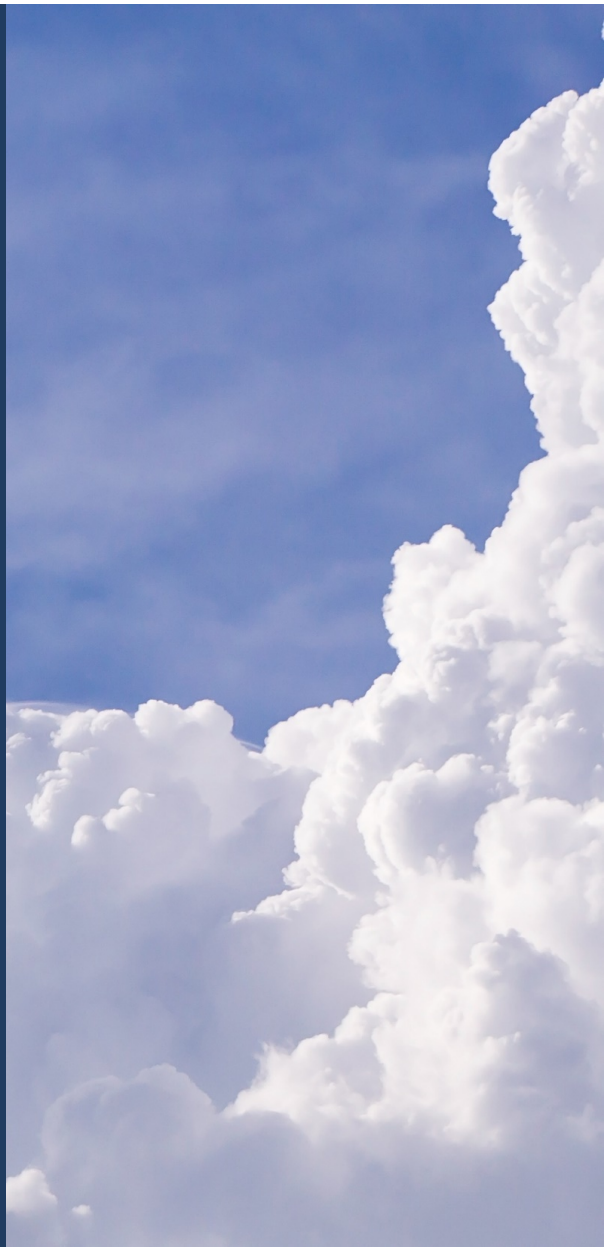
Визуализация Shadow IT и контроль данных в облаках



Как уходит контроль над данными

Shadow IT

Риски

Отсутствие данных о безопасности облачных приложений

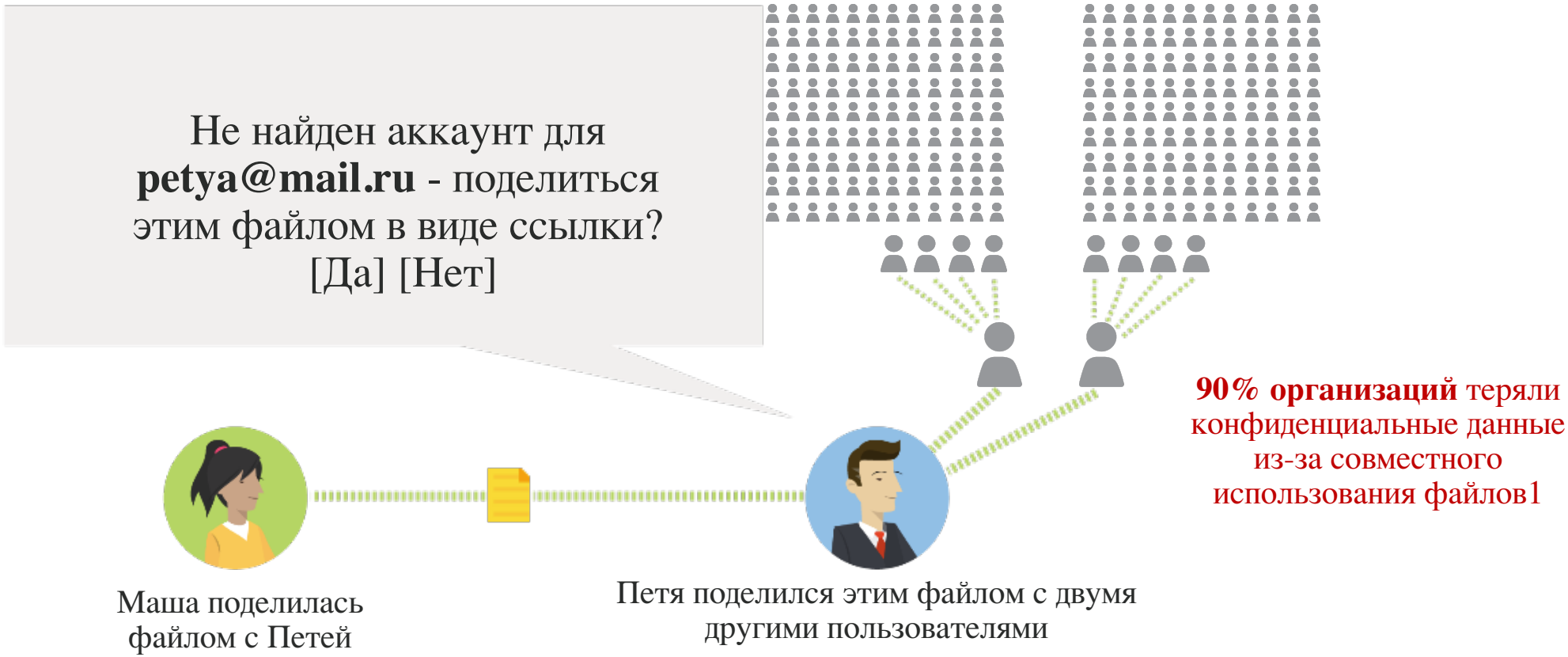
Использование устройств с прямым доступом в интернет

Хранение конфиденциальных данных в облачных приложениях

Отсутствие обнаружения взлома учетной записи

1 Источник: 2016 Shadow Data Report

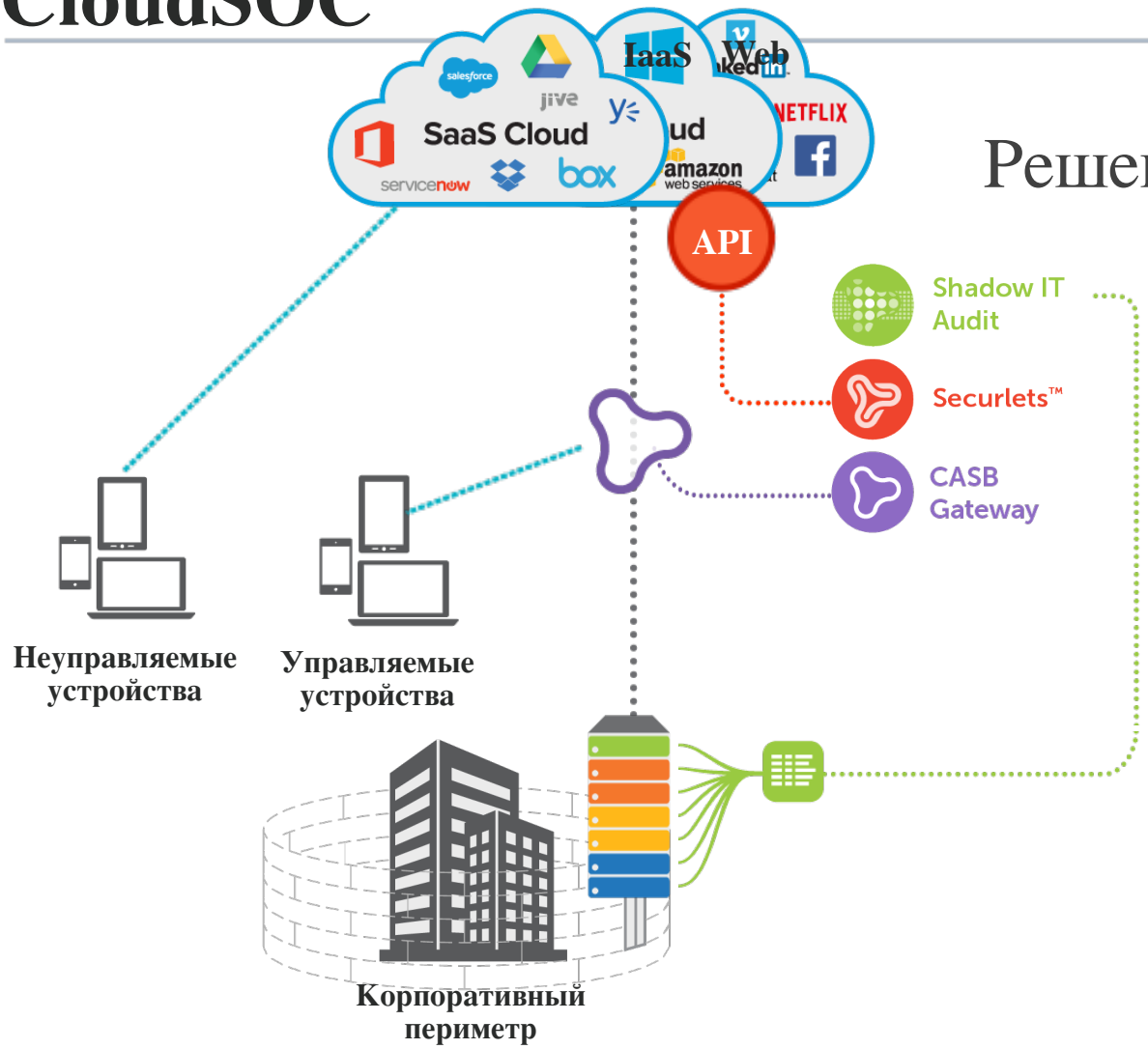
Проблема «Shadow Data»



90% организаций теряли конфиденциальные данные из-за совместного использования файлов1

1Источник: Ponemon Institute

CloudSOC



Решение проблемы Shadow IT

CASB

- Оценка рисков
- IDS
- AV/Sandbox
- Proxy
- DLP
- Расследования

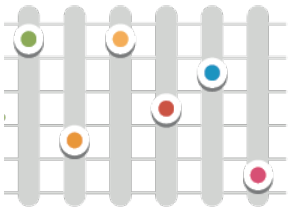
Функции CASB + DLP for cloud

Рейтинг приложений

Аналитика

Shadow IT Audit
Визуализация

Обнаружение Shadow IT и мониторинг использования облачных приложений. Идентификация чувствительной информации и ее расположения.



Защита данных

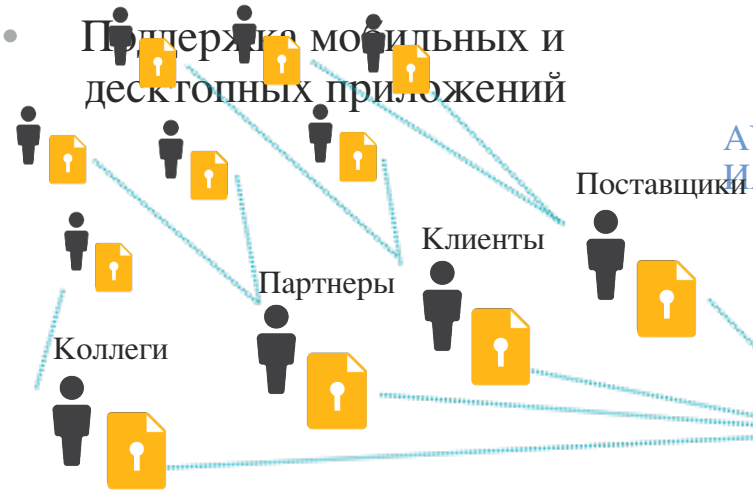
Управление конфиденциальными данными. Как и кем используется чувствительная информация, куда передается. Применение корпоративных политик.

Защита от угроз

Аналитика поведения пользователей, обнаружение вредоносной активности и реагирование на инциденты.

Шифрование данных в облачных приложениях

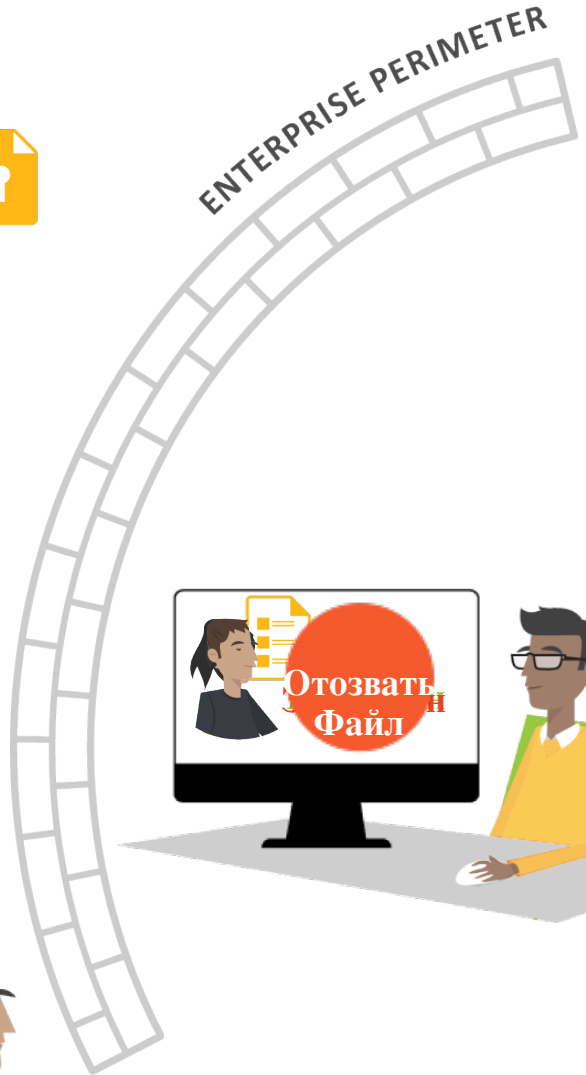
- Шифрование на уровне файла и получателя
- Доступ к содержимому путем аутентификации пользователя
- Отзыв файла
- Поддержка мобильных и десктопных приложений



КЛАССИФИКАЦИЯ ДАННЫХ

ШИФРОВАНИЕ

АУТЕНТИФИКАЦИЯ



С точки зрения защиты данных

- CASB и DLP совместно дают наиболее мощный эффект для контроля движения чувствительных данных во всех каналах – от endpoint до облаков.

Как получить видимость чувствительных данных в облаке?

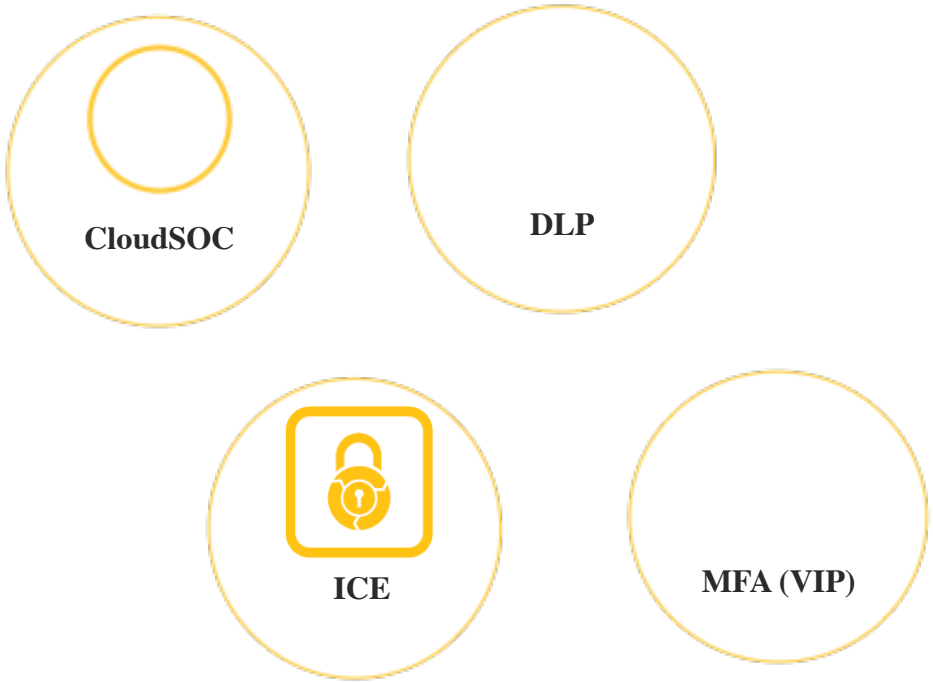
- Интеграция CloudSOC CASB и DLP позволяет распространять корпоративные политики на облачные приложения и управлять инцидентами из единой консоли.

Как защитить данные, если они уходят за периметр?

- Information Centric Encryption (ICE) защищает данные от нежелательного доступа и предоставляет единую точку контроля для отзыва доступа пользователя или к файлу.
- DLP умеет автоматически применять политики, в том числе ICE по различным векторам (для почты, файловых хранилищ, облачных приложений, сменных накопителей).

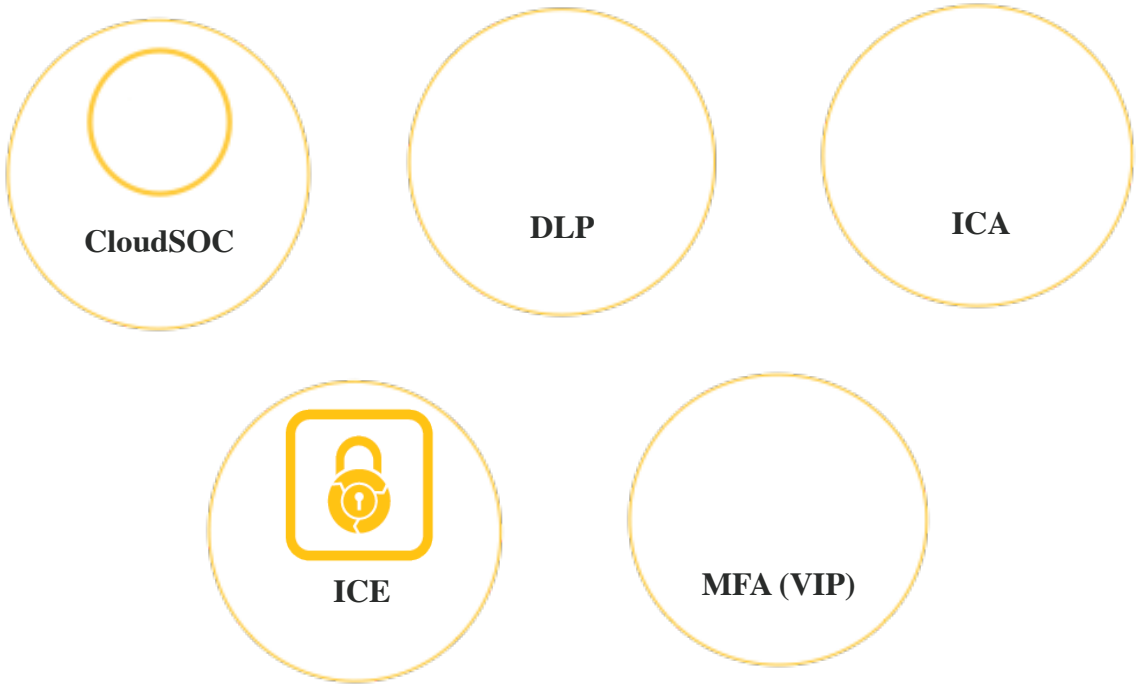
А что если учетные данные будут скомпрометированы?

- Мультифакторная аутентификация существенно повышает защиту от несанкционированного доступа.



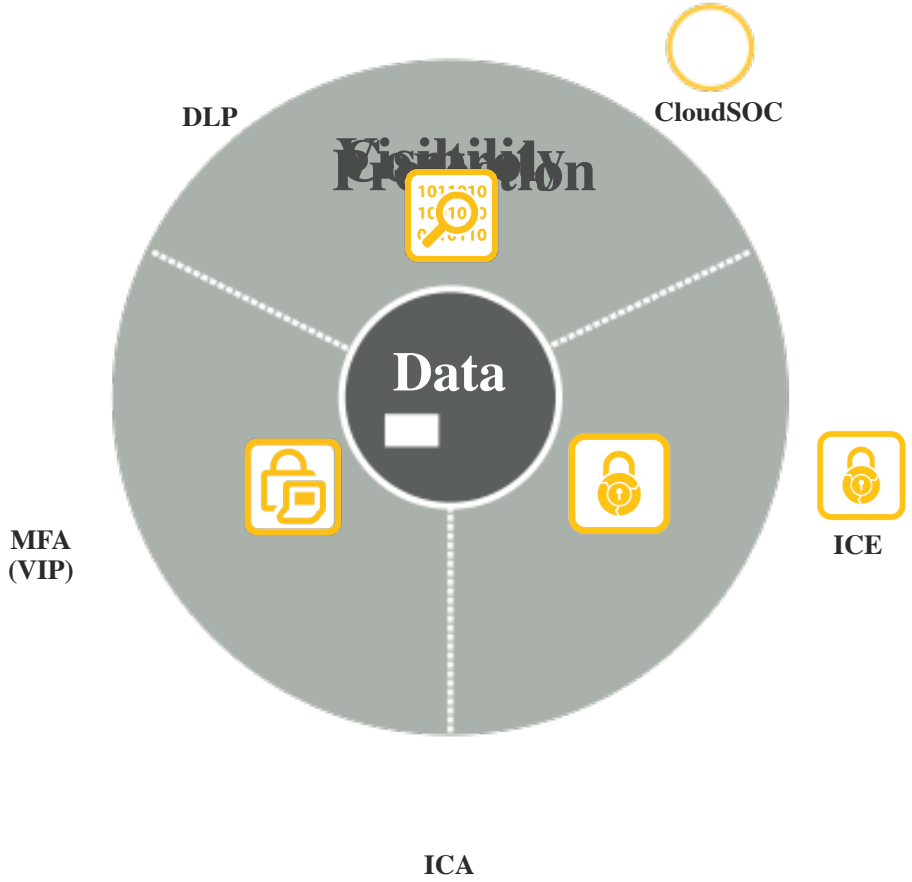
Как выявить вредоносную активность негодяя?

- Information Centric Analytics анализирует подозрительные события из разных систем, идентифицирует аномальное поведение и разоблачает волка в овечьей шкуре, темную лошадку и черную кошку.



Доверять можно… когда все под контролем

- **CloudSOC (CASB)**
  Контролирует облачные коммуникации и применяет DLP-политики
- **Data Loss Prevention (DLP)**
  Средство выявления чувствительной информации по всем каналам и центральной точкой распространения политик
- **Information Centric Encryption (ICE)**
  Запуск шифрации по правилам политик и контроля доступа
- **Validation and ID Protection Service (VIP)**
  Защищенный доступ к важным данным с мультифакторной аутентификацией
- **Information Centric Analytics (ICA)**
  User Entity Behavior Analytics для обнаружения подозрительного поведения и вредоносной активности пользователя



Спасибо!

ДОВЕРИЕ и КОНТРОЛЬ