CYBERARK®

QuadroSoft
СОВРЕМЕННЫЕ ЭФФЕКТИВНЫЕ РЕШЕНИЯ

CYBERARK. PRIVILEGED ACCOUNT MANAGEMENT

• Программно-технические средства защиты

Пользователи

Средства защиты

CS&AV

BlueCoat

ORACLE Microsoft

Целевые системы

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

CYBERARK

QuadroSoft

Analyst review

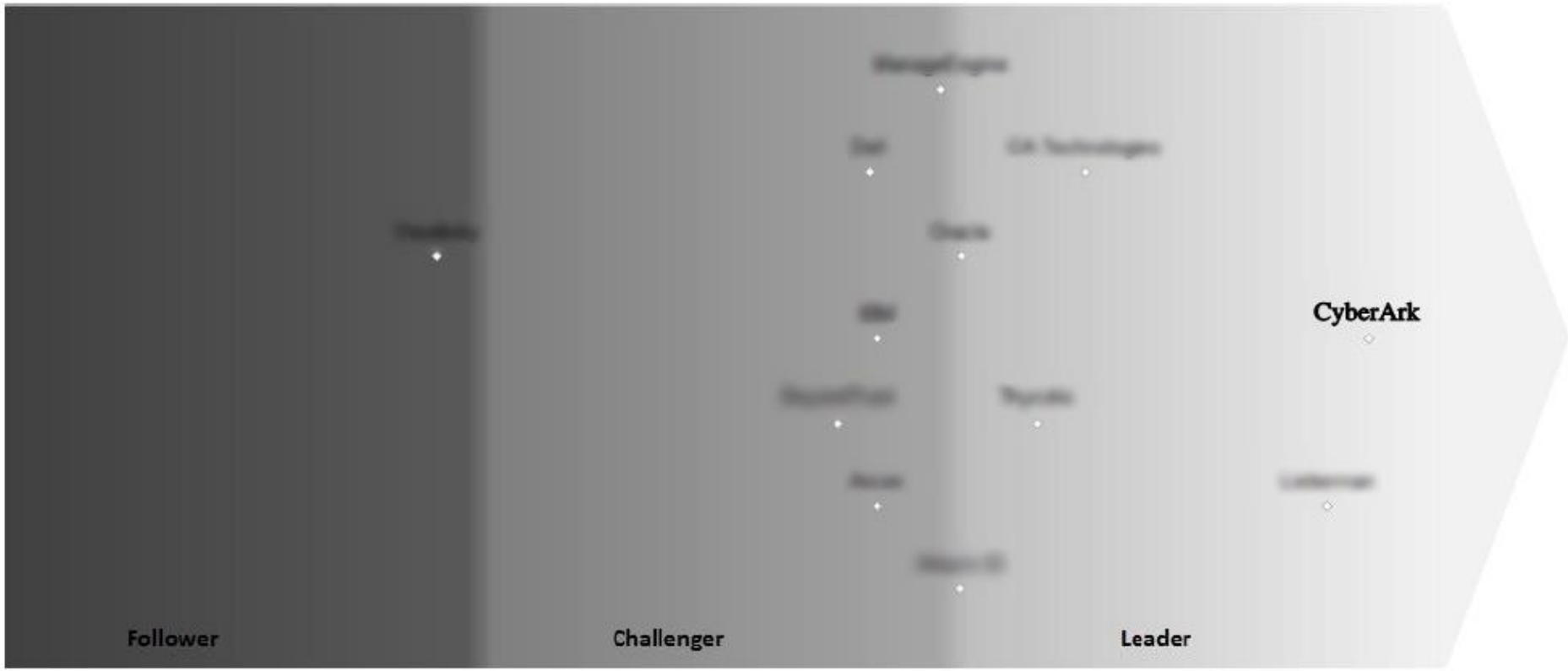


Fig. 1: The Overall Leadership rating for the Privilege Management market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.]

In this Leadership Compass CyberArk takes the Overall Leadership in Privilege Management.

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 • Cisco Enable • Local Administrators • ERP admin	• IT службы • Системные администраторы • DBA • Help Desk • Разработчики • Менеджер соц.медиа • Администраторы баз данных	• 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

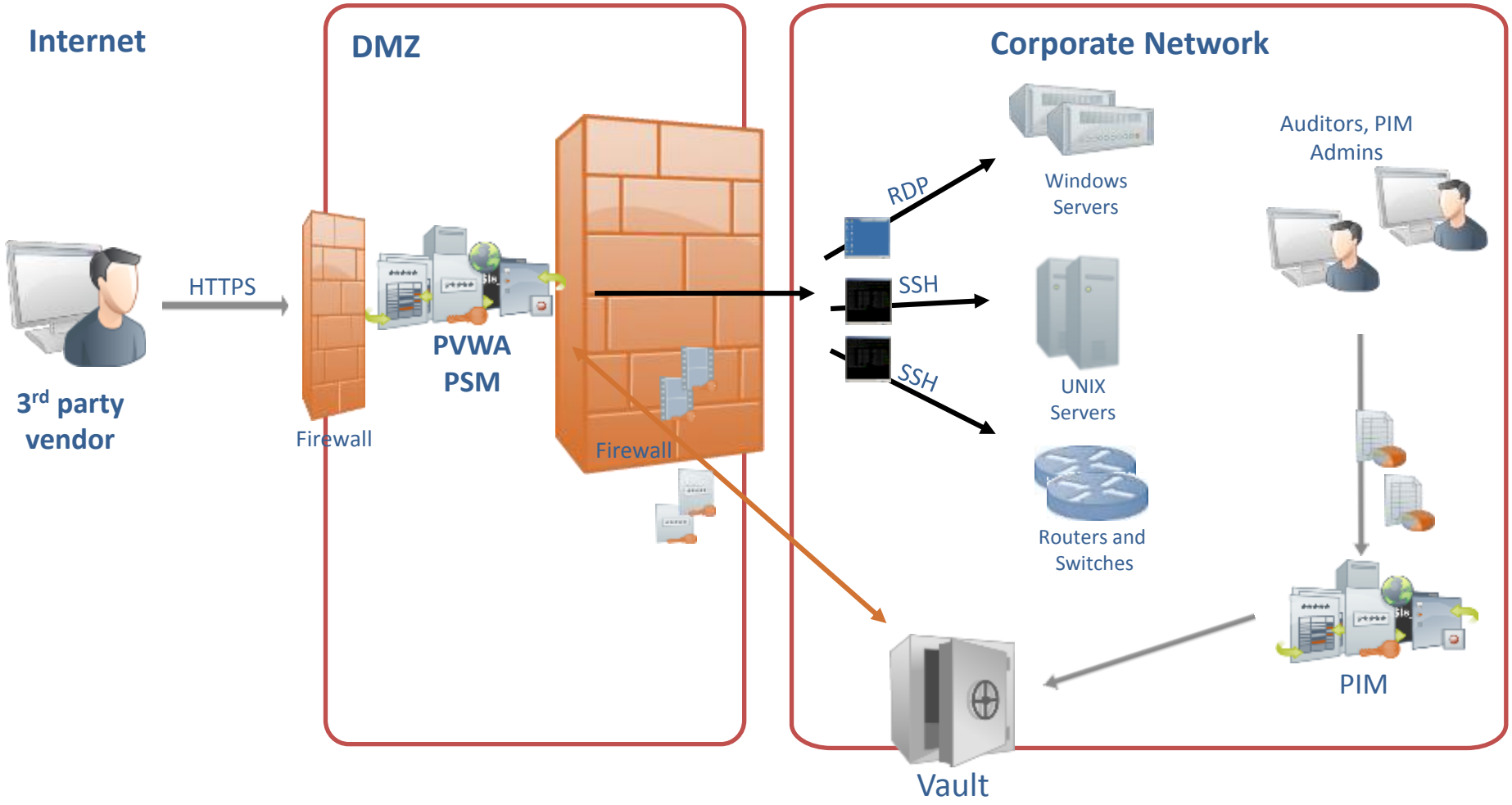
Сложно контролировать, управлять и отслеживать

Ведут к критическим рискам при неправильном использовании

CYBERARK®

QuadroSoft

PSM контролируемый удаленный доступ поставщика



CYBERARK

QuadroSoft

4 шага к эффективному контролю

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®

QuadroSoft

1. Обнаружить все привилегированные записи

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

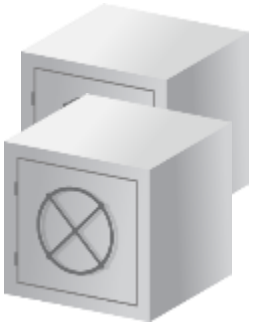
CYBERARK®

QuadroSoft

2. Защищать и управлять записями

Убедитесь, что хранилище безопасно

Внедрите процедуры проверки доступа к привилегированным записям



Упростите управление политиками за счет унифицированных мастер-политик

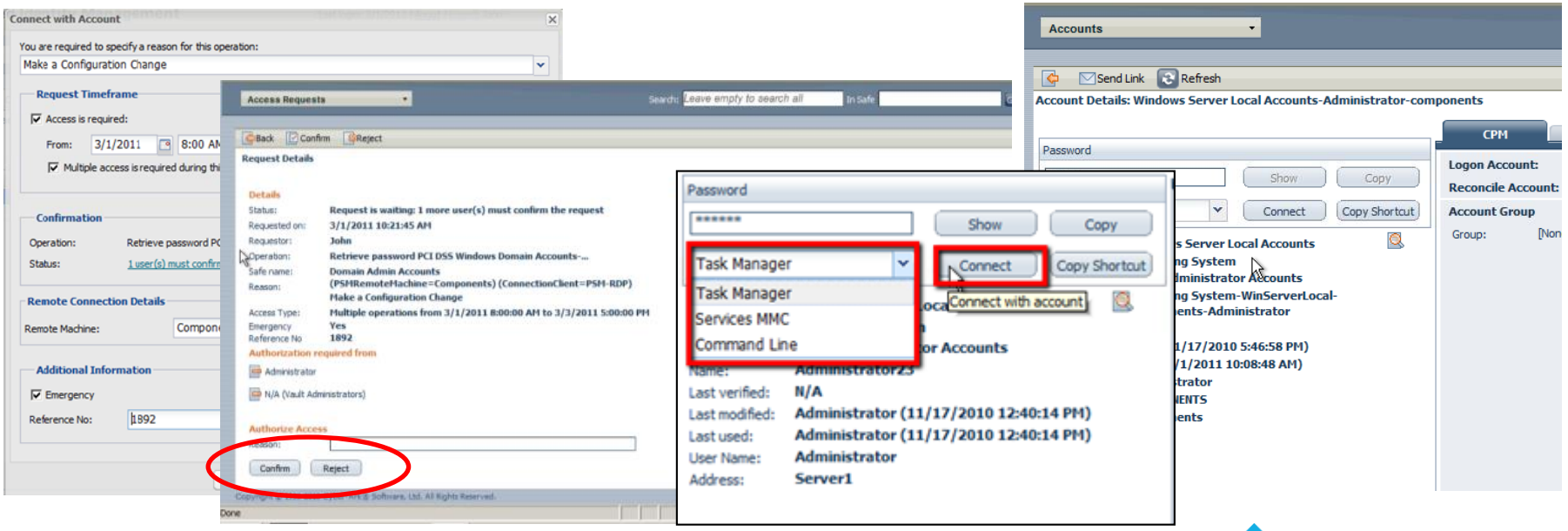
CYBERARK®

QuadroSoft

3. Контролировать, изолировать и отслеживать привилегированный доступ

Control

- Контролирует кто может подключаться к привилегированной сессии и как долго
- Предоставляет привилегированный SSO без пересылки пароля
- Обязывает использовать процесс утверждения заявки
- Внедряет строгую аутентификацию
- Дает разрешения на определенные команды



CYBERARK®

QuadroSoft

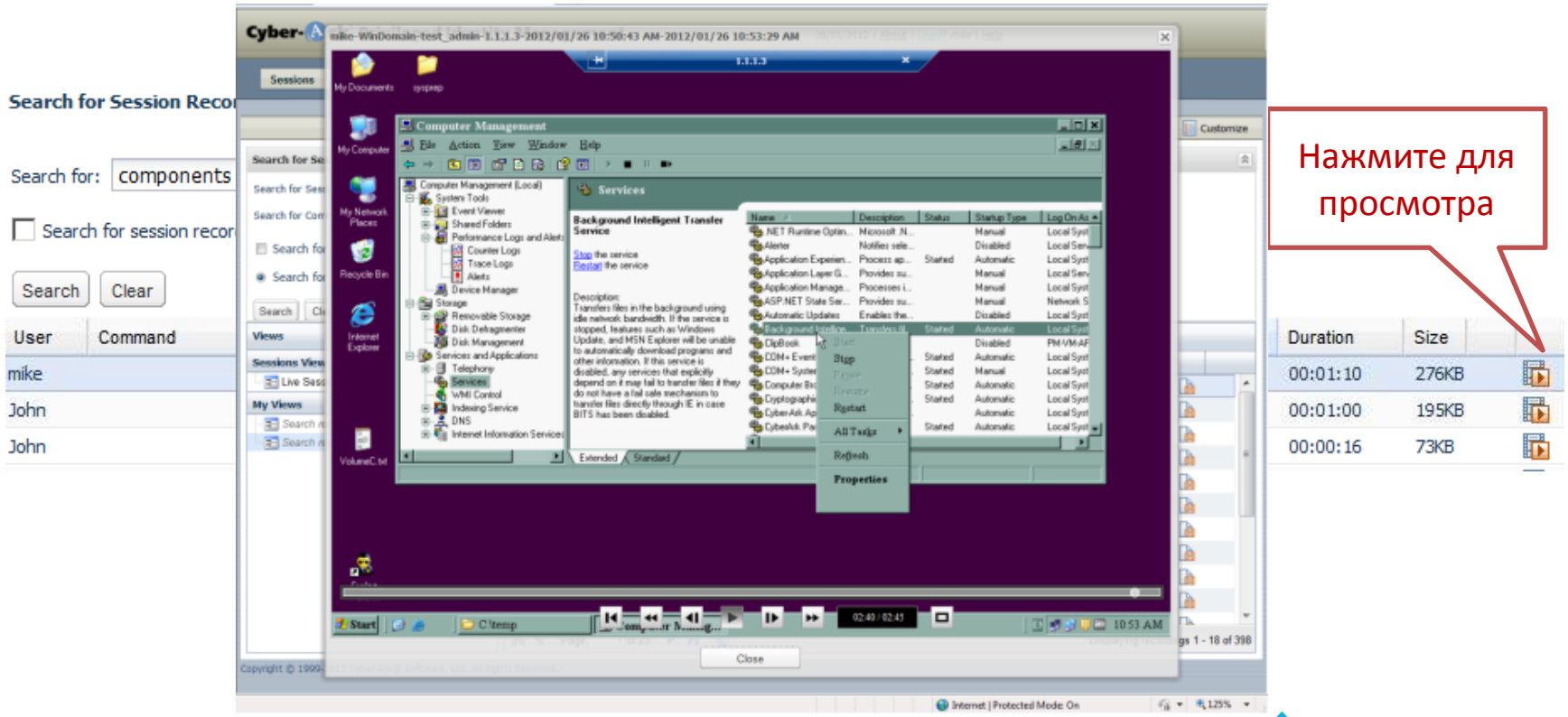
3. Контролировать, изолировать и отслеживать привилегированный доступ

Monitor

- Причинный анализ
- Короче время восстановления
- Гарантия прохождения аудита и соответствие

Что привело к падению продуктивной системы?

Какие изменения конфигурации Windows были на прошлой неделе?



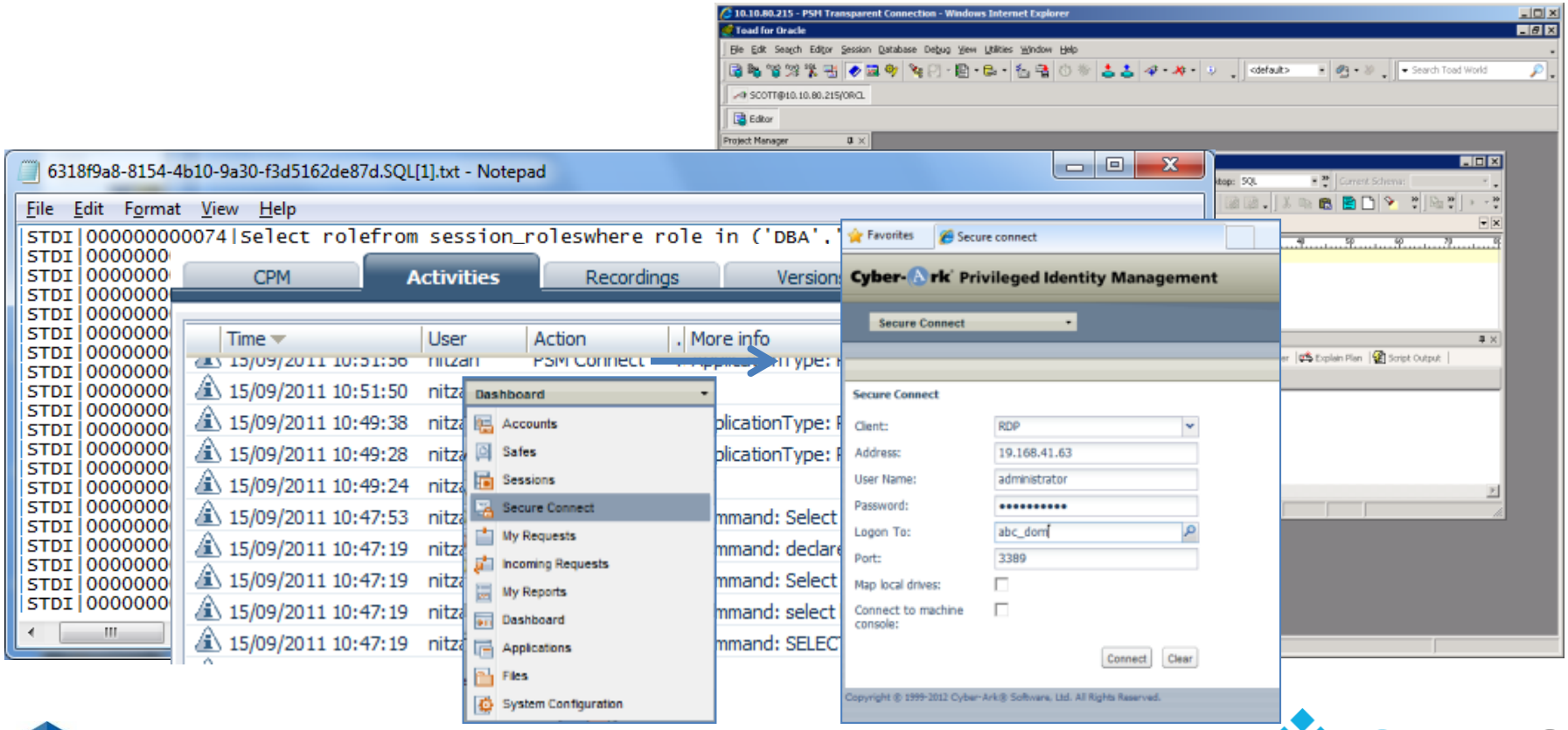
CYBERARK

QuadroSoft

3. Контролировать, изолировать и отслеживать привилегированный доступ

Monitor

- Видеозапись
- Запись текста
- Аудит по командам сессий SQL и SSH
- Мониторинг личных или неуправляемых аккаунтов

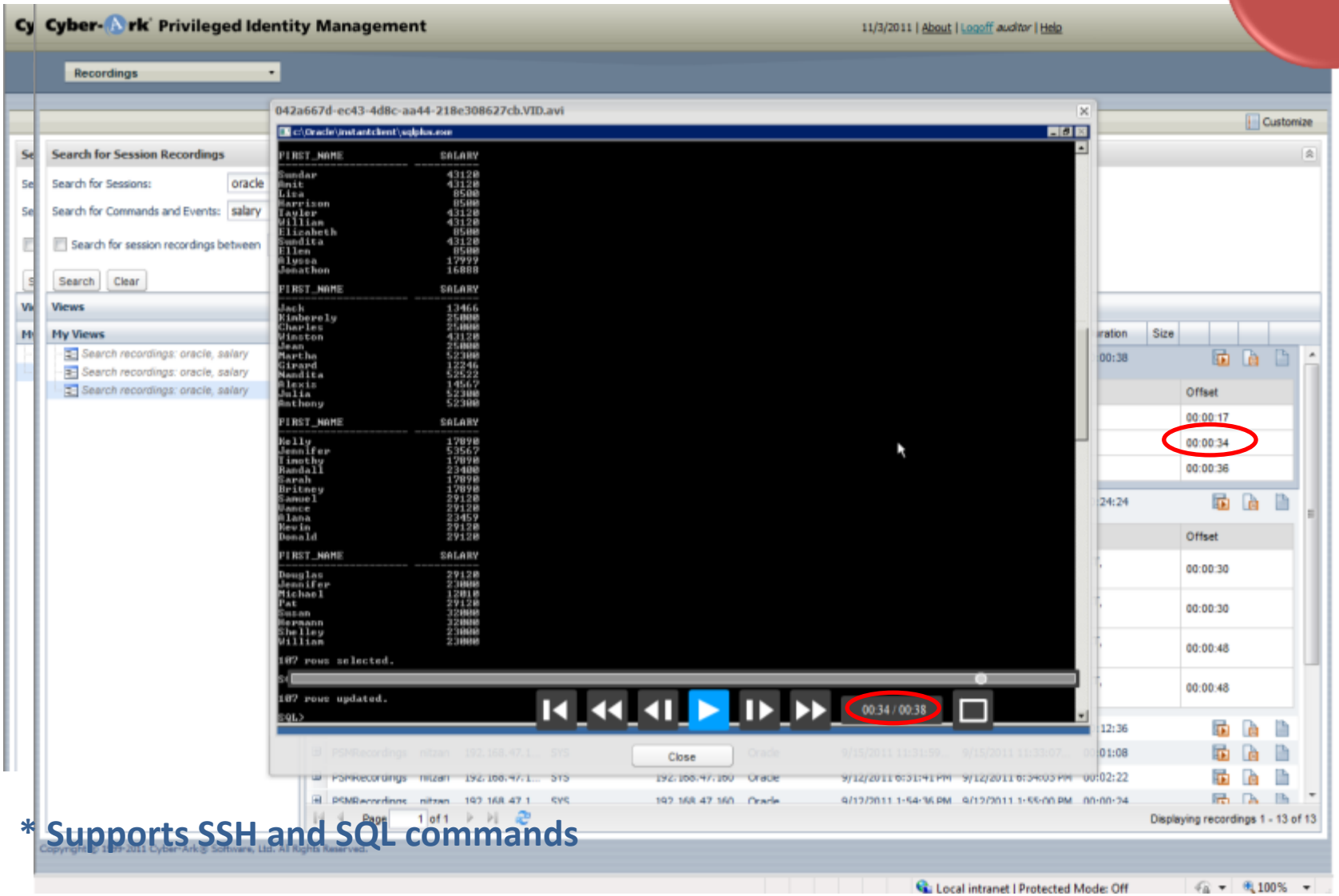


CYBERARK

QuadroSoft

3. Контролировать, изолировать и отслеживать привилегированный доступ

Monitor



* Supports SSH and SQL commands

3. Контролировать, изолировать и отслеживать привилегированный доступ

Isolate

Как снизить риск заражения систем?

Ноутбук Ивана (DBA) заражен

Прямое подключение к базе данных

Подключение через прокси

Privileged Session Manager

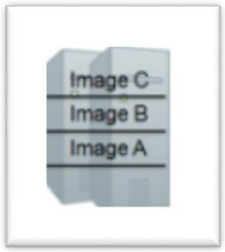
Вредоносное ПО имеет доступ к БД

Вредоносное ПО не имеет доступа к БД

Сессия выполняется на изолированном защищенном прокси, не на ноутбуке.

Сервера

Базы данных



Виртуальные машины

CYBERARK

QuadroSoft

4. Расследовать инциденты в реальном времени

Определяем атаку

Интегрируем с SIEM

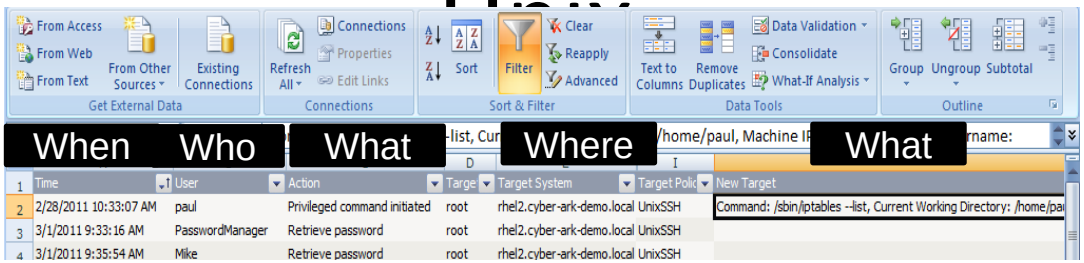
Выполняем и индексируем запись

Проводим анализ поведения администраторов и корреляция событий

CYBERARK®

QuadroSoft

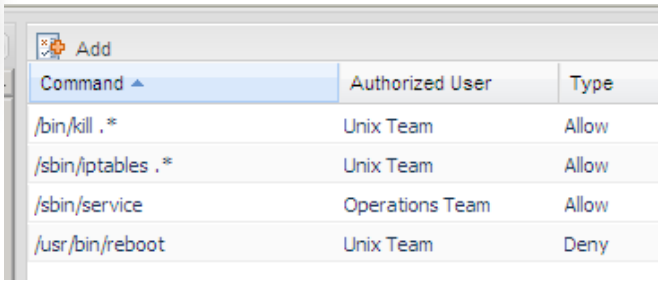
On-Demand Privilege Manager for Unix



Monitor & audit with reports and text recording

Control superuser access to the Privileged Accounts (root, oracle, app1…)

Unix /Linux Servers



Granular Access Control and Hardening

CYBERARK®

QuadroSoft

On-Demand Privilege Manager for Windows

- Objections Handling – Why Windows Built-in Security (UAC) isn't Enough?

OPM For Windows

- Standard User Account
- Granular Privilege Control
- Policy Driven via Group Policy
- Configurable End User Messages
- Privilege Monitoring and Auditing

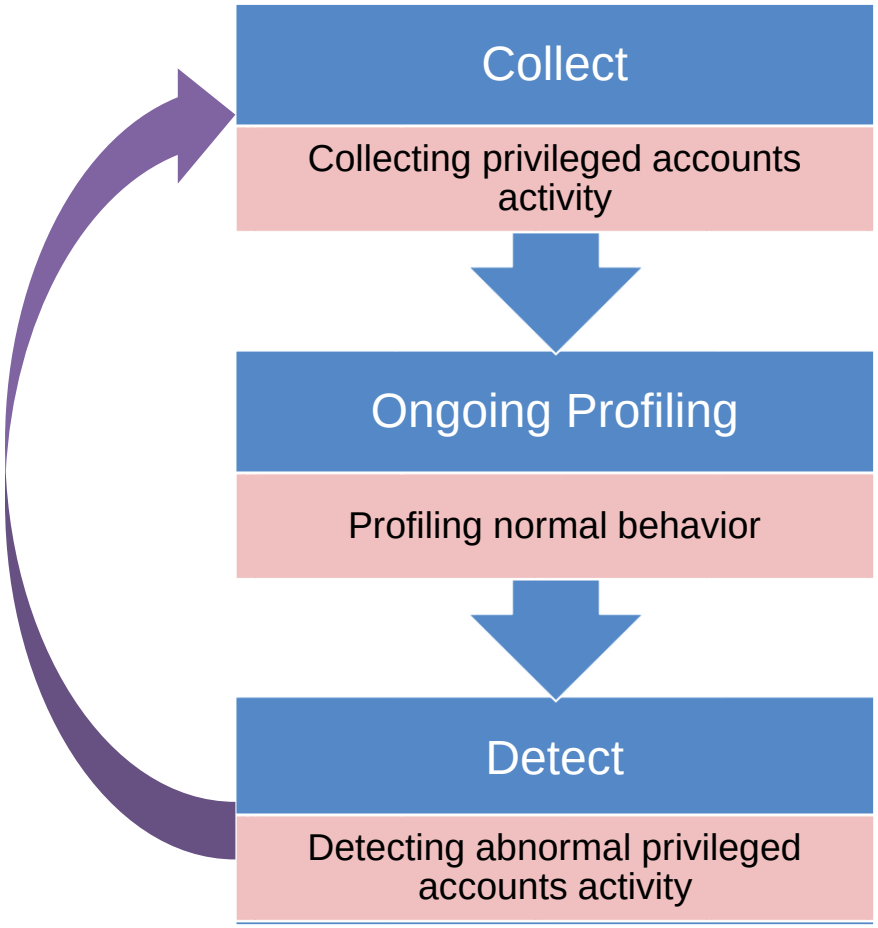
Moderately Managed

- Administrator Account Required
- Full Admin Privileges
- User Driven via UAC
- Fixed End User Messages
- No Auditing

CYBERARK®

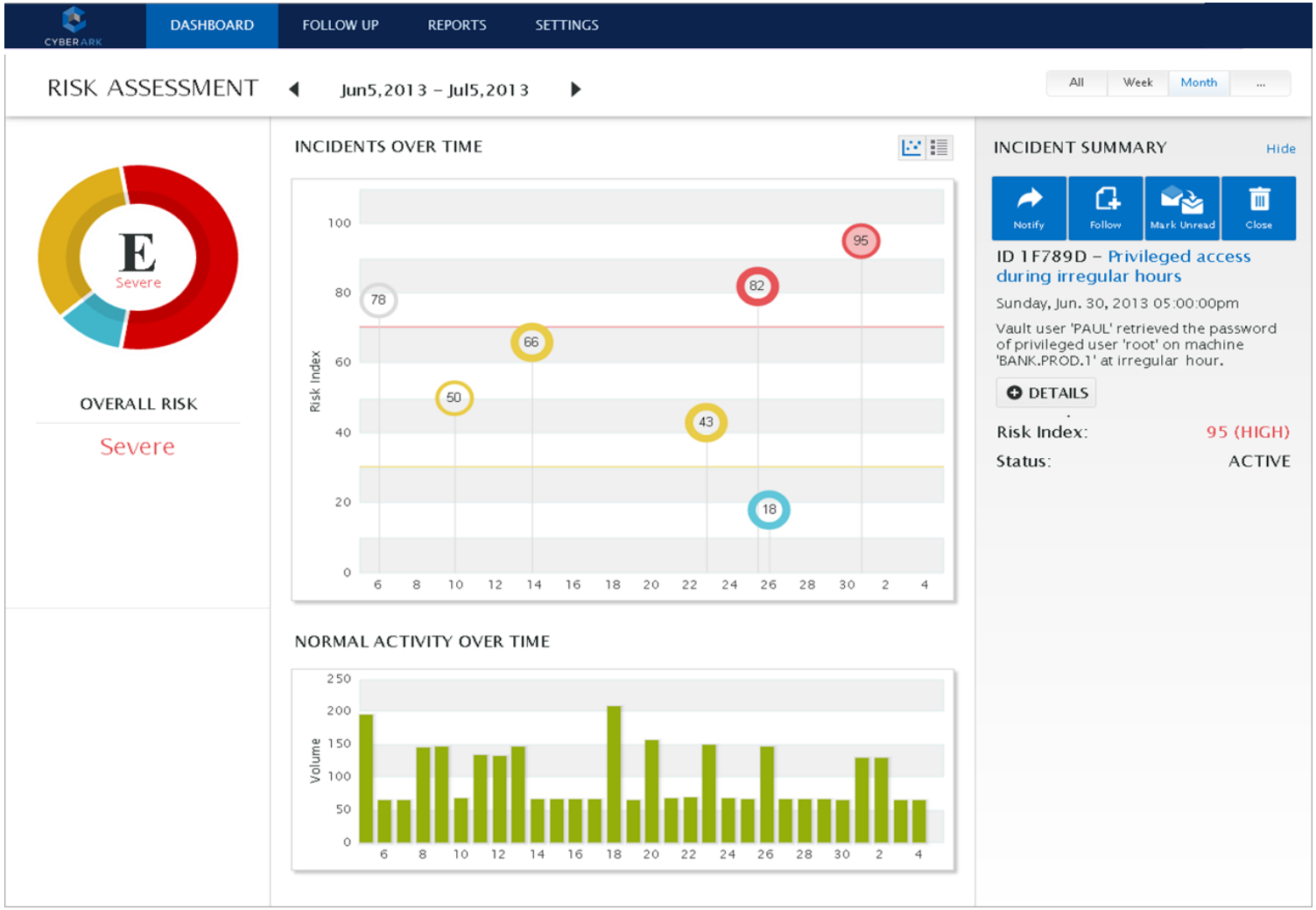
QuadroSoft

Принцип работы



CYBERARK®

QuadroSoft



CYBERARK®

QuadroSoft

SECURITY THAT EMPOWERS PEOPLE

CYBERARK®

QuadroSoft
СОВРЕМЕННЫЕ ЭФФЕКТИВНЫЕ РЕШЕНИЯ

За дополнительной информацией обращайтесь:

+375 (17) 241 77 66

info@quadrosoft.by

www.quadrosoft.by