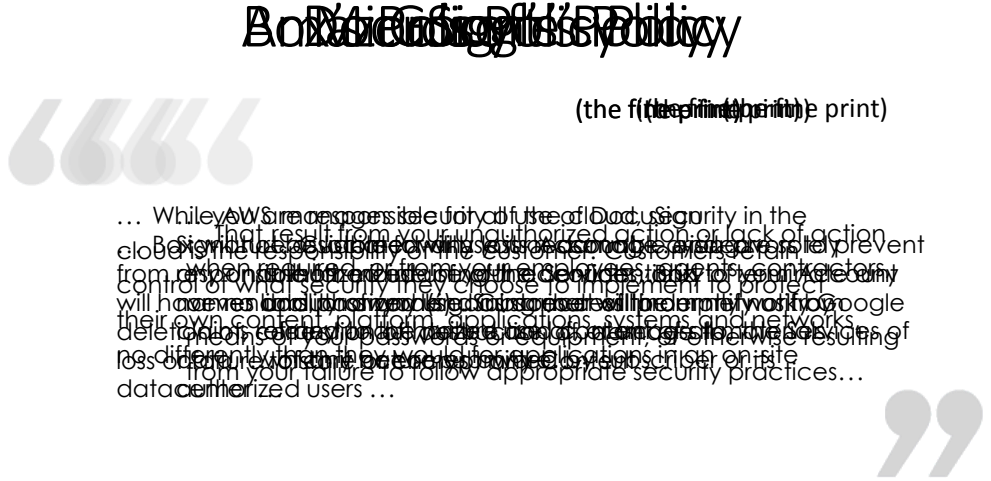
Blue Coat Cloud Security

Cloud Access Security Broker (CASB)

Павел Катунькин
Ведущий инженер, ВэбКонтрол

Кто отвечает за безопасность в облаке?

"95% нарушений безопасности в облаке будут вызваны ошибками пользователей"
- Прогноз Gartner на 2016



Цели провайдеров облачных приложений и Ваши цели не всегда совпадают

Внимания требует несколько предметных областей

Все облачные приложения

Аналитика и Мониторинг

ОБНАРУЖЕНИЕ И АНАЛИЗ ОБЛАЧНЫХ РИСКОВ, ПОЛЬЗОВАТЕЛЬСКАЯ АКТИВНОСТЬ И РАБОТА С ДАННЫМИ

Разграничение доступа

СОЗДАНИЕ ЕДИНОЙ ПОЛИТИКИ ДОСТУПА И УПРАВЛЕНИЯ ОБЛАЧНЫМИ ПРИЛОЖЕНИЯМИ

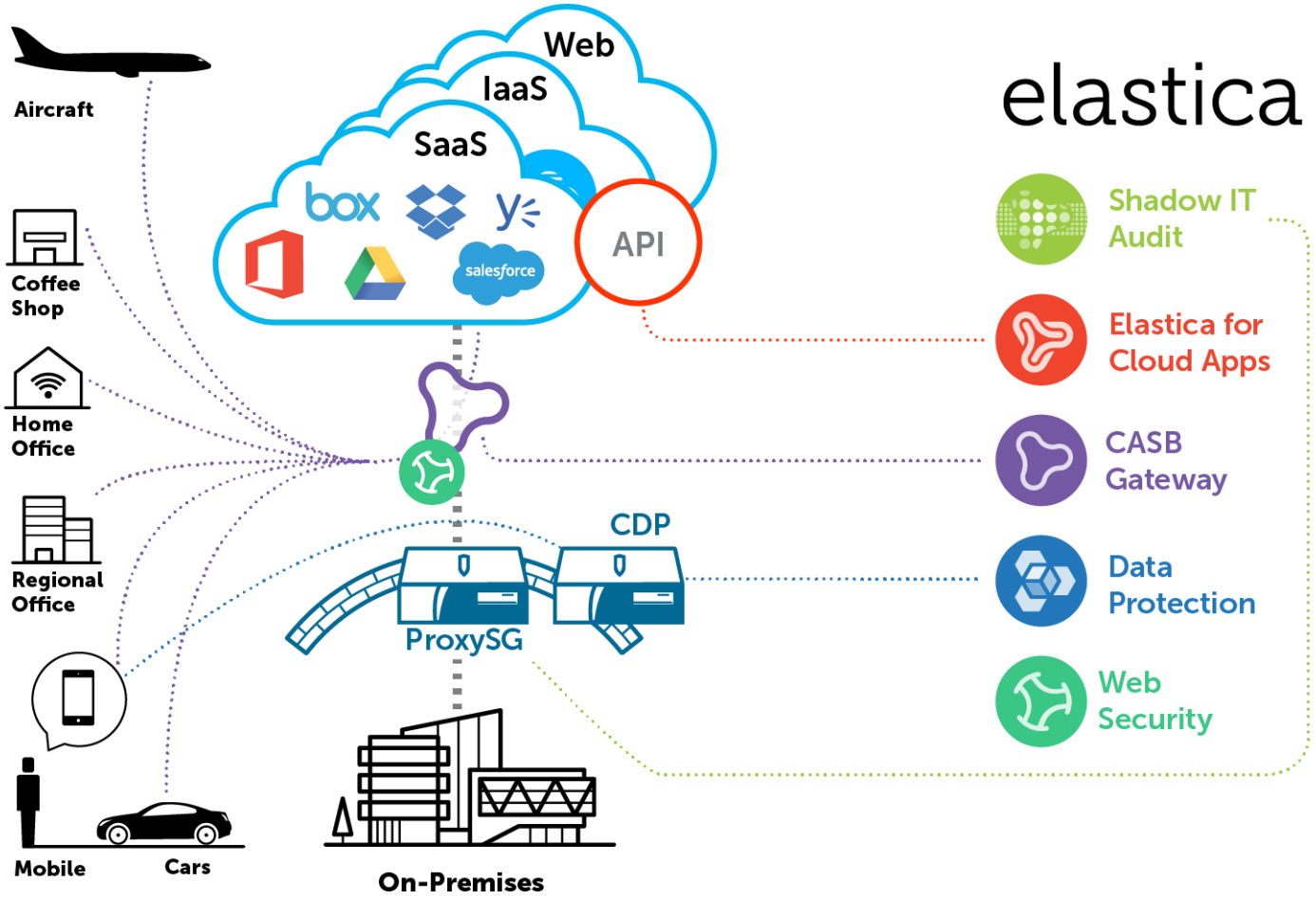
Защита данных

ОБЕСПЕЧЕНИЯ КОНТРОЛЯ ДАННЫХ В ПРОЦЕССЕ ПЕРЕДАЧИ, ХРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ

Защита от угроз

BLUE COAT

Защита созданная для облака



Elastica Cloud Security

Мониторинг Облачных приложений

Обнаружение «теневой» активности и мониторинг использования облачных приложений в реальном времени

Управление данными

Точное управление критичными данными

Защита данных

Шифрование и токенизация данных при передаче, хранении и использовании

Защита от угроз

Противодействие угрозе в ходе ее развития с использованием анализа поведения пользователей

Elastica Cloud Security

Мониторинг Облачных приложений

Обнаружение «теневой» активности и мониторинг использования облачных приложений в реальном времени

Управление данными

Точное управление критичными данными

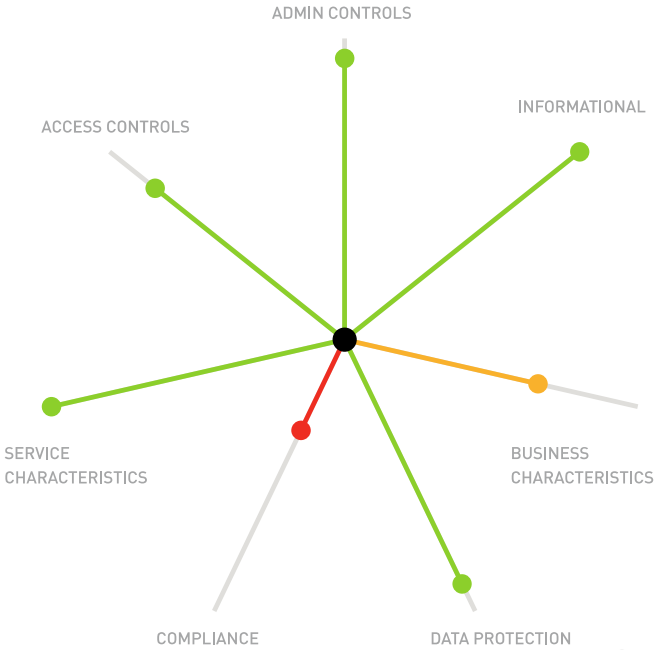
Защита данных

Шифрование и токенизация данных при передаче, хранении и использовании

Защита от угроз

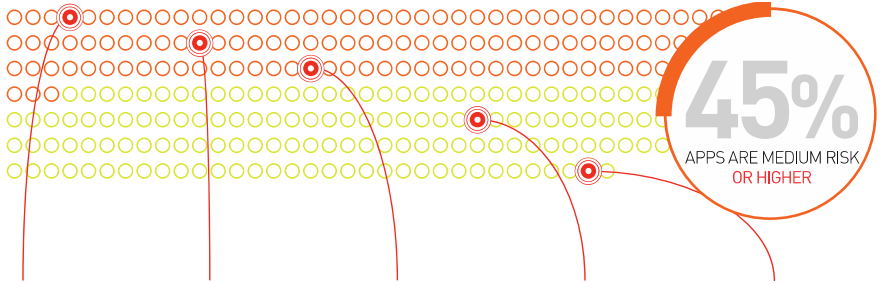
Противодействие угрозе в ходе ее развития с использованием анализа поведения пользователей

Анализ теневой активности



359 active users

273 apps



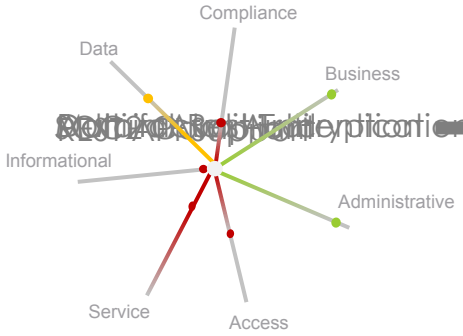
TOP 5 RISKIEST APPS

1	2	3	4	5
PERFECT MARKET	LIVERRAIL	ENSIGHTEN	ZEDO	GAUG.ES
Mountain View United States	Seattle United States	Santa Monica United States	Boston United States	San Jose United States

Elastica Audit

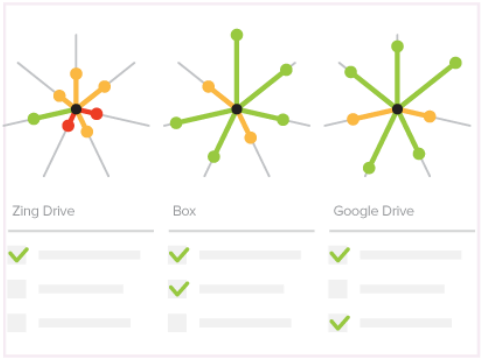
Определение приложений наилучших для вашей компании

- Оценка Business Readiness Rating основывающаяся на 70+ метриках разделенных на семь категорий
- Настройка приоритетов метрик для уточнения методики оценки под Вашу организацию
- Выполнение сравнительной оценки альтернативных приложений



Business Readiness Rating™

38



Усиление ProxySG функцией аудита теневой активности

Понимание **15,000+** приложений в ProxySG и MC

Shadow IT Audit

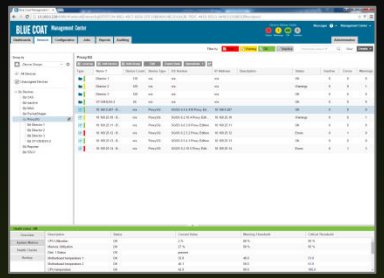
Analytics

App Rating Database

Audit – AppFeed

GIN / BCIS

Management Center



ProxySG

Не только обнаруживать Shadow IT Контролировать IT

App Controls

в ProxySG и MC на базе:

- Имена/группы приложений
- ‘Business Readiness Rating’ для каждого приложения.
- Risk Score приложение получает основываясь на 80+
- Risk Attributes относящимся к каждому типу приложений

Elastica Cloud Security

Мониторинг Облачных приложений

Обнаружение «теневой» активности и мониторинг использования облачных приложений в реальном времени

Управление данными

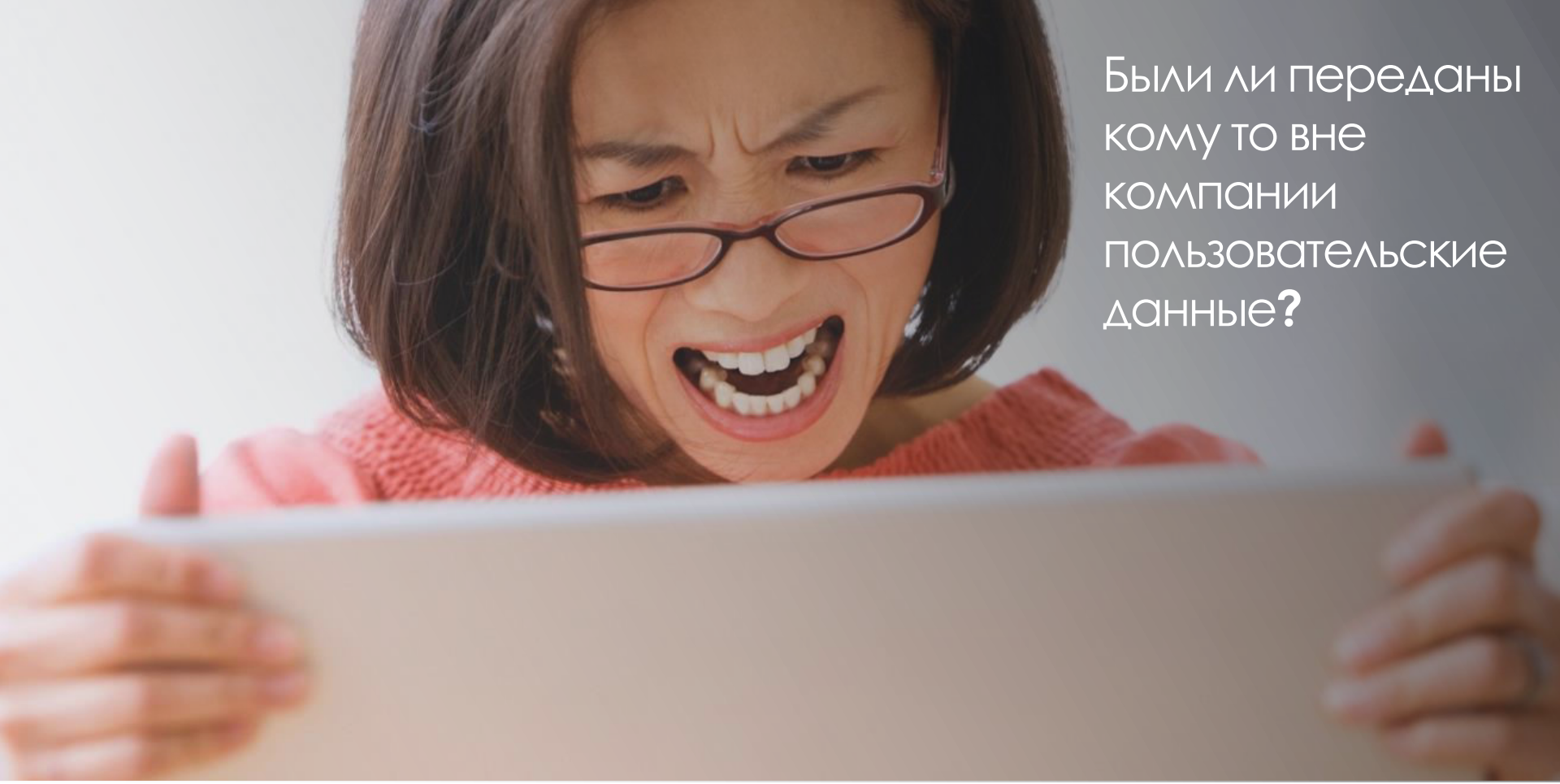
Точное управление критичными данными

Защита данных

Шифрование и токенизация данных при передаче, хранении и использовании

Защита от угроз

Противодействие угрозе в ходе ее развития с использованием анализа поведения пользователей



Были ли переданы кому то вне компании пользовательские данные?

Все организации подвержены риску **теневой** передачи данных

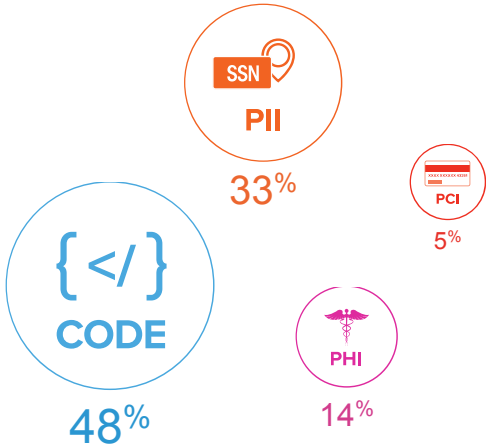
26%

Файлов пользователя находятся в широком доступе (в среднем)

Из этих файлов

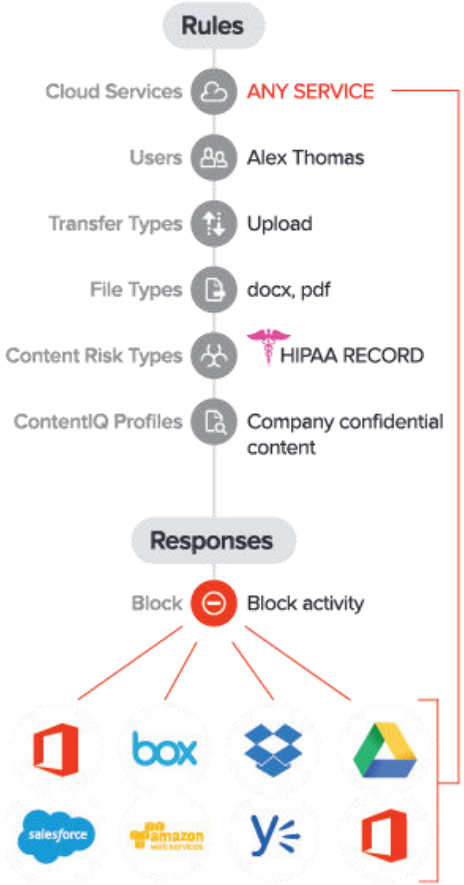
10%

содержат конфиденциальную информацию



Классификация данных и их защита

ContentIQ™



Автоматическая классификация, обнаружение и устранение нарушений при загрузке в облачные приложения используя семантический анализ

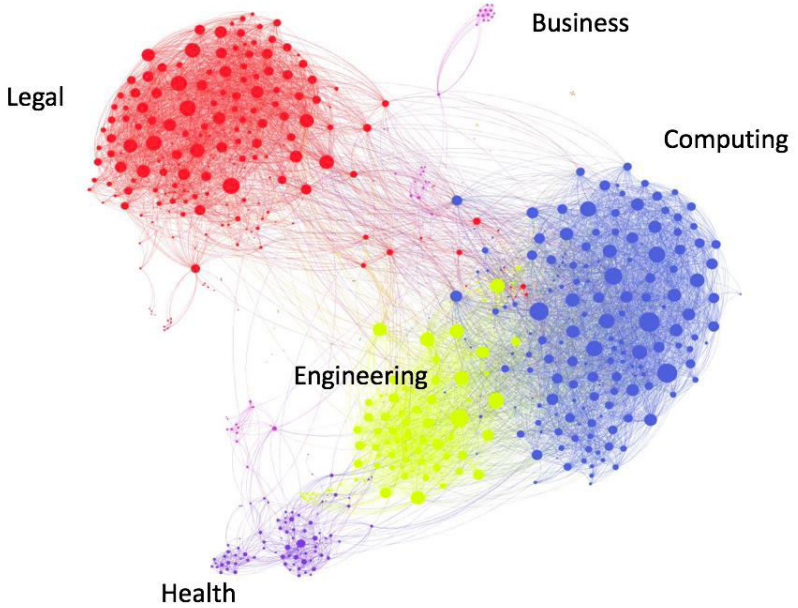
Создание и применение детализированных правил основываясь на широком спектре критериев, включая: имя, устройство, местоположение, свойства файла, права доступа, содержимое, действия, индекс угрозы

BLUE COAT

Определение природы информации (хранящейся в Облаке)

- Deep Content Inspection (DCI)

1. Computational linguistics
2. Cluster analysis
3. Document structure analysis
4. Information theory

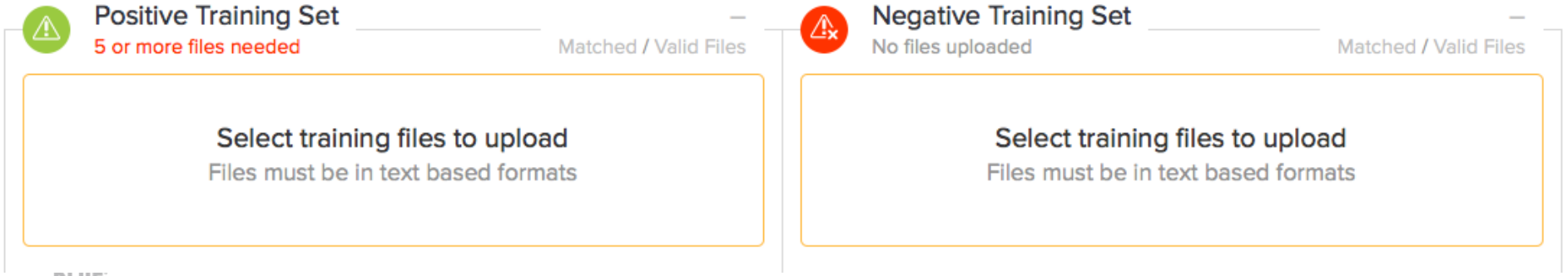


BLUE COAT

DLP для данных хранящихся облачных файловых хранилищах

Настраивается самим пользователем

- Пользовательский словарь и регулярные выражения
- Взвешенная комбинация различных параметров в одном профиле
- Продвинутый анализ данных на базе 'Training Model'



Elastica Cloud Security

Мониторинг Облачных приложений

Обнаружение «теневой» активности и мониторинг использования облачных приложений в реальном времени

Управление данными

Точное управление критичными данными

Защита данных

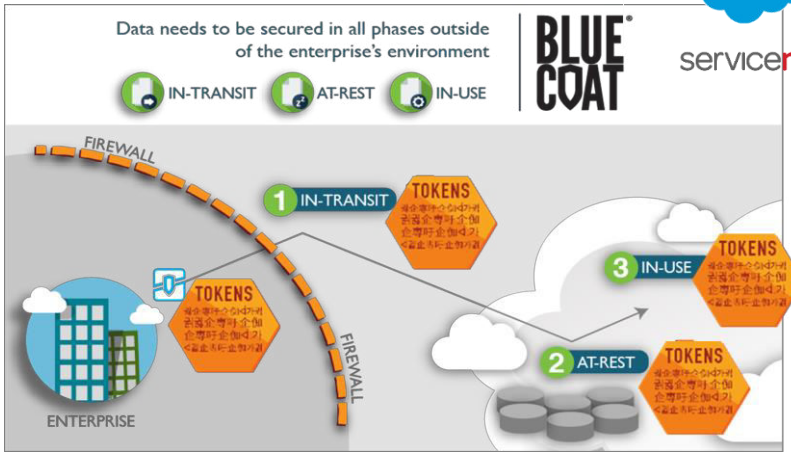
Шифрование и токенизация данных при передаче, хранении и использовании

Защита от угроз

Противодействие угрозе в ходе ее развития с использованием анализа поведения пользователей

Защита данных в разрешенных Облачных приложениях

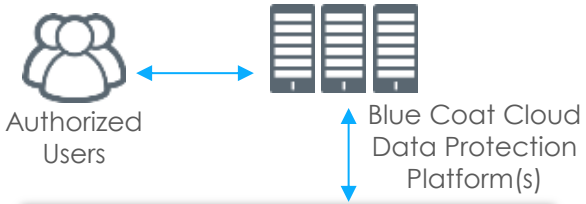
- **Шифрование/токенизация на уровне полей баз данных**
  - *Замена данных с использованием суррогатного шифрования или токенизацией в корпоративных* SaaS приложениях
  - С сохранением функционала(например поиск в защищенных данных)

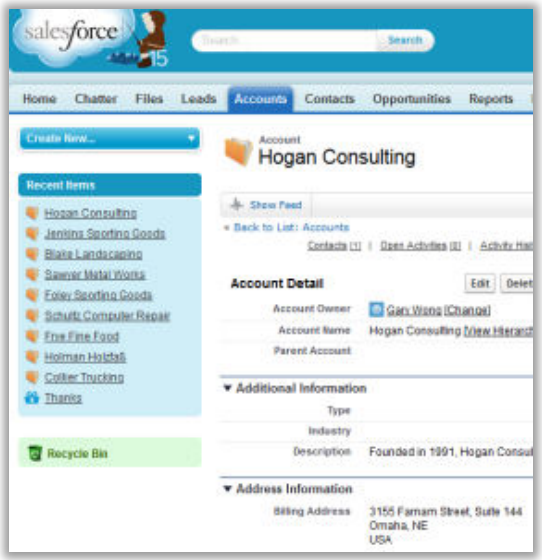


- **Шифрование на уровне фалов**
  - Шифрование файлов в приложениях таких, как Box, Dropbox, Google Drive

Blue Coat Cloud Data Protection

Как видит пользователь





Как хранится и обрабатывается в облаке

Elastica Cloud Security

Мониторинг Облачных приложений

Обнаружение «теневой» активности и мониторинг использования облачных приложений в реальном времени

Управление данными

Точное управление критичными данными

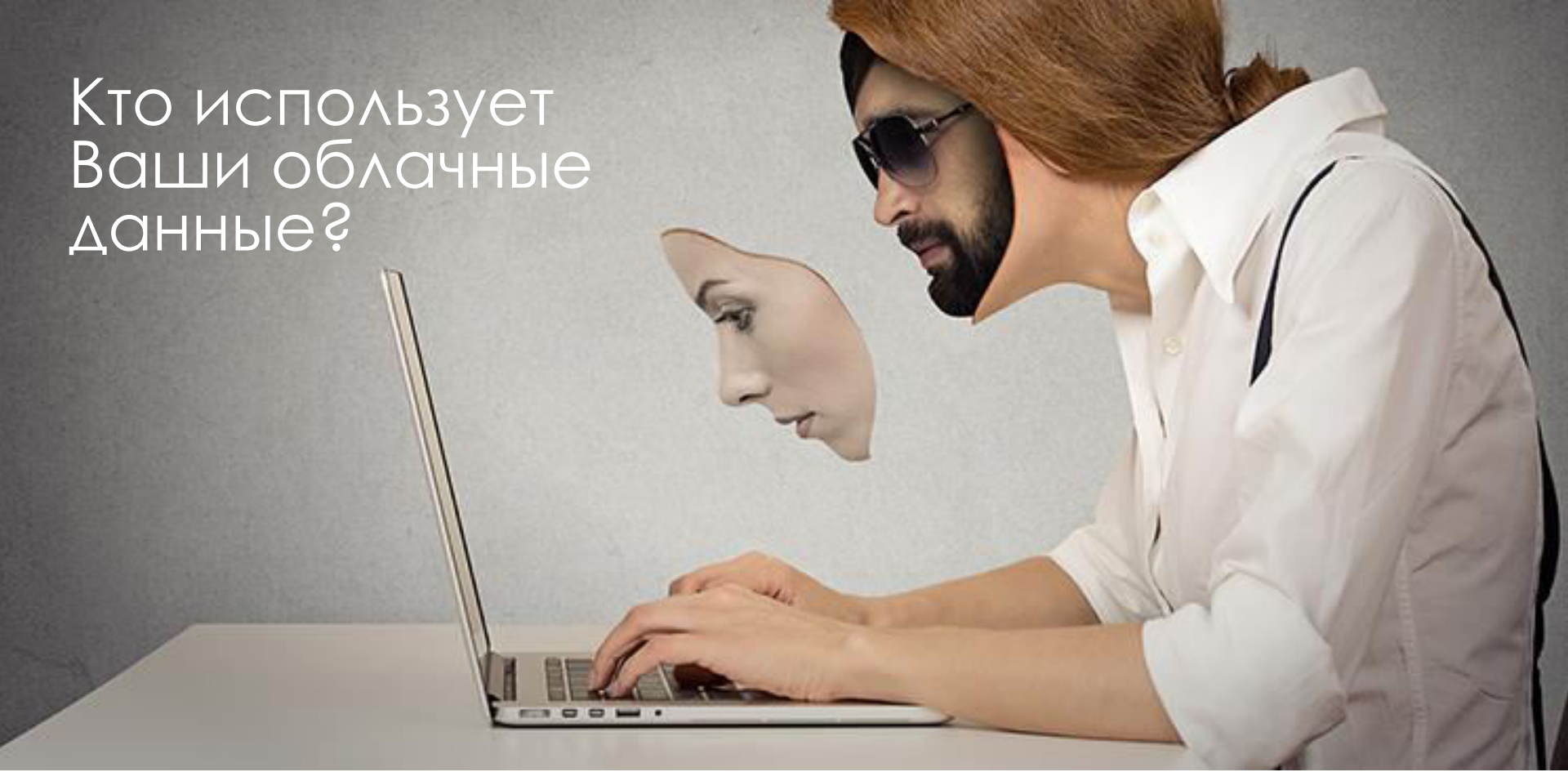
Защита данных

Шифрование и токенизация данных при передаче, хранении и использовании

Защита от угроз

Противодействие угрозе в ходе ее развития с использованием анализа поведения пользователей

Кто использует Ваши облачные данные?



Как плохие парни попадают в Ваше облако под Вашей учеткой?

Просто проходят прямо в парадную дверь…

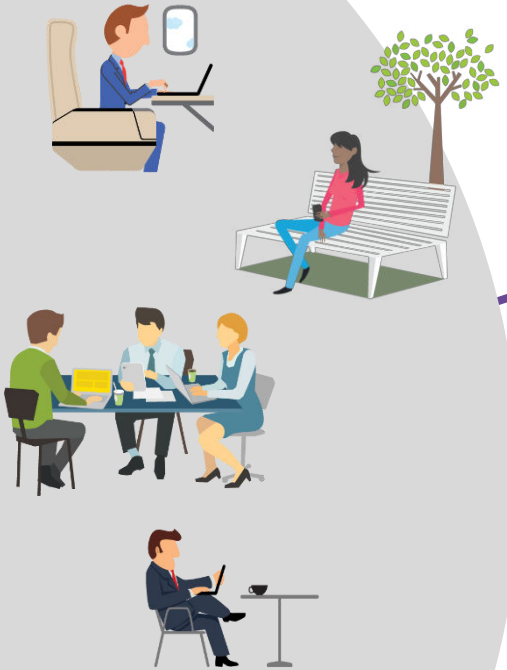
Malware
Screenscrapers
Keyloggers
Bots

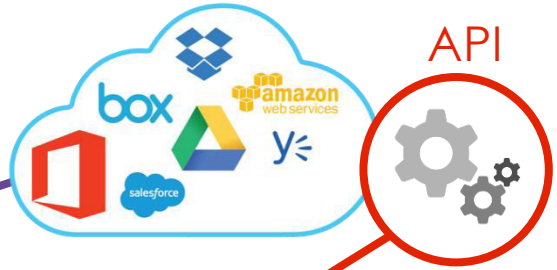
Phishing
Social engineering
Insider access

В 63% подтвержденных случаях утечки данных виновны слабые, украденные или типовые пароли.

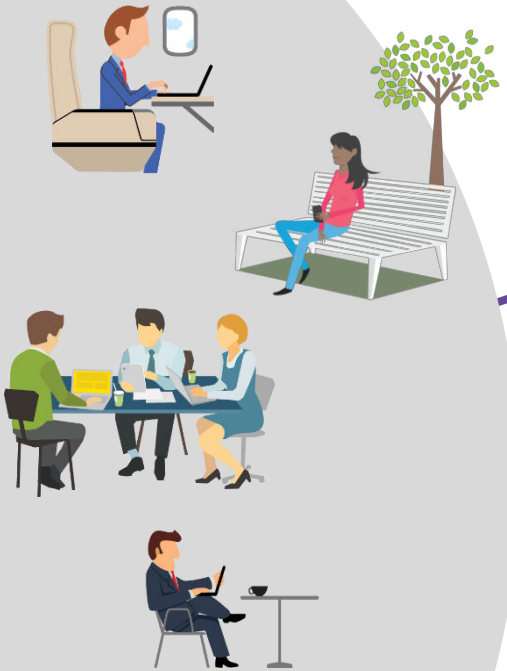
Source: Verizon Data Breach Investigations Report, 2016

Мониторинг и управление Облачными приложениями





Мониторинг и управление Облачными приложениями



GATEWAY

API

box

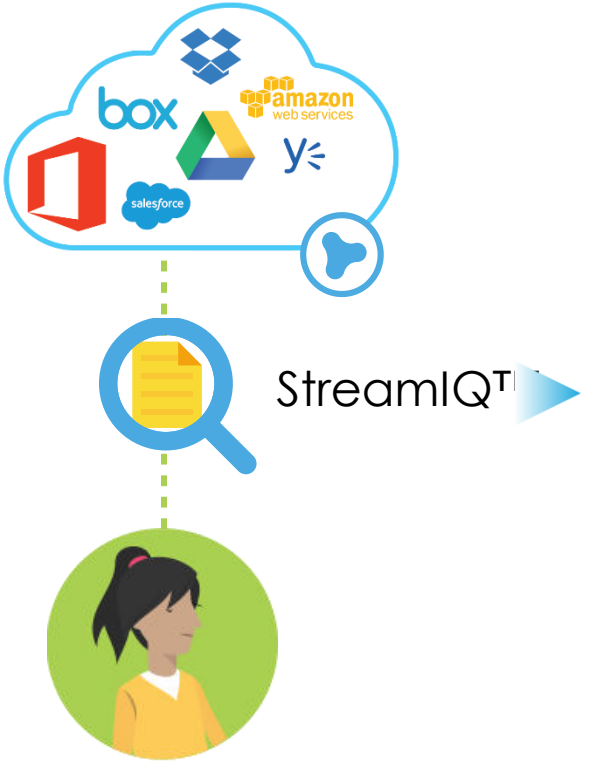
amazon web services

salesforce

elastica CloudSOC™

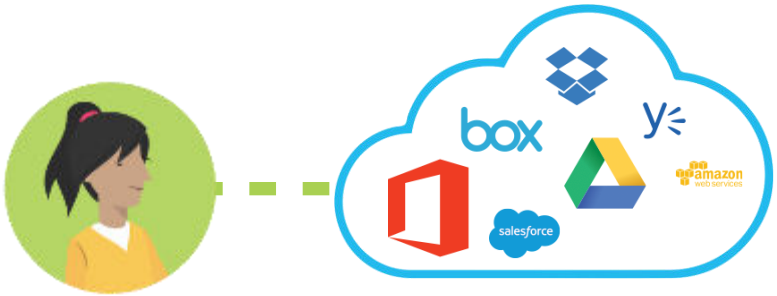

UBA
USER BEHAVIOR ANALYTICS
60 files in 3 minutes
SCREENSHOT→ EMAIL→ DELETE
7 failed logins
300+ docs
SHARED PUBLICLY
RAPID REPEAT
CONFIDENCE READING
event frequency / file (#), size
events over time
MED
HIGH
Для каждого пользователя формируется уникальный поведенческий профиль на основании его типичного поведения. Все существенные отклонения или комбинации подозрительных событий вызывает соответствующие уведомления или действия для изоляции или блокирования этих активностей
ACCOUNT LOGINS
FAILED ATTEMPTS
LOGINS 2+ LOCATIONS
CPU ACTIONS
EMAIL
DELETE
SCREEN CAPTURE
FILE TRANSFER
DOWNLOAD
UPLOAD
FILE SHARE
ALL COMPANY
EXTERNAL
PUBLIC

1. Выделение действий пользователя с StreamIQ™

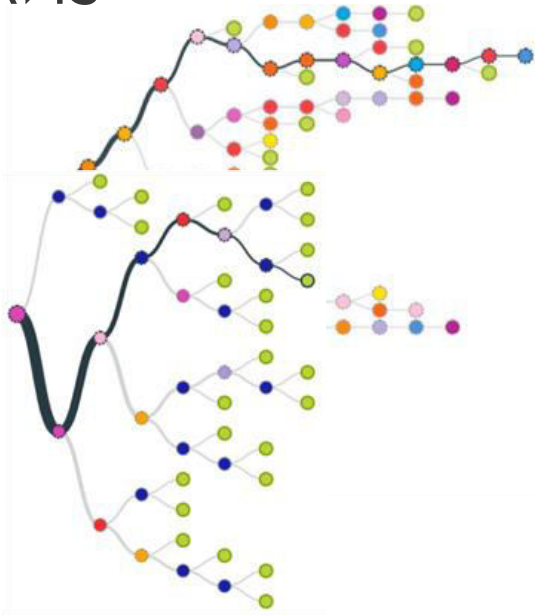


Анализ Web трафика (включая SSL) и извлечение деталей в реальном времени

2. Поведенческий анализ



Подозрительная активность

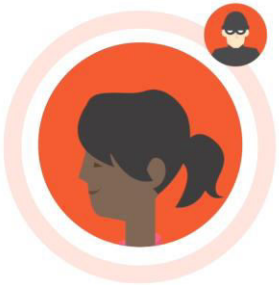


Что произойдет, когда случится эта подозрительная активность пользователя ?

Уникальный граф действий пользователя

3. ThreatScore™

Подозрительная активность



ThreatScore™ основан на значимости подозрительной активности

- Активный — визуальный drill down
- Высокоточный— на основании User Behavior Analysis
- Автоматизируемый — критерий для применения правил

Граф обнаружения

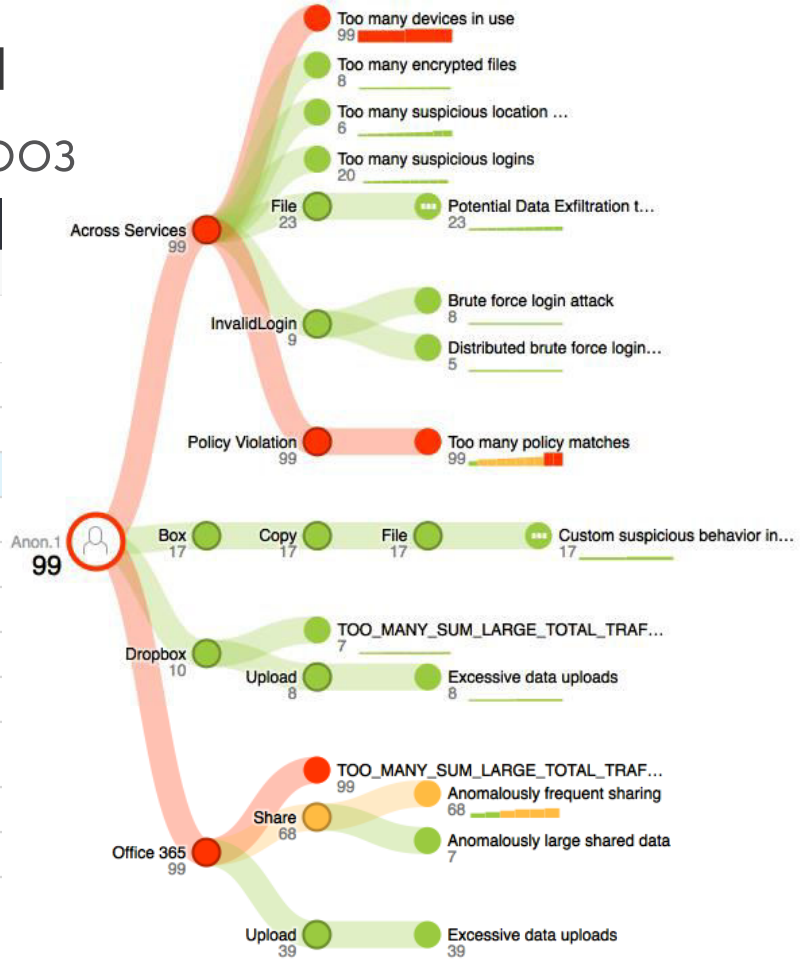
Упрощает обнаружение угроз

Anon.1 (anon.1@se-elastica.com)

Threat Tree | Incidents

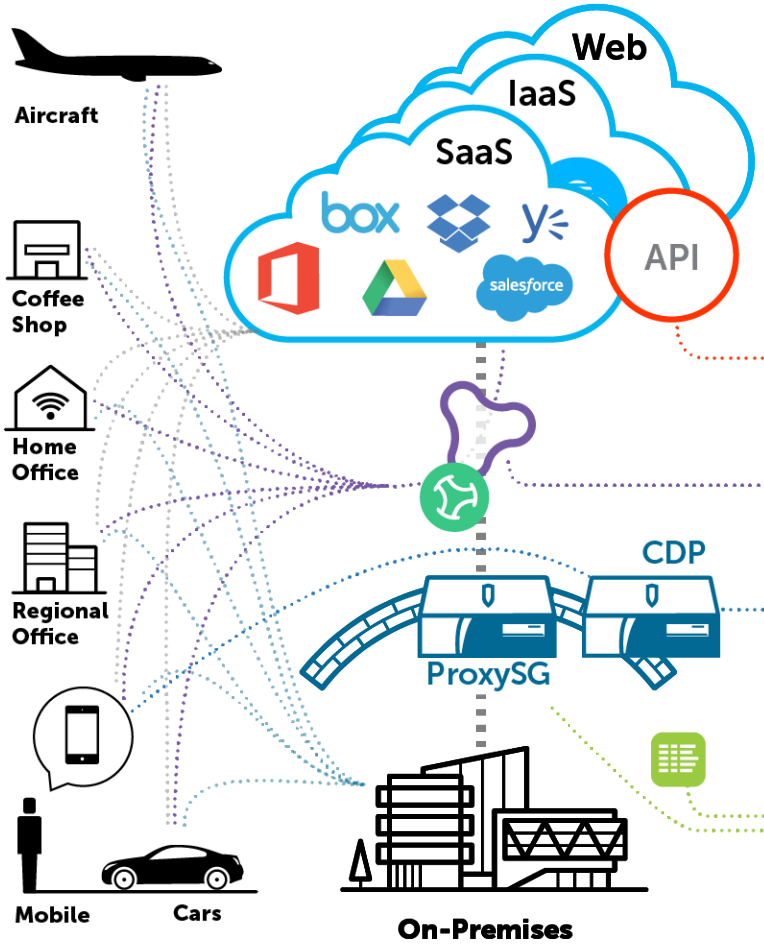
22 Incidents | View all incidents

May 23, 2016, 10:42:31 AM	Office 365	Anomalously large shared data
May 23, 2016, 10:34:20 AM	Office 365	Excessive data uploads
May 11, 2016, 2:00:25 AM	Across Services	Too many encrypted files
Mar 15, 2016, 8:21:26 PM	Office 365	Anomalously frequent sharing
Feb 25, 2016, 11:53:48 PM	Across Services	Brute force login attack
Jan 08, 2016, 9:39:58 AM	Across Services	Too many policy matches
Jan 05, 2016, 9:51:19 AM	Across Services	Too many suspicious location changes
Dec 22, 2015, 12:22:20 PM	Office 365	Excessive data uploads
Dec 05, 2015, 7:22:00 AM	Across Services	Potential Data Exfiltration through Unauthorized External Downloads Sequence
Nov 23, 2015, 2:40:14 PM	Across Services	Too many suspicious logins
Nov 04, 2015, 7:23:37 AM	Across Services	Too many suspicious location changes



Единая точка управления для Cloud Security

Дорога к полной Cloud Security



elastica

- Shadow IT Audit
- Elastica for Cloud Apps
- CASB Gateway
- Data Protection
- Web Security

$$$

- SWG in the Cloud
- URL Filtering
- Real-time ATP
- Application Controls
- Mobile Security
- Hybrid Deployment
- Always-On Global Coverage

BLUE COAT