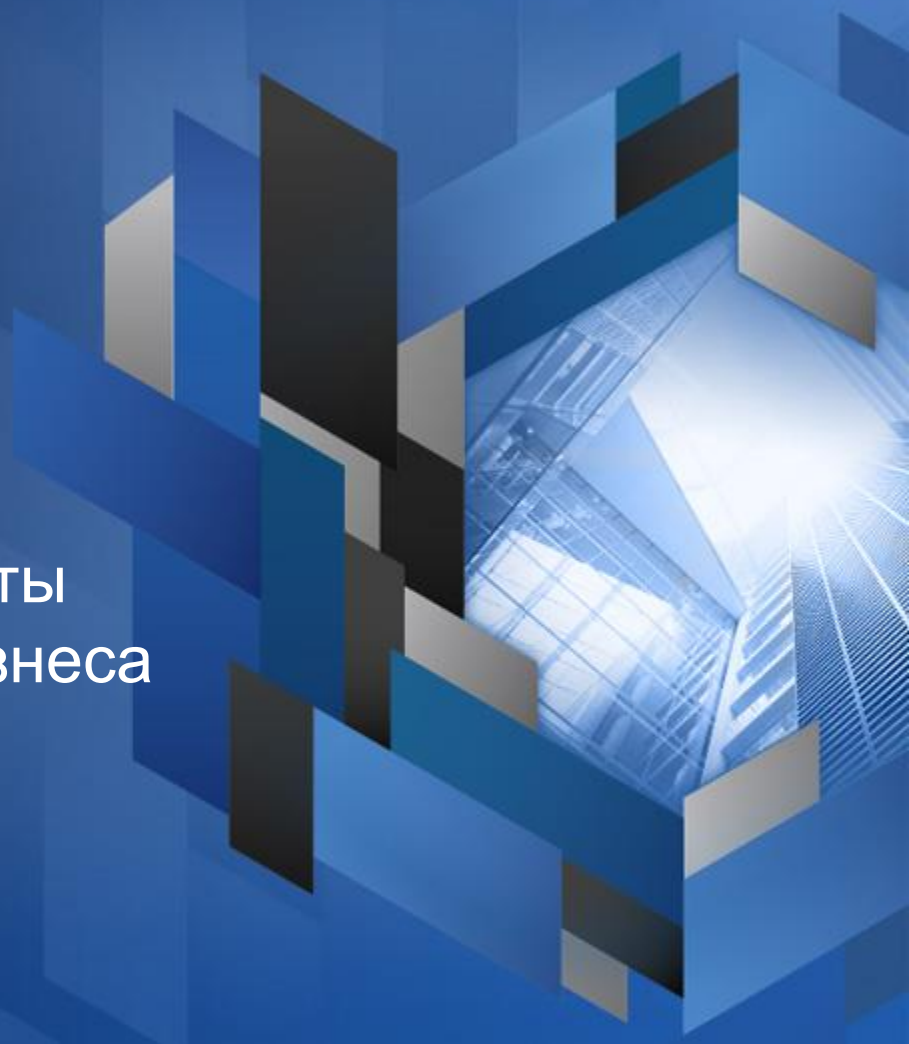
CYBERARK

# Привилегированные аккаунты как угроза безопасности бизнеса

Богдан Тоболь
Региональный директор

16.02.2016



# Борьба с возражениями: работа или пассивность?

| | |
|---|---|
| ▪ Не сейчас. | Саботаж безопасности компании? |
| ▪ Дорого. | Вы подготовили анализ рисков и ТЭО? |
| ▪ Ерунда. | У вас есть замечания по ТЗ? |
| ▪ Еще подумаю. | Где у нас календарный план? |
| ▪ Пробовали, не понравилось. | Ваши замечания в протоколе? |
| ▪ Большой брат. | Если вы крайний, кто вам поможет? |


CYBERARK

# Безопасность информации любого бизнеса

Конфиденциальность — … доступ …

Целостность — …несанкционированной …

Доступность — …права доступа…

Неотказуемость — … действие или событие …

Подотчётность — …действий …

Аутентичность — … идентичны …



Ключевые элементы контроля

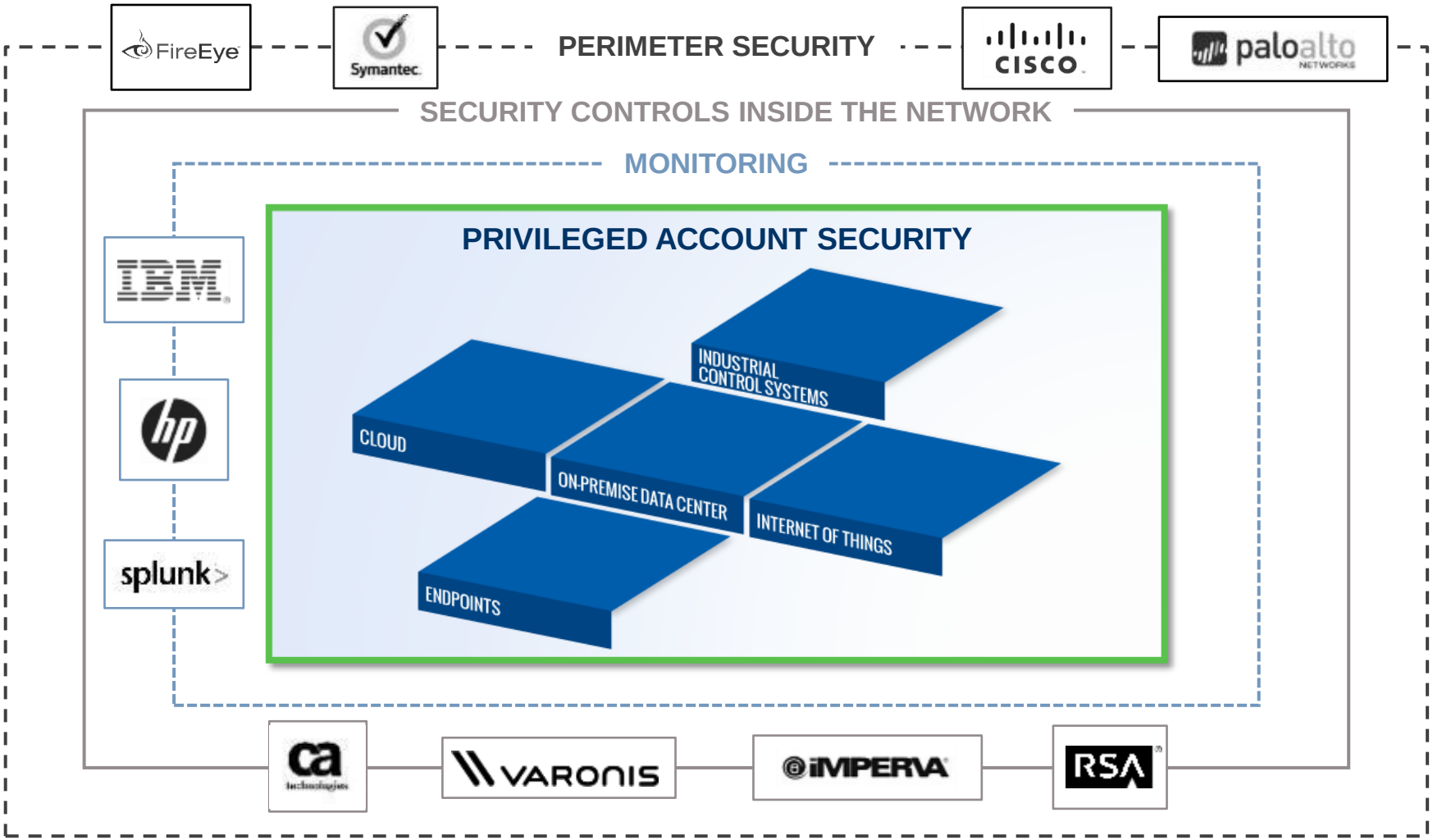
любого свойства безопасности

в каждой категории:

- **Права доступа**
- **Регистрация действий**

CYBERARK

# Стратегия защиты: активно или «детективно»?




CYBERARK

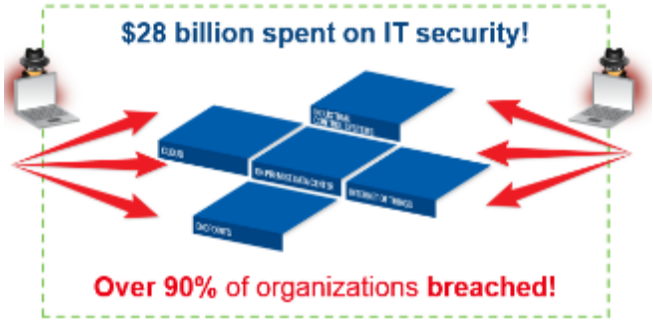
# Очевидные упущения

## Компрометация привилегированных УЗ


CYBERARK

# Неприемлемый риск

Вероятность двух независимых событий = Произведение вероятности событий


= 1.0 x 0.9 = 90%



CYBERARK

# Security or Usability?



CYBERARK

# All or nothing


| | Все разрешено | Все запрещено |
|---|---|---|
|  Operations | *Время и деньги* | *Время и деньги* |
|  Security | *Угрозы и инциденты* | *Претензии, авралы, саботаж* |

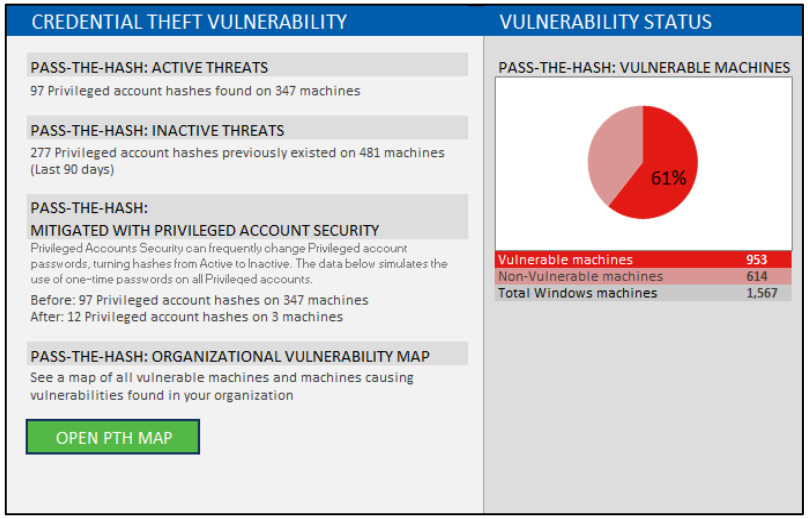
# Время пришло… как построить работу по проекту

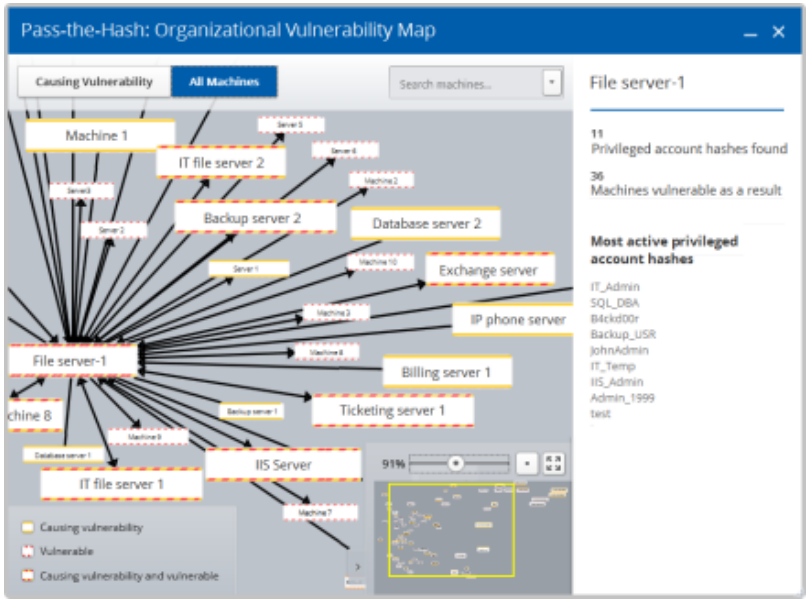
- Анализ уязвимостей. Описаны привилегированные аккаунты, связанные с ними риски и элементы контроля?
- Тест на проникновение. Как долго привилегированные аккаунты останутся недоступны квалифицированному подрядчику?
- Оценка и анализ средств защиты. Изучили лучшие практики защиты привилегированных аккаунтов?
- Требования соответствия. Применимы ли к вам рекомендации и стандарты, имеющие требования по защите привилегированные аккаунтов?
- Тестирование (Proof-of-Concept). Утвердили требования и провели пилот?

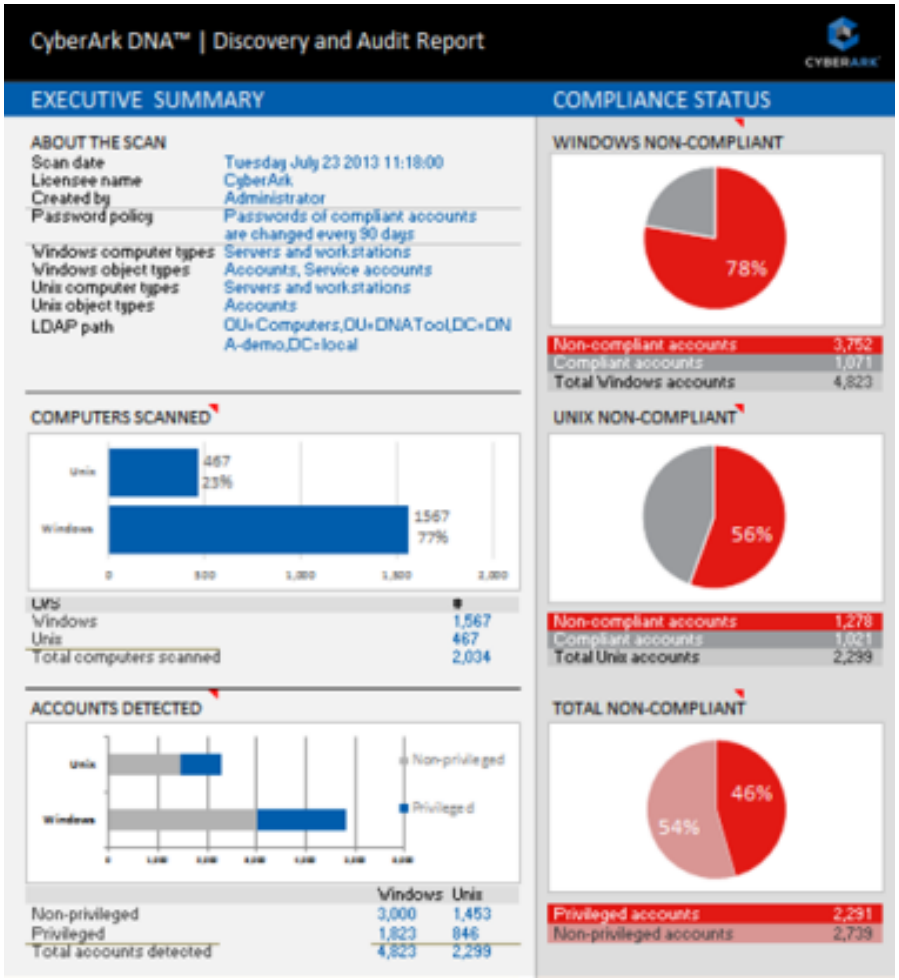


CYBERARK

# Время = деньги




CYBERARK

# Обязательные составляющие успеха


## Управление учетными данными

Пароли, SSH ключи, файлы

## Изоляция и контроль сессий

Блокировка опасного кода и контроль доступа

## Мониторинг активности

Постоянный автоматический анализ

| | | |
|---|---|---|
| Защищенное хранилище<br>Отсутствие агентов/клиентов<br>Взаимная аутентификация | Протоколонезависимость<br>Платформонезависимость<br>Высокая доступность | Автономный анализатор<br>Интеграция с SIEM<br>Независимый аудит |

CYBERARK

# О компании CyberArk

## Доверенный эксперт

- 2,500+ *privileged account security* customers
- 17 из 20 мировых банков
- 40+ клиентов за 4 года в России

## Гарантия решения проблемы

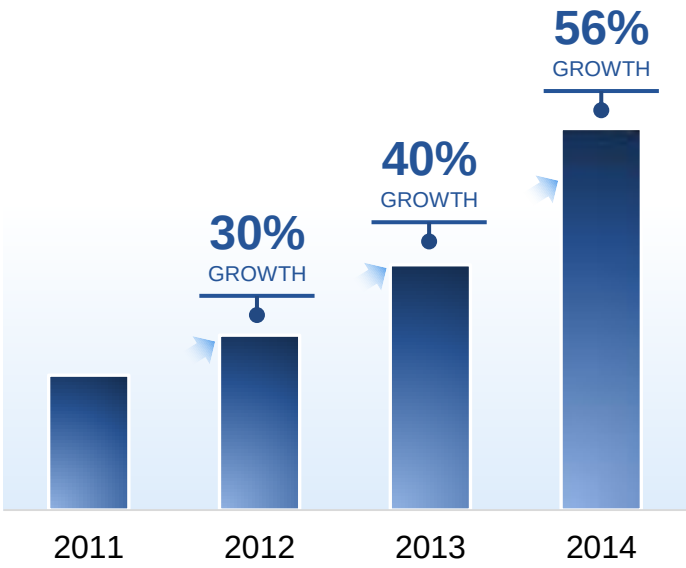
- Обследование, анализ, рекомендации
- Демонстрация, тестирование, интеграция
- Удовлетворяет ожиданиям 97% заказчиков

## 17 лет инноваций

- Первый VAULT, первый МОНИТОРИНГ, первая АНАЛИТИКА
- Более 100 инженеров-разработчиков, множество патентов

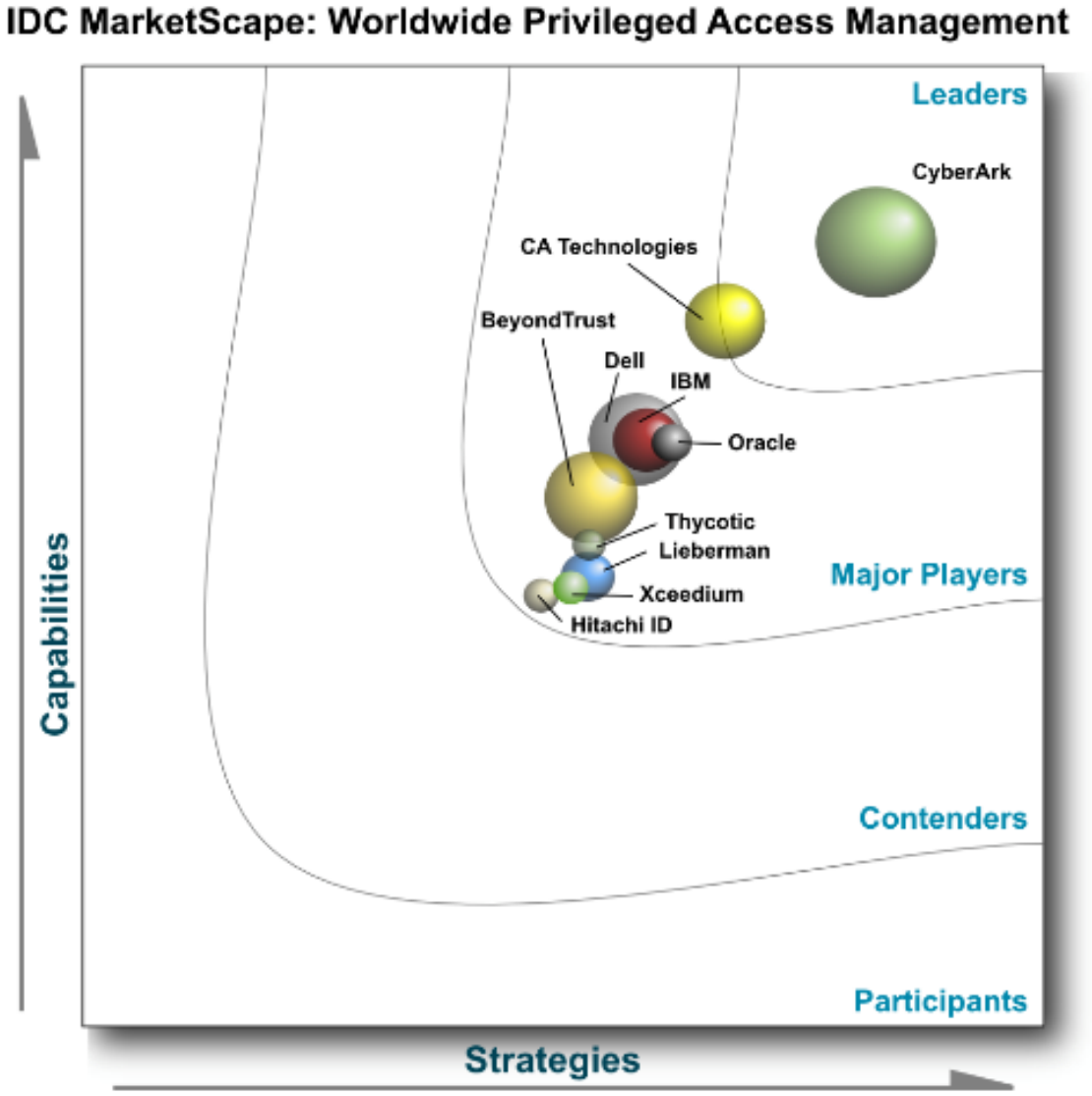
## Лучшее решение

- Одно решение, исключительно сфокусированное на защите привилегированных аккаунтов
- Enterprise-proven




CYBERARK

# Рекомендуем ознакомиться




ccess

CYBERARK


Спасибо за внимание…