



CYBERARK®

Привилегированные аккаунты как угроза безопасности бизнеса

Богдан Тоболь
Региональный директор

16.02.2016

Борьба с возражениями: работа или пассивность?

- Не сейчас.
- Дорого.
- Ерунда.
- Еще подумаю.
- Пробовали, не понравилось.
- Большой брат.

Саботаж безопасности компании?

Вы подготовили анализ рисков и ТЭО?

У вас есть замечания по ТЗ?

Где у нас календарный план?

Ваши замечания в протоколе?

Если вы крайний, кто вам поможет?



Безопасность информации любого бизнеса

Конфиденциальность — ... **доступ** ...

Целостность — ... **несанкционированной** ...

Доступность — ... **права доступа** ...

Неотказуемость — ... **действие или событие** ...

Подотчётность — ... **действий** ...

Аутентичность — ... **идентичны** ...



Ключевые элементы контроля

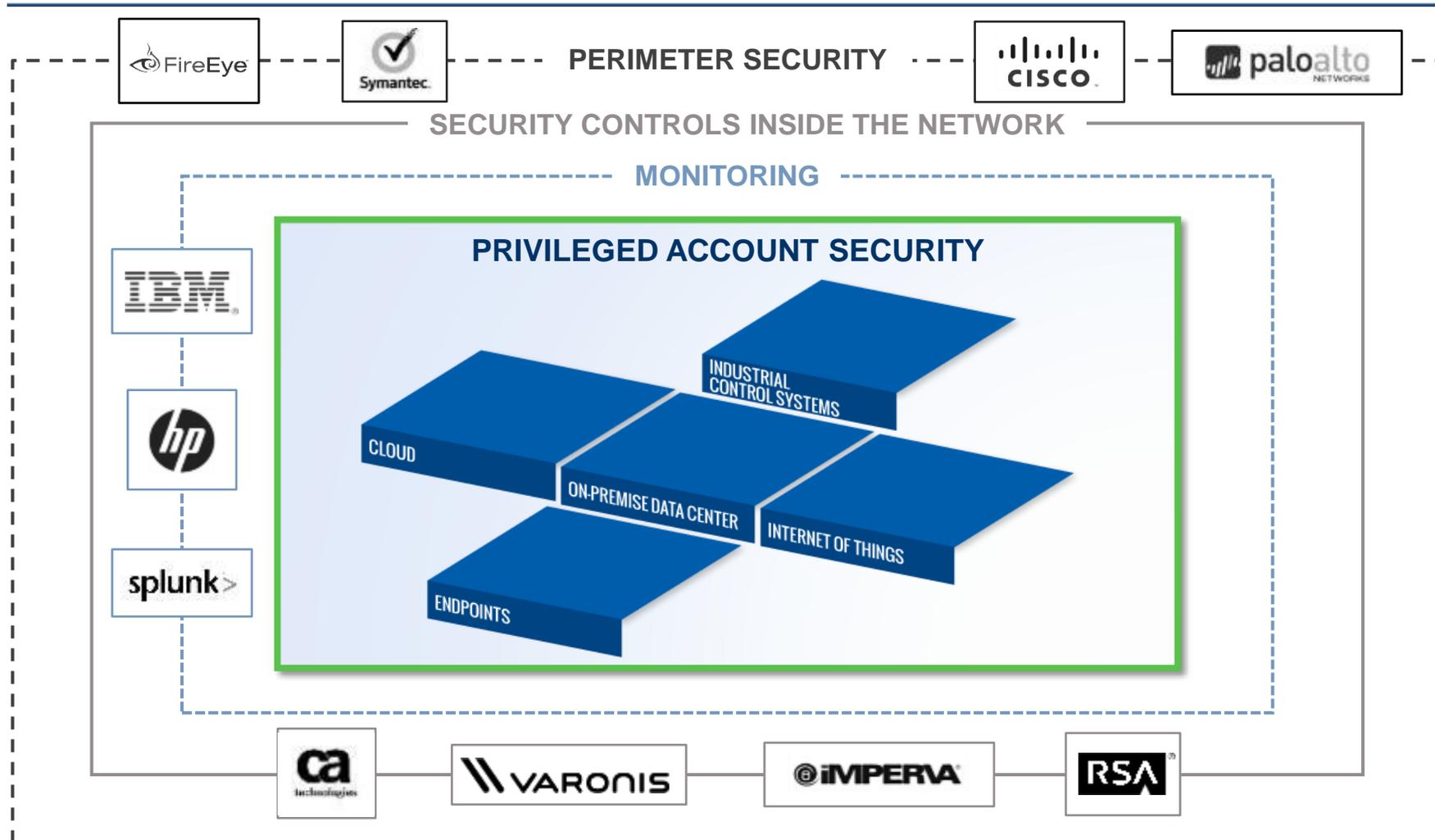
любого свойства безопасности

в каждой категории:

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



Стратегия защиты: активно или «детективно»?



Очевидные упущения



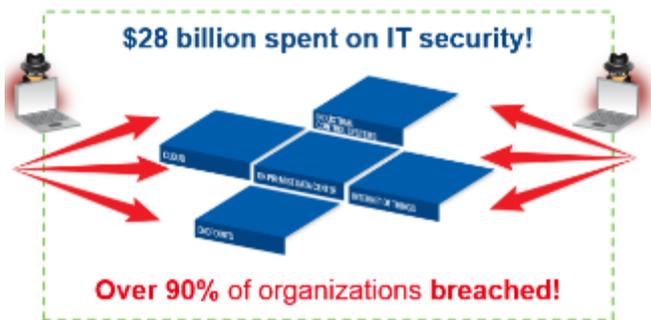
Компрометация привилегированных УЗ



Неприемлемый риск

Вероятность двух независимых событий = Произведение вероятности событий

*"...100% of breaches
involved stolen
credentials."*



$$= 1.0 \times 0.9 = 90\%$$

Security or Usability?



All or nothing



		Все разрешено	Все запрещено
	Operations	<i>Время и деньги</i>	<i>Время и деньги</i>
	Security	<i>Угрозы и инциденты</i>	<i>Претензии, авралы, саботаж</i>

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?



Время = деньги

CREDENTIAL THEFT VULNERABILITY

PASS-THE-HASH: ACTIVE THREATS
97 Privileged account hashes found on 347 machines

PASS-THE-HASH: INACTIVE THREATS
277 Privileged account hashes previously existed on 481 machines (Last 90 days)

PASS-THE-HASH: MITIGATED WITH PRIVILEGED ACCOUNT SECURITY
Privileged Accounts Security can frequently change Privileged account passwords, turning hashes from Active to Inactive. The data below simulates the use of one-time passwords on all Privileged accounts.
Before: 97 Privileged account hashes on 347 machines
After: 12 Privileged account hashes on 3 machines

PASS-THE-HASH: ORGANIZATIONAL VULNERABILITY MAP
See a map of all vulnerable machines and machines causing vulnerabilities found in your organization

[OPEN PTH MAP](#)

VULNERABILITY STATUS

PASS-THE-HASH: VULNERABLE MACHINES



Vulnerable machines	953
Non-Vulnerable machines	614
Total Windows machines	1,567

Pass-the-Hash: Organizational Vulnerability Map



File server-1

11 Privileged account hashes found
36 Machines vulnerable as a result

Most active privileged account hashes

- IT_Admin
- SQL_DBA
- Backdoor
- Backup_USR
- JohnAdmin
- IT_Temp
- IIS_Admin
- Admin_1999
- test

CyberArk DNA™ | Discovery and Audit Report

EXECUTIVE SUMMARY

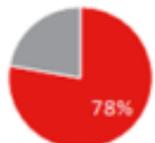
ABOUT THE SCAN

Scan date: Tuesday July 23 2013 11:18:00
 Licensee name: CyberArk
 Created by: Administrator
 Password policy: Passwords of compliant accounts are changed every 90 days

Windows computer types: Servers and workstations
Windows object types: Accounts, Service accounts
Unix computer types: Servers and workstations
Unix object types: Accounts
LDAP path: OU=Computers,OU=DNA ToolDC=DN A-demo,DC=local

COMPLIANCE STATUS

WINDOWS NON-COMPLIANT



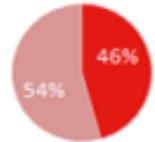
Non-compliant accounts	3,752
Compliant accounts	1,071
Total Windows accounts	4,823

UNIX NON-COMPLIANT



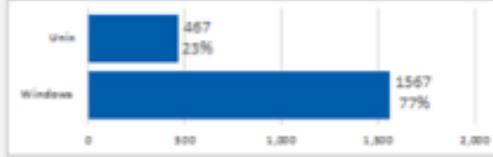
Non-compliant accounts	1,278
Compliant accounts	1,021
Total Unix accounts	2,299

TOTAL NON-COMPLIANT



Privileged accounts	2,291
Non-privileged accounts	2,739

COMPUTERS SCANNED

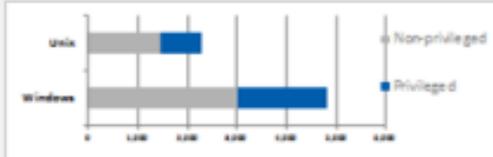


Unix	467	23%
Windows	1,567	77%

OS

Windows	1,567
Unix	467
Total computers scanned	2,034

ACCOUNTS DETECTED



Non-privileged	3,000	1,453
Privileged	1,823	846
Total accounts detected	4,823	2,299

Обязательные составляющие успеха



**Управление
учетными данными**

Пароли, SSH ключи,
файлы

Защищенное хранилище
Отсутствие агентов/клиентов
Взаимная аутентификация



**Изоляция и
контроль сессий**

Блокировка опасного
кода и контроль
доступа

Протоколнезависимость
Платформнезависимость
Высокая доступность



**Мониторинг
активности**

Постоянный
автоматический
анализ

Автономный анализатор
Интеграция с SIEM
Независимый аудит



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



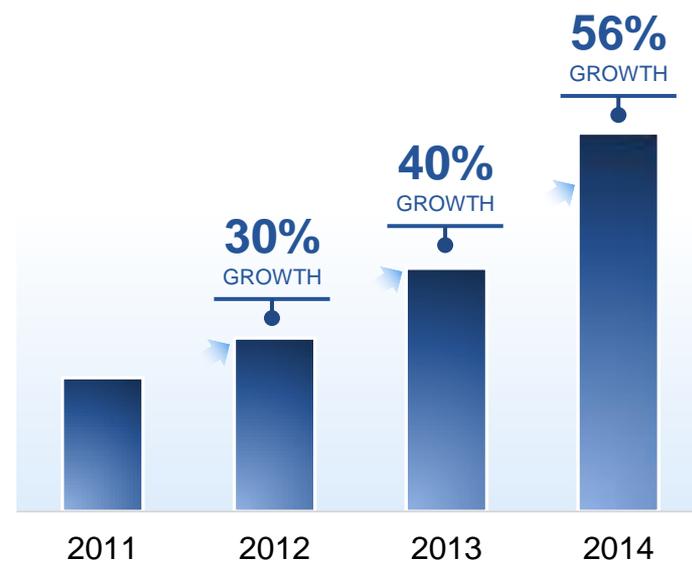
17 лет инноваций

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



Лучшее решение

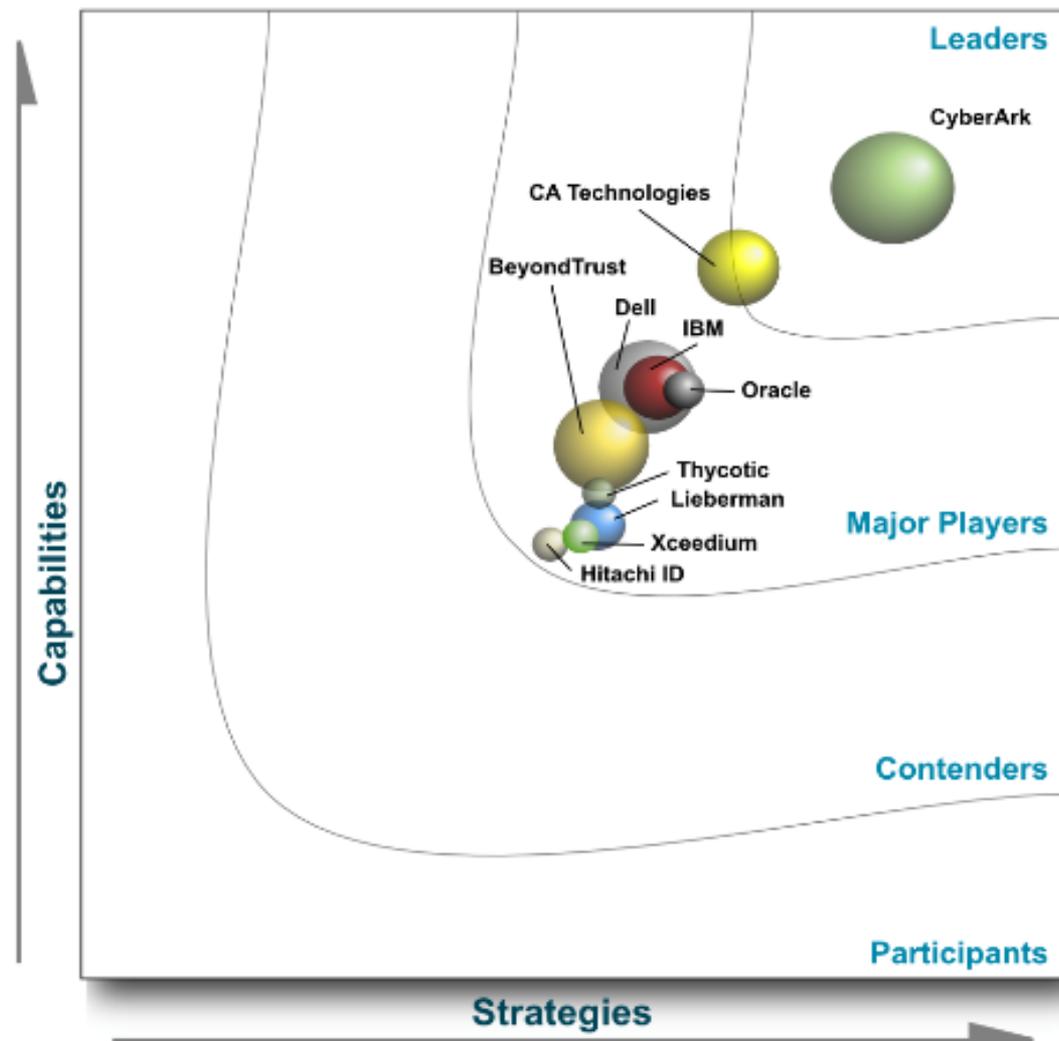
- Одно решение, исключительно сфокусированное на защите привилегированных аккаунтов
- Enterprise-proven



CYBERARK

Рекомендуем ознакомиться

IDC MarketScape: Worldwide Privileged Access Management



ccess



CYBERARK



CYBERARK®

Спасибо за внимание...