

SECURITY THAT EMPOWERS PEOPLE



CYBERARK. PRIVILEGED ACCOUNT MANAGEMENT

• Программно-технические средства защиты

Пользователи



Средства защиты

CS&AV
Blue Coat



ORACLE Microsoft

Целевые системы



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

Analyst review

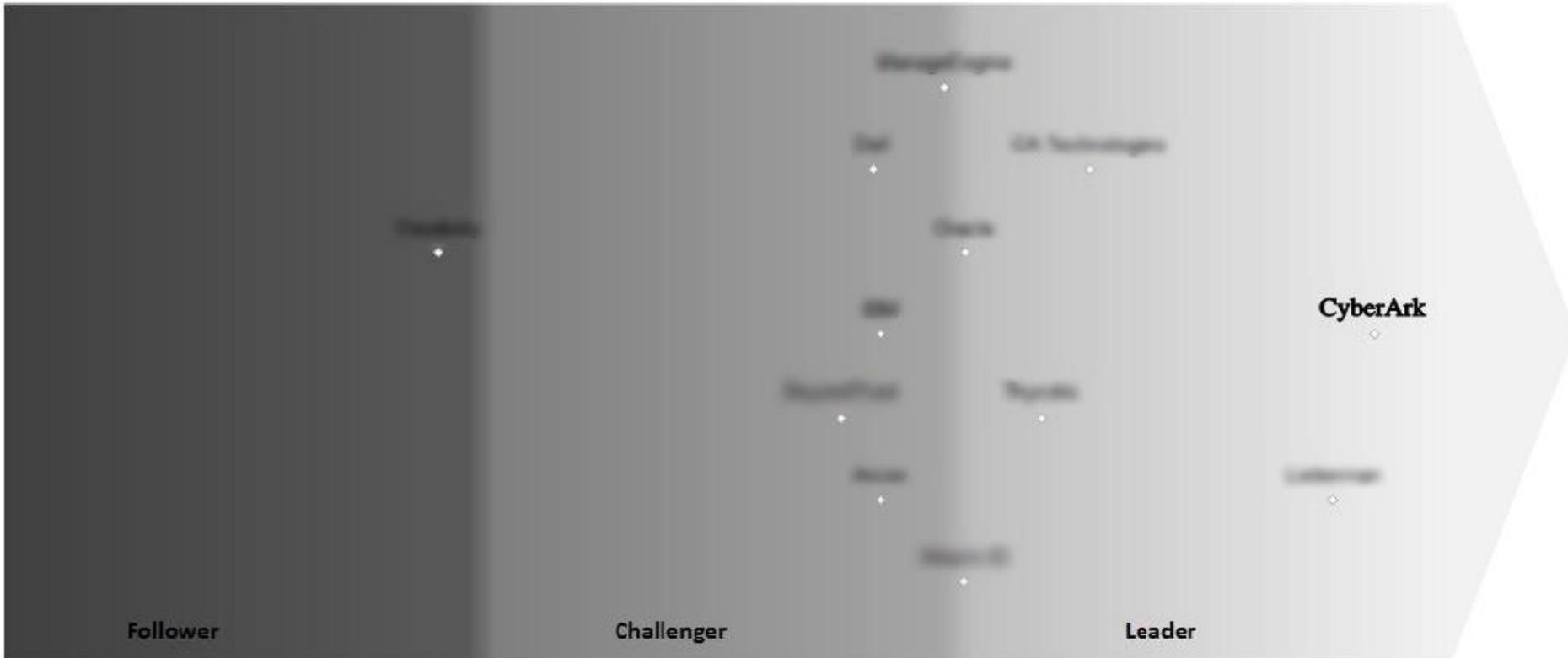


Fig. 1: The Overall Leadership rating for the Privilege Management market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.]

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

Привилегированный аккаунт: что, где и почему

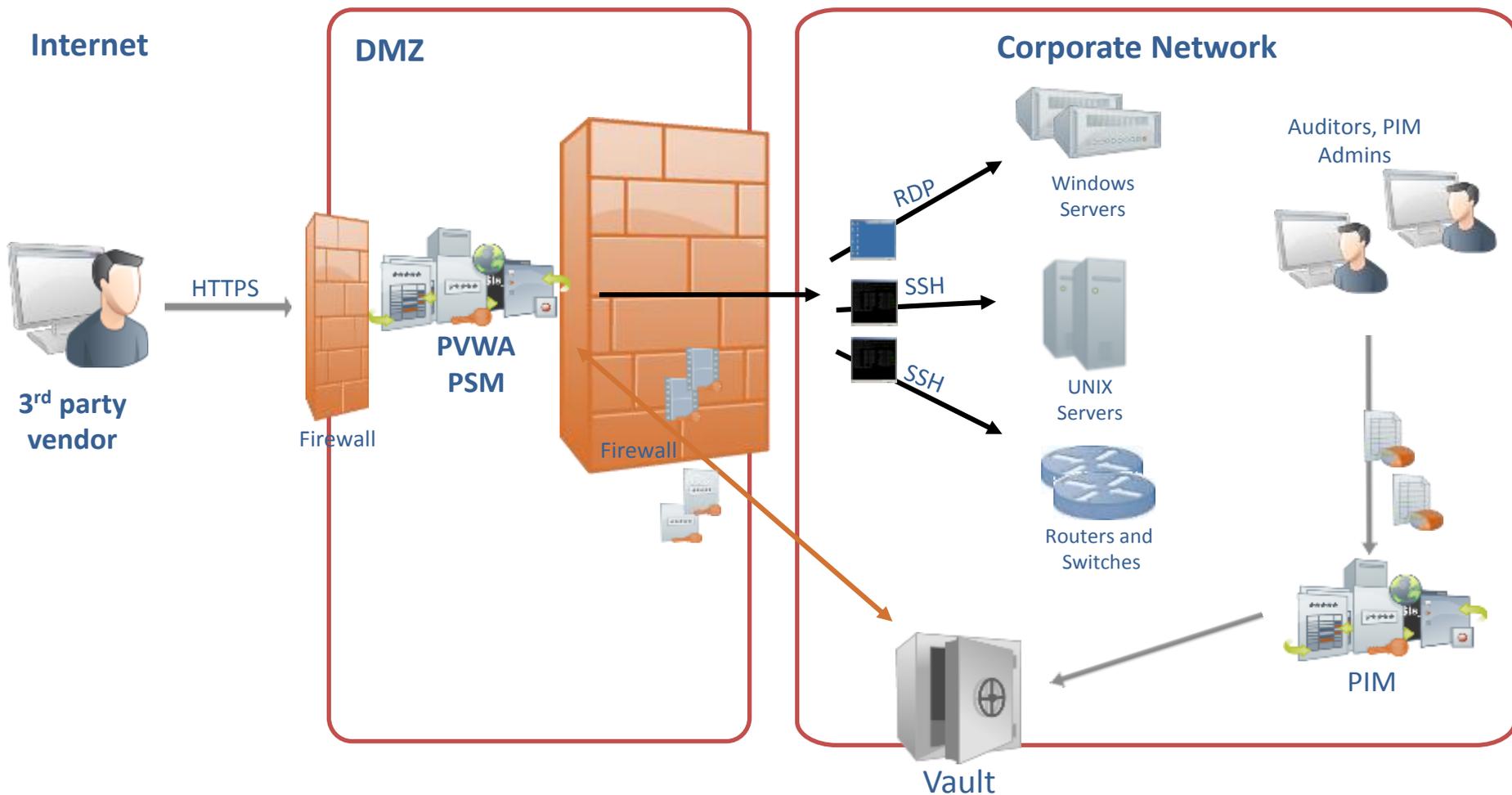
	Какие	Кем используются	Используются для
Привилегированные персональные	<ul style="list-style-type: none"> Облачные провайдеры Персональные записи с широкими привилегиями 	<ul style="list-style-type: none"> IT службы Сотрудники 	<ul style="list-style-type: none"> Привилегированные операции Доступ к критичной инф. Веб-сайты
Общие привилегированные	<ul style="list-style-type: none"> Administrator root Cisco Enable Службы Local Administrators ERP admin 	<ul style="list-style-type: none"> IT службы Системные администраторы DBA Нейлеры Разработчики Менеджер соц.медиа Мультимедиа-страницы 	<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

PSM контролируемый удаленный доступ поставщика



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

1. Обнаружить все привилегированные записи

3-ьи лица и провайдеры

Приложения

VIP бизнес-пользователи

Системные администраторы

Менеджеры социальных сетей



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

2. Защищать и управлять записями



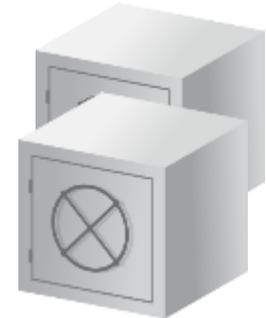
Убедитесь, что хранилище безопасно



Внедрите процедуры проверки доступа к привилегированным записям



Упростите управление политиками за счет унифицированных мастер-политик



3. Контролировать, изолировать и отслеживать привилегированный доступ



- 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

The image displays several overlapping screenshots from the CyberArk Privileged Account Management (PAM) console. The primary focus is on the 'Access Requests' and 'Password' dialog boxes. The 'Access Requests' window shows a request for 'Make a Configuration Change' by user 'John'. The 'Password' dialog box shows a dropdown menu with options like 'Task Manager', 'Services MMC', and 'Command Line', and a 'Connect' button highlighted with a red box. Other screenshots show the 'Connect with Account' dialog and the 'Accounts' list.

3. Контролировать, изолировать и отслеживать привилегированный доступ



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

*Что привело к падению продуктивной системы?
Какие изменения конфигураций Windows были на прошлой неделе?*

Duration	Size	
00:01:10	276KB	
00:01:00	195KB	
00:00:16	73KB	

Нажмите для просмотра

3. Контролировать, изолировать и отслеживать привилегированный доступ

Monitor

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

The screenshot displays the CyberArk Privileged Identity Management (PIM) interface. In the background, a Notepad window shows a SQL command: `select rolefrom session_roleswhere role in ('DBA', ...)`. The main interface features a table of activities with columns for Time, User, and Action. A 'Secure Connect' dialog box is open, showing fields for Client (RDP), Address (19.168.41.63), User Name (administrator), Password, Logon To (abc_dom), and Port (3389). A navigation menu on the left includes options like Accounts, Safes, Sessions, Secure Connect, My Requests, Incoming Requests, My Reports, Dashboard, Applications, Files, and System Configuration.

Time	User	Action	More info
15/09/2011 10:51:56	nitzan	PSIM Connect	
15/09/2011 10:51:50	nitzan		
15/09/2011 10:49:38	nitzan		
15/09/2011 10:49:28	nitzan		
15/09/2011 10:49:24	nitzan		
15/09/2011 10:47:53	nitzan		
15/09/2011 10:47:19	nitzan		

3. Контролировать, изолировать и отслеживать привилегированный доступ



042a667d-ec43-4d8c-aa44-218e308627cb.VID.avi

Search for Session Recordings

Search for Sessions: oracle

Search for Commands and Events: salary

Search for session recordings between

Search Clear

Views

My Views

- Search recordings: oracle, salary
- Search recordings: oracle, salary
- Search recordings: oracle, salary

FIRST_NAME	SALARY
Sundar	43120
Amir	43120
Lisa	85000
Harrison	85000
Taylor	43120
William	43120
Elizabeth	85000
Sudha	43120
Ellen	85000
Alyssa	17999
Jonathan	16000
FIRST_NAME SALARY	
Jack	13466
John	25000
Charles	25000
Winston	43120
Jean	25000
Martin	25000
Girard	12246
Mandita	52522
Oliver	14567
Sally	52000
Anthony	52000
FIRST_NAME SALARY	
Betty	17098
Jennifer	55567
Timothy	17098
Randall	23480
Sarah	17098
Britney	17098
Samuel	29120
Jane	29120
Alana	23459
Kevin	29120
Donald	29120
FIRST_NAME SALARY	
Douglas	29120
Jennifer	23000
Michael	12010
Pat	29120
Susan	23000
Bermann	23000
Shelley	23000
William	23000

00:34 / 00:38

Offset

00:00:17
00:00:34
00:00:36

24:24

Offset

00:00:30
00:00:30
00:00:48
00:00:48

12:36

01:08

00:02:22

00:00:34

Displaying recordings 1 - 13 of 13

* Supports SSH and SQL commands

3. Контролировать, изолировать и отслеживать привилегированный доступ

Isolate

Как снизить риск заражения систем?



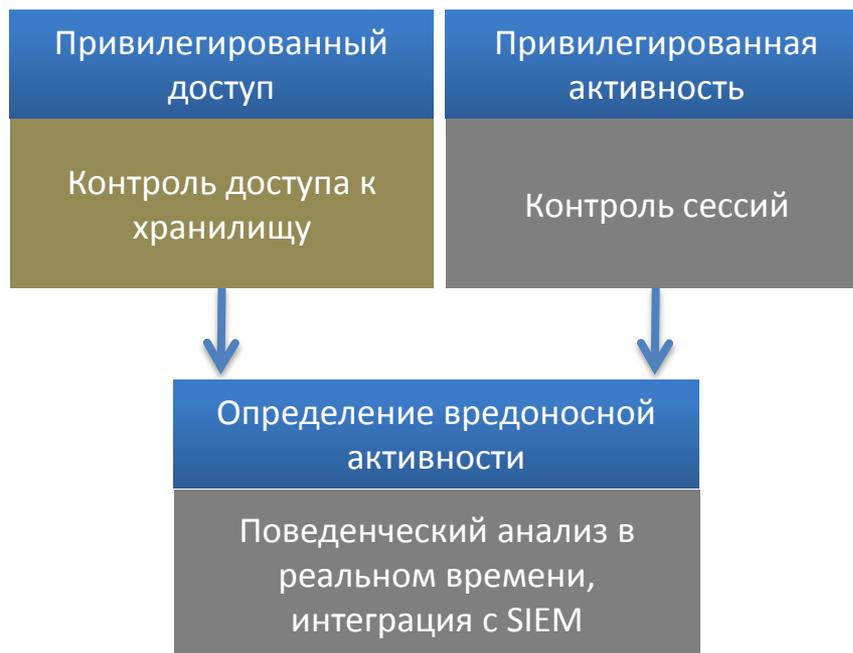
4. Расследовать инциденты в реальном времени

Определяем атаку

Интегрируем с SIEM

Выполняем и индексируем запись

Проводим анализ поведения администраторов и корреляция событий



On-Demand Privilege Manager for Unix

When	Who	What	Where	What		
1	Time	User	Action	Target System	Target Policy	New Target
2	2/28/2011 10:33:07 AM	paul	Privileged command initiated	root rhel2.cyber-ark-demo.local	UnixSSH	Command: /sbin/iptables -list, Current Working Directory: /home/pa
3	3/1/2011 9:33:16 AM	PasswordManager	Retrieve password	root rhel2.cyber-ark-demo.local	UnixSSH	
4	3/1/2011 9:35:54 AM	Mike	Retrieve password	root rhel2.cyber-ark-demo.local	UnixSSH	

Monitor & audit with reports and text recording



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



Unix /Linux Servers

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

Granular Access Control and Hardening

On-Demand Privilege Manager for Windows

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



OPM For Windows

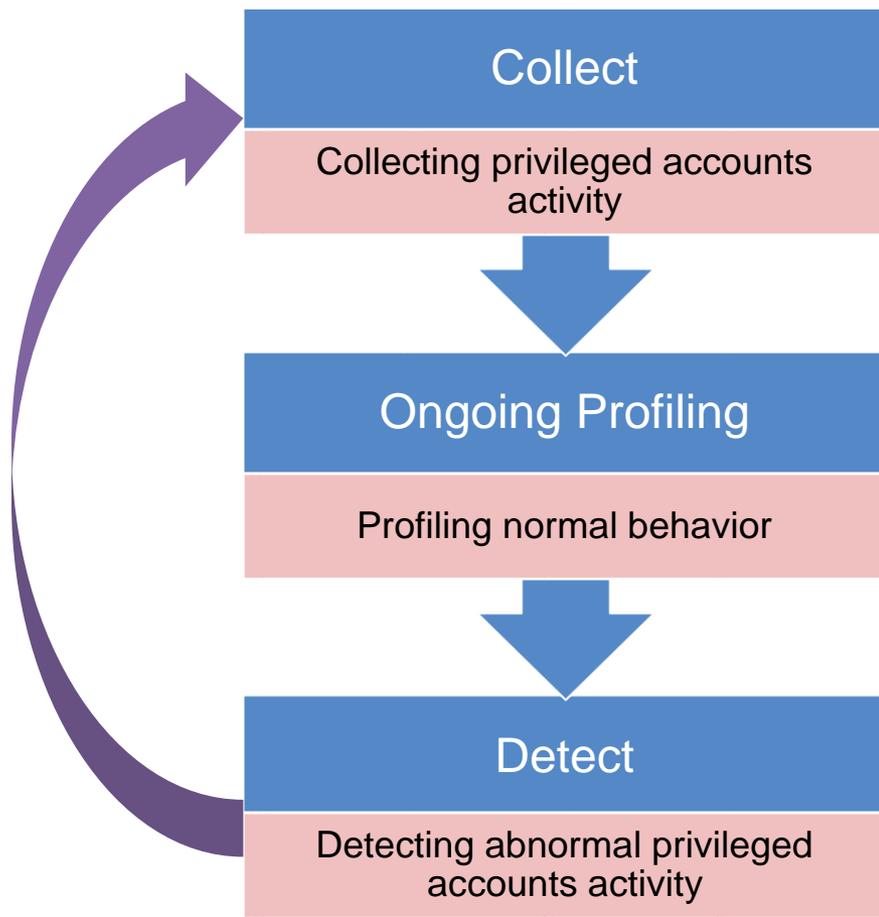
- ✓ Standard User Account
- ✓ Granular Privilege Control
- ✓ Policy Driven via Group Policy
- ✓ Configurable End User Messages
- ✓ Privilege Monitoring and Auditing



Moderately Managed

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

Принцип работы



RISK ASSESSMENT

Jun 5, 2013 - Jul 5, 2013

All Week Month ...



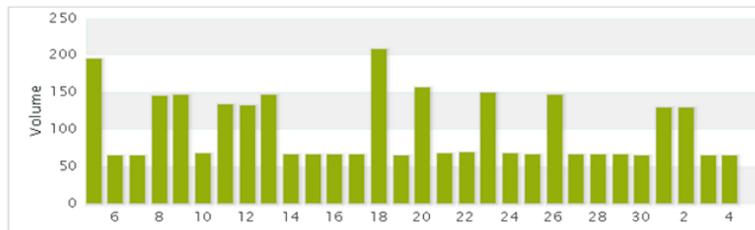
OVERALL RISK

Severe

INCIDENTS OVER TIME



NORMAL ACTIVITY OVER TIME



INCIDENT SUMMARY

Hide



ID 1 F789D - Privileged access during irregular hours

Sunday, Jun. 30, 2013 05:00:00pm

Vault user 'PAUL' retrieved the password of privileged user 'root' on machine 'BANK.PROD.1' at irregular hour.

[+ DETAILS](#)

Risk Index: 95 (HIGH)

Status: ACTIVE

SECURITY THAT EMPOWERS PEOPLE



За дополнительной информацией обращайтесь:



+375 (17) 241 77 66



info@quadrosoft.by



www.quadrosoft.by

