



## Эффективные инструменты ИБ – для бизнеса и специалистов

Богдан Тоболь, региональный менеджер

Олег Котов, сейлз-инженер



CYBERARK®



Кто  
нарушитель?

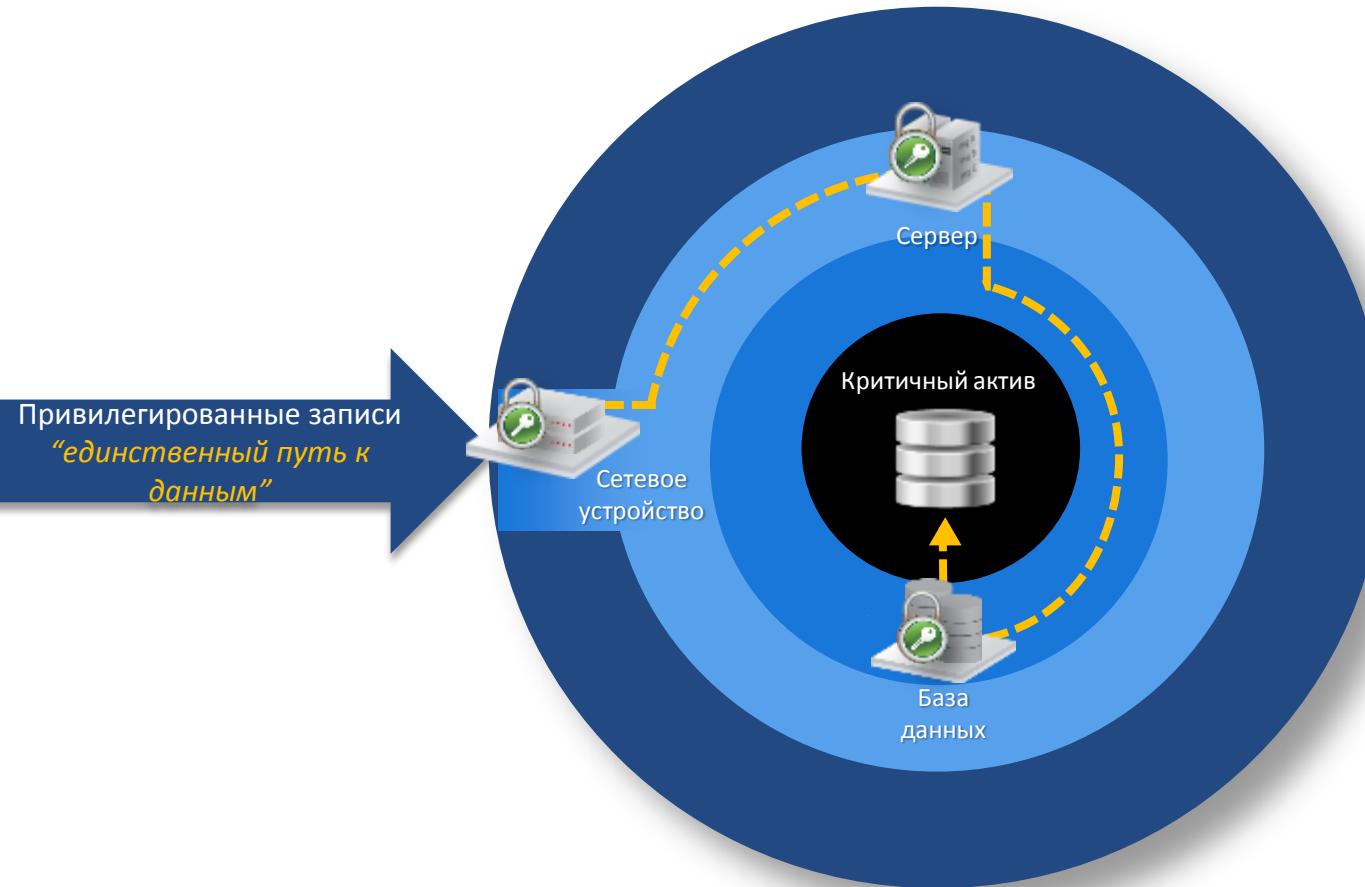
# You Need to Know!

Кто  
авторизован?



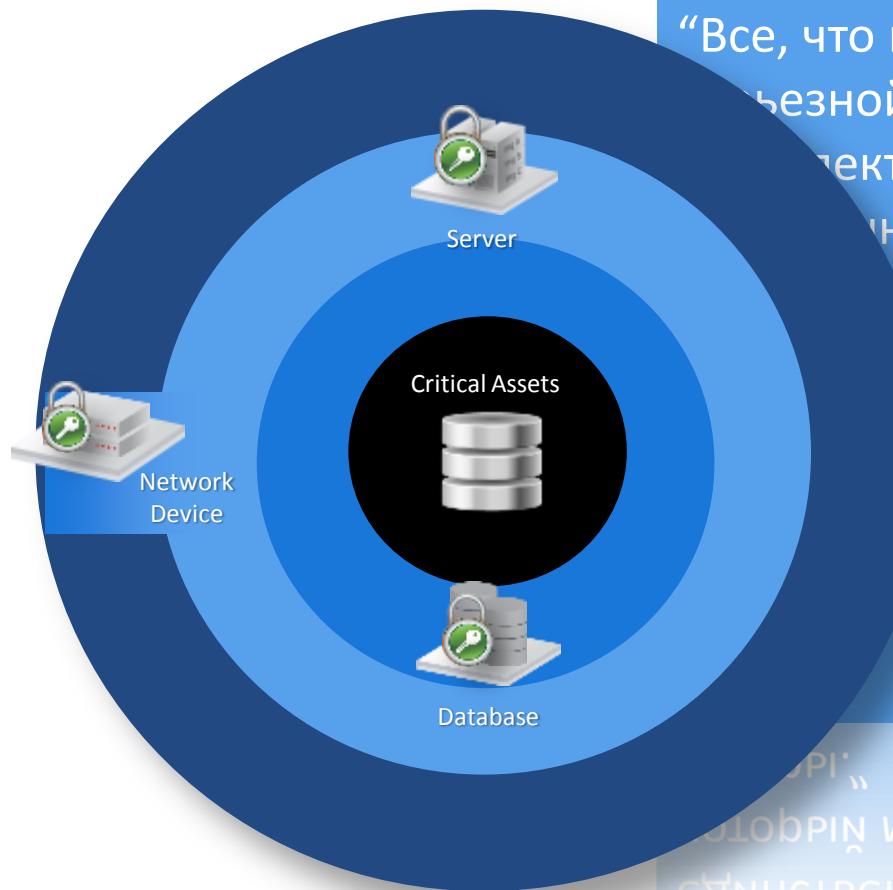
CYBERARK®

# «Все пути ведут...» к привилегированным записям



CYBERARK®

# Привилегированные записи – встроенные уязвимости (Gartner)



“Все, что касается  
безной  
текущальной  
ности,  
ся в хорошо  
ых системах, и  
рованные  
писи являются  
ным способом,  
логут получить

Avivah Litan, Vice President and Distinguished Analyst at Gartner  
*Malware Targets Vulnerable Admin Accounts*, Wall Street Journal June 2012



CYBERARK®

# Привилегированные аккаунты – вторжение

## South Korea Blames North Korea for Cyber Attack

By Adario Strange | April 10, 2013 10:15am EST | 1 Comment



Last month's mysterious cyber attack that disrupted banks and television stations in South Korea was executed by North Korea's intelligence agency, according to official investigators based in Seoul.

The findings were revealed in the *Korea Herald* today as South Korea's Ministry of Science, (information communications technology) Future Planning connected the attacks to North Korea's Reconnaissance General Bureau.

On March 20, the computer systems of local Korean television stations KBS, YTN, and MBC, as well as banking firms Shinhan, Jeju, and NongHyup experienced major disruptions in what appeared to be a coordinated attack.

Because of recent regional tensions, South Korea has been investigating the source of the attack.

**News**

### Insiders exploiting privileged accounts likely behind Saudi Aramco attack

24 October 2012

With the recent attack on Saudi oil giant Aramco being credited to Iran by the US government, a new report suggests that it may have been an inside job.

The [New York Times](#) noted that after analyzing the software code from the attack, security researchers found a company insider with

## CHINESE HACKERS TARGET NEW YORK TIMES IN FOUR-MONTH CYBERATTACK

THE CYBERATTACKS DATE BACK TO WHEN THE NEWSPAPER PUBLISHED AN EXPOSE DETAILING THE WEALTH ACCUMULATED BY THE PREVIOUS CHINESE PREMIER, WEN JIBAO.

By ADARIO STRANGE

FAST FEED

0 10 4

Topic: Security Discover Follow via: RSS Email

## Swiss spy agency warns CIA, MI6 over 'massive' secret data theft

**Summary:** Switzerland's national security agency warns that a huge amount of secret, counter-terrorist data may have been leaked by no other than a disgruntled 'administrator-level' employee.

By Zack Whittaker for Zero Day | December 4, 2012 -- 13:58 GMT (05:58 PST)

Follow @zackwhittaker

Secret counter-terrorism information shared by foreign governments, which may not limited to the U.K. and U.S. administrations, is thought to have been stolen by a senior IT employee of Switzerland's state intelligence service.

First reported by the [Reuters](#) news agency, the U.S.' Central Intelligence Agency (CIA) and the U.K.'s Secret Intelligence Service (MI6), have been warned that data they shared may no longer be secret.



CYBERARK®

# Типичная атака

---



- Несколько месяцев подготовки атаки
- Изучение распорядка дня, круга общения и мероприятий
- Доставка модуля на один компьютер – рабочее место админа
- Модуль сбора информации – адреса серверов, аккаунты
- Хищение данных вручную
- Нескольких месяцев присутствие в системе не обнаруживалось



CYBERARK®

# Привилегированные записи используются во всех современных атаках

“...100% вторжений использовали украденные учетные записи.”

“Продвинутый нарушитель предпочитает использовать привилегированные записи везде где возможно такие, как Администратор домена, служебная запись с доменными привилегиями, локальный администратор и привилегированный пользователь.”

Mandiant, M-Trends , APT1 Report



CYBERARK®

# Привилегированные записи – «Top 20» SANS

---

“Контролируемое  
использование  
административных  
привилегий:  
Идентификация и  
мониторинг  
административных  
записей...”

ЗАПИСЕЙ... “  
ADMINISTRATIVE RECORDS”

SANS; Top 20 Security Controls, #12



CYBERARK®

# Привилегированный аккаунт: что, где и почему

	Какие	Кем используются	Используются для
Привилегированные персональные	<ul style="list-style-type: none"><li>Облачные провайдеры</li><li>Персональные записи с широкими привилегиями</li></ul>	<ul style="list-style-type: none"><li>IT службы</li><li>Сотрудники</li></ul>	<ul style="list-style-type: none"><li>Привилегированные операции</li><li>Доступ к критичной инф.</li><li>Веб-сайты</li></ul>
Общие привилегированные	<ul style="list-style-type: none"><li>Administrator</li><li>root</li><li>System</li><li>Oracle SYS</li><li>Local Administrators</li></ul>	<ul style="list-style-type: none"><li>IT службы</li><li>Системные администраторы</li><li>DBA</li><li>Help desk</li><li>Разработчики</li><li>Менеджеры по IT</li><li>Наследуемые прилож.</li></ul>	<ul style="list-style-type: none"><li>Аварийные</li><li>Высокий SLA</li><li>Катастрофоустойчивость</li><li>Привилегированные операции</li><li>Доступ к критичной инф.</li></ul>
Аккаунты приложений	<ul style="list-style-type: none"><li>Hard coded/ встроенные ID</li><li>Служебные записи</li></ul>	<ul style="list-style-type: none"><li>Приложения/скрипты</li><li>Windows Services</li><li>Scheduled Tasks</li><li>Batch jobs и т.д.</li><li>Разработчики</li></ul>	<ul style="list-style-type: none"><li>Онлайн доступ к БД</li><li>Batch processing</li><li>Взаимодействие App-2-App</li></ul>



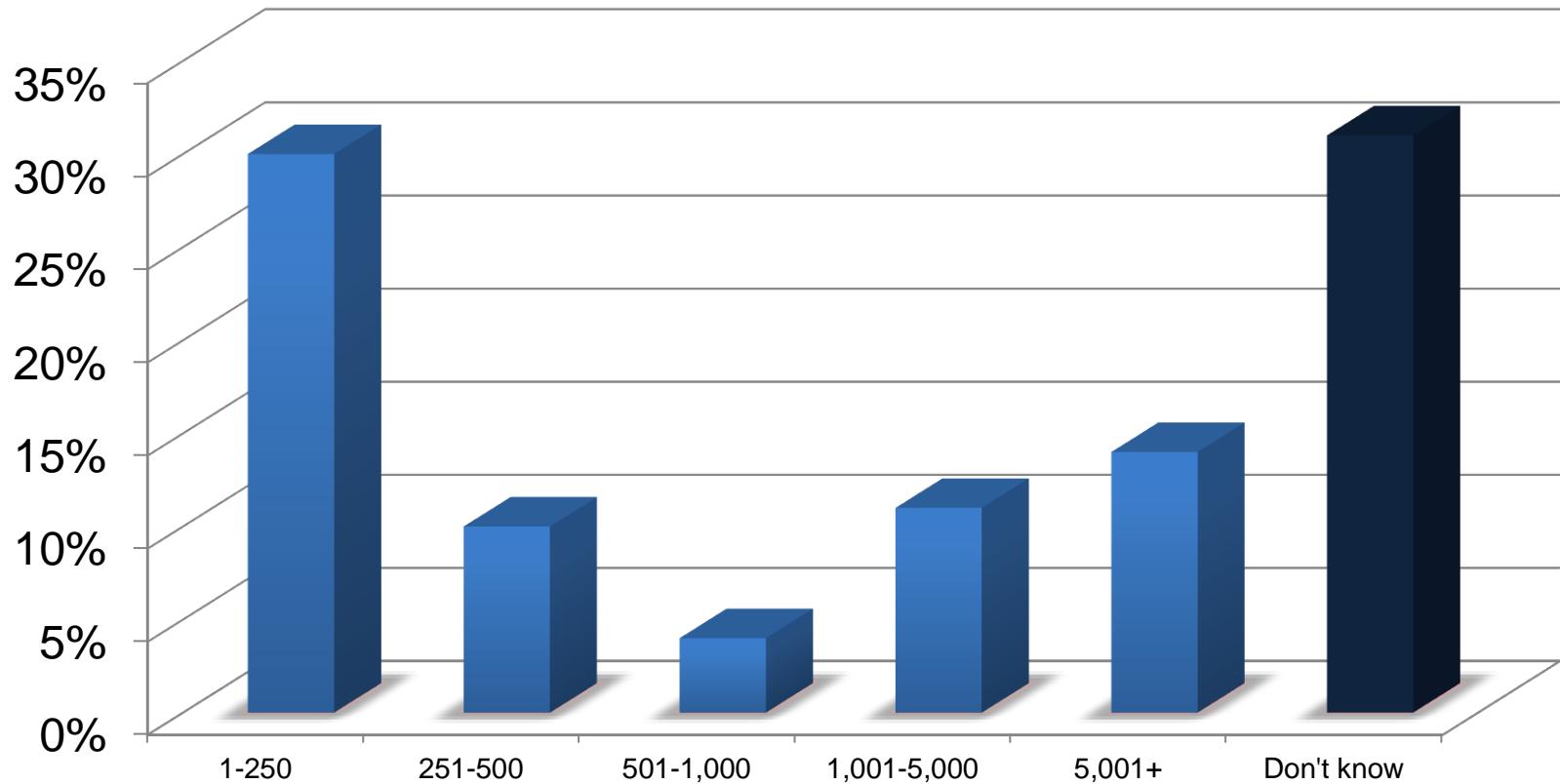
# Привилегированные записи везде!



CYBERARK®

# Но этот факт не понятен...

Сколько привилегированных записей в вашей системе?



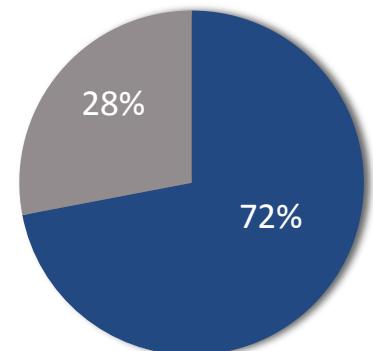
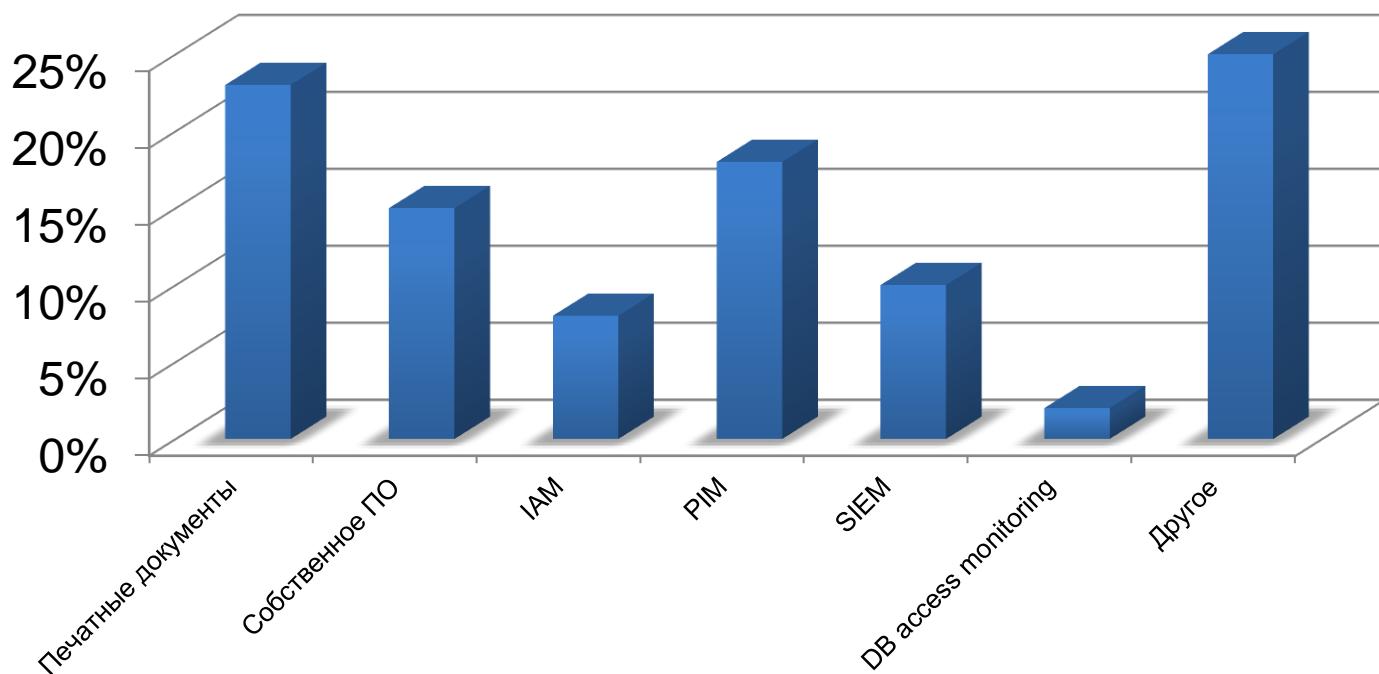
Cyber-Privileged Account Security & Compliance Survey, May 2013 (Enterprise > 5000 Employees)



CYBERARK®

# Используются вариации разных решений

Как вы отслеживаете активность привилегированных записей?



Вы отслеживаете привилегированную активность?

# Факты говорят за себя...

Не существует идеальной защиты

Нарушители профессиональны и меняют тактику все время.

Компании, уделяющие серьезное внимание ИБ и инвестирующие в ИТ, все равно подвергаются компрометации.

**100%**

Жертвы обновляли антивирусы



**94%**

Вторжений были замечены 3-ми лицами



**416**

Дней (в среднем) атака в сети не замечена



**100%**

Вторжений использовали украденные УЗ



Mandiant, 2013



CYBERARK®

# 4 обязательных шага для противодействия

---



**1. Обнаруживать все привилегированные записи**



**2. Защищать и управлять привилегированными аккаунтами**



**3. Контролировать, изолировать и отслеживать привилегированный доступ к серверам, БД и виртуальным платформам**



**4. Расследовать использование привилегированных записей в реальном времени**



CYBERARK®

# 1. Обнаружить все привилегированные записи



- Их больше, чем Вы думаете
- Вы должны знать о всех



CYBERARK®

## 2. Защищать и управлять записями

---



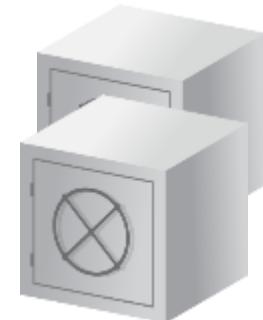
Убедитесь, что хранилище безопасно



Внедрите процедуры проверки доступа  
к привилегированным записям



Упростите управление политиками  
за счет унифицированных мастер-  
политик



CYBERARK®

### 3. Контролировать, изолировать и отслеживать

---



**Создайте единую точку контроля привилегированных сессий**



**Изолируйте вредоносный код от целевых систем**



**Отслеживайте и записывайте активность**



**Выбирайте масштабируемое, безагентское решение**



CYBERARK®

# Используйте расследование в реальном времени

Определяем атаку

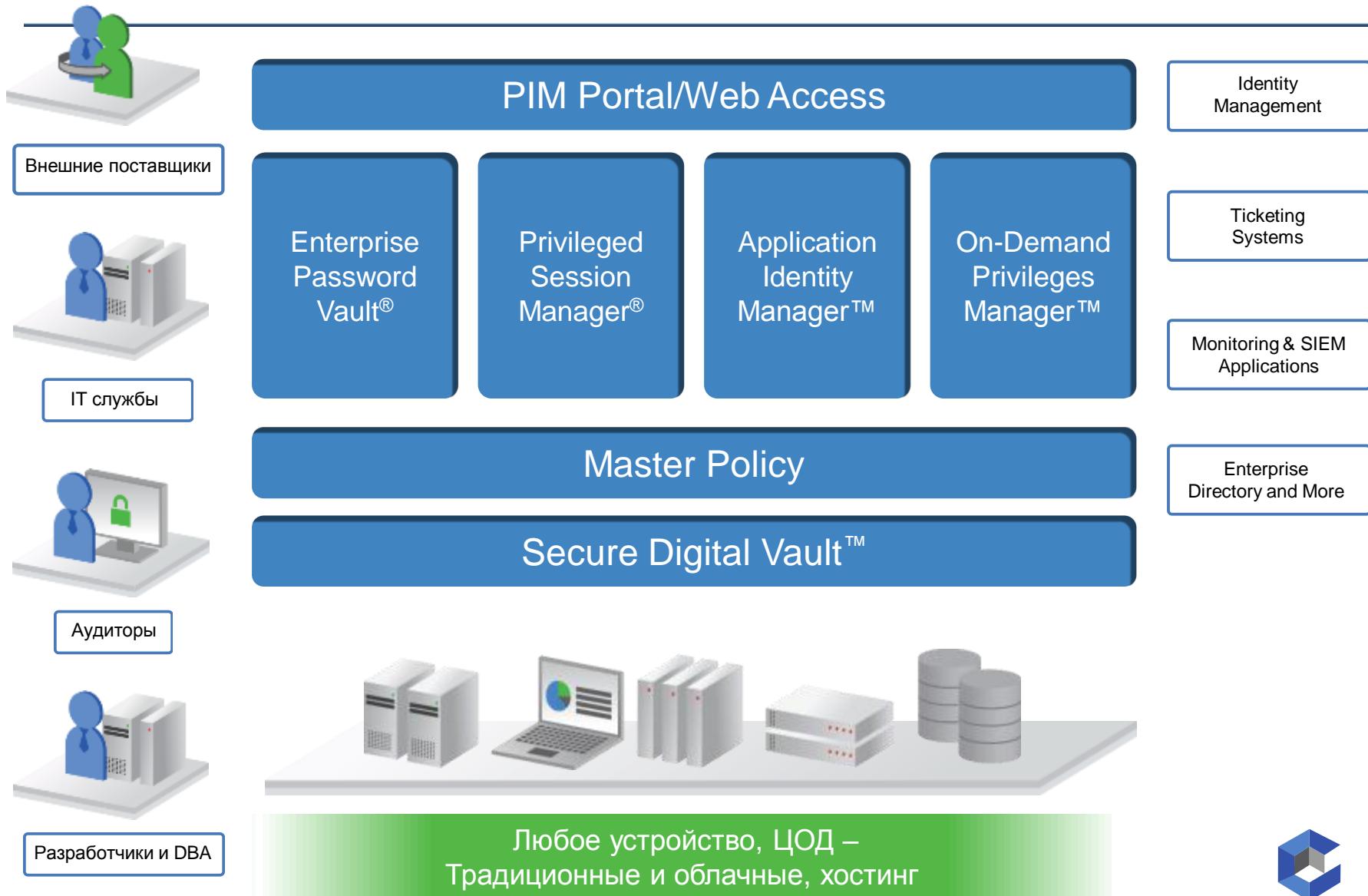
Интегрируем с SIEM

Выполняем и индексируем запись



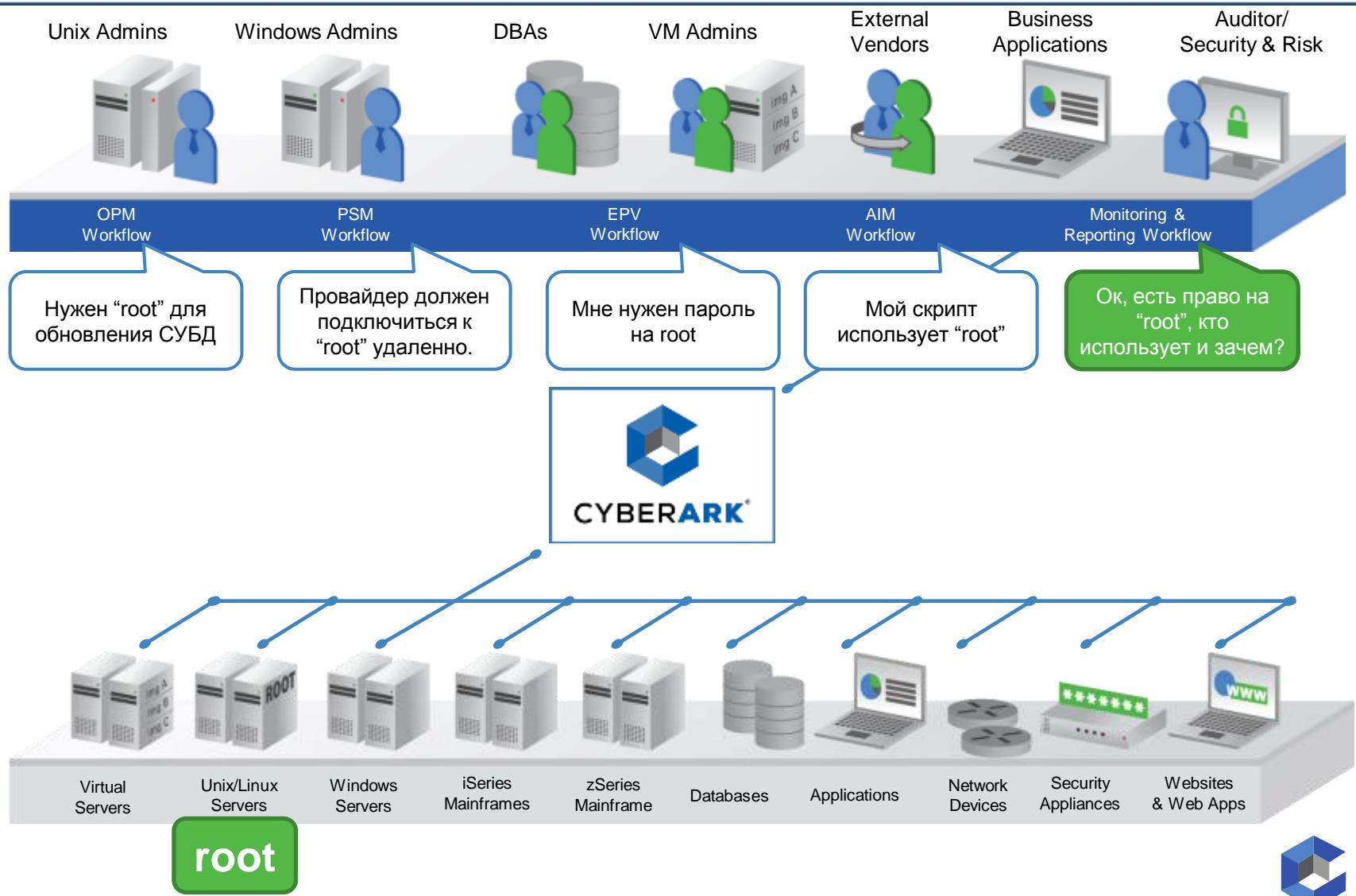
CYBERARK®

# Безопасность привилегированных записей



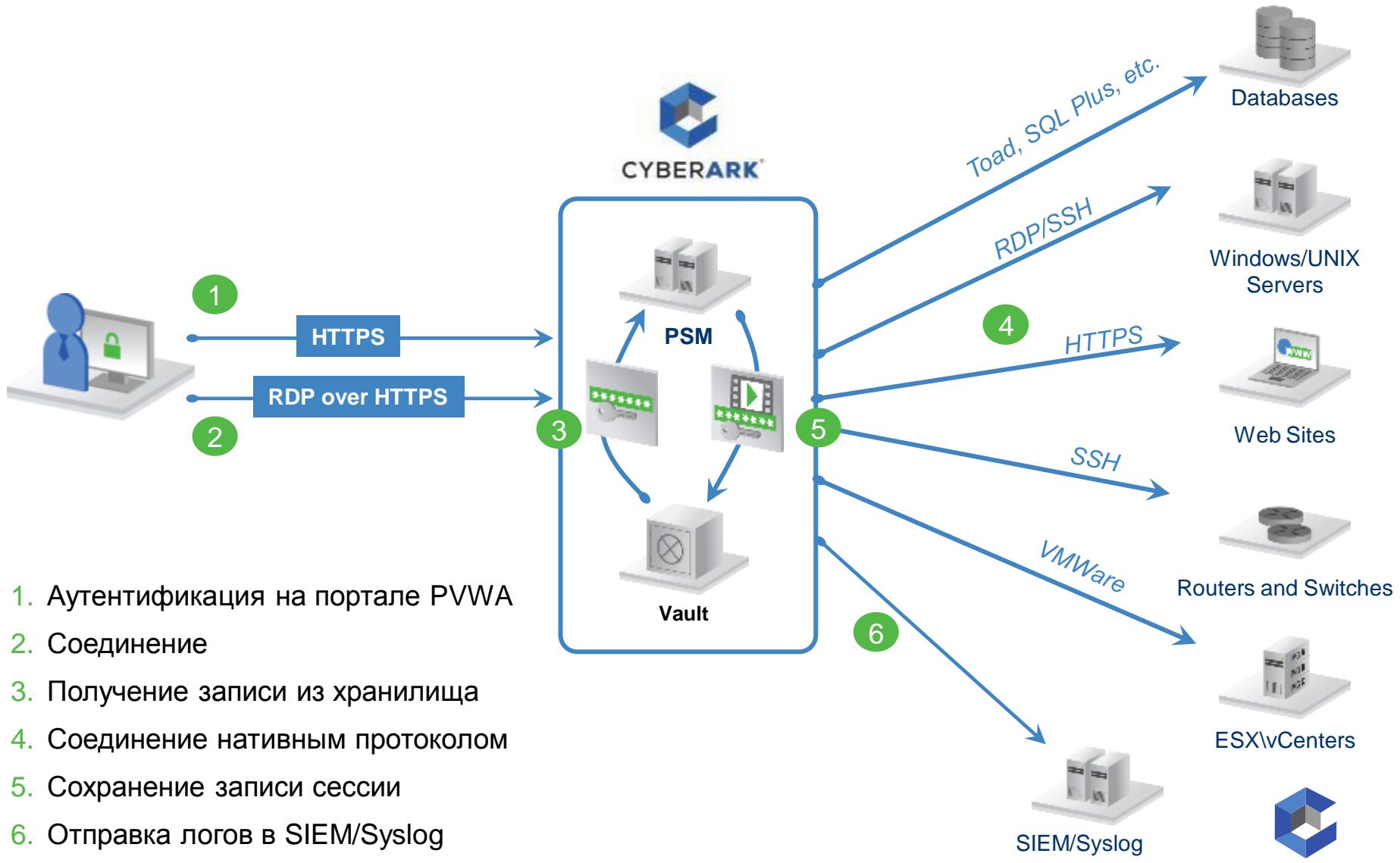
CYBERARK®

# Пример: управление привилегированными записями



CYBERARK®

# Privileged Session Manager (PSM)



# Устранение запрограммированных паролей

Конфигурационные  
файлы, базы данных

Сервера приложений

Служебные аккаунты

Запрограммируемые,  
встроенные аккаунты

Сторонние  
приложения

Конф.файлы Веба  
INI/текстовые файлы  
БД приложений

*В реестрах, FTP и т.д.*

- Windows service
- Scheduled tasks
- IIS application pool
- IIS Directory Security
- COM+
- Registry

Password = у/чегЭ!  
Host = "10.10.3.56"

ORACLE®

Q QUALYS®

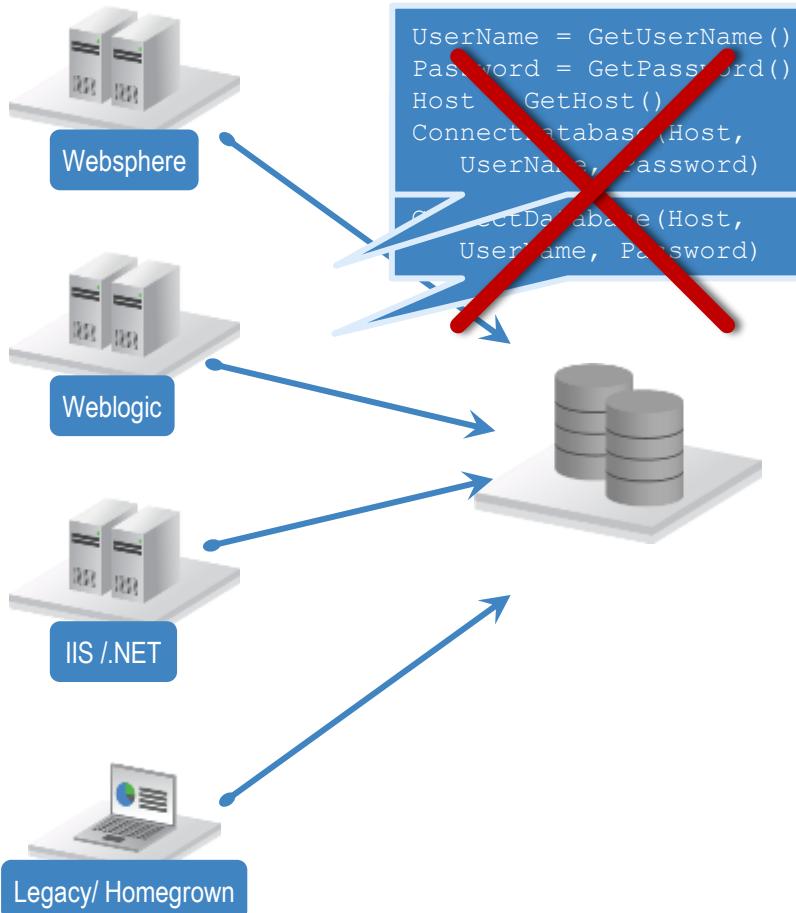
McAfee®



CYBERARK®

# Application Identity Management (AIM): Выше защита; Ближе соответствие

Billing App



- Защищает и сбрасывает учетную запись приложения без простоя и рестарта
- Безопасно кэширует для непрерывности бизнеса и высокой производительности
- Исключает изменение кода и затраты на изменения паролей или адресов машин
- Строгая аутентификация по:
  - Адресу машины
  - Пользователю OS
  - Адресу приложения
  - Цифровой подписи/хешу

HR  
App

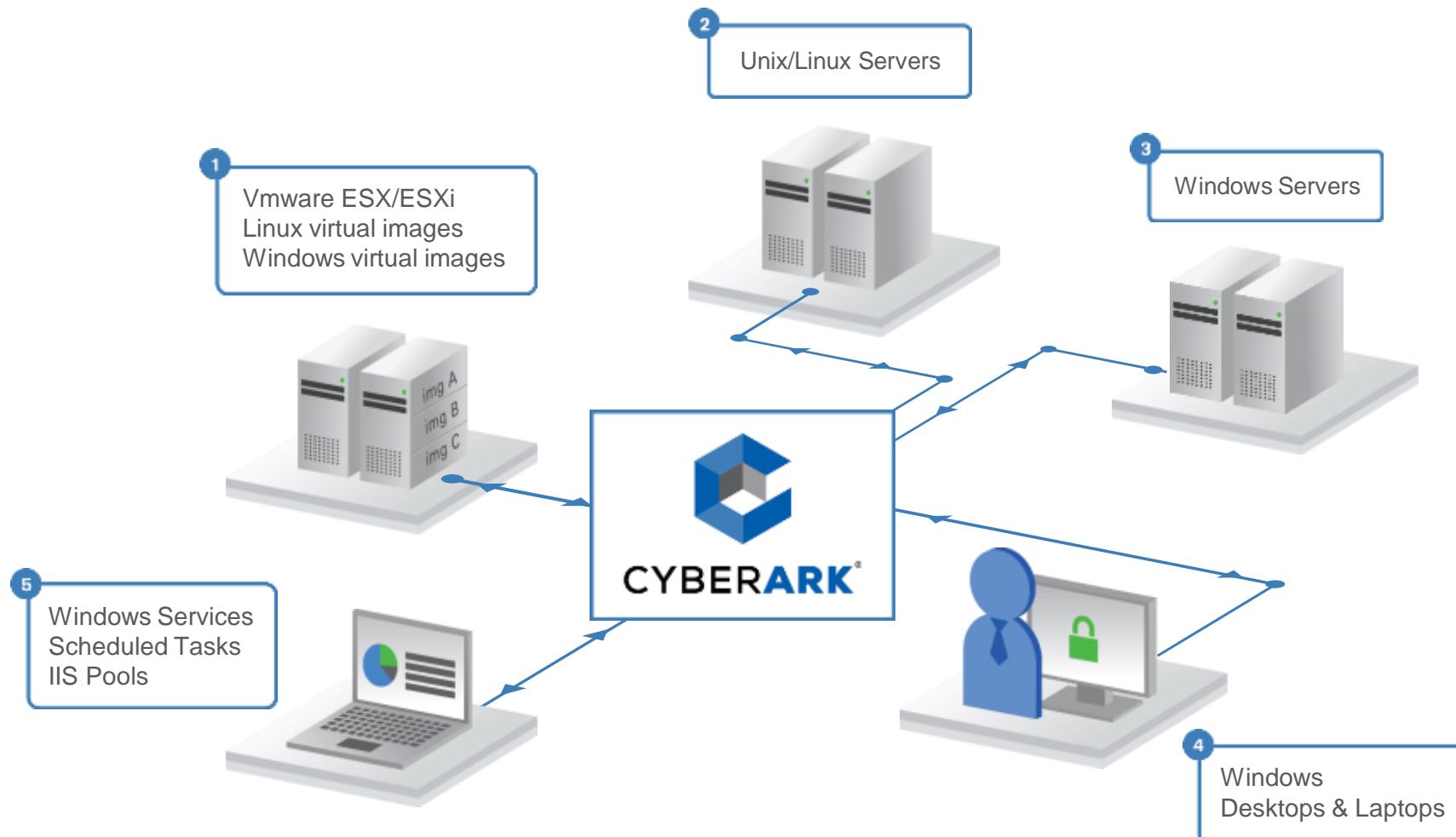
Online  
Booking  
System

Защищает, управляет и устраниет встроенные  
привилегированные аккаунты из приложений



CYBERARK®

# EPV: автоматическое определение привилегированных аккаунтов всей системы



Где привилегированные записи и суперпользователи?



CYBERARK®

# On-demand Privileges Manager (OPM) for Unix

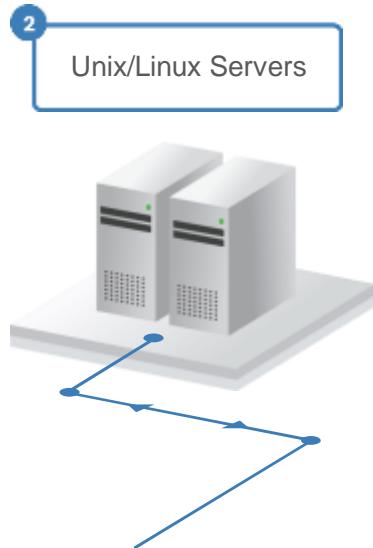
The screenshot shows a software interface with a toolbar at the top containing various icons for data management. Below the toolbar is a header with five columns: When, Who, What, Where, and What. The 'What' column is highlighted in blue. The main area displays a table of log entries:

Time	User	Action	Target System	Target Port	Command
2/28/2011 10:33:07 AM	paul	Privileged command initiated	root	rhe1.cyberark-demo.local	/sbin/iptables -list, Current Working Directory: /home/paul
3/1/2011 9:33:36 AM	PasswordManager	Retrieve password	root	rhe1.cyberark-demo.local	/sbin/iptables -list
3/1/2011 9:35:54 AM	Mike	Retrieve password	root	rhe1.cyberark-demo.local	/sbin/iptables -list

Мониторинг и аудит, отчеты и запись текстовых команд



Контроль суперпользователя



Add	Authorized User	Type
/bin/kill .*	Unix Team	Allow
/sbin/iptables .*	Unix Team	Allow
/sbin/service	Operations Team	Allow
/usr/bin/reboot	Unix Team	Deny

Гранулярный контроль  
доступа и политик



CYBERARK®

# OPM for Windows

- Снижает ТСС

- Минимум привилегий, ниже “непреднамеренный ущерб”
- Gartner: “Снижает ТСС минимум на 20%”

Standard User

- Снижает риск информационной утечки

- 90% уязвимостей Windows не используются без привилегий admin
- Исключая привилегии

Problem Applications

Basic Admin Tasks

Software Installation



Privilege  
Guard

Microsoft Bulletins ID	Severity	Code Analysis	Restart Requirement	Affected Software
MS09-020	High	Code analysis	Requires restart	Microsoft Windows, Internet Explorer



CYBERARK®

# Обмен файлами бизнес-пользователей

---

- Решения совета директоров, руководства, бизнес-планы
- Инженерная разработка, файлы дизайна
- Управление продуктом/ проектом/ развитием
- Юридический департамент
- Финансовые службы, бухгалтерия
- HR - зарплаты, контракты, характеристики, опционы
- Управление документами
- ИБ компании
- Конкурсные документы



# SIM – изоляция конфиденциальной информации

File Root\2010\Michael-Black.docx (Created on 23/05/2010 16:25:17 by Dave)

User Details: Linda

User	Last Access
Linda	23/05/2010 16:34:32
Dave	23/05/2010 16:25:33
All Users	

Action Time Previous Location Target User Reason

Store File	23/05/2010 16:34:32	Root\2010\Michael-Black.docx		
Retrieve File	23/05/2010 16:32:27	Root\2010\Michael-Black.docx		

Refresh Close

Зашифрованные архивы



Защищенная почта, уведомления  
и детальные отчеты

Request to retrieve data123.xls

This operation requires confirmation.

Reason:  
Need to Review Report for H1 Board Meeting

Access is required from 23/05/2010 16:30:09 to 26/05/2010 16:30:09

Multiple access is required during this period

Send Cancel

Двойной контроль

All files in folder Root\2010

Versions:

- Jim-Stinson.docx
- Layout plans.docx
- Michael-Black.docx
  - Version of 23/05/2010 16:45:47 by Dave (141KB)
  - Version of 23/05/2010 16:45:05 by Dave (114KB)
  - Version of 23/05/2010 16:34:32 by Linda (114KB)
  - Version of 23/05/2010 16:25:17 by Dave (0KB)

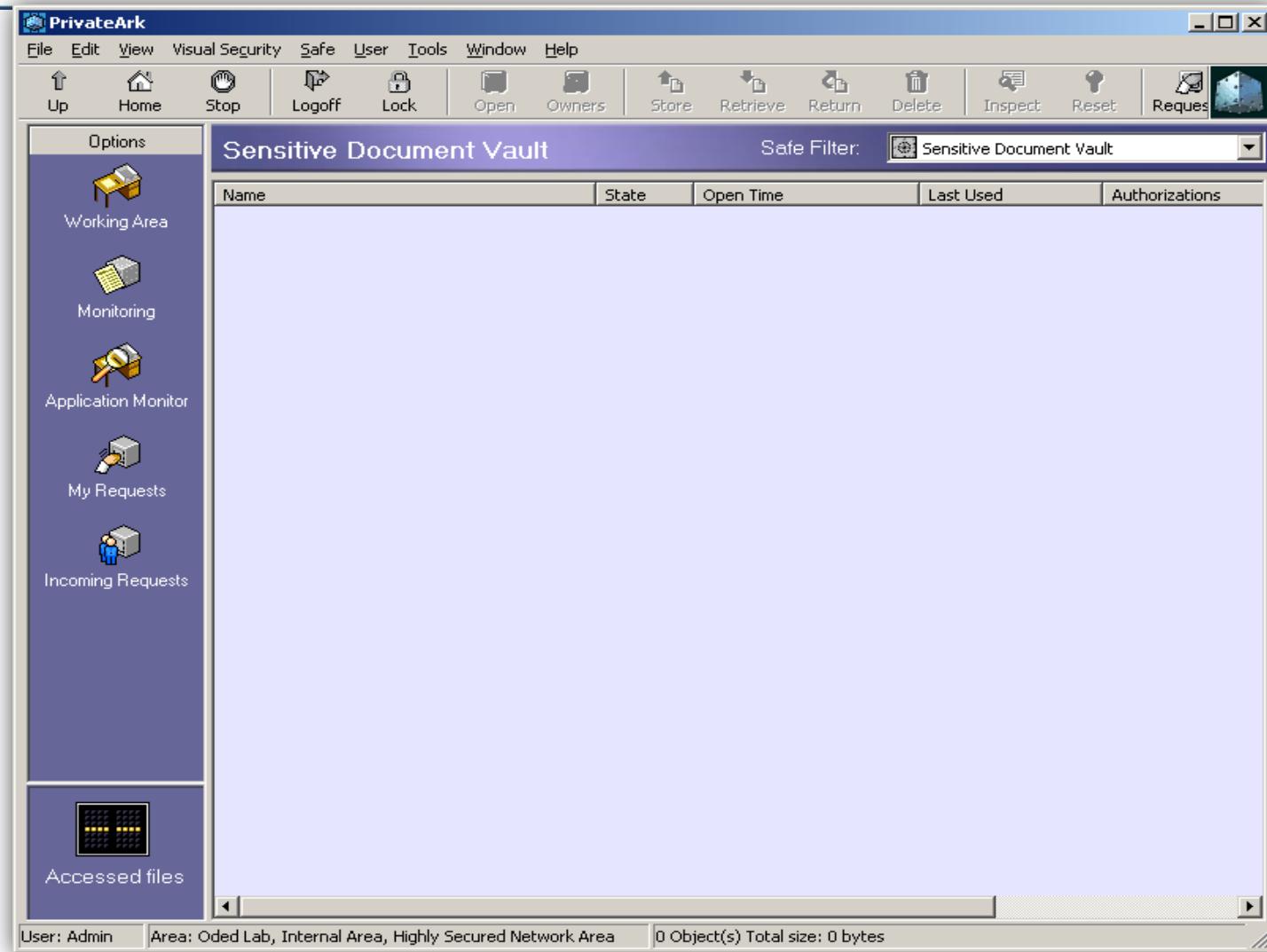
Retrieve Validation Make Current Version Undelete Close

Версии



CYBERARK®

# SIM – администратору нет доступа к данным



CYBERARK®

# SIM: Enterprise Ready – готовая интеграция

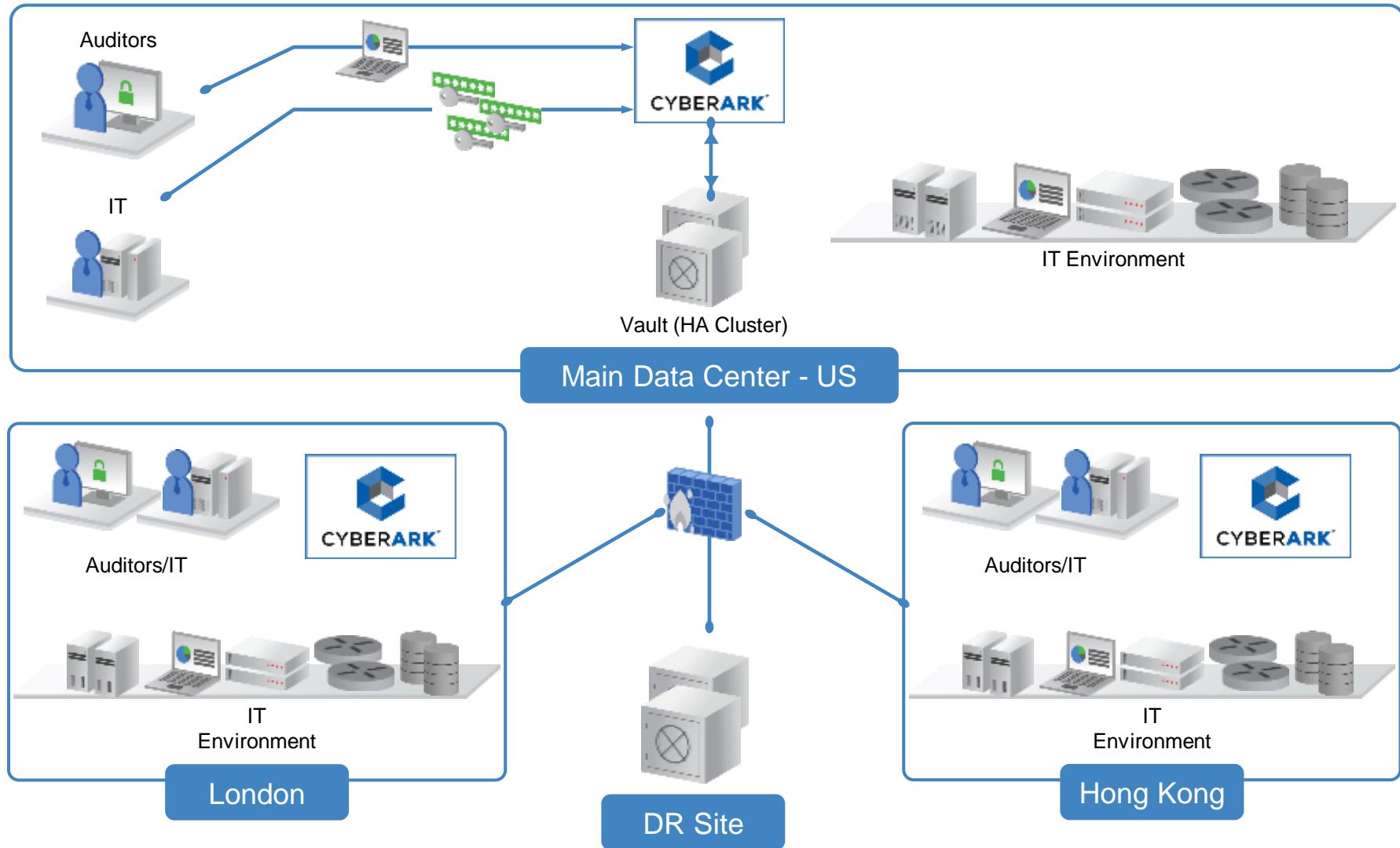
Отказоустойчивость	High Availability	Disaster Recovery	External Storage	Encrypted Backup			
Протоколы	Vault Protocol	FTP	FTP over SSL/TLS	SFTP / SSH	HTTP/S	SCP	
Аутентификация	Username / Password	RSA SecurID	Radius	PKI	Oracle SSO	LDAP	
LDAP	Active Directory	Sun One	Novell	Oracle	Any LDAP server		
SIEM и мониторинг	ArcSight	RSA Envision	CA Unicenter	IBM Tivoli	HP OpenView		
Контент и шифрование	WebSense	McAfee	TrendMicro	PGP integration	Generic Integration		
Backend	As400	Main Frame	BizTalk	Oracle Apps	MQ Series	Enterprise Service Bus	Generic Integration

Strategic Partnership



CYBERARK®

# Распределенная архитектура CyberArk



**CYBERARK**

# Решение проблем безопасности привилегированных аккаунтов

## Угрозы

- Современные атаки
- Инсайдеры
- Безопасность гибридных облаков
- Защита записей приложений
- Безопасность общих аккаунтов
- Обмен конфиден. информацией

## Аудит и соответствие

- Управление привилегиями Пользователей и отчетность
- Мониторинг и запись сессий
- Отчетность для соответствия
- Контроль удаленного доступа
- Аудируемый безопасный файлообмен

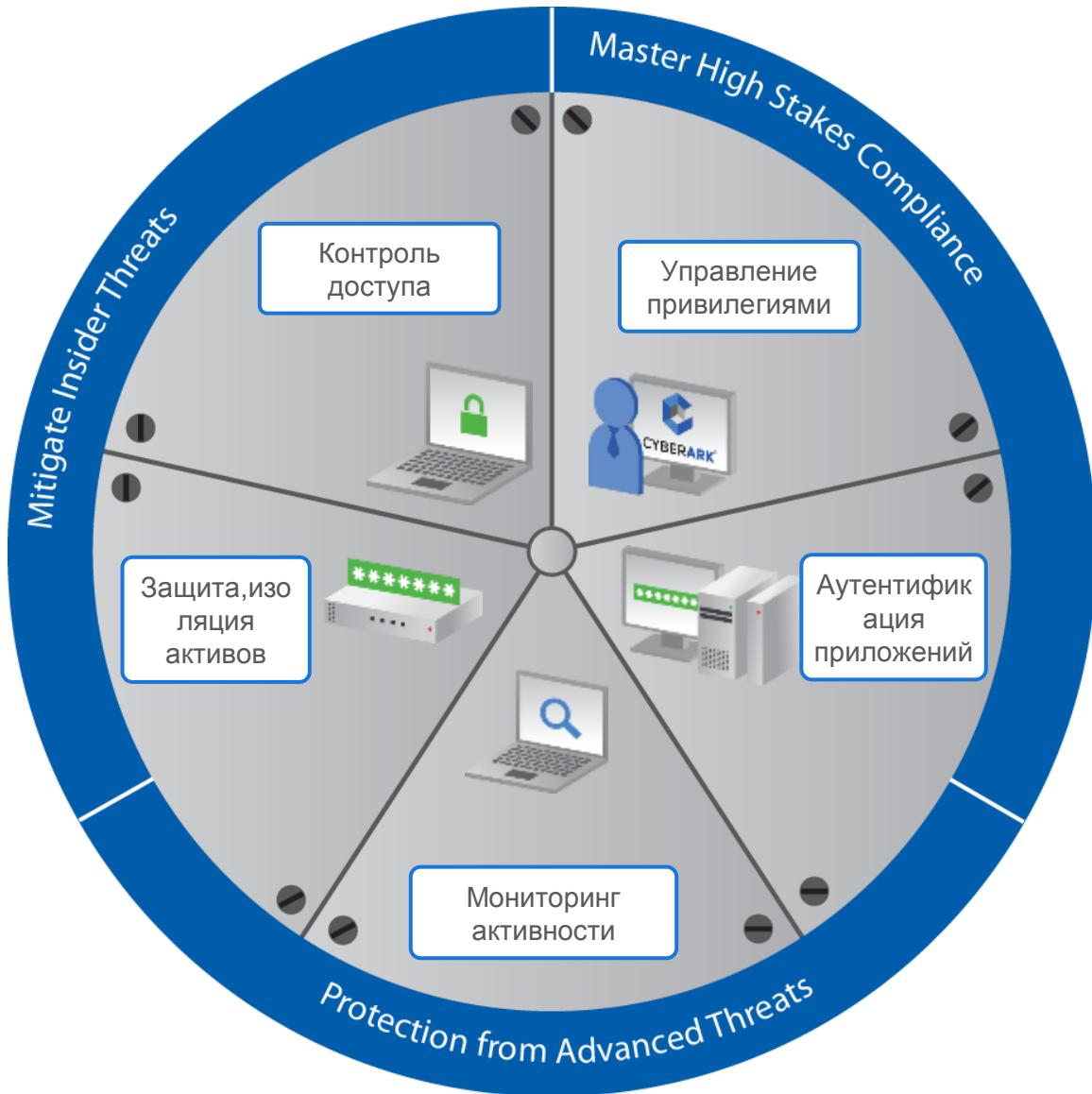
## Промышленные системы/АСУ ТП

- Безопасность и мониторинг общих админ. аккаунтов в АСУ ТП
- Контроль и мониторинг удаленных пользователей
- Безопасность Smart Grid



CYBERARK®

# Решение CyberArk для безопасности



CYBERARK®

# О компании CyberArk



## Доверенный эксперт в безопасности привилегированных записей

- Более 1,300 крупных корпоративных клиентов



## Управление привилегиями как новая безопасность

- Разрабатывается и создается по реальным потребностям



## Акцент на решение бизнес-задач

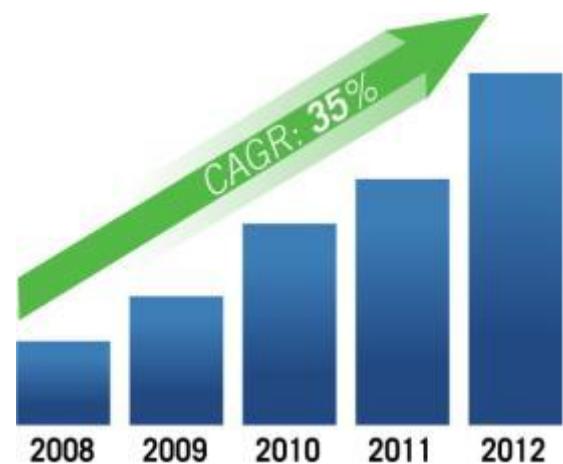
- Безопасность прозрачна для аудита



## Единое всестороннее решение

- Одно решение для всех задач
- Уровня Enterprise

## Глобальные клиенты



CYBERARK®

# Клиенты CyberArk в мире

## Communications & Media



belgacom



## Financial Services



ING GROUP



The Royal Bank of Scotland



BNP PARIBAS



## Pharmaceuticals

## Pharmaceuticals



AstraZeneca



MCKESSON

## Energy & Utilities



PEOPLES ENERGY



## Other Industries



TARGET



MOTOROLA

Доверенный эксперт для более чем 1,300 компаний мира



CYBERARK®

# Клиенты в регионе

Financial Services



Retail, Transport,  
Telecom



Others



РОСНАНО



CYBERARK



CYBERARK

Спасибо за Ваше внимание и время