Представляем CyberArk

Security for the Heart of the Enterprise

Nick Baglin, Vice President EMEA Sales

План……..

Кто мы, CyberArk…

Какие бизнес-проблемы мы решаем

Партнерство и альянсы CyberArk

Что мы рекомендуем предпринять любому бизнесу

CYBERARK®

О компании CyberArk

Доверенный эксперт в безопасности привилегированных записей

- Более 1,450 крупных корпоративных клиентов

Финансовая безопасность и постоянная прибыльность

- Goldman Sachs – главный инвестор

Акцент на решение бизнес-задач

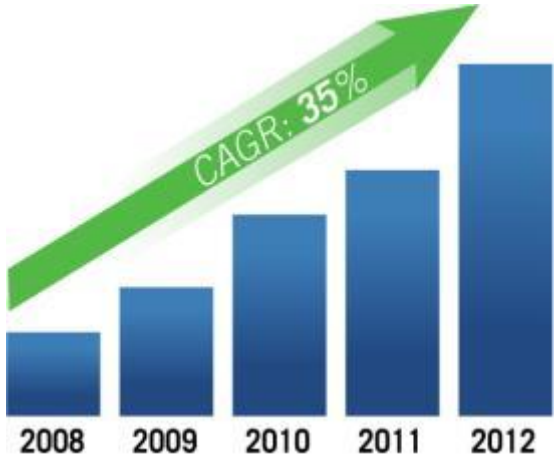
- Безопасность прозрачна для аудита

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®

Диверсифицированная клиентская база

Более 1450 глобальных корпоративных клиентов

CYBERARK

Клиенты в регионе

Финансы	Ритейл, Транспорт, Телеком	Другие

HOME CREDIT BANK

Bank Zachodni WBK

AVIVA

Русский СТАНДАРТ

РОСБАНК

SOCIETE GENERALE GROUP

ВТБ24

Raiffeisen BANK

УРАЛСИБ | БАНК

Bank BGZ

ЦЕСНАБАНК

Santander CONSUMER BANK

ORLEN

КИЇВСТАР

ЭЛЬДОРАДО

М.видео

LEROY MERLIN

GOZNAK

ГАЗПРОМ БУРЕНИЕ

РОСНАНО

Центр Внедрения ПРОТЕК

CYBERARK

CYBERARK

Какие бизнес-проблемы мы решаем?

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

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®

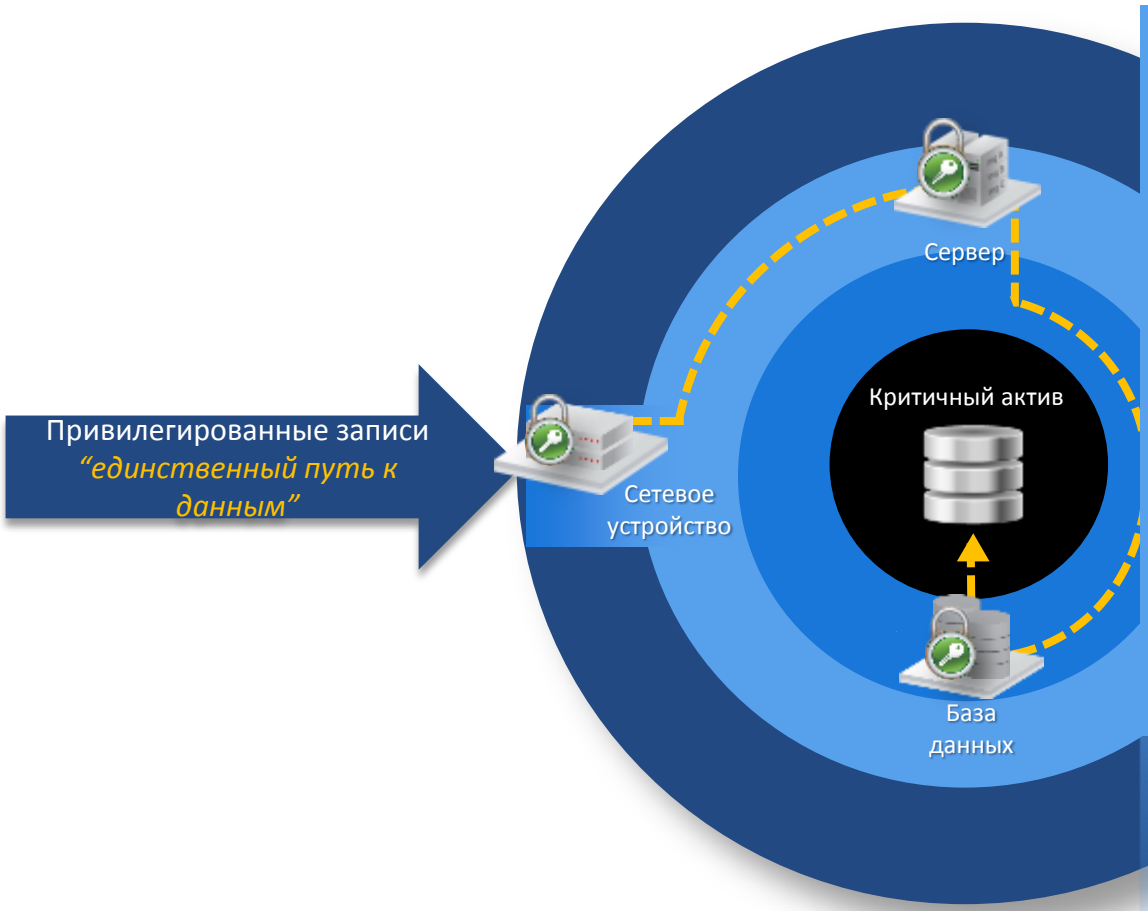
Регуляторы требуют контроль и мониторинг привилегированных аккаунтов

PCI Security Standards Council™

Sarbanes-Oxley
Financial and Accounting Disclosure Information

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

CYBERARK


Внутренние пользователи
Подрядчики
Сторонние разработчики
Провайдеры сервисов
Временные сотрудники
Системные интеграторы

CYBERARK

Вы должны знать!

Кто нарушитель?

Кто авторизован?

CYBERARK

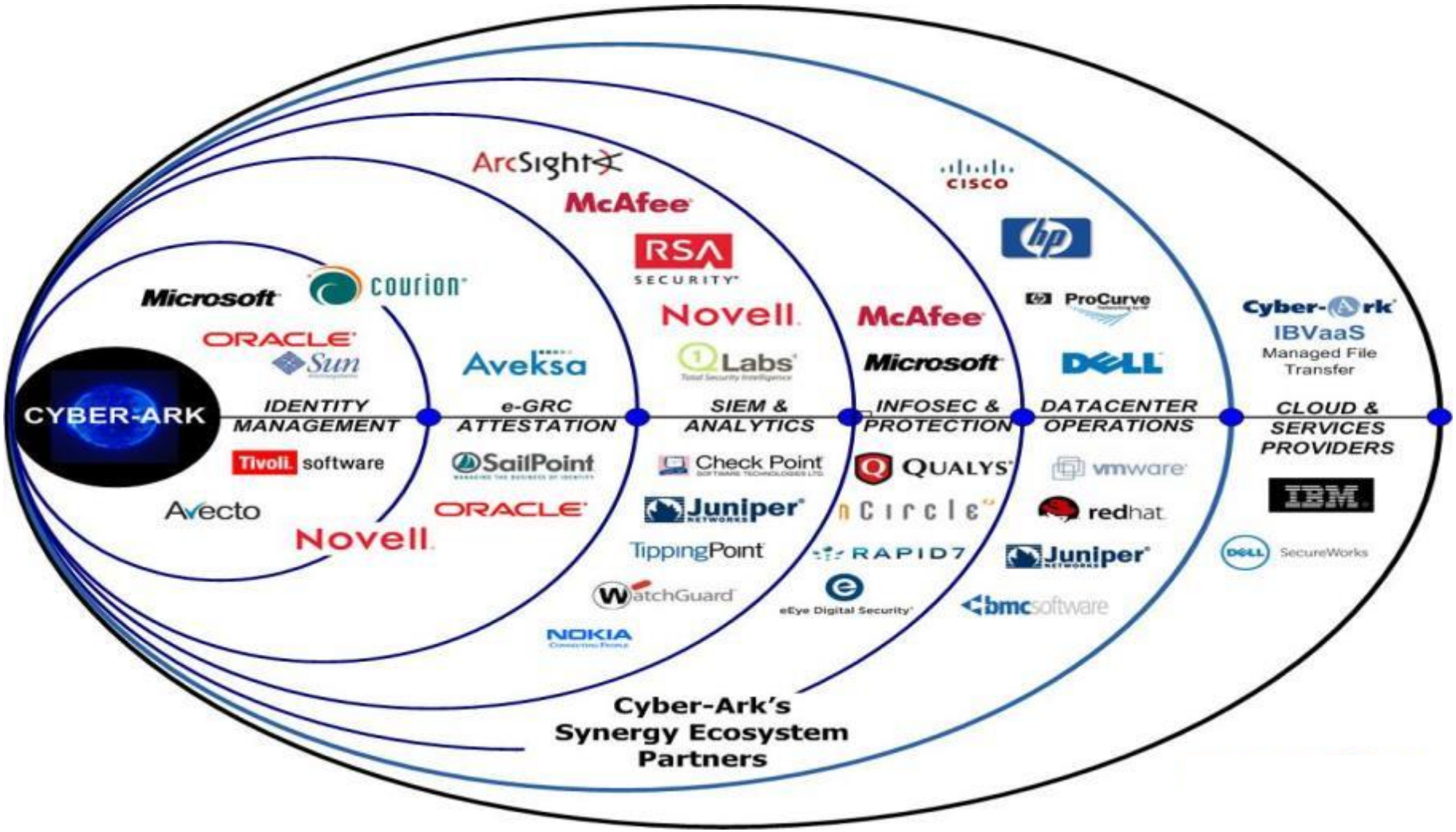
CYBERARK

Партнерство и альянсы

ЭЛВИС-ПЛЮС

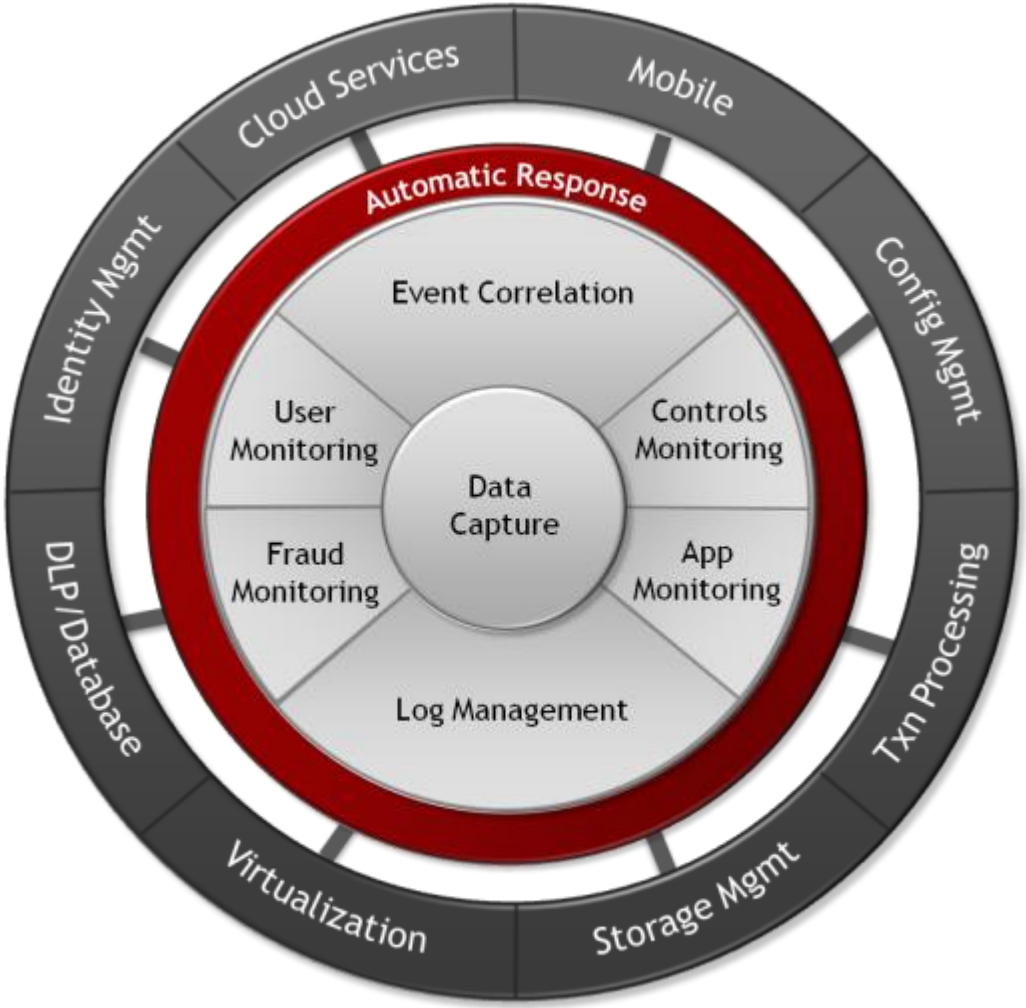
CYBERARK

CyberArk Alliance Ecosystem



CYBERARK

ArcSight in the IT Ecosystem



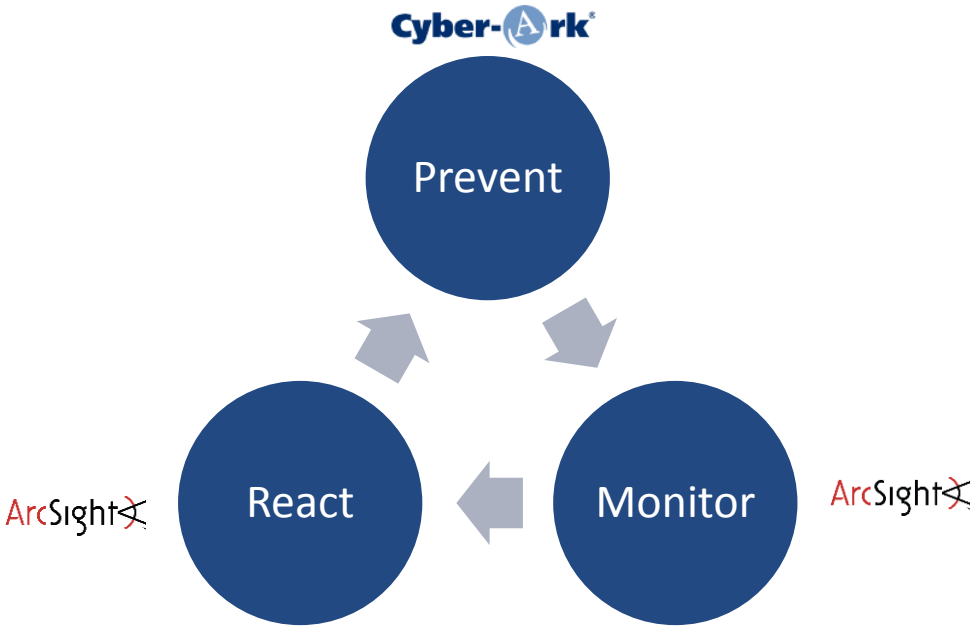
ArcSight Connects, Extends and Protects Critical Infrastructure:

- Data Leak Protection
- Mobility/device management
- Storage and backup
- Uptime/availability
- Identity lifecycle
- Cloud/virtualization
- Config/systems management
- Endpoint/patch management

CYBERARK

Identity Lifecycle Management

- **Prevent:** Защита от НСД к привилегированным аккаунтам
- **Monitor:** Detect risky privileged account access when it occurs
- **React**: Investigate, understand, and fix problems quickly



CYBERARK

McAfee SIA & Cyber-Ark: Alliance Update

CyberArk first PIM vendor to provide true integration with ePO

- Brings “Current State PIM Analysis” to the ePO console
- Allows monitoring of privileged account use from within ePO
- Creates instant value for joint Customers
- ePO integration module in Beta; available for testing
- “Real Time” Remediation possible *(via Cyber-Ark SDK)*

McAfee® COMPATIBLE

Multiple McAfee integrations

- ePO
- SIEM
- Vulnerability Management

CYBERARK

Что мы рекомендуем предпринять любому бизнесу

4 обязательных шага для противодействия

1. Обнаруживать все привилегированные записи

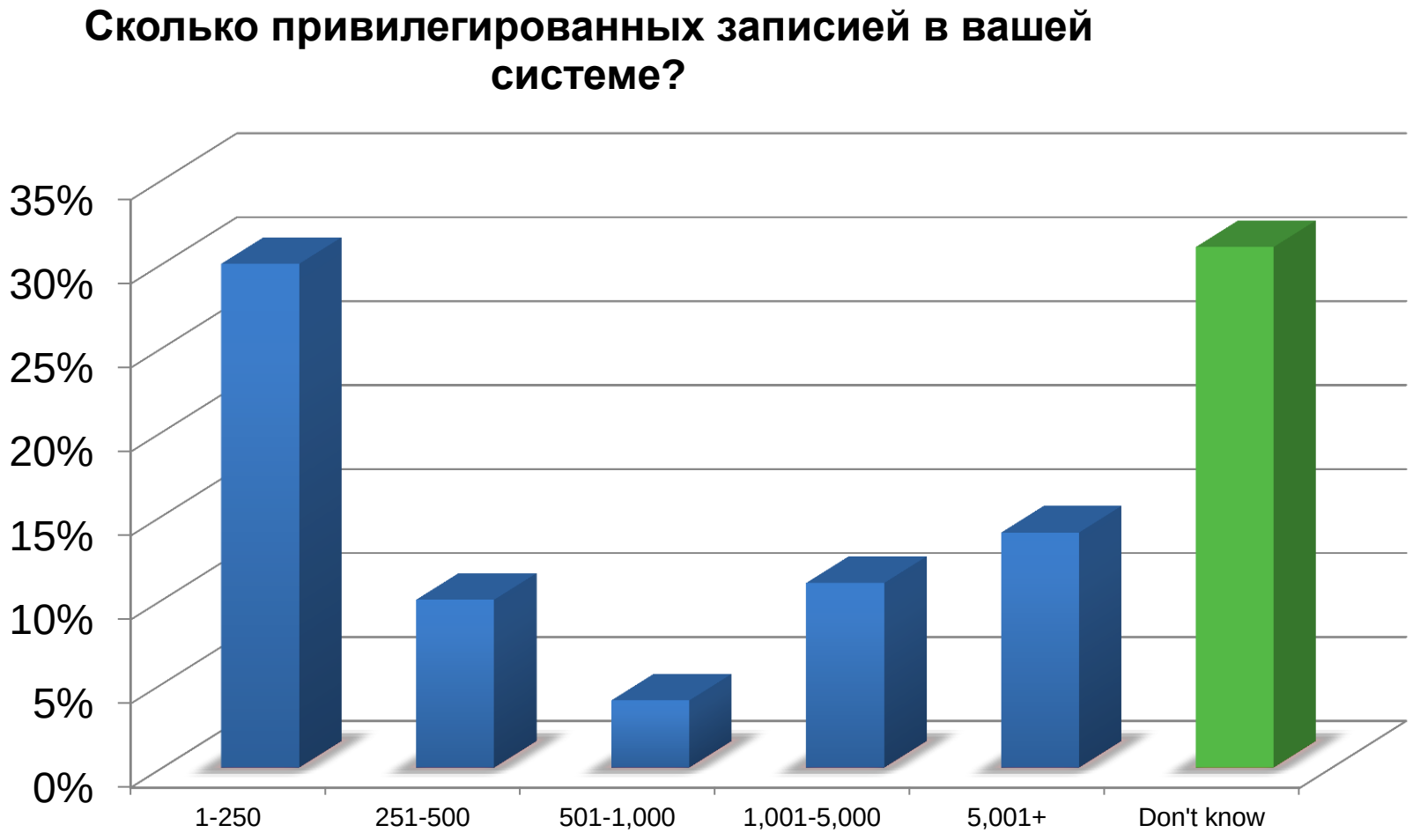
2. Защищать и управлять привилегированными аккаунтами

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

4. Расследовать использование привилегированных записей в реальном времени

CYBERARK®

Но этот факт не понятен...



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

CYBERARK®

Обнаружить все привилегированные записи

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

CYBERARK

Защищать и управлять привилегированными аккаунтами

Проактивная оборона

- Поиск и изучение привилегированных записей
- Автоматическая смена паролей
- Сложные, длинные имена и пароли
- Пароли хранятся в высокозащищенном хранилище

CYBERARK®

CYBERARK

Обзор решений

Богдан Тоболь
Директор по продажам

Типичная атака

- Подготовка атаки - несколько месяцев
- Началась с **одного компьютера**
- Правдоподобное письмо: распорядок дня, круг общения и список мероприятий
- Модуль сбора информации: внутренние адреса серверов, имена пользователей и пароли
- Хищение данных - вручную
- Присутствие в системе не обнаруживалось антивирусами в **течении нескольких месяцев**

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

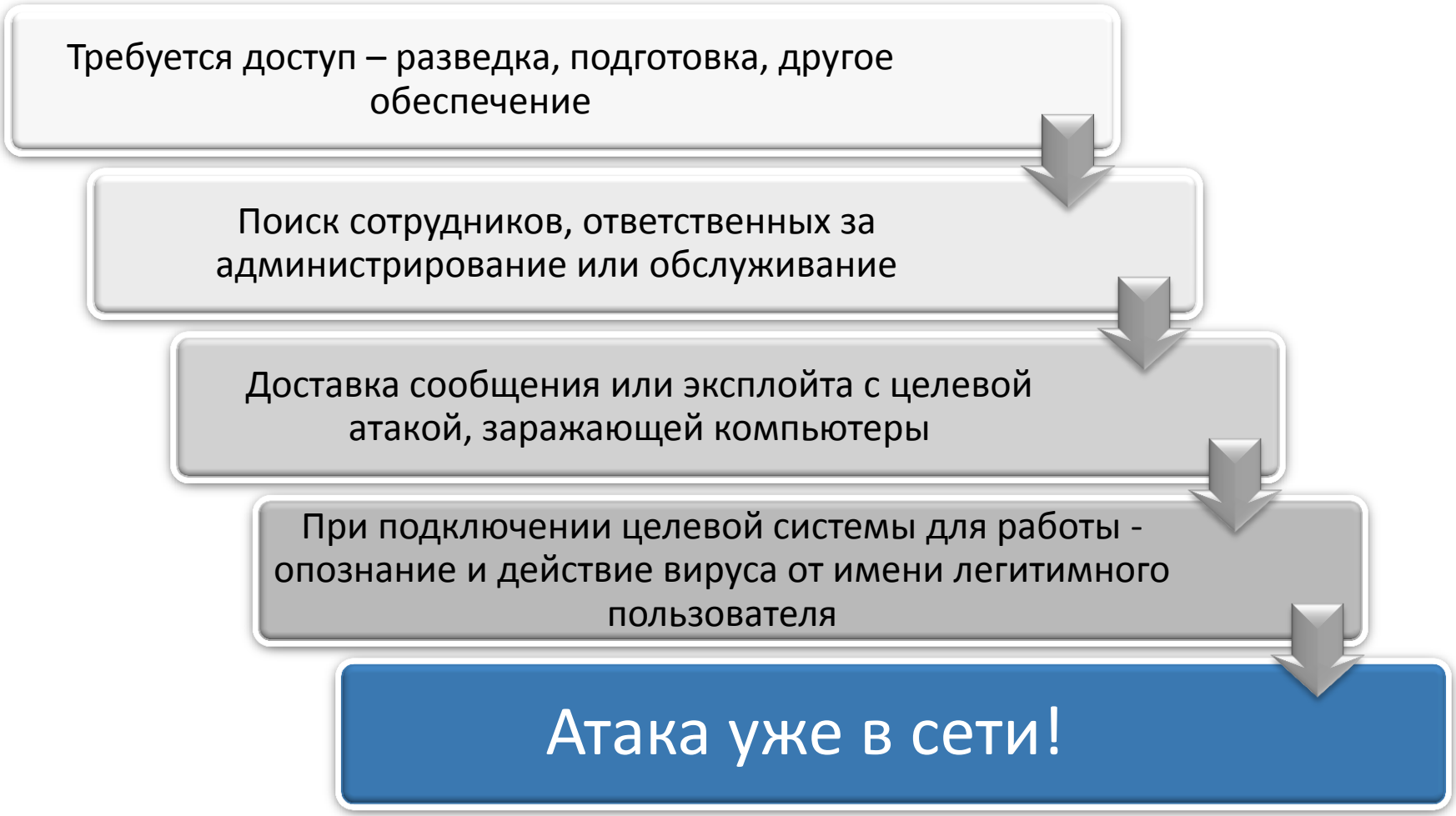
100%

Вторжений использовали украденные УЗ

Mandiant, 2013

CYBERARK

Атаки с помощью социальных сетей



CYBERARK

CYBERARK

Продукты

Решаем проблемы привилегированных УЗ

Целевые атаки (APT/AET)

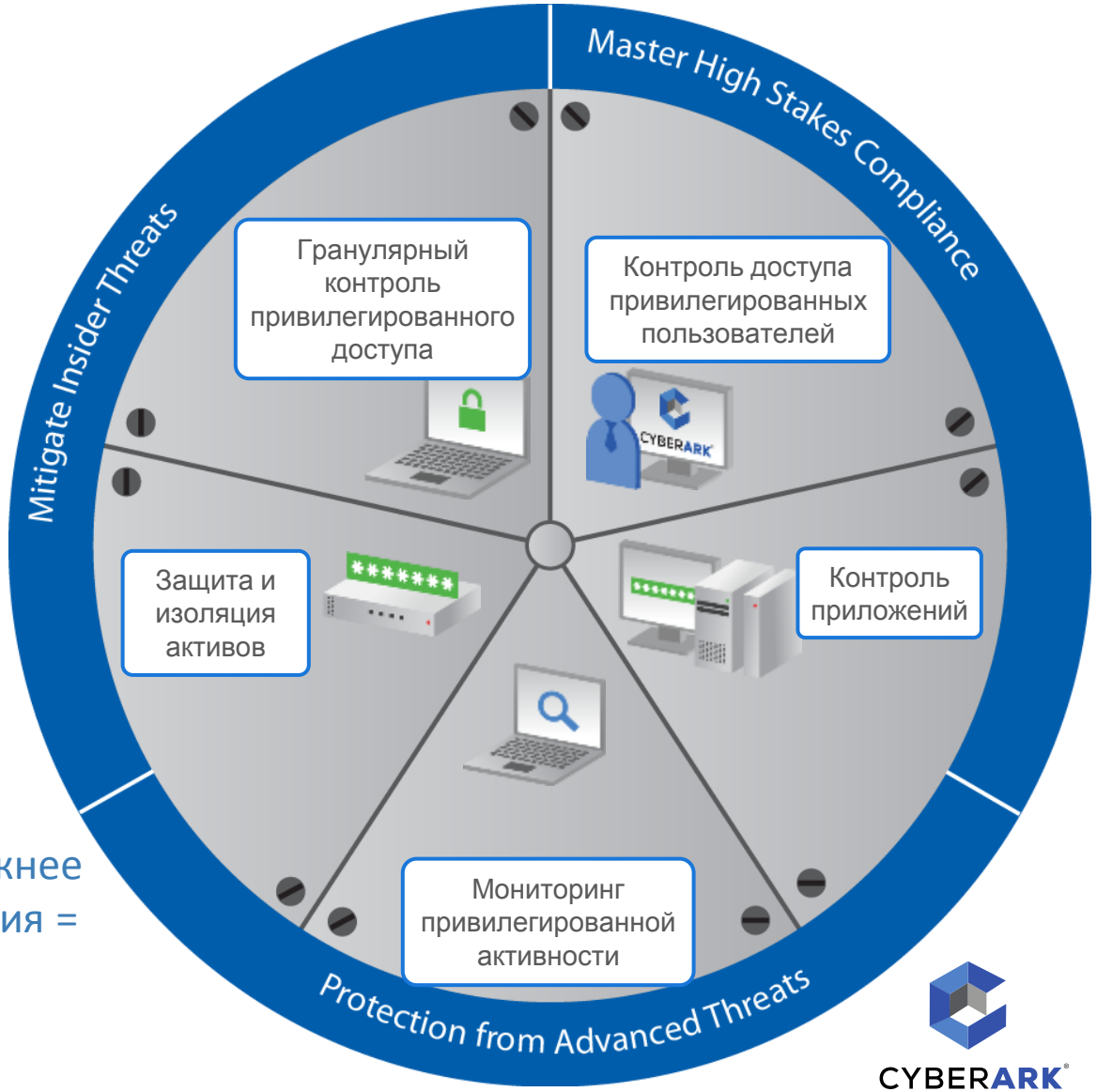
Спланированные, сложные
На наиболее ценные активы
Привилегированные аккаунты

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

Принципы решений CyberArk

Доверие администратору – не панацея.

Администратор CyberArk не имеет доступа к информации, которую защищает.

Контролируемые аккаунты не могут быть использованы злоумышленниками.

Без внесения изменений в ИТ-инфраструктуру

CyberArk не заменяет другие СЗИ, а эффективно дополняет их.

CYBERARK®

Решения CyberArk - защита в действии

Хост администратора	Хранилище	Целевая система	Сессия подключения
Пароли не попадают к пользователю	Защищенное хранилище	Замена паролей по умолчанию	Интеграция с системами отслеживания
Ограничение действий администрат.	Безопасный протокол	Смена паролей автоматом	Двойной контроль и др. процессы
	Интеграция с SIEM	Изоляция привилегиров. доступа	Мониторинг в реальном времени
	Полноценный аудит		Прекращение подозрительных сессий

Эксплойт подлинной сессии для вредоносных действий

CYBERARK

Безопасность привилегированных записей

Внешние поставщики

IT службы

Аудиторы

Разработчики и DBA

PIM Portal/Web Access

Enterprise Password Vault®

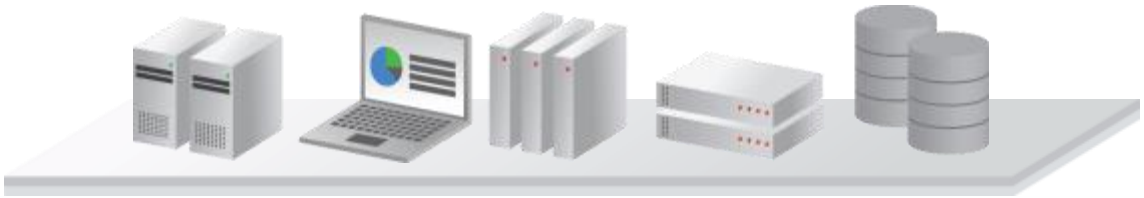
Privileged Session Manager®

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®

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

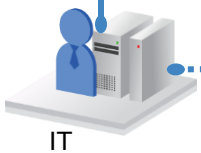
CYBERARK

Master Policy

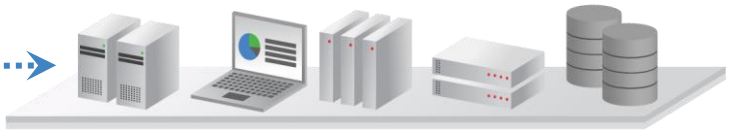
Policy

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



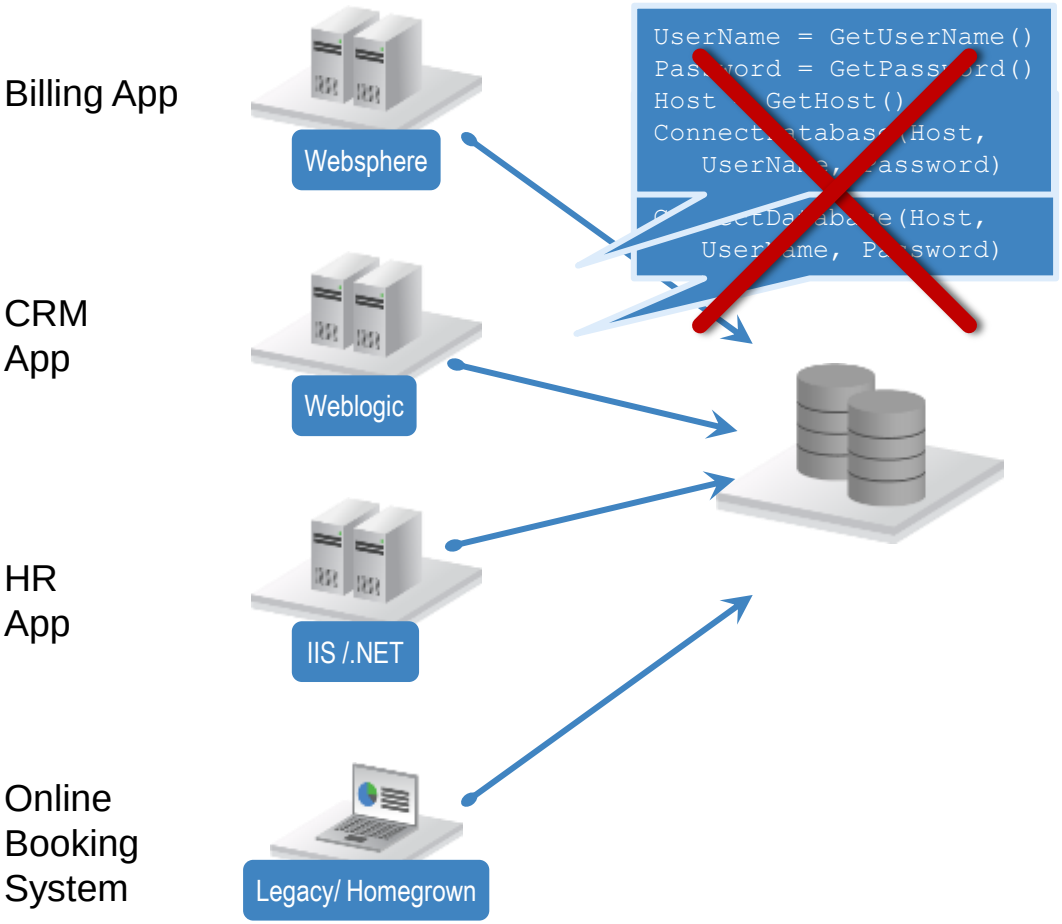
Enterprise IT Environment

Auditors

Request to view Reports

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

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

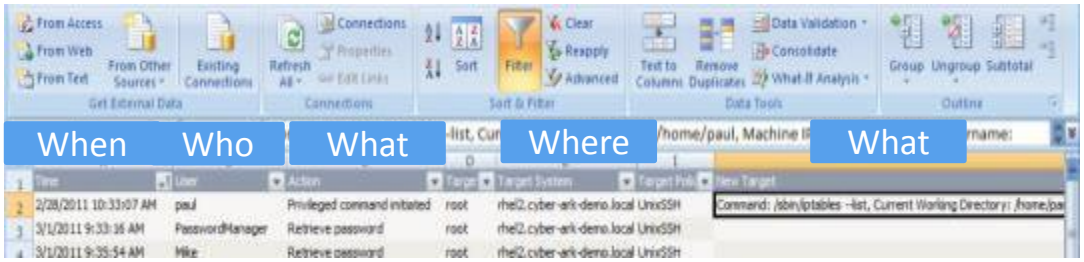
ORACLE

QUALYS

McAfee

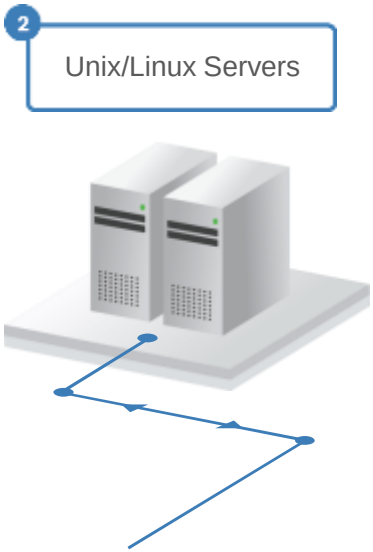
CYBERARK

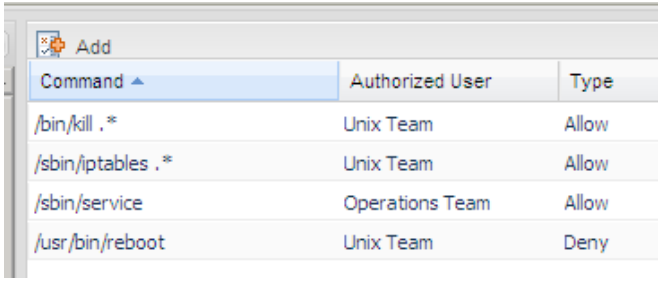
On-demand Privileges Manager (OPM) for Unix



Мониторинг и аудит, отчеты и запись текстовых команд

Контроль суперпользователя



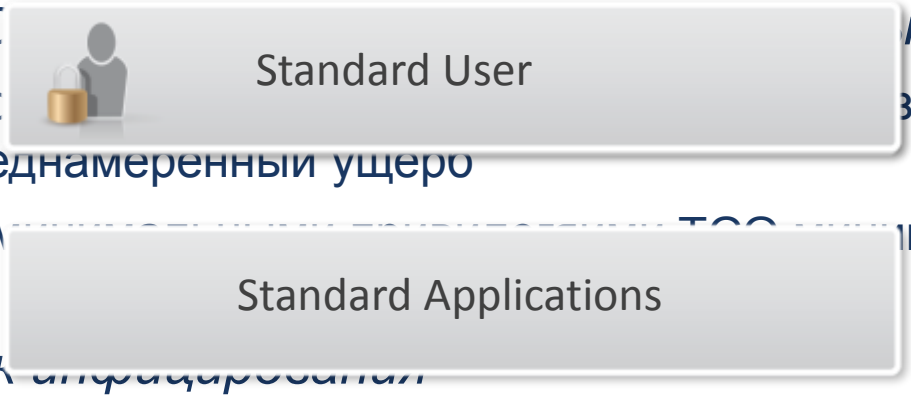


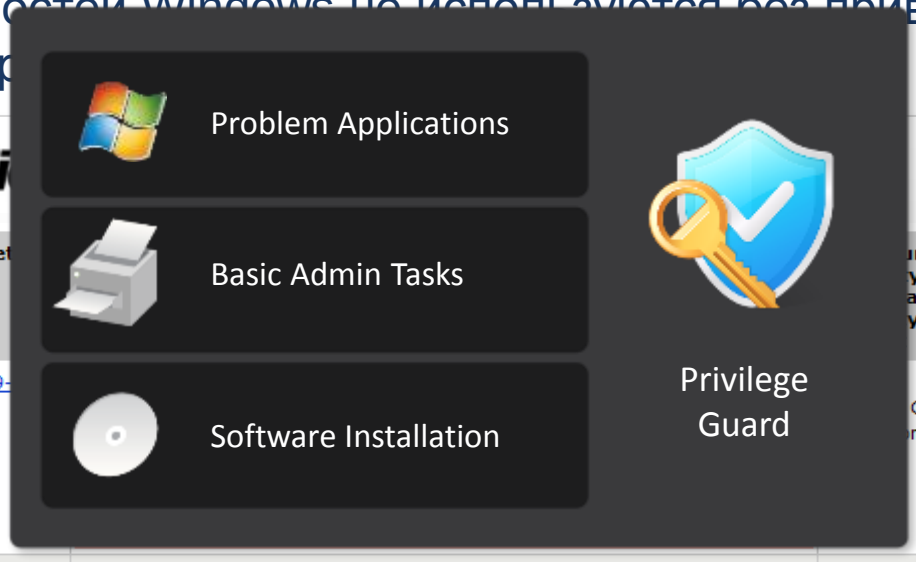
Гранулярный контроль доступа и политик

CYBERARK

OPM for Windows

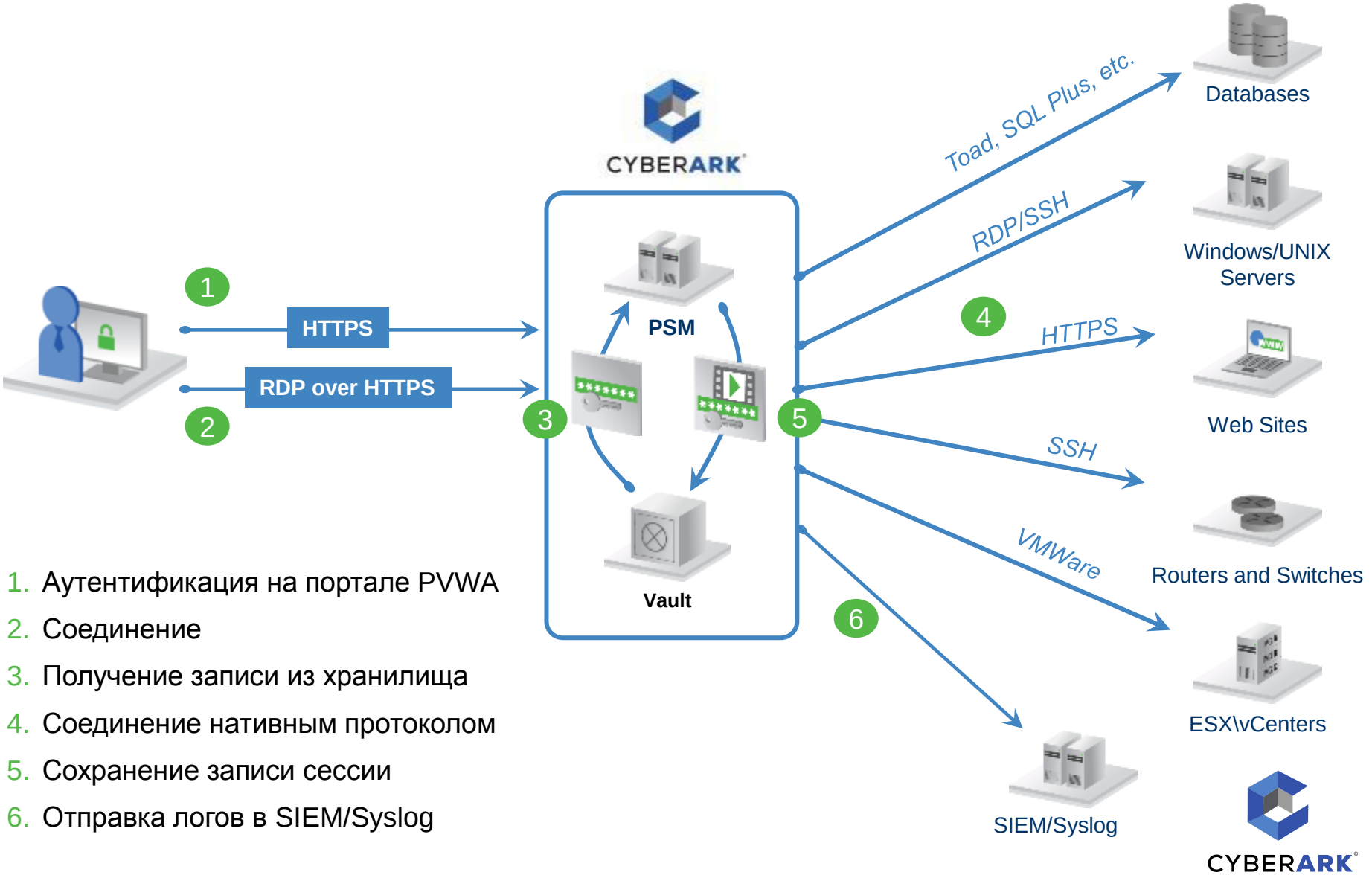
- *Снижает ТСО*
  - Минимум пр
  - Gartner: “С м
- *Снижает риск*
  - **90%** уязвимостей Windows не используются без привилегий admin
    Исключая пр





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

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

CYBERARK®

Network Devices

- Cisco
- Juniper
- Nortel
- Alcatel
- Quntum
- F5

Security Appliances

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

Directories and Credential Storage

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

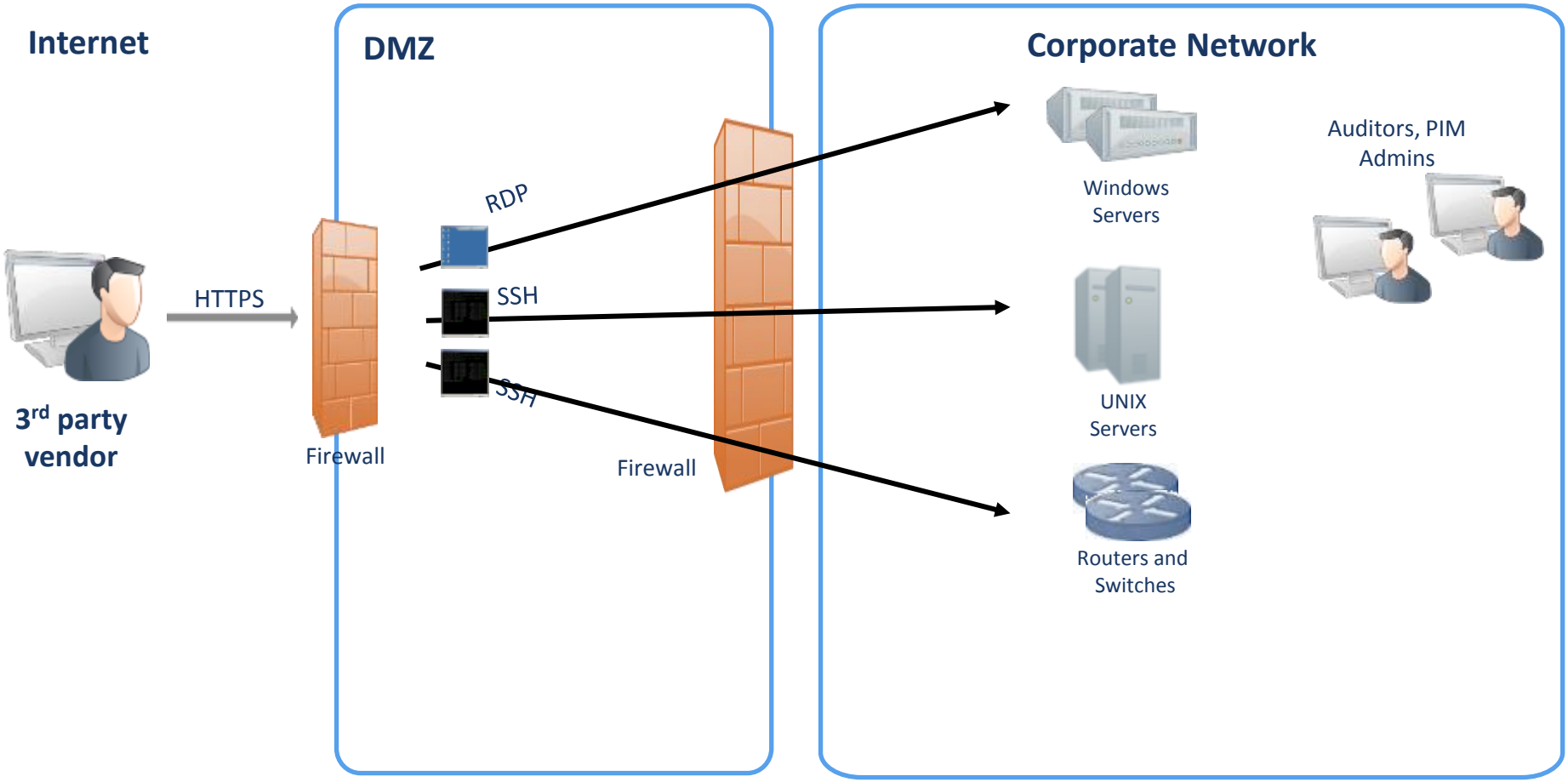
Remote Control and Monitoring

- 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

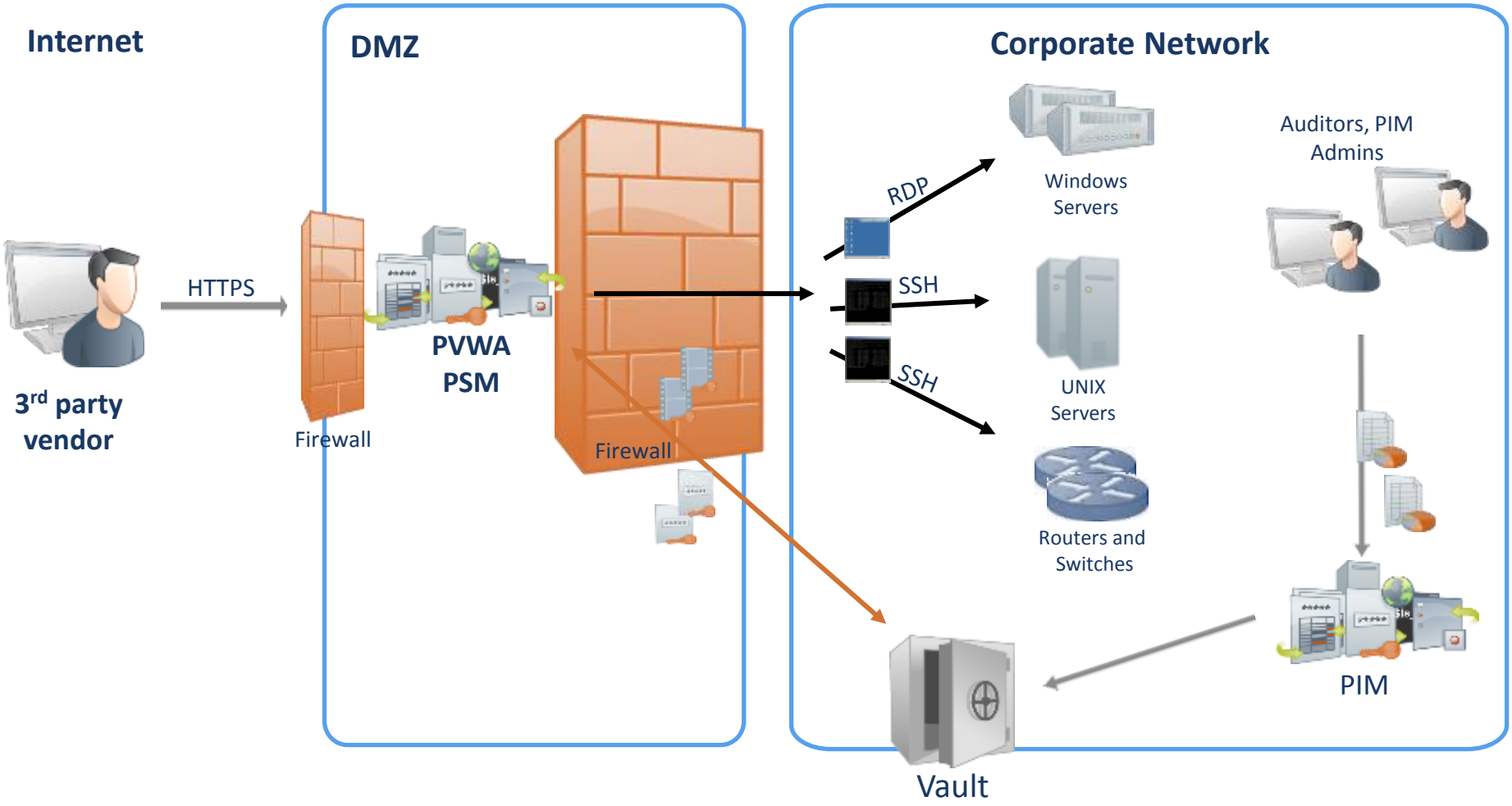
CYBERARK®

Традиционный удаленный доступ поставщика



CYBERARK

PSM контролируемый удаленный доступ поставщика



CYBERARK

PIM&PSM – всесторонняя безопасность БД

- Защита БД – контроль привилегированного доступа и активности

DB sys и общие DBA аккаунты

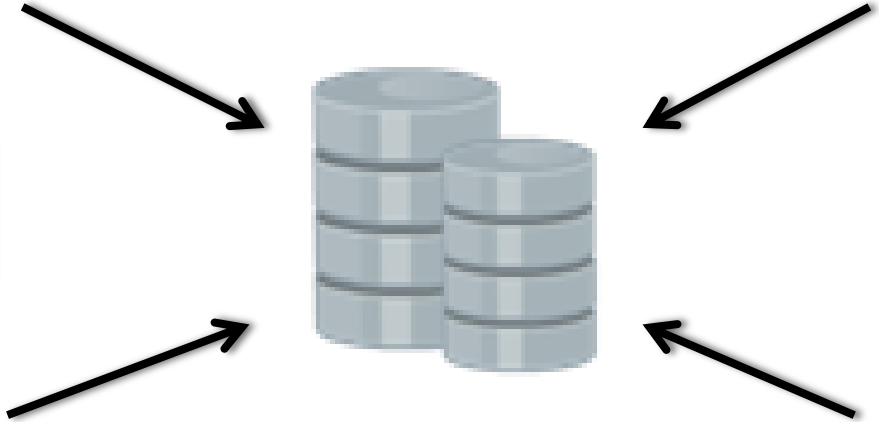
- Контроль защищенности, доступа и активности
- Автоматическое управление и замена аккаунтов

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

Безопасность виртуальных сред с единого центра управления

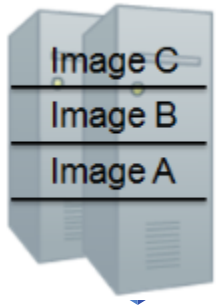
Единые политики и аудит привиегированных аккаунтов в виртуальных средах

PIM

- Автоопределение ESX серверов и всех имиджей
- Контроль доступа к гипервизорам, vCenter и готевым машинам
- Персонализованный доступ и отслеживание использования
- Применение политик безопасности по управлению учетными записями
- Управление изменениями процедурами утверждения

PSM

- Не остаются следы на гипервизоре
- Мониторинг VM admin и гостевых машин посредством DVR записи
- Контроль доступа к сессиям и процессы утверждения
- Строгая аутентификация к гипервизору
- Привилегированный SSO



CYBERARK

CyberArk: 4 шага противодействия

1. Автоматически обнаруживает привилегированные записи

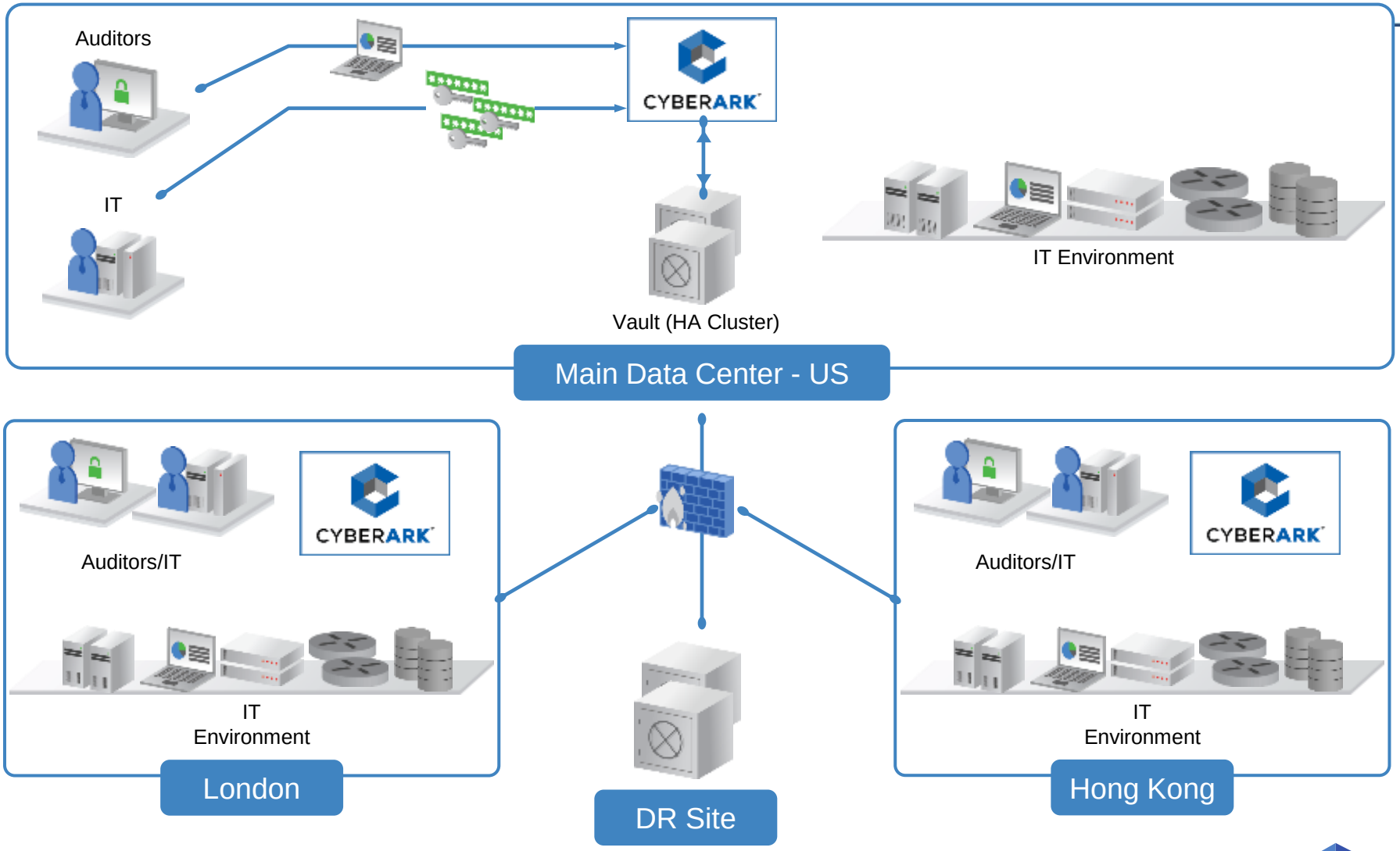
2. Защищает и управляет привилегированными аккаунтами

3. Контролирует, изолирует и отслеживает привилегированный доступ к АСО, серверам, БД и виртуальным платформам

4. Позволяет расследовать использование привилегированных записей в реальном времени

CYBERARK®

Распределенная архитектура CyberArk



CYBERARK

SIM: Enterprise Ready – готовая интеграция

Redundancy	High Availability modules	Disaster Recovery modules	External Storage support	Encrypted Backup integration		
Protocols	Vault Protocol	FTP	FTP over SSL/TLS	SFTP / SSH	HTTP/S	SCP
Authentications	Username / Password	RSA SecurID	Radius	PKI	Oracle SSO	LDAP
LDAP integration	Active Directory	Sun One	Novell	Oracle	Any LDAP server	
SIEM and Monitor	ArcSight	RSA Envision	CA Unicenter	IBM Tivoli	HP OpenView	
Content Filter and Encryption	WebSense	McAfee	TrendMicro	PGP integration	Generic Integration	
Backend Integration	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

Интеграция PIM с системами контроля уязвимостей

MAXPATROL

QUALYS
On Demand Security

nCircle

McAfee
Vulnerability Manager

CYBERARK

Интеграция PIM/PSM с SIEM-системами

ArcSight An HP Company

RSA SECURED

McAfee

CYBERARK

Спасибо за внимание…