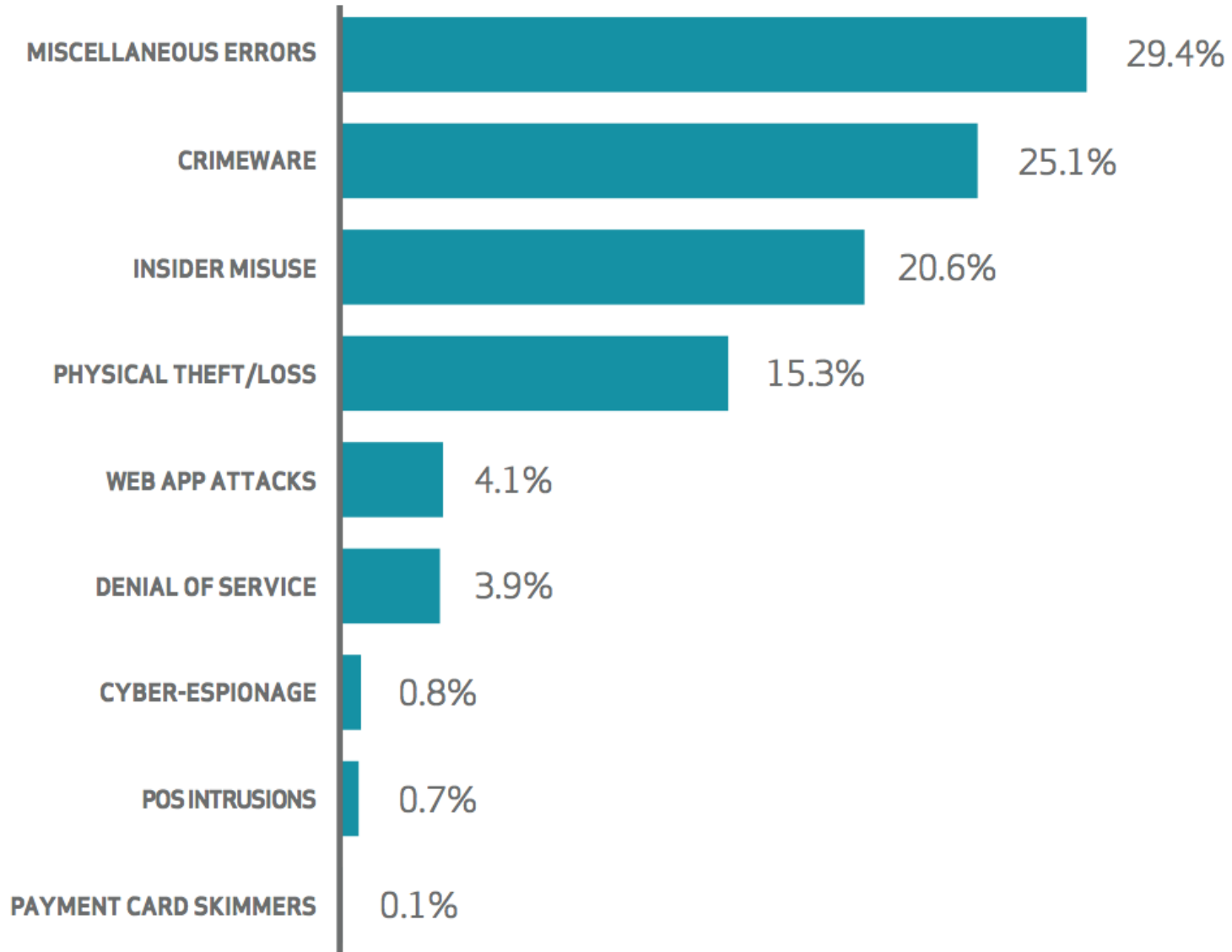


Расширенные возможности по
анализу угроз



Производительность и доступность

Дополнительно можно отметить



- Смена названия
- Более гибкое лицензирование
 - например, если раньше была лицензия WSGA, которая включала «облачный» сервис, то теперь это AP-WEB+AP-CLOUD
- Гибкие возможности по развитию системы
 - Сперва только защита от веб-угроз
 - Затем добавление защиты от утечек для веба
 - Затем интеграция с облаком

Архитектура TRITON APX



AP-WEB

- ✓ Advanced Threats
- ✓ Data Theft & Loss
- ✓ Threat Dashboard
- ✓ Malware Sandbox
- ✓ Forensic Reports
- ✓ Forensic Data
- ✓ SSL Inspection
- ✓ Social Media
- ✓ App Controls
- ✓ Video Controls
- ✓ Hybrid Solution

AP-EMAIL

- ✓ Spear-Phishing
- ✓ URL Sandboxing
- ✓ Advanced Threats
- ✓ Data Theft & Loss
- ✓ Anti-Spam
- ✓ TLS Encryption
- ✓ Advanced Encrypt.
- ✓ Cloud Archiving
- ✓ Image Analysis
- ✓ Cloud Cleansing
- ✓ Hybrid Solution

AP-DATA

- ✓ Content Aware DLP
- ✓ Data Discovery
- ✓ DLP Gateway
- ✓ DLP Endpoint
- ✓ MacOS & Windows
- ✓ Off-Network Prot.
- ✓ Portable Decrypt.
- ✓ 1,700+ Policy/Temp.
- ✓ Drip DLP Detect.
- ✓ OCR of Image Text
- ✓ Geo-Location





WEBSENSE AP-WEB

Контроль использования ресурсов сети Интернет и сетевых протоколов, защита от веб-угроз в реальном времени

Анализ в реальном времени



WebSense ACE



- **Механизмы анализа угроз в реальном времени**
 - Безопасность, данные, контент
 - Более 10000 различных классификаторов
- **Три движка Anti-Malware**
 - Коммерческий AV
 - Эвристический анализ
 - Вредоносные PDF
- **Защита от фишинга, репутационный анализ, анализ ссылок**
- **Composite Scoring Model**
- **Behavioral Analytics**

Примеры классификаторов АСЕ

- Advanced Malware Payloads ←
- Potentially Exploited Documents ←
- Mobile Malware ←
- Criminal Encrypted Uploads →
- Files Containing Passwords →
- Advanced Malware Command & Control →
- Unauthorized Mobile Marketplaces →
- OCR (Optical Character Recognition) →
- «Капельный» DLP →
- Geo-Location →

Анализ входящего трафика

Анализ исходящего трафика

**Анализ исходящего трафика
в части утечек**

- Определение вредоносного кода в коде веб-страниц (Flash, Silverlight, другие)
- RTSS анализирует веб-страницу в режиме реального времени
- Оценка уровня угрозы
- ACE использует различные технологии одновременно: RTSS для URL, репутацию, RTCC, сигнатуры и другие для выявления 0-day угроз!



Real Time Content Classification (RTCC)

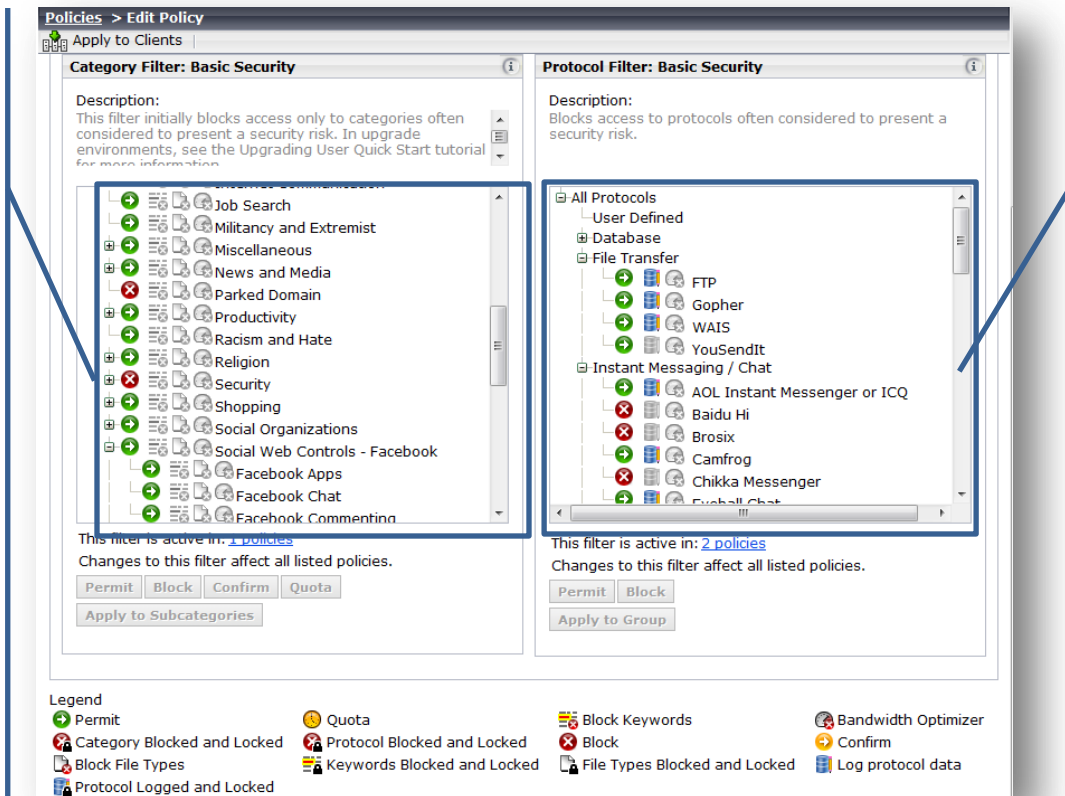


Это все сайты, отнесенные к категории «Социальные сети»?

Websense анализирует реальную информацию (контент) на странице и проводит классификацию внутри категории «Социальные сети»

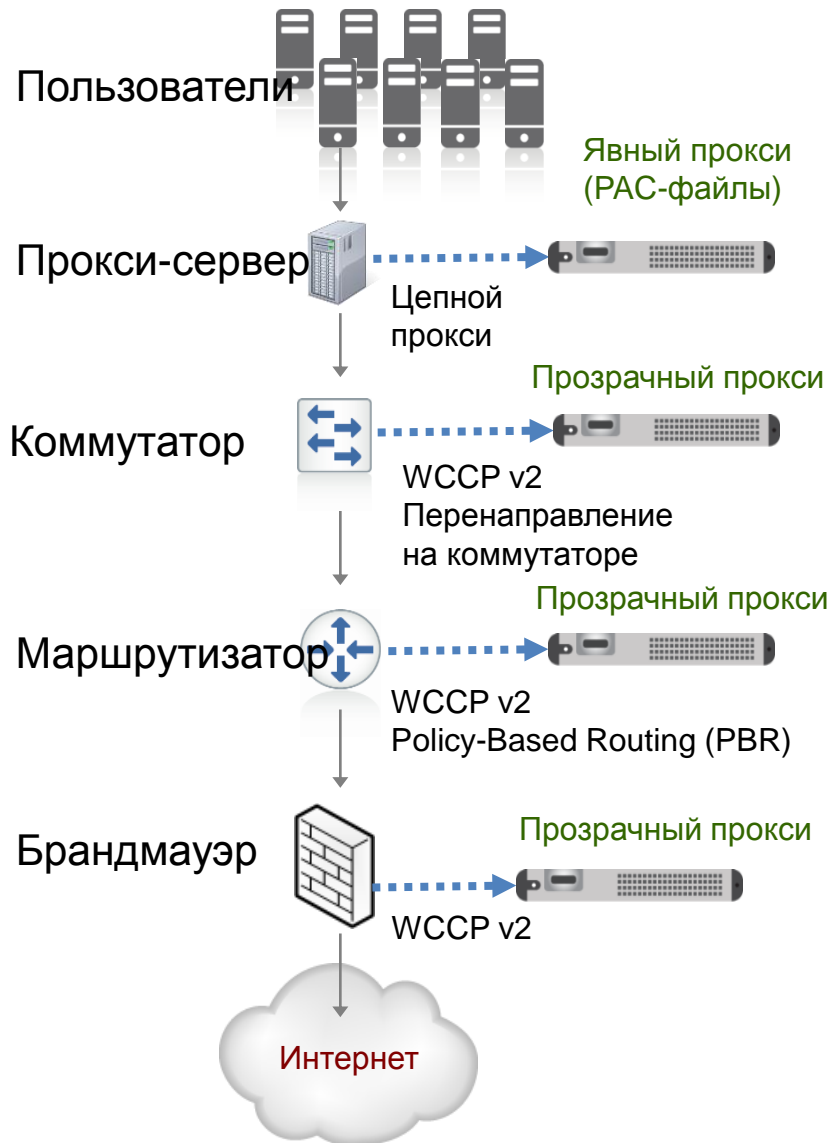
Тонкая настройка политик

- 120 различных категорий
- Тонкое управление доступом к социальным сетям
- Простое создание политик



- Более 100 различных приложений
- Включая управление видео
- Инспекция SSL

Варианты развертывания



Явный прокси-сервера

- Хорош для заказчиков, использующих GPO, SMS или WPAD-файл
- Не затрагивает сетевую инфраструктуру

Цепочка прокси-серверов

- Трафик направляется с имеющегося прокси-сервера
- Не затрагивает пользователей

Прозрачный прокси-сервера

- Трафик направляется с коммутатора, маршрутизатора или брандмауэра
- Не затрагивает пользователей

WEBSENSE AP-DATA

WebSense AP-DATA



AP-WEB

The **most effective** anti-malware protection from **advanced threats** and **data theft**.

AP-EMAIL

The **most advanced** email defenses against **blended** and **targeted attacks**.

AP-DATA

- ✓ Content Aware DLP
- ✓ Data Discovery
- ✓ DLP Gateway
- ✓ DLP Endpoint
- ✓ MacOS & Windows
- ✓ Off-Network Prot.
- ✓ Portable Decrypt.
- ✓ 1,700 Policy/Temp.
- ✓ Drip DLP Detect.
- ✓ OCR of Image Text
- ✓ Geo-Location

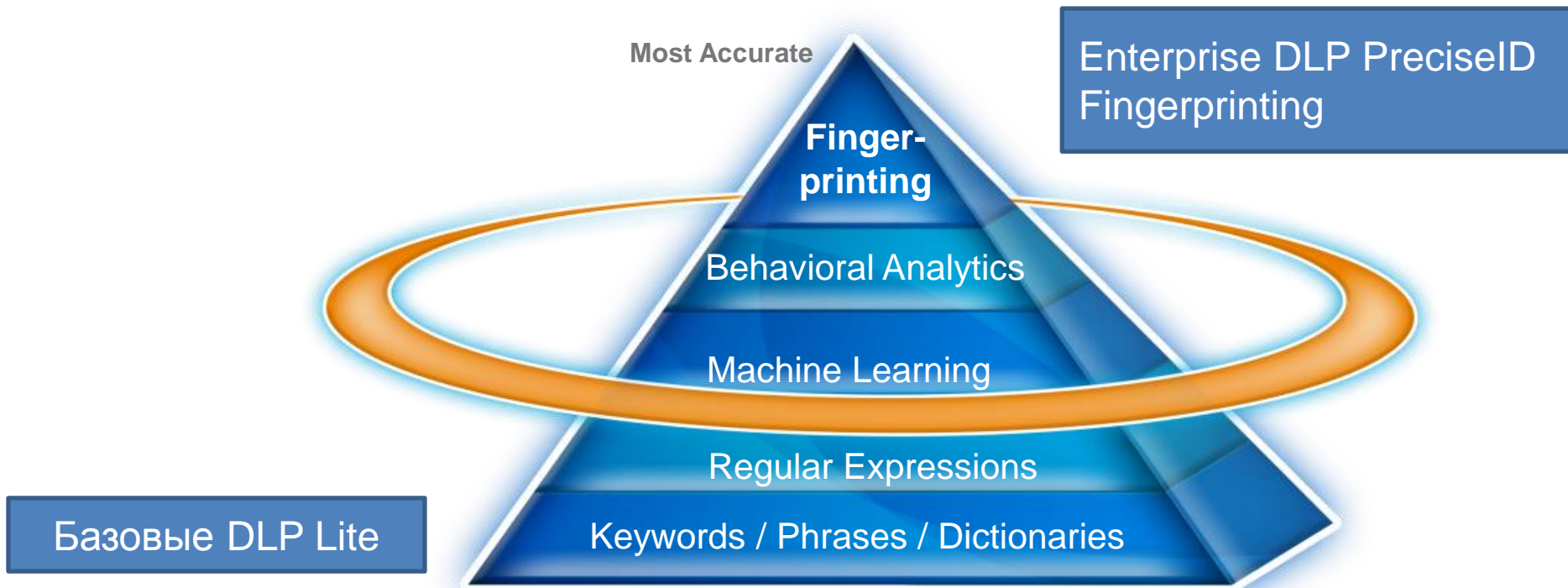


Подход к анализу

Кто	Что	Куда	Как	Действие
Отдел кадров	Исходный код	Поставщик	Передача файла	Аудит
Клиентская служба	Бизнес план	Персональный веб сайт	Web	Блокирование
Маркетинг	ПДн	Бизнес партнер	ICQ, Skype	Оповещение
Финансовый отдел	Слияния и поглощения	Блог	Peer-to-Peer	Удаление
Бухгалтерия	Информация о ЗП	Покупатель	Email	Шифрование
Отдел продаж	Финансовая отчетность	Вредоносный сайт	Печать	Карантин
Юридический отдел	Договора	USB	Съемные устройства	Подтверждение
Техподдержка	Техническая документация	Конкурент	Print Screen	
Инженеры	Результаты сравнений	Аналитик	Копирование/вставка	

Технология выявления утечек

- Кирпичик для создания политики
- Классификаторы определяют данные для защиты
- Высокая точность



Цифровые отпечатки

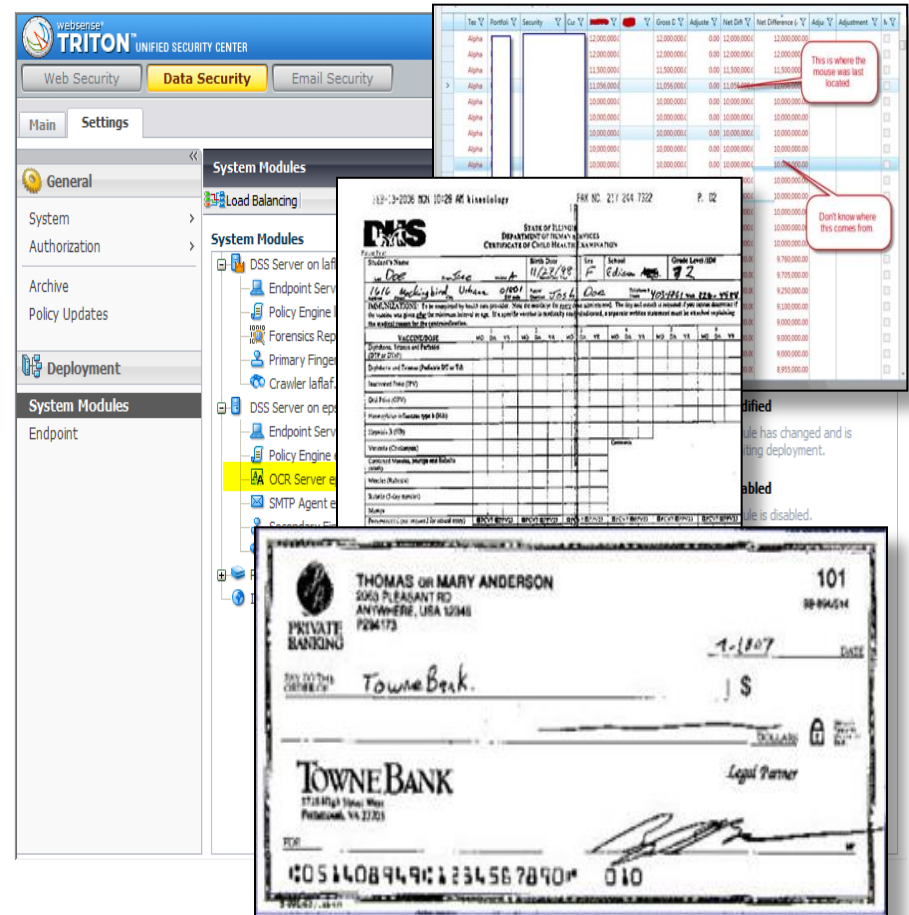
- Цифровые отпечатки:
 - Баз данных
 - Сетевых каталогов
 - SharePoint \ Lotus Domino
 - другие



- Подключение к базе данных через ODBC
- Снятие цифровых отпечатков непосредственно с БД
- Данные не покидают БД
- Инкрементальные обновления базы отпечатков при росте исходной базы

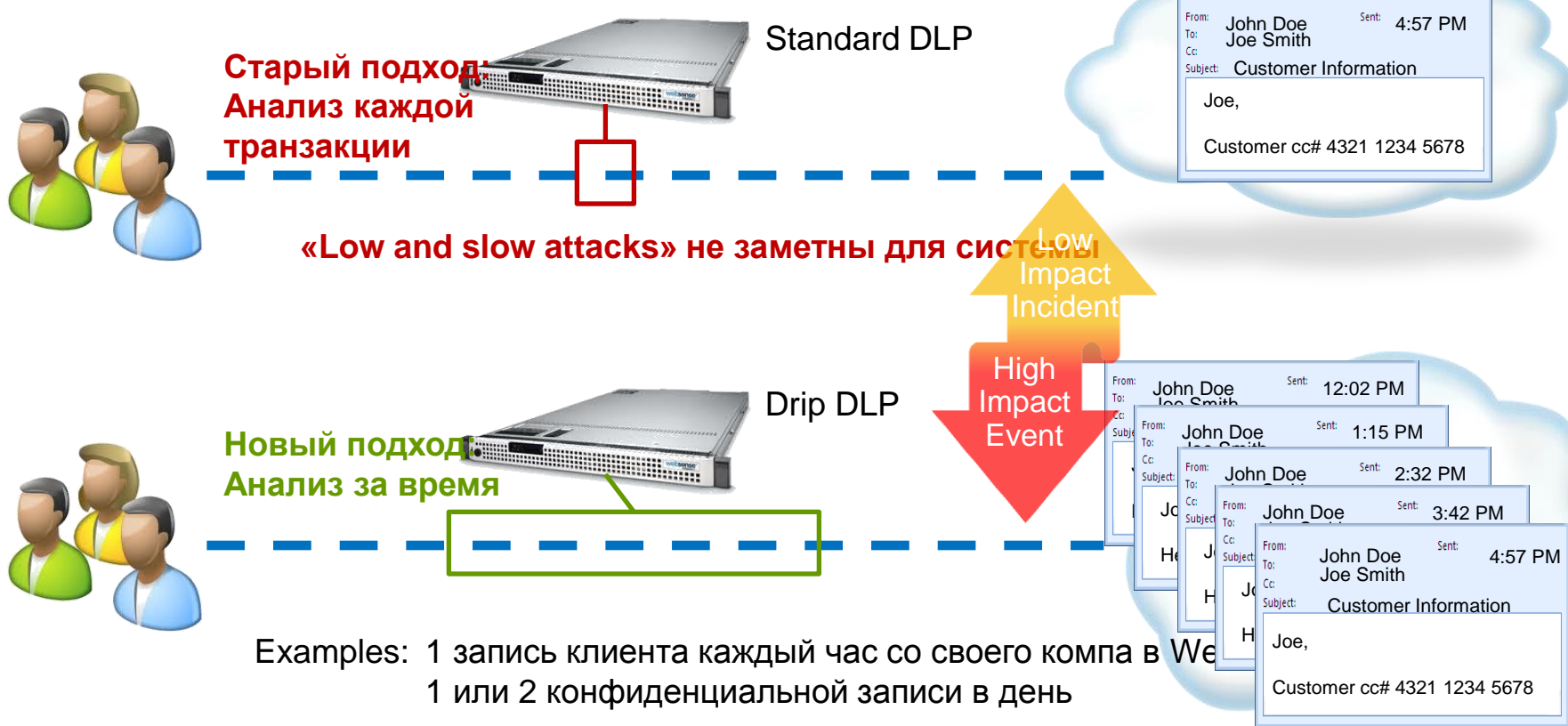
Распознавание текста (OCR)

- Используется механизмы оптического распознавания
- Определение данных в изображениях
 - Скриншоты
 - Отсканированные документы
 - Факс
 - и т.п.
- Доступен для выявления утечек через веб, почты и в рамках поиска документов по сети



Капельные утечки (Drip DLP)

Первые на рынке



Анализ поведения

The screenshot displays the TRITON Unified Security Center interface. The main content area shows a 'Policy Library' with 227 policies. A callout bubble labeled 'Индикаторы риска' (Risk Indicators) points to the 'Data Theft Risk Indicators' folder. Another callout labeled 'Индикаторы компрометации' (Compromise Indicators) points to the 'Indicators of Compromise' folder. A third callout labeled 'Suspicious User Activity' points to the 'Suspicious User Activity' folder. A fourth callout labeled 'Описание поведения и правил' (Description of behavior and rules) points to the 'Policy: Data Sent During Unusual Hours' details panel on the right.

Name	Version
Acceptable Use	
Content Protection	
Data Theft Risk Indicators	
Employee Discontent	
Disgruntled Employee	Data Theft Risk Indicators 935838
Resume for HR	Data Theft Risk Indicators 929323
Resume for HR Cyrillic	Data Theft Risk Indicators 929323
Resume for HR Israel	Data Theft Risk Indicators 929323
Indicators of Compromise	
Encrypted files	Company Confidential and intellectual property, Data Theft Risk Indicators 929323
Malware communication detection	Data Theft Risk Indicators 935838
Password files	Password files, Data Theft Risk Indicators 929323
Suspected Malicious Dissemination	Data Theft Risk Indicators 929323
Suspicious User Activity	
Data Sent During Unusual Hours	Data Theft Risk Indicators 935838
Database Files	Data Theft Risk Indicators 929323
Email to Competitors	Data Theft Risk Indicators 929323
Password Dissemination	Data Theft Risk Indicators 929323
Suspected Mail to Self	Data Theft Risk Indicators 929323
Unknown File Formats Over Time	Data Theft Risk Indicators 929323
User Traffic Over Time	Data Theft Risk Indicators 929323
Regulations, Compliance and Standards	

Policy: Data Sent During Unusual Hours

Description: Detects data that is sent at an unusual time. You define what is considered an unusual time in the script classifier, Unusual Hours. Each rule in this policy targets a different type of data, such as office or archive files. Example: If you define working days in the classifier as Monday-Friday and unusual hours as 9pm-5am, then data sent on Saturday, Sunday, or during the working week between 9 p.m. and 5 a.m. triggers this policy.

Rules (enabled: 4, total: 4)

- Source Code C Family or Java Sent During Unusual Hours (935838)**
Detects source code (C family or Java) that is sent at an unusual time. You define what is considered a usual time in the script classifier, Unusual Hours. This rule uses lexical analysis of terms, patterns, and structures for optimal accuracy.
- Confidential in Header/Footer Sent During Unusual Hours (935838)**
Detects confidential documents whose header or footer information contains terms implying confidentiality or secrecy, in English or 20 additional languages, that are sent at an unusual time.
- Office Files Sent Over Time During Unusual Hours (935838)**
Detects office files that are sent at an unusual time. This is a cumulative rule that is triggered when more than 100 files are sent during a period of 1 hour. For example: Depending on how the classifier is configured, 20 spreadsheet files and 80 word processing files sent between 11 p.m. and 12 a.m. might trigger the rule.
- Archive Files Sent Over Time During Unusual Hours (935838)**
Detects archive files sent over time during unusual hours. This is a cumulative rule that is triggered when more than 100 files are sent during a period of 1 hour. For example: Depending on how the classifier is configured, 20 zip files and 80 RAR files sent between 11 p.m. and 12 a.m. might trigger the rule.

- Различные классификаторы
 - Регулярные выражения, ключевые слова, словари
- Более 1700 готовых политик «из коробки», в том числе для РФ
- Удобный мастер настройки политик
- Определяет типы данных например: ПДн, РСІ

Select the geographical regions to include in your policy preferences

- Africa
- APAC (Asia and Pacific)
- CALA (Central and Latin America)
- Canada
- Europe
- Middle East
- USA

Select the industries to include in your policy preferences

- Hardware
- Healthcare and Pharma
- Insurance
- Manufacturer
- Retail
- Software
- Telco
- Transportation
- Other

Rules (enabled: 7, total: 12)

- Public Company

- 1. Russia PII: Russia**
Rule for detecting Russian passport numbers, when appearing in proximity to spreadsheet files.
- 2. Russia PII: Russian passport and name**
 - 2.1 Russia PII: Russian passport and name (Wide) (908320) - Disabled**
Rule for detecting Russian passport number, when appearing in proximity to Russian full name. This rule is not selected by default.
 - 2.2 Russia PII: Russian passport and name (Default) (908320)**
Rule for detecting Russian passport number, when appearing in proximity to Russian full name.
 - 2.3 Russia PII: Russian passport and name (Narrow) (908320) - Disabled**
Rule for detecting Russian passport number, when appearing in proximity to Russian full name. This rule is not selected by default.
- 3. Russia PII: Russian Phone Numbers**
 - 3.1 Russia PII: Russian Phone Numbers (Wide) (908320) - Disabled**
Rule for detecting Russian phone numbers. This rule does not require support words or explicitly delimited notation.
 - 3.2 Russia PII: Russian Phone Numbers (Default) (908320)**
Rule for detecting Russian phone numbers. This rule requires support words or explicitly delimited notation.
 - 3.3 Russia PII: Russian Phone Numbers (Narrow) (908320) - Disabled**
Rule for detecting Russian phone numbers. This rule requires support words and explicitly delimited notation.
- 4. Russia PII: Russian Taxpayer Identification Numbers - 12-digits**
 - 4.1 Russia PII: Russian Taxpayer Identification Numbers - 12-digits (Wide) (908320) - Disabled**
Rule for detecting 12-digits Russian Taxpayer Identification Numbers (INN) used by individuals. The rule does not require proximity to support terms.

Полнота информации по инцидентам



Security Alert A

Данные: PCI & PII

Источник: 10.14.222.21

Канал: Web

Получатель: 93.10.219.62



Security Alert B

Данные: PCI & PII, customer database

Источник: Joe User x1234,
juser@company.com
Title: Associate
Dept: Finance
Manager: Jane Manager x1234,
jmanager@company.com

Канал: Web

Получатель: mail.google.com
Type: Personal webmail site
Location: Mountain View, CA

Отличительные возможности AP-DATA



Drip DLP

Detect suspicious
“low and slow”
movement of data

(e.g. 4 SSNs in
an hour or 1 credit
card number)



Finger Printing

PreciseID™

Hashing
approach to
Fingerprinting on
Mac OS, and
Microsoft endpoint
devices on and off
the network



OCR

Extract text from
images and
scanned
documents for
analysis

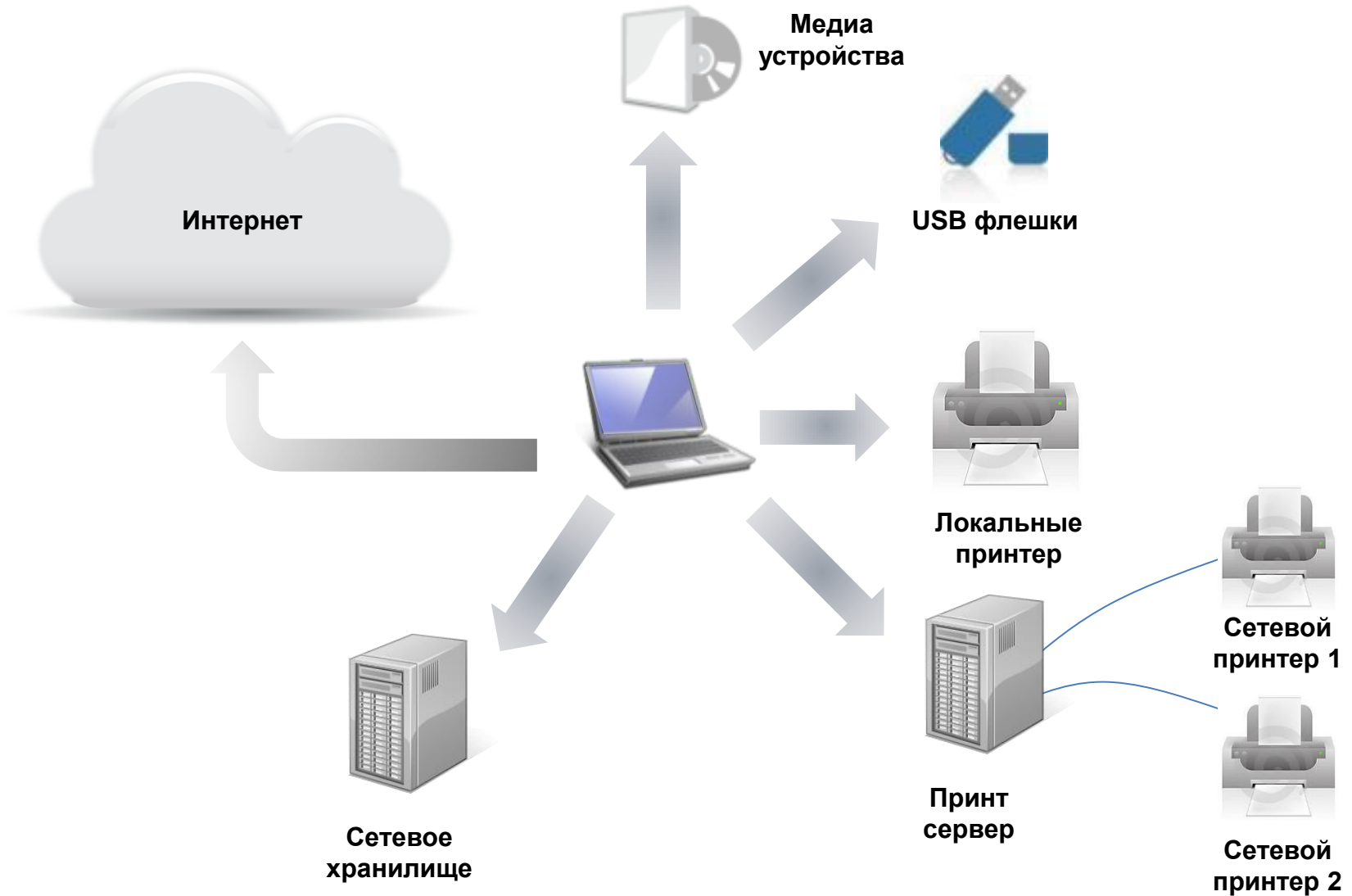
No other vendor
can do OCR for
data in motion!



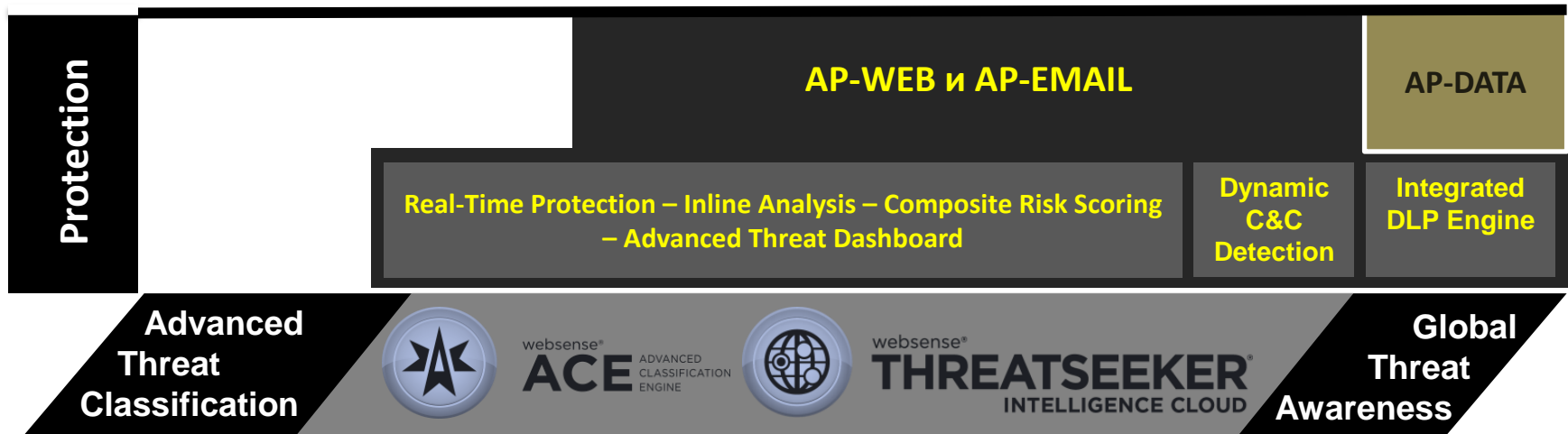
Behavioral Analytics

Predefined
policies looks at
sensitive content
and specific user
activity to identify
high risk
employee
behavior

Агент AP-Endpoint DLP



Как Websense APX защищает от АРТ

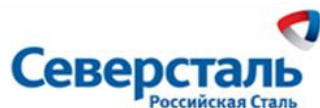


Ключевые клиенты Websense в РФ

Финансовый сектор



Промышленность



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

Телекоммуникации



- Комплексный подход к построению системы защиты
 - Более 90% утечек, согласно отчету Verizon, можно было предотвратить используя достаточно дешевые средства и способы защиты
- Руководство компании:
 - Минимизация финансовых потерь, репутационных рисков
 - Контроль нецелевого использования ресурсов Компании
- 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

Роман Ванерке

117105, г. Москва, ул. Нагатинская, д. 1, стр.1

Телефон: +7 (495) 980-67-76, ext.162

Факс: +7 (495) 980-67-75

<http://www.DialogNauka.ru>

e-mail: rv@DialogNauka.ru

