



CYBERARK

CyberArk  
защита привилегированных  
учетных записей от внутренних  
и внешних кибератак

Богдан Тоболь

Региональный директор по продажам

# План

## Привилегированные учетные записи

### Актуальность и реальность угрозы

- В прикладных ИТ-системах

- 

### Решение проблем

- Управление привилегированными пользователями
- Контроль доступа и привилегированных сессий
- Центр оперативного реагирования

### Ответы на вопросы

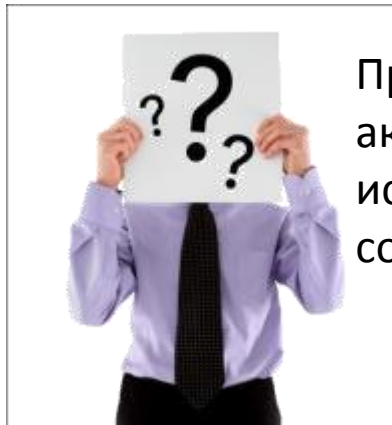
# Проблема привилегированных учетных записей.....



Бизнес без них не может.



Они предоставляют широкий доступ тем, что владеет ими.



Привилегированные аккаунты используются совместно.



Они не обеспечивают возможностей отследить кто их использует, и что с их помощью делает.

# 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>• Сотрудники</li> <li>• IT службы</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>• Cisco Enable</li> <li>• Oracle SYS</li> <li>• Local Administrators</li> </ul>	<ul style="list-style-type: none"> <li>• Системные администраторы</li> <li>• DBA</li> <li>• Help desk</li> <li>• Разработчики</li> <li>• Разработчики</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 ID</li> <li>• Служебные записи</li> </ul>	<ul style="list-style-type: none"> <li>• Приложения/скрипты</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>

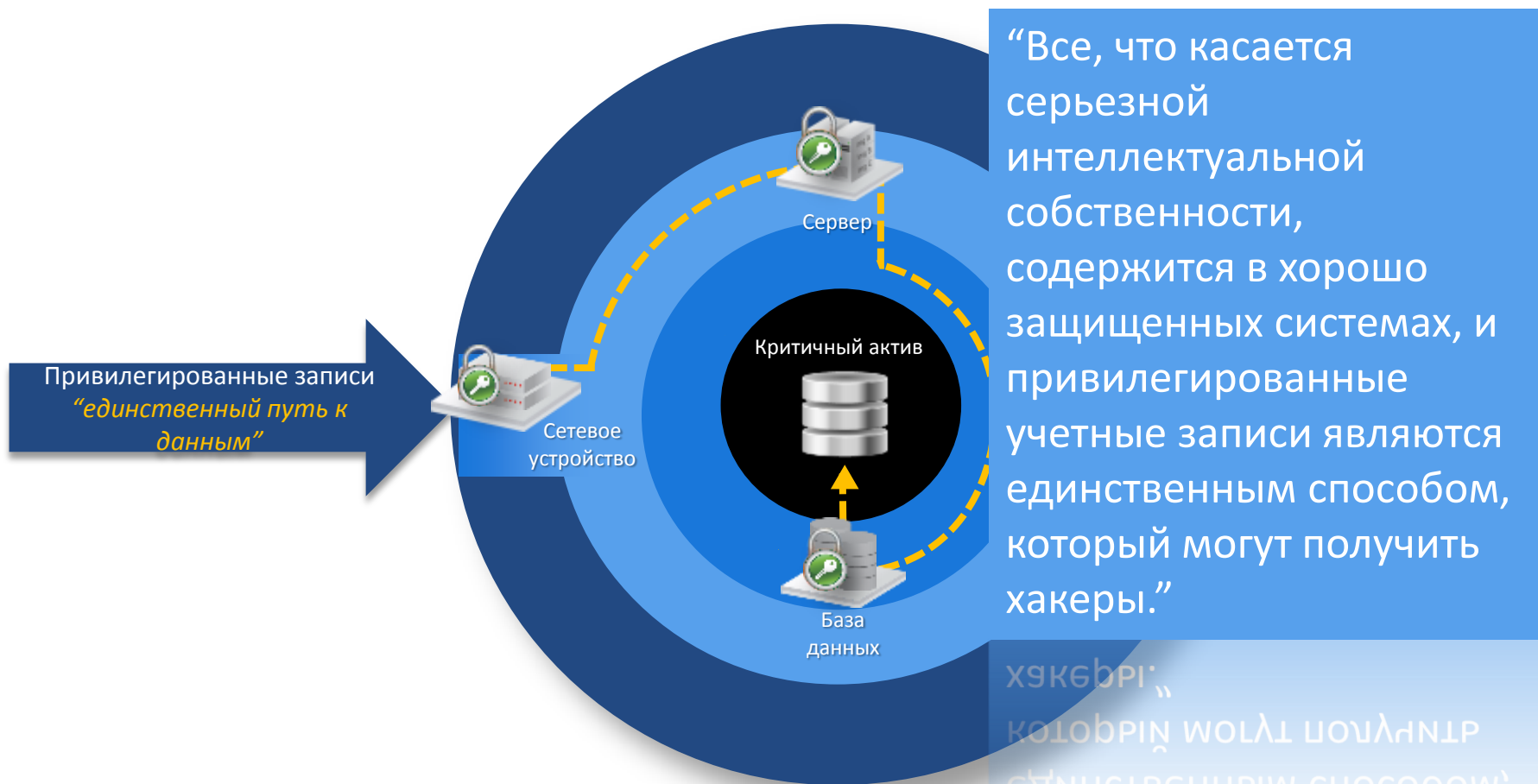
**Любая компания и организация является целью атаки**  
**Злоумышленники целенаправленны, настойчивы, скрытны**

**Высокие привилегии сложно контролировать, управлять и отслеживать**

**... ведут к критическим рискам при неправильном использовании**



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



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

- Концепция «доверия» администратору
- Любая компания, любая система

# 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 targeted banks and television stations in South Korea was executed by North Korea's intelligence agencies, according to official investigators based in Seoul.

The findings were revealed in the Korea Herald today as South Korea's Ministry of Science, ICT and 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, the attacks were widely expected.

FAST FEED

## 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 JIABAO.

BY ADDY CRIGANLE



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 be 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 Agency (MI6), have been warned that data they shared may no longer be just in

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

info security

STRATEGY /// INSIGHT /// TECHNIQUE

Dedicated to serving the information security community; In Person, In Print and Online.



CYBERARK

# 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%**

Жертв обновляли  
антивирусы



**94%**

Вторжений были  
замечены 3-ми  
лицами



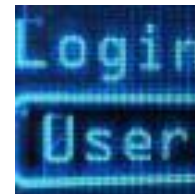
**416**

Дней (в среднем)  
атака в сети не  
замечена



**100%**

Вторжений  
использовали  
украденные УЗ



Mandiant, 2013



# Решаем проблемы привилегированных УЗ

## Целевые атаки (АРТ/АЕТ)

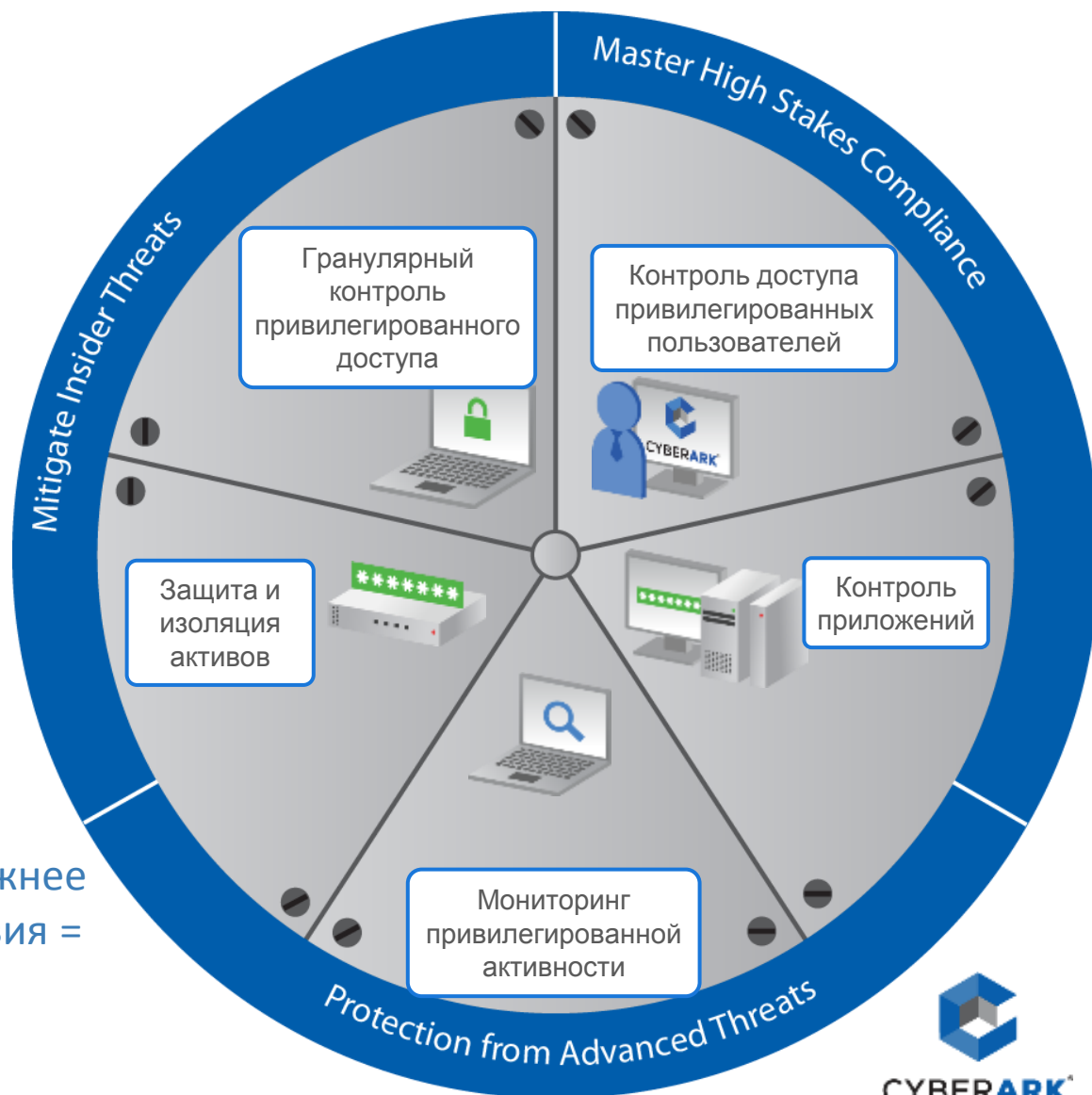
Спланированные, сложные  
На наиболее ценные активы  
Привилегированные аккаунты

## Инсайд и ошибки

Инсайдер поневоле?  
У инсайдера есть то, чего нет у хакера: доступ и доверие!

## Аудит и соответствие

Вопросы становятся шире и сложнее  
Стоимость отсутствия соответствия =  
2,65 \* стоимость соответствия





# Регуляторы требуют контроль и мониторинг привилегированных аккаунтов



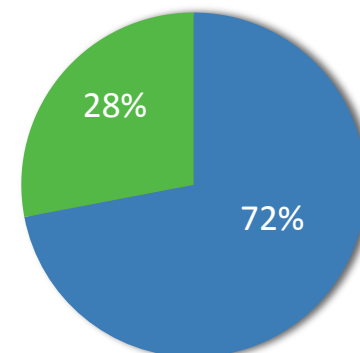
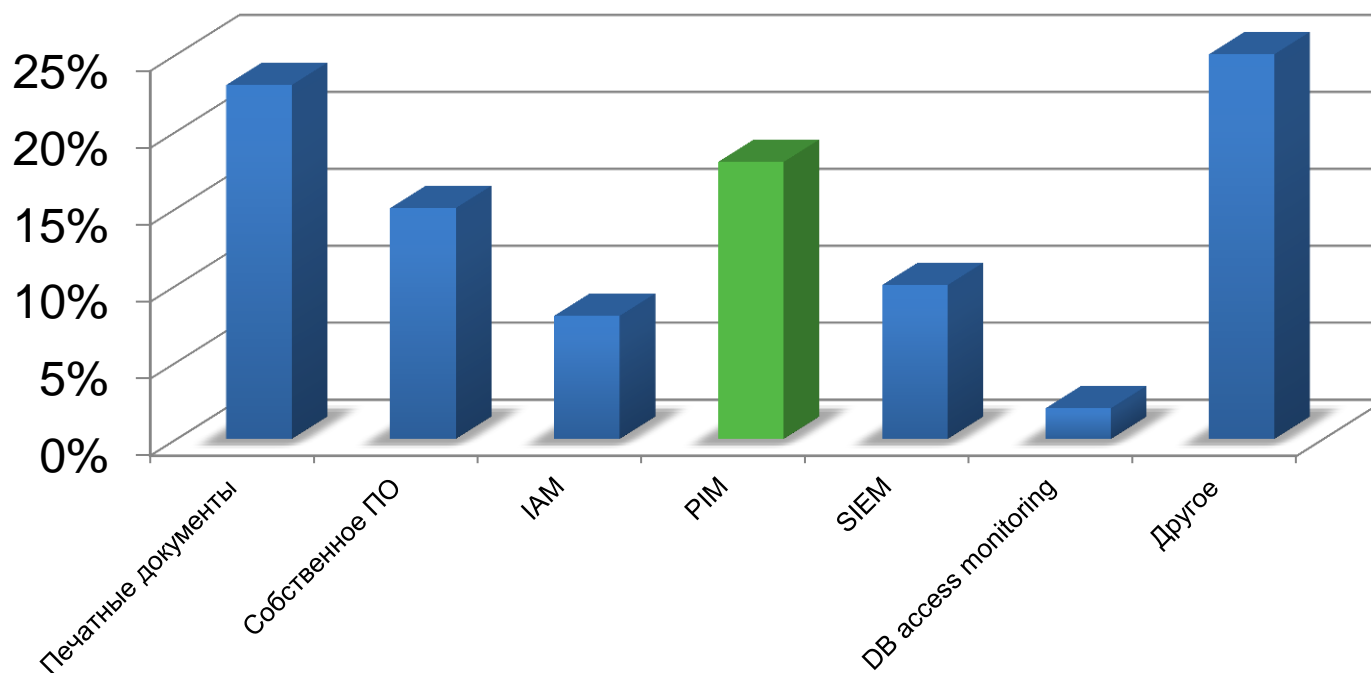
**Sarbanes-Oxley**  
Financial and Accounting Disclosure Information



CYBERARK

# Используются вариации разных решений

Как вы отслеживаете активность привилегированных записей?



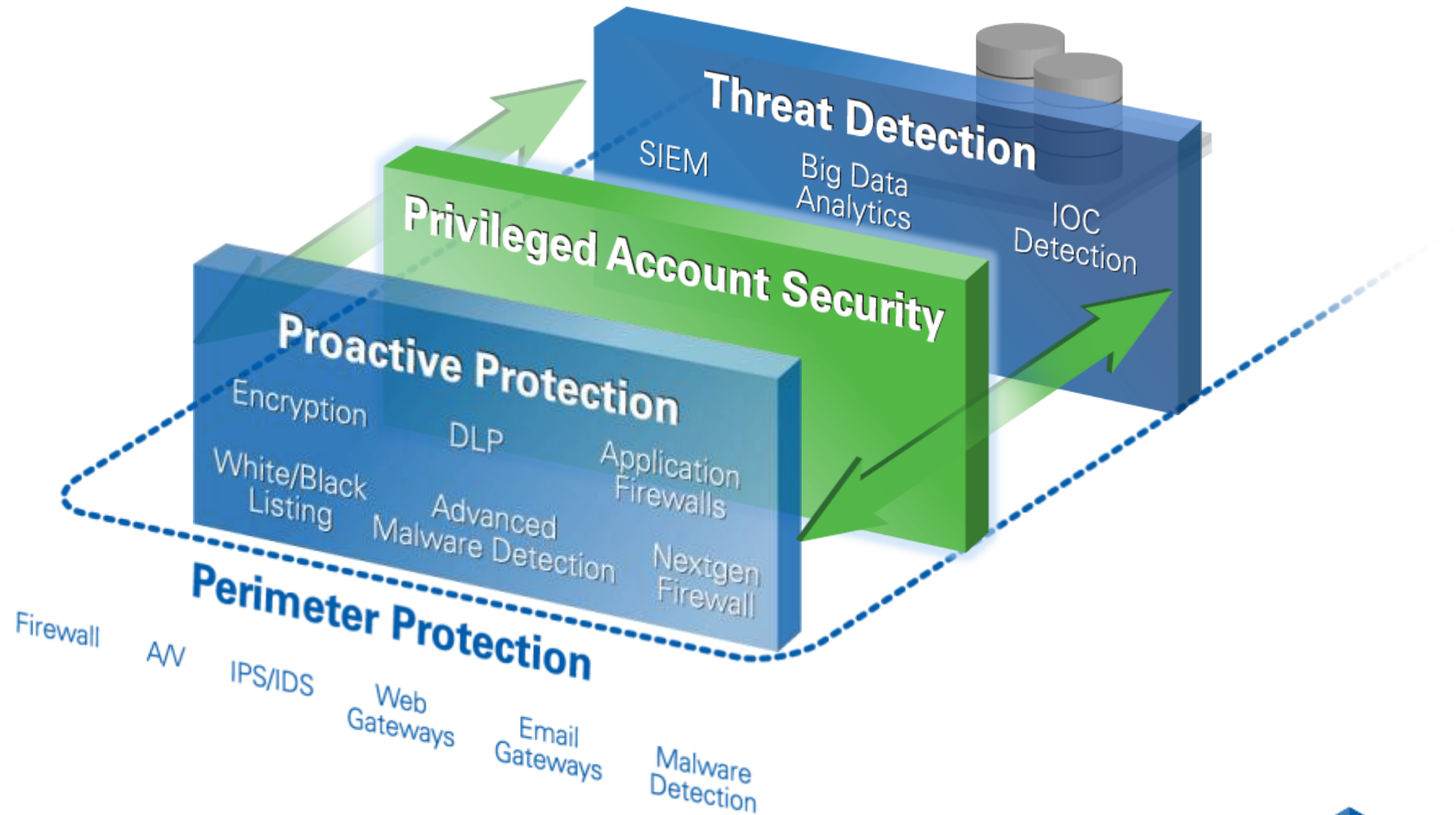
Вы отслеживаете привилегированную активность?

Cyber-Privileged Account Security & Compliance Survey, May 2013

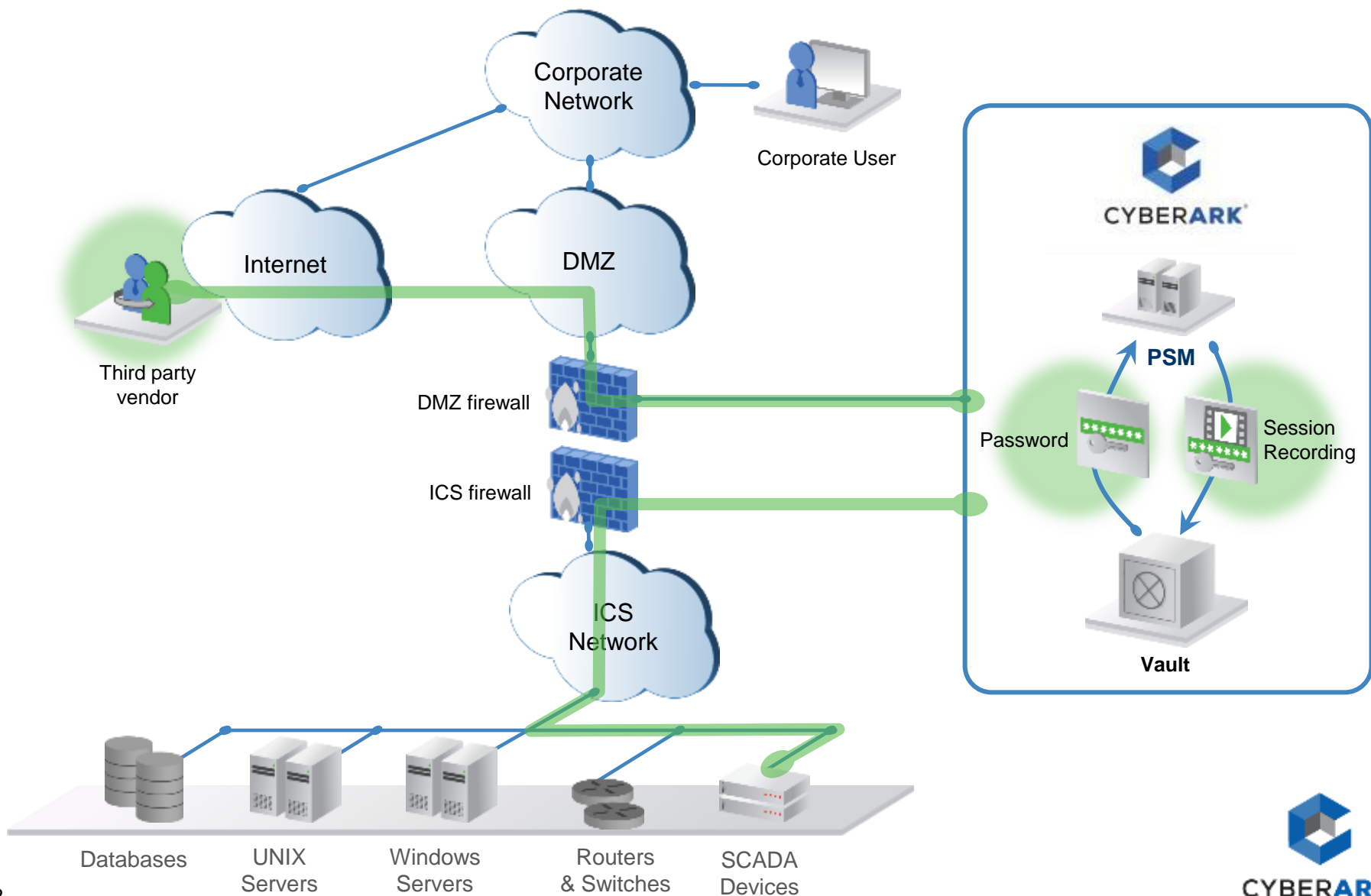


CYBERARK

# Privileged Account Security – Now a Critical Security Layer



# В промышленных системах ICS/SCADA



# 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**

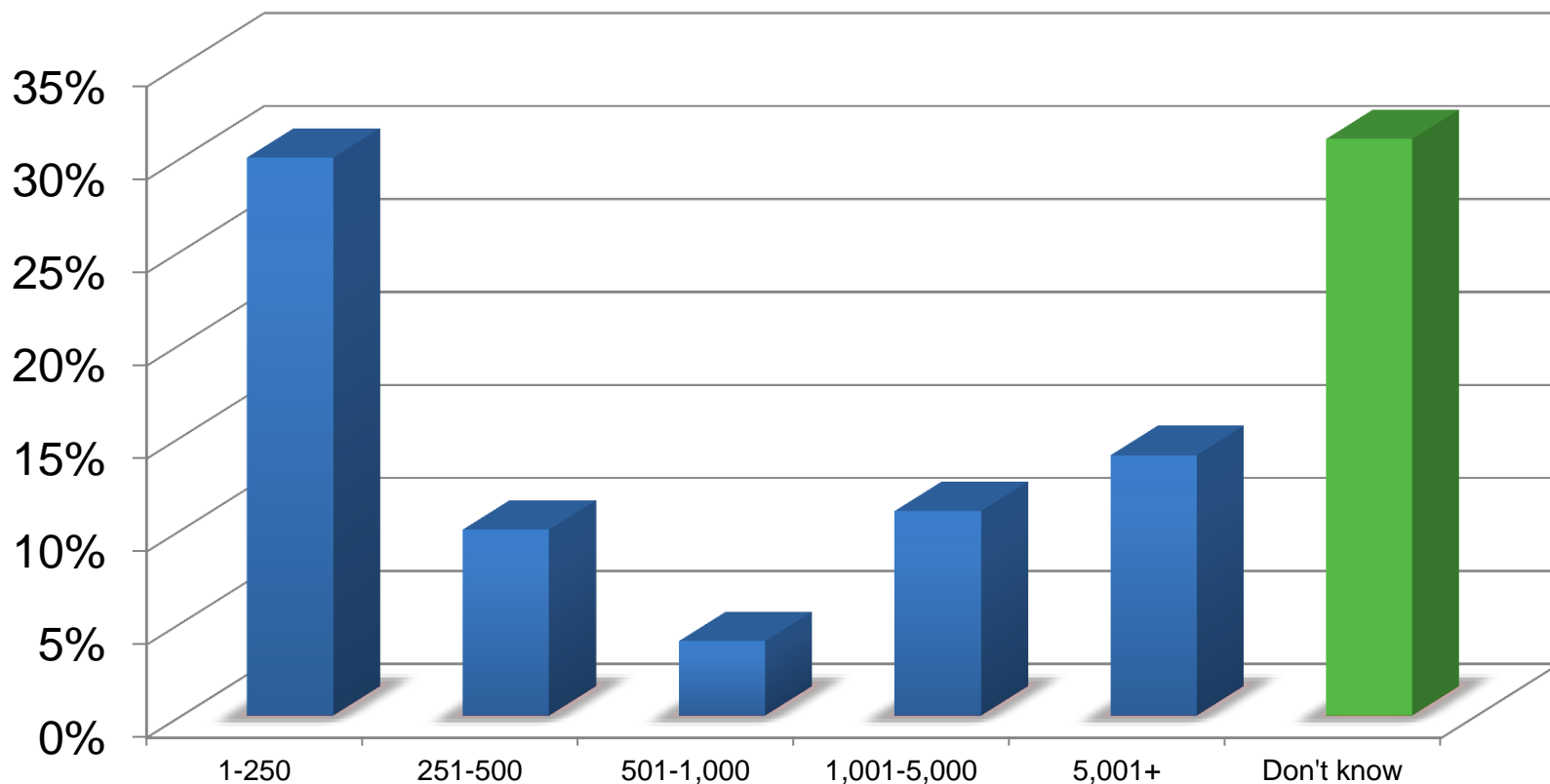


CYBERARK®

# Продукты

# Но этот факт не понятен...

Сколько привилегированных записей в вашей системе?



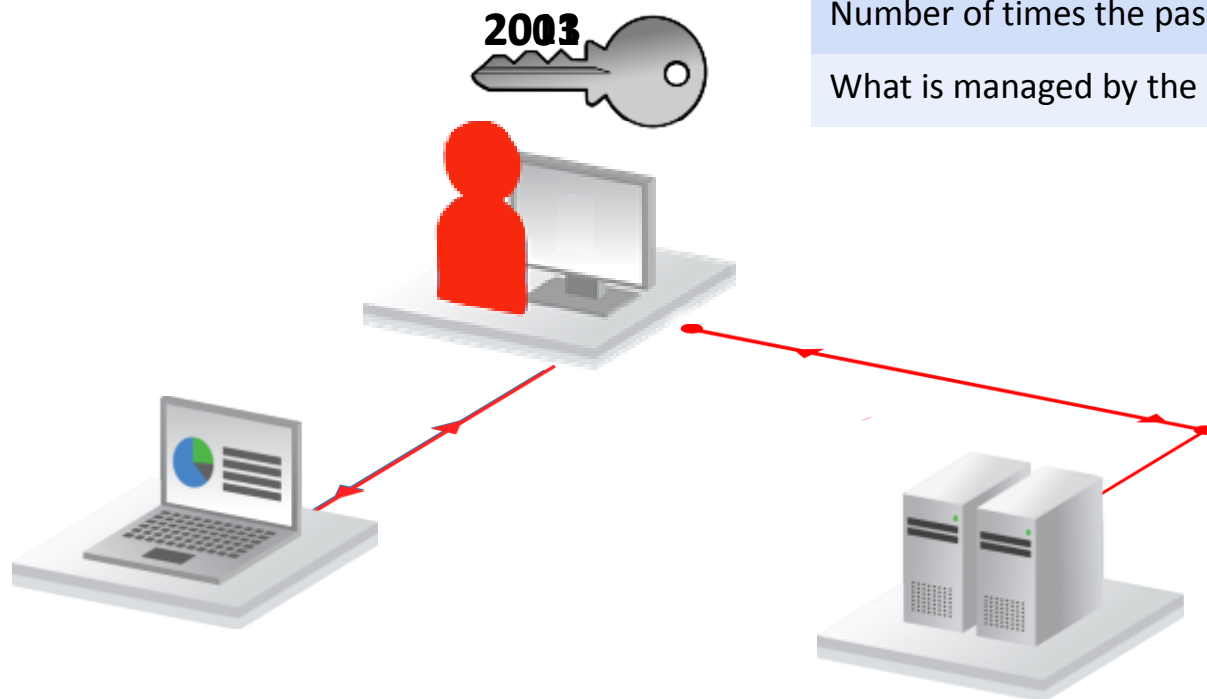
*Cyber-Privileged Account Security & Compliance Survey, May 2013 (Enterprise > 5000 Employees)*



**CYBERARK**

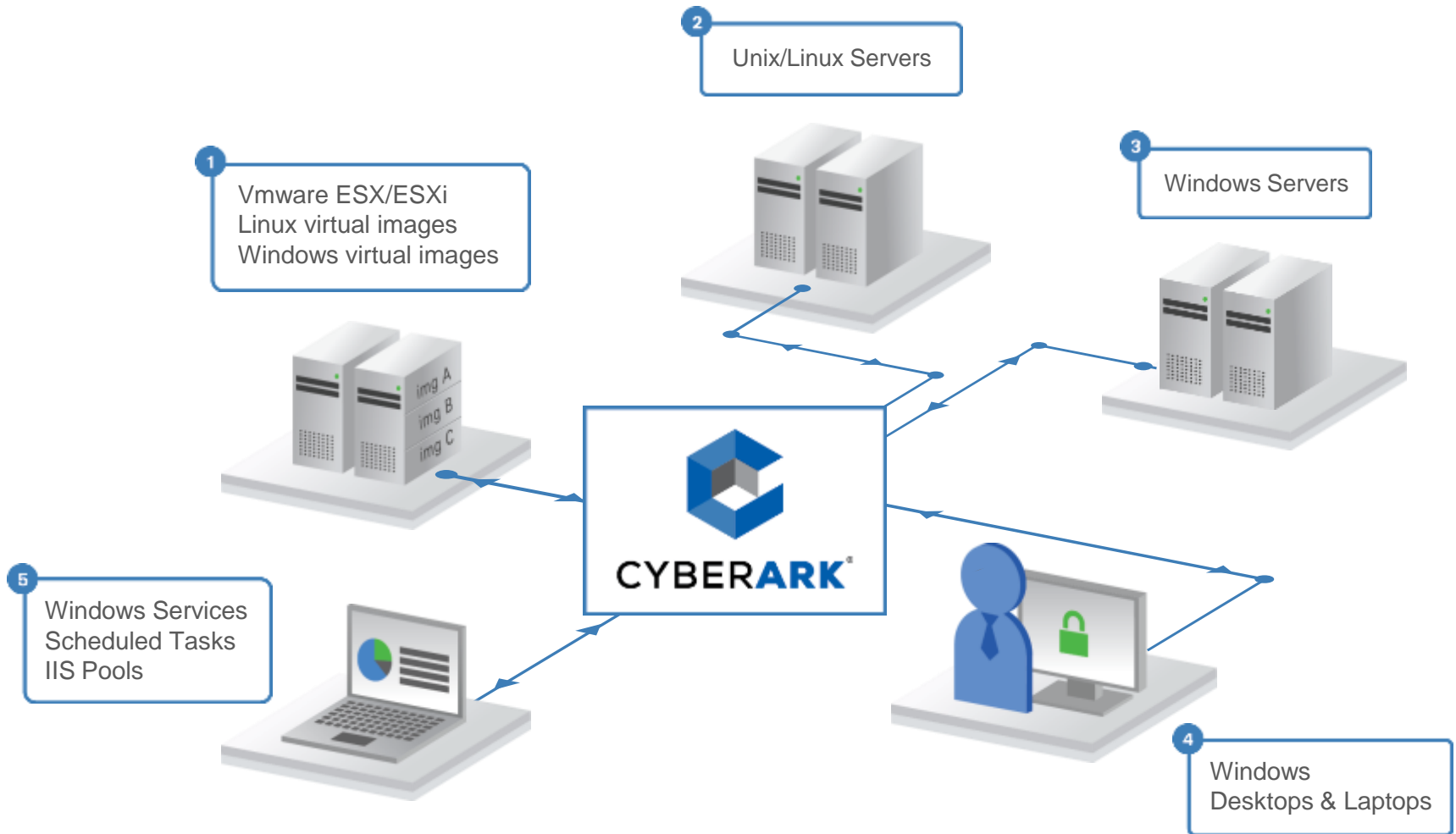


# Risk Assessment Case



Number of employees that knew the password and have left the company	40+
Number of times the password was used	100,000+
What is managed by the account	unknown

# CyberArk Auto Discovery



Where do all the privileged and superuser accounts exist?

# EPV: автоопределение в виртуальной среде

1. Подключение к vCenter
2. CPM сканирует новые/удаленные ESX hosts
3. Помогает аккаунт ESX root в Vault



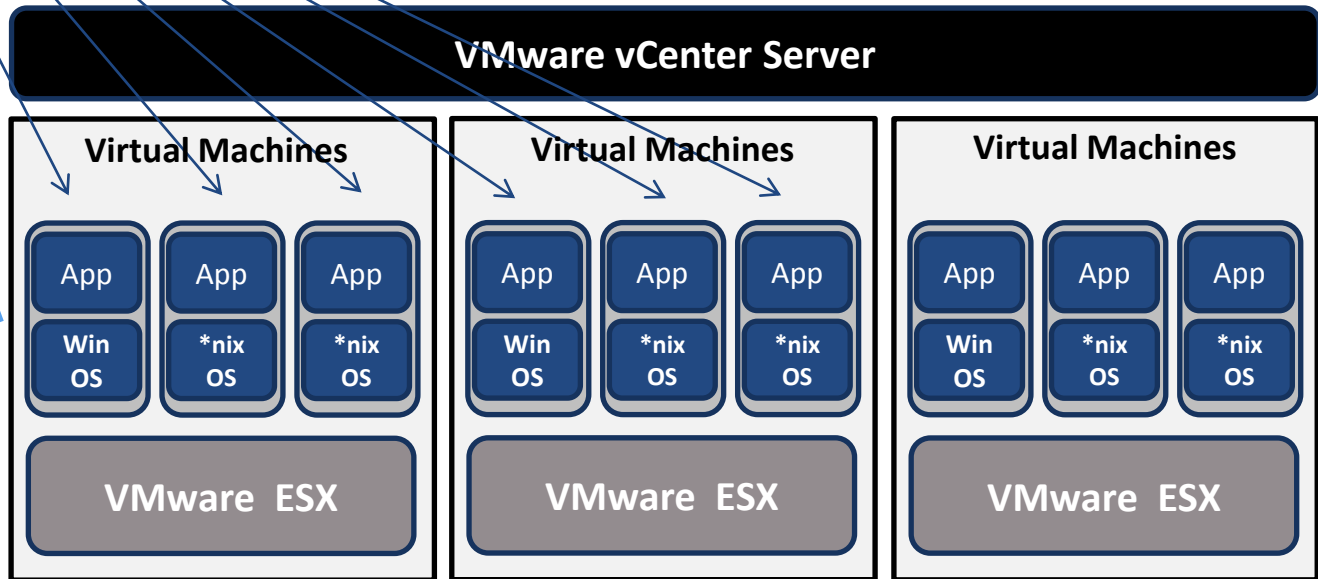
Central Policy Manager



Vault

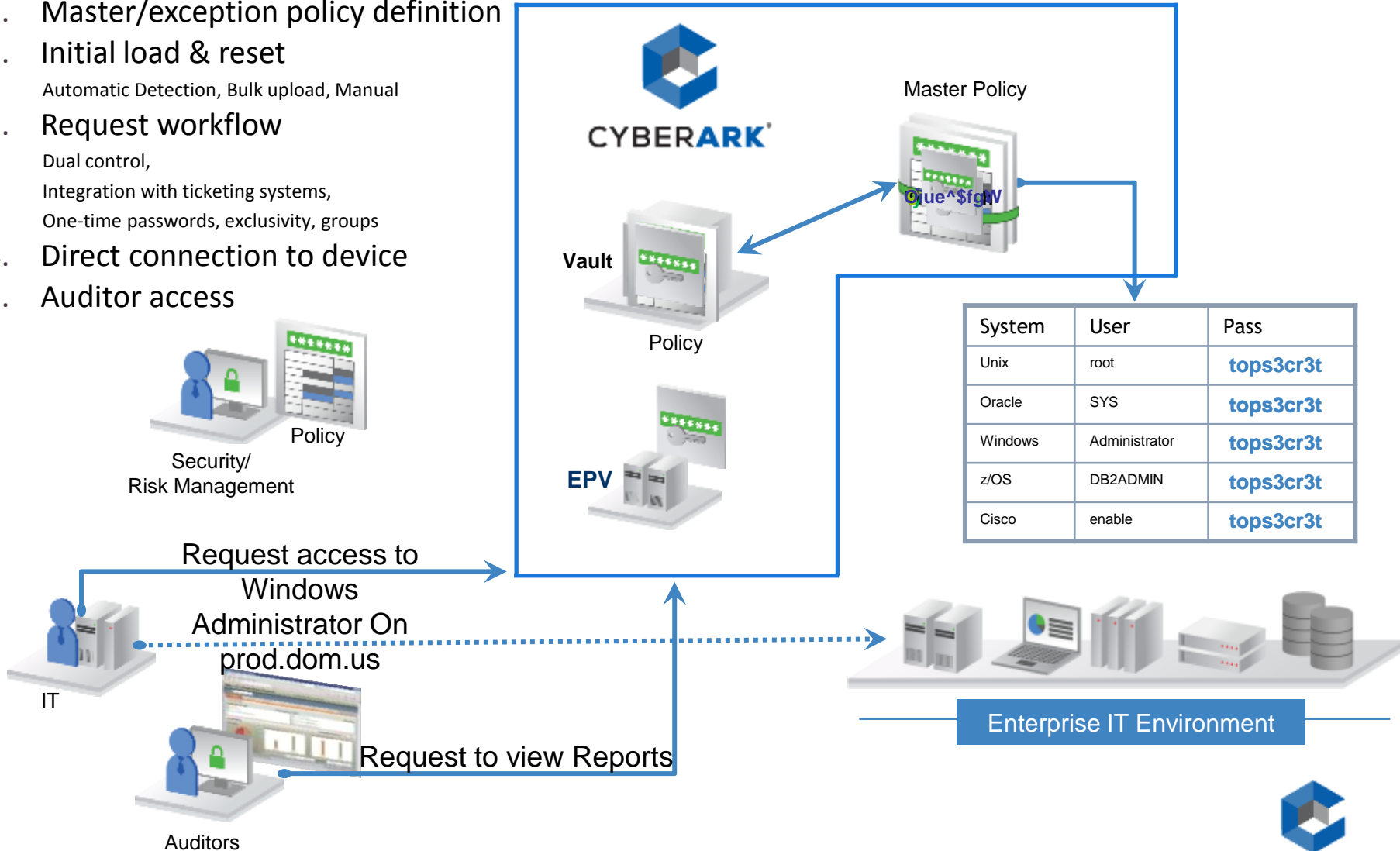
Автоопределение и обеспечение функционала, для всех ESX/ESXi и всех гостевых имиджей.

сообщает о членах группы local admin, отмечает  
неуправляемые аккаунты

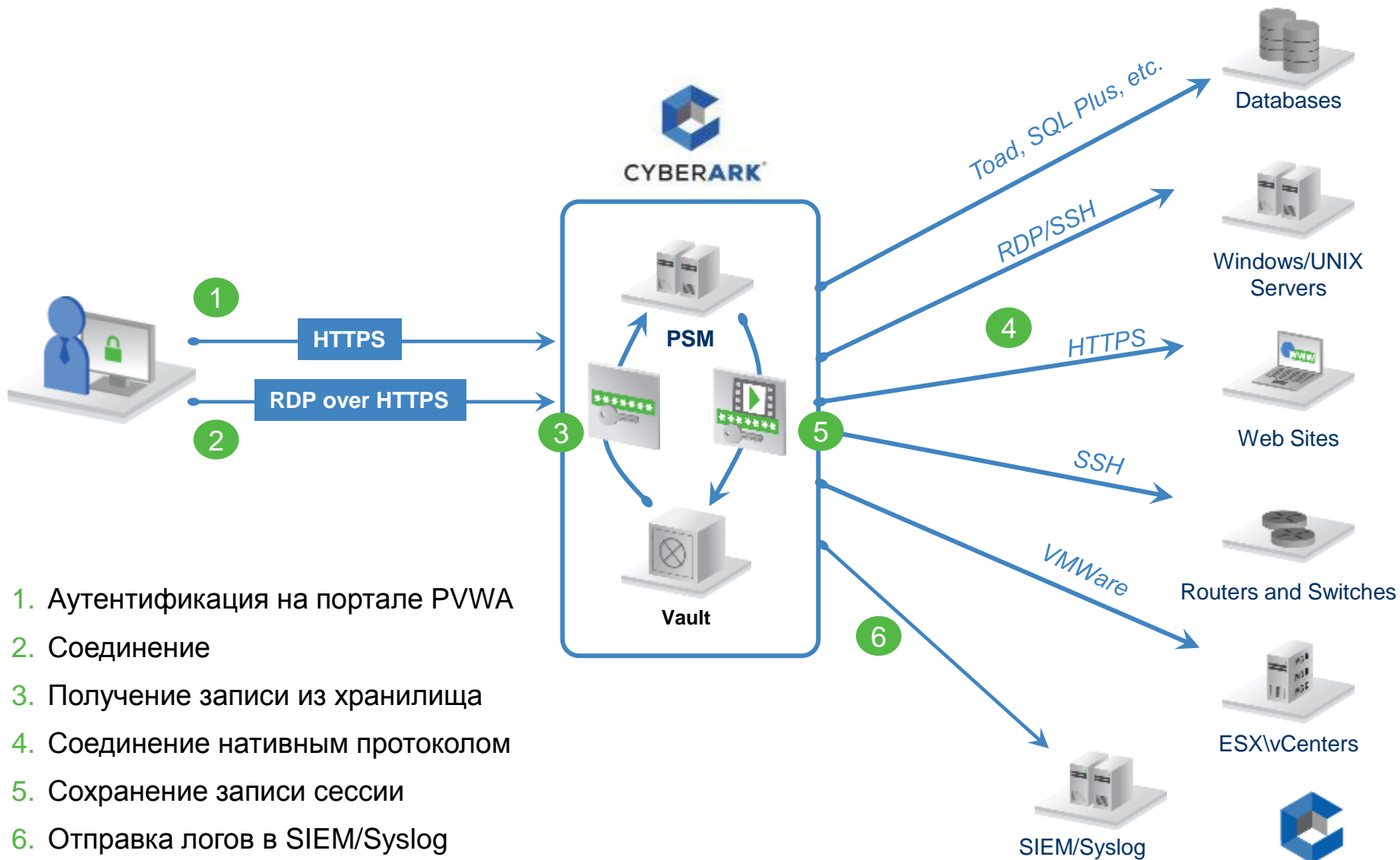


# Enterprise Password Vault Overview

1. Master/exception policy definition
2. Initial load & reset  
Automatic Detection, Bulk upload, Manual
3. Request workflow  
Dual control,  
Integration with ticketing systems,  
One-time passwords, exclusivity, groups
4. Direct connection to device
5. Auditor access

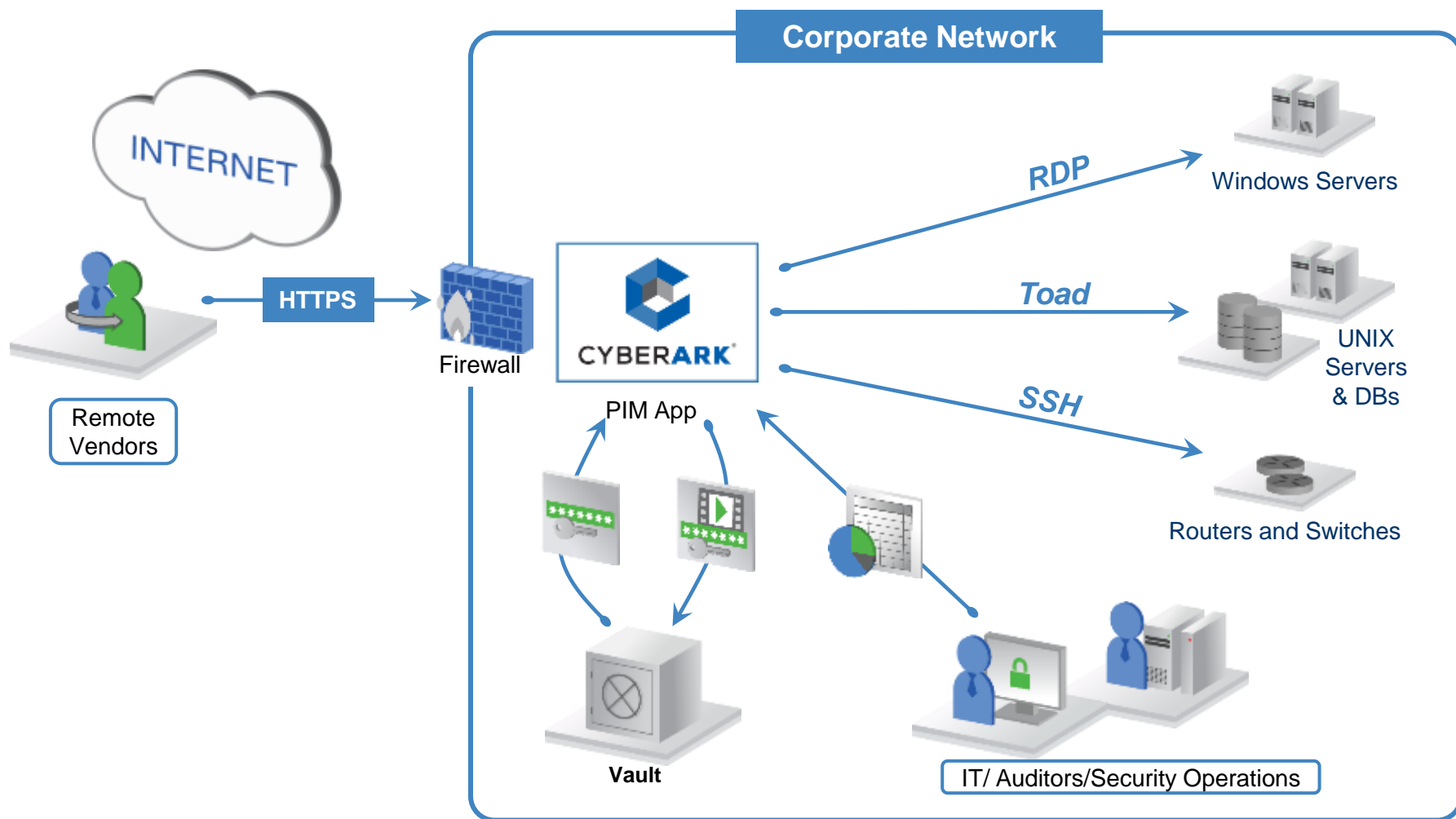


# Privileged Session Manager (PSM)

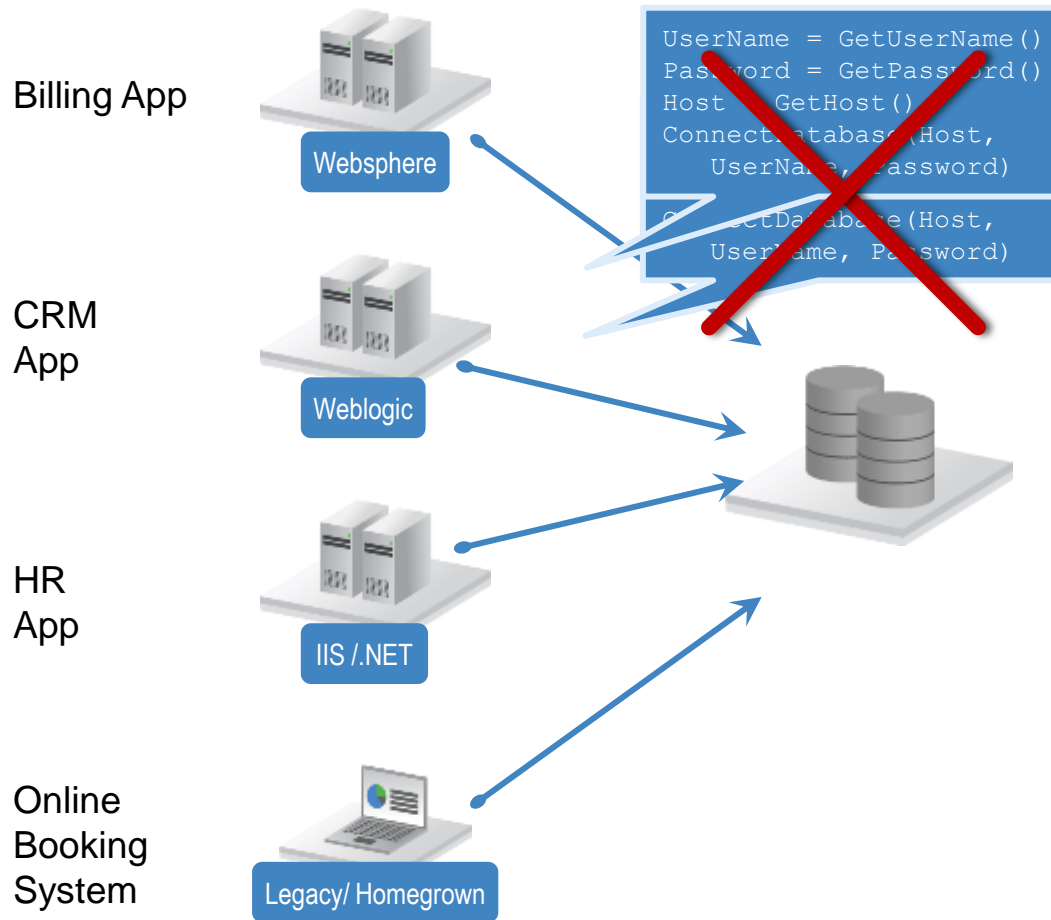


1. Аутентификация на портале PVWA
2. Соединение
3. Получение записи из хранилища
4. Соединение нативным протоколом
5. Сохранение записи сессии
6. Отправка логов в SIEM/Syslog

# Privileged Account Security for Remote Vendors



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

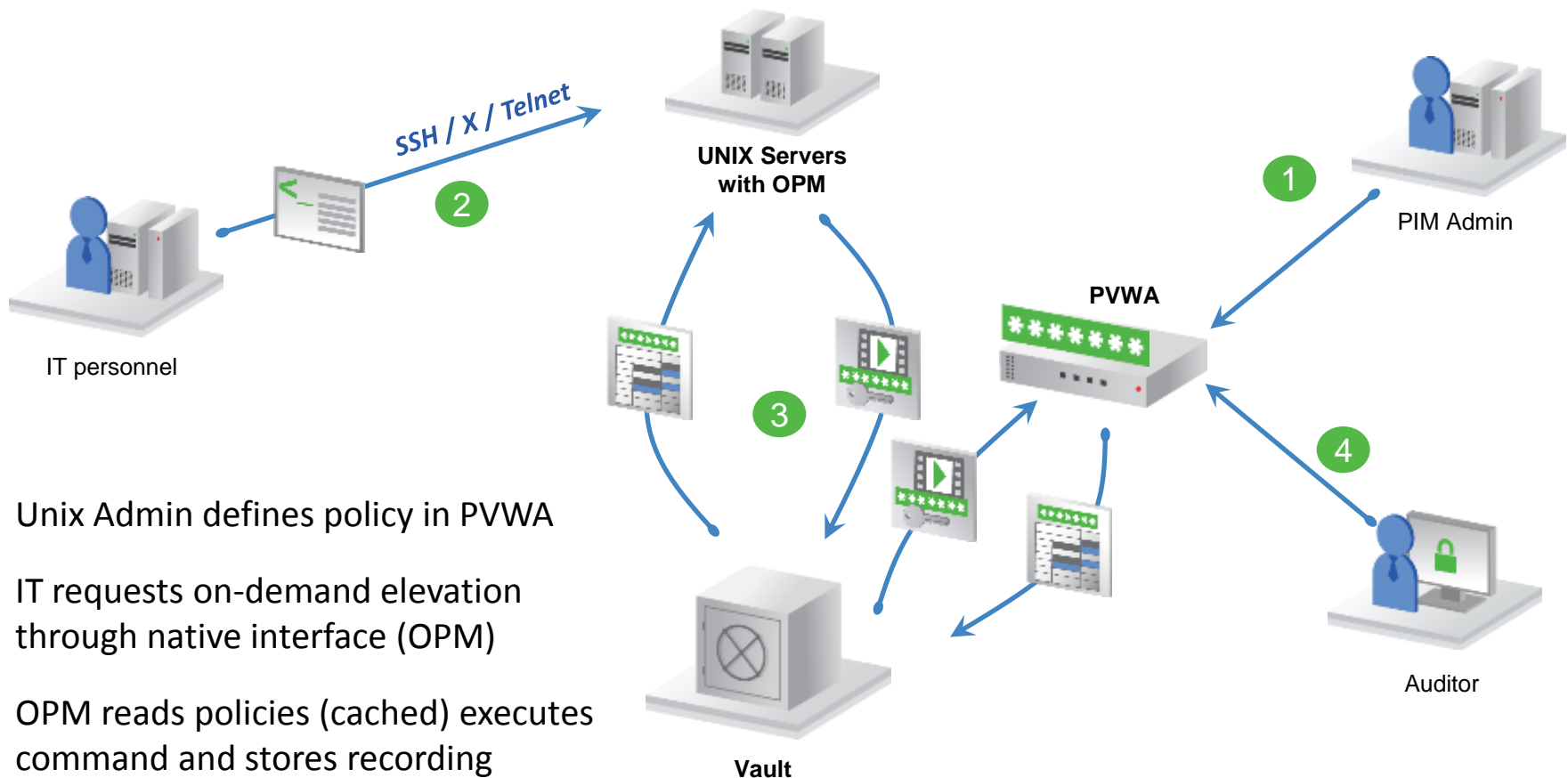


- Защищает и сбрасывает учетную запись приложения без простоя и рестарта
- Безопасно кэширует для непрерывности бизнеса и высокой производительности
- Исключает изменение кода и затраты на изменения паролей или адресов машин
- Строгая аутентификация по:
  - Адресу машины
  - Пользователю OS
  - Адресу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

Защищает, управляет и устраняет встроенные привилегированные аккаунты из приложений



# CyberArk On-Demand Privileges Manager



1. Unix Admin defines policy in PVWA
2. IT requests on-demand elevation through native interface (OPM)
3. OPM reads policies (cached) executes command and stores recording
4. Auditor reviews commands recordings / audit reports

# PIM&PSM – всесторонняя безопасность БД

- Защита БД – контроль привилегированного доступа и активности

## DB sys и общие DBA аккаунты

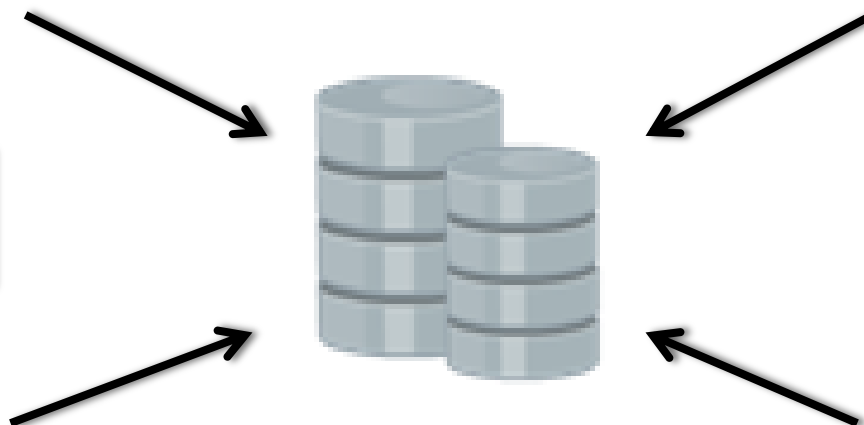
- Контроль защищенности, доступа и активности
- Автоматическое управление и замена аккаунтов

## Пользователи хостов и файлов данных

- Управление доступом к nix-хостам БД
- Гранулярный контроль
- Повышение привилегий по требованию

Ваши привилегированные DBA аккаунты управляются? Знаете, кто их использует?

Как насчет скриптов, имеющих встроенные sys-пароли?



Что если они имеют доступ к nix-серверам?

Доступ контролируется, но знаете ли Вы: что именно происходит с БД?

## Права DBA в приложениях и скриптах

- Замена встроенных паролей
- Строгая аутентификация приложений

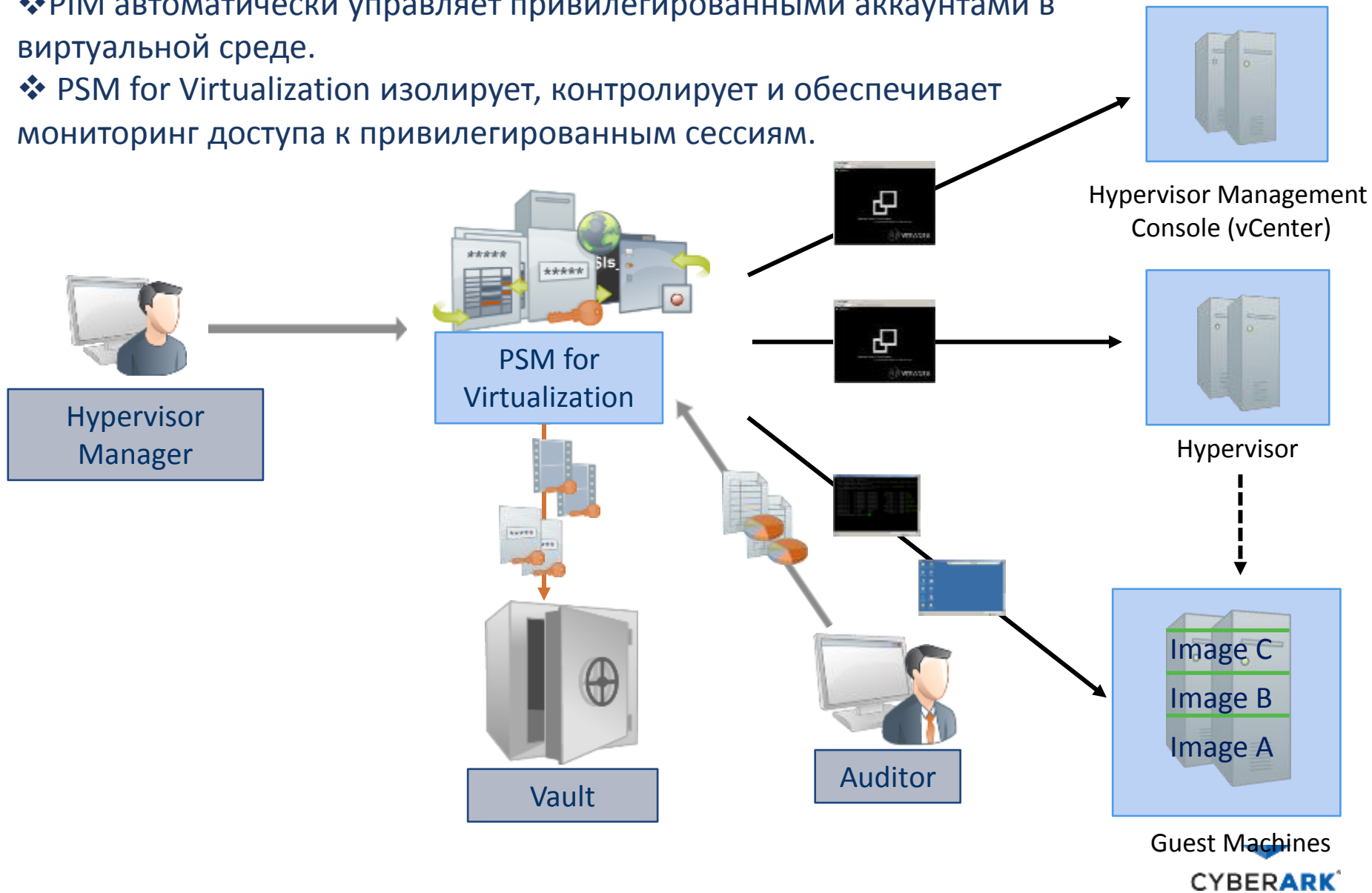
## Привилегированные сессии DBA

- Изоляция БД от прямого подключения
- Запись всех сессий
- Контроль привилегированных сессий
- Отсутствие следов и нагрузки на БД
- Контроль доступа к хостам ОС

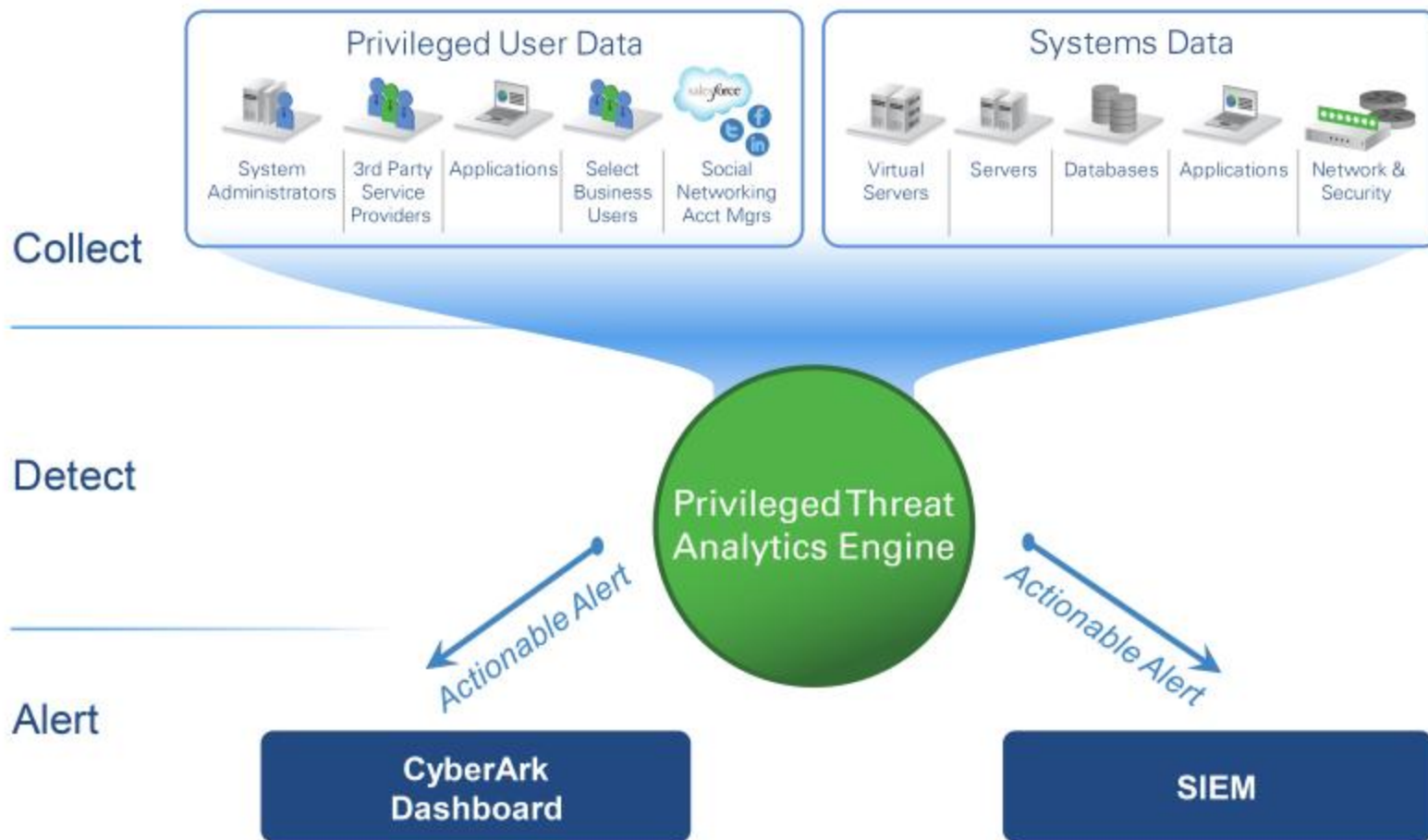
Enterprise Password Vault  
Application Identity Manager  
On-Demand Privileges Manager  
Privileged Session Manager for DBs

# PIM&PSM – инновационный подход к безопасности

- ❖ PIM автоматически управляет привилегированными аккаунтами в виртуальной среде.
- ❖ PSM for Virtualization изолирует, контролирует и обеспечивает мониторинг доступа к привилегированным сессиям.

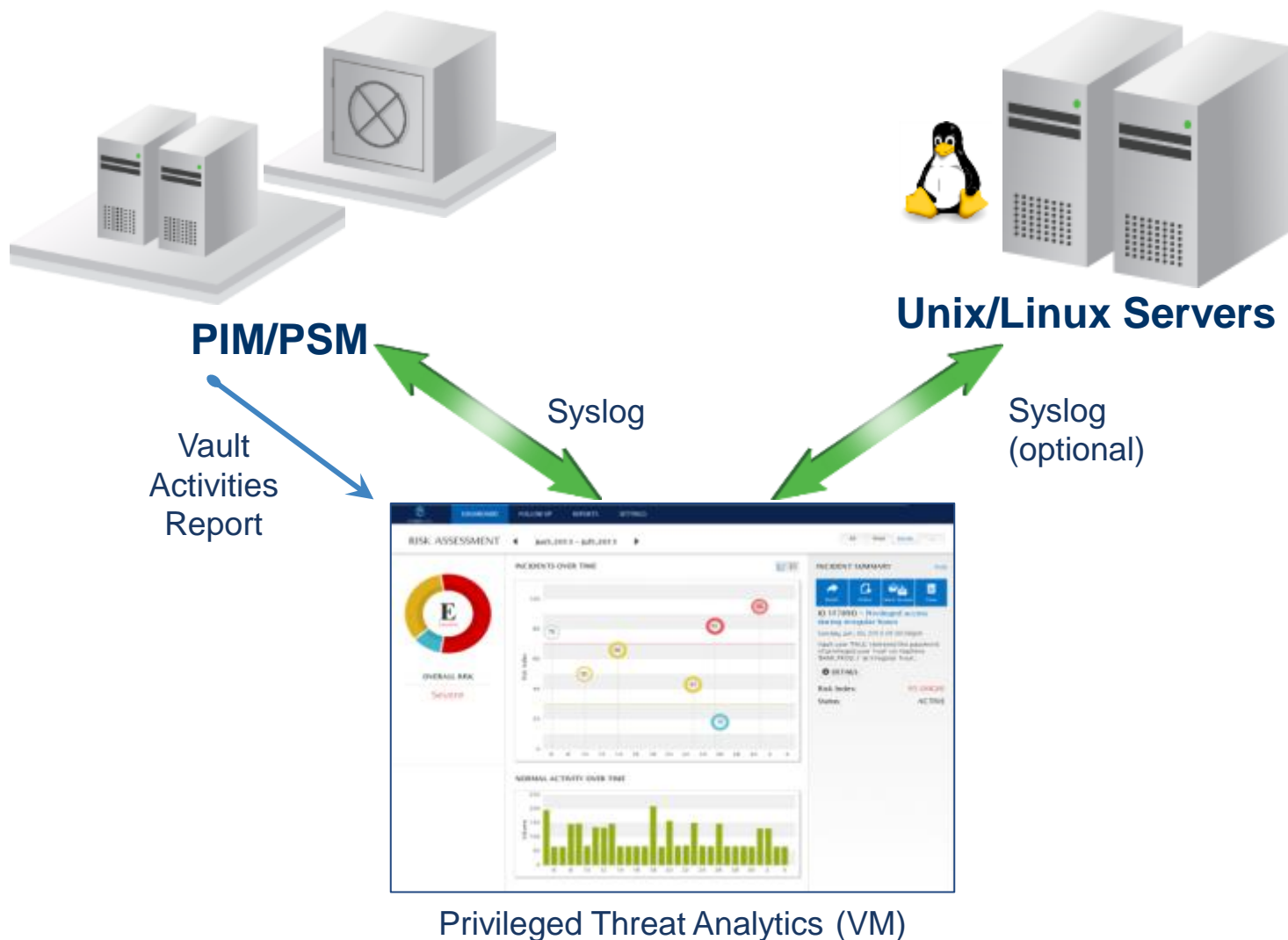


# Privileged Threat Analytics (PTA)

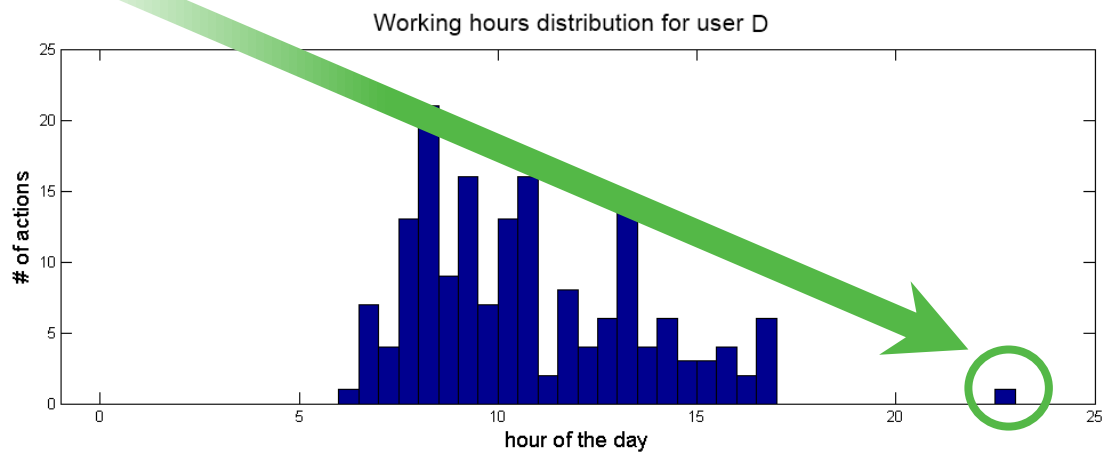
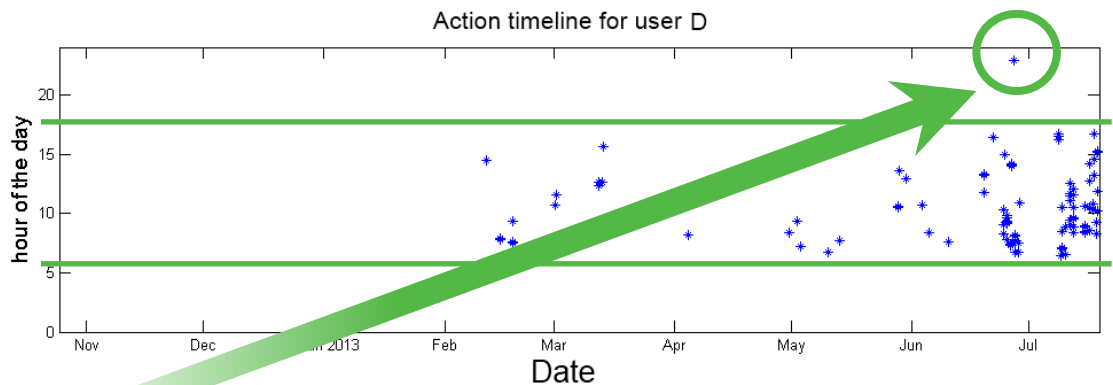
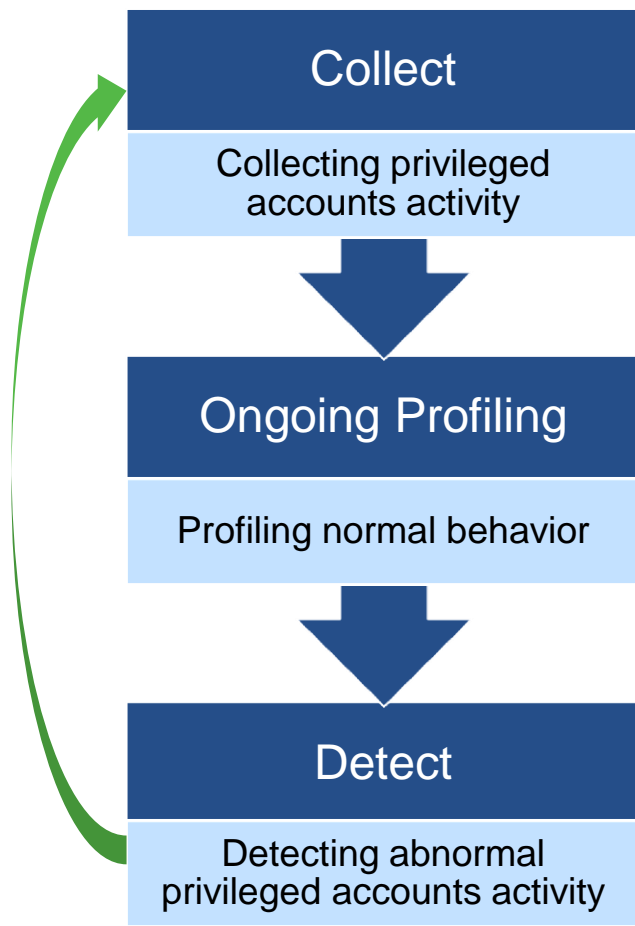


- Identify advanced attacks in-progress (analytics & alerting)
- Understand threat level (real-time detection & events correlation)
- Improve SIEM effectiveness

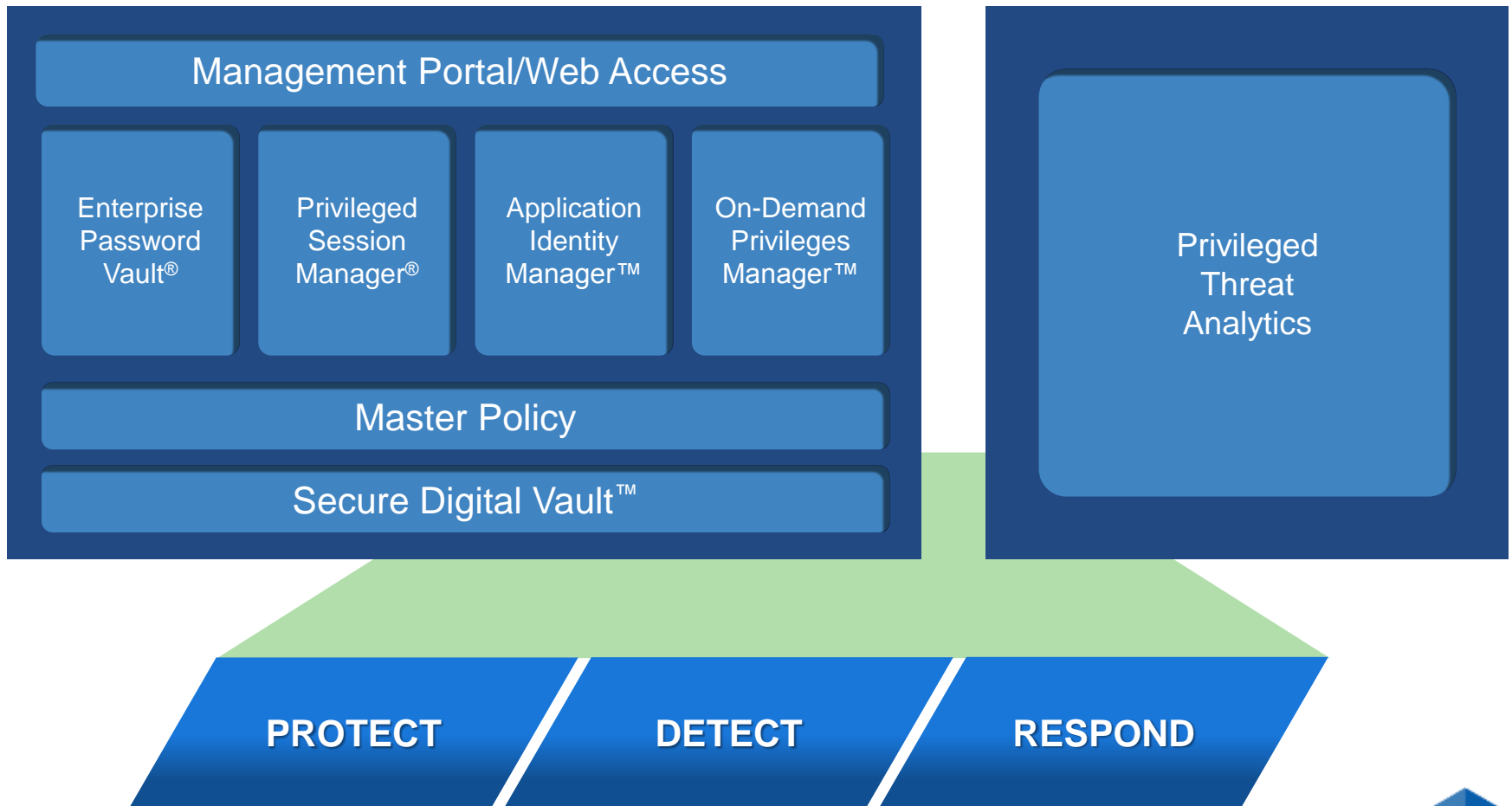
# PTA - Seamless Integration with Prod.PIM/PSM



# How Does PTA Work?



# CyberArk's Privileged Account Security Solution





# CyberArk's Integration Across the Enterprise

## Databases



- Oracle
- MSSQL
- DB2
- Informix
- Sybase
- MySQL
- Any ODBC

## Operating Systems



- Windows
- Unix/Linux
- AS400
- OS390
- HPUX
- Tru64
- NonStop
- ESX
- OVMS
- Mac

## Applications



- SAP
- WebSphere
- WebLogic
- Windows: Services
- Scheduled Tasks
- IIS App Pools
- IIS Anonymous
- COM+
- Oracle Application ERP
- System Center Configuration Manager

## Generic Interface



- SSH/Telnet
- ODBC
- Windows Registry
- Web Interfaces
- Web Sites



## Network Devices



- Cisco
- Juniper
- Nortel
- Alcatel
- Qantum
- F5

## Security Appliances



- FW1, SPLAT
- IPSO
- PIX
- Netscreen
- FortiGate
- ProxySG

## Directories and Credential Storage



- AD
- SunOne
- Novel
- UNIX Kerberos
- UNIX NIS

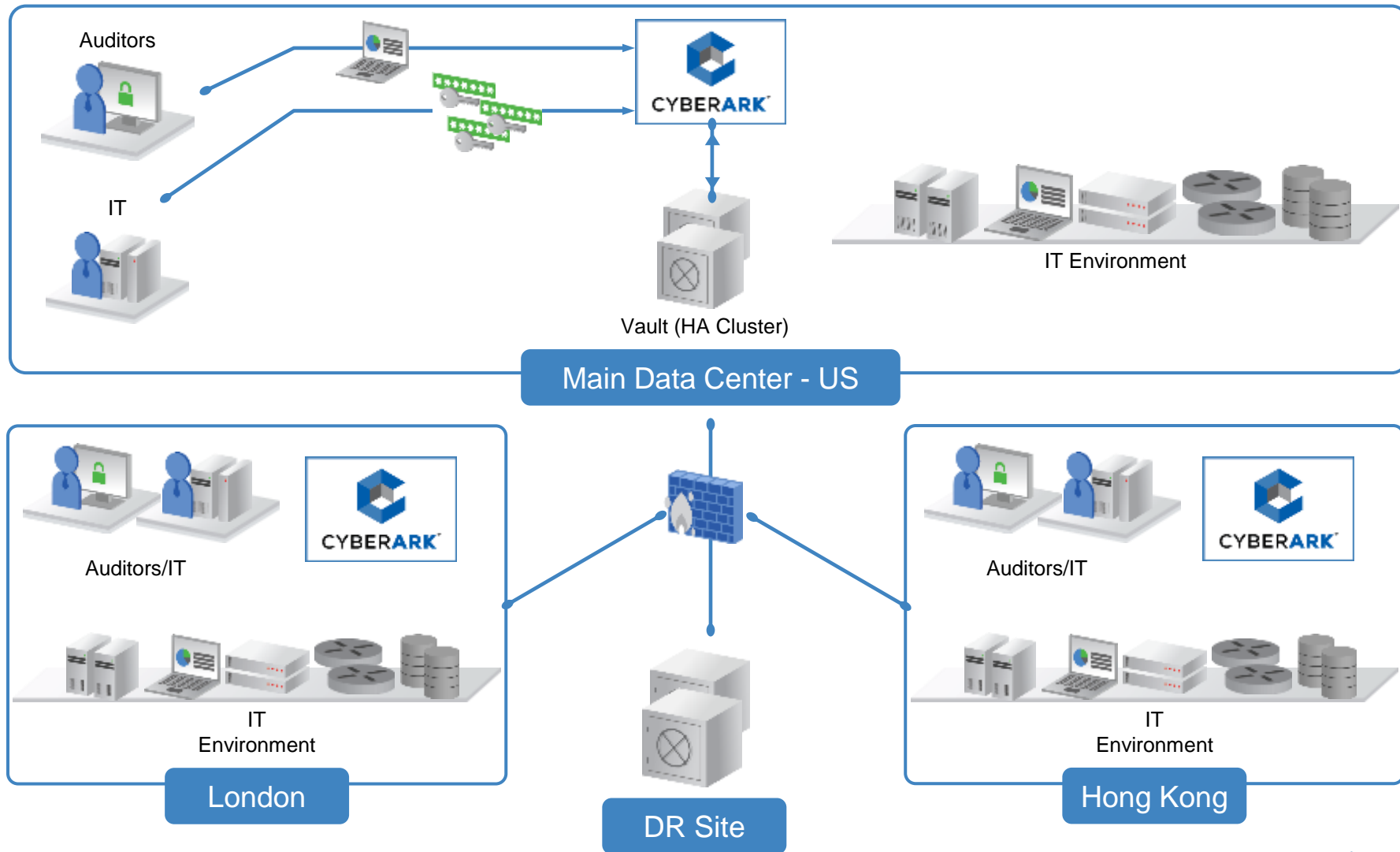
## Remote Control and Monitoring



- HMC
- HPiLO
- ALOM
- Digi CM
- DRAC

Expand to include more add category Universal Connector and platform support or other Controlled Availability (CA) Plug-ins. Sample

# Распределенная архитектура 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

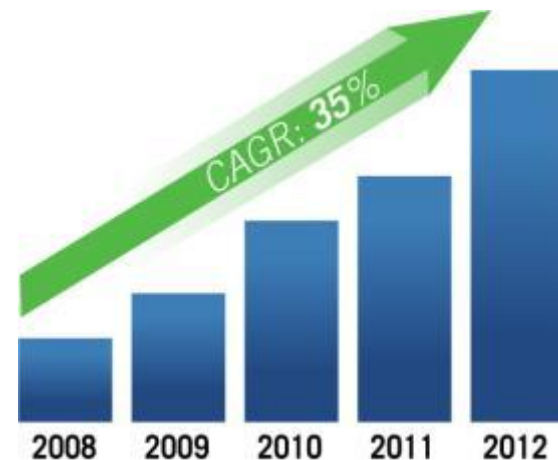
- Безопасность прозрачна для аудита



## Единое всестороннее решение

- Одно решение для всех задач
- Уровня Enterprise

## Глобальные клиенты



CYBERARK

# Клиенты CyberArk в мире

Communications & Media 	Financial Services 	Pharmaceuticals 	Energy & Utilities 	Other Industries 
     	             	      	     	              

Доверенный эксперт для более чем 1,300 компаний мира

# Клиенты в регионе

## Financial Services



## Retail, Transport, Telecom



## Others





CYBERARK®

Спасибо за внимание...