



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®



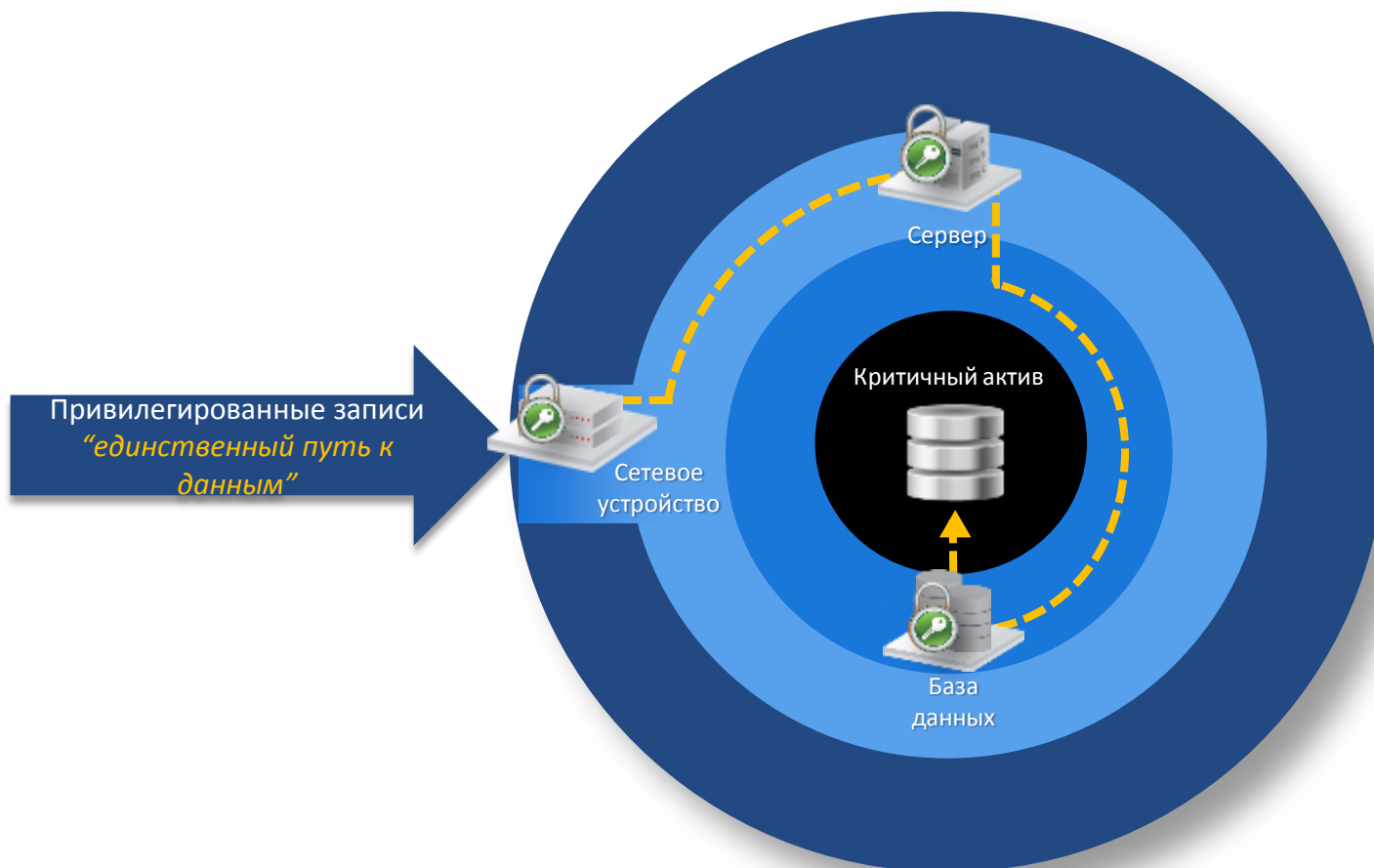
You Need to Know!

**Кто
нарушитель?**

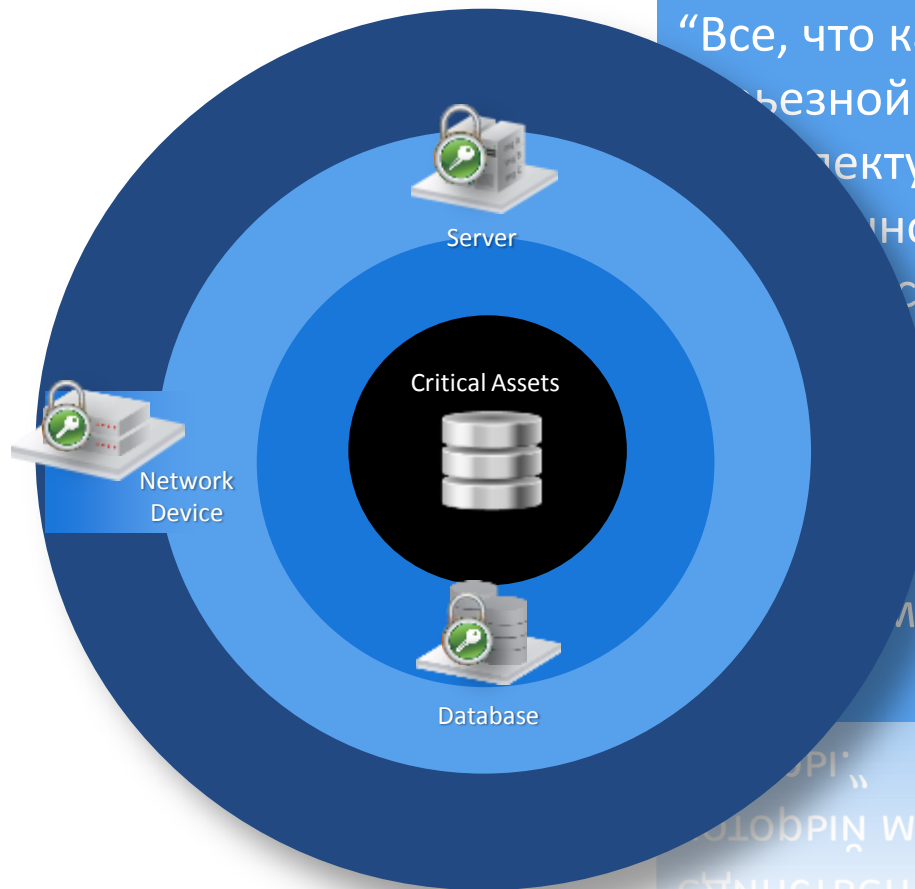
**Кто
авторизован?**



«Все пути ведут...» к привилегированным записям



Привилегированные записи – встроенные уязвимости (Gartner)



“Все, что касается
безной
интеллектуальной
ности,
ся в хорошо
ых системах, и
ованные
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

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 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 and Communications Technology (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, the attacks were seen as a warning of a potential larger-scale attack.

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 ADARIO STRANGE



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 Service (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 experts believe a company insider authorized the attack.

info security

STRATEGY /// INSIGHT /// TECHNIQUE

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



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
- Несколько месяцев присутствие в системе не обнаруживалось



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...”

392NC6N'''
94WNHNC1b91NBHPIX

SANS; Top 20 Security Controls, #12



Привилегированный аккаунт: что, где и почему

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



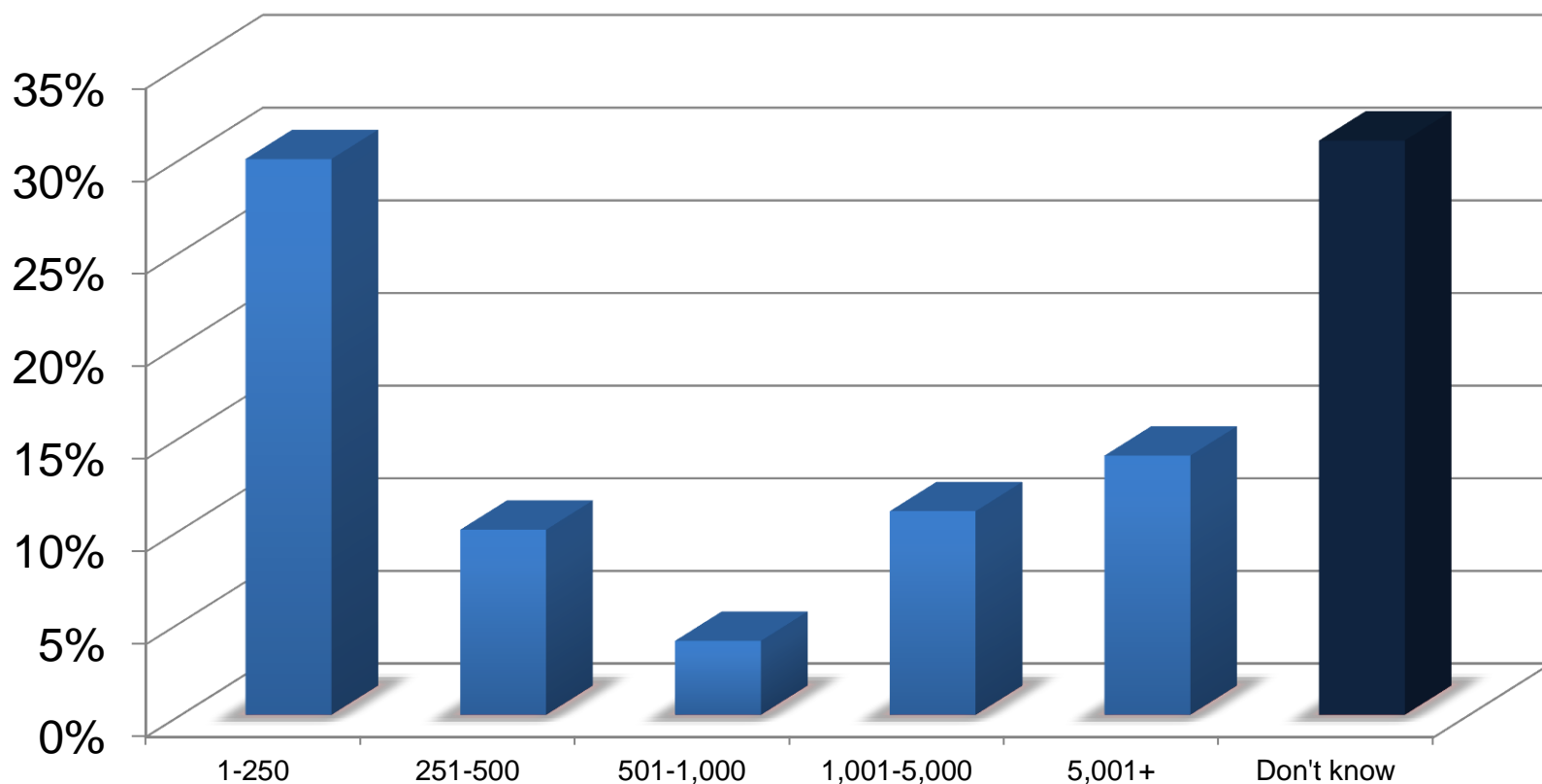
Привилегированные записи везде!



CYBERARK®

Но этот факт не понятен...

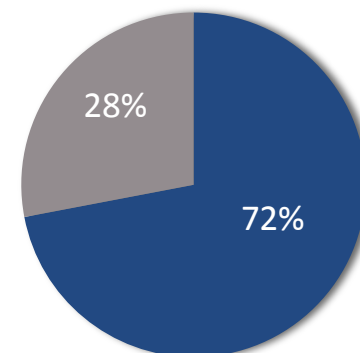
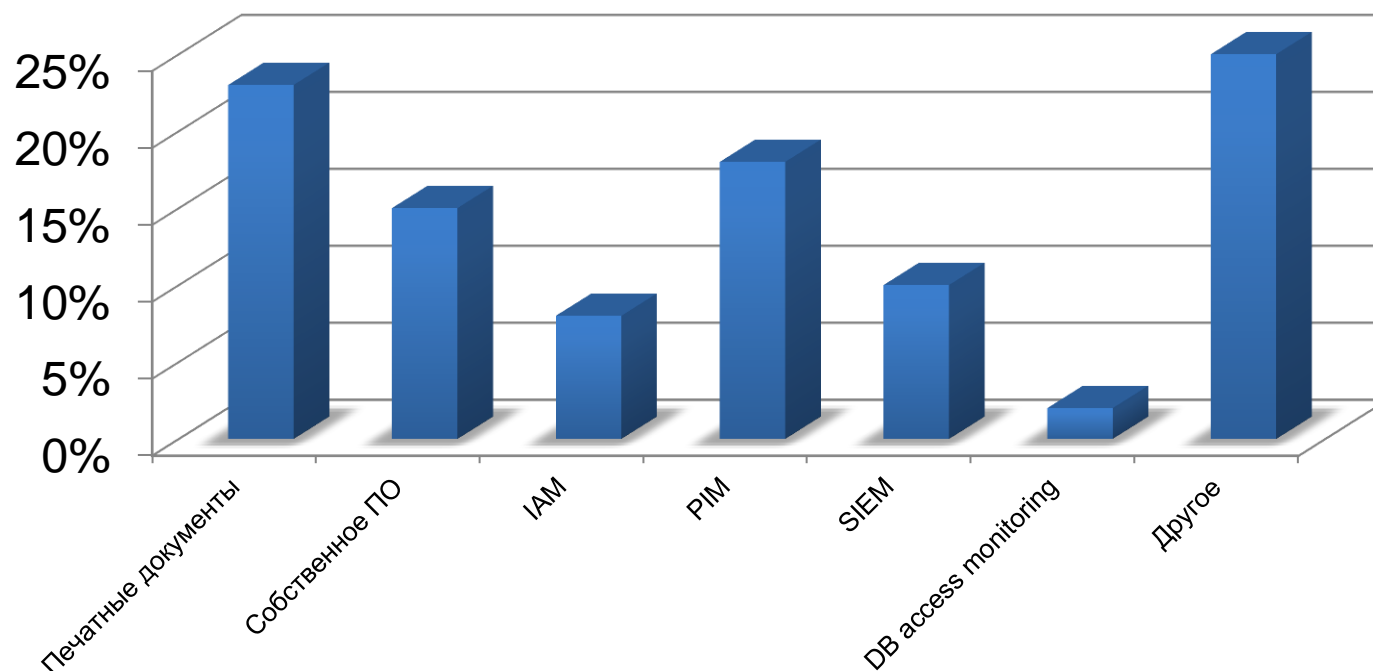
Сколько привилегированных записей в вашей системе?



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

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%

Жертв обновляли
антивирусы



94%

Вторжений были
замечены 3-ми
лицами



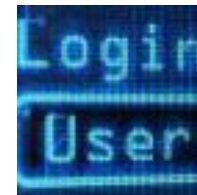
416

Дней (в среднем)
атака в сети не
замечена



100%

Вторжений
использовали
украденные УЗ



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



1. Обнаружить все привилегированные записи



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

2. Защищать и управлять записями



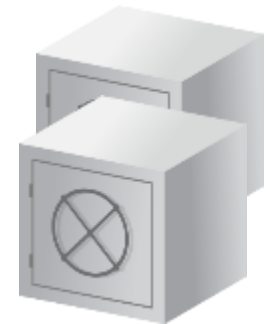
Убедитесь, что хранилище безопасно



Внедрите процедуры проверки доступа к привилегированным записям



Упростите управление политиками за счет унифицированных мастер-политик



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



Используйте расследование в реальном времени

Определяем атаку

Интегрируем с SIEM

Выполняем и индексируем запись



Безопасность привилегированных записей



Внешние поставщики



IT службы



Аудиторы



Разработчики и DBA

PIM Portal/Web Access

Identity
Management

Enterprise
Password
Vault®

Privileged
Session
Manager®

Application
Identity
Manager™

On-Demand
Privileges
Manager™

Ticketing
Systems

Monitoring & SIEM
Applications

Master Policy

Enterprise
Directory and More

Secure Digital Vault™

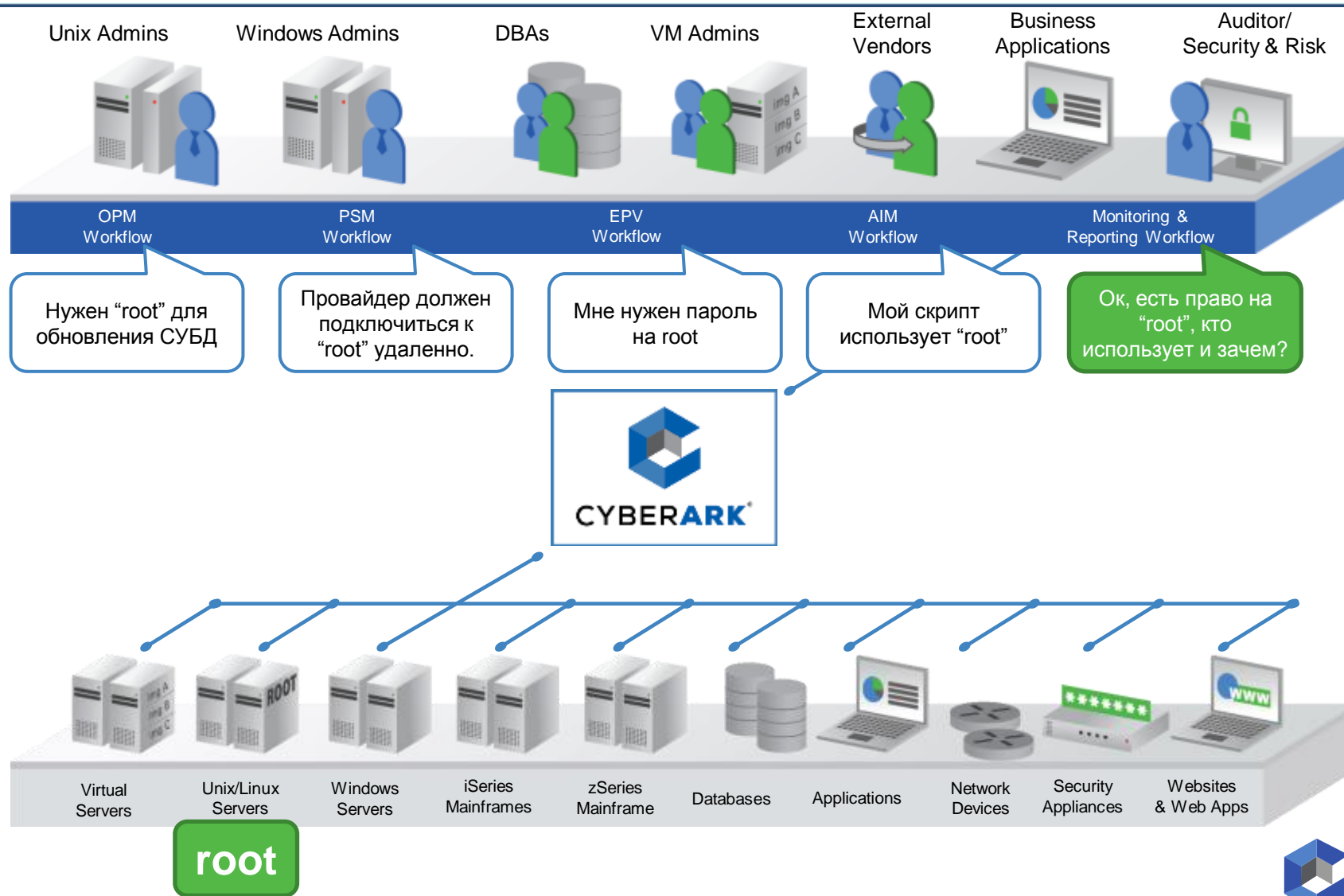


Любое устройство, ЦОД –
Традиционные и облачные, хостинг

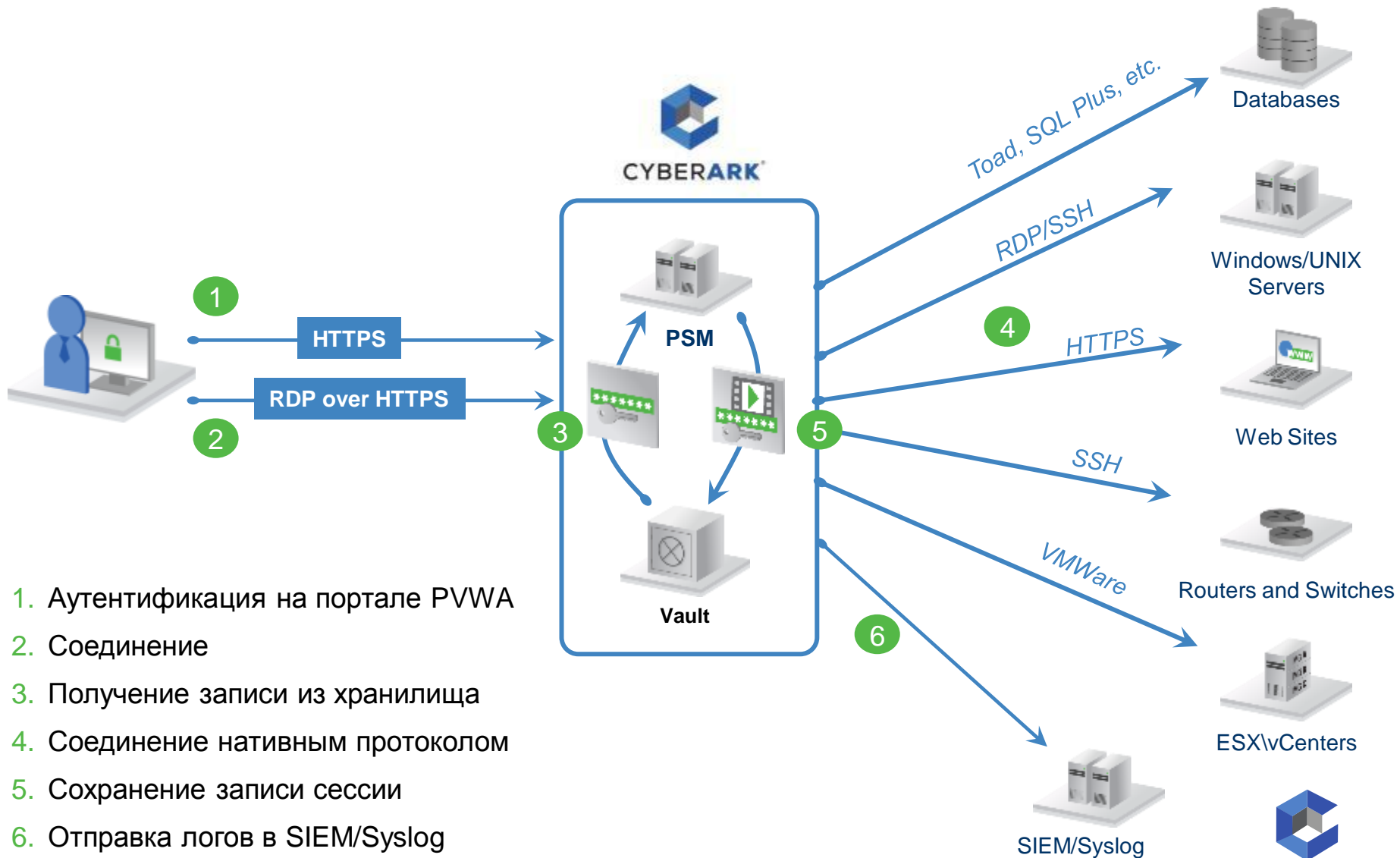


CYBERARK®

Пример: управление привилегированными записями



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

Запрограммируемые,
встроенные аккаунты

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

Сторонние
приложения

ORACLE®

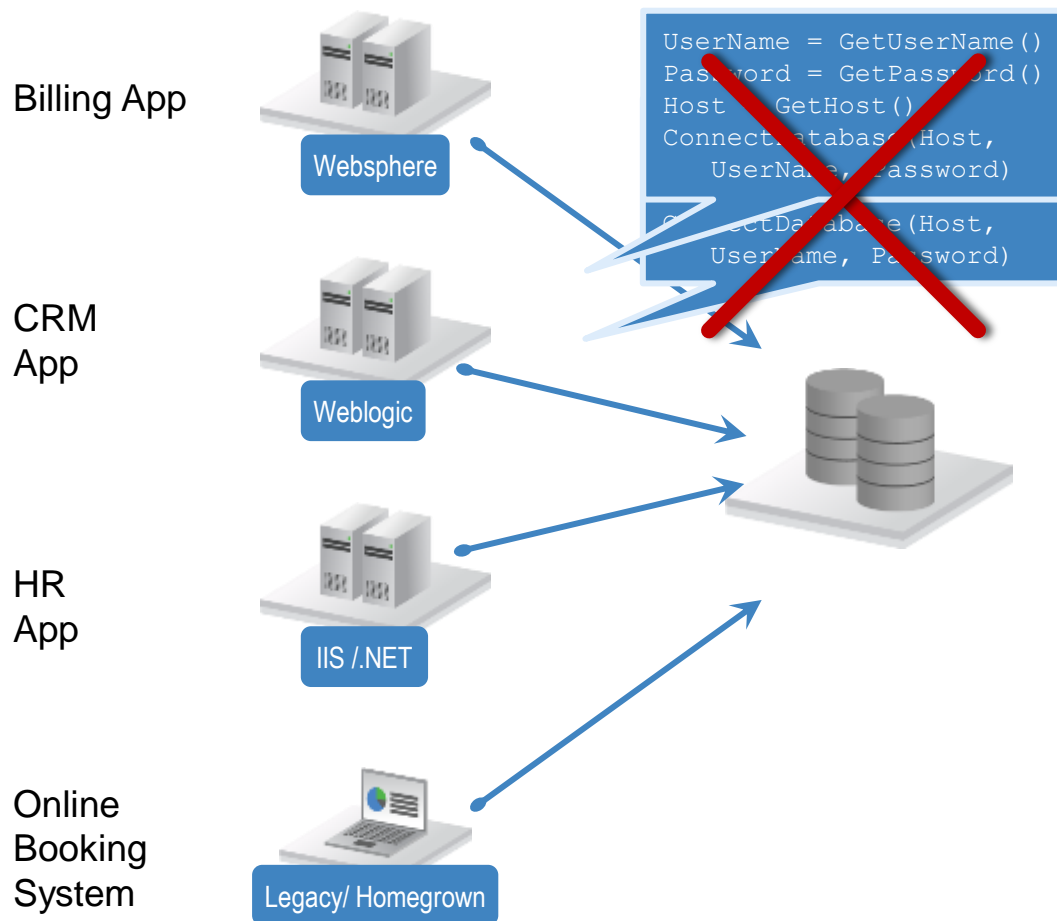


McAfee®



CYBERARK®

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

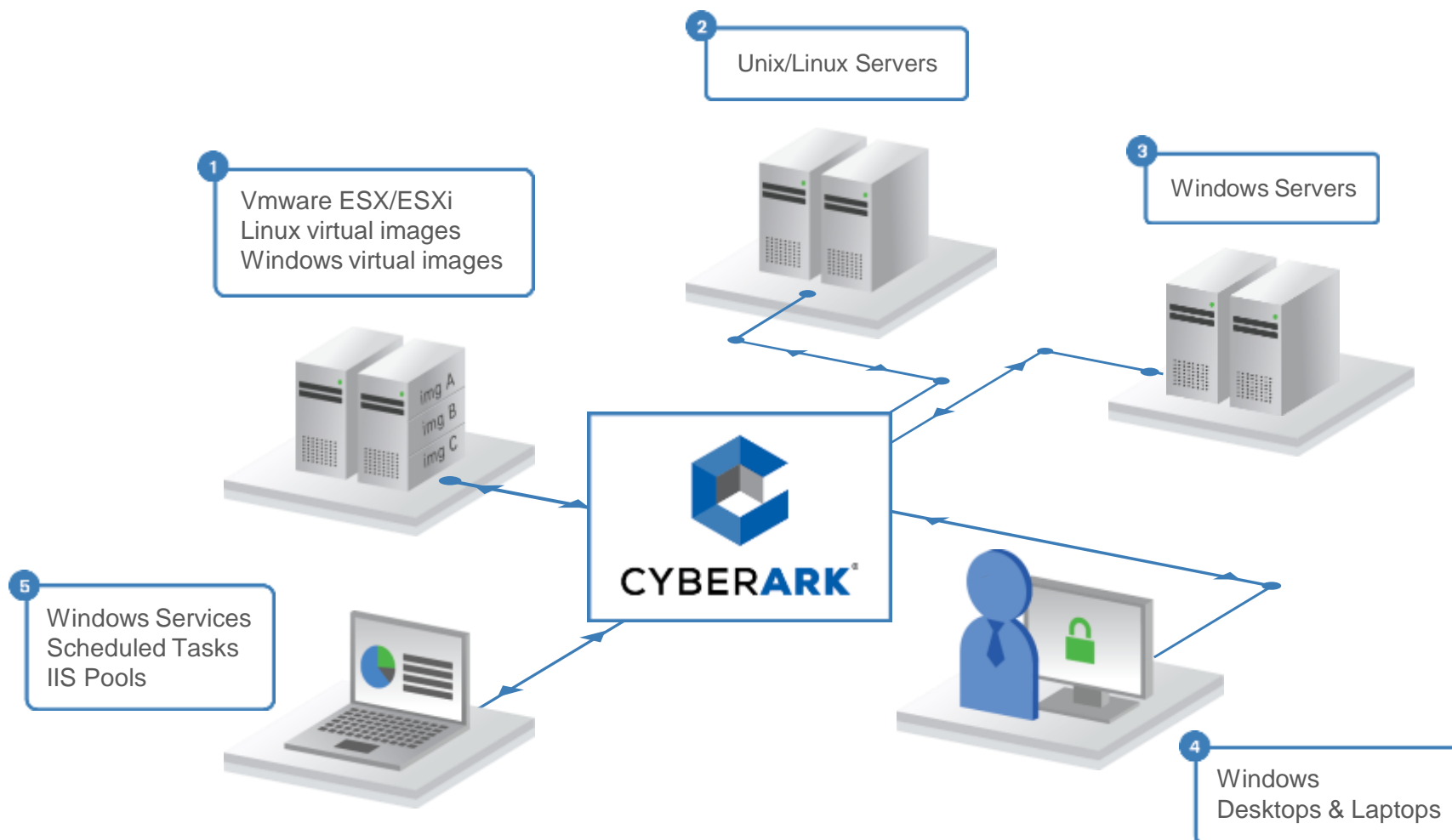


- Защищает и сбрасывает учетную запись приложения без простоя и рестарта
- Безопасно кэширует для непрерывности бизнеса и высокой производительности
- Исключает изменение кода и затраты на изменения паролей или адресов машин
- Строгая аутентификация по:
 - Адресу машины
 - Пользователю OS
 - Адресу приложения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

Защищает, управляет и устраняет встроенные привилегированные аккаунты из приложений

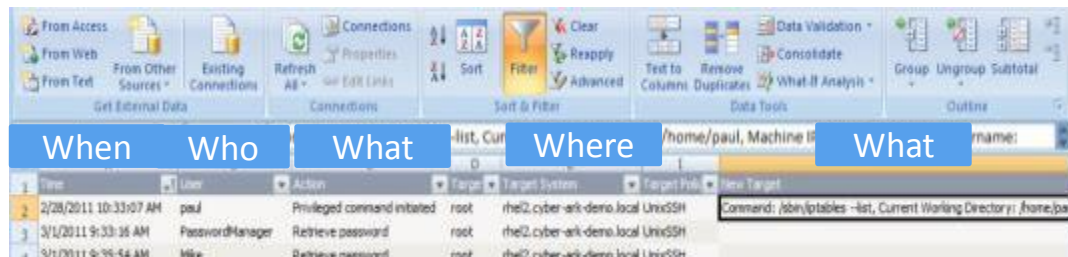


EPV: автоматическое определение привилегированных аккаунтов всей системы



Где привилегированные записи и суперпользователи?

On-demand Privileges Manager (OPM) for Unix



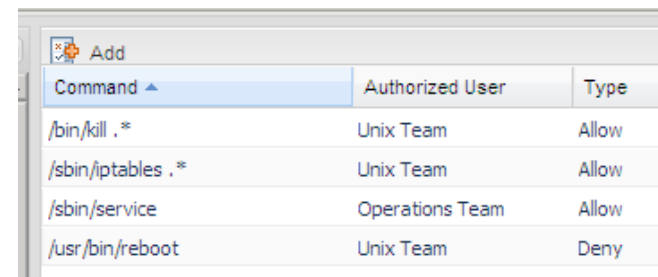
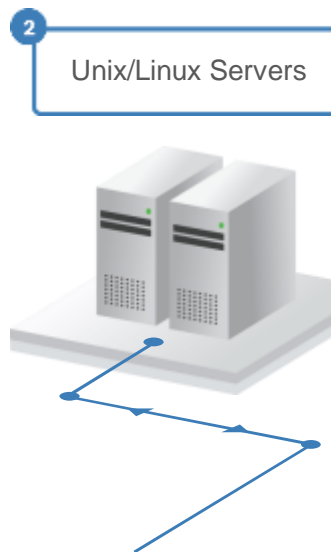
The screenshot shows the OPM interface with a toolbar at the top containing various data manipulation tools like 'From Access', 'From Web', 'From Text', 'Connections', 'Refresh', 'Sort', 'Filter', 'Clear', 'Reapply', 'Advanced', 'Data Validation', 'Consolidate', 'What-If Analysis', 'Group', 'Ungroup', and 'Subtotal'. Below the toolbar is a table with columns: 'When', 'Who', 'What', 'Where', and 'What'. The table contains three rows of log entries.

When	Who	What	Where	What
2/28/2011 10:33:07 AM	paul	Privileged command initiated	root	Command: /sbin/iptables -list, Current Working Directory: /home/paul
3/1/2011 9:33:36 AM	PasswordManager	Retrieve password	root	
3/1/2011 9:35:54 AM	Mike	Retrieve password	root	

Мониторинг и аудит, отчеты и запись текстовых команд



Контроль суперпользователя



The screenshot shows a table with columns: 'Command', 'Authorized User', and 'Type'. It lists four commands with their authorized users and permissions.

Command	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

OPM for Windows

- *Снижает TCO*
 - Минимум привилегий для пользователей IT, вызвонок в ИТ, ниже “непреднамеренный ущерб”
 - Gartner: “С м TCO минимум на 20% ниже”
- *Снижает риск эксплуатации*
 - 90% уязвимостей Windows не используются без привилегий admin
 - Исключая пр

The diagram illustrates the security model of Windows. At the top, a grey box labeled 'Standard User' contains an icon of a person with a padlock. Below it, another grey box labeled 'Standard Applications' contains an icon of a document. In the foreground, a dark grey window titled 'Privilege Guard' is open. It features a blue shield icon with a gold key and a checkmark. Inside the window, there are three buttons: 'Problem Applications' (with a Windows logo icon), 'Basic Admin Tasks' (with a printer icon), and 'Software Installation' (with a CD icon). In the background, a table is partially visible with columns for 'Restart Requirement' and 'Affected Software'.

Bullet ID	Restart Requirement	Affected Software
MS09-001	Requires restart	Microsoft Windows, Internet Explorer

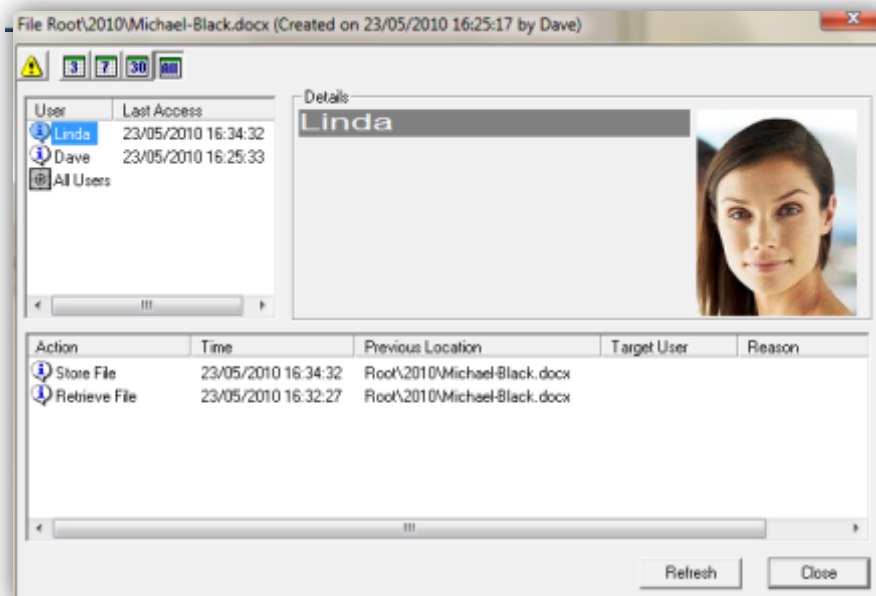


Обмен файлами бизнес-пользователей

- 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



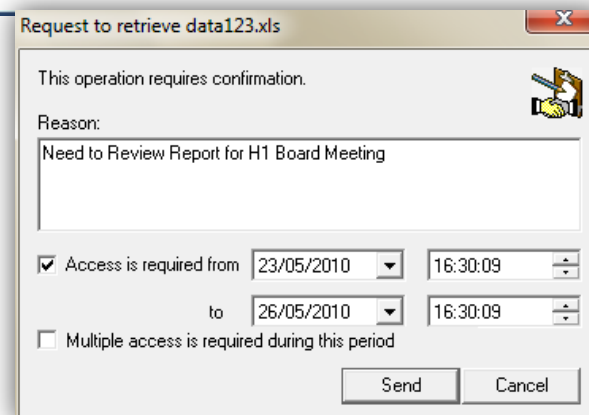
SIM – изоляция конфиденциальной информации



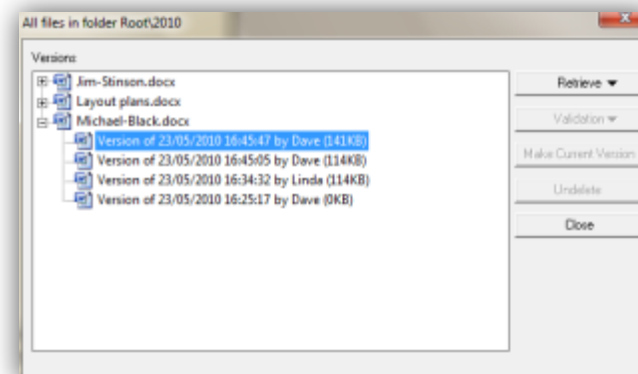
Зашифрованные архивы



Защищенная почта, уведомления
и детальные отчеты

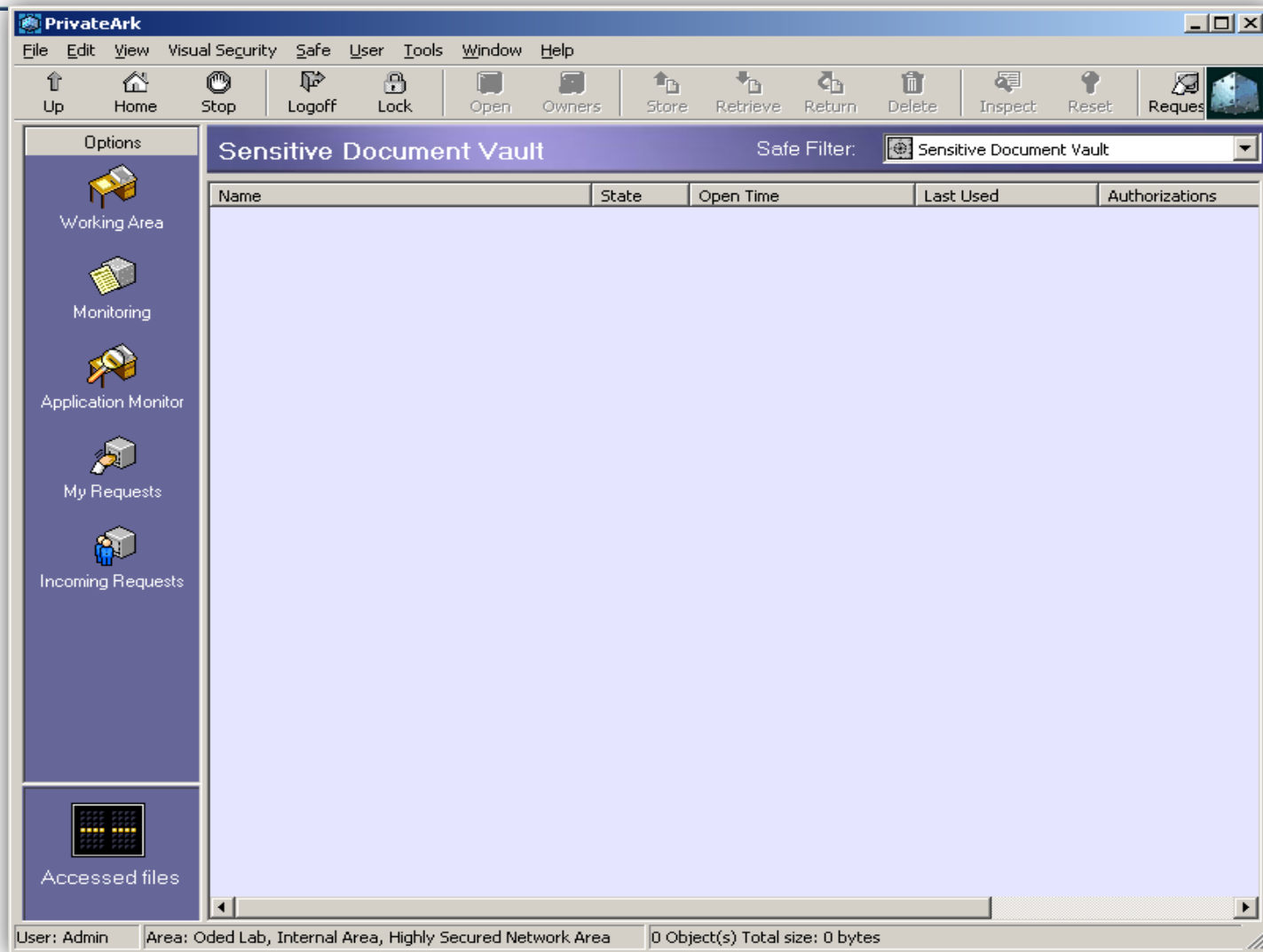


Двойной контроль



Версии

SIM – администратору нет доступа к данным



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

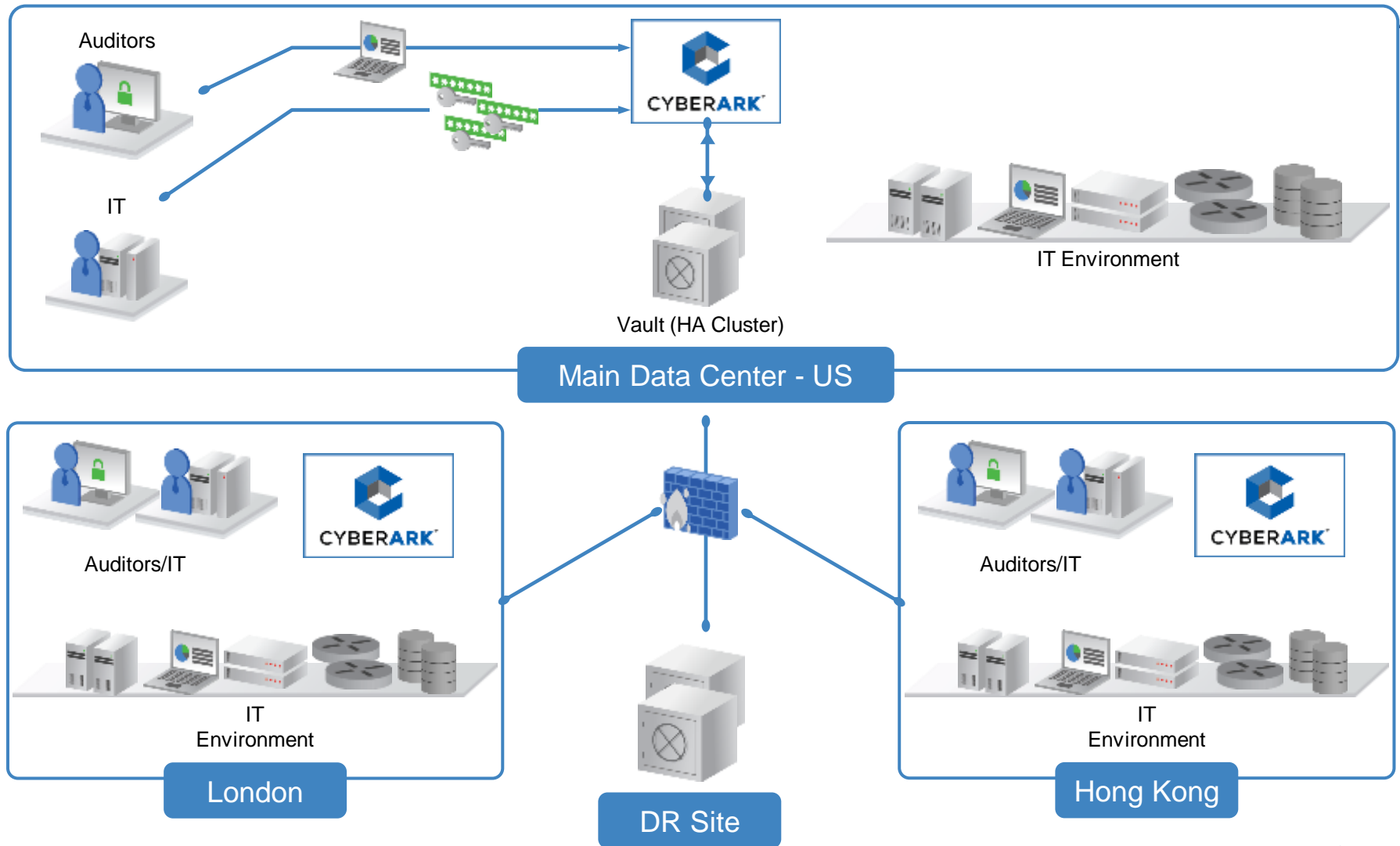


McAfee



CYBERARK®

Распределенная архитектура 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

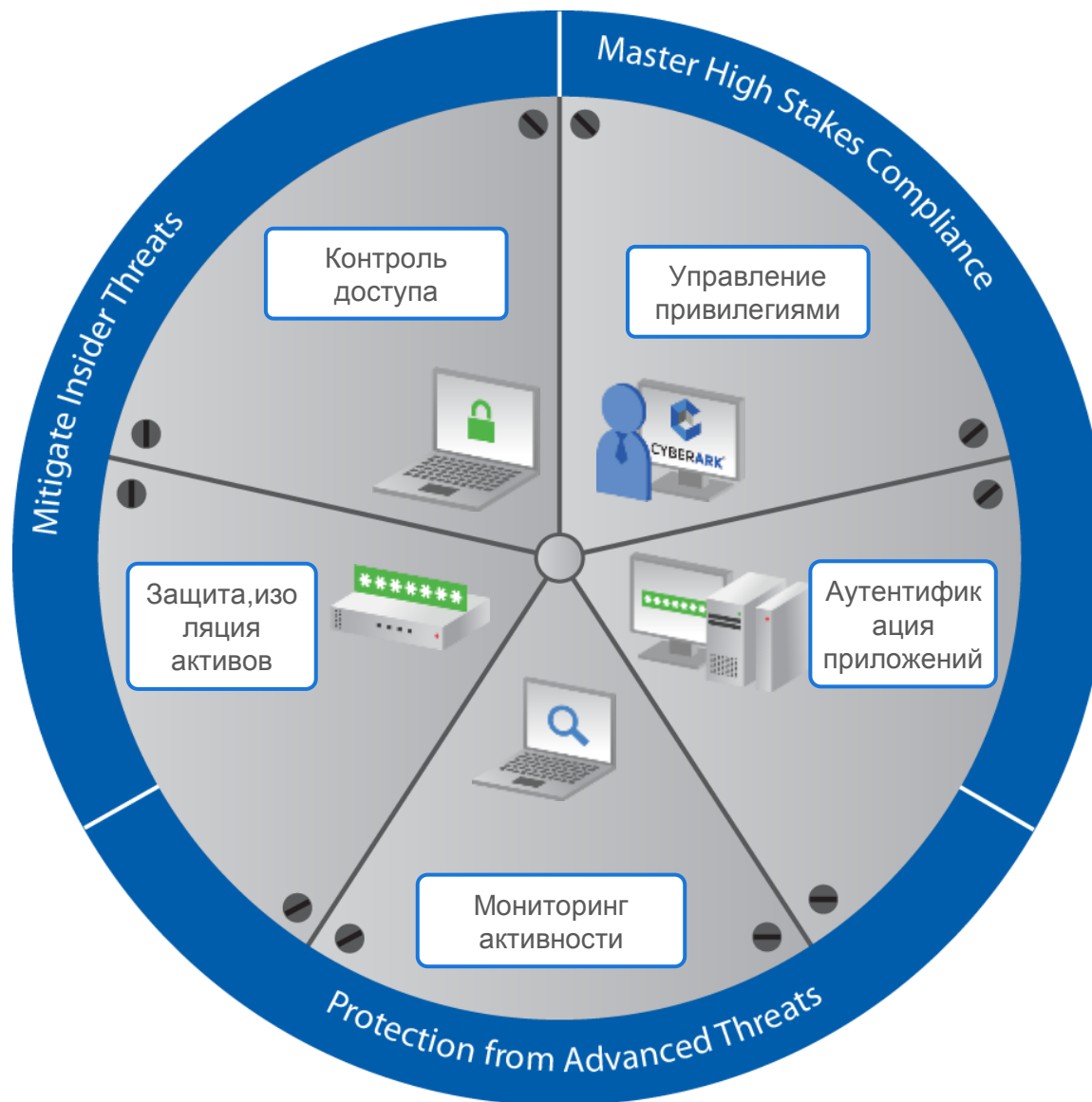
- Управление привилегиями Пользователей и отчетность
- Мониторинг и запись сессий
- Отчетность для соответствия
- Контроль удаленного доступа
- Аудируемый безопасный файлообмен

Промышленные системы/АСУ ТП

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



Решение CyberArk для безопасности



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

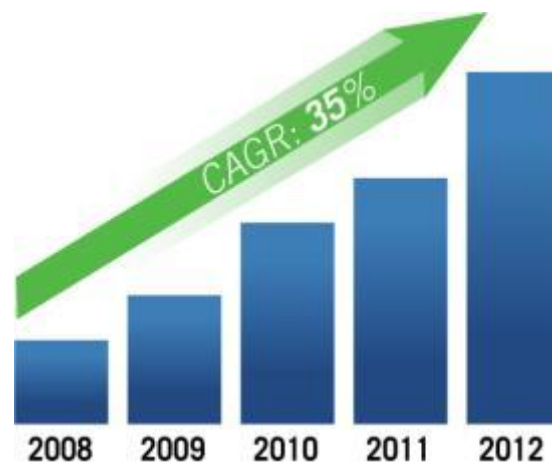
- Безопасность прозрачна для аудита



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



SOCIETE GENERALE GROUP



Retail, Transport, Telecom



Others



РОСНАНО



CYBERARK



CYBERARK

Спасибо за Ваше внимание и время