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
-

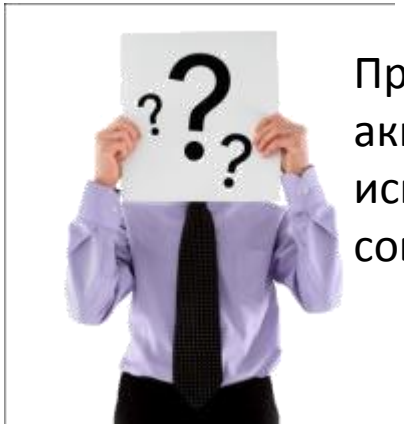
Решение проблем
- Управление привилегированными пользователями
- Контроль доступа и привилегированных сессий
- Центр оперативного реагирования

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.

CYBERARK

Привилегированный аккаунт: что, где и почему

	Какие	Кем используются	Используются для
Привилегированные персональные	• Облачные провайдеры • Персональные записи с широкими привилегиями	• Сотрудники	• Привилегированные операции • Доступ к критичной инф. • Веб-сайты
Общие привилегированные	• Administrator • root • Cisco Enable • Oracle SYS • Local Administrators	• IT службы • Системные администраторы • DBA • Help desk • Разработчики • Наследуемые прилож.	• Аварийные • Высокий SLA • Катастрофоустойчивость • Привилегированные операции • Доступ к критичной инф.
Аккаунты приложений	• Hard coded / встроенные ID • Служебные записи	• Приложения/скрипты • Windows Services • Scheduled Tasks • Batch jobs и т.д. • Разработчики	• Онлайн доступ к БД • Batch processing • Взаимодействие App-2-App

Любая компания и организация является целью атаки

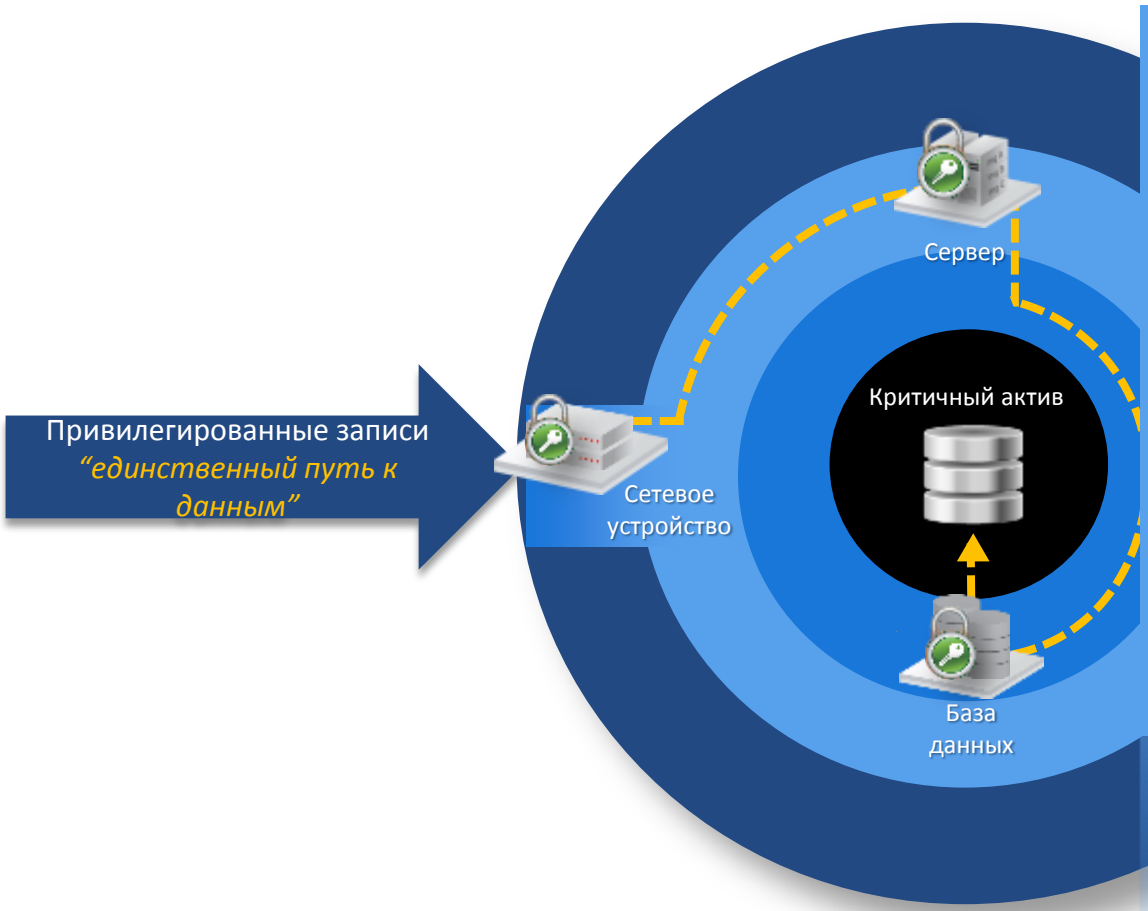
Злоумышленники целенаправленны, настойчивы, скрытны

Высокие привилегии сложно контролировать, управлять и отслеживать

… ведут к критическим рискам при неправильном использовании

CYBERARK

«Все пути ведут...» к привилегированым записям



“Все, что касается серьезной интеллектуальной собственности, содержится в хорошо защищенных системах, и привилегированные учетные записи являются единственным способом, который могут получить хакеры.”

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

CYBERARK

Привилегированные аккаунты – вторжение

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

CYBERARK

Решаем проблемы привилегированных УЗ

Целевые атаки (APT/AET)

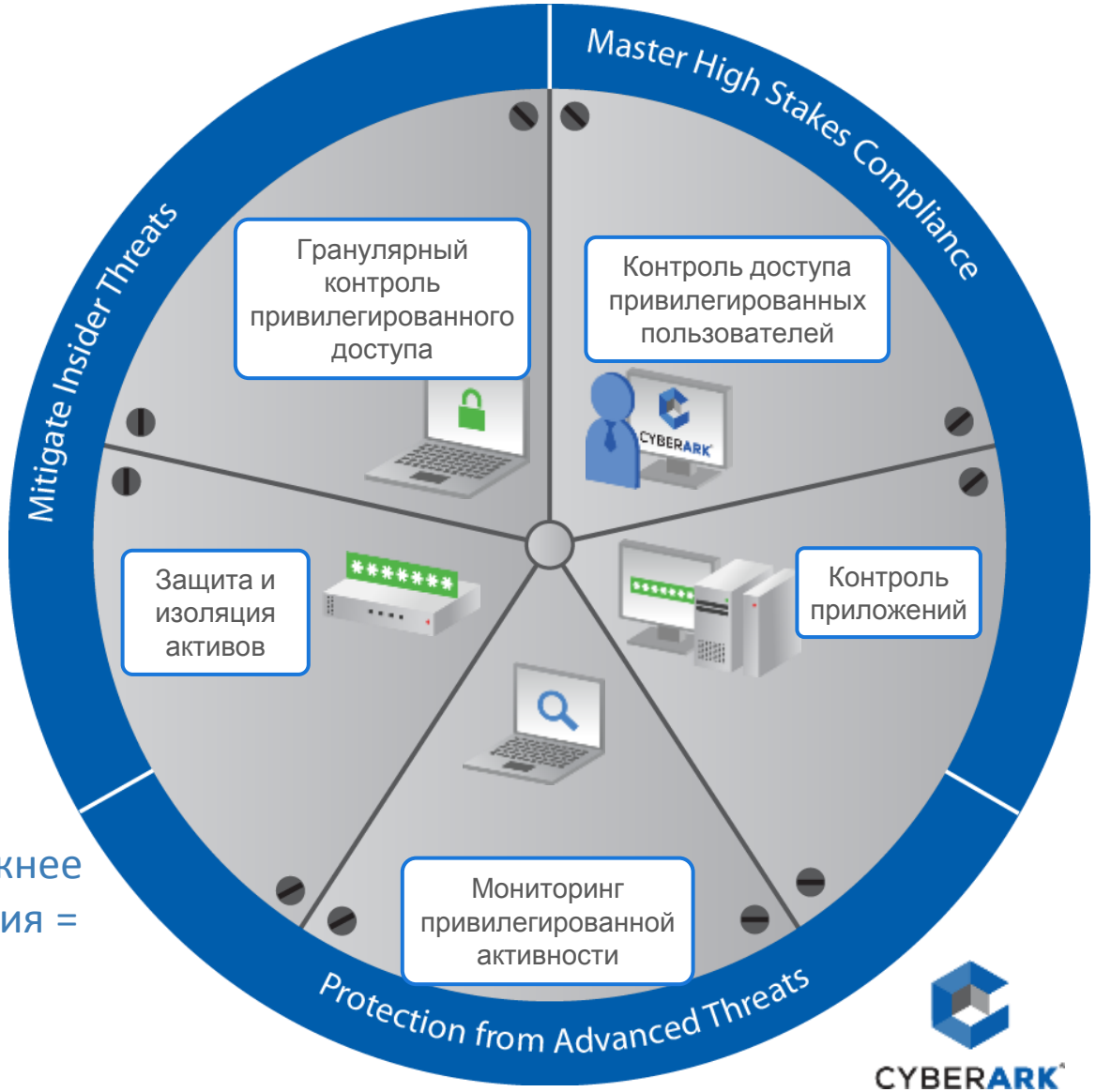
Спланированные, сложные
На наиболее ценные активы
Привилегированные аккаунты

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



CYBERARK

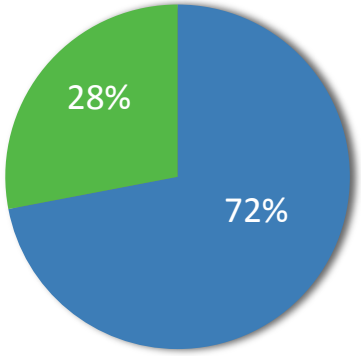
Регуляторы требуют контроль и мониторинг привилегированных аккаунтов

PCI Security Standards Council™

Sarbanes-Oxley
Financial and Accounting Disclosure Information

CYBERARK

Используются вариации разных решений

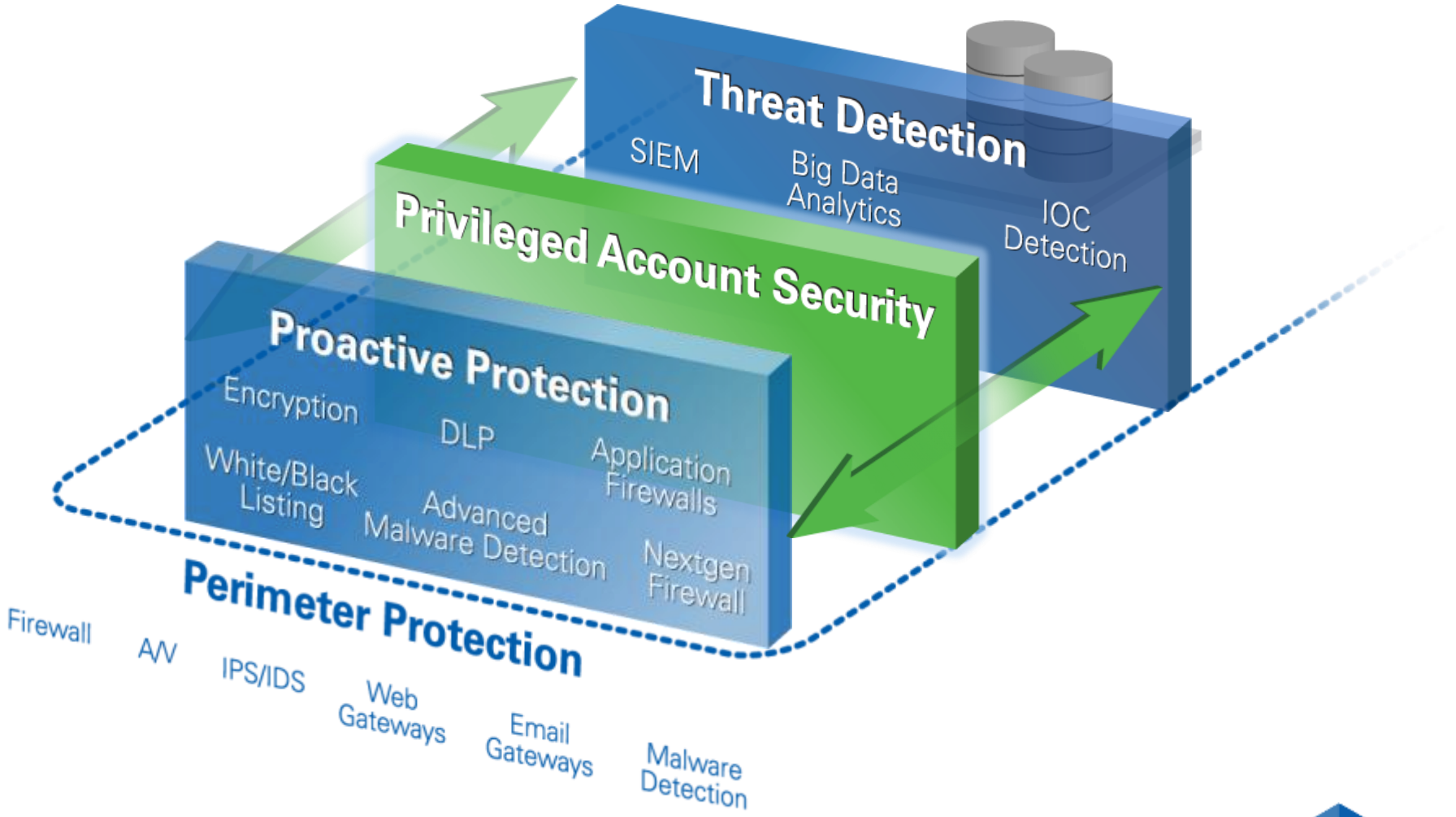


Вы отслеживаете привилегированную активность?

Cyber-Privileged Account Security & Compliance Survey, May 2013

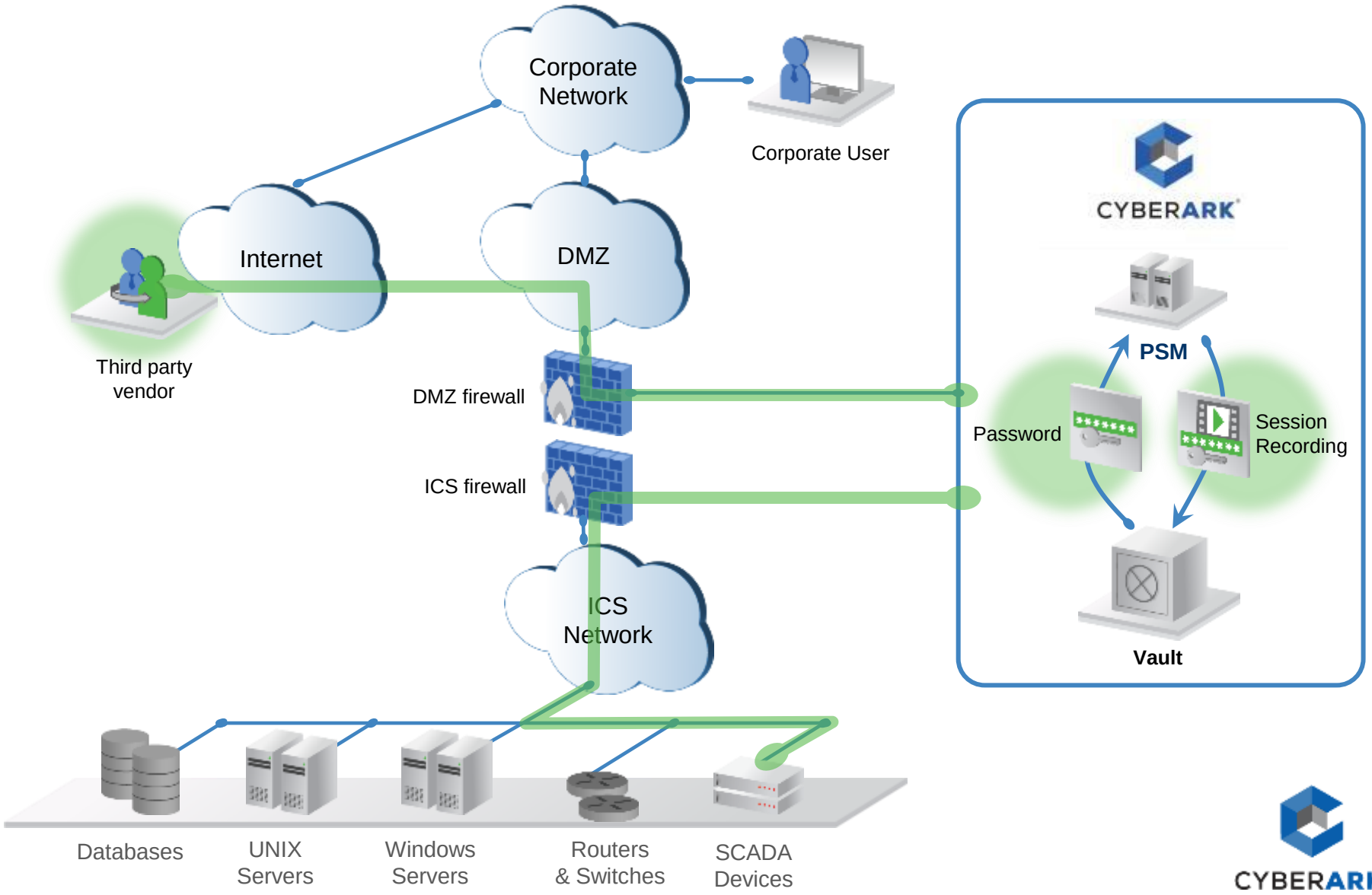
CYBERARK

Privileged Account Security – Now a Critical Security Layer



CYBERARK

В индустриальных системах ICS/SCADA



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

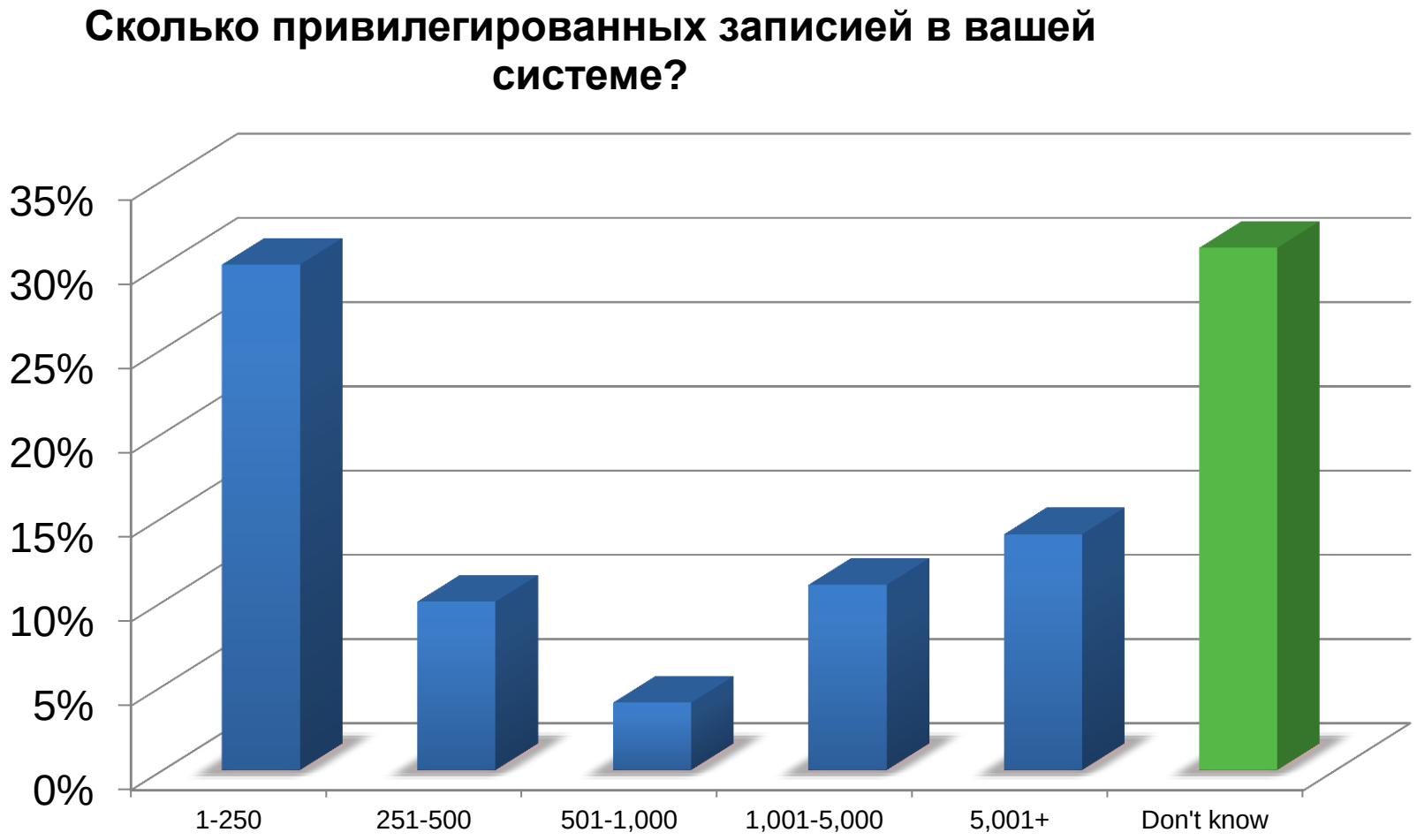
4. Расследовать использование привилегированных записей в реальном времени

CYBERARK

CYBERARK

Продукты

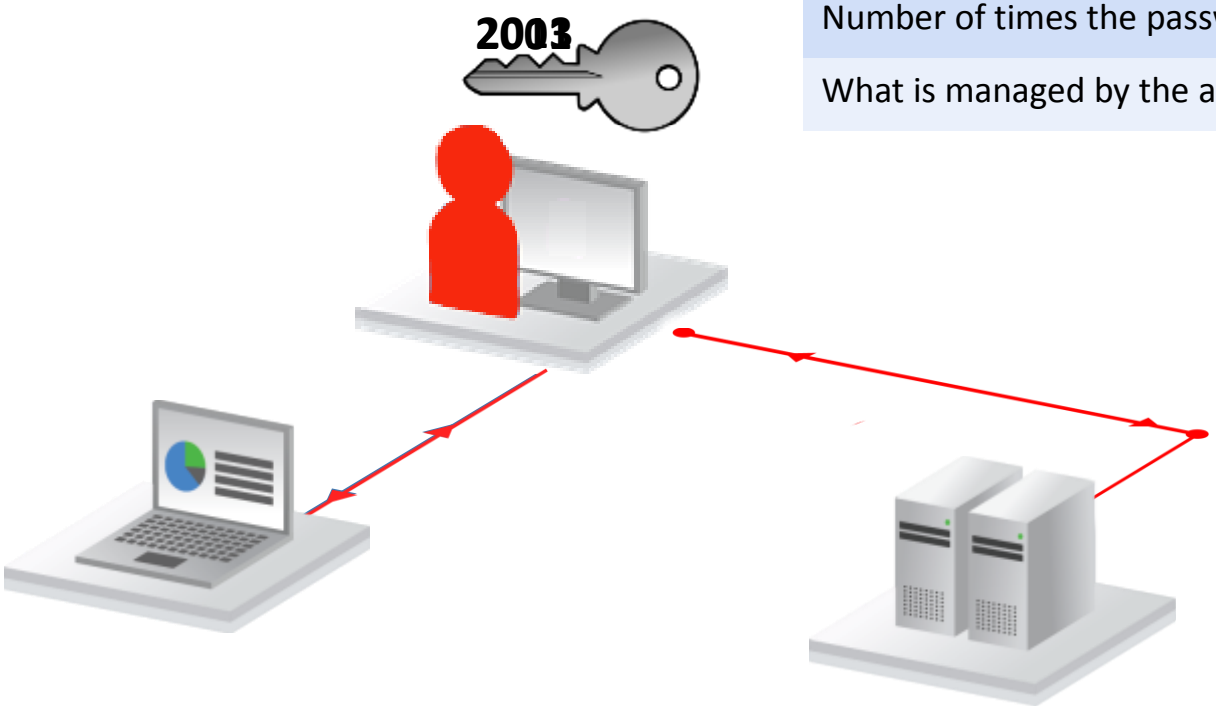
Но этот факт не понятен...



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

CYBERARK

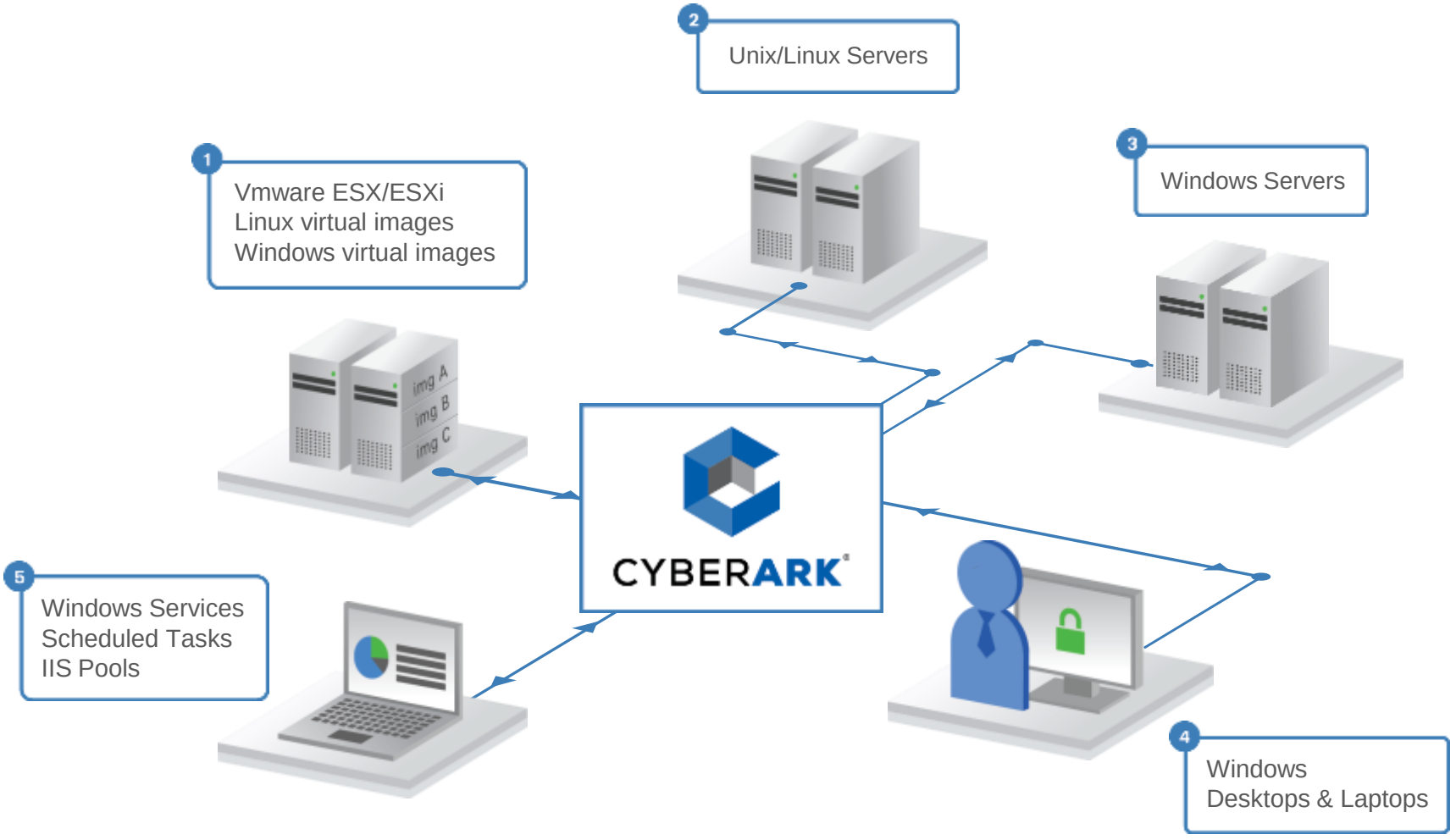
Risk Assessment Case



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

CyberArk Auto Discovery



Where do all the privileged and superuser accounts exist?

CYBERARK

EPV: автоопределение в виртуальной среде

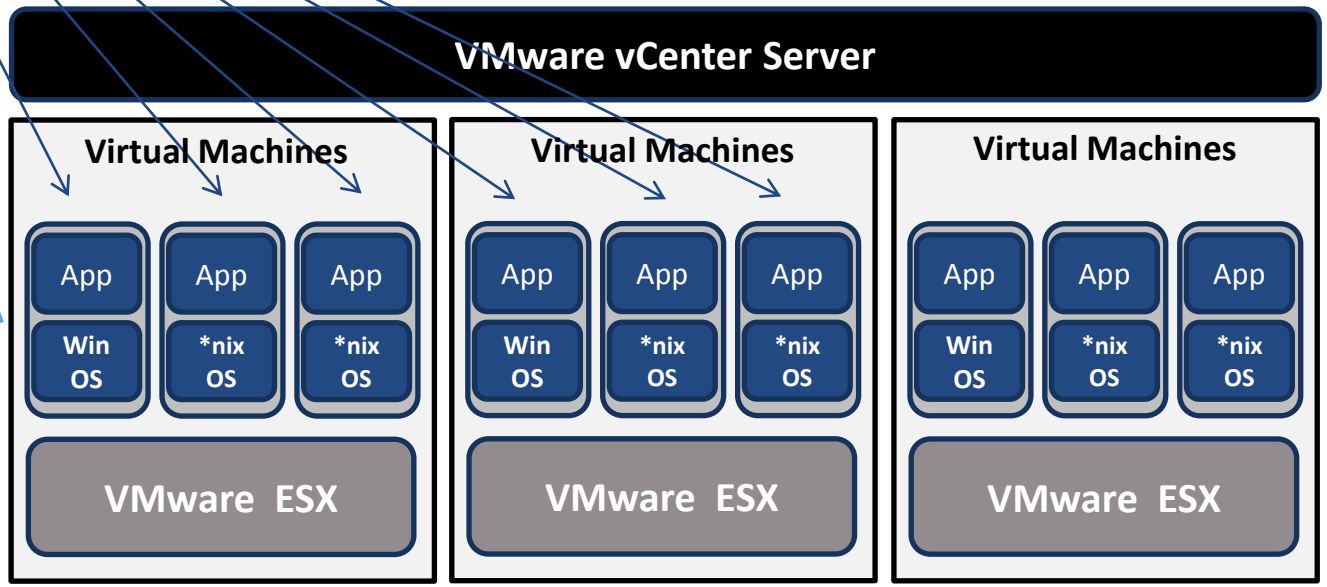
1. Подключение к vCenter
2. CPM сканирует новые/уаленные ESX хосты
3. Помещает аккаунт ESX root в Vault

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

сообщает о членах группы local admin, отмечает неуправляемые аккаунты

Central Policy Manager

Vault



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

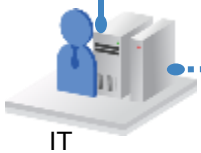
Security/
Risk Management

Master Policy

Policy

System	User	Pass
Unix	root	tops3cr3t
Oracle	SYS	tops3cr3t
Windows	Administrator	tops3cr3t
z/OS	DB2ADMIN	tops3cr3t
Cisco	enable	tops3cr3t

Request access to Windows Administrator On prod.dom.us



IT

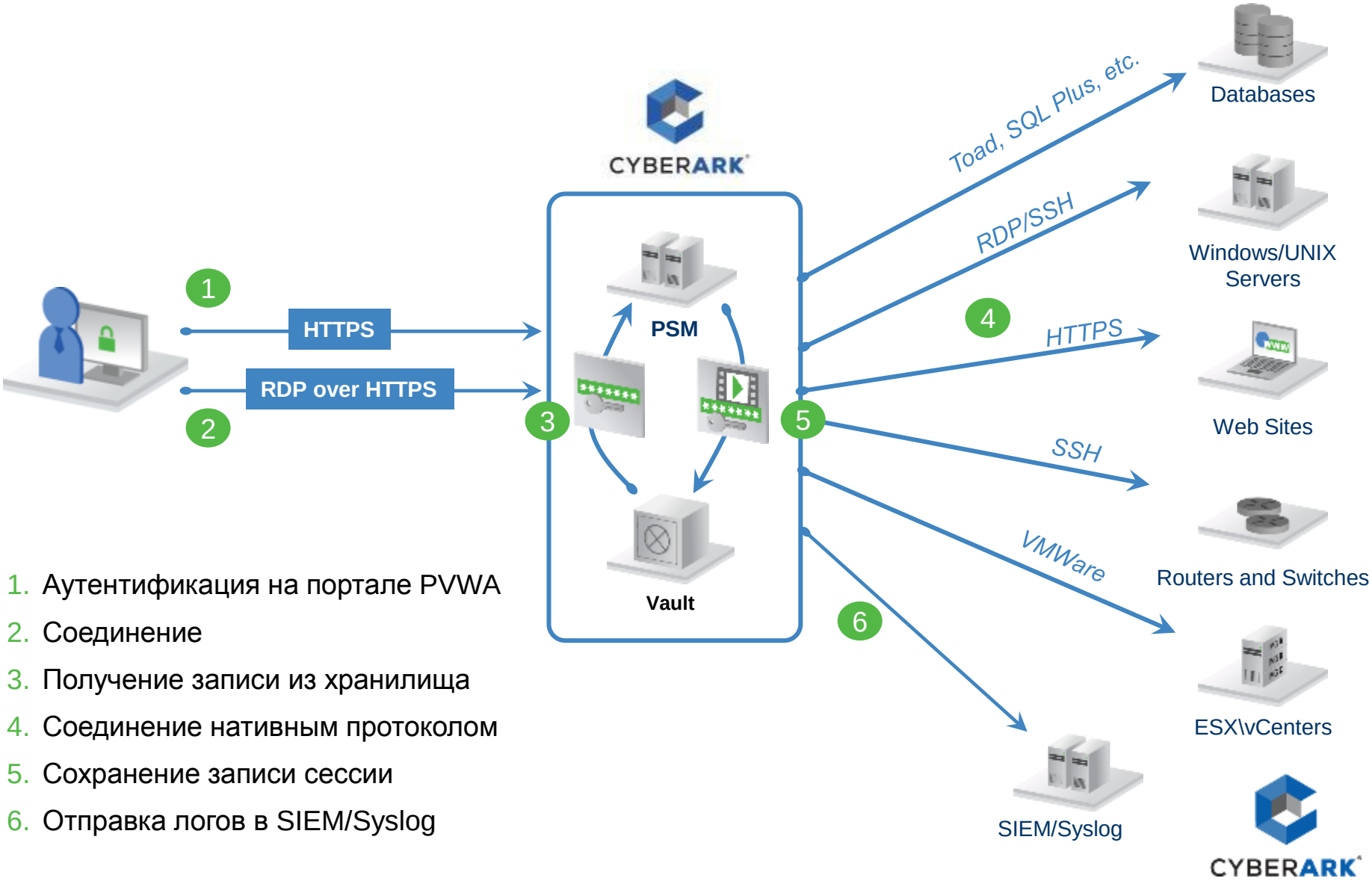
Enterprise IT Environment

Request to view Reports

Auditors

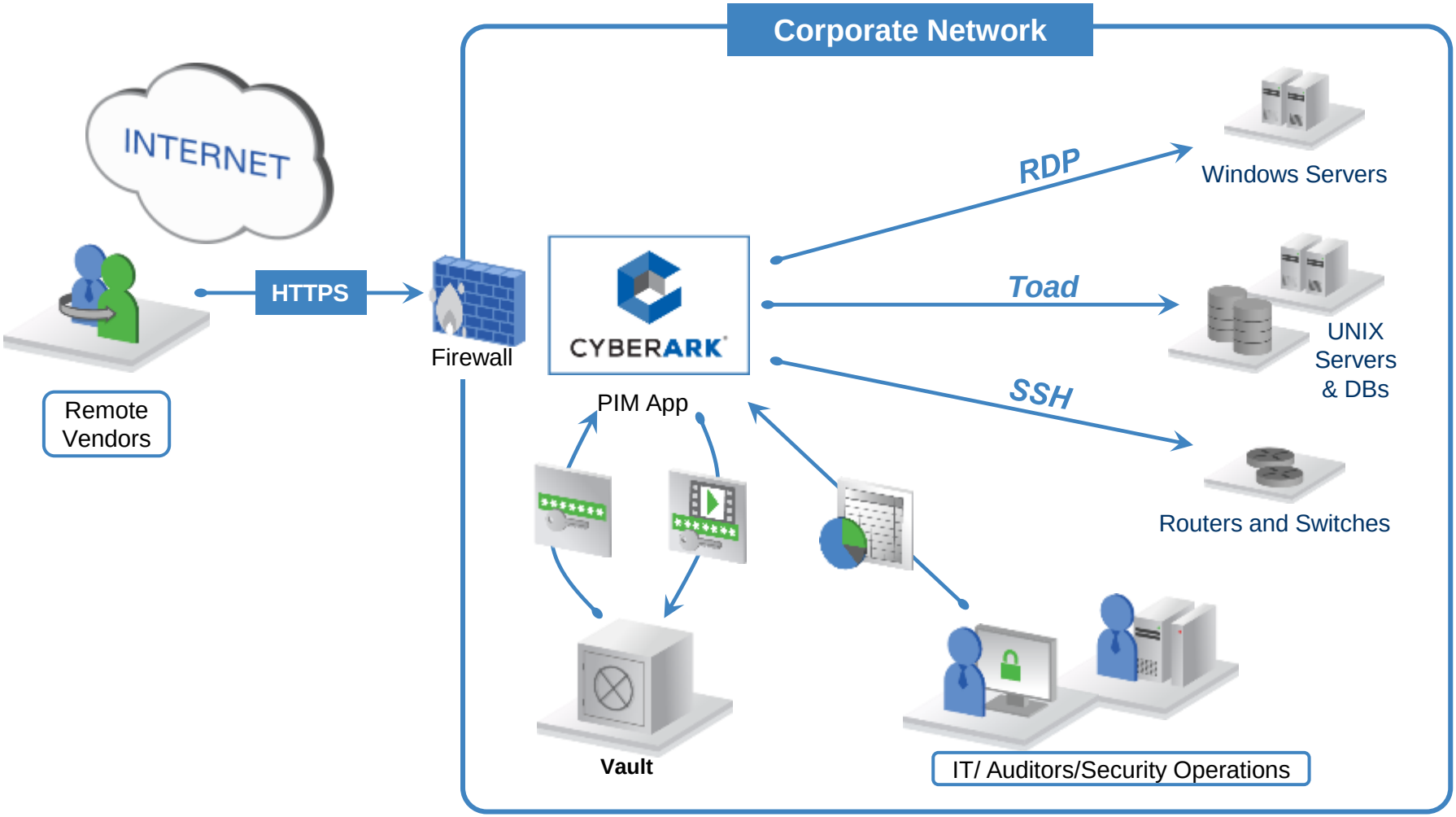
CYBERARK

Privileged Session Manager (PSM)



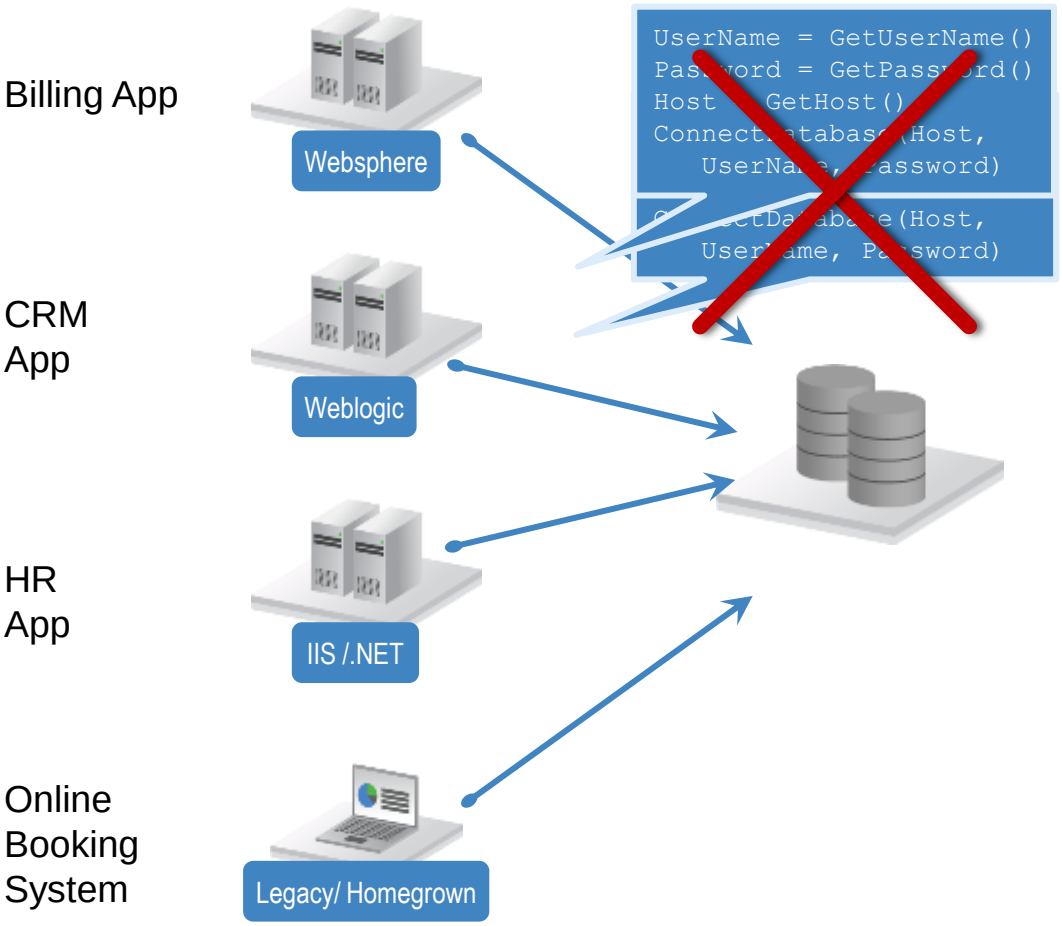
1. Аутентификация на портале PVWA
2. Соединение
3. Получение записи из хранилища
4. Соединение нативным протоколом
5. Сохранение записи сессии
6. Отправка логов в SIEM/Syslog

Privileged Account Security for Remote Vendors



CYBERARK

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

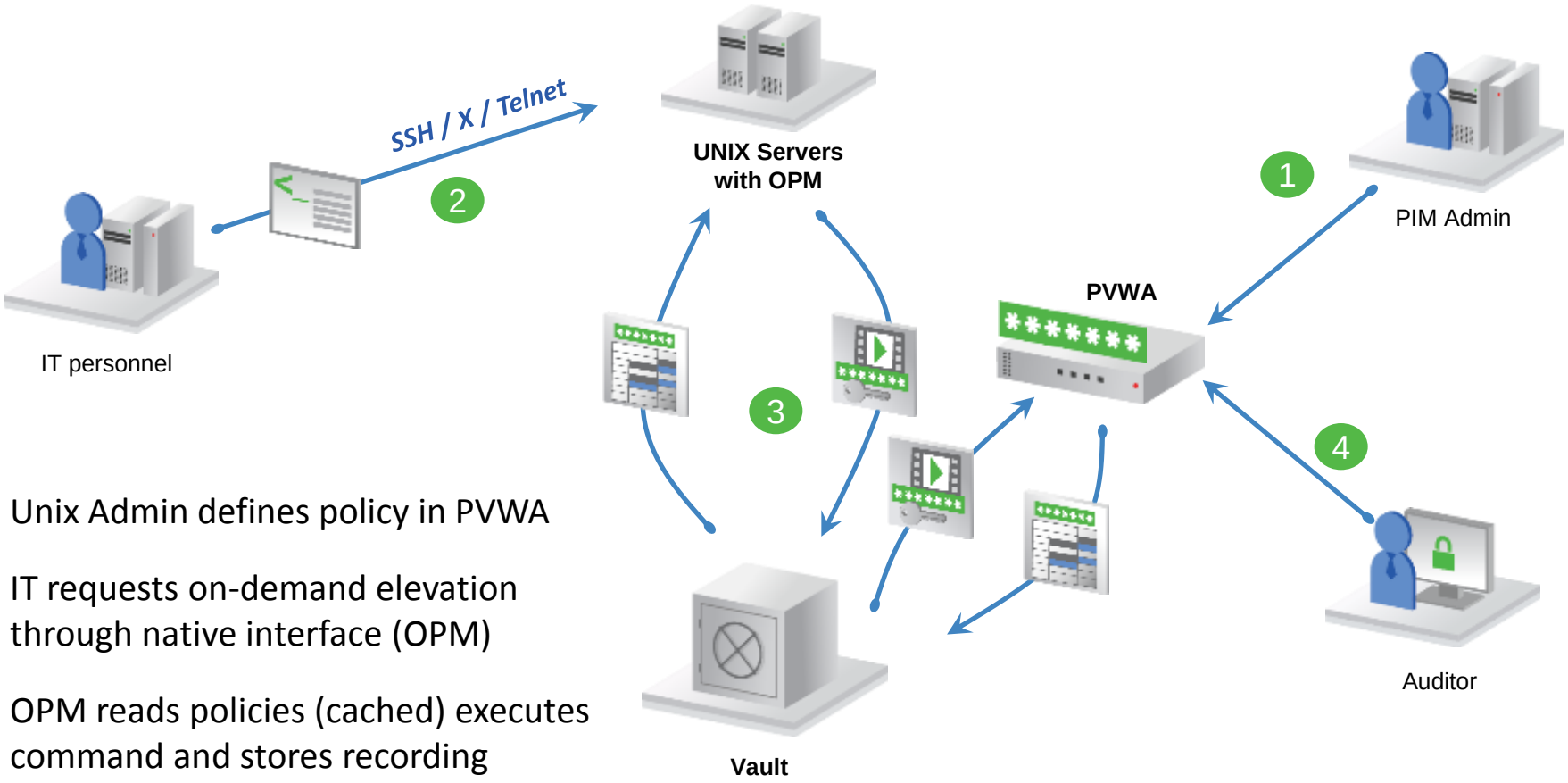


- Защищает и сбрасывает учетную запись приложения без простоя и рестарта
- Безопасно кэширует для непрерывности бизнеса и высокой производительности
- Исключает изменение кода и затраты на изменения паролей или адресов машин
- Строгая аутентификация по:
  - Адресу машины
  - Пользователю OS
  - Адресу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

Защищает, управляет и устраняет встроенные привилегированные аккаунты из приложений

CYBERARK

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

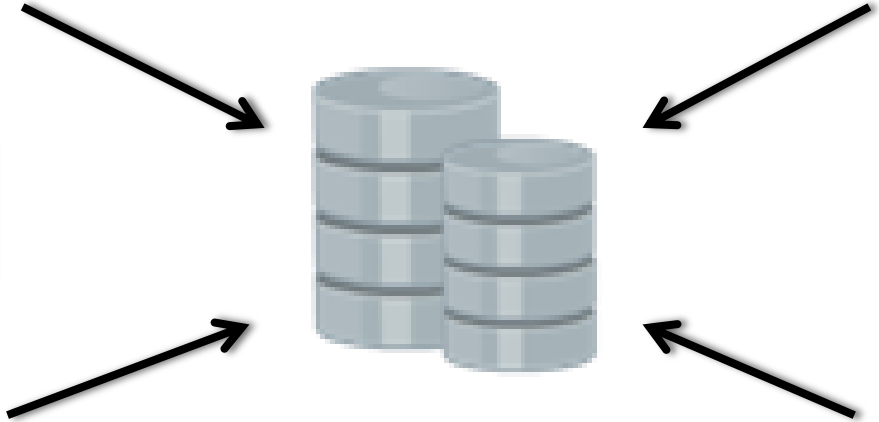
- Контроль защищенности, доступа и активности
- Автоматическое управление и замена аккаунтов

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

Как насчет скриптов, имеющих встроенные sys-пароли?

Права DBA в приложениях и скриптах

- Замена встроенных паролей
- Строгая аутентификация приложений



Пользователи хостов и файлов данных

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

Что если они имеют доступ к nix-серверам?

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

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

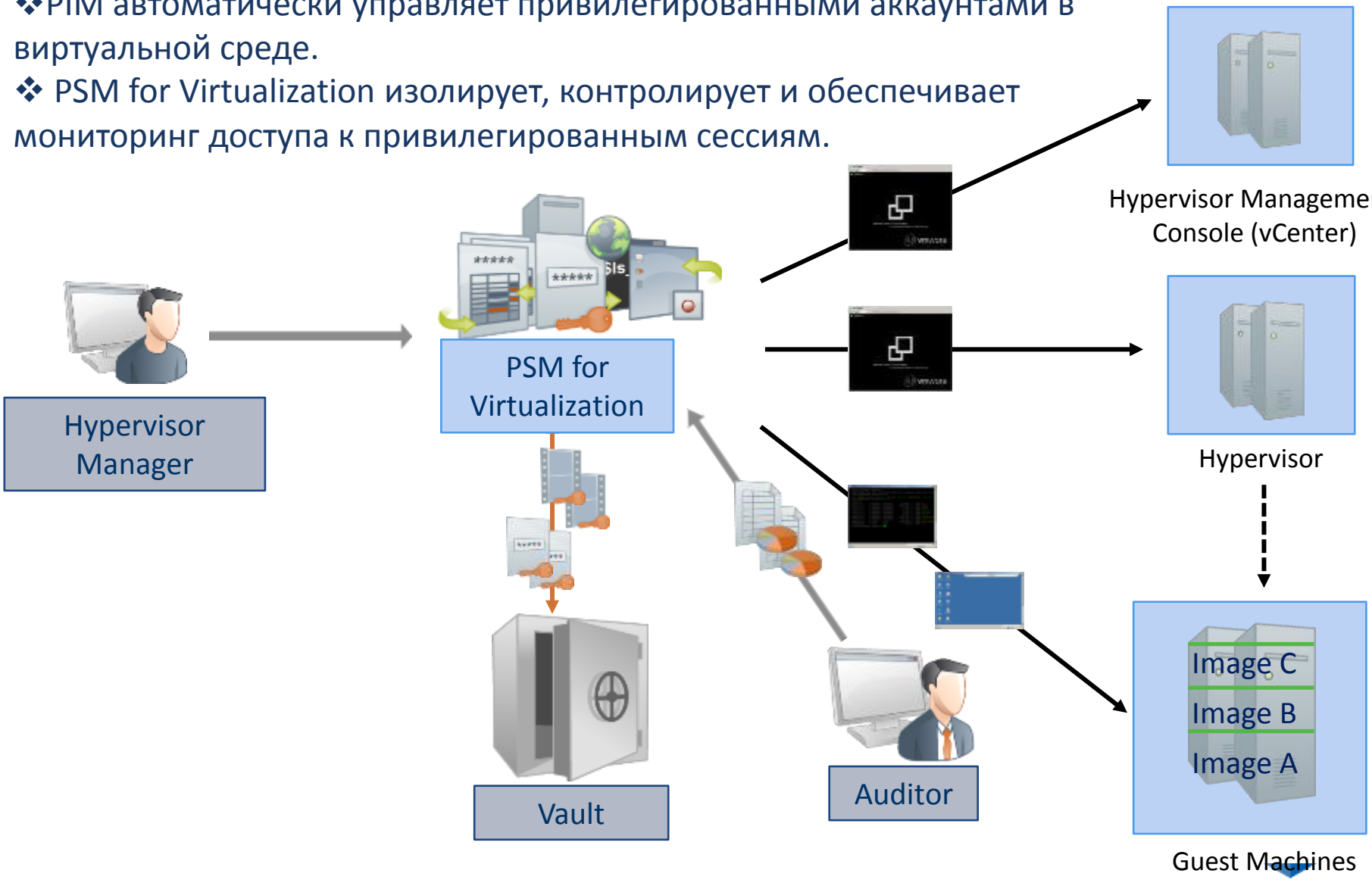
Enterprise Password Vault
Application Identity Manager
On-Demand Privileges Manager
Privileged Session Manager for DBs

CYBERARK

PIM&PSM – инновационный подход к безопасности

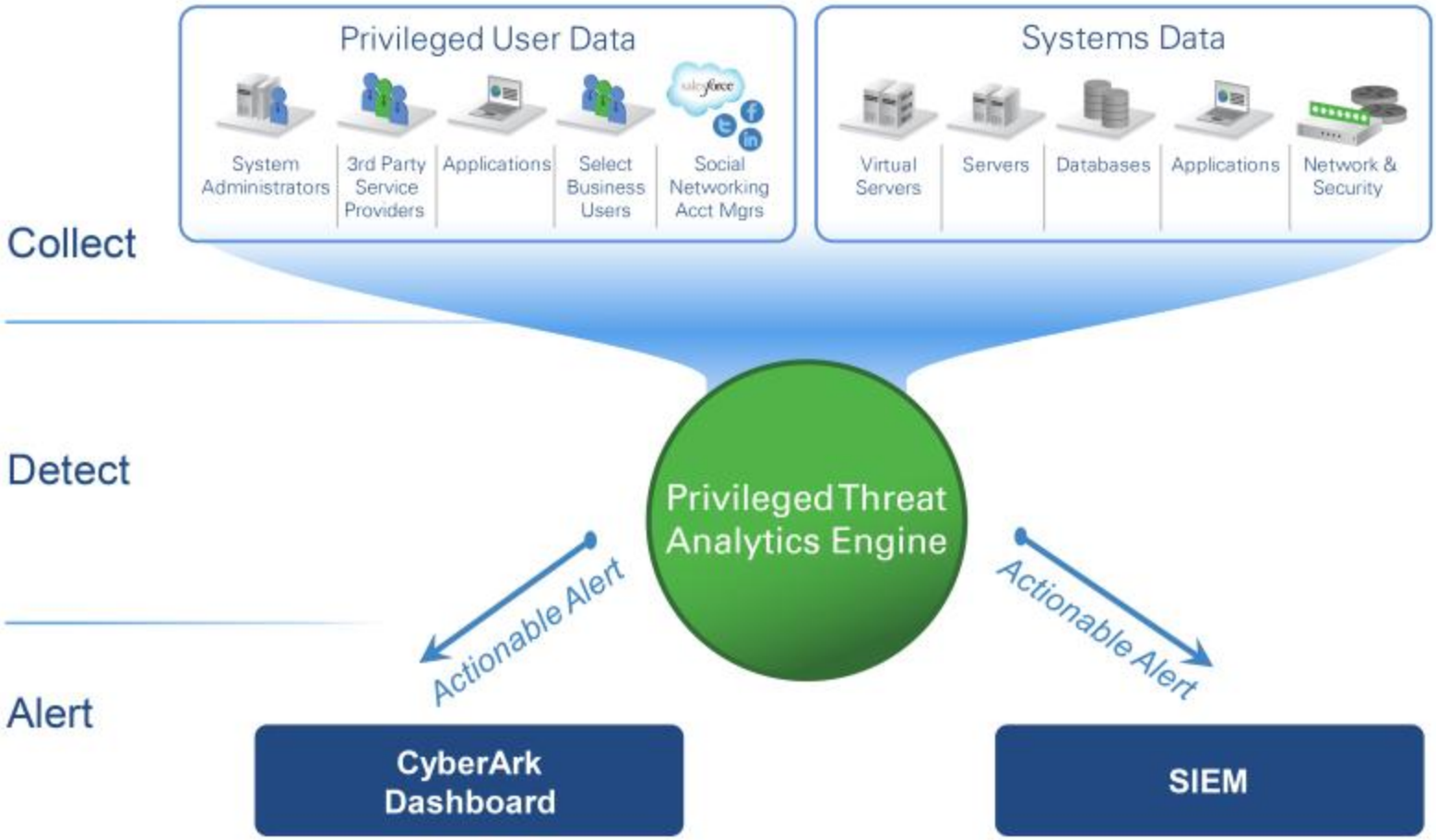
❖PIM автоматически управляет привилегированными аккаунтами в виртуальной среде.

❖ PSM for Virtualization изолирует, контролирует и обеспечивает мониторинг доступа к привилегированным сессиям.



CYBERARK

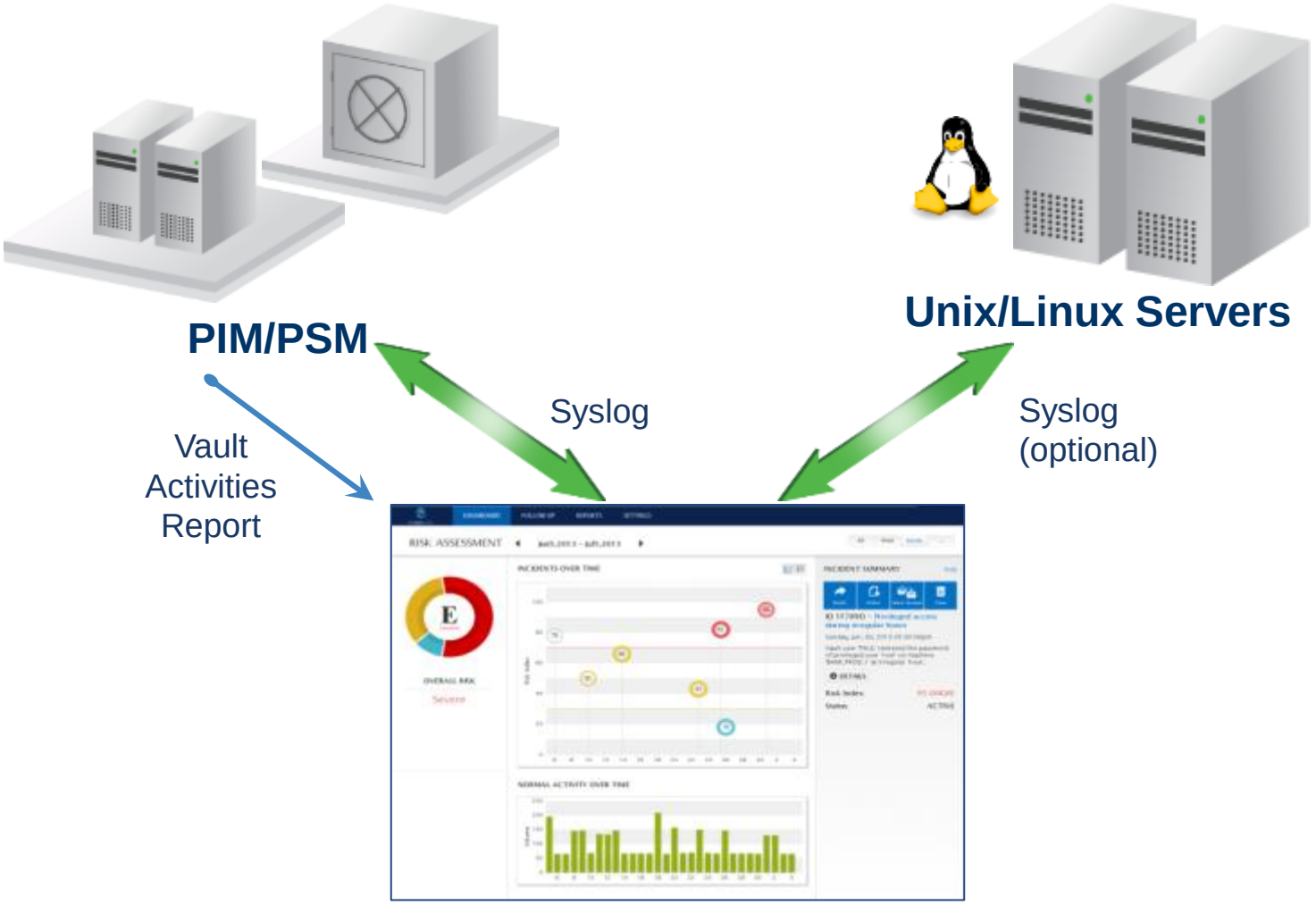
Privileged Threat Analytics (PTA)



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

CYBERARK

PTA - Seamless Integration with Prod.PIM/PSM



How Does PTA Work?

Collect

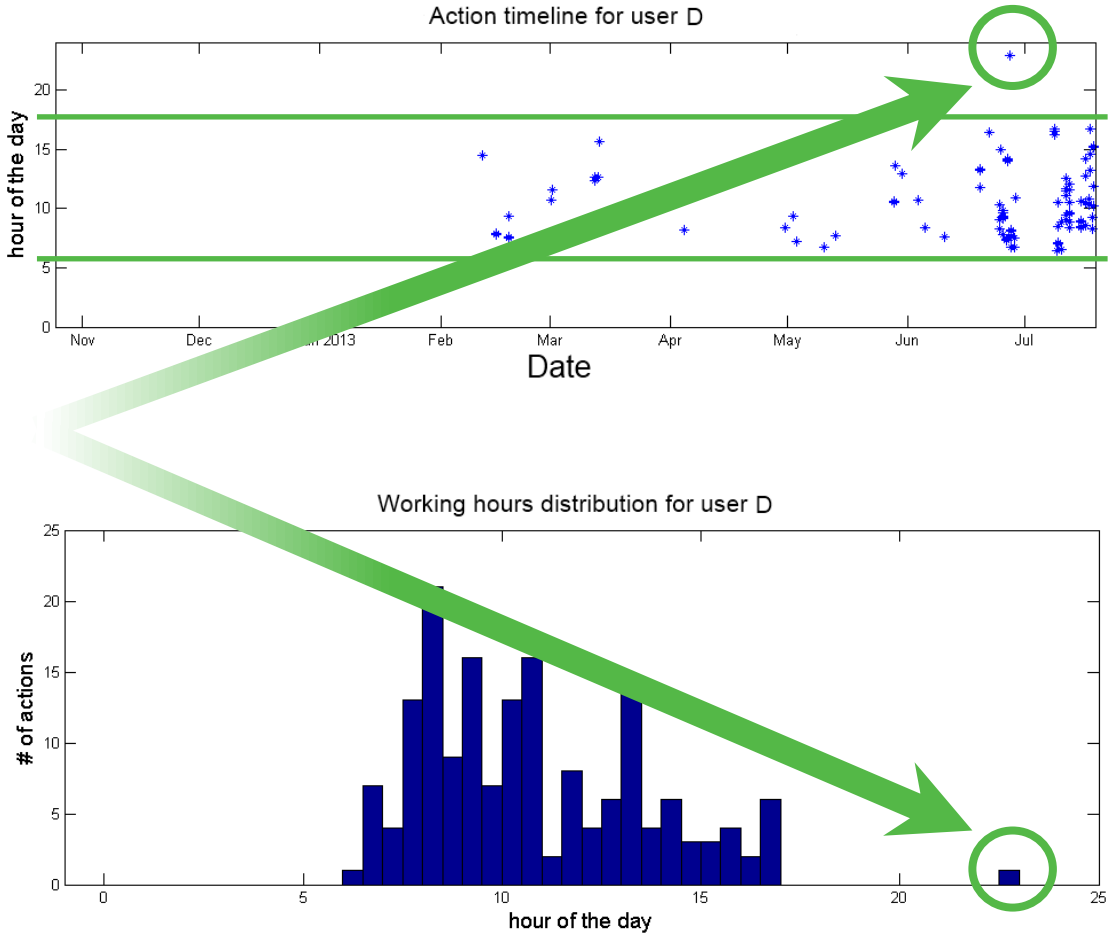
Collecting privileged accounts activity

Ongoing Profiling

Profiling normal behavior

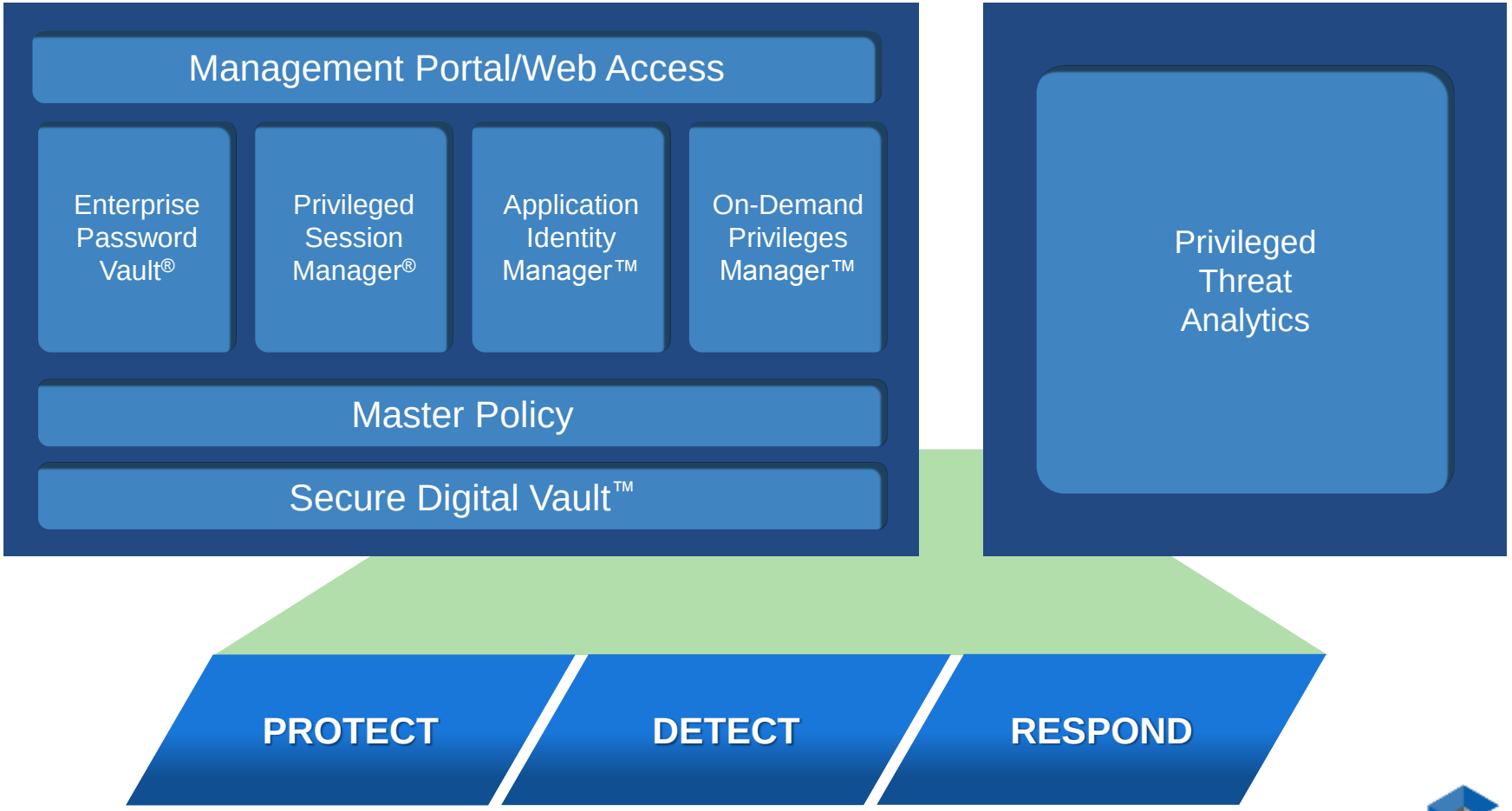
Detect

Detecting abnormal privileged accounts activity



CYBERARK

CyberArk's Privileged Account Security Solution



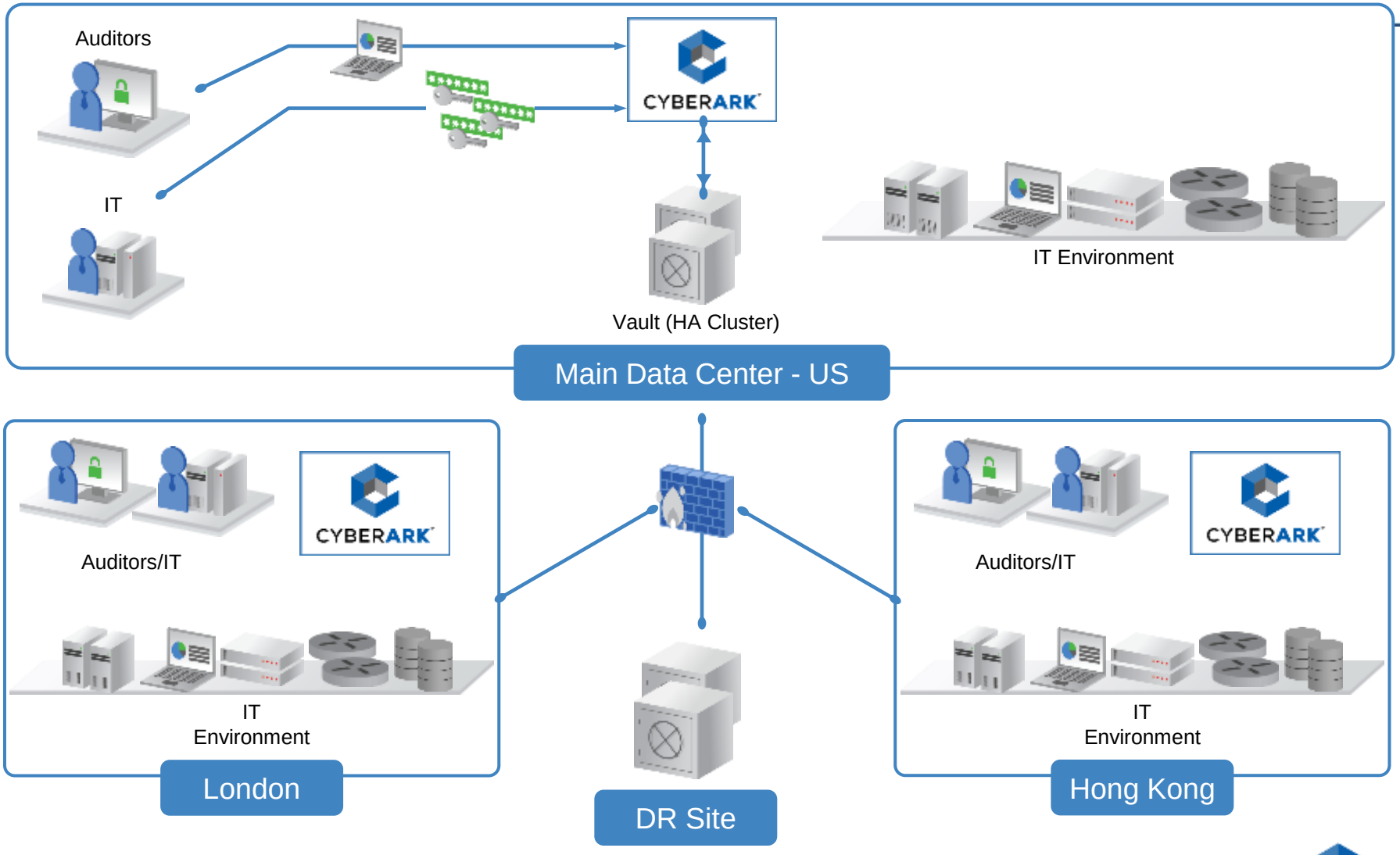
CYBERARK

CyberArk's Integration Across the Enterprise

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

CYBERARK

Распределенная архитектура CyberArk



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

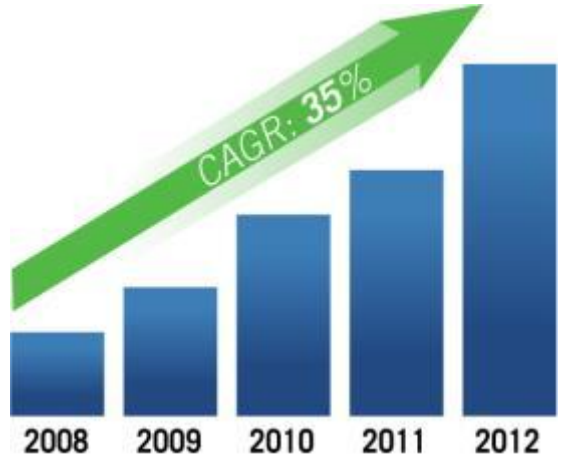
- Безопасность прозрачна для аудита

Единое всестороннее решение

- Одно решение для всех задач
- Уровня Enterprise

Глобальные клиенты

Deutsche Bank · NOVARTIS · QUALCOMM · BARCLAYS · Williams · McKESSON (Empowering Healthcare) · ING DIRECT · BT · FannieMae. · BRAUN



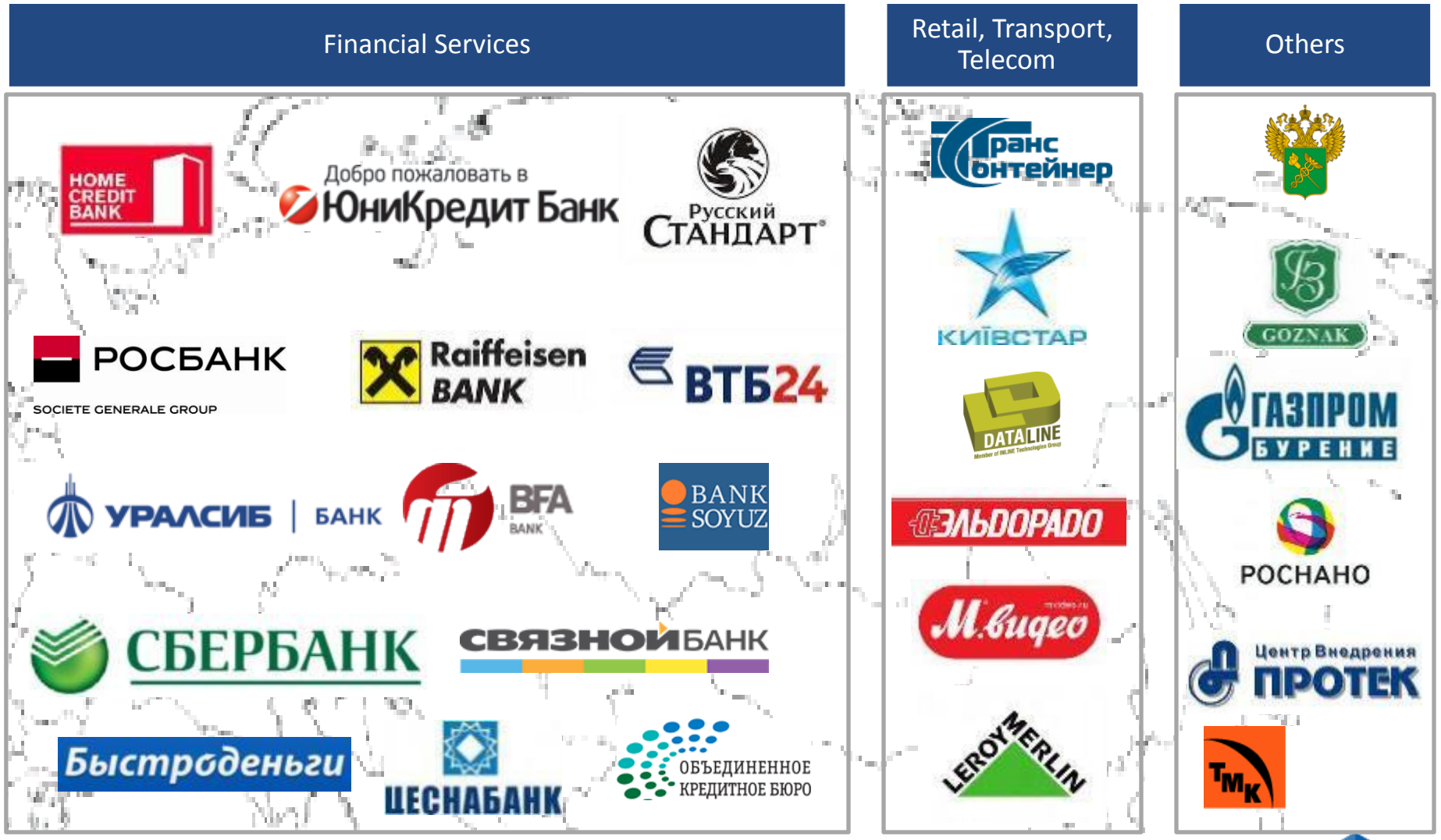
CYBERARK

Клиенты CyberArk в мире

Доверенный эксперт для более чем 1,300 компаний мира

CYBERARK

Клиенты в регионе



CYBERARK

Спасибо за внимание…