Визуализация Shadow IT и контроль данных в облаках

Константин Челушкин

Технический консультант Symantec

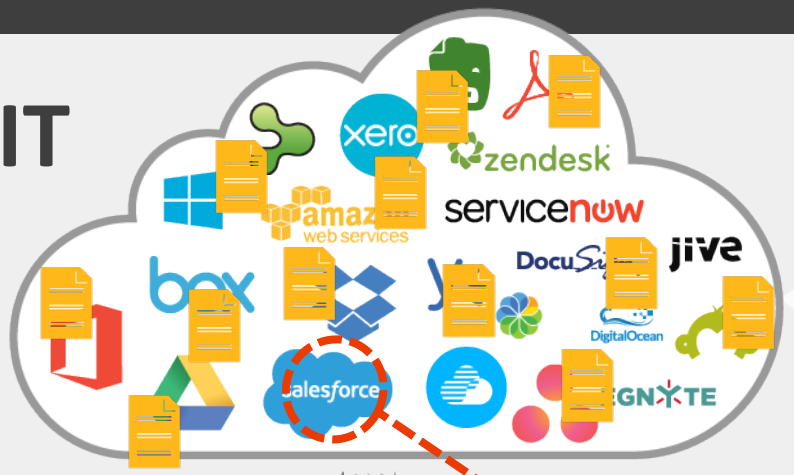
Возникновение Shadow IT

800-900 приложений
В РЕАЛЬНОСТИ

40-50 приложений
«ПО ОЩУЩЕНИЯМ»

[1] Источник: 2016 Shadow Data Report

Риски Shadow IT



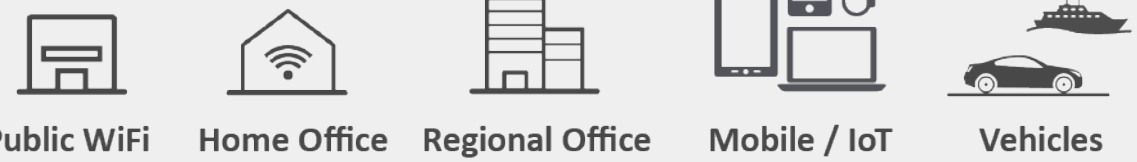
23% документов в облаке расшарены всем[1]

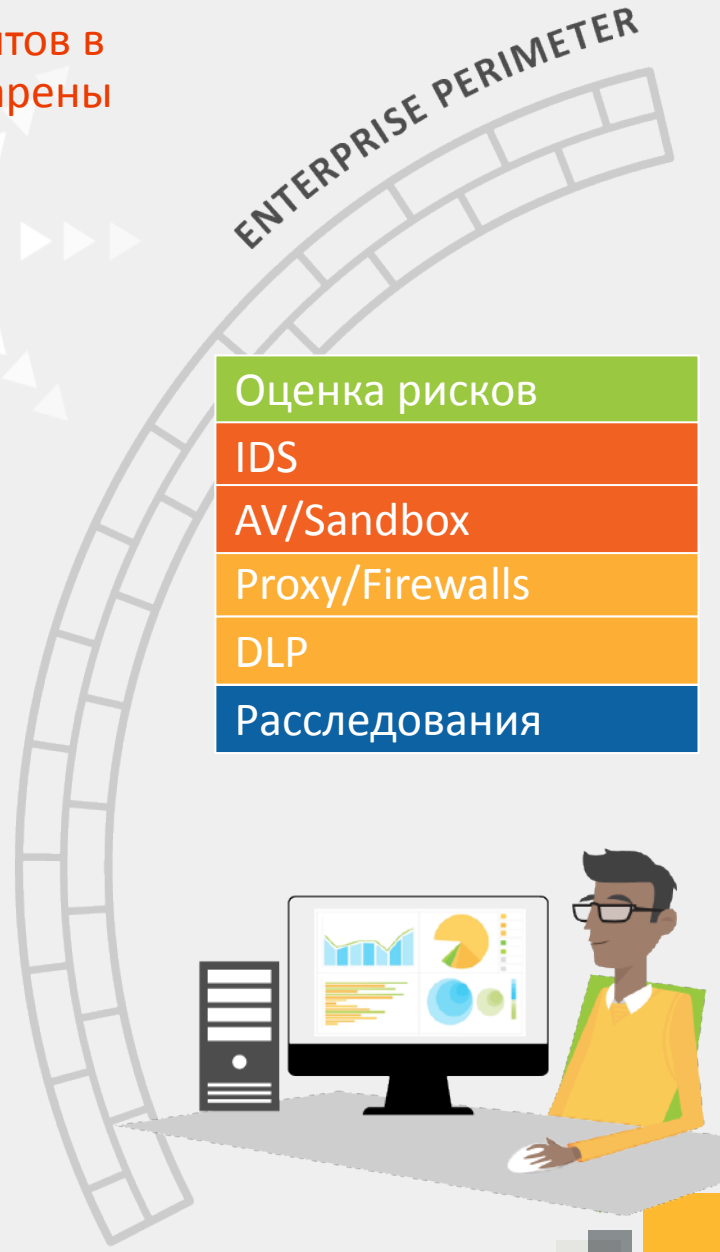
Отсутствие данных о безопасности облачных приложений

Использование устройств с прямым доступом в интернет

Хранение конфиденциальных данных в облачных приложениях

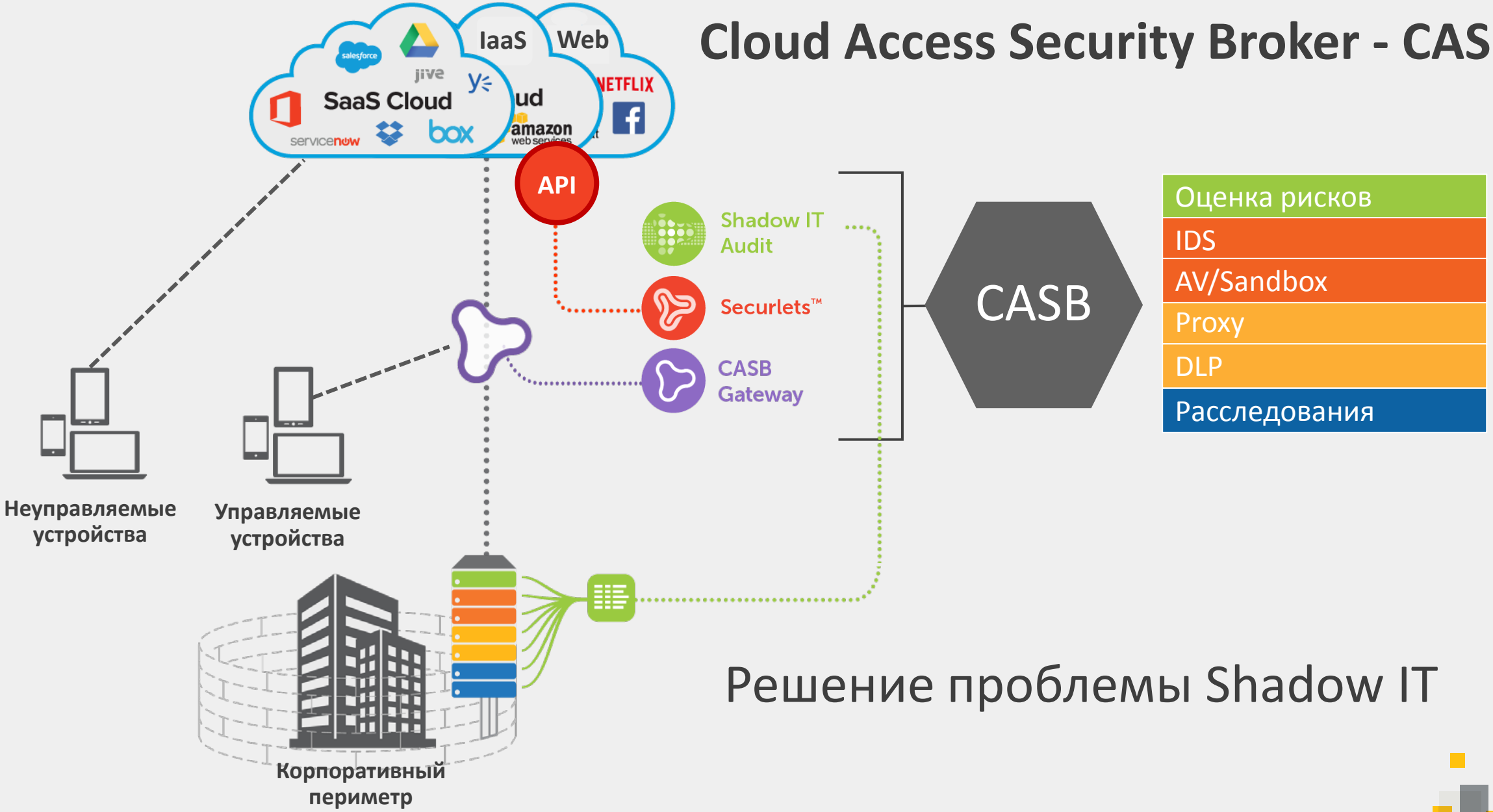
Отсутствие обнаружения взлома учетной записи





[1] Источник: 2016 Shadow Data Report

Cloud Access Security Broker - CASB

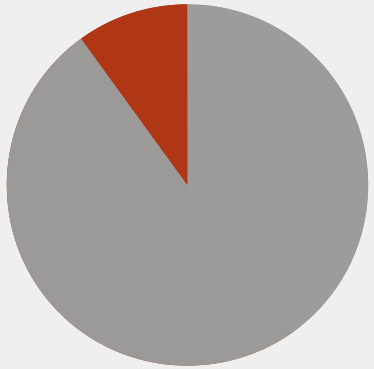


Решение проблемы Shadow IT

Рынок решений CASB

99% сбоев в облачной безопасности будет происходить по вине клиентов, а не провайдеров облачных сервисов

CASB в 2020 – 60%

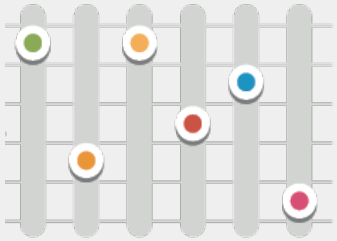


Источник: Gartner, Inc., Magic Quadrant for Cloud Access Security Brokers, Steve Riley, Craig Lawson, November 30, 2017

Функции CASB

Визуализация

Обнаружение Shadow IT и мониторинг использования облачных приложений на гранулярном уровне



Защита данных

Управление конфиденциальными данными

Защита от угроз

Аналитика поведения пользователей, обнаружение вредоносных программ и реагирование на инциденты

Показатели безопасности облачных приложений

General Information:

- Description
- Icon
- URL
- Application Group
- Risk Score
- Alexa Ranking

Service Provider information:

- Headquarters Location
- Founding Year
- Domain
- Terms and Conditions
- Hosting Company
- Hosting Location
- Year Domain Registered
- Private/Public Company
- Data Center Location
- Last Known Breech Date

Compliance:

- COBIT Compliant
- CSA Compliant
- FedRAMP Compliant
- FINRA Compliant
- FISMA Compliant
- GAAP Compliant
- HIPAA Compliant
- ISAE 3402 Compliant
- ISO 27001 Certified
- ITAR Compliant
- PCI DSS Compliant
- PCI DSS 2.0 Compliant
- Safe Harbor Compliant
- SAS 70 Compliant
- SOC 1 Compliant
- SOC 2 Compliant
- SOC 3 Compliant
- SOX Compliant
- SP800-53 Compliant
- SSAE 16 Compliant
- PCI DSS 3.0 Compliant

Transport Security:

- SSL Protocol Score
- SSL Cipher Suite Score
- Valid & Trusted Server Certificates
- Server Certificate Issuer
- Heartbleed Patched

AAA Security:

- Authentication Types
- Admin Audit
- Data Audit
- IP Restricted Access
- Supports MFA
- Remembers Password
- Strong Authentication
- User Can Track Usage History

Data Security:

- Encrypted Data at Rest
- Type of Encryption for Data at Rest
- Allows File Upload/Sharing

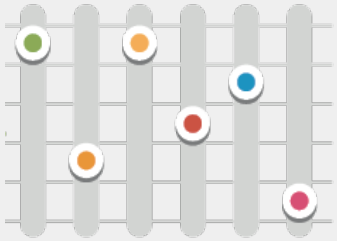
Визуализация Shadow IT

- Обнаружение Shadow IT и оценка риска используемых облачных приложений
- Помощь при выборе безопасного облачного приложения
- Оптимизация затрат на облачные приложения
- Постоянный мониторинг использования и соответствия требованиям

Функции CASB

Визуализация

Обнаружение Shadow IT и мониторинг использования облачных приложений на гранулярном уровне



Защита данных

Управление конфиденциальными данными

Защита от угроз

Аналитика поведения пользователей, обнаружение вредоносных программ и реагирование на инциденты

Проблема «Shadow Data»

Не найден аккаунт для **vasya@mail.ru** - поделиться этим файлом в виде ссылке? [Да] [Нет]

Маша поделилась файлом с Петей

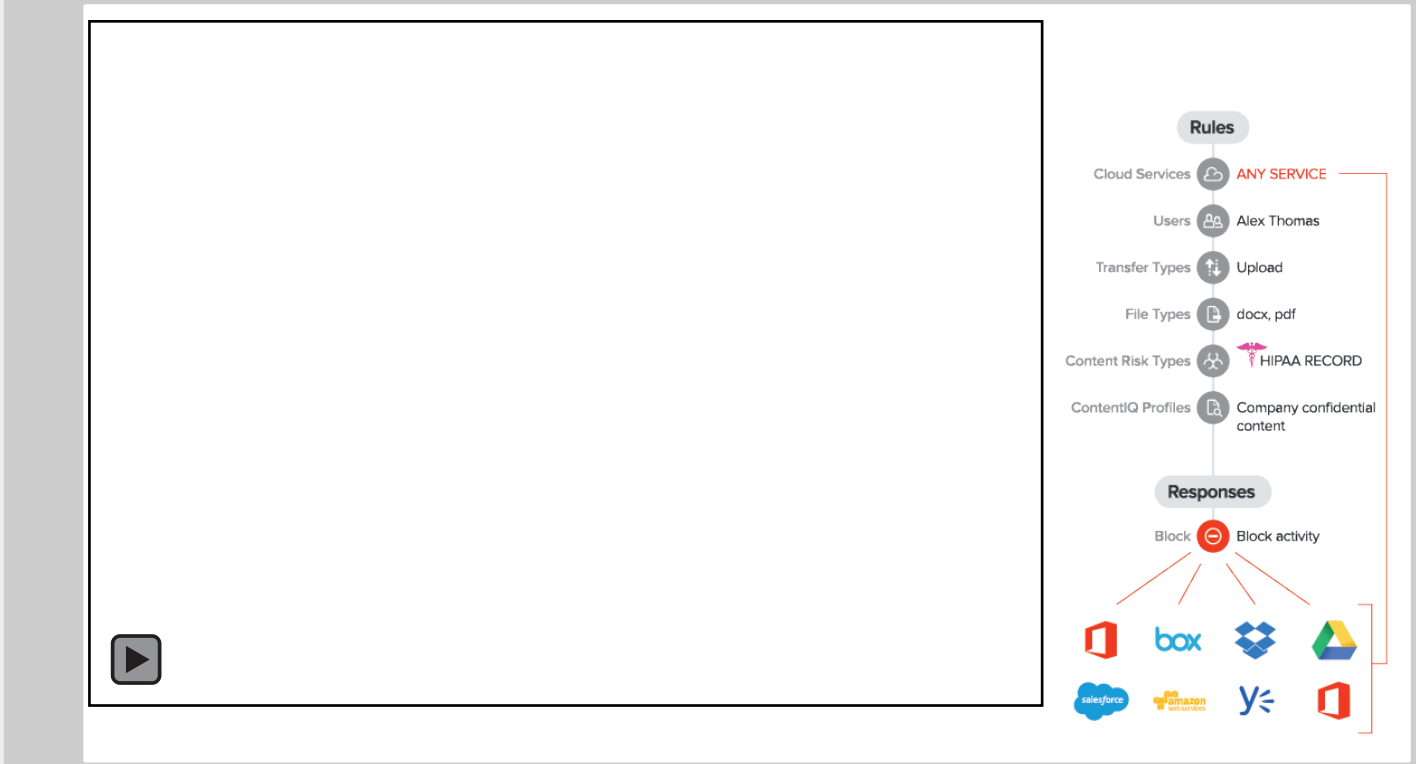
Петя поделился этим файлом с двумя другими пользователями

90% организаций теряли конфиденциальные данные из-за совместного использования файлов[1]

[1]Источник: Ponemon Institute

Управление данными в облачных приложениях

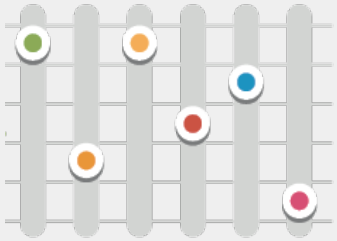
- Обнаружение и исправление риска совместного использования конфиденциальных данных
- Автоматическая классификация контента
- Определение гранулярных контентных и контекстно-зависимых политик доступа:
  - пользователь, тип устройства, местоположение, действие, уровень угрозы



Функции CASB

Визуализация

Обнаружение Shadow IT и мониторинг использования облачных приложений на гранулярном уровне



Защита данных

Управление конфиденциальными данными

Защита от угроз

Аналитика поведения пользователей, обнаружение вредоносных программ и реагирование на инциденты

Угрозы при работе в облаках

Угрозы учетным записям

Перехват сеанса

Вредоносные программы (или боты) в системах конечных пользователей могут захватывать сеансы облачных приложений.

Захват учетной записи

Учетные данные пользователя могут быть скомпрометированы с помощью фишинговых атак или аналогичных методов.

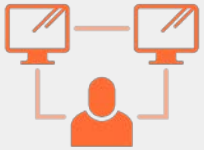
Злоумышленники

Недовольный сотрудник может злоупотреблять активами компании.

Угрозы данным и инфраструктуре

Вредоносы и APT

Могут использовать облачные учетные записи для распространения по всей организации.



Шифровальщики

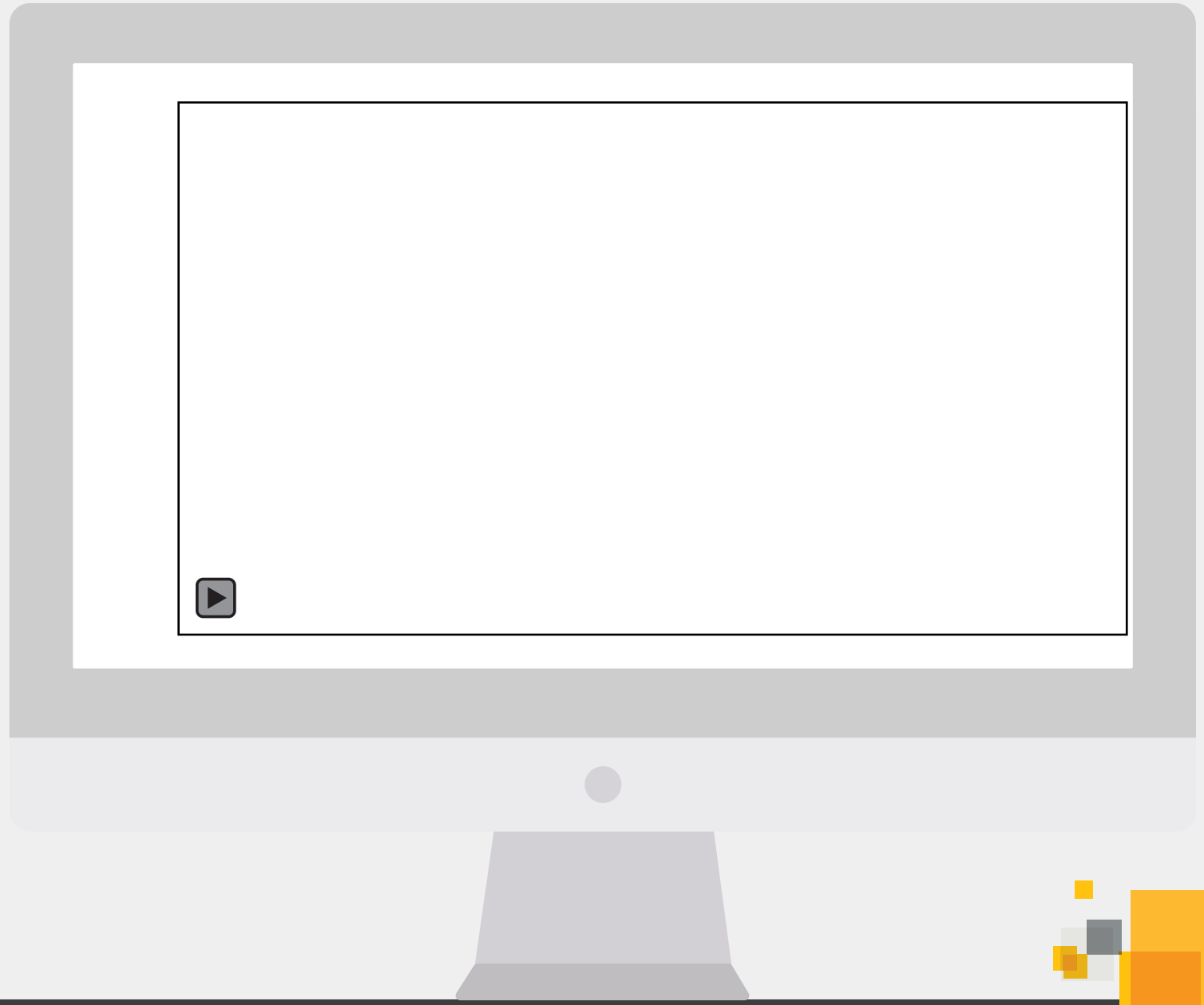
Могут использовать облачные учетные записи с высокими правами.

Боты и трояны

Могут использовать облачные учетные записи для кражи данных.

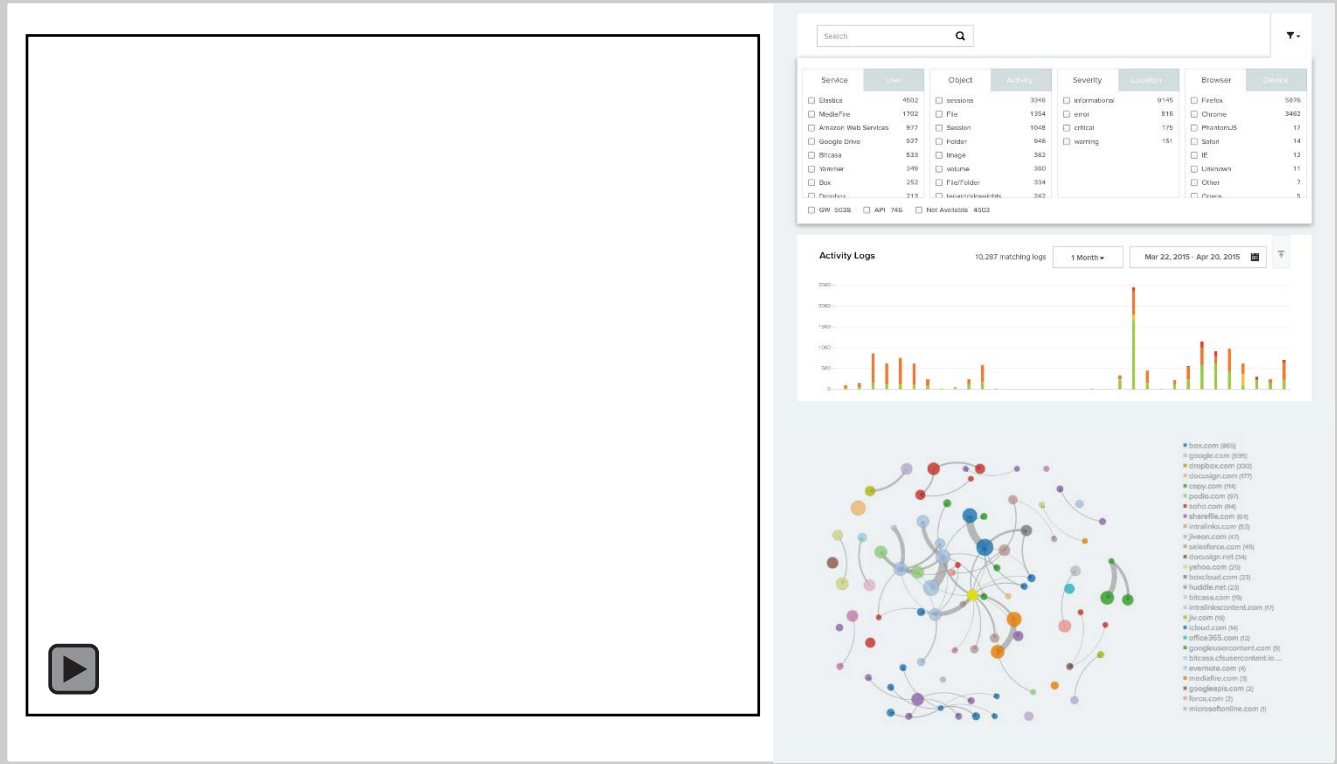
Защита от угроз

- Аналитика поведения пользователей для выявления вредоносного поведения
- Предупреждение администраторов или карантин активности
- Обнаружение продвинутых атак утечки данных
- Обнаружение и предотвращение распространения вредоносных программ



Анализ данных и расследования

- Анализ «больших данных» в реальном времени
- Инструменты визуализации и поиска
  - Поиск в свободной форме
  - Расширенный язык запросов
  - Динамические фильтры
  - Сводные таблицы
- Экспорт данных в SIEM или CSV



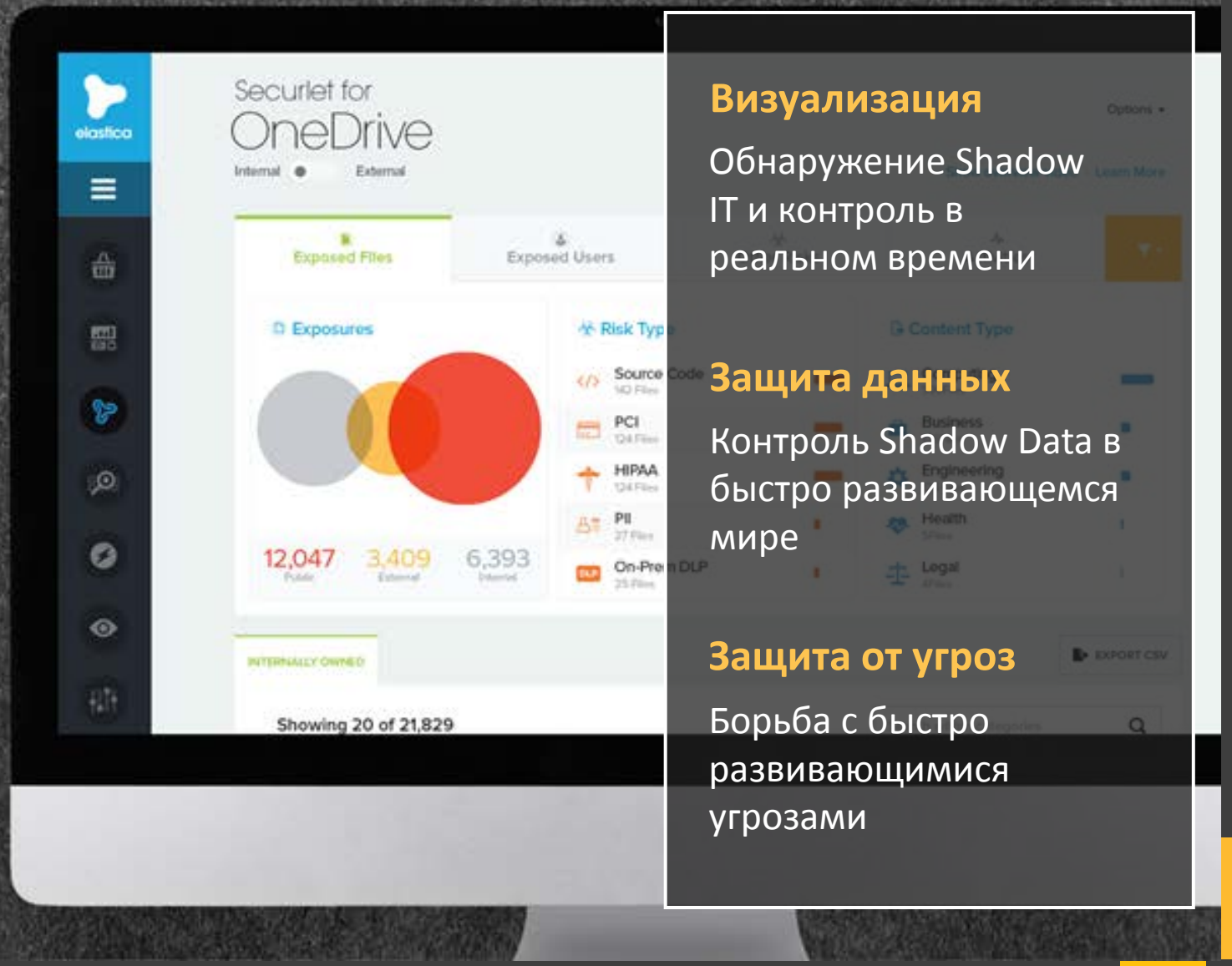
Оценка риска Shadow IT

SHADOW IT ОЦЕНКА РИСКА

- Аналитика о рисках и проблемах с облачными приложениями
- Аномалии использования приложений в вашей организации
- Какие приложения вы должны санкционировать и какие приложения вы должны блокировать

SHADOW DATA ОЦЕНКА РИСКА

- Внешние и публичные контентные риски, включая риски соответствия
- Рискованный контент, совместно используемый сотрудниками (например, вредоносное ПО, ИС и т. д.)
- Рискованные пользователи и действия пользователей



Визуализация

Обнаружение Shadow IT и контроль в реальном времени

Защита данных

Контроль Shadow Data в быстро развивающемся мире

Защита от угроз

Борьба с быстро развивающимися угрозами

Спасибо!

Константин Челушкин

konstantin_chelushkin@symantec.com