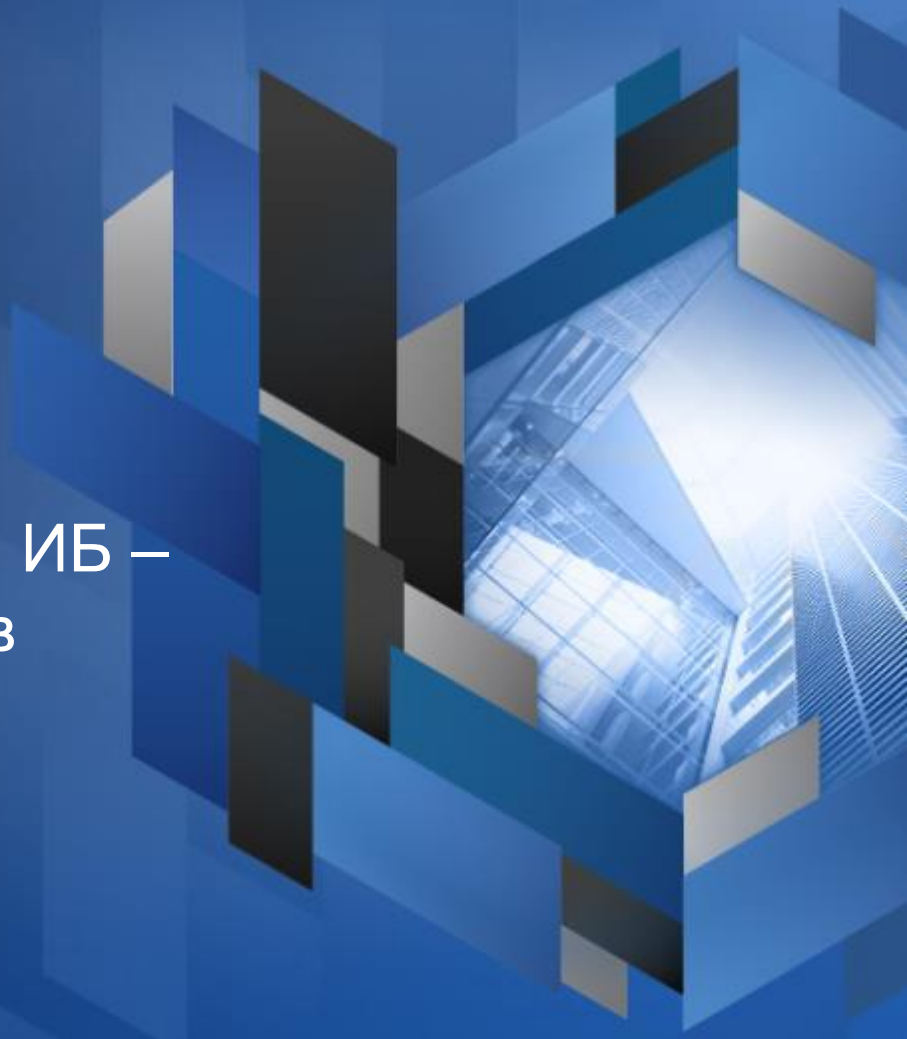
CYBERARK

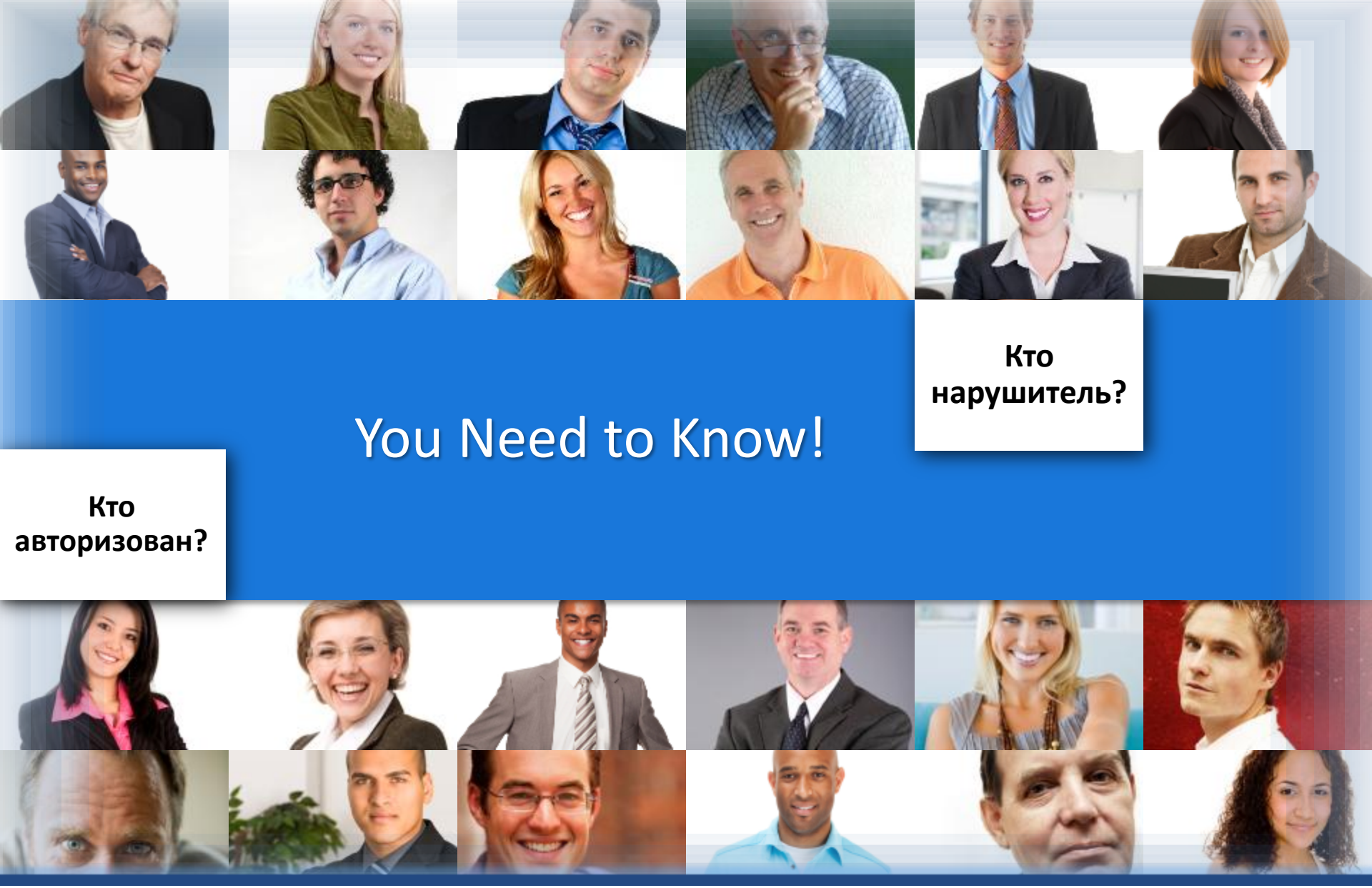


Эффективные инструменты ИБ – для бизнеса и специалистов

Богдан Тоболь, региональный менеджер
Олег Котов, сейлз-инженер


Внутренние пользователи
Подрядчики
Сторонние разработчики
Провайдеры сервисов
Временные сотрудники
Системные интеграторы

CYBERARK



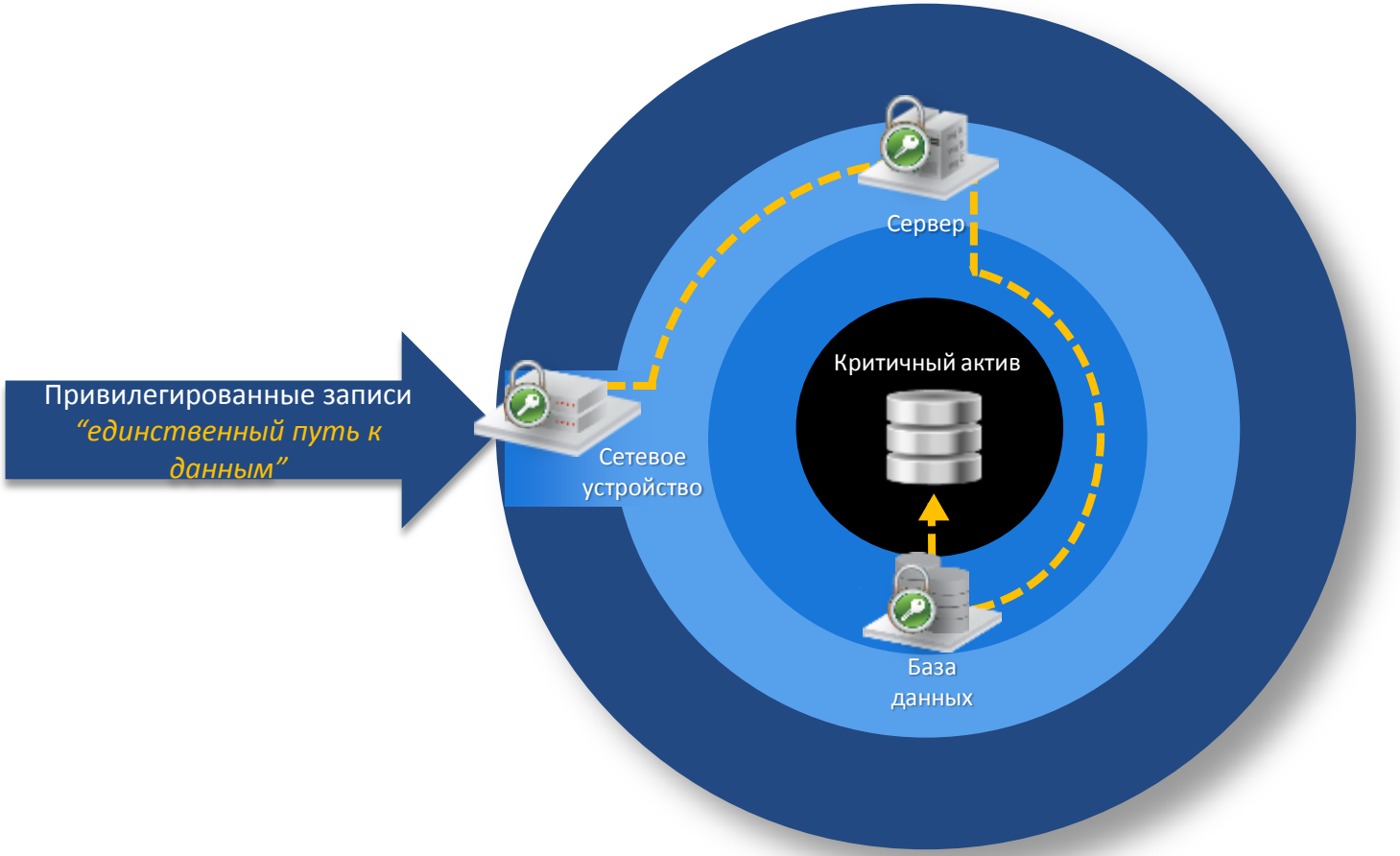
You Need to Know!

Кто нарушитель?

Кто авторизован?

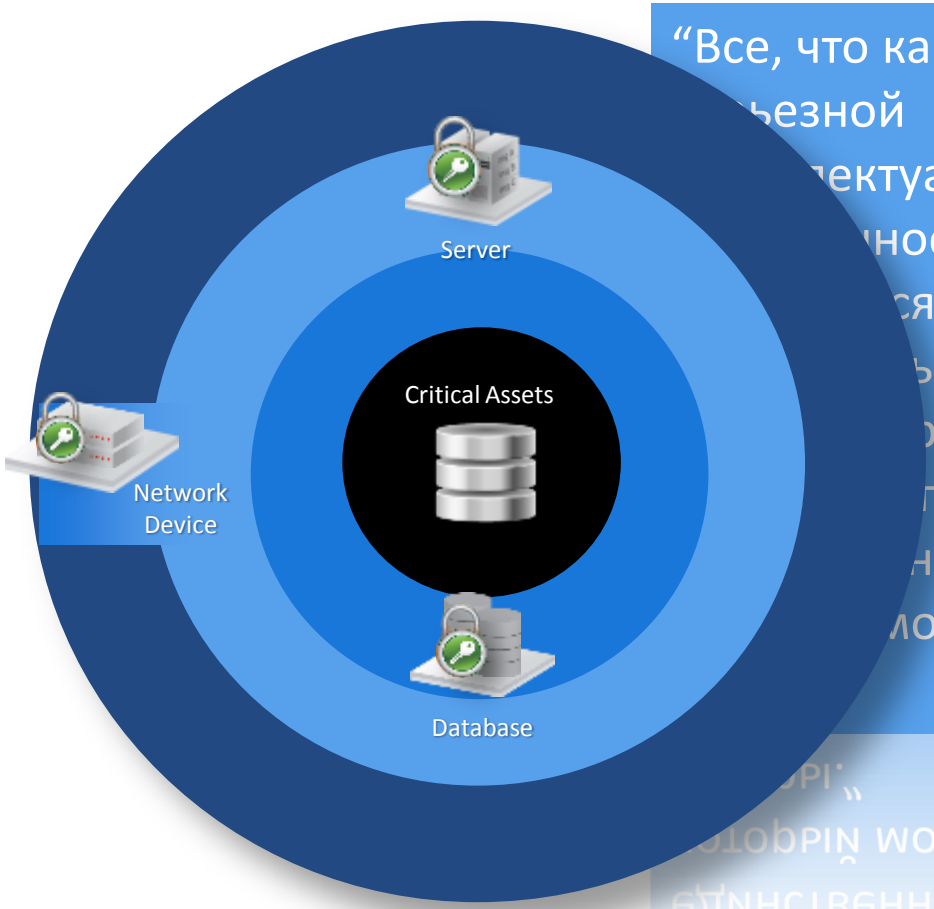
CYBERARK

«Все пути ведут...» к привилегированым записям



CYBERARK

Привилегированные записи – встроенные уязвимости (Gartner)



"Все, что касается
ьезной
лектуальной
ности,
ся в хорошо
ых системах, и
рованные
писи являются
ным способом,
могут получить

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

CYBERARK

Привилегированные аккаунты – вторжение

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…”

SANS; Top 20 Security Controls, #12

CYBERARK

Привилегированный аккаунт: что, где и почему

	Какие	Кем используются	Используются для
Привилегированные персональные	• Облачные провайдеры • Персональные записи с широкими привилегиями	• IT службы • Сотрудники	• Привилегированные операции • Доступ к критичной инф. • Веб-сайты
Общие привилегированные	• Administrator • root • 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

Все высокие привилегии

Сложно контролировать, управлять и отслеживать

Ведут к критическим рискам при неправильном использовании

CYBERARK®

Привилегированные записи везде!

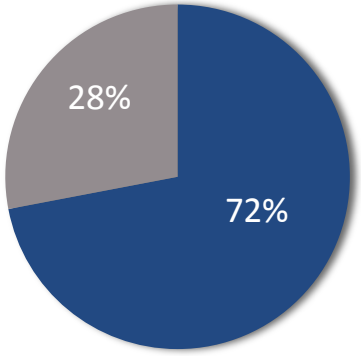
CYBERARK

Но этот факт не понятен...

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

CYBERARK®

Используются вариации разных решений



Вы отслеживаете привилегированную активность?

Cyber-Privileged Account Security & Compliance Survey, May 2013

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

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

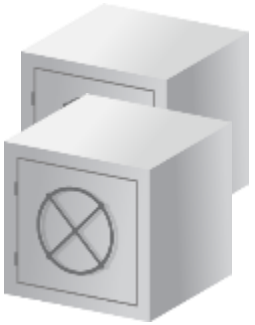
- Их больше, чем Вы думаете
- Вы должны знать о всех

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

Внешние поставщики

IT службы

Аудиторы

Разработчики и DBA

PIM Portal/Web Access

Enterprise Password Vault®

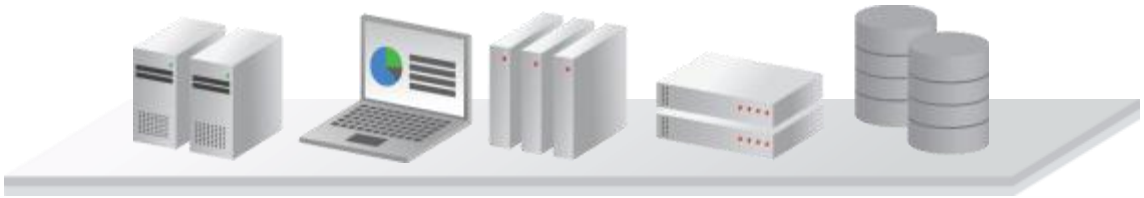
Privileged Session Manager®

Application Identity Manager™

On-Demand Privileges Manager™

Master Policy

Secure Digital Vault™



Любое устройство, ЦОД –
Традиционные и облачные, хостинг

Identity Management

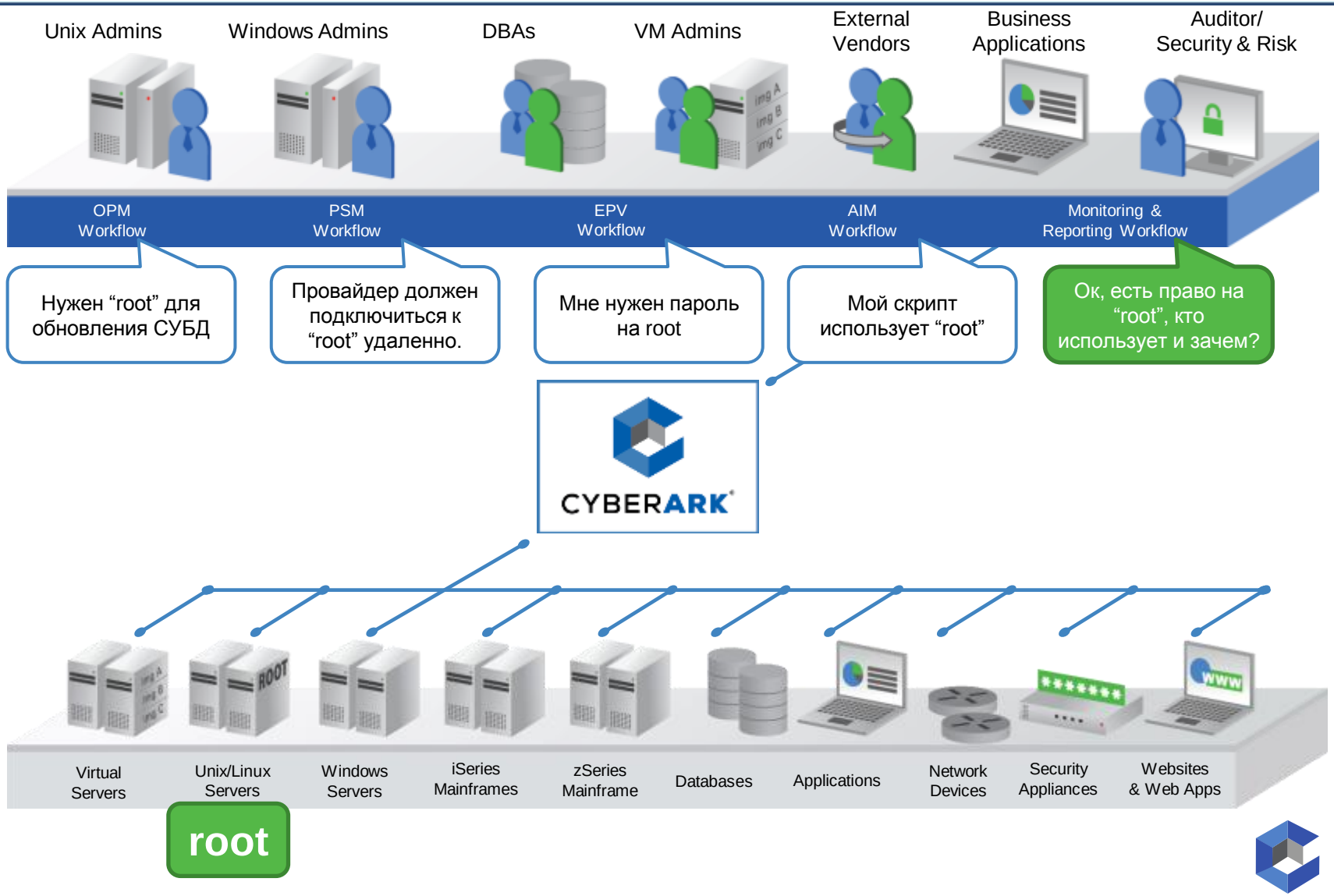
Ticketing Systems

Monitoring & SIEM Applications

Enterprise Directory and More

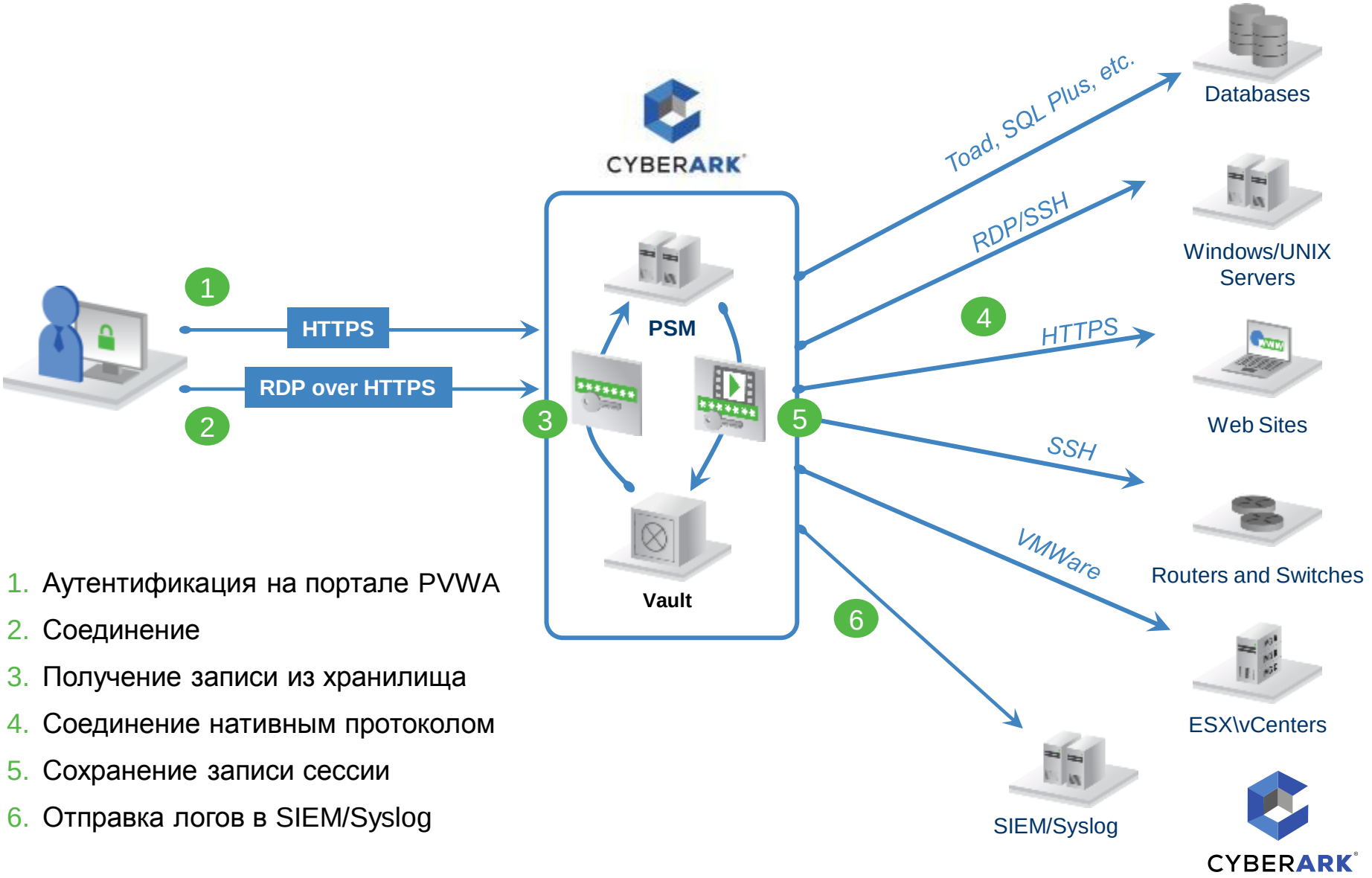
CYBERARK®

Пример: управление привилегированными записями



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

Устранение запрограммированных паролей

Конфигурационные файлы,базы данных

Конф.файлы Веба

INI/текстовые файлы

БД приложений

```
<Resource name="jdbc/db1"
  auth="Container"
  type="oracle.jdbc.pool.OracleDataSource"
  driverClassName="oracle.jdbc.driver.OracleDriver"
  factory="oracle.jdbc.pool.OracleDataSourceFactory"
  url="jdbc:oracle:thin:@oracle.microdeveloper.com:1521:db1"
  user="scott"
  password="tiger"
  maxActive="20"
  maxIdle="10"
  maxWait="-1" />
```

Сервера приложений

В реестрах, FTP и т.д.

Служебные аккаунты

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

Запрограммируемые, встроенные аккаунты

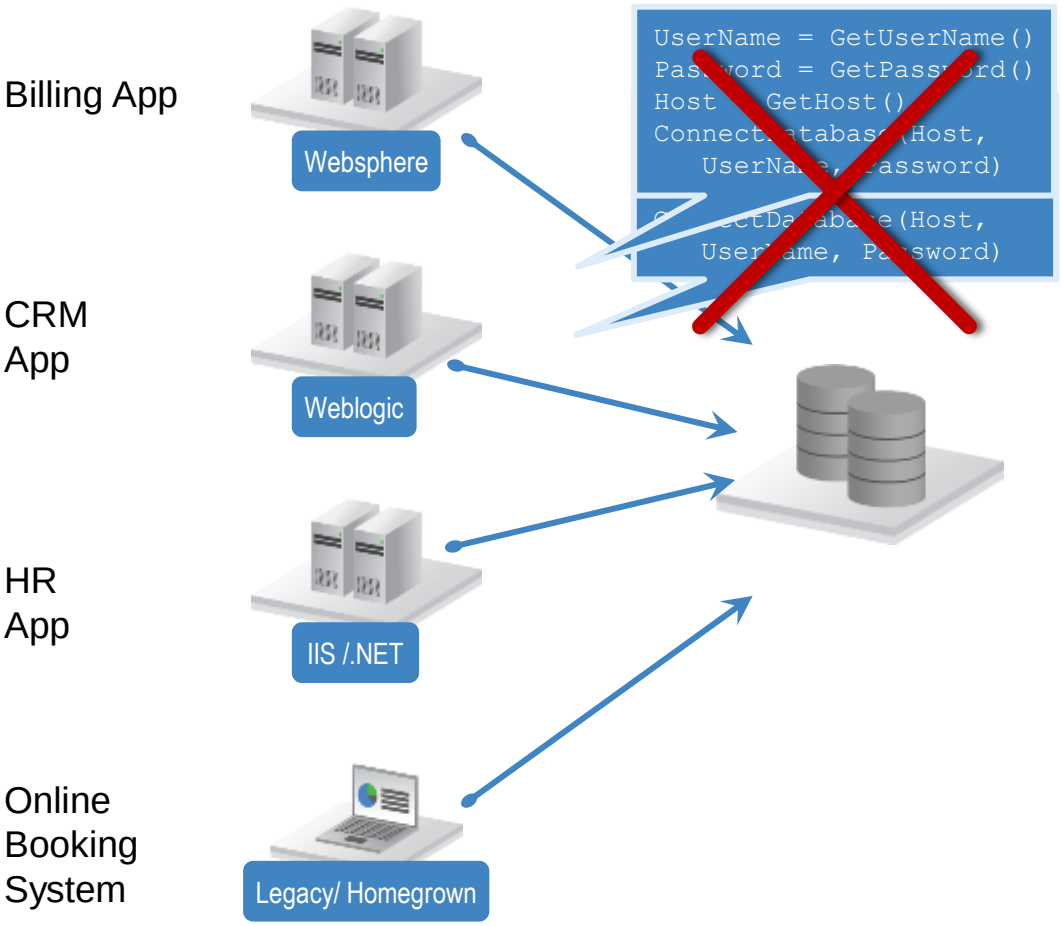
```
Password = y7qer$1
Host = "10.10.3.56"
```

Сторонние приложения

ORACLE QUALYS McAfee

CYBERARK

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

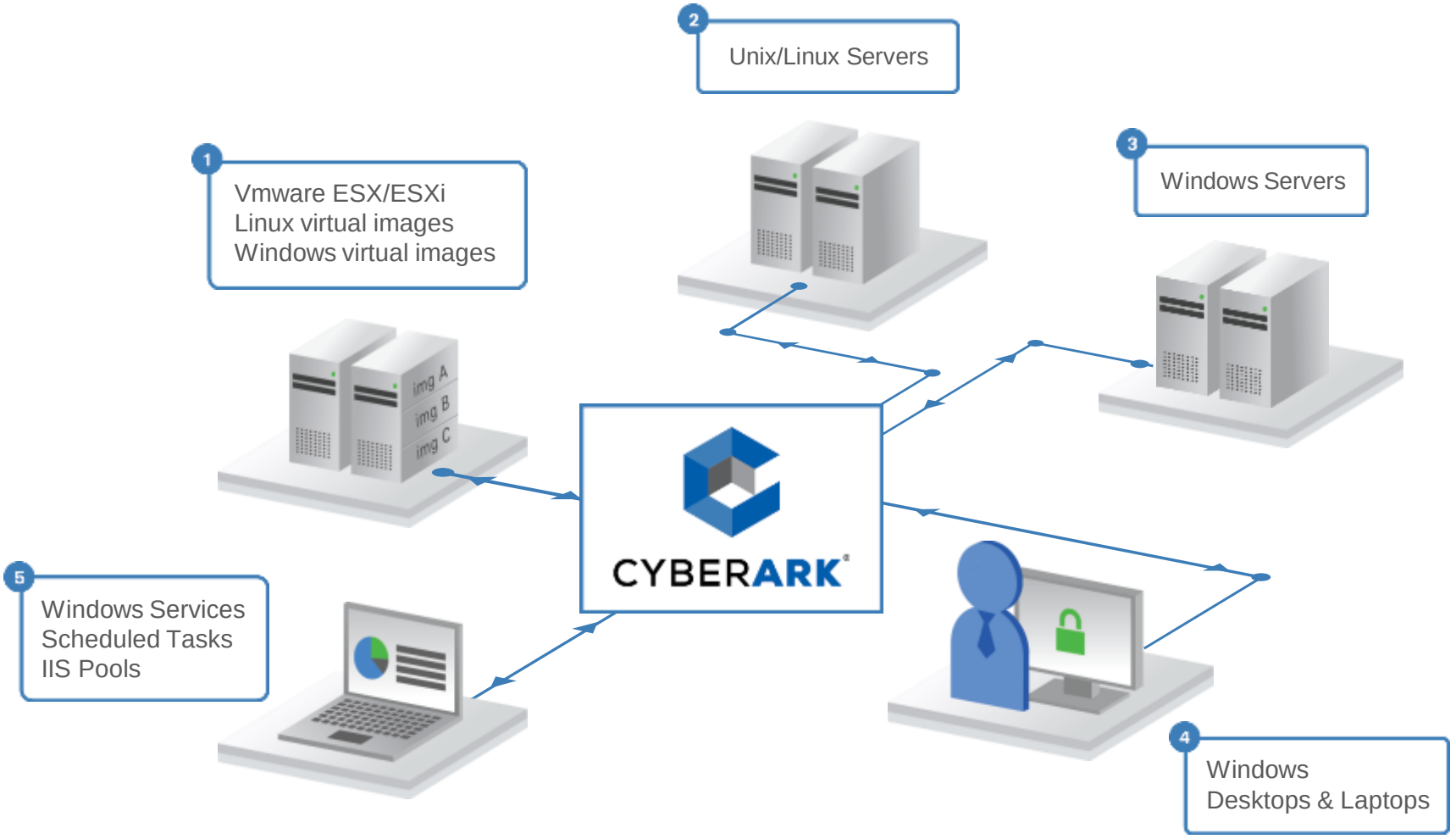


- Защищает и сбрасывает учетную запись приложения без простоя и рестарта
- Безопасно кэширует для непрерывности бизнеса и высокой производительности
- Исключает изменение кода и затраты на изменения паролей или адресов машин
- Строгая аутентификация по:
  - Адресу машины
  - Пользователю OS
  - Адресу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

Защищает, управляет и устраняет встроенные привилегированные аккаунты из приложений

CYBERARK

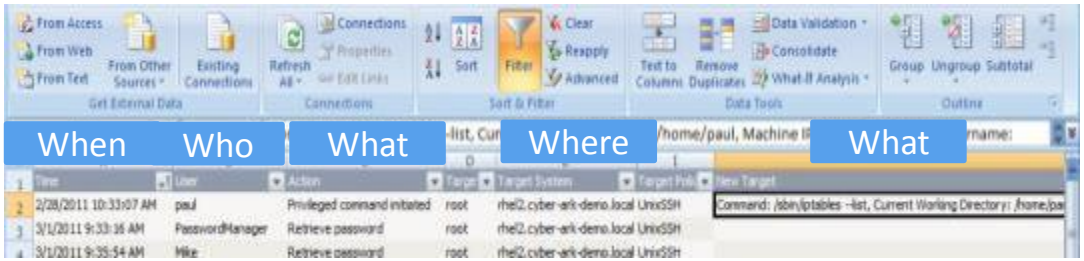
EPV: автоматическое определение привилегированных аккаунтов всей системы



Где привилегированные записи и суперпользователи?

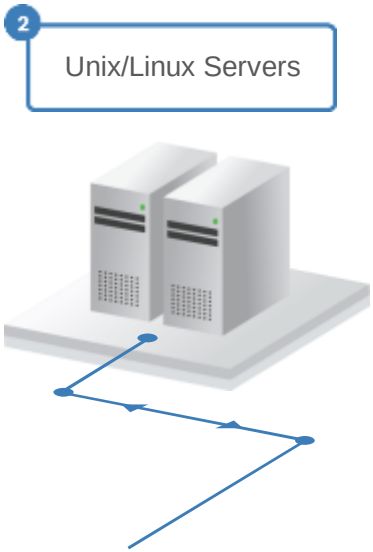
CYBERARK

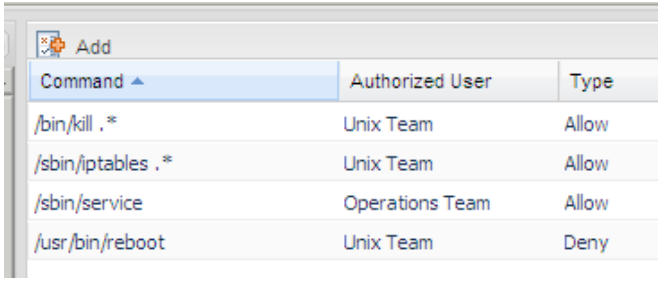
On-demand Privileges Manager (OPM) for Unix



Мониторинг и аудит, отчеты и запись текстовых команд

Контроль суперпользователя



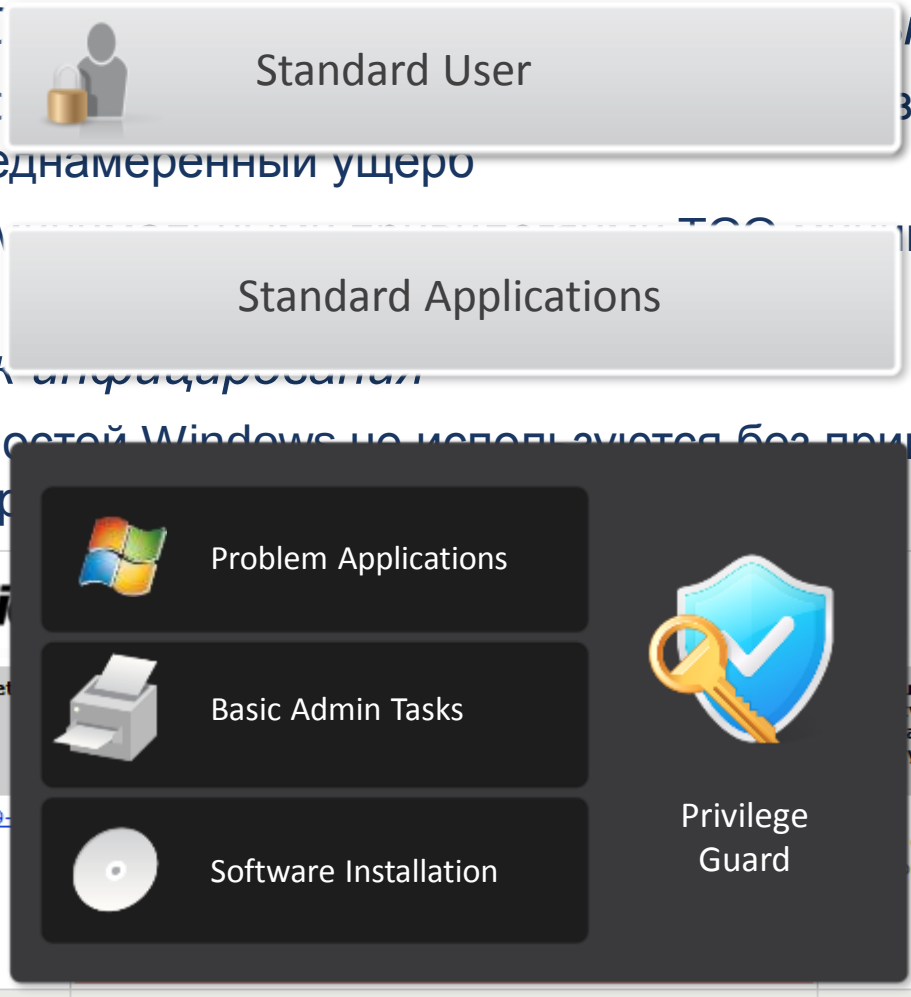


Гранулярный контроль доступа и политик

CYBERARK

OPM for Windows

- *Снижает TCO* *и ИТ*
  - Минимум пр звонков в ИТ, ниже “непреднамеренный ущерб”
  - Gartner: “С м мум на 20% ниже”
- *Снижает риск инфицирования*
  - **90%** уязвимостей Windows не используются без привилегий admin Исключая пр



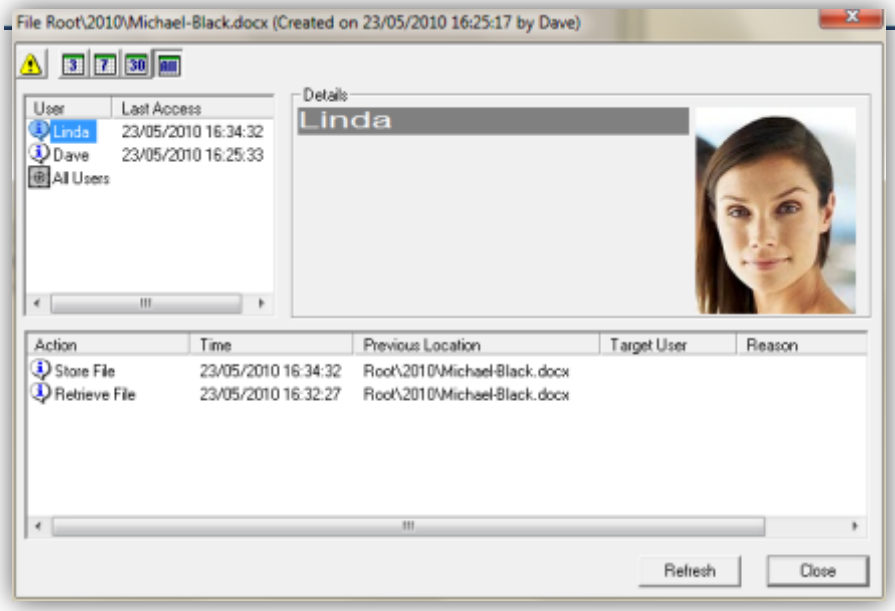
CYBERARK

Обмен файлами бизнес-пользователей

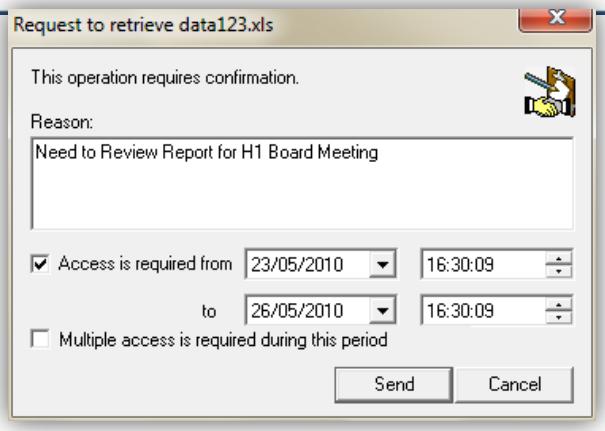
- Решения совета директоров, руководства, бизнес-планы
- Инженерная разработка, файлы дизайна
- Управление продуктом/ проектом/ развитием
- Юридический департамент
- Финансовые службы, бухгалтерия
- HR - зарплаты, контракты, характеристики, опционы
- Управление документами
- ИБ компании
- Конкурсные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

CYBERARK®

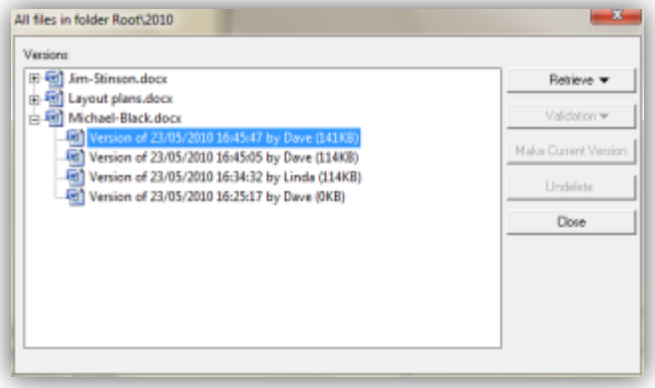
SIM – изоляция конфиденциальной информации



Зашифрованные архивы



Двойной контроль

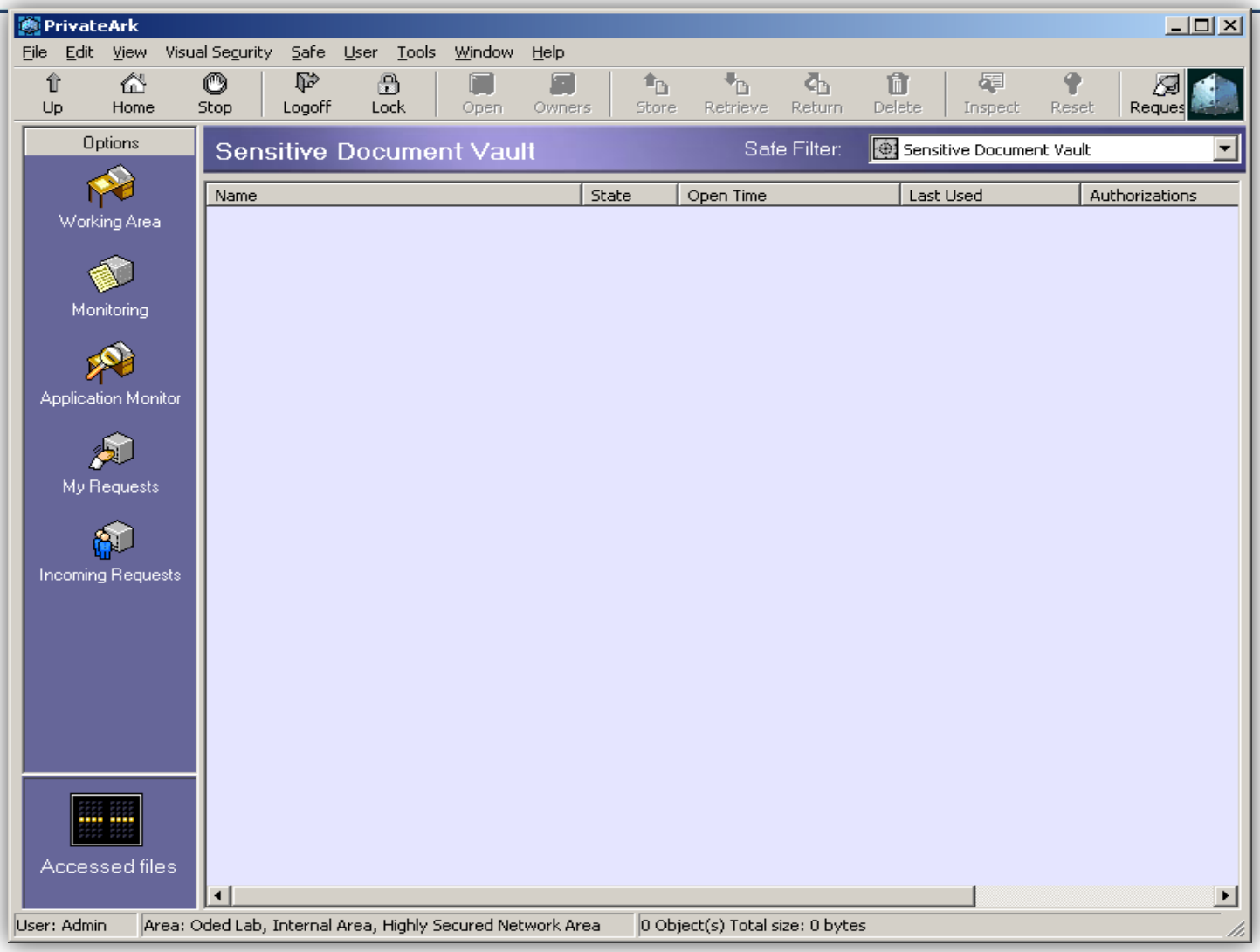


Версии

Защищенная почта, уведомления
и детальные отчеты

CYBERARK

SIM – администратору нет доступа к данным



CYBERARK

SIM: Enterprise Ready – готовая интеграция

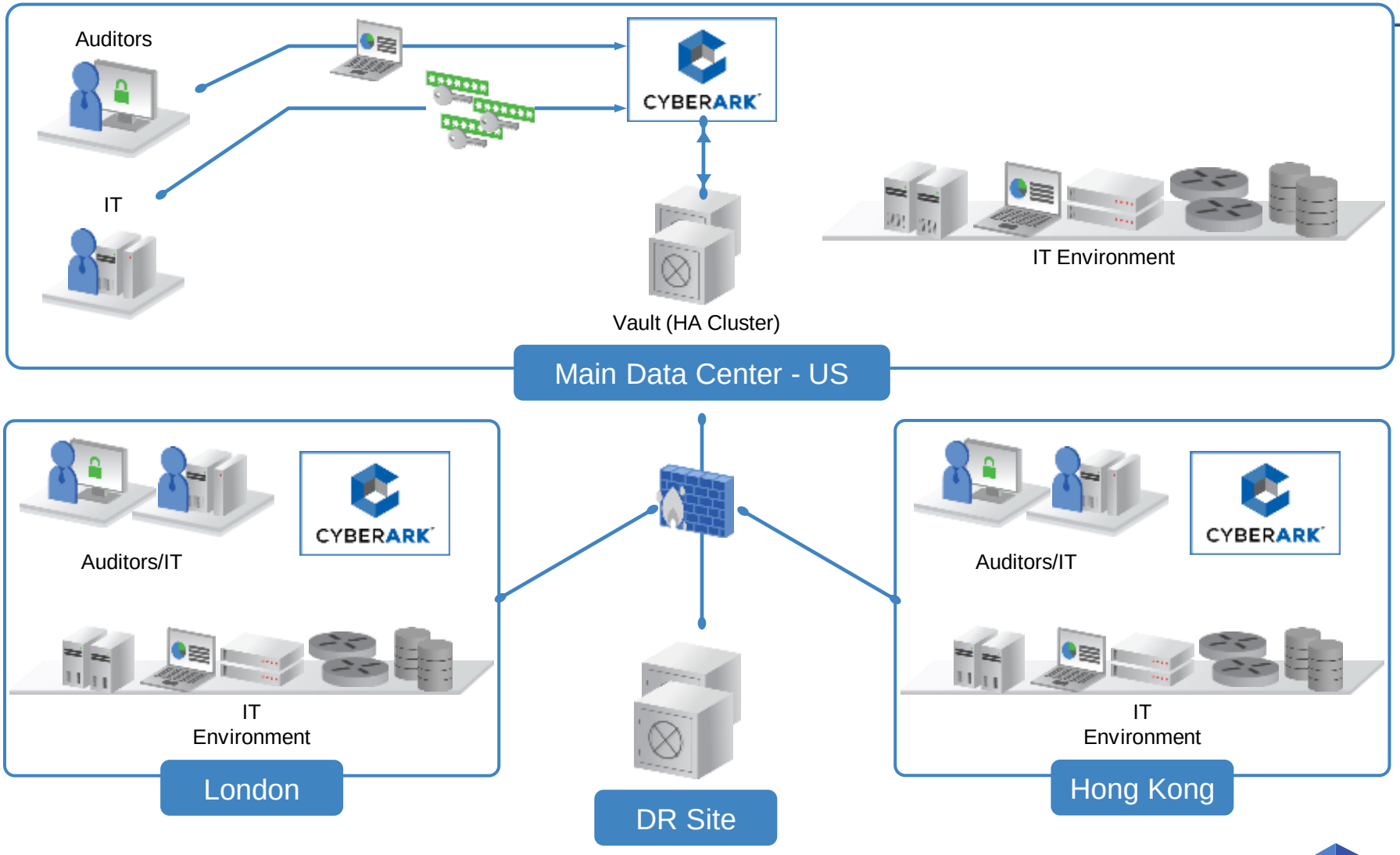
Отказоустойчивость	High Availability	Disaster Recovery	External Storage	Encrypted Backup			
Протоколы	Vault Protocol	FTP	FTP over SSL/TLS	SFTP / SSH	HTTP/S	SCP	
Аутентификация	Username / Password	RSA SecurID	Radius	PKI	Oracle SSO	LDAP	
LDAP	Active Directory	Sun One	Novell	Oracle	Any LDAP server		
SIEM 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

ORACLE PARTNERNETWORK · Microsoft GOLD CERTIFIED Partner · RSA · McAfee · IBM Business Partner · websense

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

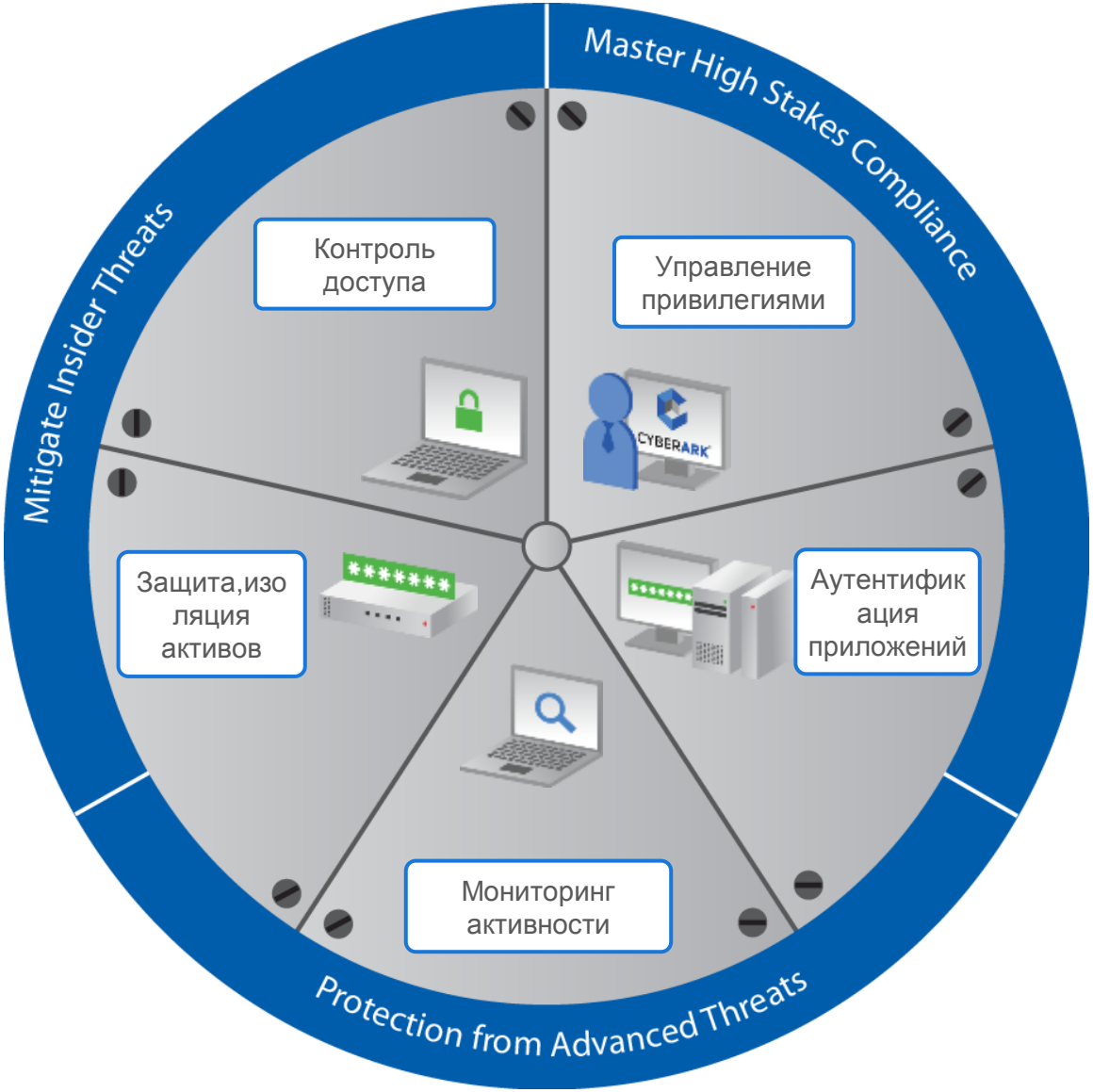
- Управление привилегиями Пользователей и отчетность
- Мониторинг и запись сессий
- Отчетность для соответствия
- Контроль удаленного доступа
- Аудируемый безопасный файлообмен

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

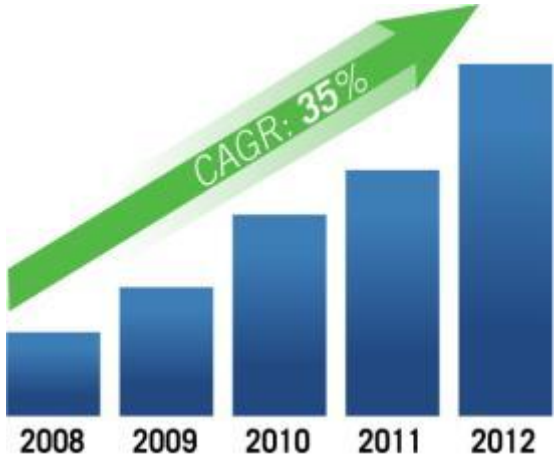
- Безопасность прозрачна для аудита

Единое всестороннее решение

- Одно решение для всех задач
- Уровня Enterprise

Глобальные клиенты

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

Financial Services	Retail, Transport, Telecom	Others

CYBERARK

Спасибо за Ваше внимание и время